

Exam : CISSP

Title : Certified Information Systems Security Professional (CISSP)

Ver : 10-15-08

QUESTION 1:

All of the following are basic components of a security policy EXCEPT the

A. definition of the issue and statement of relevant terms.
B. statement of roles and responsibilities
C. statement of applicability and compliance requirements.
D. statement of performance of characteristics and requirements.

Answer: D
Policies are considered the first and highest level of documentation, from which the lower level elements of standards, procedures, and guidelines flow. This order, however, does not mean that policies are more important than the lower elements. These higher-level policies, which are the more general policies and statements, should be created first in the process for strategic reasons, and then the more tactical elements can follow. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 13

QUESTION 2:

A security policy would include all of the following EXCEPT

A. Background
B. Scope statement
C. Audit requirements
D. Enforcement

Answer: B

QUESTION 3:

Which one of the following is an important characteristic of an information security policy?

A. Identifies major functional areas of information.
B. Quantifies the effect of the loss of the information.
C. Requires the identification of information owners.
D. Lists applications that support the business function.

Answer: A
Information security policies area high-level plans that describe the goals of the procedures. Policies are not guidelines or standards, nor are they procedures or controls. Policies describe security in general terms, not specifics. They provide the blueprints for an overall security program just as a specification defines your next product - Roberta Bragg CISSP Certification Training Guide (que) pg 206

QUESTION 4:

Ensuring the integrity of business information is the PRIMARY concern of

A. Encryption Security
B. Procedural Security.
C. Logical Security
D. On-line Security

Answer: B
Procedures are looked at as the lowest level in the policy chain because they are closest to the computers and provide detailed steps for configuration and installation issues. They provide the steps to actually implement the statements in the policies, standards, and guidelines...Security procedures, standards, measures, practices, and policies cover a number of different subject areas. - Shon Harris All-in-one CISSP Certification Guide pg 44-45

QUESTION 5:

Which of the following would be the first step in establishing an information security program?
A.) Adoption of a corporate information security policy statement
B.) Development and implementation of an information security standards manual
C.) Development of a security awareness-training program
D.) Purchase of security access control software

Answer: A

QUESTION 6:

Which of the following department managers would be best suited to oversee the development of an information security policy?
A.) Information Systems
B.) Human Resources
C.) Business operations
D.) Security administration

Answer: C

QUESTION 7:

What is the function of a corporate information security policy?

A. Issue corporate standard to be used when addressing specific security problems.
B. Issue guidelines in selecting equipment, configuration, design, and secure operations.
C. Define the specific assets to be protected and identify the specific tasks which must be completed to secure them.

D. Define the main security objectives which must be achieved and the security framework to meet business objectives.

Answer: D
Information security policies are high-level plans that describe the goals of the procedures or controls. Policies describe security in general, not specifics. They provide the blueprint fro an overall security program just as a specification defines your next product. - Roberta Bragg CISSP Certification Training Guide (que) pg 587

QUESTION 8:

Why must senior management endorse a security policy?

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.
D. So that they can be held legally accountable.

Answer: A
This really does not a reference as it should be known. Upper management is legally accountable (up to 290 million
fine). External organizations answer is not really to pertinent (however it stated that other organizations will respect
a BCP and disaster recover plan). Employees need to be bound to the policy regardless of who signs it but it gives
validity. Ownership is the correct answer in this statement. However, here is a reference. "Fundamentally important
to any security program's success us the senior management's high-level statement of commitment to the information security policy process and a senior management's understanding of how important security controls
and protections are to the enterprise's continuity. Senior management must be aware of the importance of security
implementation to preserve the organization's viability (and for their own 'due care' protection) and must publicly
support that process throughout the enterprise." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 13

QUESTION 9:

In which one of the following documents is the assignment of individual roles and responsibilities MOST appropriately defined?

A. Security policy
B. Enforcement guidelines
C. Acceptable use policy
D. Program manual

Answer: C
An acceptable use policy is a document that the employee signs in which the expectations, roles and responsibilities are outlined.
Issue -specific policies address specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply to these security issues. - Shon Harris All-in-one CISSP Certification Guide pg 62

QUESTION 10:

Which of the following defines the intent of a system security policy?

A. A definition of the particular settings that have been determined to provide optimum security.
B. A brief, high-level statement defining what is and is not permitted during the operation of the system.
C. A definition of those items that must be excluded on the system.
D. A listing of tools and applications that will be used to protect the system.

Answer: A
"A system-specific policy presents the management's decisions that are closer to the actual computers, networks,
applications, and data. This type of policy can provide an approved software list, which contains a list of applications that can be installed on individual workstations. This policy can describe how databases are to be protected, how computers are to be locked down, and how firewall, intrusion diction systems, and scanners are to be
employed." Pg 93 Shon Harris CISSP All-In-One Certification Exam Guide

---

QUESTION 11:

When developing an information security policy, what is the FIRST step that should be taken?

A. Obtain copies of mandatory regulations.
B. Gain management approval.
C. Seek acceptance from other departments.
D. Ensure policy is compliant with current working practices.

Answer: B

QUESTION 12:

Which one of the following should NOT be contained within a computer policy?

A. Definition of management expectations.
B. Responsibilities of individuals and groups for protected information.
C. Statement of senior executive support.
D. Definition of legal and regulatory controls.

Answer: B

QUESTION 13:

Which one of the following is NOT a fundamental component of a Regulatory Security Policy?

A. What is to be done.
B. When it is to be done.
C. Who is to do it.
D. Why is it to be done

Answer: C
Regulatory Security policies are mandated to the organization but it up to them to implement it. "Regulatory - This policy is written to ensure that the organization is following standards set by a specific industry and is regulated by law. The policy type is detailed in nature and specific to a type of industry. This is used in financial institutions, health care facilities, and public utilities." - Shon Harris All-in-one CISSP Certification Guide pg 93-94

QUESTION 14:

Which one of the following statements describes management controls that are instituted to implement a security policy?

A. They prevent users from accessing any control function.
B. They eliminate the need for most auditing functions.
C. They may be administrative, procedural, or technical.
D. They are generally inexpensive to implement.

Answer: C
Administrative, physical, and technical controls should be utilized to achieve the management's directives. - Shon Harris All-in-one CISSP Certification Guide pg 60

QUESTION 15:

Which must bear the primary responsibility for determining the level of protection needed for information systems resources?
A.) IS security specialists
B.) Senior Management
C.) Seniors security analysts
D.) system auditors

Answer: B

QUESTION 16:

Which of the following choices is NOT part of a security policy?
A.) definition of overall steps of information security and the importance of security
B.) statement of management intend, supporting the goals and principles of information security
C.) definition of general and specific responsibilities for information security management
D.) description of specific technologies used in the field of information security

Answer: D

QUESTION 17:

In an organization, an Information Technology security function should:
A.) Be a function within the information systems functions of an organization
B.) Report directly to a specialized business unit such as legal, corporate security or insurance
C.) Be lead by a Chief Security Officer and report directly to the CEO
D.) Be independent but report to the Information Systems function

Answer: C

QUESTION 18:

Which of the following embodies all the detailed actions that personnel are required to follow?
A.) Standards
B.) Guidelines
C.) Procedures
D.) Baselines

Answer: C

QUESTION 19:

A significant action has a state that enables actions on an ADP system to be traced to individuals who may then be held responsible. The action does NOT include:

A. Violations of security policy.
B. Attempted violations of security policy.
C. Non-violations of security policy.
D. Attempted violations of allowed actions.

Answer: D

Explanation:
Significant action: The quality or state that enables actions on an ADP system to be traced to individuals who may then be held responsible. These actions include violations and attempted violations of the security policy, as well as allowed actions.

QUESTION 20:

Network Security is a
A.) Product
B.) protocols
C.) ever evolving process
D.) quick-fix solution

Answer: C

QUESTION 21:

Security is a process that is:

A. Continuous
B. Indicative
C. Examined
D. Abnormal

Answer: A

Explanation:
Security is a continuous process; as such you must closely monitor your systems on a regular basis. Log files are usually a good way to find an indication of abnormal activities. However some care must be exercise as to what will be logged and how the logs are protected. Having corrupted logs is about as good as not having logs at all.

QUESTION 22:

What are the three fundamental principles of security?
A.) Accountability, confidentiality, and integrity
B.) Confidentiality, integrity, and availability
C.) Integrity, availability, and accountability
D.) Availability, accountability, and confidentiality

Answer: B

QUESTION 23:

Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?
A.) Communications security management and techniques
B.) Networks security management and techniques
C.) Clients security management and techniques
D.) Servers security management and techniques

Answer: A

QUESTION 24:

Making sure that the data is accessible when and where it is needed is which of the following?
A.) Confidentiality
B.) integrity
C.) acceptability
D.) availability

Answer: D

QUESTION 25:

Which of the following describes elements that create reliability and stability in networks and systems and which assures that connectivity is accessible when needed?
A.) Availability
B.) Acceptability
C.) Confidentiality
D.) Integrity

Answer: A

QUESTION 26:

Most computer attacks result in violation of which of the following security properties?

A. Availability
B. Confidentiality
C. Integrity and control
D. All of the choices.

Answer: D

Explanation:
Most computer attacks only corrupt a system's security in very specific ways. For example, certain attacks may enable a hacker to read specific files but don't allow alteration of any system components. Another attack may allow a hacker to shut down certain system components but doesn't allow access to any files. Despite the varied capabilities of computer attacks, they usually result in violation of only four different security properties: availability, confidentiality, integrity, and control.

QUESTION 27:

Which of the following are objectives of an information systems security program?

A. Threats, vulnerabilities, and risks
B. Security, information value, and threats
C. Integrity, confidentiality, and availability.
D. Authenticity, vulnerabilities, and costs.

Answer: C
There are several small and large objectives of a security program, but the main three principles in all programs are confidentiality, integrity, and availability. These are referred to as the CIA triad. - Shon Harris All-in-one CISSP Certification Guide pg 62

QUESTION 28:

An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:
A.) Netware availability
B.) Network availability
C.) Network acceptability
D.) Network accountability

Answer: B

QUESTION 29:

The Structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, and authentication, and confidentiality for transmissions over private and public communications networks and media includes:
A.) The Telecommunications and Network Security domain
B.) The Telecommunications and Netware Security domain
C.) The Technical communications and Network Security domain
D.) The Telnet and Security domain

Answer: A
The Telecommunications, Network, and Internet Security Domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media." Pg 515 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 30:

Which one of the following is the MOST crucial link in the computer security chain?

A. Access controls
B. People

C. Management
D. Awareness programs

Answer: C

QUESTION 31:

The security planning process must define how security will be managed, who will be responsible, and

A. Who practices are reasonable and prudent for the enterprise.
B. Who will work in the security department.
C. What impact security will have on the intrinsic value of data.
D. How security measures will be tested for effectiveness.

Answer: D

QUESTION 32:

Information security is the protection of data. Information will be protected mainly based on:

A. Its sensitivity to the company.
B. Its confidentiality.
C. Its value.
D. All of the choices.

Answer: D

Explanation:
Information security is the protection of data against accidental or malicious disclosure, modification, or destruction. Information will be protected based on its value, confidentiality, and/or sensitivity to the company, and the risk of loss or compromise. At a minimum, information will be update-protected so that only authorized individuals can modify or erase the information.

QUESTION 33:

Organizations develop change control procedures to ensure that

A. All changes are authorized, tested, and recorded.
B. Changes are controlled by the Policy Control Board (PCB).
C. All changes are requested, scheduled, and completed on time.
D. Management is advised of changes made to systems.

Answer: A

"Change Control: Changes must be authorized, tested, and recorded. Changed systems may require re-certification and re-accreditation." Pg 699 Shon Harris: All-in-One CISSP Certification

---

QUESTION 34:

Within the organizational environment, the security function should report to an organizational level that

A. Has information technology oversight.
B. Has autonomy from other levels.
C. Is an external operation.
D. Provides the internal audit function.

Answer: B

QUESTION 35:

What is the MAIN purpose of a change control/management system?

A. Notify all interested parties of the completion of the change.
B. Ensure that the change meets user specifications.
C. Document the change for audit and management review.
D. Ensure the orderly processing of a change request.

Answer: C

QUESTION 36:

Which of the following is most relevant to determining the maximum effective cost of access control?
A.) the value of information that is protected
B.) management's perceptions regarding data importance
C.) budget planning related to base versus incremental spending.
D.) the cost to replace lost data

Answer: A

QUESTION 37:

Which one of the following is the MAIN goal of a security awareness program when addressing senior management?

A. Provide a vehicle for communicating security procedures.
B. Provide a clear understanding of potential risk and exposure.
C. Provide a forum for disclosing exposure and risk analysis.
D. Provide a forum to communicate user responsibilities.

Answer: B

Explanation:
When the Security Officer is addressing Senior Management, the focus would not be on user responsibilities, it would be on making sure the Senior Management have a clear understanding of the risk and potential liability is
Not D: Item D would be correct in a situation where Senior Management is addressing organizational staff.

QUESTION 38:

In developing a security awareness program, it is MOST important to

A. Understand the corporate culture and how it will affect security.
B. Understand employees preferences for information security.
C. Know what security awareness products are available.
D. Identify weakness in line management support.

Answer: A
The controls and procedures of a security program should reflect the nature of the data being processed...These different types of companies would also have very different cultures. For a security awareness program to be effective, these considerations must be understood and the program should be developed in a fashion that makes sense per environment - Shon Harris All-in-one CISSP Certification Guide pg 109

QUESTION 39:

Which of the following would be best suited to provide information during a review of the controls over the process of defining IT service levels?
A.) Systems programmer
B.) Legal stuff
C.) Business unit manager
D.) Programmer

Answer: C

QUESTION 40:

Which of the following best explains why computerized information systems frequently fail to meet the needs of users?
A.) Inadequate quality assurance (QA) tools
B.) Constantly changing user needs
C.) Inadequate user participation in defining the system's requirements
D.) Inadequate project management.

Answer: C

QUESTION 41:

Which of the following is not a compensating measure for access violations?
A.) Backups
B.) Business continuity planning
C.) Insurance
D.) Security awareness

Answer: D

QUESTION 42:

Risk analysis is MOST useful when applied during which phase of the system development process?
A.) Project identification
B.) Requirements definition
C.) System construction
D.) Implementation planning

Answer: A
Reference: pg 684 Shon Harris: All-in-One CISSP Certification

QUESTION 43:

Which one of the following is not one of the outcomes of a vulnerability analysis?
A.) Quantative loss assessment
B.) Qualitative loss assessment
C.) Formal approval of BCP scope and initiation document
D.) Defining critical support areas

Answer: C

QUESTION 44:

Which of the following is not a part of risk analysis?
A.) Identify risks
B.) Quantify the impact of potential threats
C.) Provide an economic balance between the impact of the risk and the cost of the associated countermeasures
D.) Choose the best countermeasure

Answer: D

QUESTION 45:

A new worm has been released on the Internet. After investigation, you have not been able to determine if you are at risk of exposure. Management is concerned as they have heard that a number of their counterparts are being affected by the worm. How could you determine if you are at risk?

A. Evaluate evolving environment.
B. Contact your anti-virus vendor.
C. Discuss threat with a peer in another organization.
D. Wait for notification from an anti-virus vendor.

Answer: B

QUESTION 46:

When conducting a risk assessment, which one of the following is NOT an acceptable social engineering practice?

A. Shoulder surfing
B. Misrepresentation
C. Subversion
D. Dumpster diving

Answer: A

Explanation:
Shoulder Surfing: Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing password files, and social engineering. These topics will be address more in-depth in later chapters, but shoulder surfing is when a person looks over another person's shoulder and watches keystrokes or data as it appears on the screen. Social engineering is tricking another person into sharing confidential information by posing as an authorized individual to that information. Shon Harris: CISSP Certification pg. 63. Shoulder surfing is not social engineering.

QUESTION 47:

Which one of the following risk analysis terms characterizes the absence or weakness of a risk-reducing safegaurd?

A. Threat
B. Probability
C. Vulnerability
D. Loss expectancy

Answer: C
A weakness in system security procedures, system design, implementation, internal controls, and so on that could be exploited to violate system security policy. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 927

QUESTION 48:

Risk is commonly expressed as a function of the

A. Systems vulnerabilities and the cost to mitigate.
B. Types of countermeasures needed and the system's vulnerabilities.
C. Likelihood that the harm will occur and its potential impact.
D. Computer system-related assets and their costs.

Answer: C
The likelihood of a threat agent taking advantage of a vulnerability. A risk is the loss potential, or probability, that a threat will exploit a vulnerability. - Shon Harris All-in-one CISSP Certification Guide pg 937

QUESTION 49:

How should a risk be handled when the cost of the countermeasures outweighs the cost of the risk?
A.) Reject the risk
B.) Perform another risk analysis
C.) Accept the risk
D.) Reduce the risk

Answer: C

QUESTION 50:

Which of the following is an advantage of a qualitative over quantitative risk analysis?

A.) It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B.) It provides specific quantifiable measurements of the magnitude of the impacts
C.) It makes cost-benefit analysis of recommended controls easier

Answer: A

QUESTION 51:

The absence or weakness in a system that may possibly be exploited is called a(n)?
A.) Threat
B.) Exposure
C.) Vulnerability
D.) Risk

Answer: C

QUESTION 52:

What tool do you use to determine whether a host is vulnerable to known attacks?

A. Padded Cells
B. Vulnerability analysis
C. Honey Pots
D. IDS

Answer: B

Explanation:
Vulnerability analysis (also known as vulnerability assessment) tools test to determine whether a network or host is vulnerable to known attacks. Vulnerability assessment represents a special case of the intrusion detection process. The information sources used are system state attributes and outcomes of attempted attacks. The information sources are collected by a part of the assessment engine. The timing of analysis is interval-based or batch-mode, and the type of analysis is misuse detection. This means that vulnerability assessment systems are essentially batch mode misuse detectors that operate on system state information and results of specified test routines.

QUESTION 53:

Which of the following statements pertaining to ethical hacking is incorrect?
A.) An organization should use ethical hackers who do not sell auditing, consulting, hardware, software, firewall, hosting, and/or networking services
B.) Testing should be done remotely
C.) Ethical hacking should not involve writing to or modifying the target systems
D.) Ethical hackers should never use tools that have potential of exploiting vulnerabilities in the organizations IT system.

Answer: D

QUESTION 54:

Why would an information security policy require that communications test equipment be controlled?
A.) The equipment is susceptible to damage
B.) The equipment can be used to browse information passing on a network
C.) The equipment must always be available for replacement if necessary
D.) The equipment can be used to reconfigure the network multiplexers

Answer: B

QUESTION 55:

Management can expect penetration tests to provide all of the following EXCEPT

A. identification of security flaws
B. demonstration of the effects of the flaws
C. a method to correct the security flaws.
D. verification of the levels of existing infiltration resistance

Answer: C

Explanation:
Not B: It is not the objective of the pen tester to supply a method on how to correct the flaws. In fact management may decide to accept the risk and not repair the flaw. They may be able to demonstrate the effects of a flaw - especially if they manage to clobber a system!
Penetration testing is a set of procedures designed to test and possibly bypass security controls of a system. Its goal is to measure an organization's resistance to an attack and to uncover any weaknesses within the environment...The result of a penetration test is a report given to management describing the list of vulnerabilities that were identified and the severity of those vulnerabilities. From here, it is up to management to determine how the vulnerabilities are dealt with and what countermeasures are implemented. - Shon Harris All-in-one CISSP Certification Guide pg 837-839

QUESTION 56:

Which one of the following is a characteristic of a penetration testing project?

A. The project is open-ended until all known vulnerabilities are identified.
B. The project schedule is plotted to produce a critical path.
C. The project tasks are to break into a targeted system.
D. The project plan is reviewed with the target audience.

Answer: C
"One common method to test the strength of your security measures is to perform penetration testing. Penetration testing is a vigorous attempt to break into a protected network using any means necessary." Pg 430 Tittel: CISSP Study Guide

---

QUESTION 57:

Which one of the following is the PRIMARY objective of penetration testing?

A. Assessment
B. Correction
C. Detection
D. Protection

Answer: C

Explanation:
Its goal is to measure an organization's resistance to an attack and to uncover any weakness within the environment...The result of a penetration test is a report given to management describing the list of vulnerabilities that were identified and the severity of those vulnerabilities. - Shon Harris All-in-one CISSP Certification Guide pg 837-839
Not A: Assessment would imply management deciding whether they can live with a given vulnerability.

QUESTION 58:

Open box testing, in the Flaw Hypothesis Methodology of Penetration Testing applies to the analysis of

A. Routers and firewalls
B. Host-based IDS systems
C. Network-based IDS systems
D. General purpose operating systems

Answer: D

Explanation:
Flaw Hypothesis Methodology - A system analysis and penetration technique where specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw actually exists and, assuming a flaw does exist, on the ease of exploiting it and on the extent of control or compromise it would provide. The prioritized list is used to direct the actual testing of the system.
http://www.kernel.org/pub/linux/libs/security/Orange-Linux/refs/Orange/Orange0-5.html

---

QUESTION 59:

What is the FIRST step that should be considered in a penetration test?

A. The approval of change control management.
B. The development of a detailed test plan.
C. The formulation of specific management objectives.
D. The communication process among team members.

Answer: C

Explanation:
The type of penetration test depends on the organization, its security objectives, and the management's goals. - Shon Harris All-in-one CISSP Certification Guide pg 838

QUESTION 60:

Penetration testing will typically include

A. Generally accepted auditing practices.
B. Review of Public Key Infrastructure (PKI) digital certificate, and encryption.
C. Social engineering, configuration review, and vulnerability assessment.
D. Computer Emergency Response Team (CERT) procedures.

Answer: C

QUESTION 61:

Which of the following is not a valid reason to use external penetration service firms rather than corporate resources?
A.) They are more cost-effective
B.) They offer a lack of corporate bias
C.) They use highly talented ex-hackers
D.) They insure a more complete reporting

Answer: C

QUESTION 62:

Which of the following tools can you use to assess your networks vulnerability?

A. ISS
B. All of the choices.
C. SATAN
D. Ballista

Answer: B

Explanation:
ISS, Ballista and SATAN are all penetration tools.

QUESTION 63:

Annualized Loss Expectancy (ALE) value is derived from an algorithm of the product of annual rate of occurrence and

A. Cost of all losses expected.
B. Previous year's actual loss.
C. Average of previous losses.
D. Single loss expectancy.

Answer: D
Single Loss Expectancy (SLE) x Annualized Rate of Occurance (ARO) = ALE pg. 18 Krutz: The CISSP Prep Guide

---

QUESTION 64:

If your property insurance has Actual Cost Evaluation (ACV) clause your damaged property will be compensated:
A.) Based on the value of the item on the date of loss
B.) Based on new item for old regardless of condition of lost item
C.) Based on value of item one month before loss
D.) Based on value of item on the date of loss plus 10 percent

Answer: D

QUESTION 65:

How is Annualized Loss Expectancy (ALE) derived from a threat?
A.) ARO x (SLE - EF)
B.) SLE x ARO
C.) SLE/EF
D.) AV x EF

Answer: B
"SLE x annualized rate of occurrence (ARO) = ALE" pg 70 Shon Harris: All-in-One CISSP Certification

---

QUESTION 66:

Qualitative loss resulting from the business interruption does not include:
A.) Loss of revenue
B.) Loss of competitive advantage or market share
C.) Loss of public confidence and credibility
D.) Public embarrassment

Answer: A
"Another method of risk analysis is qualitative, which does not assign numbers and monetary valu8es to components and losses." Pg 72 Shon Harris: All-in-One CISSP Certification

---

QUESTION 67:

Which risk management methodology uses the exposure factor multiplied by the asset value to determine its outcome?

A. Annualized Loss Expectancy
B. Single Loss Expectancy

C. Annualized Rate of Occurrence
D. Information Risk Management

Answer: B
Single Loss Expectancy (SLE) AN SLE is the dollar figure that is assigned to a single event. It represents an organization's loss from a single threat and is derived from the following formula: Asset Value ($) X Exposure Factor (EF) = SLE -Ronald Krutz The CISSP PREP Guide (gold edition) pg 18

QUESTION 68:

Valuable paper insurance coverage does not cover damage to which of the following?
A.) Inscribed, printed and written documents
B.) Manuscripts
C.) Records
D.) Money and Securities

Answer: D

QUESTION 69:

What is the window of time for recovery of information processing capabilities based on?
A.) Quality of the data to be processed
B.) Nature of the disaster
C.) Criticality of the operations affected
D.) Applications that are mainframe based

Answer: C

QUESTION 70:

What is the Maximum Tolerable Downtime (MTD):
A.) Maximum elapsed time required to complete recovery of application data
B.) Minimum elapsed time required to complete recovery of application data
C.) Maximum elapsed time required to move back to primary site a major disruption
D.) It is maximum delay businesses that can tolerate and still remain viable

Answer: D
"The MTD is the period of time a business function or process can remain interrupted before its ability to recover becomes questionable." Pg 678 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 71:

A "critical application" is one that MUST

A. Remain operational for the organization to survive.
B. Be subject to continual program maintenance.
C. Undergo continual risk assessments.
D. Be constantly monitored by operations management.

Answer: A
I am assuming that I don't need to put a reference for this answer. Yeah ok here it is but I cheated and used a earlier reference
"A BIA is performed at the beginning of disaster recovery and continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of disaster or disruption." - Shon Harris All-in-one CISSP Certification Guide pg 597

QUESTION 72:

Which of the following questions is less likely to help in assessing physical and environmental protection?
A.) Are entry codes changed periodically?
B.) Are appropriate fire suppression and prevention devices installed and working?
C.) Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
D.) Is physical access to data transmission lines controlled?

Answer: C

QUESTION 73:

A common Limitation of information classification systems is the INABILITY to

A. Limit the number of classifications.
B. Generate internal labels on diskettes.
C. Declassify information when appropriate.
D. Establish information ownership.

Answer: C
I could not find a reference for this. However I do agree that declassifying information is harder to do the classifying, but use your best judgment based on experience and knowledge.

QUESTION 74:

The purpose of information classification is to

A. Assign access controls.
B. Apply different protective measures.
C. Define the parameters required for security labels.

D. Ensure separation of duties.

Answer: C

QUESTION 75:

Who should determine the appropriate access control of information?

A. Owner
B. User
C. Administrator
D. Server

Answer: A

Explanation:
All information generated, or used must have a designated owner. The owner must determine appropriate sensitivity classifications, and access controls. The owner must also take steps to ensure the appropriate controls for the storage, handling, distribution, and use of the information in a secure manner.

QUESTION 76:

What is the main responsibility of the information owner?
A.) making the determination to decide what level of classification the information requires
B.) running regular backups
C.) audit the users when they require access to the information
D.) periodically checking the validity and accuracy for all data in the information system

Answer: A

QUESTION 77:

What process determines who is trusted for a given purpose?

A. Identification
B. Authorization
C. Authentication
D. Accounting

Answer: B

Explanation:
Authorization determines who is trusted for a given purpose. More precisely, it determines whether a particular principal, who has been authenticated as the source of a request to do something, is trusted for that operation. Authorization may also

include controls on the time at which something can be done (e.g. only during working hours) or the computer terminal from which it can be requested (e.g. only the one on the system administrator desk).

QUESTION 78:

The intent of least privilege is to enforce the most restrictive user rights required

A. To execute system processes.
B. By their job description.
C. To execute authorized tasks.
D. By their security role.

Answer: C
Least Privilege; the security principle that requires each subject to be granted the most restrictive set of privileges
needed for the performance of authorized tasks. The application of this principle limits the damage that can result
from accident, error, or unauthorized.
- Shon Harris All-in-one CISSP Certification Guide pg 933

QUESTION 79:

What principle requires that a user be given no more privilege then necessary to perform a job?

A. Principle of aggregate privilege.
B. Principle of most privilege.
C. Principle of effective privilege.
D. Principle of least privilege.

Answer: D

Explanation:
As described at http://hissa.nist.gov/rbac/paper/node5.html, the principle of least privilege has been described as important for meeting integrity objectives. The principle of least privilege requires that a user be given no more privilege than necessary to perform a job.

QUESTION 80:

To ensure least privilege requires that _____ is identified.

A. what the users privilege owns
B. what the users job is
C. what the users cost is

D. what the users group is

Answer: B

Explanation:
Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges couldn't be used to circumvent the organizational security policy. Although the concept of least privilege currently exists within the context of the TCSEC, requirements restrict those privileges of the system administrator. Through the use of RBAC, enforced minimum privileges for general system users can be easily achieved.

QUESTION 81:

The concept of least privilege currently exists within the context of:

A. ISO
B. TCSEC
C. OSI
D. IEFT

Answer: B

Explanation:
Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges couldn't be used to circumvent the organizational security policy. Although the concept of least privilege currently exists within the context of the TCSEC, requirements restrict those privileges of the system administrator. Through the use of RBAC, enforced minimum privileges for general system users can be easily achieved.

QUESTION 82:

Which of the following rules is less likely to support the concept of least privilege?
A.) The number of administrative accounts should be kept to a minimum
B.) Administrators should use regular accounts when performing routing operations like reading mail
C.) Permissions on tools that are likely to be used by hackers should be as restrictive as possible
D.) Only data to and from critical systems and applications should be allowed through the firewall

Answer: D

QUESTION 83:

Which level of "least privilege" enables operators the right to modify data directly in it's original location, in addition to data copied from the original location?
A.) Access Change
B.) Read/Write
C.) Access Rewrite
D.) Access modify

Answer: A

QUESTION 84:

This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and privileges that what is required for the tasks the user needs to fulfill. What best describes this scenario?
A.) Excessive Rights
B.) Excessive Access
C.) Excessive Permissions
D.) Excessive Privileges

Answer: D
Reference: "Excessive Privileges: This is a common security issue that is extremely hard to control in vast, complex environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks she needs to fulfill." pg 603 Shon Harris: All-in-One CISSP Certification

QUESTION 85:

One method to simplify the administration of access controls is to group

A. Capabilities and privileges
B. Objects and subjects
C. Programs and transactions
D. Administrators and managers

Answer: B

QUESTION 86:

Cryptography does not concern itself with:
A.) Availability
B.) Integrity
C.) Confidentiality
D.) Authenticity

Answer: A

QUESTION 87:

Which of the following measures would be the BEST deterrent to the theft of corporate information from a laptop which was left in a hotel room?
A.) Store all data on disks and lock them in an in-room safe
B.) Remove the batteries and power supply from the laptop and store them separately from the computer
C.) Install a cable lock on the laptop when it is unattended
D.) Encrypt the data on the hard drive

Answer: D

QUESTION 88:

To support legacy applications that rely on risky protocols (e.g,, plain text passwords), which one of the following can be implemented to mitigate the risks on a corporate network?

A. Implement strong centrally generated passwords to control use of the vulnerable applications.
B. Implement a virtual private network (VPN) with controls on workstations joining the VPN.
C. Ensure that only authorized trained users have access to workstations through physical access control.
D. Ensure audit logging is enabled on all hosts and applications with associated frequent log reviews.

Answer: B
It makes more sense to provide VPN client to workstations opposed to physically securing workstations.

QUESTION 89:

Which of the following computer crime is more often associated with insiders?
A.) IP spoofing
B.) Password sniffing
C.) Data diddling
D.) Denial of Service (DOS)

Answer: C

QUESTION 90:

The technique of skimming small amounts of money from multiple transactions is called the

A. Scavenger technique
B. Salami technique
C. Synchronous attack technique
D. Leakage technique

Answer: B

QUESTION 91:

What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?
A.) Data fiddling
B.) Data diddling
C.) Salami techniques
D.) Trojan horses

Answer: C

QUESTION 92:

What is the act of willfully changing data, using fraudulent input or removal of controls called?

A. Data diddling
B. Data contaminating
C. Data capturing
D. Data trashing

Answer: A
Data-diddling - the modification of data -Ronald Krutz The CISSP PREP Guide (gold edition) pg 417

QUESTION 93:

In the context of computer security, "scavenging" refers to searching

A. A user list to find a name.
B. Through storage to acquire information.
C. Through data for information content.
D. Through log files for trusted path information.

Answer: C
Scavenging is a form of dumpster diving performed electronically. Online scavenging searches for useful information in the remnants of data left over after processes or tasks are completed.

This could include audit trails, logs files, memory dumps, variable settings, port mappings, and cached data. - Ed Tittle CISSP Study Guide (sybex) pg 476

QUESTION 94:

Which security program exists if a user accessing low-level data is able to draw conclusions about high-level information?

A. Interference
B. Inference
C. Polyinstatiation
D. Under-classification

Answer: B
Main Entry: in*fer*ence
Function: noun
Date: 1594
1 : the act or process of inferring : as a : the act of passing from one proposition, statement, or judgment considered as true to another whose truth is believed to follow from that of the former b : the act of passing from statistical sample data to generalizations (as of the value of population parameters) usually with calculated degrees of certainty
2 : something that is inferred especially : a proposition arrived at by inference
3 : the premises and conclusion of a process of inferring
http://www.m-w.com/cgi-bin/dictionary

QUESTION 95:

Which of the following is not a form of a passive attack?
A.) Scavenging
B.) Data diddling
C.) Shoulder surfing
D.) Sniffing

Answer: B
Data diddling is an active attack opposed to a passive attack.
Reference: "Data Diddling occurs when an attacker gains access to a system and makes small, random, or incremental changes to data rather than obviously altering file contents or damaging or deleting entire files." Pg 383 Tittel

---

QUESTION 96:

An example of an individual point of verification in a computerized application is

A. An inference check.
B. A boundary protection.
C. A sensitive transaction.

D. A check digit.

Answer: D
Checkdigit: A one-digit checksum.
Checksum: A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.
The checksum may be 8 bits (modulo 256 sum), 16, 32, or some other size. It is computed by summing the bytes or words of the data block ignoring overflow. The checksum may be negated so that the total of the data words plus the checksum is zero.

QUESTION 97:

Data inference violations can be reduced using

A. Polyinstantiation technique.
B. Rules based meditation.
C. Multi-level data classification.
D. Correct-state transformation.

Answer: A
"Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object. In the database information security, this term is concerned with the same primary key for different relations at different classification levels being stored in the same database. For example, in a relational database, the same of a military unit may be classified Secret in the database and may have an identification number as the primary key. If another user at a lower classification level attempts to create a confidential entry for another military unit using the same identification number as a primary key, a rejection of this attempt would imply to the lower level user that the same identification number existed at a higher level of classification. To avoid this inference channel of information, the lower level user would be issued the same identification number for their unit and the database management system would manage this situation where the same primary key was used for different units." Pg 352-353 Krutz: The CISSP Prep Guide: Gold Edition.
"As with aggregation, the best defense against inference attacks is to maintain constant vigilance over the permissions granted to individual users. Furthermore, intentional blurring of data may be used to prevent the inference of sensitive information." - Ed Tittle CISSP Study Guide (sybex)
The other security issue is inference, which is very similar to aggregation. The inference problem happens when a subject deduces information that is restricted from data he has access to. This is seen when data at a lower security level indirectly portrays data at a higher level...This problem is usually dealt with in the development of the database by implementing content and context-dependent classification rules; this tracks the subject's query requests and restricts patterns that represent inference.
"Polyinstantiation is a process of interactively producing more detailed versions of objects by

populating variables with values or other variables"- Shon Harris All-in-one CISSP Certification Guide pg 725-727

QUESTION 98:

What is it called when a computer uses more than one CPU in parallel to execute instructions?
A.) Multiprocessing
B.) Multitasking
C.) Multithreading
D.) Parallel running

Answer: A

QUESTION 99:

What is the main purpose of undertaking a parallel run of a new system?
A.) Resolve any errors in the program and file interfaces
B.) Verify that the system provides required business functionality
C.) Validate the operation of the new system against its predecessor
D.) Provide a backup of the old system

Answer: B

QUESTION 100:

Which of the following provide network redundancy in a local network environment?
A.) Mirroring
B.) Shadowing
C.) Dual backbones
D.) Duplexing

Answer: C

QUESTION 101:

A server farm is an example of:
A.) Server clustering
B.) Redundant servers
C.) Multiple servers
D.) Server fault tolerance

Answer: A

QUESTION 102:

In which state must a computer system operate to process input/output instructions?

A. User mode
B. Stateful inspection
C. Interprocess communication
D. Supervisor mode

Answer: D
A computer is in a supervisory state when it is executing these privileged instructions. (privileged instructions are executed by the system administrator or by an individual who is authorized to use those instructions.) . -Ronald Krutz The CISSP PREP Guide (gold edition) pg 254-255

QUESTION 103:

What should be the size of a Trusted Computer Base?

A. Small - in order to permit it to be implemented in all critical system components without using excessive resources.
B. Small - in order to facilitate the detailed analysis necessary to prove that it meets design requirements.
C. Large - in order to accommodate the implementation of future updates without incurring the time and expense of
recertification.
D. Large - in order to enable it to protect the potentially large number of resources in a typical commercial system
environment.

Answer: B
"It must be small enough to be able to be tested and verified in a complete and comprehensive manner." Shon Harris All-In-One CISSP Certification Guide pg. 232-233.

QUESTION 104:

Which one of the following are examples of security and controls that would be found in a "trusted" application system?

A. Data validation and reliability
B. Correction routines and reliability
C. File integrity routines and audit trail
D. Reconciliation routines and data labels

Answer: C
I have no specific reference for this question but the major resources hammer that there needs to be methods to check the data for correctness.

QUESTION 105:

Which of the following is an operating system security architecture that provides flexible support for security policies?

A. OSKit
B. LOMAC
C. SE Linux
D. Flask

Answer: D

Explanation:
Flask is an operating system security architecture that provides flexible support for security policies. The architecture was prototyped in the Fluke research operating system. Several of the Flask interfaces and components were then ported from the Fluke prototype to the OSKit. The Flask architecture is now being implemented in the Linux operating system (Security-Enhanced Linux) to transfer the technology to a larger developer and user community.

QUESTION 106:

Which of the following statements pertaining to the security kernel is incorrect?
A.) It is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B.) It must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof
C.) It must be small enough to be able to be tested and verified in a complete and comprehensive manner
D.) Is an access control concept, not an actual physical component

Answer: D

QUESTION 107:

What is a PRIMARY reason for designing the security kernel to be as small as possible?

A. The operating system cannot be easily penetrated by users.
B. Changes to the kernel are not required as frequently.
C. Due to its compactness, the kernel is easier to formally verify.
D. System performance and execution are enhanced.

Answer: C
I disagree with the original answer which was B (changes to the kernel) and think it is C (Due to its compactness). However, use your best judgment based on knowledge and experience. Below is why I think it is C.

"There are three main requirements of the security kernel:
It must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
The reference monitor must be invoked for every access attempt and must be impossible to circumvent. Thus the reference monitor must be implemented in a complete and foolproof way.
à It must be small enough to be able to be tested and verified in a complete and comprehensive manner." - Shon Harris All-in-one CISSP Certification Guide pg 232-233

QUESTION 108:

Which of the following implements the authorized access relationship between subjects and objects of a system?

A. Security model
B. Reference kernel
C. Security kernel
D. Information flow model

Answer: C

QUESTION 109:

The concept that all accesses must be meditated, protected from modification, and verifiable as correct is the concept of

A. Secure model
B. Security locking
C. Security kernel
D. Secure state

Answer: C
A security kernel is defined as the hardware, firmware, and software elements of a trusted computing base that implements the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. Therefore, the reference monitor concept is an abstract machine that mediates all access of subjects to objects. The Security Kernel must:
Mediate all accesses
Be protected from modification
Be verified as correct.
-Ronald Krutz The CISSP PREP Guide (gold edition) pg 262

QUESTION 110:

What is an error called that causes a system to be vulnerable because of the environment in which it is installed?
A.) Configuration error
B.) Environmental error

C.) Access validation error
D.) Exceptional condition handling error

Answer: B

QUESTION 111:

Which of the following ensures that security is not breached when a system crash or other system failure occurs?
A.) trusted recovery
B.) hot swappable
C.) redundancy
D.) secure boot

Answer: A
"Trusted Recovery
When an operating system or application crashes or freezes, it should not put the sytem in any time of secure state." Pg 762 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 112:

What type of subsystem is an application program that operates outside the operating system and carries out functions for a group of users, maintains some common data for all users in the group, and protects the data from improper access by users in the group?

A. Prevented subsystem
B. Protected subsystem
C. File subsystem
D. Directory subsystem

Answer: B

QUESTION 113:

A 'Pseudo flaw' is which of the following?
A.) An apparent loophole deliberately implanted in an operating system
B.) An omission when generating Pseudo-code
C.) Used for testing for bounds violations in application programming
D.) A Normally generated page fault causing the system halt

Answer: A

QUESTION 114:

Which of the following yellow-book defined types of system recovery happens after a system fails in an uncrontrolled manner in response to a TCB or media failure and the

system cannot be brought to a consistent state?
A.) Recovery restart
B.) System reboot
C.) Emergency system restart
D.) System Cold start

Answer: C
Reference: "Emergency system restart is done after a system fails in an uncontrolled manner in response to a TCB or media failure. In such cases, TCB and user objects on nonvolatile storage belonging to processes active at the time of TCB or media failure may be left in an inconsistent state. The system enters maintenance mode, recovery is performed automatically, and the system restarts with no user processes in progress after bringing up the system in a consistent state."

QUESTION 115:

Which one of the following describes a reference monitor?

A. Access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.
B. Audit concept that refers to monitoring and recording of all accesses to objects by subjects.
C. Identification concept that refers to the comparison of material supplied by a user with its reference profile.
D. Network control concept that distributes the authorization of subject accesses to objects.

Answer: A
A reference monitor is a system component that enforces access controls on an object. Therefore, the reference monitor concept is an abstract machine that mediates all access of subjects to objects -Ronald Krutz The CISSP PREP Guide (gold edition) pg 262

QUESTION 116:

What can best be described as an abstract machine which must mediate all access to subjects to objects?
A.) A security domain
B.) The reference monitor
C.) The security kernel
D.) The security perimeter

Answer: B
Reference: pg 882 Shon Harris: All-in-One CISSP Certification

---

QUESTION 117:

What is the PRIMARY component of a Trusted Computer Base?

A. The computer hardware
B. The security subsystem
C. The operating system software
D. The reference monitor

Answer: D
"The security kernel is made
up of hardware, software, and firmware components that fall within the TCB and
implements and enforces the reference monitor concept. The security kernel
mediates all access and functions between subjects and objects. The security kernel
is the core of the TCB and is the most commonly used approach to building trusted
computing systems. There are three main requirements of the security kernel:
It must provide isolation for the processes carrying out the reference monitor concept,
and the processes must be tamperproof.
It must be invoked for every access attempt and must be impossible to circumvent.
Thus, the security kernel must be implemented in a complete and foolproof way.
It must be samall enough to be able to be tested and verified in a complete and
comprehensive manner.
These are the requirements of the reference monitor; therefor,they are the requirements
of the components that provide and enforce the reference monitor concept-the security
kernel." - Shon Harris, "CISSP All-in-One Exam Guide", 3rd Ed, p

---

QUESTION 118:

Which of the following is best defined as a mode of system termination that automatically
leaves system processes and components in a secure state when a failure occurs or is
detected in the system?
A.) Fail proof
B.) Fail soft
C.) Fail safe
D.) Fail resilient

Answer: C

QUESTION 119:

LOMAC uses what Access Control method to protect the integrity of processes and data?

A. Linux based EFS.
B. Low Water-Mark Mandatory Access Control.
C. Linux based NFS.
D. High Water-Mark Mandatory Access Control.

Answer: B

Explanation:
LOMAC is a security enhancement for Linux that uses Low Water-Mark Mandatory Access Control to protect the integrity of processes and data from viruses, Trojan horses, malicious remote users and compromised root daemons. LOMAC is implemented as a loadable kernel module - no kernel recompilations or changes to existing applications are required. Although not all the planned features are currently implemented, it presently provides sufficient protection to thwart script-kiddies, and is stable enough for everyday use.

QUESTION 120:

On Linux, LOMAC is implemented as:

A. Virtual addresses
B. Registers
C. Kernel built in functions
D. Loadable kernel module

Answer: D

Explanation:
LOMAC is a security enhancement for Linux that uses Low Water-Mark Mandatory Access Control to protect the integrity of processes and data from viruses, Trojan horses, malicious remote users and compromised root daemons. LOMAC is implemented as a loadable kernel module - no kernel recompilations or changes to existing applications are required. Although not all the planned features are currently implemented, it presently provides sufficient protection to thwart script-kiddies, and is stable enough for everyday use.
"Security Kernel - The hardware, firmware, and software elements of a trusted computing base (TCB) that implements the reference monitor concept. It must mediate all accesses between subjects and objects, be protected from modification, and be verifiable as correct." - Shon Harris All-in-one CISSP Certification Guide pg 355

QUESTION 121:

LOMAC is a security enhancement for what operating system?

A. Linux
B. Netware
C. Solaris

Answer: A

Explanation:
LOMAC is a security enhancement for Linux that uses Low Water-Mark Mandatory Access Control to protect the integrity of processes and data from viruses, Trojan horses,

malicious remote users and compromised root daemons. LOMAC is implemented as a loadable kernel module - no kernel recompilations or changes to existing applications are required. Although not all the planned features are currently implemented, it presently provides sufficient protection to thwart script-kiddies, and is stable enough for everyday use.

QUESTION 122:

What was introduced for circumventing difficulties in classic approaches to computer security by limiting damages produces by malicious programs?

A. Integrity-preserving
B. Ref Mon
C. Integrity-monitoring
D. Non-Interference

Answer: B

Explanation:
"reference monitor ... mediates all access subjects have to objects ... protect the objects from unauthorized access and destructive modification" , Ibid p 273
Reference monitor is part of the TCB concept
Not D: "noninterference ... is implemented to ensure that any actions that take place at a higher security level do not affect ... actions that take place at a lower level", Harris, 3rd Ed, p 290.
It is part of the information flow model.

QUESTION 123:

A feature deliberately implemented in an operating system as a trap for intruders is called a:

A. Trap door
B. Trojan horse
C. Pseudo flaw
D. Logic bomb

Answer: C
"An apparent loophole deliberately implanted in an operating system program as a trap for intruders." As defined by the Aqua Book NCSC-TG-004 a pseudo-flaw is an apparent loophole deliberately implanted in an operating system program as a trap for intruders. Answer from http://www.cccure.org

---

QUESTION 124:

Fault tolerance countermeasures are designed to combat threats to
A.) an uninterruptible power supply

B.) backup and retention capability
C.) design reliability
D.) data integrity

Answer: C

QUESTION 125:

A 'Psuedo flaw' is which of the following?
A.) An apparent loophole deliberately implanted in an operating system program as a trap for intruders
B.) An omission when generating Psuedo-code
C.) Used for testing for bounds violations in application programming
D.) A normally generated page fault causing the system to halt

Answer: A

QUESTION 126:

What Distributed Computing Environment (DCE) component provides a mechanism to ensure that services are made available only to properly designated parties?

A. Directory Service
B. Remote Procedure Call Service
C. Distributed File Service
D. Authentication and Control Service

Answer: A
A directory service has a hierarchical database of users, computers, printers, resources, and attributes of each. The directory is mainly used for lookup operations, which enable users to track down resources and other users...The administrator can then develop access control, security, and auditing policies that dictate who can access these objects, how the objects can be accessed, and audit each of these actions. - Shon Harris All-in-one CISSP Certification Guide pg 436-437

QUESTION 127:

What can be accomplished by storing on each subject a list of rights the subject has for every object?

A. Object
B. Capabilities
C. Key ring
D. Rights

Answer: B

Explanation:
Capabilities are accomplished by storing on each subject a list of rights the subject has for every object. This effectively gives each user a key ring. To remove access to a particular object, every user (subject) that has access to it must be "touched". A touch is an examination of a user's rights to that object and potentially removal of rights. This brings back the problem of sweeping changes in access rights.

QUESTION 128:

In the Information Flow Model, what relates two versions of the same object?

A. Flow
B. State
C. Transformation
D. Successive points

Answer: A

Explanation:
A flow is a type of dependency that relates two versions of the same object, and thus the transformation of one state of that object into another, at successive points in time.

QUESTION 129:

What is a security requirement that is unique to Compartmented Mode Workstations (CMW)?
A.) Sensitivity Labels
B.) Object Labels
C.) Information Labels
D.) Reference Monitors

Answer: C

QUESTION 130:

The Common Criteria (CC) represents requirements for IT security of a product or system under which distinct categories?

A. Functional and assurance
B. Protocol Profile (PP) and Security Target (ST)
C. Targets of Evaluation (TOE) and Protection Profile (PP)
D. Integrity and control

Answer: A

"Like other evaluation criteria before it, Common Criteria works to answer two basic and general questions about products being evaluated: what does it do (functionality), and how sure are you of that (assurance)?" pg 232 Shon Harris CISSP All-In-One Certification Exam Guide

---

QUESTION 131:

What are the assurance designators used in the Common Criteria (CC)?

A. EAL 1, EAL 2, EAL 3, EAL 4, EAL 5, EAL 6, and EAL 7
B. A1, B1, B2, B3, C2, C1, and D
C. E0, E1, E2, E3, E4, E5, and E6
D. AD0, AD1, AD2, AD3, AD4, AD5, and AD6

Answer: A
Original Answer was C. This is wrong in my view as the original answer confused ITSEC with the CC per the following
The Common criteria terminology for the degree of examination of the product to be tested is the Evaluation Assurance level (EAL). EALs range from EA1 (functional testing to EA7 (detailed testing and formal design verification). -Ronald Krutz The CISSP PREP Guide (gold edition) pg 266-267
Note that Shon Harris All-in-one CISSP Certification Guide uses EAL (not just EA).
EALs are combinations of assurance components. They also can be conveniently compared to TSCEC and ITSEC. Like these security evaluation criteria, EALs are scaled with from EAL1 through EAL7. Other EALs exist, but EAL 7 is the highest with international recognition. - Roberta Bragg Cissp Certification Training Guide (que) pg 368
ITSEC separately evaluates functionality and assurance, and it includes 10 functionality classes (f), eight assurance levels (q), seven levels of correctness (e), and eight basic security functions in its criteria.). -Ronald Krutz The CISSP PREP Guide (gold edition) pg 266

QUESTION 132:

Which of the following uses protection profiles and security targets?
A.) ITSEC
B.) TCSEC
C.) CTCPEC
D.) International Standard 15408

Answer: D
"For historical and continuity purposes, ISO has accepted the continued use of the term "Common Criteria" (CC) within this document, while recognizing the official ISO name for the new IS 15408 is "Evaluation Criteria for Information Technology Security." Pg. 552 Krutz: The CISSP Prep Guide: Gold Edition
"The Common Criteria define a Protection Profile (PP), which is an implementation-independent specification of the security requirements and protections of a product that could be built. The Common Criteria terminology for the degree of examination of the product to be tested is the Evaluation Assurance Level (EAL). EALs range from EA1 (functional testing) to EA7 (detailed testing and formal design verification). The Common Criteria TOE refers to the product to be

tested. A Security Target (ST) is a listing of the security claims for a particular IT security product. Also, the Common Criteria describe an intermediate grouping of security requirement components as a package." Pg. 266-267 Krutz: The CISSP Prep Guide: Gold Edition

---

QUESTION 133:

According to Common Criteria, what can be described as an intermediate combination of security requirement components?
A.) Protection profile (PP)
B.) Security target (ST)
C.) Package
D.) The Target of Evaluation (TOE)

Answer: C
"The Common Criteria define a Protection Profile (PP), which is an implementation-independent specification of the security requirements and protections of a product that should be built. The Common Criteria terminology for the degree of examination of the product to be tested is the Evaluation Assurance Level (EAL.) EALs range from EA1 (functional testing() to EA7 (detailed testing and formal design verification). The Common Criteria TOE refers to the product to be tested. A Security Target (ST) is a listing of the security claims for a particular IT security product. Also, the Common Criteria describe an intermedicate grouping of security requirement components as a package."
Pg. 266- 267 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 134:

The Common Criteria construct which allows prospective consumers or developers to create standardized sets of security requirements to meet there needs is

A. a Protection Profile (PP).
B. a Security Target (ST).
C. an evaluation Assurance Level (EAL).
D. a Security Functionality Component Catalog (SFCC).

Answer: A
Protection Profiles: The Common Criteria uses protection profiles to evaluate products. The protection profile contains the set of security requirements, their meaning and reasoning, and the corresponding EAL rating. The profile describes the environmental assumptions, the objectives, and functional and assurance level expectations. Each relevant threat is listed along with how it is to be controlled by specific objectives. It also justifies the assurance level and requirements for the strength of each protection mechanism. The protection profile provides a means for the consumer, or others, to identify specific security needs ;p this is the security problems to be conquered.
EAL: An evaluation is carried out on a product and is assigned an evaluation assurance level (EAL) The thoroughness and stringent testing increases in detailed-oriented tasks as the levels increase. The Common Criteria has seven aassurance levels. The ranges go from EAL1, where

the functionality testing takes place, to EAL7,where thorough testing is performed and the system is verified.
All-In-One CISSP Certification Exam Guide by Shon Harris pg. 262
Note: "The Common Criteria defines a Protection Profile (PP), which is an implementation-independent specification of the security requirements and protections of a product that could be built. The Common Criteria terminology for the degree of examination of the product to be tested is the Evaluation Assurance Level (EAL). EALs range from EA1 (functional testing) to EA7 (detailed testing and formal design verification). The Common Criteria TOE [target of evaluation] refers to the product to be tested. A Security Target (ST) is a listing of the security claims for a particular IT security product." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 266-267

QUESTION 135:

The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?
A.) integrity and confidentiality
B.) confidentiality and availability
C.) integrity and availability
D.) none of the above

Answer: C
"ITSEC TCSEC (Orange Book)
E0 D
F1+E1 C1
F2+E2 C2
F3+E3 B1
F4+E4 B2
F5+E5 B3
F5+E6 A1
F6=Systems that provide high integrity
F7=Systems that provide high availability
F8=Systems that provide data integrity during communication
F9=Systems that provide high confidentiality
F10=Networks with high demands on confidentiality and integrity"
Pg. 230 Shon Harris: All-in-One CISSP Certification

QUESTION 136:

Which of the following was developed by the National Computer Security Center (NCSC)?
A.) TCSEC
B.) ITSEC
C.) DITSCAP
D.) NIACAP

Answer: A
Reference: pg 129 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 137:

The Trusted Computer Security Evaluation Criteria (TBSEC) provides

A. a basis for assessing the effectiveness of security controls built into automatic data-processing system products
B. a system analysis and penetration technique where specifications and document for the system are analyzed.
C. a formal static transition model of computer security policy that describes a set of access control rules.
D. a means of restricting access to objects based on the identity of subjects and groups to which they belong.

Answer: A
TBSEC provides guidelines to be used with evaluating a security product. The TBSEC guidelines address basic security functionality and allow evaluators to measure and rate the functionality of a system and how trustworthy it is. Functionality and assurance are combined and not separated, as in criteria developed later. TCSEC guidelines can be used for evaluating vendor products or by vendors to design necessary functionality into new products. CISSP Study Guide by Tittel pg. 413.

QUESTION 138:

Which Orange Book evaluation level is described as "Verified Design"?
A.) A1
B.) B3
C.) B2
D.) B1

Answer: A

QUESTION 139:

Which of the following classes is defined in the TCSEC (Orange Book) as mandatory protection?
A.) B
B.) A
C.) C
D.) D

Answer: A

QUESTION 140:

Which Orange Book security rating requires that formal techniques are used to prove the equivalence between the TCB specifications and the security policy model?
A.) B2
B.) B3
C.) A1
D.) A2

Answer: C
Reference: Pg 226 Shon Harris: All-in-One CISSP Certification

---

QUESTION 141:

According to the Orange Book, which security level is the first to require trusted recovery?
A.) A1
B.) B2
C.) B3
D.) B1

Answer: B
"Trusted recovery is required only for B3 and A1 level systems." Pg 305 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 142:

According to the Orange Book, which security level is the first to require a system to protect against covert timing channels?
A.) A1
B.) B3
C.) B2
D.) B1

Answer: B

Explanation: A B2 system mustmeet all the requirement of a B1 system and support hierarchical devices labels, trusted path communications between the user and the system, and covert channel analysis.
Exam Cram 2pg 103 and ALL-IN-ONE CISSP Third Edition by Shon Harris pg 304.
The key to this question is knowingthe difference between various system ratings and keeping in mind a higher ratedsystem have all of the same security implementations as a lower rated system. In this case both B3 and A1 systems supportcovert channelanalysis, but it isimplementedfor B2 systems.

QUESTION 143:

Which of the following is not an Orange Book-defined operational assurance requirement?
A.) System architecture
B.) Trusted facility management
C.) Configuration management
D.) Covert channel analysis

Answer: C

QUESTION 144:

Which of the following is least likely to be found in the Orange Book?
A.) Security policy
B.) Documentation
C.) Accountability
D.) Networks and network components

Answer: D

QUESTION 145:

According to the Orange Book, which security level is the first to require a system to support separate operator and system administrator rules?
A.) A1
B.) B1
C.) B2
D.) B3

Answer: C

QUESTION 146:

Which of the following is not an Orange book-defined life cycle assurance requirement?
A.) Security testing
B.) Design specification and testing
C.) Trusted distribution
D.) System integrity

Answer: D
Systems Integrity is a part of operational assurance opposed to life cycle assurance.
"The operational assurance requirements specified in the Orange Book are as follows:
System Architecture
System integrity
Covert channel analysis
Trusted facility management
Trusted recovery
The life cycle assurance requirements specified in the Orange Book are as follows:

Security testing
Design specification and testing
Configuration Management
Trusted Distribution"
Pg. 301 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 147:

At what Trusted Computer Security Evaluation Criteria (TCSEC) or Information Technology Security Evaluation
Criteria (ITSEC) security level are database elements FIRST required to have security labels?

A. A1/E6
B. B1/E3
C. B2/E4
D. C2/E2

Answer: B
"B1: Labeled Security
Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject and object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement and the design specifications are reviewed and verified. It is intended for environments that require systems to handle classified data."
" pg. 224-226 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 148:

Which of the following statements pertaining to the Trusted Computer System Evaluation Criteria (TCSEC) is incorrect?
A.) With TCSEC, functionality and assurance are evaluated separately.
B.) TCSEC provides a means to evaluate the trustworthiness of an information system
C.) The Orange Book does not cover networks and communications
D.) Database management systems are not covered by the TCSEC

Answer: A

QUESTION 149:

Which of the following is the lowest TCSEC class wherein the systems must support separate operator and system administrator roles?
A.) B2
B.) B1
C.) A1
D.) A2

Answer: A
Reference: pg 129 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 150:

Which TCSEC (Orange Book) level requires the system to clearly identify functions of security administrator to perform security-related functions?

A.) C2
B.) B1
C.) B2
D.) B3

Answer: D
B1: Labeled Security
Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject and object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement and the design specifications are reviewed and verified. It is intended for environments that require systems to handle classified data.
B2: Structured Protection
The security policy is clearly defined and documented, and the system design and implementation are subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces among layers. Subjects and devices require labels, and the system must not allow covert channels. A trusted path for logon and authentication processes must be in place, which means there are no trapdoors. A trusted path means that the subject is communicating directly with the application or operating system. There is no way to circumvent or compromise this communication channel. There is a separation of operator and administration functions within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolate processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system.
The environment that would require B2 systems could process sensitive data that require a higher degree of security. This environment would require systems that are relatively resistant to penetration and compromise.
(A trusted path means that the user can be sure that he is talking to a genuine copy of the operating system.)
B3: Security Domains
In this class, more granularity is provided in each protection mechanism, and the programming code that is not necessary to support the security policy is exclude. The design and implementation should not provide too much complexity because as the complexity of a system increases, the ability of the individual who need to test, maintain, and configure it reduces; thus, the overall security can be threatened. The reference monitor components must be small enough to test properly and be tamperproof. The security administrator role is clearly defined, and the

system must be able to recover from failures without it security level being compromised. When the system starts up and loads it operating system and components, it must be done in an initial secure state to ensure that any weakness of the system cannot be taken advantage of in this slice of time. " pg. 226 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 151:

Which of the following statements pertaining to the trusted computing base (TCB) is false?
A.) It addresses the level of security a system provides
B.) It originates from the Orange Book
C.) It includes hardware, firmware, and software
D.) A higher TCB rating will require that details of their testing procedures and documentation be reviewed with more granularity

Answer: A

QUESTION 152:

Which of the following is not an Orange book-defined operational assurance requirement?
A.) System architecture
B.) Trusted facility management
C.) Configuration management
D.) Covert channel analysis

Answer: C
Configuration management is a part of life cycle assurance opposed to operational assurance.
"The operational assurance requirements specified in the Orange Book are as follows:
System Architecture
System integrity
Covert channel analysis
Trusted facility management
Trusted recovery
The life cycle assurance requirements specified in the Orange Book are as follows:
Security testing
Design specification and testing
Configuration Management
Trusted Distribution"
Pg. 301 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 153:

Which of the following focuses on the basic features and architecture of a system?
A.) operational assurance
B.) life cycle assurance
C.) covert channel assurance
D.) level A1

Answer: A
"The operational assurance requirements specified in the Orange Book are as follows:
System Architecture
System integrity
Covert channel analysis
Trusted facility management
Trusted recovery"
Pg. 301 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 154:

Which level(s) must protect against both covert storage and covert timing channels?
A.) B3 and A1
B.) B2, B3 and A1
C.) A1
D.) B1, B2, B3 and A1

Answer: A
Reference: pg 302 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 155:

According to the Orange Book, trusted facility management is not required for which of the following security levels?
A.) B1
B.) B2
C.) B3
D.) A1

Answer: A
B1 does not provide trusted facility management, the next highest level that does is B2.
"Trusted facility management is defined as the assignment of a specific individual to administer the security-related functions of a system. Although trusted facility management is an assurance requirement only for highly secure systems (B2, B3, and A1), many systems evaluated at lower security levels CK structured to try to meet this requirement." Pg. 302 Krutz: The CISSP Prep Guide: Gold Edition

---

QUESTION 156:

Which factor is critical in all systems to protect data integrity?

A. Data classification
B. Information ownership
C. Change control
D. System design

Answer: A
A Integrity is dependent on confidentiality, which relies on data classification. Also Biba integrity model relies on data classification.
"There are numerous countermeasures to ensure confidentiality against possible threats. These include the use of encryption, network traffic padding, strict access control, rigorous authentication procedures, data classification, and extensive personnel training.
Confidentiality and integrity are dependent upon each other. Without object integrity, confidentiality cannon be maintained. Other concepts, conditions, and aspects of confidentiality include sensitivity, discretion, criticality, concealment, secrecy, privacy, seclusion, and isolation." Pg 145 Tittel: CISSP Study Guide.
"Biba Integrity Model
Integrity is usually characterized by the three following goals:
1.) The data is protected from modification by unauthorized users.
2.) The data is protected from unauthorized modification by authorized users.
3) The data is internally and externally consistent; the data held in a database must balance internally and correspond to the external, real world situation."
Pg. 277 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 157:

Which of the following is not a common integrity goal?
A.) Prevent unauthorized users from making modifications
B.) Maintain internal and external consistency
C.) Prevent authorized users from making improper modifications
D.) Prevent paths that could lead to inappropriate disclosure

Answer: D

QUESTION 158:

Which security model introduces access to objects only through programs?
A.) The Biba model
B.) The Bell-LaPadula model
C.) The Clark-Wilson model
D.) The information flow model

Answer: C
"The Clark-Wilson model is also an integrity-protecting model. The Clark-Wilson model was developed after Biba and approaches integrity protection from a different perspective. Rather than employing a lattice structure, it uses a three-part relationship of subject/program/object known as a triple. Subjects do not have direct access to objects. Objects can be access only through programs." Pg 347 Tittel: CISSP Study Guide

---

QUESTION 159:

To ensure that integrity is attainted through the Clark and Wilson model, certain rules are needed.These rules are:

A. Processing rules and enforcement rules.
B. Integrity-bouncing rules.
C. Certification rules and enforcement rules.
D. Certification rules and general rules.

Answer: C

Explanation:
To ensure that integrity is attained and preserved, Clark and Wilson assert, certain integrity-monitoring and integrity-preserving rules are needed. Integrity-monitoring rules are called certification rules, and integrity-preserving rules are called enforcement rules.

QUESTION 160:

What can be defined as a formal security model for the integrity of subjects and objects in a system?

A. Biba
B. Bell LaPadulaLattice
C. Lattice
D. Info Flow

Answer: A
The Handbook of Information System Management, 1999 Edition, ISBN: 0849399742 presents the following definition:
In studying the two properties of the Bell-LaPadula model, Biba discovered a plausible notion of integrity, which he defined as prevention of unauthorized modification. The resulting Biba integrity model states that maintenance of integrity requires that data not flow from a receptacle of given integrity to a receptacle of higher integrity. For example, if a process can write above its security level, trustworthy data could be contaminated by the addition of less trustworthy data. SANS glossary at http://www.sans.org/newlook/resources/glossary.htm define it as:
Formal security model for the integrity of subjects and objects in a system.

QUESTION 161:

The Clark Wilson model has its emphasis on:

A. Security
B. Integrity
C. Accountability
D. Confidentiality

Answer: B

Explanation:
This model attempts to capture security requirements of commercial applications.
'Military' and 'Commercial' are shorthand for different ways of using computers. This model has emphasis on integrity:
Internal consistency: properties of the internal state of a system
External consistency: relation of the internal state of a system to the outside world

---

QUESTION 162:

What does * (star) integrity axiom mean in the Biba model?
A.) No read up
B.) No write down
C.) No read down
D.) No write up

Answer: D
"Biba has two integrity axioms:
1. Simple Integrity Axiom The Simple Integrity Axiom (SI Axiom) state that a subject at a specific classification level cannot read data with a lower classification level. This is often shortened to "no read down."
1. Integrity Axiom The * (star) Integrity Axiom (* Axiom) states that a subject at a specific classification level cannot write data to a higher classification level. This is often shortened to "no write up."" Pg 347 Tittel: CISSP Study Guide

---

QUESTION 163:

Which access control model states that for integrity to be maintained data must not flow from a receptacle of given integrity to a receptacle of higher integrity?

A. Lattice Model
B. Bell-LaPadula Model
C. Biba Model
D. Take-Grant Model

Answer: C
If implemented and enforced properly, the Biba model prevents data from any integrity level from flowing to a higher integrity level. - Shon Harris All-in-one CISSP Certification Guide pg 244

QUESTION 164:

Which one of the following is a KEY responsibility for the "Custodian of Data"?

A. Data content and backup
B. Integrity and security of data
C. Authentication of user access
D. Classification of data elements

Answer: B
Custodian - Preserves the information's CIA (chart) -Ronald Krutz The CISSP PREP Guide (gold edition) pg 15

QUESTION 165:

Which one of the following is true about information that is designated with the highest of confidentiality in a private sector organization?

A. It is limited to named individuals and creates and audit trail.
B. It is restricted to those in the department of origin for the information.
C. It is available to anyone in the organization whose work relates to the subject and requires authorization for each access.
D. It is classified only by the information security officer and restricted to those who have made formal requests for access.

Answer: C

QUESTION 166:

Related to information security, confidentiality is the opposite of which of the following?
A.) closure
B.) disclosure
C.) disposal
D.) disaster

Answer: B

QUESTION 167:

What is the main concern of the Bell-LaPadula security model?

A.) Accountability
B.) Integrity
C.) Confidentiality
D.) Availability

Answer: C
"An important thing to note is that the Bell-LaPadula model was developed to make sure secrets stay secret; thus, it provides and addresses confidentially only. This model does not address

integrity of the data the system maintains - only who can and cannot access the data." Pg 214
Shon Harris: All-in-One CISSP Certification

QUESTION 168:

Which of the following are the limitations of the Bell-LaPadula model?

A. No policies for changing access data control.
B. All of the choices.
C. Contains covert channels.
D. Static in nature.

Answer: B

Explanation:
Limitations of the BLP model:
Have no policies for changing access data control
Intended for systems with static security levels
Contains covert channels: a low subject can detect the existence of a high object when it is denied access. Sometimes it is enough to hide the content of an abject; also their existence may have to be hidden.
Restricted to confidentiality

QUESTION 169:

Which of the following is a state machine model capturing confidentiality aspects of access control?

A. Clarke Wilson
B. Bell-LaPadula
C. Chinese Wall
D. Lattice

Answer: B

Explanation:
Bell-LaPadula is a state machine model capturing confidentiality aspects of access control. Access permissions are defined through an Access Control matrix and through a partial ordering of security levels. Security policies prevent information flowing downwards from a high security level to a low security level. BLP only considers the information flow that occurs when a subject observes or alters an object.

QUESTION 170:

With the BLP model, access permissions are defined through:

A. Filter rules
B. Security labels
C. Access Control matrix
D. Profiles

Answer: C

Explanation:
Bell-LaPadula is a state machine model capturing confidentiality aspects of access control. Access permissions are defined through an Access Control matrix and through a partial ordering of security levels. Security policies prevent information flowing downwards from a high security level to a low security level. BLP only considers the information flow that occurs when a subject observes or alters an object.

QUESTION 171:

With the BLP model, security policies prevent information flowing downwards from a:

A. Low security level
B. High security level
C. Medium security level
D. Neutral security level

Answer: B

Explanation:
Bell-LaPadula is a state machine model capturing confidentiality aspects of access control. Access permissions are defined through an Access Control matrix and through a partial ordering of security levels. Security policies prevent information flowing downwards from a high security level to a low security level. BLP only considers the information flow that occurs when a subject observes or alters an object.

QUESTION 172:

When will BLP consider the information flow that occurs?

A. When a subject alters on object.
B. When a subject accesses an object.
C. When a subject observer an object.
D. All of the choices.

Answer: D

Explanation:
Bell-LaPadula is a state machine model capturing confidentiality aspects of access control. Access permissions are defined through an Access Control matrix and through a

partial ordering of security levels. Security policies prevent information flowing downwards from a high security level to a low security level. BLP only considers the information flow that occurs when a subject observes or alters an object.

QUESTION 173:

In the Bell-LaPadula model, the Star-property is also called:
A.) The simple security property
B.) The confidentiality property
C.) The confinement property
D.) The tranquility property

Answer: C

QUESTION 174:

The Lattice Based Access Control model was developed MAINLY to deal with:

A. Affinity
B. None of the choices.
C. Confidentiality
D. Integrity

Answer: D

Explanation:
We think this is D:
"Identity-Based Access Control"
"...grant or deny access based on the identity of the subject. ...user identity or group membership." Harris, 3rd Ed, p 163. Group membership would be part of a user profile. Rule based based can be ID or "a set of complex rules that must be met. ... Rule-based access control is not necessarily identity based." Harris, 3rd Ed, p 167. So item "C" is out.
"A" and "B" are not access control methods. I would note that in Harris, there is no reference to "ID based access control". "Role-based access control would be the VERY best answer to the question - role information would be included as part of the users profile.

QUESTION 175:

With the Lattice Based Access Control model, a security class is also called a:

A. Control factor
B. Security label
C. Mandatory number
D. Serial ID

Answer: B

Explanation:
The Lattice Based Access Control model was developed to deal mainly with information flow in computer systems. Information flow is clearly central to confidentiality but to some extent it also applies to integrity. The basic work in this area was done around 1970 and was driven mostly by the defense sector. Information flow in computer systems is concerned with flow from one security class (also called security label) to another. These controls are applied to objects. An object is a container of information, and an object can be a directory or file.

QUESTION 176:

Under the Lattice Based Access Control model, a container of information is a(n):

A. Object
B. Model
C. Label

Answer: A

Explanation:
The Lattice Based Access Control model was developed to deal mainly with information flow in computer systems. Information flow is clearly central to confidentiality but to some extent it also applies to integrity. The basic work in this area was done around 1970 and was driven mostly by the defense sector. Information flow in computer systems is concerned with flow from one security class (also called security label) to another. These controls are applied to objects. An object is a container of information, and an object can be a directory or file.

QUESTION 177:

What Access Control model was developed to deal mainly with information flow in computer systems?

A. Lattice Based
B. Integrity Based
C. Flow Based
D. Area Based

Answer: A

Explanation:
The Lattice Based Access Control model was developed to deal mainly with information flow in computer systems. Information flow is clearly central to confidentiality but to

some extent it also applies to integrity. The basic work in this area was done around 1970 and was driven mostly by the defense sector. Information flow in computer systems is concerned with flow from one security class (also called security label) to another. These controls are applied to objects. An object is a container of information, and an object can be a directory or file.

QUESTION 178:

The Lattice Based Access Control model was developed to deal mainly with _____ in computer systems.

A. Access control
B. Information flow
C. Message routes
D. Encryption

Answer: B

Explanation:
Information flow is clearly central to confidentiality but to some extent it also applies to integrity. The basic work in this area was done around 1970 and was driven mostly by the defense sector. Information flow in computer systems is concerned with flow from one security class (also called security label) to another. These controls are applied to objects. An object is a container of information, and an object can be a directory or file.

QUESTION 179:

In the Lattice Based Access Control model, controls are applied to:

A. Scripts
B. Objects
C. Models
D. Factors

Answer: B

Explanation:
Information flow is clearly central to confidentiality but to some extent it also applies to integrity. The basic work in this area was done around 1970 and was driven mostly by the defense sector. Information flow in computer systems is concerned with flow from one security class (also called security label) to another. These controls are applied to objects. An object is a container of information, and an object can be a directory or file.

QUESTION 180:

Access control techniques do not include:
A.) Rule-Based Access Controls
B.) Role-Based Access Controls
C.) Mandatory Access Controls
D.) Random Number Based Access Control

Answer: D

QUESTION 181:

An access control policy for a bank teller is an example of the implementation of which of the following?
A.) rule-based policy
B.) identity-based policy
C.) user-based policy
D.) role-based policy

Answer: D

QUESTION 182:

Access control techniques do not include which of the following choices?
A.) Relevant Access Controls
B.) Discretionary Access Controls
C.) Mandatory Access Controls
D.) Lattice Based Access Controls

Answer: A
"Mandatory Access Control. The authorization of a subject's access to an object depends upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object."
"Rule-based access control is a type of mandatory access control because rules determine this access, rather than the identity of the subjects and objects alone."
"Discretionary Access Control.The subject has authority, within certain limitations, to specify what objects are accessible."
"When a user with certain limitations has the right to alter the access control to certain objects, this is termed as user-directed discretionary access control."
"An identity-based access control is a type of a discretionary access control based on an individual's identity."
"In some instances, a hybrid approach is used, which combines the features of user-based and identity-based discretionary access control."
"Non-discretionary Access Control. A Central authority determines what subjects can have access to certain objects based on the organizational security policy."
"The access controls might be based on the individuals role in the organization (role-based) or the subject's responsibilities and duties (task-based)."

"[Lattice-based] In this type of control, a lattice model is applied.
"Access control can be characterized as context-dependent or content dependent."
Pg. 45-46 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 183:

What is called a type of access control where a central authority determines what subjects can have access to certain objects, based on the organizational security policy?
A.) Mandatory Access Control
B.) Discretionary Access Control
C.) Non-discretionary Access Control
D.) Rule-based access control

Answer: C
Non-Discretionary Access Control. A central authority determines what subjects can have access to certain objects based on organizational security policy. The access controls may be based on the individual's role in the organization (role-based) or the subject's responsibilities and duties (task-based).
Pg. 33 Krutz: The CISSP Prep Guide.

QUESTION 184:

In non-discretionary access control, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:
A.) the society's role in the organization
B.) the individual's role in the organization
C.) the group-dynamics as they relate to the individual's role in the organization
D.) the group-dynamics as they relate to the master-slave role in the organization

Answer: B
Non-Discretionary Access Control. A central authority determines what subjects can have access to certain objects based on organizational security policy. The access controls may be based on the individual's role in the organization (role-based) or the subject's responsibilities and duties (task-based).
Pg. 33 Krutz: The CISSP Prep Guide.

QUESTION 185:

This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks the user needs to fulfill. What best describes this scenario?
A.) Excessive Rights
B.) Excessive Access
C.) Excessive Permissions
D.) Excessive Privileges

Answer: D

QUESTION 186:

The default level of security established for access controls should be

A. All access
B. Update access
C. Read access
D. No access

Answer: D
"Need to Know and the Principle of Least Privilege are two standard axioms of high-security environments. A user must have a need-to-know to gain access to data or resources. Even if that ser has an equal or greater security classification than the requested information, if they do not have a need-to-know, they are denied access. A need-to-know is the requirement to have access to, knowledge about, or possession of data or a resource to perform specific work tasks. The principle of least privilege is the notion that users should be granted the least amount of access to the secure environment as possible for them to be able to complete their work tasks." Pg 399
Tittel: CISSP Study Guide

QUESTION 187:

Access Control techniques do not include which of the following choices?
A.) Relevant Access Controls
B.) Discretionary Access Control
C.) Mandatory Access Control
D.) Lattice Based Access Controls

Answer: A

QUESTION 188:

Which of the following is a type of mandatory access control?
A.) Rule-based access control
B.) Role-based access control
C.) User-directed access control
D.) Lattice-based access control

Answer: A
Reference: pg 46 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 189:

A central authority determines what subjects can have access to certain objects based on

the organizational security policy is called:
A.) Mandatory Access Control
B.) Discretionary Access Control
C.) Non-Discretionary Access Control
D.) Rule-based Access Control

Answer: C
Reference: pg 46 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 190:

What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?
A.) A capacity table
B.) An access control list
C.) An access control matrix
D.) A capability table

Answer: C

QUESTION 191:

What access control methodology facilitates frequent changes to data permissions?

A. Rule-based
B. List-based
C. Role-based
D. Ticket-based

Answer: A
RBAC - This type of model provides access to resources based on the role the users holds within the company or the tasks that user has been assigned. - Shon Harris All-in-one CISSP Certification Guide pg 937
Rule-based access control is a type of mandatory access control because rules determine this access (such as the correspondence of clearances labels to classification labels), rather than the identity of the subjects and objects alone. . -Ronald Krutz The CISSP PREP Guide (gold edition) pg 45-46

QUESTION 192:

Which of the following is a means of restricting access to objects based on the identity of the subject to which they belong?

A. Mandatory access control
B. Group access control
C. Discretionary access control

D. User access control

Answer: C
The question does not ask about the identity of the accessing subject, the question refers to the subject to which the object belongs (ie the owner).
The owner setting the access rights is the definition of DAC.
"DAC systems grant or deny access based on the identity of the subject. ...." Harris, 3rd Ed, p 163

QUESTION 193:

What is the method of coordinating access to resources based on the listening of permitted IP addresses?

A. MAC
B. ACL
C. DAC
D. None of the choices.

Answer: B

Explanation:
The definition of ACL: A method of coordinating access to resources based on the listing of permitted (or denied) users, network addresses or groups for each resource.

QUESTION 194:

What control is based on a specific profile for each user?

A. Lattice based access control.
B. Directory based access control.
C. Rule based access control.
D. ID based access control.

Answer: C

Explanation:
With this model, information can be easily changed for only one user but this scheme may become a burden in a very large environment. A rule-based access control unit will intercept every request to the server and compare the source specific access conditions with the rights of the user in order to make an access decision. A good example could be a firewall. Here a set of rules defined by the network administrator is recorded in a file. Every time a connection is attempted (incoming or outgoing), the firewall software checks the rules file to see if the connection is allowed. If it is not, the firewall closes the connection.

QUESTION 195:

In a very large environment, which of the following is an administrative burden?

A. Rule based access control.
B. Directory based access control.
C. Lattice based access control
D. ID bases access control

Answer: D

QUESTION 196:

Which of the following is a feature of the Rule based access control?

A. The use of profile.
B. The use of information flow label.
C. The use of data flow diagram.
D. The use of token.

Answer: A

Explanation:
Rule based access control is based on a specific profile for each user. Information can be easily changed for only one user but this scheme may become a burden in a very large environment. A rule-based access control unit will intercept every request to the server and compare the source specific access conditions with the rights of the user in order to make an access decision. A good example could be a firewall. Here a set of rules defined by the network administrator is recorded in a file. Every time a connection is attempted (incoming or outgoing), the firewall software checks the rules file to see if the connection is allowed. If it is not, the firewall closes the connection.

QUESTION 197:

What is an access control model?

A. A formal description of access control ID specification.
B. A formal description of security policy.
C. A formal description of a sensibility label.
D. None of the choices.

Answer: B

Explanation:
What is an access control model? It is a formal description of a security policy. What

is a security policy? A security policy captures the security requirements of an enterprise or describes the steps that have to be taken to achieve security. Security models are used in security evaluation, sometimes as proofs of security.

QUESTION 198:

Which of the following is true about MAC?

A. It is more flexible than DAC.
B. It is more secure than DAC.
C. It is less secure than DAC.
D. It is more scalable than DAC.

Answer: B

Explanation:
Mandatory controls are access controls that are based on a policy that the user, and more importantly the processes running with that user's privileges, is not allowed to violate. An example of this is "Top Secret" data is configured so that regardless of what the user does, the data cannot be transmitted to someone who does not have "Top Secret" status. Thus no "trojan horse" program could ever do what the user is not allowed to do anyway. The restrictions of mandatory controls are (at least in normal mode) also applied to the user who in a discretionary system would be "root", or the superuser.

QUESTION 199:

Which of the following is true regarding a secure access model?

A. Secure information cannot flow to a more secure user.
B. Secure information cannot flow to a less secure user.
C. Secure information can flow to a less secure user.
D. None of the choices.

Answer: B

Explanation:
Access restrictions such as access control lists and capabilities sometimes are not enough. In some cases, information needs to be tightened further, sometimes by an authority higher than the owner of the information. For example, the owner of a top-secret document in a government office might deem the information available to many users, but his manager might know the information should be restricted further than that. In this case, the flow of information needs to be controlled -- secure information cannot flow to a less secure user.

QUESTION 200:

In the Information Flow Model, what acts as a type of dependency?

A. State
B. Successive points
C. Transformation
D. Flow

Answer: D

Explanation:
A flow is a type of dependency that relates two versions of the same object, and thus the transformation of one state of that object into another, at successive points in time.

QUESTION 201:

A firewall can be classified as a:

A. Directory based access control.
B. Rule based access control.
C. Lattice based access control.
D. ID based access control.

Answer: B

Explanation:
Rule based access control is based on a specific profile for each user. Information can be easily changed for only one user but this scheme may become a burden in a very large environment. A rule-based access control unit will intercept every request to the server and compare the source specific access conditions with the rights of the user in order to make an access decision. A good example could be a firewall. Here a set of rules defined by the network administrator is recorded in a file. Every time a connection is attempted (incoming or outgoing), the firewall software checks the rules file to see if the connection is allowed. If it is not, the firewall closes the connection.

QUESTION 202:

Which of the following are the two most well known access control models?

A. Lattice and Biba
B. Bell LaPadula and Biba
C. Bell LaPadula and Chinese war
D. Bell LaPadula and Info Flow

Answer: B

Explanation:
The two most well known models are Bell&LaPadula [1973] and Biba[1977]. Both were designed in and for military environments.

QUESTION 203:

What security model implies a central authority that determines what subjects can have access to what objects?
A.) Centralized access control
B.) Discretionary access control
C.) Mandatory access control
D.) Non-discretionary access control

Answer: D
A role-based access control (RBAC) model, also called nondiscretionary access control, uses a centrally administrated set of controls to determine how subjects and objects interact. - Shon Harris, "CISSP All-in-One Exam Guide", 3rd Ed, p 165.

QUESTION 204:

Which of the following is best known for capturing security requirements of commercial applications?

A. Lattice
B. Biba
C. Bell LaPadula
D. Clark and Wilson

Answer: D

Explanation:
This model attempts to capture security requirements of commercial applications. 'Military' and 'Commercial' are shorthand for different ways of using computers. This model has emphasis on integrity:
Internal consistency: properties of the internal state of a system
External consistency: relation of the internal state of a system to the outside world

---

QUESTION 205:

Which of the following is a straightforward approach that provides access rights to subjects for objects?
A.) Access Matrix model

B.) Take-Grant Model
C.) Bell-LaPadula Model
D.) Biba Model

Answer: A
"The access matrix is a straightforward approach that provides access rights to subjects for objects. Access rights are of the type read, write, and execute. A subject is an active entity that is seeking rights to a resource or object. A subject can be a person, a program, or a process. An object is a passive entity, such as a file or a storage resource." Pg 272 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 206:

What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?
A.) Mandatory model
B.) Discretionary model
C.) Lattice model
D.) Rule model

Answer: C
Lattice-based access control provides an upper bound and lower bound of access capabilities for every subject and object relationship.
Pg 156 Shon Harris All-In-One CISSP Certification Exam Guide

QUESTION 207:

Which access control would a lattice-based access control be an example of?
A.) Mandatory access control
B.) Discretionary access control
C.) Non-discretionary access control
D.) Rule-based access control

Answer: C
"Lattice-based access control is a variation of nondiscretionary access controls. Lattice-based controls define upper and lower bounds of access for every relationship between object and subject. These boundaries can be arbitrary, but they usually follow the military or corporate security label levels.
Subjects under lattice-based access controls are said to have the least upper bound and the greatest lower bound of access to labeled objects based on their assigned lattice position."
Pg. 16 Tittel: CISSP Prep Guide

QUESTION 208:

Who developed one of the first mathematical models of a multilevel-security computer system?

A.) Diffie Hillman
B.) Clark and Wilson
C.) Bell and LaPadula
D.) Gasser and Lipner

Answer: C

QUESTION 209:

Which of the following was the first mathematical model of multilevel security policy?

A. Biba
B. Take-Grant
C. Bell-La Padula
D. Clark Wilson

Answer: C
"In the 1970's, the U.S. military used time-sharing mainframe systems and was concerned about these systems and leakage of classified information. The Bell-LaPadula model was developed to address these concerns. It was the first mathematical model of a multilevel security policy used to define the concept of a secure state machine and modes of access and outline rules of access."
Pg 212 Shon Harris: All-in-One CISSP Certification

QUESTION 210:

Which security model allows the data custodian to grant access privileges to other users?

A. Mandatory
B. Bell-LaPadula
C. Discretionary
D. Clark-Wilson

Answer: C
" Discretionary Access Control. The subject has authority, within certain limitations, to specify what objects are accessible." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 46

QUESTION 211:

What is one issue NOT addressed by the Bell-LaPadula model?

A. Information flow control
B. Security levels
C. Covert channels
D. Access modes

Answer: C

As with any model, the Bell-LaPadula model has some weaknesses. These are the major ones. The model considers normal channels of the information exchange and does not address covert channels. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 275-276

QUESTION 212:

Which one of the following access control models associates every resource and every user of a resource with one of an ordered set of classes?

A. Take-Grant model
B. Biba model
C. Lattice model
D. Clark-Wilson model

Answer: C
With a lattice model you first have to define a set of security classes that can be assigned to users or objects...After
you have defined set of security classes, you define a set flow operations showing when information can flow from
one class to another - Roberta Bragg Cissp Certification Training Guide (que) pg 23

QUESTION 213:

What scheme includes the requirement that the system maintain the separation of duty requirement expressed in the access control triples?

A. Bella
B. Lattice
C. Clark-Wilson
D. Bell-LaPadula

Answer: C

Explanation:
Separation of duty is necessarily determined by conditions external to the computer system. The Clark-Wilson scheme includes the requirement that the system maintain the separation of duty requirement expressed in the access control triples. Enforcement is on a per-user basis, using the user ID from the access control triple.

QUESTION 214:

The access matrix model consists of which of the following parts? (Choose all that apply)

A. A function that returns an objects type.
B. A list of subjects.
C. A list of objects.

Answer: A, B, C

Explanation:
The access matrix model consists of four major parts:
A list of objects
A list of subjects
A function T that returns an object's type
The matrix itself, with the objects making the columns and the subjects making the rows
Note: This question seems to confuse access control matrix, Harris, 3rd Ed, p 169 with access control types, Ibid, p 188ff
"An access control matrix is a table of subjects and objects indicating what actions ... subjects can take upon ... objects", Harris, 3rd Ed, p 169.
It would be right if item "A" was "a function that returned an access right"

QUESTION 215:

The access matrix model has which of the following common implementations?

A. Access control lists and capabilities.
B. Access control lists.
C. Capabilities.
D. Access control list and availability.

Answer: A

Explanation:
The two most used implementations are access control lists and capabilities. Access control lists are achieved by placing on each object a list of users and their associated rights to that object.

QUESTION 216:

The lattice-based model aims at protecting against:

A. Illegal attributes.
B. None of the choices.
C. Illegal information flow among the entities.
D. Illegal access rights

Answer: C

Explanation:
The lattice-based model aims at protecting against illegal information flow among the entities. One security class is given to each entity in the system. A flow relation

among the security classes is defined to denote that information in one class can flow into another class.

QUESTION 217:

Which of the following are the components of the Chinese wall model?

A. Conflict if interest.
B. All of the choices.
C. Subject
D. Company Datasets.

Answer: B

Explanation:
The model has the following component:
COMPONENT EXAMPLE
Subject Analyst
Object Data item for a single client
Company Datasets Give for each company its own company dataset
Conflict of interest classes Give for each object companies that have a conflict of interest
Labels Company dataset + conflict of interest class
Sanitized information No access restriction

QUESTION 218:

Enforcing minimum privileges for general system users can be easily achieved through the use of:

A. TSTEC
B. RBAC
C. TBAC
D. IPSEC

Answer: B

Explanation:
Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges couldn't be used to circumvent the organizational security policy. Although the concept of least privilege currently exists within the context of the TCSEC, requirements restrict those privileges of the system administrator. Through the use of RBAC, enforced minimum privileges for general system users can be easily achieved.

QUESTION 219:

What is necessary for a subject to have write access to an object in a Multi-Level Security Policy?
A.) The subject's sensitivity label must dominate the object's sensitivity label
B.) The subject's sensitivity label subordinates the object's sensitivity label
C.) The subject's sensitivity label is subordinated by the object's sensitivity label
D.) The subject's sensitivity label is dominated by the object's sensitivity label

Answer: D
Reference: "
"The Bell-LaPadula model has a simple security rule, which means that a subject cannot read data from a higher level (no read up). The *-property rule means that a subject cannot write to an object at a lower level (no write down)." - Shon Harris, "CISSP All-in-One Exam Guide", 3rd Ed, p 327. Therefore the object must be at the same or higher level.
"The Bell-LaPadula model is an example of a multilevel security modelThe Bell-LaPadula model is an example of a multilevel security model..." - Shon Harris, "CISSP All-in-One Exam Guide", 3rd Ed, p 298.
Simple security property. A subject can read an object if the access of the class of the subject dominates the access class of the object. Thus, a subject can read down but cannot read up." Pg 105 Hansche: Official (ISC)2 Guide to the CISSP Exam

QUESTION 220:

Which of the following security modes of operation involved the highest risk?
A.) Compartmented Security Mode
B.) Multilevel Security Mode
C.) System-High Security Mode
D.) Dedicated Security Mode

Answer: B
"Security Modes
In a secure environment, information systems are configured to process information in one of four security modes. These modes are set out by the Department of Defense as follows:
Systems running compartmental security mode may process two or more types of compartmented information. All system users must have an appropriate clearance to access all information processed by the system but do not necessarily have a need to know all of the information in the system. Compartments are subcategories or compartments within the different classification levels and extreme care is taken to preserve the information within the different compartments. The system may be classified at the Secret level but contain five different compartments, all classified Secret. If a user has only the need to know about two of the five different compartments to do their job, that user can access the system but can only access the two compartments. Compartmented systems are usually dedicated systems for each specific compartment to prevent the chance of any errors, because compartmentalization is the most

secret of all the secrets.
Systems running in the dedicated security mode are authorized to process only a specific classification level at a time, and all system users must have clearance and a need to know that information.
Systems running in multilevel security mode are authorized to process information at more than one level of security even when all system users do not have appropriate clearances or a need to know for all information processed by the system.
Systems running in system-high security mode are authorized to process only information that all system users are cleared to read and to have a valid need to know. These systems are not trusted to maintain separation between security levels, and all information processed by these systems must be handled as if it were classified at the same level as the most highly classified information processed by the system."
Pg. 234 Tittel: CISSP Study Guide

QUESTION 221:

Controlled Security Mode is also known as:
A.) Multilevel Security Mode
B.) Partitioned Security Mode
C.) Dedicated Security Mode
D.) System-high Security Mode

Answer: A
Reference: pg 264 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 222:

The unauthorized mixing of data of one sensitivity level and need-to-know with data of a lower sensitivity level, or different need-to-know, is called data

A. Contamination
B. Seepage
C. Aggregation
D. Commingling

Answer: A ?
WOW if you are reading these comments then you know I have disagreed with a bunch of the original answers!Well here is another.The original was Seepage.I think it is Contamination.
"The intermixing of data at different sensitivity and need-to-know levels.The lower-level data is said to be contaminated by the higher-level data; thus contaminating (higher-level) data might
not receive the required level of protection"-Ronald Krutz The CISSP PREP Guide (gold edition) pg 890

QUESTION 223:

Which one of the following should be employed to protect data against undetected corruption?

A. Non-repudiation
B. Encryption
C. Authentication
D. Integrity

Answer: D

QUESTION 224:

Which of the following is a communication path that is not protected by the system's normal security mechanisms?
A.) A trusted path
B.) A protection domain
C.) A covert channel
D.) A maintenance hook

Answer: C

QUESTION 225:

A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?
A.) Covert channel
B.) Overt channel
C.) Opened channel
D.) Closed channel

Answer: B
"An overt channel is a channel of communication that was developed specifically for communication purposes. Processes should be communicating through overt channels, not covert channels." Pg 237 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 226:

Covert channel is a communication channel that can be used for:

A. Hardening the system.
B. Violating the security policy.
C. Protecting the DMZ.
D. Strengthening the security policy.

Answer: B

Explanation:
Covert channel is a communication channel that allows transfer of information in a manner that violates the system's security policy.

QUESTION 227:

What is an indirect way to transmit information with no explicit reading of confidential information?

A. Covert channels
B. Backdoor
C. Timing channels
D. Overt channels

Answer: A

Explanation:
Covert channels: indirect ways for transmitting information with no explicit reading of confidential information. This kind of difficulties induced some researchers to re-think from scratch the whole problem of guaranteeing security in computer systems.

QUESTION 228:

Which one of the following describes a covert timing channel?

A. Modulated to carry an unintended information signal that can only be detected by special, sensitive receivers.
B. Used by a supervisor to monitor the productivity of a user without their knowledge.
C. Provides the timing trigger to activate a malicious program disguised as a legitimate function.
D. Allows one process to signal information to another by modulating its own use of system resources.

Answer: D
A covert channel in which one process signals information to another by modulating its own use of system resources (for example, CPU time) in such a way that this manipulation affects the real response time observed by the second process. - Shon Harris All-in-one CISSP Certification Guide pg 929

QUESTION 229:

Covert channel analysis is required for

A. Systems processing Top Secret or classified information.
B. A Trusted Computer Base with a level of trust B2 or above.
C. A system that can be monitored in a supervisor state.
D. Systems that use exposed communication links.

Answer: B
Table 6.6 Standards Comparison
B2 Structured Protection (covert channel, device labels, subject sensitivity labels, trusted path, trusted facility management, configuration management) F4+E4 EAL5 - Roberta Bragg CISSP Certification Training Guide (que) pg 370

QUESTION 230:

In multi-processing systems, which one of the following lacks mandatory controls and is NORMALLY AVOIDED for communication?

A. Storage channels
B. Covert channels
C. Timing channels
D. Object channels

Answer: B
Covert channel - A communication path that enables a process to transmit information in a way that violates the system's security policy.- Shon Harris All-in-one CISSP Certification Guide pg 929

QUESTION 231:

What security risk does a covert channel create?

A. A process can signal information to another process.
B. It bypasses the reference monitor functions.
C. A user can send data to another user.
D. Data can be disclosed by inference.

Answer: B
The risk is not that a process can signal another process. The risk is that the signaling bypasses the reference monitor functions
(ie the communication is not screened by the security kernel that implements the reference monitor).

QUESTION 232:

What is the essential difference between a self-audit and an independent audit?
A.) Tools used
B.) Results
C.) Objectivity
D.) Competence

Answer: C

QUESTION 233:

What is called the formal acceptance of the adequacy of a system's overall security by the management?
A.) Certification
B.) Acceptance
C.) Accreditation
D.) Evaluation

Answer: C

QUESTION 234:

FIPS-140 is a standard for the security of:

A.) Cryptographic service providers
B.) Smartcards
C.) Hardware and software cryptographic modules
D.) Hardware security modules

Answer: C

QUESTION 235:

Which of the following will you consider as the MOST secure way of authentication?

A. Biometric
B. Password
C. Token
D. Ticket Granting

Answer: A

Explanation:
Biometric authentication systems take advantage of an individual's unique physical characteristics in order to authenticate that person's identity. Various forms of biometric authentication include face, voice, eye, hand, signature, and fingerprint, each have their own advantages and disadvantages. When combined with the use of a PIN it can provide two factors authentication.

QUESTION 236:

In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessicity of answering 2 questions:

A.) what was the sex of a person and his age
B.) what part of the body to be used and how to accomplish identification to be viable
C.) what was the age of a person and his income level
D.) what was the tone of the voice of a person and his habits

Answer: B

QUESTION 237:

What is called the percentage of invalid subjects that are falsely accepted?
A.) False Rejection Rate (FRR) or Type I Error
B.) False Acceptance Rate (FAR) or Type II Error
C.) Crossover Error Rate (CER)
D.) True Acceptance Rate (TAR) or Type III error

Answer: B

QUESTION 238:

Which of the following biometrics devices has the highs Crossover Error Rate (CER)?
A.) Iris scan
B.) Hang Geometry
C.) Voice pattern
D.) Fingerprints

Answer: C

QUESTION 239:

Which of the following biometric parameters are better suited for authentication use over a long period of time?
A.) Iris pattern
B.) Voice pattern
C.) Signature dynamics
D.) Retina pattern

Answer: A

QUESTION 240:

Which one of the following is the MOST critical characteristic of a biometrics system?

A. Acceptability
B. Accuracy
C. Throughput
D. Reliability

Answer: B
We don't agree with the original answer, which was throughput. Granted throughput is vital but Krutz lists accuracy is most important.
In addition to the accuracy of the biometric systems, there are OTHER factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
-Ronald Krutz The CISSP PREP Guide (gold edition) pg 51

QUESTION 241:

Which of the following biometric devices has the lowest user acceptance level?
A.) Voice recognition
B.) Fingerprint scan
C.) Hand geometry
D.) Signature recognition

Answer: B

QUESTION 242:

Biometric performance is most commonly measured in terms of:

A. FRR and FAR
B. FAC and ERR
C. IER and FAR
D. FRR and GIC

Answer: A

Explanation:
Biometric performance is most commonly measured in two ways: False Rejection Rate (FRR), and False Acceptance Rate (FAR). The FRR is the probability that you are not authenticated to access your account. A strict definition states that the FRR is the probability that a mated comparison (i.e. 2 biometric samples of the same finger) incorrectly determines that there is no match.

QUESTION 243:

What is the most critical characteristic of a biometric identifying system?
A.) Perceived intrusiveness
B.) Storage requirements
C.) Accuracy
D.) Reliability

Answer: C

QUESTION 244:

Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?
A.) Retina scans
B.) Iris scans
C.) Palm scans
D.) Skin scans

Answer: D
Biometrics:
Fingerprints
Palm Scan
Hand Geometry
Retina Scan
Iris Scan
Signature Dynamics
Keyboard Dynamic
Voice Print
Facial Scan
Hand Topology
Pg. 128-130 Shon Harris All-In-One CISSP Certification Exam Guide

---

QUESTION 245:

In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessicity of answering 2 questions:
A.) What was the sex of a person and his age
B.) what part of body to be used and how to accomplish identification to be viable
C.) what was the age of a person and his income level
D.) what was the tone of the voice of a person and his habits

Answer: B

QUESTION 246:

You are comparing biometric systems. Security is the top priority. A low _____ is most important in this regard.

A. FAR
B. FRR
C. MTBF
D. ERR

Answer: A

Explanation:
When comparing biometric systems, a low false acceptance rate is most important when security is the priority. Whereas, a low false rejection rate is most important when convenience is the priority. All biometric implementations balance these two criteria. Some systems use very high FAR's such as 1 in 300. This means that the likelihood that the system will accept someone other than the enrolled user is 1 in 300. However, the likelihood that the system will reject the enrolled user (its FRR) is very low, giving them ease of use, but with low security. Most fingerprint systems should be able to run with FARs of 1 in 10,000 or better.

QUESTION 247:

Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. To have a valid measure of the system performance:
A.) The CER is used.
B.) the FRR is used
C.) the FAR is used
D.) none of the above choices is correct

Answer: A
"When a biometric system reject an authorized individual, it is called a Type 1 error. When the system accepts impostors who should be rejected, it is called a Type II error. The goal is to obtain low numbers for each type of error. When comparing different biometric systems, many different variables are used, but one of the most important variables is the crossover error rate (CER). This rating is stated in a percentage and represents the point at which the false rejection rate equals the false acceptance rate. This rating is the most important measurement when determining the system's accuracy." Pg 113 Shon Harris: All-in-One CISSP Certification

---

QUESTION 248:

The quality of finger prints is crucial to maintain the necessary:

A. FRR
B. ERR and FAR
C. FAR
D. FRR and FAR

Answer: D

Explanation:
Another factor that must be taken into account when determining the necessary FAR and FRR for your organization is the actual quality of the fingerprints in your user population. ABC's experience with several thousand users, and the experience of its customers, indicates that a percentage of the populations do not have fingerprints of sufficient quality to allow for authentication of the individual. Approximately 2.5% of

employees fall into this group in the general office worker population. For these users, a smart card token with password authentication is recommended.

QUESTION 249:

By requiring the user to use more than one finger to authenticate, you can:

A. Provide statistical improvements in EAR.
B. Provide statistical improvements in MTBF.
C. Provide statistical improvements in FRR.
D. Provide statistical improvements in ERR.

Answer: C

Explanation:
Statistical improvements in false rejection rates can also be achieved by requiring the user to use more than one finger to authenticate. Such techniques are referred to as flexible verification.

QUESTION 250:

Which of the following is being considered as the most reliable kind of personal identification?

A. Token
B. Finger print
C. Password
D. Ticket Granting

Answer: B

Explanation:
Every person's fingerprint is unique and is a feature that stays with the person throughout his/her life. This makes the fingerprint the most reliable kind of personal identification because it cannot be forgotten, misplaced, or stolen. Fingerprint authorization is potentially the most affordable and convenient method of verifying a person's identity.

QUESTION 251:

Which of the following methods is more microscopic and will analyze the direction of the ridges of the fingerprints for matching?

A. None of the choices.
B. Flow direct
C. Ridge matching

D. Minutia matching

Answer: D

Explanation:
There are two approaches for capturing the fingerprint image for matching: minutia matching and global pattern matching. Minutia matching is a more microscopic approach that analyzes the features of the fingerprint, such as the location and direction of the ridges, for matching. The only problem with this approach is that it is difficult to extract the minutiae points accurately if the fingerprint is in some way distorted. The more macroscopic approach is global pattern matching where the flow of the ridges is compared at all locations between a pair of fingerprint images; however, this can be affected by the direction that the image is rotated.

QUESTION 252:

Which of the following are the types of eye scan in use today?

A. Retinal scans and body scans.
B. Retinal scans and iris scans.
C. Retinal scans and reflective scans.
D. Reflective scans and iris scans.

Answer: B

Explanation:
There are two types of eye scan in use today for authentication purposes: retinal scans and iris scans. Retinal Scan technology maps the capillary pattern of the retina, a thin (1/50th inch) nerve on the back of the eye. To enroll, a minimum of five scans is required, which takes 45 seconds. The subject must keep his head and eye motionless within 1/2" of the device, focusing on a small rotating point of green light. 320 - 400 points of reference are captured and stored in a 35-byte field, ensuring the measure is accurate with a negligible false rejection rate.
This compares to 30-70 points of reference for a finger scan. Unfortunately a retinal scan is considerably more intrusive than an iris scans and many people are hesitant to use the device [Retina-scan]. In addition a significant number of people may be unable to perform a successful enrolment, and there exist degenerative diseases of the retina that alter the scan results over time. Despite these disadvantages, there are several successful implementations of this technology [Retina-scan].

QUESTION 253:

Which of the following eye scan methods is considered to be more intrusive?

A. Iris scans
B. Retinal scans

C. Body scans
D. Reflective scans

Answer: B

Explanation:
There are two types of eye scan in use today for authentication purposes: retinal scans and iris scans. Retinal Scan technology maps the capillary pattern of the retina, a thin (1/50th inch) nerve on the back of the eye. To enroll, a minimum of five scans is required, which takes 45 seconds. The subject must keep his head and eye motionless within 1/2" of the device, focusing on a small rotating point of green light. 320 - 400 points of reference are captured and stored in a 35-byte field, ensuring the measure is accurate with a negligible false rejection rate.
This compares to 30-70 points of reference for a finger scan. Unfortunately a retinal scan is considerably more intrusive than an iris scans and many people are hesitant to use the device [Retina-scan]. In addition a significant number of people may be unable to perform a successful enrolment, and there exist degenerative diseases of the retina that alter the scan results over time. Despite these disadvantages, there are several successful implementations of this technology [Retina-scan].

QUESTION 254:

Which of the following offers greater accuracy then the others?

A. Facial recognition
B. Iris scanning
C. Finger scanning
D. Voice recognition

Answer: B

Explanation:
Iris scanning offers greater accuracy than finger scanning, voice or facial recognition, hand geometry or keystroke analysis. It is safer and less invasive than retinal scanning, an important legal consideration [Nuger]. Any company thinking of using biometrics would do well to ensure that they comply with existing privacy laws.

QUESTION 255:

In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
A.) These factors include the enrollment time and the throughput rate, but not acceptability.
B.) These factors do not include the enrollment time, the throughput rate, and acceptability.
C.) These factors include the enrollment time, the throughput rate, and acceptability.
D.) These factors include the enrollment time, but not the throughput rate, neither the acceptability.

Answer: C
In addition to the accuracy of the biometric systems, there are OTHER factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
-Ronald Krutz The CISSP PREP Guide (gold edition) pg 51

QUESTION 256:

What physical characteristics does a retinal scan biometric device measure?
A.) The amount of light reaching the retina
B.) The amount of light reflected by the retina
C.) The size, curvature, and shape of the retina
D.) The pattern of blood vessels at the back of the eye

Answer: D

QUESTION 257:

Type II errors occur when which of the following biometric system rates is high?

A. False accept rate
B. False reject rate
C. Crossover error rate
D. Speed and throughput rate

Answer: A
There are three main performance issues in biometrics. These measures are as follows:
False Rejection Rate (FRR) or Type 1 Error. The percentage of valid subjects that are falsely rejected.
False Acceptance Rate (FAR) or Type 2 Error. The percentage of invalid subjects that are falsely accepted.
Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate.
pg 38 Krutz: The CISSP Prep Guide

QUESTION 258:

Which of the following are the valid categories of hand geometry scanning?

A. Electrical and image-edge detection.
B. Mechanical and image-edge detection.
C. Logical and image-edge detection.
D. Mechanical and image-ridge detection.

Answer: B

Explanation:
Hand geometry reading (scanning) devices usually fall into one of two categories: mechanical or image-edge detection. Both methods are used to measure specific characteristics of a person's hand such as length of fingers and thumb, widths, and depth.

QUESTION 259:

In the world of keystroke dynamics, what represents the amount of time you hold down in a particular key?

A. Dwell time
B. Flight time
C. Dynamic time
D. Systems time

Answer: A

Explanation:
Keystroke dynamics looks at the way a person types at a keyboard. Specifically, keyboard dynamics measures two distinct variables: "dwell time" which is the amount of time you hold down a particular key and "flight time" which is the amount of time it takes a person to switch between keys. Keyboard dynamics systems can measure one's keyboard input up to 1000 times per second.

QUESTION 260:

In the world of keystroke dynamics, what represents the amount of time it takes a person to switch between keys?

A. Dynamic time
B. Flight time
C. Dwell time
D. Systems time.

Answer: B

Explanation:
Keystroke dynamics looks at the way a person types at a keyboard. Specifically, keyboard dynamics measures two distinct variables: "dwell time" which is the amount of time you hold down a particular key and "flight time" which is the amount of time it takes a person to switch between keys. Keyboard dynamics systems can measure one's keyboard input up to 1000 times per second.

QUESTION 261:

Which of the following are the benefits of Keystroke dynamics?

A. Low cost
B. Unintrusive device
C. Transparent
D. All of the choices.

Answer: D

Explanation:
Keystroke dynamics is behavioral in nature. It works well with users that can "touch type". Key advantages in applying keyboard dynamics are that the device used in this system, the keyboard, is unintrusive and does not detract from one's work. Enrollment as well as identification goes undetected by the user. Another inherent benefit to using keystroke dynamics as an identification device is that the hardware (i.e. keyboard) is inexpensive. Currently, plug-in boards, built-in hardware and firmware, or software can represent keystroke dynamics systems.

QUESTION 262:

DSV as an identification method check against users:

A. Fingerprints
B. Signature
C. Keystrokes
D. Facial expression

Answer: B

Explanation:
Signature identification, also known as Dynamic Signature Verification (DSV), is another natural fit in the world of biometrics since identification through one's signature occurs during many everyday transactions. Any process or transaction that requires an individual's signature is a prime contender for signature identification.

QUESTION 263:

Signature identification systems analyze what areas of an individual's signature?

A. All of the choices EXCEPT the signing rate.
B. The specific features of the signature.
C. The specific features of the process of signing one's signature.
D. The signature rate.

Answer: A

Explanation:
Signature identification systems analyze two different areas of an individual's signature: the specific features of the signature and specific features of the process of signing one's signature. Features that are taken into account and measured include speed, pen pressure, directions, stroke length, and the points in time when the pen is lifted from the paper.

QUESTION 264:

What are the advantages to using voice identification?

A. All of the choices.
B. Timesaving
C. Reliability
D. Flexibility

Answer: A

Explanation:
The many advantages to using voice identification include:
Considered a "natural" biometric technology
Provides eyes and hands-free operation
Reliability
Flexibility
Timesaving data input
Eliminate spelling errors
Improved data accuracy

QUESTION 265:

What are the methods used in the process of facial identification?

A. None of the choices.
B. Detection and recognition.
C. Scanning and recognition.
D. Detection and scanning.

Answer: B

Explanation:
The process of facial identification incorporates two significant methods: detection and recognition.

QUESTION 266:

In the process of facial identification, the basic underlying recognition technology of facial

identification involves:

A. Eigenfeatures of eigenfaces.
B. Scanning and recognition.
C. Detection and scanning.
D. None of the choices.

Answer: A

Explanation:
Recognition is comparing the captured face to other faces that have been saved and stored in a database. The basic underlying recognition technology of facial feature identification involves either eigenfeatures (facial metrics) or eigenfaces. The German word "eigen" refers to recursive mathematics used to analyze unique facial characteristics.

QUESTION 267:

What is known as the probability that you are not authenticated to access your account?

A. ERR
B. FRR
C. MTBF
D. FAR

Answer: B

Explanation:
Biometric performance is most commonly measured in two ways: False Rejection Rate (FRR), and False Acceptance Rate (FAR). The FRR is the probability that you are not authenticated to access your account. A strict definition states that the FRR is the probability that a mated comparison (i.e. 2 biometric samples of the same finger) incorrectly determines that there is no match.

QUESTION 268:

What is known as the chance that someone other than you is granted access to your account?

A. ERR
B. FAR
C. FRR
D. MTBF

Answer: B

Explanation:
The FAR is the chance that someone other than you is granted access to your account, in other words, the probability that a non-mated comparison (i.e. two biometric samples of different fingers) match. FAR and FRR numbers are generally expressed in terms of probability.

QUESTION 269:

What is typically used to illustrate the comparative strengths and weaknesses of each biometric technology?

A. Decipher Chart
B. Zephyr Chart
C. Cipher Chart
D. Zapper Chart

Answer: B

Explanation:
The Zephyr Chart illustrates the comparative strengths and weaknesses of each biometric technology. The eight primary biometric technologies are listed around the outer border, and for each technology the four major evaluation criteria are ranked from outside (better) to inside (worse). Looking at dynamic signature verification (DSV) will illustrate how the Zephyr Chart works.

QUESTION 270:

In terms of the order of effectiveness, which of the following technologies is the most affective?

A. Fingerprint
B. Iris scan
C. Keystroke pattern
D. Retina scan

Answer: B

Explanation:
The order of effectiveness has not changed for a few years. It is still the same today as it was three years ago. The list below present them from most effective to list effective:
Iris scan
Retina scan
Fingerprint
Hand geometry
Voice pattern

Keystroke pattern
Signature

QUESTION 271:

In terms of the order of effectiveness, which of the following technologies is the least effective?

A. Voice pattern
B. Signature
C. Keystroke pattern
D. Hand geometry

Answer: B

Explanation:
The order of effectiveness has not changed for a few years. It is still the same today as it was three years ago. The list below present them from most effective to list effective:
Iris scan
Retina scan
Fingerprint
Hand geometry
Voice pattern
Keystroke pattern
Signature

QUESTION 272:

In terms of the order of acceptance, which of the following technologies is the MOST accepted?

A. Hand geometry
B. Keystroke pattern
C. Voice Pattern
D. Signature

Answer: C

Explanation:
The order of acceptance has slightly changed in the past years. It was Iris that was the most accepted method three years ago but today we have Voice Pattern that is by far the most accepted. Here is the list from most accepted first to least accepted at the bottom of the list:
Voice Pattern
Keystroke pattern

Signature
Hand geometry
Handprint
Fingerprint
Iris
Retina pattern

QUESTION 273:

In terms of the order of acceptance, which of the following technologies is the LEAST accepted?

A. Fingerprint
B. Iris
C. Handprint
D. Retina patterns

Answer: D

Explanation:
The order of acceptance has slightly changed in the past years. It was Iris that was the most accepted method three years ago but today we have Voice Pattern that is by far the most accepted. Here is the list from most accepted first to least accepted at the bottom of the list:
Voice Pattern
Keystroke pattern
Signature
Hand geometry
Handprint
Fingerprint
Iris
Retina pattern

QUESTION 274:

Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?
A.) Retina scans
B.) Iris scans
C.) Palm scans
D.) Skin scans

Answer: D

QUESTION 275:

Which of the following is true of two-factor authentication?
A.) It uses the RSA public-key signature based algorithm on integers with large prime factors
B.) It requires two measurements of hand geometry
C.) It does not use single sign-on technology
D.) It relies on two independent proofs of identity

Answer: D

QUESTION 276:

What is Kerberos?
A.) A three-headed dog from Egyptian Mythology
B.) A trusted third-party authentication protocol
C.) A security model
D.) A remote authentication dial in user server

Answer: B

QUESTION 277:

Which of the following is true about Kerberos?
A.) It utilized public key cryptography
B.) It encrypts data after a ticket is granted, but passwords are exchanged in plain text
C.) It depends upon symmetric ciphers
D.) It is a second party authentication system

Answer: C
"Kerberos relies upon symmetric key cryptography, specifically Data Encryption Standard (DES), and provides end-to-end security for authentication traffic between the client and the Key Distribution Center (KDC)." Pg. 15 Tittel: CISSP Study Guide

---

QUESTION 278:

Kerberos depends upon what encryption method?
A.) Public Key cryptography
B.) Private Key cryptography
C.) El Gamal cryptography
D.) Blowfish cryptography

Answer: B
Kerberos uses symmetric key cryptography and provides end-to-end security, meaning that information being passed between a user and a service is protected without the need of an intermediate component. Although it allows the use of passwords for authentication, it was designed specifically to eliminate the need for transmitting passwords over the network. Most Kerberos implementations work with cryptography keys and shared secret keys (private keys) instead of passwords. Pg 148 Shon Harris All-In-One CISSP Certification Exam Guide

---

QUESTION 279:

The primary service provided by Kerberos is which of the following?
A.) non-repudiation
B.) confidentiality
C.) authentication
D.) authorization

Answer: C

QUESTION 280:

Which of the following are authentication server systems with operational modes that can implement SS0?
A.) Kerberos, SESAME and KryptoKnight
B.) SESAME, KryptoKnight and NetSP
C.) Kerberos and SESAME
D.) Kerberos, SESAME, KryptoKnight, and NetSP

Answer: D
"Scripts, directory services, thin clients, Kerberos, SESAME, NetSP, scripted access, and KrtyptoKnight are examples of SSO mechanisms."
Pg. 14 Tittel: CISSP Study Guide Second Edition

QUESTION 281:

Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?
A.) Kerberos
B.) SESAME
C.) KryptoKnight
D.) NetSP

Answer: A
"Kerberos is an authentication protocol and was designed in the mid-1980s as part of MIT's Project Athena." Pg 129 Shon Harris: All-in-One CISSP Certification

---

QUESTION 282:

Which of the following is true about Kerberos?
A.) It utilizes public key cryptography
B.) It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C.) It depends upon symmetric ciphers
D.) It is a second party authentication system

Answer: C

QUESTION 283:

One of the differences between Kerberos and KryptoKnight is that there is:
A.) a mapped relationship among the parties takes place
B.) there is a peer-to-peer relationship among the parties with themselves.
C.) there is no peer-to-peer relationship among the parties and the KDC
D.) a peer-to-peer relationship among the parties and the KDC

Answer: D
"Krytponight
The IBM Kryptonight system provides authentication, SSO, and key distribution services. It was designed to support computers with widely varying computational capabilities. KryptoKnight uses a trusted Key Distribution Center (KDC) that knows the secret key of each party. One of the differences between kerberos and KrytoKnight is that there is a peer-to-peer relationship among the parties and the KDC."
Pg. 58 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 284:

Which of the following is the MOST secure network access control procedure to adopt when using a callback device?

A. The user enters a userid and PIN, and the device calls back the telephone number that corresponds to the userid.
B. The user enters a userid, PIN, and telephone number, and the device calls back the telephone number entered.
C. The user enters the telephone number, and the device verifies that the number exists in its database before calling back.
D. The user enters the telephone number, and the device responds with a challenge.

Answer: A

Explanation: Usually a request for a username and password takes place and the NAS may hang up the call in order to call the user back at a predefined phone number. This is a security activity that is used to try and ensure that only authenticated users are given access to the network and it reverse the long distance charges back to the company...However, this security measure can be compromised if someone implements call forwarding. - Shon Harris All-in-one CISSP Certification Guide pg 463

QUESTION 285:

What is called the access protection system that limits connections by calling back the number of a previously authorized location?

A.) Sendback system
B.) Callback forward systems
C.) Callback systems
D.) Sendback forward systems

Answer: C
"Callback systems provide access protection by calling back the number of a previously authorized location, but this control can be compromised by call forwarding." Pg 48 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 286:

A confidential number to verify a user's identity is called a:
A.) PIN
B.) userid
C.) password
D.) challenge

Answer: A

QUESTION 287:

How are memory cards and smart cards different?
A.) Memory cards normally hold more memory than smart cards
B.) Smart cards provide a two-factor authentication whereas memory cards don't
C.) Memory cards have no processing power
D.) Only smart cards can be used for ATM cards

Answer: C
"The main difference between memory cards and smart cards is the processing power. A memory card holds information, but does not process information. A smart card has the necessary hardware and logic to actually process information." Pg 121 Shon Harris CISSP All-In-One Exam Guide

---

QUESTION 288:

They in form of credit card-size memory cards or smart cards, or those resembling small calculators, are used to supply static and dynamic passwords are called:
A.) Tickets
B.) Tokens
C.) Token passing networks
D.) Coupons

Answer: B

QUESTION 289:

Tokens, as a way to identify users are subject to what type of error?

A. Token error
B. Decrypt error
C. Human error
D. Encrypt error

Answer: C

Explanation:
Tokens are a fantastic way of ensuring the identity of a user. However, you must remember that no system is immune to "human error". If the token is lost with it's pin written on it, or if it were loaned with the corresponding pin it would allow for masquerading. This is one of the greatest threats that you have with tokens.

QUESTION 290:

Which of the following factors may render a token based solution unusable?

A. Token length
B. Card size
C. Battery lifespan
D. None of the choices.

Answer: C

Explanation:
Another limitation of some of the tokens is their battery lifespan. For example, in the case of SecurID you have a token that has a battery that will last from 1 to 3 years depending on the type of token you acquired. Some token companies such as Cryptocard have introduced tokens that have a small battery compartment allowing you to change the battery when it is discharged.

QUESTION 291:

Memory only cards work based on:

A. Something you have.
B. Something you know.
C. None of the choices.
D. Something you know and something you have.

Answer: D

Explanation:
Memory Only Card - This type of card is the most common card. It has a magnetic stripe on the back. These cards can offer two-factor authentication, the card itself (something you have) and the PIN (something you know). Everyone is familiar with the use of an ATM (Automated Teller Machine) card. These memory cards are very easy to counterfeit. There was a case in Montreal where a storeowner would swipe the card through for the transaction; he hould then swipe it through a card reader to get a copy while a small hidden camera was registering the PIN as the user was punching it on the pad. This scheme was quickly identified as the victims had one point in common; they all visited the same store.

QUESTION 292:

Which of the following is a disadvantage of a memory only card?

A. High cost to develop.
B. High cost to operate.
C. Physically infeasible.
D. Easy to counterfeit.

Answer: D

Explanation:
Memory Only Card - This type of card is the most common card. It has a magnetic stripe on the back. These cards can offer two-factor authentication, the card itself (something you have) and the PIN (something you know). Everyone is familiar with the use of an ATM (Automated Teller Machine) card. These memory cards are very easy to counterfeit. There was a case in Montreal where a storeowner would swipe the card through for the transaction; he hould then swipe it through a card reader to get a copy, while a small hidden camera was registering the PIN as the user was punching it on the pad. This scheme was quickly identified as the victims had one point in common; they all visited the same store.

QUESTION 293:

The word "smart card" has meanings of:

A. Personal identity token containing IC-s.
B. Processor IC card.
C. IC card with ISO 7816 interface.
D. All of the choices.

Answer: D

Explanation:
The word "smart card" has four different meanings (in order of usage frequency):

IC card with ISO 7816 interface
Processor IC card
Personal identity token containing IC-s
Integrated Circuit(s) Card is ad ID-1 type (specified in ISO 7810) card, into which has been inserted one or more integrated circuits. [ISO 7816]

QUESTION 294:

Processor card contains which of the following components?

A. Memory and hard drive.
B. Memory and flash.
C. Memory and processor.
D. Cache and processor.

Answer: C

Explanation:
Processor cards contain memory and a processor. They have remarkable data processing capabilities. Very often the data processing power is used to encrypt/decrypt data, which makes this type of card a very unique personal identification token. Data processing also permits dynamic storage management, which enables the realization of flexible multifunctional cards.

QUESTION 295:

Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, and faster resource access?
A.) Smart cards
B.) Single Sign-on (SSO)
C.) Kerberos
D.) Public Key Infrastructure (PKI)

Answer: B

QUESTION 296:

What is the main concern with single sign-on?
A.) Maximum unauthorized access would be possible if a password is disclosed
B.) The security administrator's workload would increase
C.) The users' password would be to hard to remember
D.) User access rights would be increased

Answer: A

QUESTION 297:

Which of the following describes the major disadvantage of many SSO implementations?
A.) Once a user obtains access to the system through the initial log-on they can freely roam the network resources without any restrictions
B.) The initial logon process is cumbersome to discourage potential intruders
C.) Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D.) Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Answer: A
Reference: "The major disadvantage of many SSO implementations is that once a user obtains access to the system through the initial logon, the user can freely roam the network resources without any restrictions." pg 53 Krutz: CISSP Prep Guide: Gold Edition

---

QUESTION 298:

Which of the following addresses cumbersome situations where users need to log on multiple times to access different resources?
A.) Single Sign-On (SSO) systems
B.) Dual Sign-On (DSO) systems
C.) Double Sign-On (DS0) systems
D.) Triple Sign-On (TSO) systems

Answer: A

QUESTION 299:

A method for a user to identify and present credentials only once to a system is known as:

A. SEC
B. IPSec
C. SSO
D. SSL

Answer: C

Explanation:
Single Sign-On (SSO) - This is a method for a users to identify and present credentials only once to a system. Information needed for future system access to resources is forwarded by the initial System.
BENEFITS
More efficient user log-on process
Users select stronger passwords
Inactivity timeout and attempt thresholds applied uniformly closer to user point of

entry
Improved timely disabling of all network/computer accounts for terminated users

---

QUESTION 300:

Which of the following correctly describe the features of SSO?

A. More efficient log-on.
B. More costly to administer.
C. More costly to setup.
D. More key exchanging involved.

Answer: A

Explanation:
Single Sign-On (SSO) - This is a method for a users to identify and present credentials only once to a system. Information needed for future system access to resources is forwarded by the initial System.
BENEFITS
More efficient user log-on process
Users select stronger passwords
Inactivity timeout and attempt thresholds applied uniformly closer to user point of entry
Improved timely disabling of all network/computer accounts for terminated users

---

QUESTION 301:

What is the PRIMARY advantage of using a separate authentication server (e.g., Remote Access Dial-In User System, Terminal Access Controller Access Control System) to authenticate dial-in users?

A. Single user logons are easier to manage and audit.
B. Each session has a unique (one-time) password assigned to it.
C. Audit and access information are not kept on the access server.
D. Call-back is very difficult to defeat.

Answer: C

Explanation:
TACACS integrates the authentication and authorization processes. XTACACS keeps the authentication, authorization and accounting processes separate. TACACS+ improves XTACACS by adding two-factor authentication. - Ed Tittle CISSP Study Guide (sybex) pg 745

QUESTION 302:

Within the Open Systems Interconnection (OSI) Reference Model, authentication addresses the need for a network entity to verify both

A. The identity of a remote communicating entity and the authenticity of the source of the data that are received.
B. The authenticity of a remote communicating entity and the path through which communications are received.
C. The location of a remote communicating entity and the path through which communications are received.
D. The identity of a remote communicating entity and the level of security of the path through which data are received.

Answer: A

Explanation:
OSI model needs to know the source of the data and that it is who it says it is. Path it the data take is not cared about
unless source routing is used. The level of security is not cared about inherently by the receiving node (in general)
unless configured. A is the best option in this question.

QUESTION 303:

Which of the following is the most reliable authentication device?
A.) Variable callback system
B.) Smart card system
C.) fixed callback system
D.) Combination of variable and fixed callback system

Answer: B

QUESTION 304:

Which of the following are proprietarily implemented by CISCO?

A. RADIUS+
B. TACACS
C. XTACACS and TACACS+
D. RADIUS

Answer: C

Explanation:
Cisco implemented an enhanced version of TACACS, known as XTACACS (extended TACACS),
which was also compatible with TACACS. It allowed for UDP and TCP encoding. XTACACS contained several improvements: It provided accounting functionality to track length of login and which hosts a user connected to, and it also separated the authentication, authorization, and accounting processes such that they could be independently implemented. None of the three functions are mandatory. XTACACS is described in RFC

1492.
TACACS+ is the latest Cisco implementation. It is best described as XTACACS with improved attribute control (authorization) and accounting.

QUESTION 305:

What is a protocol used for carrying authentication, authorization, and configuration information between a Network Access Server and a shared Authentication Server?

A. IPSec
B. RADIUS
C. L2TP
D. PPTP

Answer: B

Explanation:
RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server, which desires to authenticate its links and a shared Authentication Server. RADIUS is a standard published in RFC2138 as mentioned above.

QUESTION 306:

RADIUS is defined by which RFC?

A. 2168
B. 2148
C. 2138
D. 2158

Answer: C

Explanation:
RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server, which desires to authenticate its links and a shared Authentication Server. RADIUS is a standard published in RFC2138 as mentioned above.

QUESTION 307:

In a RADIUS architecture, which of the following acts as a client?

A. A network Access Server.
B. None of the choices.
C. The end user.

D. The authentication server.

Answer: A

Explanation:
A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response, which is returned.

QUESTION 308:

In a RADIUS architecture, which of the following can ac as a proxy client?

A. The end user.
B. A Network Access Server.
C. The RADIUS authentication server.
D. None of the choices.

Answer: C

Explanation:
A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

QUESTION 309:

Which of the following statements pertaining to RADIUS is incorrect?
A.) A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
B.) Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy
C.) Most RADIUS servers have built-in database connectivity for billing and reporting purposes
D.) Most RADIUS servers can work with DIAMETER servers.

Answer: D

QUESTION 310:

Which of the following is the weakest authentication mechanism?
A.) Passphrases
B.) Passwords
C.) One-time passwords
D.) Token devices

Answer: B

QUESTION 311:

What is the PRIMARY use of a password?
A.) Allow access to files
B.) Identify the user
C.) Authenticate the user
D.) Segregate various user's accesses

Answer: C

QUESTION 312:

Software generated passwords have what drawbacks?

A. Passwords are not easy to remember.
B. Password are too secure.
C. None of the choices.
D. Passwords are unbreakable.

Answer: A

Explanation:
Passwords generated by a software package or some operating systems. These password generators are good at producing unique and hard to guess passwords, however you must ensure that they are not so hard that people can't remember them. If you force your users to write their passwords down then you are defeating the purpose of having strong password management.

QUESTION 313:

What are the valid types of one time password generator?

A. All of the choices.
B. Transaction synchronous
C. Synchronous/PIN synchronous
D. Asynchronous/PIN asynchronous

Answer: A

Explanation:
One-time Passwords are changed after every use. Handheld password generator (tokens) 3 basic types: Synchronous/PIN synchronous, Transaction synchronous, Asynchronous/PIN asynchronous.

QUESTION 314:

Which of the following will you consider as most secure?

A. Password
B. One time password
C. Login phrase
D. Login ID

Answer: B

Explanation:
Each time the user logs in, the token generates a unique password that is synchronized with the network server. If anyone tries to reuse this dynamic password, access is denied, the event is logged and the network remains secure.

QUESTION 315:

What type of password makes use of two totally unrelated words?

A. Login phrase
B. One time password
C. Composition
D. Login ID

Answer: C

Explanation:
Usage of two totally unrelated words or a series of unrelated characters, such as pizza!wood for example. Such a password is easy to remember but very hard to guess. It would require a cracker quite a bit of time to do a brute force attack on a password that is that long and that uses an extended character as well.

QUESTION 316:

Which of the following is the correct account policy you should follow?

A. All of the choices.
B. All active accounts must have a password.
C. All active accounts must have a long and complex pass phrase.
D. All inactive accounts must have a password.

Answer: B

Explanation:
All active accounts must have a password. Unless you are using an application or service designed to be accessed without the need of a proper ID and password. Such service must however be monitored by other means (not a recommended practicE.)

QUESTION 317:

Which of the following are the advantages of using passphrase?

A. Difficult to crack using brute force.
B. Offers numerous characters.
C. Easier to remember.
D. All of the choices.

Answer: D

Explanation:
The use of passphrases is a good way of having very strong passwords. A passphrase is easier to remember, it offers numerous characters, and it is almost impossible to crack using brute force with today's processing power. An example of a passphrase could be: "Once upon a time in the CISSP world"

QUESTION 318:

Which of the following are the correct guidelines of password deployment?

A. Passwords must be masked.
B. All of the choices.
C. Password must have a minimum of 8 characters.
D. Password must contain a mix of both alphabetic and non-alphabetic characters.

Answer: B

Explanation:
Passwords must not be displayed in plain text while logging on. Passwords must be masked. Password must have a minimum of 8 characters. Password must contain a mix of both alphabetic and non-alphabetic characters. Passwords must be kept private, e.g. not shared, coded into programs, or written down.

QUESTION 319:

Why would a 16 characters password not desirable?

A. Hard to remember
B. Offers numerous characters.
C. Difficult to crack using brute force.
D. All of the choices.

Answer: A

Explanation:
When the password is too hard to memorize, the user will actually write it down, which is totally insecure and unacceptable.

QUESTION 320:

Which of the following is NOT a good password deployment guideline?

A. Passwords must not be he same as user id or login id.
B. Password aging must be enforced on all systems.
C. Password must be easy to memorize.
D. Passwords must be changed at least once every 60 days, depending on your environment.

Answer: C

Explanation:
Passwords must be changed at least once every 60 days (depending on your environment). Password aging or expiration must be enforced on all systems. Upon password expiration, if the password is not changed, only three grace logins must be allowed then the account must be disable until reset by an administrator or the help desk. Password reuse is not allowed (rotating passwords).

QUESTION 321:

Routing password can be restricted by the use of:

A. Password age
B. Password history
C. Complex password
D. All of the choices

Answer: B

Explanation:
Passwords must be changed at least once every 60 days (depending on your environment). Password aging or expiration must be enforced on all systems. Upon password expiration, if the password is not changed, only three grace logins must be allowed then the account must be disable until reset by an administrator or the help desk. Password reuse is not allowed (rotating passwords).

QUESTION 322:

What should you do immediately if the root password is compromised?

A. Change the root password.
B. Change all passwords.

C. Increase the value of password age.
D. Decrease the value of password history.

Answer: B

Explanation:
All passwords must be changed if the root password is compromised or disclosure is suspected. (This is a separate case; the optimal solution would be to reload the compromised computer. A computer that has been downgraded can never be upgraded to higher security level)

QUESTION 323:

Which of the following is the most secure way to distribute password?

A. Employees must send in an email before obtaining a password.
B. Employees must show up in person and present proper identification before obtaining a password.
C. Employees must send in a signed email before obtaining a password.
D. None of the choices.

Answer: B

Explanation:
Employees must show up in person and present proper identification before obtaining a new or changed password (depending on your policy). After three unsuccessful attempts to enter a password, the account will be locked and only an administrator or the help desk can reactivate the involved user ID.

QUESTION 324:

Which of the following does not apply to system-generated passwords?
A.) Passwords are harder to remember for users
B.) If the password-generating algorithm gets to be known, the entire system is in jeopardy
C.) Passwords are more vulnerable to brute force and dictionary attacks.
D.) Passwords are harder to guess for attackers

Answer: C

QUESTION 325:

Passwords can be required to change monthly, quarterly, or any other intervals:
A.) depending on the criticality of the information needing protection
B.) depending on the criticality of the information needing protection and the password's frequency of use
C.) depending on the password's frequency of use

D.) not depending on the criticality of the information needing protection but depending on the password's frequency of use

Answer: B

QUESTION 326:

In SSL/TLS protocol, what kind of authentication is supported?
A.) Peer-to-peer authentication
B.) Only server authentication (optional)
C.) Server authentication (mandatory) and client authentication (optional)
D.) Role based authentication scheme

Answer: C
"The server sends a message back to the client indicating that a secure session needs to be established, and the client sends it security parameters. The server compares those security parameters to its own until it finds a match. This is the handshaking phase. The server authenticates to the client by sending it a digital certificate, and if the client decides to trust the server the process continues. The server can require the client to send over a digital certificate for mutual authentication, but that is rare."
Pg. 523 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 327:

Which of the following correctly describe the difference between identification and authentication?

A. Authentication is a means to verify who you are, while identification is what you are authorized to perform.
B. Identification is a means to verify who you are, while authentication is what you are authorized to perform.
C. Identification is another name of authentication.
D. Identification is the child process of authentication.

Answer: B

Explanation:
Identification is a means to verify who you are. Authentication is what you are authorized to perform, access, or do. User identification enables accountability. It enables you to trace activities to individual users that may be held responsible for their actions. Identification usually takes the form of Logon ID or User ID. Some of the Logon ID characteristics are: they must be unique, not shared, and usually non descriptive of job function.

QUESTION 328:

Identification establishes:

A. Authentication
B. Accountability
C. Authorization
D. None of the choices.

Answer: B

Explanation:
Identification is a means to verify who you are. Authentication is what you are authorized to perform, access, or do. User identification enables accountability. It enables you to trace activities to individual users that may be held responsible for their actions. Identification usually takes the form of Logon ID or User ID. Some of the Logon ID characteristics are: they must be unique, not shared, and usually non descriptive of job function.

QUESTION 329:

Identification usually takes the form of:

A. Login ID.
B. User password.
C. None of the choices.
D. Passphrase

Answer: A

Explanation:
Identification is a means to verify who you are. Authentication is what you are authorized to perform, access, or do. User identification enables accountability. It enables you to trace activities to individual users that may be held responsible for their actions. Identification usually takes the form of Logon ID or User ID. Some of the Logon ID characteristics are: they must be unique, not shared, and usually non descriptive of job function

---

QUESTION 330:

What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?
A.) Authentication
B.) Identification
C.) Integrity
D.) Confidentiality

Answer: B

"Identification is the act of a user professing an identity to a system, usually in the form of a logon ID to the system." Pg 49 Krutz The CISSP Prep Guide.
"Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token." Pg 110 Shon Harris: All-in-One CISSP Certification

---

QUESTION 331:

What is called the verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time?
A.) Authentication
B.) Identification
C.) Integrity
D.) Confidentiality

Answer: A

QUESTION 332:

Identification and authentication are the keystones of most access control systems. Identification establishes:
A.) user accountability for the actions on the system
B.) top management accountability for the actions on the system
C.) EDP department accountability for the actions of users on the system
D.) authentication for actions on the system

Answer: A

QUESTION 333:

Which one of the following authentication mechanisms creates a problem for mobile users?
A.) address-based mechanism
B.) reusable password mechanism
C.) one-time password mechanism
D.) challenge response mechanism

Answer: A

QUESTION 334:

Which of the following centralized access control mechanisms is not appropriate for mobile workers access the corporate network over analog lines?
A.) TACACS

B.) Call-back
C.) CHAP
D.) RADIUS

Answer: B

QUESTION 335:

Authentication is typically based upon:

A. Something you have.
B. Something you know.
C. Something you are.
D. All of the choices.

Answer: D

Explanation:
Authentication is a means of verifying the eligibility of an entity to receive specific categories of information. The entity could be individual user, machine, or software component. Authentication is typically based upon something you know, something you have, or something you are.

QUESTION 336:

A password represents:

A. Something you have.
B. Something you know.
C. All of the choices.
D. Something you are.

Answer: B

Explanation:
The canonical example of something you know is a password or pass phrase. You might type or speak the value. A number of schemes are possible for obtaining what you know. It might be assigned to you, or you may have picked the value yourself. Constraints may exist regarding the form the value can take, or the alphabet from which you are allowed to construct the value might be limited to letters only. If you forget the value, you may not be able to authenticate yourself to the system.

QUESTION 337:

A smart card represents:

A. Something you are.
B. Something you know.
C. Something you have.
D. All of the choices.

Answer: C

Explanation:
Another form of authentication requires possession of something such as a key, a smart card, a disk, or some other device. Whatever form it takes, the authenticating item should be difficult to duplicate and may require synchronization with systems other than the one to which you are requesting access. Highly secure environments may require you to possess multiple things to guarantee authenticity.

QUESTION 338:

Which of the following is the most commonly used check on something you know?

A. One time password
B. Login phrase
C. Retinal
D. Password

Answer: D

Explanation:
Passwords even though they are always mentioned as being unsecured, necessary evils, that put your infrastructure at risk, are still commonly used and will probably be used for quite a few years. Good passwords can provide you with a good first line of defense. Passwords are based on something the user knows. They are used to authenticate users before they can access specific resources.

QUESTION 339:

Retinal scans check for:

A. Something you are.
B. Something you have.
C. Something you know.
D. All of the choices.

Answer: A

Explanation:
Something you are is really a special case of something you have. The usual examples given include fingerprint, voice, or retinal scans.

QUESTION 340:

What type of authentication takes advantage of an individuals unique physical characteristics in order to authenticate that persons identity?

A. Password
B. Token
C. Ticket Granting
D. Biometric

Answer: D

Explanation:
Biometric authentication systems take advantage of an individual's unique physical characteristics in order to authenticate that person's identity. Various forms of biometric authentication include face, voice, eye, hand, signature, and fingerprint, each have their own advantages and disadvantages. When combined with the use of a PIN it can provide two factors authentication.

QUESTION 341:

What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?
A.) Biometrics
B.) Micrometrics
C.) Macrometrics
D.) MicroBiometrics

Answer: A

QUESTION 342:

Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?
A.) Dynamic authentication
B.) Continuous authentication
C.) Encrypted authentication
D.) Robust authentication

Answer: C
The correct answer is C. Unable to find any references to continuous encryption.
"A digital signature is the encrypted hash value of a message." Pg 550 Shon Harris: CISSP All-In-One Certification Exam Guide.
"There are other options to improve the security offered by password authentication:
Use the strongest form of one-way encryption available for password storage.

Never allow passwords to be transmitted in clear text or with weak encryption." Pg. 9 Tittel: CISSP Study Guide
"[Kerberos] A complicated exchange of tickets (i.e., cryptographic messages) between the client, the server, and the TGS is used to prove identity and provide authentication between the client and server. This allows the client to request resources from the server while having full assurance that both entities are who they claim to be. The exchange of encrypted tickets also ensures that no logon credentials, session keys, or authentication messages are ever transmitted in the clear text." Pg 14 Tittel: CISSP Study Guide

---

QUESTION 343:

In which situation would TEMPEST risks and technologies be of MOST interest?

A. Where high availability is vital.
B. Where the consequences of disclose are very high.
C. Where countermeasures are easy to implement
D. Where data base integrity is crucial

Answer: B
Emanation eavesdropping. Receipt and display of information, which is resident on computers or terminals, through the interception of radio frequency (RF) signals generated by those computers or terminals. The U.S. government established a program called TEMPEST that addressed this problem by requiring a shielding and other emanation-reducing mechanisms to be employed on computers processing sensitive and classified government information. . -Ronald Krutz The CISSP PREP Guide (gold edition) pg 416

QUESTION 344:

Which one of the following addresses the protection of computers and components from electromagnetic emissions?

A. TEMPEST
B. ISO 9000
C. Hardening
D. IEEE 802.2

Answer: A
Receipt and Display of information, which is resident on computers or terminals, thorugh the interception of Radio Frequency (RF) signals generated by those computers or terminals. The U.S. government established a program called Tempest that addressed this problem by requiring shielding and other emanation-reducing mechanisms to be employed on computers processing sensitive and classified government information. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 416

QUESTION 345:

Monitoring electromagnetic pulse emanations from PCs and CRTs provides a hacker with that significant advantage?

A. Defeat the TEMPEST safeguard
B. Bypass the system security application.
C. Gain system information without trespassing
D. Undetectable active monitoring.

Answer: D
Tempest equipment is implemented to prevent intruders from picking up information through the airwaves with listening devices. - Shon Harris All-in-one CISSP Certification Guide pg 192. In Harris's other book CISSP PASSPORT, she talks about tempest in terms of spy movies and how a van outside is listening or monitoring to the activities of someone. This lends credence to the answer of C (trespassing) but I think D is more correct. In that all the listener must do is listen to the RF. Use your best judgment based on experience and knowledge.

QUESTION 346:

What name is given to the study and control of signal emanations from electrical and electromagnetic equipment?

A. EMI
B. Cross Talk
C. EMP
D. TEMPEST

Answer: D

QUESTION 347:

TEMPEST addresses

A. The vulnerability of time-dependent transmissions.
B. Health hazards of electronic equipment.
C. Signal emanations from electronic equipment.
D. The protection of data from high energy attacks.

Answer: C
"Tempest is the study and control of spurious electrical signals that are emitted by electrical equipment." Pg 167 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 348:

Which one of the following is the MOST solid defense against interception of a network transmission?

A. Frequency hopping
B. Optical fiber
C. Alternate routing
D. Encryption

Answer: B
An alternative to conductor-based network cabling is fiber-optic cable. Fiber-optic cables transmit pulses of light rather than electricity. This has the advantage of being extremely fast and near impervious to tapping.
Pg 85 Tittel: CISSP Study Guide.

QUESTION 349:

Which of the following media is MOST resistant to tapping?
A.) Microwave
B.) Twisted pair
C.) Coaxial cable
D.) Fiber optic

Answer: D

QUESTION 350:

What type of wiretapping involves injecting something into the communications?

A. Aggressive
B. Captive
C. Passive
D. Active

Answer: D
Most communications are vulnerable to some type of wiretapping or eavesdropping. It can usually be done undetected and is referred to as a passive attack versus an active attack. - Shon Harris All-in-one CISSP Certification Guide pg 649
"(I) An attack that intercepts and accesses data and other information contained in a flow in a communication system. (C) Although the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to reading information from any sort of medium used for a link or even directly from a node, such as gateway or subnetwork switch. (C) "Active wiretapping" attempts to alter the data or otherwise affect the flow; "passive wiretapping" only attempts to observe the flow and gain knowledge of information it contains. (See: active attack, end-to-end encryption, passive attack.)"
http://www.linuxsecurity.com/dictionary/dict-455.html

QUESTION 351:

Why would an Ethernet LAN in a bus topology have a greater risk of unauthorized

disclosure than switched Ethernet in a hub-and-spoke or star topology?

A. IEEE 802.5 protocol for Ethernet cannot support encryption.
B. Ethernet is a broadcast technology.
C. Hub and spoke connections are highly multiplexed.
D. TCP/IP is an insecure protocol.

Answer: B
Ethernet is broadcast and the question asks about a bus topology vs a SWITCHED Ethernet. Most switched Ethernet lans are divided by vlans which contain broadcasts to a single vlan, but remember only a layer 3 device can stop a broadcast.

QUESTION 352:

What type of attacks occurs when a smartcard is operating under normal physical conditions, but sensitive information is gained by examining the bytes going to and from the smartcard?

A. Physical attacks.
B. Logical attacks.
C. Trojan Horse attacks.
D. Social Engineering attacks.

Answer: B

Explanation:
Logical attacks occur when a smartcard is operating under normal physical conditions, but sensitive information is gained by examining the bytes going to and from the smartcard. One example is the so-called "timing attack" described by Paul Kocher. In this attack, various byte patterns are sent to the card to be signed by the private key. Information such as the time required to perform the operation and the number of zeroes and ones in the input bytes are used to eventually obtain the private key. There are logical countermeasures to this attack but not all smartcard manufacturers have implemented them. This attack does require that the PIN to the card be known, so that many private key operations can be performed on chosen input bytes.

QUESTION 353:

What is an effective countermeasure against Trojan horse attack that targets smart cards?

A. Singe-access device driver architecture.
B. Handprint driver architecture.
C. Fingerprint driver architecture.
D. All of the choices.

Answer: A

Explanation:
The countermeasure to prevent this attack is to use "single-access device driver" architecture. With this type of architecture, the operating system enforces that only one application can have access to the serial device (and thus the smartcard) at any given time. This prevents the attack but also lessens the convenience of the smartcard because multiple applications cannot use the services of the card at the same time. Another way to prevent the attack is by using a smartcard that enforces a "one private key usage per PIN entry" policy model. In this model, the user must enter their PIN every single time the private key is to be used and therefore the Trojan horse would not have access to the key.

QUESTION 354:

Which of the following could illegally capture network user passwords?
A.) Data diddling
B.) Sniffing
C.) Spoofing
D.) Smurfing

Answer: B

QUESTION 355:

Which of the following statements is incorrect?
A.) Since the early days of mankind humans have struggled with the problems of protecting assets
B.) The addition of a PIN keypad to the card reader was a solution to unreported card or lost cards problems
C.) There has never been a problem of lost keys
D.) Human guard is an inefficient and sometimes ineffective method of protecting resources

Answer: C

QUESTION 356:

A system uses a numeric password with 1-4 digits. How many passwords need to be tried before it is cracked?
A.) 1024
B.) 10000
C.) 100000
D.) 1000000

Answer: B
The largest 4 digit number is 9999. So 10,000 is the closest answer.

QUESTION 357:

Which of the following can be used to protect your system against brute force password attack?

A. Decrease the value of password history.
B. Employees must send in a signed email before obtaining a password.
C. After three unsuccessful attempts to enter a password, the account will be locked.
D. Increase the value of password age.

Answer: C

Explanation:
Employees must show up in person and present proper identification before obtaining a new or changed password (depending on your policy). After three unsuccessful attempts to enter a password, the account will be locked and only an administrator or the help desk can reactivate the involved user ID.

QUESTION 358:

Which of the following is an effective measure against a certain type of brute force password attack?

A. Password used must not be a word found in a dictionary.
B. Password history is used.
C. Password reuse is not allowed.
D. None of the choices.

Answer: A

Explanation:
Password reuse is not allowed (rotating passwords). Password history must be used to prevent users from reusing passwords. On all systems with such a facility the last 12 passwords used will be kept in the history. All computer system users must choose passwords that cannot be easily guessed. Passwords used must not be a word found in a dictionary.

QUESTION 359:

Which type of attack will most likely provide an attacker with multiple passwords to authenticate to a system?
A.) Password sniffing
B.) Dictionary attack
C.) Dumpster diving
D.) Social engineering

Answer: A

QUESTION 360:

Which of the following are measures against password sniffing?

A. Passwords must not be sent through email in plain text.
B. Passwords must not be stored in plain text on any electronic media.
C. You may store passwords electronically if it is encrypted.
D. All of the choices.

Answer: D

Explanation:
Passwords must not be sent through email in plain text. Passwords must not be stored in plain text on any electronic media. It is acceptable to store passwords in a file if it is encrypted with PGP or equivalent strong encryption (once again depending on your organization policy). All vendor supplied default passwords must be changed.

QUESTION 361:

Which one of the following conditions is NOT necessary for a long dictionary attack to succeed?

A. The attacker must have access to the target system.
B. The attacker must have read access to the password file.
C. The attacker must have write access to the password file.
D. The attacker must know the password encryption mechanism and key variable.

Answer: C

Explanation:
The program encrypts the combination of characters and compares them to the encrypted entries in the password file. If a match is found, the program has uncovered a password. - Shon Harris All-in-one CISSP Certification Guide pg 199

QUESTION 362:

What is an important factor affecting the time required to perpetrate a manual trial and error attack to gain access to a target computer system?

A. Keyspace for the password.
B. Expertise of the person performing the attack.
C. Processing speed of the system executing the attack.
D. Encryption algorithm used for password transfer.

Answer: A

Explanation:
I am not sure of the answer on this question. B seems good but the reference below states that Keyspace (or length of password) is the main deterrent. I did not come across something that directly relates in my readings.
"If an attacker mounts a trial-and-error attack against your password, a longer password gives the attacker a larger number of alternatives to try. If each character in the password may take on 96 different values (typical of printable ASCII characters) then each additional character presents the attacker with 96 times as many passwords to try. If the number of alternatives is large enough, the trial-and-error attack might discourage the attacker, or lead to the attacker's detection." http://www.smat.us/sanity/riskyrules.html

---

QUESTION 363:

Which one of the following BEST describes a password cracker?

A. A program that can locate and read a password file.
B. A program that provides software registration passwords or keys.
C. A program that performs comparative analysis.
D. A program that obtains privileged access to the system.

Answer: C

Explanation:
In a dictionary crack, L0phtCrack encrypts (i.e., hashes) all the passwords in a dictionary file you specify and compares every result with the password hash. If L0phtCrack finds any matches, it knows the password is the dictionary word. L0phtCrack comes with a default dictionary file, words-english. You can download additional files from the Internet or create a custom file. In the Tools Options dialog box, you can choose to run the dictionary attack against the LANMAN password hash, the NT LAN Manager (NTLM) password hash, or both (which is the default).
In a hybrid crack, L0phtCrack extends the dictionary crack by appending numbers or symbols to each word in the dictionary file. For example, in addition to trying "Galileo," L0phtCrack also tries "Galileo24," "13Galileo," "?Galileo," "Galileo!," and so on. The default number of characters L0phtCrack tries is two, and you can change this number in the Tools Options dialog box.
In a brute-force crack, L0phtCrack tries every possible combination of characters in a character set. L0phtCrack offers four character sets, ranging from alpha only to all alphanumeric plus all symbol characters. You can choose a character set from the Character Set drop-down box in the Tools Options dialog box or type a custom character set in the Character Set drop-down box. L0phtCrack saves custom sets in files with an .lc extension. You can also specify a character set in the password file, as the example in Figure 2 shows.
Not B: A key generator is what is being described by the registration password or key answer.

QUESTION 364:

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday
B. Brute force
C. Man-in-the-middle
D. Smurf

Answer: B

Explanation:
Brute force attacks are performed with tools that cycle through many possible character, number, and symbol combinations to guess a password. Pg 134 Shon Harris CISSP All-In-One Certification Exam Guide. Since the token allows offline checking of PIN, the cracker can keep trying PINS until it is cracked.

QUESTION 365:

Which of the following actions can increase the cost of an exhaustive attack?

A. Increase the age of a password.
B. Increase the length of a password.
C. None of the choices.
D. Increase the history of a password.

Answer: B

Explanation:
Defenses against exhaustive attacks involve increasing the cost of the attack by increasing the number of possibilities to be exhausted. For example, increasing the length of a password will increase the cost of an exhaustive attack. Increasing the effective length of a cryptographic key variable will make it more resistant to an exhaustive attack.

QUESTION 366:

Which of the following attacks focus on cracking passwords?

A. SMURF
B. Spamming
C. Teardrop
D. Dictionary

Answer: D

Explanation:

Dictionaries may be used in a cracking program to determine passwords. A short dictionary attack involves trying a list of hundreds or thousands of words that are frequently chosen as passwords against several systems. Although most systems resist such attacks, some do not. In one case, one system in five yielded to a particular dictionary attack.

QUESTION 367:

Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?
A.) Using TACACS+ server
B.) Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C.) Setting modem ring count to at least 5
D.) Only attaching modems to non-networked hosts.

Answer: B

QUESTION 368:

What is known as decoy system designed to lure a potential attacker away from critical systems?

A. Honey Pots
B. Vulnerability Analysis Systems
C. File Integrity Checker
D. Padded Cells

Answer: A

Explanation:
Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems. Honey pots are designed to:
Divert an attacker from accessing critical systems,
Collect information about the attacker's activity, and encourage the attacker to stay on the system long enough for administrators to respond.

QUESTION 369:

Which of the following will you consider as a program that monitors data traveling over a network?

A. Smurfer
B. Sniffer
C. Fragmenter
D. Spoofer

Answer: B

Explanation:
A sniffer is a program and/or device that monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect

---

QUESTION 370:

Which of the following is NOT a system-sensing wireless proximity card?
A.) magnetically striped card
B.) passive device
C.) field-powered device
D.) transponder

Answer: A

QUESTION 371:

Attacks on smartcards generally fall into what categories?

A. Physical attacks.
B. Trojan Horse attacks.
C. Logical attacks.
D. All of the choices, plus Social Engineering attacks.

Answer: D

Explanation:
Attacks on smartcards generally fall into four categories: Logical attacks, Physical attacks, Trojan Horse attacks and Social Engineering attacks.

QUESTION 372:

Which of the following attacks could be the most successful when the security technology is properly implemented and configured?

A. Logical attacks
B. Physical attacks
C. Social Engineering attacks
D. Trojan Horse attacks

Answer: C

Explanation:

Social Engineering attacks - In computer security systems, this type of attack is usually the most successful, especially when the security technology is properly implemented and configured. Usually, these attacks rely on the faults in human beings. An example of a social engineering attack has a hacker impersonating a network service technician. The serviceman approaches a low-level employee and requests their password for network servicing purposes. With smartcards, this type of attack is a bit more difficult. Most people would not trust an impersonator wishing to have their smartcard and PIN for service purposes.

QUESTION 373:

What type of attacks occurs when normal physical conditions are altered in order to gain access to sensitive information on the smartcard?

A. Physical attacks
B. Logical attacks
C. Trojan Horse attacks
D. Social Engineering attacks

Answer: A

Explanation:
Physical attacks occur when normal physical conditions, such as temperature, clock frequency, voltage, etc, are altered in order to gain access to sensitive information on the smartcard. Most smartcard operating systems write sensitive data to the EEPROM area in a proprietary, encrypted manner so that it is difficult to obtain clear text keys by directly hacking into the EEPROM. Other physical attacks that have proven to be successful involve an intense physical fluctuation at the precise time and location where the PIN verification takes place. Thus, sensitive card functions can be performed even though the PIN is unknown. This type of attack can be combined with the logical attack mentioned above in order to gain knowledge of the private key. Most physical attacks require special equipment.

QUESTION 374:

Which one of the following is an example of electronic piggybacking?

A. Attaching to a communications line and substituting data.
B. Abruptly terminating a dial-up or direct-connect session.
C. Following an authorized user into the computer room.
D. Recording and playing back computer transactions.

Answer: C
Ok this is a weird little question. The term electronic is kinda of throwing me a bit. A lot of times piggybacking can
be used in terms of following someone in a building.

Piggyback - Gaining unauthorized access to a system via another user's legitimate connection. (see between-the-lines entry)
Between-the-lines entry 0 Unauthorized access obtained by tapping the temporarily inactive terminal of a legitimate
user. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 914, 885

QUESTION 375:

A system using Discretionary Access Control (DAC) is vulnerable to which one of the following attacks?

A. Trojan horse
B. Phreaking
C. Spoofing
D. SYN flood

Answer: C
An attempt to gain access to a system by posing as an authorized user. Synonymous with impersonating, masquerading, or mimicking.-Ronald Krutz The CISSP PREP Guide (gold edition) pg 921
"Spoofing - The act of replacing the valid source and/or destination IP address and node numbers with false ones.
Spoofing attack - any attack that involves spoofed or modified packets." - Ed Tittle CISSP Study Guide (sybex)

QUESTION 376:

Which of the following is an example of an active attack?
A.) Traffic analysis
B.) Masquerading
C.) Eavesdropping
D.) Shoulder surfing

Answer: B

QUESTION 377:

What attack involves actions to mimic one's identity?

A. Brute force
B. Exhaustive
C. Social engineering
D. Spoofing

Answer: D

Explanation:
Spoofing is an attack in which one person or process pretends to be a person or process that has more privileges. For example, user A can mimic behavior to make process B believe user A is user C. In the absence of any other controls, B may be duped into giving to user A the data and privileges that were intended for user C.

QUESTION 378:

Which access control model enables the owner of the resource to specify what subjects can access specific resources?
A.) Discretionary Access Control
B.) Mandatory Access Control
C.) Sensitive Access Control
D.) Role-based Access Control

Answer: A

QUESTION 379:

The type of discretionary access control that is based on an individual's identity is called:
A.) Identity-based access control
B.) Rule-based access control
C.) Non-Discretionary access control
D.) Lattice-based access control

Answer: A

QUESTION 380:

Which of the following access control types gives "UPDATE" privileges on Structured Query Language (SQL) database objects to specific users or groups?

A. Supplemental
B. Discretionary
C. Mandatory
D. System

Answer: C
Supplemental and System are not access control types. The most correct answer is mandatory opposed to discretionary. The descriptions below sound typical of how a sql accounting database controls access.
"In a mandatory access control (MAC) model, users and data owners do not have as much freedom to determine who can access their files. Data owners can allow others to have access to their files, but it is the operating system that will make the final decision and can override the data owner's wishes." Pg. 154 Shon Harris CISSP All-In-One Certification Exam Guide
"Rule-based access controls are a variation of mandatory access controls. A rule based systems

uses a set of rules, restrictions or filters to determine what can and cannot occur on the system, such as granting subject access, performing an action on an object, or accessing a resource. Pg 16 Tittle: CISSP Study Guide.

QUESTION 381:

With Discretionary access controls, who determines who has access and what privilege they have?

A. End users.
B. None of the choices.
C. Resource owners.
D. Only the administrators.

Answer: C

Explanation:
Discretionary access controls can extend beyond limiting which subjects can gain what type of access to which objects. Administrators can limit access to certain times of day or days of the week. Typically, the period during which access would be permitted is 9 a.m. to 5 p.m. Monday through Friday. Such a limitation is designed to ensure that access takes place only when supervisory personnel are present, to discourage unauthorized use of data. Further, subjects' rights to access might be suspended when they are on vacation or leave of absence. When subjects leave an organization altogether, their rights must be terminated rather than merely suspended. Under this type of control, the owner determines who has access and what privilege they have.

QUESTION 382:

What defines an imposed access control level?

A. MAC
B. DAC
C. SAC
D. CAC

Answer: A

Explanation:
MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

QUESTION 383:

Under MAC, who can change the category of a resource?

A. All users.
B. Administrators only.
C. All managers.
D. None of the choices.

Answer: B

Explanation:
MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

QUESTION 384:

Under MAC, who may grant a right of access that is explicitly forbidden in the access control policy?

A. None of the choices.
B. All users.
C. Administrators only.
D. All managers.

Answer: A

Explanation:
MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

QUESTION 385:

You may describe MAC as:

A. Opportunistic
B. Prohibitive
C. None of the choices.
D. Permissive

Answer: B

Explanation:
It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. In this type of control system decisions are based on privilege (clearance) of subject (user) and sensitivity (classification) of object (file). It requires labeling.

QUESTION 386:

Under MAC, which of the following is true?

A. All that is expressly permitted is forbidden.
B. All that is not expressly permitted is forbidden.
C. All that is not expressly permitted is not forbidden.
D. None of the choices.

Answer: B

Explanation:
It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. In this type of control system decisions are based on privilege (clearance) of subject (user) and sensitivity (classification) of object (file). It requires labeling.

QUESTION 387:

Under MAC, a clearance is a:

A. Sensitivity
B. Subject
C. Privilege
D. Object

Answer: C

Explanation:
It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. In this type of control system decisions are based on privilege

(clearance) of subject (user) and sensitivity (classification) of object (file). It requires labeling.

QUESTION 388:

Under MAC, a file is a(n):

A. Privilege
B. Subject
C. Sensitivity
D. Object

Answer: D

Explanation:
It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. In this type of control system decisions are based on privilege (clearance) of subject (user) and sensitivity (classification) of object (file). It requires labeling.

QUESTION 389:

Under MAC, classification reflects:

A. Sensitivity
B. Subject
C. Privilege
D. Object

Answer: A

Explanation:
It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. In this type of control system decisions are based on privilege (clearance) of subject (user) and sensitivity (classification) of object (file). It requires labeling.

QUESTION 390:

MAC is used for:

A. Defining imposed access control level.

B. Defining user preferences.
C. None of the choices.
D. Defining discretionary access control level.

Answer: A

Explanation:
As the name implies, the Mandatory Access Control defines an imposed access control level. MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

QUESTION 391:

With MAC, who may make decisions that bear on policy?

A. None of the choices.
B. All users.
C. Only the administrator.
D. All users except guests.

Answer: C

Explanation:
As the name implies, the Mandatory Access Control defines an imposed access control level. MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

QUESTION 392:

With MAC, who may NOT make decisions that derive from policy?

A. All users except the administrator.
B. The administrator.
C. The power users.
D. The guests.

Answer: A

Explanation:
As the name implies, the Mandatory Access Control defines an imposed access control

level. MAC is defined as follows in the Handbook of Information Security Management: With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy.

QUESTION 393:

Under the MAC control system, what is required?

A. Performance monitoring
B. Labeling
C. Sensing
D. None of the choices

Answer: B

Explanation:
It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden), not permissive. Only within that context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. In this type of control system decisions are based on privilege (clearance) of subject (user) and sensitivity (classification) of object (file). It requires labeling.

QUESTION 394:

Access controls that are not based on the policy are characterized as:

A. Secret controls
B. Mandatory controls
C. Discretionary controls
D. Corrective controls

Answer: C

Explanation:
Access controls that are not based on the policy are characterized as discretionary controls by the U.S. government and as need-to-know controls by other organizations. The latter term connotes least privilege - those who may read an item of data are precisely those whose tasks entail the need.

QUESTION 395:

DAC are characterized by many organizations as:

A. Need-to-know controls
B. Preventive controls
C. Mandatory adjustable controls
D. None of the choices

Answer: A

Explanation:
Access controls that are not based on the policy are characterized as discretionary controls by the U.S. government and as need-to-know controls by other organizations. The latter term connotes least privilege - those who may read an item of data are precisely those whose tasks entail the need.

QUESTION 396:

Which of the following correctly describe DAC?

A. It is the most secure method.
B. It is of the B2 class.
C. It can extend beyond limiting which subjects can gain what type of access to which objects.
D. It is of the B1 class.

Answer: C

Explanation:
With DAC, administrators can limit access to certain times of day or days of the week. Typically, the period during which access would be permitted is 9 a.m. to 5 p.m. Monday through Friday. Such a limitation is designed to ensure that access takes place only when supervisory personnel are present, to discourage unauthorized use of data. Further, subjects' rights to access might be suspended when they are on vacation or leave of absence. When subjects leave an organization altogether, their rights must be terminated rather than merely suspended.

QUESTION 397:

Under DAC, a subjects rights must be _____ when it leaves an organization altogether.

A. recycled
B. terminated
C. suspended
D. resumed

Answer: B

Explanation:
Discretionary access controls can extend beyond limiting which subjects can gain what

type of access to which objects. Administrators can limit access to certain times of day or days of the week. Typically, the period during which access would be permitted is 9 a.m. to 5 p.m. Monday through Friday. Such a limitation is designed to ensure that access takes place only when supervisory personnel are present, to discourage unauthorized use of data. Further, subjects' rights to access might be suspended when they are on vacation or leave of absence. When subjects leave an organization altogether, their rights must be terminated rather than merely suspended.

QUESTION 398:

In a discretionary mode, which of the following entities is authorized to grant information access to other people?
A.) manager
B.) group leader
C.) security manager
D.) user

Answer: D

QUESTION 399:

With RBAC, each user can be assigned:

A. One or more roles.
B. Only one role.
C. A token role.
D. A security token.

Answer: A

Explanation:
With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Roles can be hierarchical.

QUESTION 400:

With RBAC, roles are:

A. Based on labels.
B. All equal
C. Hierarchical
D. Based on flows.

Answer: C

Explanation:
With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Roles can be hierarchical.

QUESTION 401:

With _____, access decisions are based on the roles that individual users have as part of an organization.

A. Server based access control.
B. Rule based access control.
C. Role based access control.
D. Token based access control.

Answer: C

Explanation:
With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.

QUESTION 402:

Under Role based access control, access rights are grouped by:

A. Policy name
B. Rules
C. Role name
D. Sensitivity label

Answer: C

Explanation:
With role-based access control, access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies.

QUESTION 403:

Which of the following will you consider as a "role" under a role based access control system?

A. Bank rules
B. Bank computer
C. Bank teller
D. Bank network

Answer: C

Explanation:
With role-based access control, access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies.

QUESTION 404:

Role based access control is attracting increasing attention particularly for what applications?

A. Scientific
B. Commercial
C. Security
D. Technical

Answer: B

Explanation:
Role based access control (RBAC) is a technology that is attracting increasing attention, particularly for commercial applications, because of its potential for reducing the complexity and cost of security administration in large networked applications.

QUESTION 405:

What is one advantage of deploying Role based access control in large networked applications?

A. Higher security
B. Higher bandwidth
C. User friendliness
D. Lower cost

Answer: D

Explanation:
Role based access control (RBAC) is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies. The principle motivation behind RBAC is the desire to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Traditionally, managing security has required mapping an organization's security policy to a relatively low-level set of controls, typically access control lists.

QUESTION 406:

DAC and MAC policies can be effectively replaced by:

A. Rule based access control.
B. Role based access control.
C. Server based access control.
D. Token based access control

Answer: B

Explanation:
Role based access control (RBAC) is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies. The principle motivation behind RBAC is the desire to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Traditionally, managing security has required mapping an organization's security policy to a relatively low-level set of controls, typically access control lists.

QUESTION 407:

Which of the following correctly describe Role based access control?

A. It allows you to specify and enforce enterprise-specific security policies in a way that maps to your user profile groups.
B. It allows you to specify and enforce enterprise-specific security policies in a way that maps to your organizations structure.
C. It allows you to specify and enforce enterprise-specific security policies in a way that maps to your ticketing system.
D. It allows you to specify and enforce enterprise-specific security policies in a way that maps to your ACL.

Answer: B

Explanation:
Role based access control (RBAC) is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies. The principle motivation behind RBAC is

the desire to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Traditionally, managing security has required mapping an organization's security policy to a relatively low-level set of controls, typically access control lists.

QUESTION 408:

Which of the following RFC talks about Rule Based Security Policy?

A. 1316
B. 1989
C. 2717
D. 2828

Answer: D

Explanation:
The RFC 2828 - Internet Security Glossary talks about Rule Based Security Policy: A security policy based on global rules imposed for all users. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

QUESTION 409:

With Rule Based Security Policy, a security policy is based on:

A. Global rules imposed for all users.
B. Local rules imposed for some users.
C. Global rules imposed for no body.
D. Global rules imposed for only the local users.

Answer: A

Explanation:
The RFC 2828 - Internet Security Glossary talks about Rule Based Security Policy: A security policy based on global rules imposed for all users. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

QUESTION 410:

With Rule Based Security Policy, global rules usually rely on comparison of the _____ of the resource being accessed.

A. A group of users.
B. Users
C. Sensitivity
D. Entities

Answer: C

Explanation:
The RFC 2828 - Internet Security Glossary talks about Rule Based Security Policy: A security policy based on global rules imposed for all users. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

QUESTION 411:

Which of the following is a facial feature identification product that can employ artificial intelligence and can require the system to learn from experience?

A. All of the choices.
B. Digital nervous system.
C. Neural networking
D. DSV

Answer: C

Explanation:
There are facial feature identification products that are on the market that use other technologies or methods to capture one's face. One type of method used is neural networking technology. This type of technology can employ artificial intelligence that requires the system to "learn" from experience. This "learning" experience helps the system to close in on an identification of an individual. Most facial feature identification systems today only allow for two-dimensional frontal images of one's face.
Not DSV:
Signature biometrics are often referred to dynamic signature verification (DSV) and look at the way we sign our names. [15] The dynamic nature differentiates it from the study of static signatures on paper. Within DSV a number of characteristics can be extracted from the physical signing process. Examples of these behavioral characteristics are the angle of the pen is held, the time taken to sign, velocity and acceleration of the tip of the pen, number of times the pen is lifted from the paper. Despite the fact that the way we sign is mostly learnt during the years it is very hard to forge and replicate.

QUESTION 412:

Which option is NOT a benefit derived from the use of neural networks?

A. Linearity
B. Input-Output Mapping
C. Adaptivity
D. Fault Tolerance

Answer: D
Linearity: "If the sum of the weighted inputs then exceeds the threshold, the neuron will "fire" and there will be an output from that neuron. An alternative approach would be to have the output of the neuron be a linear function of the sum of the artificial neuron inputs."
Input-Output Mapping: "For example, if a specific output vector was required for a specific input where the relationship between input and output was non-linear, the neural network would be trained by applying a set of input vector."
Adaptivity: "The neural network would have then be said to have learned to provide the correct response for each input vector."
Pg. 261 Krutz: The CISSP Prep Guide

QUESTION 413:

Which of the following is a characteristic of a decision support system (DSS)?
A.) DSS is aimed at solving highly structured problems
B.) DSS emphasizes flexibility in the decision making approach of users
C.) DSS supports only structured decision-making tasks
D.) DSS combines the use of models with non-traditional data access and retrieval functions

Answer: B

QUESTION 414:

Which of the following is a communication mechanism that enables direct conversation between two applications?
A.) DDE
B.) OLE
C.) ODBC
D.) DCOM

Answer: A
"Dynamic Data Exchange (DDE) enables applications to share data by providing IPC. It is based on the client/server model and enables two programs to send commands to each other directly. DDE is a communication mechanism that enables direct conversation between two applications. The source of the data is called the server, and the receiver of the data is the client." Pg. 718
Shon Harris: All-In-One CISSP Certification Exam Guide

QUESTION 415:

Which expert system operating mode allows determining if a given hypothesis is valid?

A.) Vertical chaining
B.) Lateral chaining
C.) Forward chaining
D.) Backward chaining

Answer: D
"The expert system operates in either a forward-chaining or backward-chaining mode. In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs. In a backward-chaining mode, the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs. Another type of expert system is the blackboard. A blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual "blackboard," wherein information or portential solutions are placed on the blackboard by the plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated." Pg 354 Krutz: The CISSP Prep Guide: Gold Edition

---

QUESTION 416:

Which one of the following is a security issue related to aggregation in a database?

A. Polyinstantiation
B. Inference
C. Partitioning
D. Data swapping

Answer: B
Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privileges. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 358
The other security issue is inference, which is very similar to aggregation. - Shon Harris All-in-one CISSP Certification Guide pg 727
Partitioning a database involves dividing the database into different parts, which makes it much harder for an unauthorized individual to find connecting pieces of data that can be brought together and other information that can be deduced or uncovered. - Shon Harris All-in-one CISSP Certification Guide pg 726
Polyinstantiation- This enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. - Shon Harris All-in-one CISSP Certification Guide pg 727

QUESTION 417:

How is polyinstantiation used to secure a multilevel database?

A. It prevents low-level database users from inferring the existence of higher level data.
B. It confirms that all constrained data items within the system conform to integrity specifications.
C. It ensures that all mechanism in a system are responsible for enforcing the database security policy.
D. Two operations at the same layer will conflict if they operate on the same data item and at least one of them is an update.

Answer: A
"Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object. In the database information security, this term is concerned with the same primary key for different relations at different classification levels being stored in the same database. For example, in a relational database, the same of a military unit may be classified Secret in the database and may have an identification number as the primary key. If another user at a lower classification level attempts to create a confidential entry for another military unit using the same identification number as a primary key, a rejection of this attempt would imply to the lower level user that the same identification number existed at a higher level of classification. To avoid this inference channel of information, the lower level user would be issued the same identification number for their unit and the database management system would manage this situation where the same primary key was used for different units." Pg 352-353
Krutz: The CISSP Prep Guide: Gold Edition.
"Polyinstantiation occurs when to or more rows in the same table appear to have identical primary key elements but contain different data for use at differing classification levels. Polyinstantiation is often used as a defense against some types of inference attacks.
For example, consider a database table containing the location of various naval ships on patrol. Normally, this database contains the exact position of each ship stored at the level with secret classification. However, on particular ship, the USS UpToNoGood, is on an undercover mission to a top-secret location. Military commanders do not want anyone to know that the ship deviated from its normal patrol. If the database administrators simply change the classification of the UpToNoGood's location to top secret, a user with secret clearance would know that something unusual was going on when they couldn't query the location of the ship. However, if polyinstantiation is used, two records could be inserted into the table. The first one, classified at the top secret level, would reflect the true location of the ship and be available only to users with the appropriate top secret security clearance. The second record, classified at the secret level, would indicate that the ship was on routine patrol and would be returned to users with a secret clearance."
Pg. 191 Tittel: CISSP Study Guide Second Edition

QUESTION 418:

Which of the following defines the software that maintains and provides access to the database?
A.) database management system (DBMS)
B.) relational database management systems (RDBMS)
C.) database identification system (DBIS)
D.) Interface Definition Language system (IDLS)

Answer: A

QUESTION 419:

Which of the following is not a responsibility of a database administrator?
A.) Maintaining databases
B.) Implementing access rules to databases
C.) Reorganizing databases
D.) Providing access authorization to databases

Answer: D

QUESTION 420:

SQL commands do not include which of the following?
A.) Select, Update
B.) Grant, Revoke
C.) Delete, Insert
D.) Add, Replace

Answer: D
"SQL commands include Select, Update, Delete, Insert, Grant, and Revoke." Pg 62 Krutz: CISSP Prep Guide: Gold Edition

---

QUESTION 421:

A persistent collection of interrelated data items can be defined as which of the following?
A.) database
B.) database management system
C.) database security
D.) database shadowing

Answer: A

QUESTION 422:

Which one of the following is commonly used for retrofitting multilevel security to a Database Management System?

A. Trusted kernel
B. Kernel controller
C. Front end controller
D. Trusted front-end

Answer: D

QUESTION 423:

Which of the following is the marriage of object-oriented and relational technologies combining the attributes of both?
A.) object-relational database
B.) object-oriented database
C.) object-linking database
D.) object-management database

Answer: A

QUESTION 424:

A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

A.) content-dependent access control
B.) context-dependent access control
C.) least privileges access control
D.) ownership-based access control

Answer: A
"Database security takes a different approach than operating system security. In an operating system, the identity and authentication of the subject controls access. This is done through access control lists (ACLs), capability tables, roles, and security labels. The operating system only makes decisions about where a subject can access a file; it does not make this decisions based on the contents of the file itself. If Mitch can access file A, it does not matter if that file contains information about a cookie recipe or secret information from the Cold War. On the other hand, database security does look at the contents of a file when it makes an access control decision, which is referred to as content-dependent access control. This type of access control increases processing overhead, but it provides higher granular control." Pg. 677 Shon Harris: CISSP Certification All-in-One Exam Guide

QUESTION 425:

Which of the following is an important part of database design that ensures that attributes in a table depend only on the primary key?
A.) Normalization
B.) Assimilation
C.) Reduction
D.) Compaction

Answer: A

QUESTION 426:

Which of the following does not address Database Management Systems (DBMS) Security?
A.) Perturbation
B.) Cell suppression
C.) Padded Cells
D.) Partitioning

Answer: C

QUESTION 427:

Which of the following is commonly used for retrofitting multilevel security to a database management system?
A.) trusted front-end
B.) trusted back-end
C.) controller
D.) kernel

Answer: A

QUESTION 428:

Normalizing data within a database includes all of the following except which?
A.) Eliminating repeating groups by putting them into separate tables
B.) Eliminating redundant data
C.) Eliminating attributes in a table that are not dependent on the primary key of that table
D.) Eliminating duplicate key fields by putting them into separate tables

Answer: D
"Data Normalization
Normalization is an important part of database design that ensures that attributes in a table depend only on the primary key. This process makes it easier to maintain data and have consistent reports.
Normalizing data in the database consists of three steps:
1.) Eliminating any repeating groups by putting them into separate tables
2.) Eliminating redundant data (occurring in more than one table)
3.) Eliminating attributes in a table that are not dependent on the primary key of that table"
Pg. 62 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 429:

SQL commands do not include which of the following?
A.) Select, Update
B.) Grant, Revoke

C.) Delete, Insert
D.) Add, Replace

Answer: D
"SQL commands include Select, Update, Delete, Grant, and Revoke." Pg. 62 Krutz: The CISSP Prep Guide: Gold Edition
"Developed by IBM, SQL is a standard data manipulation and relational database definition language. The SQL Data Definition Language creates and deletes views and relations (tables). SQL commands include Select, Update, Delete, Insert, Grant, and Revoke. The latter two commands are used in access control to grant and revoke privileges to resources. Usually, the owner of an object can withhold or transfer GRANT privileges to an object to another subject. If the owner intentionally does not transfer the GRANT privileges, however, which are relative to an object to the individual A, A cannot pass on the GRANT privileges to another subject. In some instances, however, this security control can be circumvented. For example, if A copies the object, A essentially becomes the owner of that object and thus can transfer the GRANT privileges to another user, such as user B.
SQL security issues include the granularity of authorization and the number of different ways you can execute the same query.
Pg. 63 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 430:

SQL security issues include which of the following?
A.) The granularity of authorizations
B.) The size of databases
C.) The complexity of key structures
D.) The number of candidate key elements

Answer: A
Developed by IBM, SQL is a standard data manipulation and relational database definition language. The SQL Data Definition Language creates and deletes views and relations (tables). SQL commands include Select, Update, Delete, Insert, Grant, and Revoke. The latter two commands are used in access control to grant and revoke privileges to resources. Usually, the owner of an object can withhold or transfer GRANT privileges to an object to another subject. If the owner intentionally does not transfer the GRANT privileges, however, which are relative to an object to the individual A, A cannot pass on the GRANT privileges to another subject. In some instances, however, this security control can be circumvented. For example, if A copies the object, A essentially becomes the owner of that object and thus can transfer the GRANT privileges to another user, such as user B.
SQL security issues include the granularity of authorization and the number of different ways you can execute the same query.
Pg. 63 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 431:

Which of the following are placeholders for literal values in a Structured Query Language

(SQL) query being sent to the database on a server?
A.) Bind variables
B.) Assimilation variables
C.) Reduction variables
D.) Resolution variables

Answer: A

QUESTION 432:

What ensures that attributes in a table depend only on the primary key?
A.) Referential integrity
B.) The database management system (DBMS)
C.) Data Normalization
D.) Entity integrity

Answer: C

QUESTION 433:

Which of the following represent the rows of the table in a relational database?
A.) attributes
B.) records or tuples
C.) record retention
D.) relation

Answer: B

QUESTION 434:

With regard to databases, which of the following has characteristics of ease of reusing code and analysis and reduced maintenance?
A.) Object-Oriented Data Bases (OODB)
B.) Object-Relational Data Bases (ORDB)
C.) Relational Data Bases
D.) Data Base management systems (DBMS)

Answer: A

QUESTION 435:

Complex applications involving multimedia, computer aided design, video, graphics, and expert systems are more suited to which of the following?
A.) Object-Oriented Data Bases (OODB)
B.) Object-Relational Data Bases
C.) Relational Data Bases

D.) Data base management systems (DBMS)

Answer: A

QUESTION 436:

Which of the following refers to the number of columns in a table?
A.) Schema
B.) Relation
C.) Degree
D.) Cardinality

Answer: C

QUESTION 437:

Which of the following refers to the number of rows in a relation?
A.) cardinality
B.) degree
C.) depth
D.) breadth

Answer: A

QUESTION 438:

Which of the following refers to the number of columns in a relation?
A.) degree
B.) cardinality
C.) depth
D.) breadth

Answer: A

QUESTION 439:

What is one disadvantage of content-dependent protection of information?
A.) It increases processing overhead
B.) It requires additional password entry
C.) It exposes the system to data locking
D.) It limits the user's individual address space

Answer: A
Content-Dependent Access Control
"Just like the name sounds, access to objects is determined by the content within the object. This is used many times in databases and the type of Web-based material a firewall allows...If a table

within the database contains information about employees' salaries, the managers were not allowed to view it, but they could view information about an employee's work history. The content of the database fields dictates which user can see specific information within the database tables." pg 161 Shon Harris: All-In-One CISSP Certification. Decisions will have to be made about the content, therefore increasing processing overhead.

QUESTION 440:

Which one of the following control steps is usually NOT performed in data warehousing applications?

A. Monitor summary tables for regular use.
B. Control meta data from being used interactively.
C. Monitor the data purging plan.
D. Reconcile data moved between the operations environment and data warehouse.

Answer: A
Not B: It is important to control meta data from being used interactively by unauthorized users. "Data warehouses and data mining are significant to security professionals for two reasons. First, as previously mentioned, data warehouses contain large amounts of potentially sensitive information vulnerable to aggregation and inference attacks, and security practitioners must ensure that adequate access controls and other security measures are in place to safeguard this data." Pg 192 Tittel: CISSP Study Guide
Not C: "The data in the data warehouse must be maintained to ensure that it is timely and valid. The term data scrubbing refers to maintenance of the data warehouse by deleting information that is unreliable or no longer relevant." Pg 358-359 Krutz: The CISSP Prep Guide: Gold Edition
Not D: "To create a data warehouse, data is taken from an operational database, redundancies are removed, and the data is "cleaned up" in general." Pg 358 Krutz: The CISSP Prep Guide: Gold Edition

---

QUESTION 441:

A storage information architecture does not address which of the following?
A.) archiving of data
B.) collection of data
C.) management of data
D.) use of data

Answer: A

QUESTION 442:

Which of the following can be defined as the set of allowable values that an attribute can take?
A.) domain of a relation
B.) domain name service of a relation

C.) domain analysis of a relation
D.) domains, in database of a relation

Answer: A

QUESTION 443:

Programmed procedures which ensure that valid transactions are processed accurately and only once in the current timescale are referred to as

A. Data installation controls
B. Application controls
C. Operation controls
D. Physical controls

Answer: B

QUESTION 444:

What is the most effective means of determining how controls are functioning within an operating system?
A.) Interview with computer operator
B.) Review of software control features and/or parameters
C.) Review of operating system manual
D.) Interview with product vendor

Answer: B

QUESTION 445:

What is the most effective means of determining how controls are functioning within an operating system?
A.) Interview with computer operator
B.) Review of software control features and/or parameters
C.) Review of operating system manual
D.) Interview with product vendor

Answer: B

QUESTION 446:

Program change controls must ensure that all changes are

A. Audited to verify intent.
B. Tested to ensure correctness.
C. Implemented into production systems.

D. Within established performance criteria.

Answer: B
Document of the change. Once the change is approved, it should be entered into a change log and the log should be updated as the process continues toward completion.
Tested and presented. The change must be fully tested to uncover any unforeseen results. Depending on the severity of the change and the company's organization, the change and implementation may need to be presented to a change control committee. This helps show different sides to the purpose and outcome of the change and the possible ramifications. - Shon Harris All-in-one CISSP Certification Guide pg 815

QUESTION 447:

Which question is NOT true concerning Application Control?
A.) It limits end users use of applications in such a way that only particular screens are visible
B.) Only specific records can be requested choice
C.) Particular uses of application can be recorded for audit purposes
D.) Is non-transparent to the endpoint applications so changes are needed to the applications involved

Answer: D

QUESTION 448:

A computer program used to process the weekly payroll contains an instruction that the amount of the gross pay cannot exceed $2,500 for any one employee. This instruction is an example of a control that is referred to as a:

A. sequence check
B. check digit
C. limit check
D. record check

Answer: C

QUESTION 449:

What are edit controls?
A.) Preventive controls
B.) Detective controls
C.) Corrective controls
D.) Compensating controls

Answer: A

Explanation:

"Challenge Handshake Authentication Protocol (CHAP) One of the authentication protocols used over PPP links. CHAP encrypts usernames and passwords." Pg. 682 Glossary: Tittel: CISSP Study Guide

---

QUESTION 450:

Which one of the following properties of a transaction processing system ensures that once a transaction completes successfully (commits), the update service even if there is a system failure?

A. Atomicity
B. Consistency
C. Isolation
D. Durability

Answer: A
Atomicity is correct. Consistency is not a viable answer.
Atomicity states that database modifications must follow an "all or nothing" rule. Each transaction is said to be "atomic." If one part of the transaction fails, the entire transaction fails. It is critical that the database management system maintain the atomic nature of transactions in spite of any DBMS, operating system or hardware failure.
Consistency states that only valid data will be written to the database. If, for some reason, a transaction is executed that violates the database's consistency rules, the entire transaction will be rolled back and the database will be restored to a state consistent with those rules. On the other hand, if a transaction successfully executes, it will take the database from one state that is consistent with the rules to another state that is also consistent with the rules.
Isolation requires that multiple transactions occurring at the same time not impact each other's execution. For example, if Joe issues a transaction against a database at the same time that Mary issues a different transaction, both transactions should operate on the database in an isolated manner. The database should either perform Joe's entire transaction before executing Mary's or vice-versa. This prevents Joe's transaction from reading intermediate data produced as a side effect of part of Mary's transaction that will not eventually be committed to the database. Note that the isolation property does not ensure which transaction will execute first, merely that they will not interfere with each other.
Durability ensures that any transaction committed to the database will not be lost. Durability is ensured through the use of database backups and transaction logs that facilitate the restoration of committed transactions in spite of any subsequent software or hardware failures.

QUESTION 451:

To ensure integrity, a payroll application program may record transactions in the appropriate accounting period by using

A. Application checkpoints
B. Time and date stamps
C. Accrual journal entries
D. End of period journals

Answer: B

QUESTION 452:

What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?
A.) Accountability controls
B.) Mandatory access controls
C.) Assurance procedures
D.) Administrative controls

Answer: C
Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Pg 33 Krutz: The CISSP Prep Guide.

QUESTION 453:

Development staff should:
A.) Implement systems
B.) Support production data
C.) Perform unit testing
D.) Perform acceptance testing

Answer: C

QUESTION 454:

Which of the following is not used as a cost estimating technique during the project planning stage?
A.) Delphi technique
B.) Expert Judgment
C.) Program Evaluation Review Technique (PERT) charts
D.) Function points (FP)

Answer: C

Explanation:
"Methods and techniques for cost estimation:
Experts' evaluation
Delphi
Bottom-up approaches
Empirical models
COCOMO

Function Points
Combining Methods"

QUESTION 455:

Which of the following methodologies is appropriate for planning and controlling activities and resources in a system project?
A.) Gantt charts
B.) Program evaluation review technique (PERT)
C.) Critical path methodology (CPM)
D.) Function point analysis (FP)

Answer: A
A Gantt chart is a popular type of bar chart showing the interrelationships of how projects, schedules, and other time-related systems progress over time.
Not B:
Program Evaluation and Review Technique - (PERT) A method used to size a software product and calculate the Standard Deviation (SD) for risk assessment. The PERT equation (beta distribution) estimates the Equivalent Delivered Source Instructions (EDSIs) and the SD based on the analyst's estimates of the lowest possible size, the most likely size, and the highest possible size of each computer program component (CPC).
http://computing-dictionary.thefreedictionary.com/

QUESTION 456:

Which of the following is an advantage of using a high-level programming language?
A.) It decreases the total amount of code writters
B.) It allows programmers to define syntax
C.) It requires programmer-controlled storage management
D.) It enforces coding standards

Answer: A

QUESTION 457:

The design phase in a system development life cycle includes all of the following EXCEPT

A. Determining sufficient security controls.
B. Conducting a detailed design review.
C. Developing an operations and maintenance manual.
D. Developing a validation, verification, and testing plan.

Answer: C
Systems Development Life Cycle
Conceptual Defintion
Functional Requirements Determination

Protection Specifications Development
Design Review
Code Review Walk-Through
System Test Review
Certification and Accreditation
Maintenance
Pg 224-228 Tittel: CISSP Study Guide.

QUESTION 458:

By far, the largest security exposure in application system development relates to

A. Maintenance and debugging hooks.
B. Deliberate compromise.
C. Change control.
D. Errors and lock of training

Answer: A
Maintenance hook - instructions within a program's code that enable the developer or maintainer to enter the program without having to go through the usual access control and authentication processes. They should be removed from the code before being released for production; otherwise, they can cause serious security risks. They are also referred to as trapdoors. - Shon Harris All-in-one CISSP Certification Guide pg 933

QUESTION 459:

Which of the following is a 5th Generation Language?
A.) LISP
B.) BASIC
C.) NATURAL
D.) Assembly Language

Answer: A

QUESTION 460:

When considering the IT Development Life-Cycle, security should be:
A.) Mostly considered during the initiation phase.
B.) Mostly considered during the development phase.
C.) Treated as an integral part of the overall system design.
D.) Add once the design is completed.

Answer: C

QUESTION 461:

Which of the following represents the best programming?
A.) Low cohesion, low coupling
B.) Low cohesion, high coupling
C.) High cohesion, low coupling
D.) High cohesion, high coupling

Answer: C

QUESTION 462:

The INITIAL phase of the system development life cycle would normally include

A. Cost-benefit analysis
B. System design review
C. Executive project approval
D. Project status summary

Answer: C
Project management is an important part of product development and security management is an important part of project management. - Shon Harris All-in-one CISSP Certification Guide pg 732

QUESTION 463:

Which of the following computer design approaches is based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle?
A.) Pipelining
B.) Reduced Instruction Set Computers (RISC)
C.) Complex Instruction Set Computers (CISC)
D.) Scolar processors

Answer: C
Reference: pg 255 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 464:

Which one of the following tests determines whether the content of data within an application program falls within predetermined limits?

A. Parity check
B. Reasonableness check
C. Mathematical accuracy check
D. Check digit verification

Answer: B
Reasonableness check: A test to determine whether a value conforms to specified criteria. Note:

A reasonableness check can be used to eliminate questionable data points from subsequent processing.

QUESTION 465:

Buffer overflow and boundary condition errors are subsets of:
A.) Race condition errors
B.) Access validation errors
C.) Exceptional condition handling errors
D.) Input validation errors

Answer: D

QUESTION 466:

Which of the following statements pertaining to software testing approaches is correct?
A.) A bottom-up approach allows interface errors to be detected earlier
B.) A top-down approach allows errors in critical modules to be detected earlier
C.) The test plan and results should be retained as part of the system's permanent documentation
D.) Black box testing is predicated on a close examination of procedural detail

Answer: C

QUESTION 467:

Which of the following phases of a system development life-cycle is most concerned with authenticating users and processes to ensure appropriate access control decisions?
A.) Development/acquisition
B.) Implementation
C.) Operation/Maintenance
D.) Initiation

Answer: C

QUESTION 468:

Which of the following would be the most serious risk where a systems development life cycle methodology is inadequate?
A.) The project will be completed late
B.) The project will exceed the cost estimates
C.) The project will be incompatible with existing systems
D.) The project will fail to meet business and user needs

Answer: D

QUESTION 469:

Which of the following would best describe the difference between white-box testing and black-box testing?
A.) White-box testing is performed by an independent programmer team
B.) Black-box testing uses the bottom-up approach
C.) White-box testing examines the program internal logical structure
D.) Black-box testing involves the business units

Answer: C

QUESTION 470:

Which of the following refers to the work product satisfying the real-world requirements and concepts?
A.) validation
B.) verification
C.) concurrence
D.) accuracy

Answer: A
Reference: pg 820 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 471:

Which model, based on the premise that the quality of a software product is a direct function of the quality of it's associated software development and maintenance processes, introduced five levels with which the maturity of an organization involved in the software process is evaluated?
A.) The total Quality Model (TQM)
B.) The IDEAL Model
C.) The Software Capability Maturity Model
D.) The Spiral Model

Answer: C

QUESTION 472:

Which of the following would provide the best stress testing environment?
A.) Test environment using test data
B.) Test environment using live workloads
C.) Production environment using test data
D.) Production environment using live workloads

Answer: B

QUESTION 473:

In a change control environment, which one of the following REDUCES the assurance of proper changes to source programs in production status?

A. Authorization of the change.
B. Testing of the change.
C. Programmer access.
D. Documentation of the change.

Answer: C
I think I am going to disagree with the original answer (B testing of the change) here. The question has REDUCES the assurance.
"Personnel separate from the programmers should conduct this testing." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 345

QUESTION 474:

Why should batch files and scripts be stored in a protected area?

A.) Because of the least privilege concept
B.) Because they cannot be accessed by operators
C.) Because they may contain credentials
D.) Because of the need-to-know concept

Answer: C

QUESTION 475:

The PRIMARY purpose of operations security is

A. Protect the system hardware from environment damage.
B. Monitor the actions of vendor service personnel.
C. Safeguard information assets that are resident in the system.
D. Establish thresholds for violation detection and logging.

Answer: C
I think A or C could be the answers. I am leaning towards the C answer but use your best judgment.
"Operations Security can be described as the controls over the hardware in a computing facility, the data media used in a facility, and the operators using these resources in a facility...A Cissp candidate will be expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms that are available, the potential for access abuse, the appropriate controls, and the principles of good practice." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 297

QUESTION 476:

Which of the following is not a component of a Operations Security "triples"?
A.) Asset
B.) Threat
C.) Vulnerability
D.) Risk

Answer: D
Reference: pg 298 Krutz: CISSP Study Guide: Gold Edition

QUESTION 477:

A periodic review of user account management should not determine:
A.) Conformity with the concept of least privilege
B.) Whether active accounts are still being used
C.) Strength of user-chosen passwords
D.) Whether management authorizations are up-to-date

Answer: C

QUESTION 478:

Which of the following functions is less likely to be performed by a typical security administrator?
A.) Setting user clearances and initial passwords
B.) Adding and removing system users
C.) Setting or changing file sensitivity labels
D.) Reviewing audit data

Answer: B

QUESTION 479:

Who is responsible for setting user clearances to computer-based information?
A.) Security administrators
B.) Operators
C.) Data owners
D.) Data custodians

Answer: A

QUESTION 480:

Who is the individual permitted to add users or install trusted programs?

A. Database Administrator
B. Computer Manager
C. Security Administrator
D. Operations Manager

Answer: D
Typical system administrator or enhanced operator functions can include the following
Installing system software
Starting up (booting) and shutting down a system
Adding and removing system users
Performing back-ups and recovery
Handling printers and managing print queues -Ronald Krutz The CISSP PREP Guide (gold edition) pg 305-304

QUESTION 481:

In Unix, which file is required for you to set up an environment such that every used on the other host is a trusted user that can log into this host without authentication?

A. /etc/shadow
B. /etc/host.equiv
C. /etc/passwd
D. None of the choices.

Answer: B

Explanation:
The /etc/hosts.equiv file is saying that every user on the other host is a trusted user and allowed to log into this host without authentication (i.e. NO PASSWORD). The only thing that must exist for a user to log in to this system is an /etc/passwd entry by the same login name the user is currently using. In other words, if there is a user trying to log into this system whose login name is "bhope", then there must be a "bhope" listed in the /etc/passwd file.

QUESTION 482:

For what reason would a network administrator leverage promiscuous mode?

A. To screen out all network errors that affect network statistical information.
B. To monitor the network to gain a complete statistical picture of activity.
C. To monitor only unauthorized activity and use.
D. To capture only unauthorized internal/external use.

Answer: B

QUESTION 483:

Which of the following questions is less likely to help in assessing controls over hardware and software maintenance?
A.) In access to all program libraries restricted and controlled?
B.) Are integrity verification programs used by applications to look for evidences of data tampering, errors, and omissions?
C.) Is there version control?
D.) Are system components tested, documented, and approved prior to promotion to production?

Answer: B

QUESTION 484:

Which of the following correctly describe "good" security practice?

A. Accounts should be monitored regularly.
B. You should have a procedure in place to verify password strength.
C. You should ensure that there are no accounts without passwords.
D. All of the choices.

Answer: D

Explanation:
In many organizations accounts are created and then nobody ever touches those accounts again. This is a very poor security practice. Accounts should be monitored regularly, you should look at unused accounts and you should have a procedure in place to ensure that departing employees have their rights revoke prior to leaving the company. You should also have a procedure in place to verify password strength or to ensure that there are no accounts without passwords.

QUESTION 485:

Access to the _____ account on a Unix server must be limited to only the system administrators that must absolutely have this level of access.

A. Superuser of inetd.
B. Manager or root.
C. Fsf or root
D. Superuser or root.

Answer: D

Explanation:
Access to the superuser or root account on a server must be limited to only the system administrators that must absolutely have this level of access. Use of programs such as

SUDO is recommended to give limited and controlled root access to administrators that have a need for such access.

QUESTION 486:

Which of the following files should the security administrator be restricted to READ only access?
A.) Security parameters
B.) User passwords
C.) User profiles
D.) System log

Answer: D

QUESTION 487:

Root login should only be allowed via:

A. Rsh
B. System console
C. Remote program
D. VNC

Answer: B

Explanation:
The root account must be the only account with a user ID of 0 (zero) that has open access to the UNIX shell. It must not be possible for root to sign on directly except at the system console. All other access to the root account must be via the 'su' command.

QUESTION 488:

What does "System Integrity" mean?
A.) The software of the system has been implemented as designed.
B.) Users can't tamper with processes they do not own
C.) Hardware and firmware have undergone periodic testing to verify that they are functioning properly
D.) Design specifications have been verified against the formal top-level specification

Answer: C

QUESTION 489:

Operations Security seeks to primarily protect against which of the following?
A.) object reuse

B.) facility disaster
C.) compromising emanations
D.) asset threats

Answer: D

QUESTION 490:

In order to avoid mishandling of media or information, you should consider using:

A. Labeling
B. Token
C. Ticket
D. SLL

Answer: A

Explanation:
In order to avoid mishandling of media or information, proper labeling must be used.
All tape, floppy disks, and other computer storage media containing sensitive information must be externally marked with the appropriate sensitivity classification.
All tape, floppy disks, and other computer storage media containing unrestricted information must be externally marked as such.
All printed copies, printouts, etc., from a computer system must be clearly labeled with the proper classification.

QUESTION 491:

In order to avoid mishandling of media or information, which of the following should be labeled?

A. All of the choices.
B. Printed copies
C. Tape
D. Floppy disks

Answer: A

Explanation:
In order to avoid mishandling of media or information, proper labeling must be used.
All tape, floppy disks, and other computer storage media containing sensitive information must be externally marked with the appropriate sensitivity classification.
All tape, floppy disks, and other computer storage media containing unrestricted information must be externally marked as such.
All printed copies, printouts, etc., from a computer system must be clearly labeled with the proper classification.

As a rule of thumb, you should have an indication of the classification of the document. The classification is based on the sensitivity of information. It is usually marked at the minimum on the front and back cover, title, and first pages.

QUESTION 492:

Compact Disc (CD) optical media types is used more often for:
A.) very small data sets
B.) very small files data sets
C.) larger data sets
D.) very aggregated data sets

Answer: A

QUESTION 493:

At which temperature does damage start occurring to magnetic media?
A.) 100 degrees
B.) 125 degrees
C.) 150 degrees
D.) 175 degrees

Answer: A

QUESTION 494:

Which of the following statements pertaining to air conditioning for an information processing facility is correct?
A.) The AC units must be controllable from outside the area
B.) The AC units must keep negative pressure in the room so that smoke and other gases are forced out of the room
C.) The AC units must be n the same power source as the equipment in the room to allow for easier shutdown
D.) The AC units must be dedicated to the information processing facilities

Answer: D

QUESTION 495:

Removing unnecessary processes, segregating inter-process communications, and reducing executing privileges to increase system security is commonly called

A. Hardening
B. Segmenting
C. Aggregating
D. Kerneling

Answer: A
What is hardening? Naturally, there is more than one definition, but in general, one tightens control using policies which affect authorization, authentication and permissions. Nothing happens by default. You only give out permission after thinking about it, something like "deny all" to everyone, then "allow" with justification. Shut off everything, then only turn on that which must be turned on. It is not unlike locking every single door, window and access point in your house, then unlocking only those that need to be. It is quite common for users to take all the defaults when their new system gets turned on making for instant vulnerability. A major problem is trying to figure out where all those details are that need to be turned off, without making the system unusable.

QUESTION 496:

RAID levels 3 and 5 run:
A.) faster on hardware
B.) slower on hardware
C.) faster on software
D.)at the same speed on software and hardware

Answer: A

QUESTION 497:

Which of the following RAID levels functions as a single virtual disk?
A.) RAID Level 7
B.) RAID Level 5
C.) RAID Level 10
D.) RAID Level 2

Answer: A

QUESTION 498:

Which of the following takes the concept of RAID 1 (mirroring) and applies it to a pair of servers?
A.) A redundant server implementation
B.) A redundant client implementation
C.) A redundant guest implementation
D.) A redundant host implementation

Answer: A

QUESTION 499:

Which of the following enables the drive array to continue to operate if any disk or any

path to any disk fails?
A.) RAID Level 7
B.) RAID Level 1
C.) RAID Level 2
D.) RAID Level 5

Answer: A
"RAID Level 7 is a variation of RAID 5 wherein the array functions as a single virtual disk in the hardware. This is sometimes simulated by software running over a RAID level 5 hardware implementation, which enables the drive array to continue to operate if any disk or any path to any disk fails. It also provides parity protection." Pg 91 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 500:

Depending upon the volume of data that needs to be copied, full backups to tape can take:
A.) an incredible amount of time
B.) a credible amount of time
C.) an ideal amount of time
D.) an exclusive amount of time

Answer: A

QUESTION 501:

Which one of the following entails immediately transmitting copies of on-line transactions to a remote computer
facility for backup?

A. Archival storage management (ASM)
B. Electronic vaulting
C. Hierarchical storage management (HSM)
D. Data compression

Answer: B
"Electronic vaulting makes an immediate copy of a changed file or transaction and sends it to a remote location where the original backup is stored....Another technology used for automated backups is hierarrchial storage management (HSM). In this situation, the HSM system dynamically manages the storage and covery of files, which
are copied to storage media devices that vary in speed and cost. The faster media hold the data that is accessed more
often and the seldom-useed files are stored on the slower devices, or near-line devices. The different storage media
rang from optical disk, magnetic disks, and tapes. Pg. 619 Shon Harris CISSP All-In-One Certification Exam Guide

---

QUESTION 502:

When continuous availability (24 hours-a-day processing) is required, which one of the following provides a good alternative to tape backups?

A. Disk mirroring
B. Backup to jukebox
C. Optical disk backup
D. Daily archiving

Answer: B
Hierarchical Storage Management (HSM). HSM provides continuous on-line backup by using optical or tape 'jukeboxes,' similar to WORMs. It appears as an infinite disk to the system, and can be configured to provide the closest version of an available real-time backup. This is commonly employed in very large data retrieval systems." Pg. 71 Krutz: The CISSP Prep Guide.

QUESTION 503:

Zip/Jaz drives are frequently used for the individual backups of small data sets of:
A.) specific application data
B.) sacrificial application data
C.) static application data
D.) dynamic application data

Answer: A

QUESTION 504:

With non-continuous backup systems, data that was entered after the last backup prior to a system crash will have to be:
A.) recreated
B.) created
C.) updated
D.) deleted

Answer: A

QUESTION 505:

The alternate processing strategy in a business continuity plan can provide for required backup computing capacity through a hot site, a cold site, or

A. A dial-up services program.
B. An off-site storage replacement.
C. An online backup program.
D. A crate and ship replacement.

Answer: C
What I believe is being wanted here is not the other data center backup alternatives but transaction redundancy implementation.
The CISSP candidate should understand the three concepts used to create a level of fault tolerance and redundancy in transaction processing. While these processes are not used solely for disaster recovery, they are often elements of a larger disaster recovery plan. If one or more of these processes are employed, the ability of a company to get back online is greatly enhanced.
-Ronald Krutz The CISSP PREP Guide (gold edition) pg 394 (they are Electronic Vaulting, Remote journaling, and Database shadowing)

QUESTION 506:

The 8mm tape format is commonly used in Helical Scan tape drives, but was superseded by:
A.) Digital Linear Tape (DLT)
B.) Analog Linear Tape (ALT)
C.) Digital Signal Tape (DST)
D.) Digital Coded Tape (DCT)

Answer: A
"8mm Tape. This format was commonly used in Helical Scan tape drives, but was superseded by Digital Linear Tape (DLT)." Pg 95 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 507:

The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server in which of the following scenarios?
A.) system is up and running
B.) system is quiesced but operational
C.) system is idle but operational
D.) system is up and in single-user-mode

Answer: A

QUESTION 508:

Primarily run when time and tape space permits, and is used for the system archive or baselined tape sets is the:
A.) full backup method
B.) Incremental backup method
C.) differential backup method
D.) tape backup method

Answer: A

QUESTION 509:

This backup method makes a complete backup of every file on the server every time it is run by:
A.) full backup method
B.) incremental backup method
C.) differential backup method
D.) tape backup method

Answer: A

QUESTION 510:

A backup of all files that are new or modified since the last full backup is

A. In incremental backup
B. A father/son backup
C. A differential backup
D. A full backup

Answer: C
"Incremental backup -A procedure that backs up only those files that have been modified since the previous backup of any sort. It does remove the archive attribute.
Differential backup - A procedure that backs up all files that have been modified since the last full backup. It does not remove the archive attribute." - Shon Harris All-in-one CISSP Certification Guide pg 618

QUESTION 511:

What two factors should a backup program track to ensure the serviceability of backup tape media?

A. The initial usage data of the media and the number of uses.
B. The physical characteristics and rotation cycle of the media.
C. The manufactured and model number of the tape media.
D. The frequency of usage and magnetic composition.

Answer: B
The answer should be B. The physical charecteristics (what type of tape drive) and rotation cyle. (Frequency of backup cycles and retention timE.)

QUESTION 512:

Which of the following virus types changes some of its characteristics as it spreads?
A.) boot sector
B.) parasitic

C.) stealth
D.) polymorphic

Answer: D

QUESTION 513:

Which one of the following is a good defense against worms?

A. Differentiating systems along the lines exploited by the attack.
B. Placing limits on sharing, writing, and executing programs.
C. Keeping data objects small, simple, and obvious as to their intent.
D. Limiting connectivity by means of well-managed access controls.

Answer: B
Take as general information regarding worms
"Although the worm is not technically malicious, opening the attachment allows the file to copy itself to the user's PC Windows folder and then send the .pif-based program to any e-mail address stored on the hard drive.
Ducklin said the huge risks associated with accepting program files such as .pif, .vbs (visual basic script) or the more common .exe (executable) as attachments via e-mail outweighs the usefulness of distributing such files in this manner.
"There's no business sense for distributing programs via e-mail," he said.
To illustrate the point, Ducklin said six of the top 10 viruses reported to Sophos in April spread as Windows programs inside e-mails."
http://security.itworld.com/4340/030521stopworms/page_1.html

QUESTION 514:

An active content module, which attempts to monopolize and exploits system resources is called a

A. Macro virus
B. Hostile applet
C. Plug-in worm
D. Cookie

Answer: B
This applet can execute in the network browser and may contain malicious code. The types of downloadable programs are also known as mobile code. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 361
"ActiveX Controls are Microsoft's answer to Sun's Java applets. They operate in a very similar fashion, but they are implemented using any on of a variety of languages, including Visual Basic, C, C++ and Java. There are two key distinctions between Java applets and ActiveX controls. First, ActiveX controls use proprietary Microsoft technology and, therefore, can only execute on systems running Microsoft operating systems. Second, ActiveX controls are not

subject to the sandbox restrictions placed on Java applets. They have full access to the Windows operating environment and can perform a number of privileged actions. Therefore, special precautions must be taken when deciding which ActiveX controls to download and execute. Many security administrators have taken the somewhat harsh position of prohibiting the download of any ActiveX content from all but a select handful of trusted sites." Pg. 214 Tittel: CISSP Study Guide

---

QUESTION 515:

Macro viruses written in Visual Basic for Applications (VDA) are a major problem because

A. Floppy disks can propagate such viruses.
B. These viruses can infect many types of environments.
C. Anti-virus software is usable to remove the viral code.
D. These viruses almost exclusively affect the operating system.

Answer: D

QUESTION 516:

What is the term used to describe a virus that can infect both program files and boot sectors?

A. Polymorphic
B. Multipartite
C. Stealth
D. Multiple encrypting

Answer: B

QUESTION 517:

Why are macro viruses easy to write?

A. Active contents controls can make direct system calls
B. The underlying language is simple and intuitive to apply.
C. Only a few assembler instructions are needed to do damage.
D. Office templates are fully API compliant.

Answer: B
Macro Languages enable programmers to edit, delete, and copy files. Because these languages are so easy to use, many more types of macro viruses are possible. - Shon Harris All-in-one CISSP Certification Guide pg 785

QUESTION 518:

Which one of the following traits alow macro viruses to spread more effectively than other

types?

A. They infect macro systems as well as micro computers.
B. They attach to executable and batch applications.
C. They can be transported between different operating systems.
D. They spread in distributed systems without detection

Answer: C
Macro virus is a virus written in one of these programming languages and is platform independent. They infect and replicate in templates and within documents. - Shon Harris All-in-one CISSP Certification Guide pg 784

QUESTION 519:

In what way could Java applets pose a security threat?
A.) Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
B.) Java interpreters do not provide the ability to limit system access that an applet could have on a client system
C.) Executables from the Internet may attempt an intentional attack when they are downloaded on a client system
D.) Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.

Answer: C

Explanation:
"Java Security
Java applets use a security scheme that employs a sandbox to limit the applet's access to certain specific areas within the user's system and protects the system from malicious or poorly written applets. The applet is supposed to run only within the sandbox. The sandbox restricts the applet's environment by restricting access to a user's hard drives and system resources. If the applet does not go outside the sandbox, it is considered safe.
However, as with many other things in the computing world, the bad guys have figured out how to escape their confines and restrictions. Programmers have figured out how to write applets that enable the code to access hard drives and resources that are supposed to be protected by the Java security scheme. This code can be malicious in nature and cause destruction and mayhem to the user and her system.
Java employs a sandbox in its security scheme, but if an applet can escape the confines of the sandbox, the system can be easily compromised." Pg 726 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 520:

What setup should an administrator use for regularly testing the strength of user passwords?

A.) A networked workstation so that the live password database can easily be accessed by the cracking program
B.) A networked workstation so the password database can easily be copied locally and processed by the cracking program
C.) A standalone workstation on which the password database is copied and processed by the cracking program
D.) A password-cracking program is unethical; therefore it should not be used.

Answer: C

QUESTION 521:

On UNIX systems, passwords shall be kept:

A. In any location on behalf of root.
B. In a shadow password file.
C. In the /etc/passwd file.
D. In root.

Answer: B

Explanation:
When possible, on UNIX systems, passwords shall not be kept in the /etc/passwd file, but rather in a shadow password file which can be modified only by root or a program executing on behalf of root.

QUESTION 522:

Which of the following would constitute the best example of a password to use for access to a system by a network administrator?
A.) holiday
B.) Christmas12
C.) Jenny&30
D.) TrZc&45g

Answer: D

QUESTION 523:

Which of the following is not a media viability control used to protect the viability of data storage media?
A.) clearing
B.) marking
C.) handling
D.) storage

Answer: A
Reference: pg 315 Krutz: CISSP Study Guide: Gold Edition

QUESTION 524:

Which of the following refers to the data left on the media after the media has been erased?
A.) remanence
B.) recovery
C.) sticky bits
D.) semi-hidden

Answer: A

QUESTION 525:

What is the main issue with media reuse?
A.) Degaussing
B.) Data remanence
C.) Media destruction
D.) Purging

Answer: B

QUESTION 526:

What should a company do first when disposing of personal computers that once were used to store confidential data?
A.) Overwrite all data on the hard disk with zeroes
B.) Delete all data contained on the hard disk
C.) Demagnetize the hard disk
D.) Low level format the hard disk

Answer: C

QUESTION 527:

Which of the following is not a critical security aspect of Operations Controls?
A.) Controls over hardware
B.) data media used
C.) Operations using resources
D.) Environment controls

Answer: D
Reference: pg 311 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 528:

What tool is being used to determine whether attackers have altered system files of executables?

A. File Integrity Checker
B. Vulnerability Analysis Systems
C. Honey Pots
D. Padded Cells

Answer: A

Explanation:
Although File Integrity Checkers are most often used to determine whether attackers have altered system files or executables, they can also help determine whether vendor-supplied bug patches or other desired changes have been applied to system binaries. They are extremely valuable to those conducting a forensic examination of systems that have been attacked, as they allow quick and reliable diagnosis of the footprint of an attack. This enables system managers to optimize the restoration of service after incidents occur.

QUESTION 529:

A system file that has been patched numerous times becomes infected with a virus. The anti-virus software warns that disinfecting the file can damage it. What course of action should be taken?
A.) Replace the file with the original version from master media
B.) Proceed with automated disinfection
C.) Research the virus to see if it is benign
D.) Restore an uninfected version of the patched file from backup media

Answer: D

QUESTION 530:

In an on-line transaction processing system, which of the following actions should be taken when erroneous or invalid transactions are detected?
A.) The transactions should be dropped from processing
B.) The transactions should be processed after the program makes adjustments
C.) The transactions should be written to a report and reviewed
D.) The transactions should be corrected and reprocessed

Answer: C

QUESTION 531:

Which of the following is a reasonable response from the intrusion detection system when it detects Internet

Protocol (IP) packets where the IP source address is the same as the IP destination address?

A. Allow the packet to be processed by the network and record the event.
B. Record selected information about the item and delete the packet.
C. Resolve the destination address and process the packet.
D. Translate the source address and resend the packet.

Answer: B
RFC 1918 and RFC 2827 state about private addressing and ip spoofing using the same source address as destination address. Drop the packet.

QUESTION 532:

Which of the following is not a good response to a detected intrusion?
A.) Collect additional information about the suspected attack
B.) Inject TCP reset packets into the attacker's connection to the victim system
C.) Reconfigure routers and firewalls to block packets from the attacker's apparent connection
D.) Launch attacks or attempt to actively gain information about the attacker's host

Answer: D

QUESTION 533:

Once an intrusion into your organizations information system has been detected, which of the following actions should be performed first?
A.) Eliminate all means of intruder access
B.) Contain the intrusion
C.) Determine to what extent systems and data are compromised
D.) Communicate with relevant parties

Answer: B

QUESTION 534:

After an intrusion has been contained and the compromised systems having been reinstalled, which of the following need not be reviewed before bringing the systems back to service?
A.) Access control lists
B.) System services and their configuration
C.) Audit trails
D.) User accounts

Answer: C

QUESTION 535:

Which of the following includes notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects?
A.) Intrusion Evaluation (IE) and Response
B.) Intrusion Recognition (IR) and Response
C.) Intrusion Protection (IP) and Response
D.) Intrusion Detection (ID) and Response

Answer: D
"Intrusion Detection (ID) and Response is the task of monitoring systems for evidence of an intrusion or an inappropriate usage. This includes notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects." Pg 86 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 536:

Which of the following is used to monitor network traffic or to monitor host audit logs in order to determine violations of security policy that have taken place?
A.) Intrusion Detection System
B.) Compliance Validation System
C.) Intrusion Management System
D.)Compliance Monitoring System

Answer: A

QUESTION 537:

Which of the following is not a technique used for monitoring?
A.) Penetration testing
B.) Intrusion detection
C.) Violation processing (using clipping levels)
D.) Countermeasures testing

Answer: D

QUESTION 538:

Which one of the following is NOT a characteristic of an Intrusion Detection System? (IDS)

A. Determines the source of incoming packets.
B. Detects intruders attempting unauthorized activities.
C. Recognizes and report alterations to data files.
D. Alerts to known intrusion patterns.

Answer: C

Explanation: Software employed to monitor and detect possible attacks and behaviors that

vary from the normal and expected activity. The IDS can be network-based, which monitors network traffic, or host-based, which monitors activities of a specific system and protects system files and control mechanisms. - Shon Harris All-in-one CISSP Certification Guide pg 932

QUESTION 539:

An IDS detects an attach using which of the following?
A.) an event-based ID or a statistical anomaly-based ID
B.) a discrete anomaly-based ID or a signature-based ID
C.) a signature-based ID or a statistical anomaly-based ID
D.) a signature-based ID or an event-based ID

Answer: C

QUESTION 540:

Which of the following monitors network traffic in real time?
A.) network-based IDS
B.) host-based IDS
C.) application-based IDS
D.) firewall-based IDS

Answer: A

QUESTION 541:

What technology is being used to detect anomalies?

A. IDS
B. FRR
C. Sniffing
D. Capturing

Answer: A

Explanation:
Intrusion Detection is a quickly evolving domain of expertise. In the past year we have seen giant steps forward in this area. We are now seeing IDS engines that will detect anomalies, and that have some built-in intelligence. It is no longer a simple game of matching signatures in your network traffic.

QUESTION 542:

IDSs verify, itemize, and characterize threats from:

A. Inside your organization's network.
B. Outside your organization's network.
C. Outside and inside your organization's network.
D. The Internet.

Answer: C

Explanation:
IDSs verify, itemize, and characterize the threat from both outside and inside your organization's network, assisting you in making sound decisions regarding your allocation of computer security resources. Using IDSs in this manner is important, as many people mistakenly deny that anyone (outsider or insider) would be interested in breaking into their networks. Furthermore, the information that IDSs give you regarding the source and nature of attacks allows you to make decisions regarding security strategy driven by demonstrated need, not guesswork or folklore.

QUESTION 543:

IDS can be described in terms of what fundamental functional components?

A. Response
B. Information Sources
C. Analysis
D. All of the choices.

Answer: D

Explanation:
Many IDSs can be described in terms of three fundamental functional components:
Information Sources - the different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.
Analysis - the part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection.
Response - the set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

QUESTION 544:

What are the primary goals of intrusion detection systems? (Select all that apply.)

A. Accountability
B. Availability
C. Response
D. All of the choices

Answer: A, C

Explanation:
Although there are many goals associated with security mechanisms in general, there are two overarching goals usually stated for intrusion detection systems.
Accountability is the capability to link a given activity or event back to the party responsible for initiating it. This is essential in cases where one wishes to bring criminal charges against an attacker. The goal statement associated with accountability is: "I can deal with security attacks that occur on my systems as long as I know who did it (and where to find them.)" Accountability is difficult in TCP/IP networks, where the protocols allow attackers to forge the identity of source addresses or other source identifiers. It is also extremely difficult to enforce accountability in any system that employs weak identification and authentication mechanisms.
Response is the capability to recognize a given activity or event as an attack and then taking action to block or otherwise affect its ultimate goal. The goal statement associated with response is "I don't care who attacks my system as long as I can recognize that the attack is taking place and block it." Note that the requirements of detection are quite different for response than for accountability.

QUESTION 545:

What is the most common way to classify IDSs?

A. Group them by information source.
B. Group them by network packets.
C. Group them by attackers.
D. Group them by signs of intrusion.

Answer: A

Explanation:
The most common way to classify IDSs is to group them by information source. Some IDSs analyze network packets, captured from network backbones or LAN segments, to find attackers. Other IDSs analyze information sources generated by the operating system or application software for signs of intrusion.

QUESTION 546:

The majority of commercial intrusion detection systems are:

A. Identity-based

B. Network-based
C. Host-based
D. Signature-based

Answer: B

Explanation:
The majority of commercial intrusion detection systems are network-based. These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts.

QUESTION 547:

Which of the following is a drawback of Network-based IDSs?

A. It cannot analyze encrypted information.
B. It is very costly to setup.
C. It is very costly to manage.
D. It is not effective.

Answer: A

Explanation:
Network-based IDSs cannot analyze encrypted information. This problem is increasing as more organizations (and attackers) use virtual private networks. Most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.

QUESTION 548:

Host-based IDSs normally utilize information from which of the following sources?

A. Operating system audit trails and system logs.
B. Operating system audit trails and network packets.
C. Network packets and system logs.
D. Operating system alarms and system logs.

Answer: A

Explanation:
Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs. Operating system audit trails are usually generated at

the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs. However, system logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend. Some host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with network management systems.

QUESTION 549:

When comparing host based IDS with network based ID, which of the following is an obvious advantage?

A. It is unaffected by switched networks.
B. It cannot analyze encrypted information.
C. It is not costly to setup.
D. It is not costly to manage.

Answer: A

Explanation:
Host-based IDSs are unaffected by switched networks. When Host-based IDSs operate on OS audit trails, they can help detect Trojan horse or other attacks that involve software integrity breaches. These appear as inconsistencies in process execution.

QUESTION 550:

You are comparing host based IDS with network based ID. Which of the following will you consider as an obvious disadvantage of host based IDS?

A. It cannot analyze encrypted information.
B. It is costly to remove.
C. It is affected by switched networks.
D. It is costly to manage.

Answer: D

Explanation:
Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored. Since at least the information sources (and sometimes part of the analysis engines) for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network, because the IDS only sees those network packets received by its host. Host-based IDSs can be disabled by certain denial-of-service attacks.

QUESTION 551:

Which of the following IDS inflict a higher performance cost on the monitored systems?

A. Encryption based
B. Host based
C. Network based
D. Trusted based

Answer: B

Explanation:
Host-based IDSs use the computing resources of the hosts they are monitoring, therefore inflicting a performance cost on the monitored systems.

QUESTION 552:

Application-based IDSs normally utilize information from which of the following sources?

A. Network packets and system logs.
B. Operating system audit trails and network packets.
C. Operating system audit trails and system logs.
D. Application's transaction log files.

Answer: D

Explanation:
Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. The most common information sources used by application-based IDSs are the application's transaction log files.

QUESTION 553:

Which of the following are the major categories of IDSs response options?

A. Active responses
B. Passive responses
C. Hybrid
D. All of the choices.

Answer: D

Explanation:
Once IDSs have obtained event information and analyzed it to find symptoms of attacks, they generate responses. Some of these responses involve reporting results and findings to a pre-specified location. Others involve more active automated responses. Though

researchers are tempted to underrate the importance of good response functions in IDSs, they are actually very important. Commercial IDSs support a wide range of response options, often categorized as active responses, passive responses, or some mixture of the two.

QUESTION 554:

Alarms and notifications are generated by IDSs to inform users when attacks are detected. The most common form of alarm is:

A. Onscreen alert
B. Email
C. Pager
D. Icq

Answer: A

Explanation:
Alarms and notifications are generated by IDSs to inform users when attacks are detected. Most commercial IDSs allow users a great deal of latitude in determining how and when alarms are generated and to whom they are displayed.
The most common form of alarm is an onscreen alert or popup window. This is displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS. The information provided in the alarm message varies widely, ranging from a notification that an intrusion has taken place to extremely detailed messages outlining the IP addresses of the source and target of the attack, the specific attack tool used to gain access, and the outcome of the attack. Another set of options that are of utility to large or distributed organizations are those involving remote notification of alarms or alerts. These allow organizations to configure the IDS so that it sends alerts to cellular phones and pagers carried by incident response teams or system security personnel.

QUESTION 555:

Which of the following is a valid tool that complements IDSs?

A. All of the choices.
B. Padded Cells
C. Vulnerability Analysis Systems
D. Honey Pots

Answer: A

Explanation:
Several tools exist that complement IDSs and are often labeled as intrusion detection products by vendors since they perform similar functions. They are Vulnerability

Analysis Systems, File Integrity Checkers, Honey Pots, and Padded Cells.
"IDS-Related Tools
Intrusion detection systems are often deployed in concert with several other components. These IDS-related tools expand the usefulness and capabilities of IDSs and make IDSs more efficient and less prone to false positives. These tools include honey pots, padded cells, and vulenerability scanners." Pg. 46 Tittel: CISSP Study Guide

---

QUESTION 556:

A problem with a network-based ID system is that it will not detect attacks against a host made by an intruder who is logged in at which of the following?
A.) host's terminal
B.) guest's terminal
C.) client's terminal
D.) server's terminal

Answer: A

QUESTION 557:

When the IDS detect attackers, the attackers are seamlessly transferred to a special host. This method is called:

A. Vulnerability Analysis Systems
B. Padded Cell
C. Honey Pot
D. File Integrity Checker

Answer: B

Explanation:
Padded cells take a different approach. Instead of trying to attract attackers with tempting data, a padded cell operates in tandem with traditional IDS. When the IDS detect attackers, it seamlessly transfers then to a special padded cell host.

QUESTION 558:

Which of the following is a weakness of both statistical anomaly detection and pattern matching?

A. Lack of ability to scale.
B. Lack of learning model.
C. Inability to run in real time.
D. Requirement to monitor every event.

Answer: B

Explanation: Disadvantages of Knowledge-based ID systems:
This system is resources- intensive; the knowledge database continually needs maintenance and updates
New, unique, or original attacks often go unnoticed.Disadvantages of Behavior-based ID systems:
The system is characterized by high false alarm rates. High positives are the most common failure of ID systems and can create data noise that makes the system unusable.
The activity and behavior of the users while in the networked system might not be static enough to effectively implement a behavior-based ID system. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 88

QUESTION 559:

The two most common implementations of Intrusion Detection are which of the following?
A.) They commonly reside on a discrete network segment and monitor the traffic on that network segment
B.) They commonly will not reside on a discrete network segment and monitor the traffic on that network segment
C.) They commonly reside on a discrete network segment but do not monitor the traffic on that network segment
D.) They commonly do not reside on a discrete network segment and monitor the traffic on that network segment

Answer: A

QUESTION 560:

What are the primary approaches IDS takes to analyze events to detect attacks?

A. Misuse detection and anomaly detection.
B. Log detection and anomaly detection.
C. Misuse detection and early drop detection.
D. Scan detection and anomaly detection.

Answer: A

Explanation:
There are two primary approaches to analyzing events to detect attacks: misuse detection and anomaly detection. Misuse detection, in which the analysis targets something known to be "bad", is the technique used by most commercial systems. Anomaly detection, in which the analysis looks for abnormal patterns of activity, has been, and continues to be, the subject of a great deal of research. Anomaly detection is used in limited form by a number of IDSs. There are strengths and weaknesses associated with each approach, and it appears that the most effective IDSs use mostly misuse detection methods with a smattering of anomaly detection components.

QUESTION 561:

Misuse detectors analyze system activity and identify patterns. The patterns corresponding to know attacks are called:

A. Attachments
B. Signatures
C. Strings
D. Identifications

Answer: B

Explanation:
Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection." The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

QUESTION 562:

Which of the following is an obvious disadvantage of deploying misuse detectors?

A. They are costly to setup.
B. They are not accurate.
C. They most be constantly updated with signatures of new attacks.
D. They are costly to use.

Answer: C

Explanation:
Misuse detectors can only detect those attacks they know about - therefore they must be constantly updated with signatures of new attacks. Many misuse detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks. State-based misuse detectors can overcome this limitation, but are not commonly used in commercial IDSs.

QUESTION 563:

What detectors identify abnormal unusual behavior on a host or network?

A. None of the choices.

B. Legitimate detectors.
C. Anomaly detectors.
D. Normal detectors.

Answer: C

Explanation:
Anomaly detectors identify abnormal unusual behavior (anomalies) on a host or network. They function on the assumption that attacks are different from "normal" (legitimate) activity and can therefore be detected by systems that identify these differences. Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation. The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.

QUESTION 564:

A network-based IDS is which of the following?
A.) active while it acquires data
B.) passive while it acquires data
C.) finite while it acquires data
D.) infinite while it acquires data

Answer: B

QUESTION 565:

Which of the following usually provides reliable, real-time information without consuming network or host resources?
A.) network-based IDS
B.) host-based IDS
C.) application-based IDS
D.) firewall-based IDS

Answer: A
"A network-based IDS has little negative affect on overall network performance, and because it is deployed on a single-purpose system, it doesn't adversely affect the performance of any other computer." Pg 34 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 566:

Which of the following would assist in intrusion detection?
A.) audit trails
B.) access control lists
C.) security clearances
D.) host-based authentication

Answer: A

QUESTION 567:

Using clipping levels refers to:
A.) setting allowable thresholds on reported activity
B.) limiting access to top management staff
C.) setting personnel authority limits based on need-to-know basis
D.) encryption of data so that it cannot be stolen

Answer: A

QUESTION 568:

In what way can violation clipping levels assist in violation tracking and analysis?
A.) Clipping levels set a baseline for normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred
B.) Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant
C.) Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to usercodes with a privileged status
D.) Clipping levels enable a security administrator to view all reductions in security levels which have been made to usercodes which have incurred violations

Answer: A

QUESTION 569:

When establishing a violation tracking and analysis process, which one of the following parameters is used to keep the quantity of data to manageable levels?

A. Quantity baseline
B. Maximum log size
C. Circular logging
D. Clipping levels

Answer: D
To make violation tracking effective, clipping levels must be established. A clipping level is a baseline of user activity that is considered a routine level of user errors. When a clipping level is exceeded, a violation record is then produced. Clipping levels are also used for variance detection. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 318

QUESTION 570:

Audit trails based upon access and identification codes establish...

A. intrustion detection thresholds
B. individual accountability
C. audit review critera
D. individual authentication

Answer: B
Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on the system and on the network. Audit trails can be used for intrusion detection and for the reconstruction of past events. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 65

QUESTION 571:

The primary reason for enabling software audit trails is which of the following?
A.) Improve system efficiency
B.) Improve response time for users
C.) Establish responsibility and accountability
D.) Provide useful information to track down processing errors

Answer: C
"Auditing capabilities ensure that users are accountable for their actions, verify that the security polices are enforced, and are used as investigation tools." Pg 161 Shon Harris: All-in-One CISSP Certification

---

QUESTION 572:

Tracing violations, or attempted violations of system security to the user responsible is a function of?

A. authentication
B. access management
C. integrity checking
D. accountability

Answer: D
Auditing capabilities ensure that users are accountable for their actions, verify that the security policies are enforced, worked as a deterrent to improper actions, and are used as investigation tools. - Shon Harris All-in-one CISSP Certification Guide pg 182

QUESTION 573:

According to the Minimum Security Requirements (MSR) for Multi-User Operating Systems (NISTIR 5153) document, which of the following statements pertaining to audit data recording is incorrect?

A.) The system shall provide end-to-end user accountability for all security-relevant events
B.) The system shall protect the security audit trail from unauthorized access
C.) For maintenance purposes, it shall be possible to disable the recording of activities that require privileges.
D.) The system should support an option to maintain the security audit trail data in encrypted format

Answer: C

QUESTION 574:

Which of the following questions is less likely to help in assessing controls over audit trails?
A.) Does the audit trail provide a trace of user actions?
B.) Are incidents monitored and tracked until resolved?
C.) Is access to online logs strictly controlled?
D.) Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Answer: B

QUESTION 575:

You should keep audit trail on which of the following items?

A. Password usage.
B. All unsuccessful logon.
C. All of the choices.
D. All successful logon.

Answer: C

Explanation:
Keep audit trail of password usage; log all Successful logon, Unsuccessful logon, Date, Time, ID, Login name. Control maximum logon attempt rate where possible.Where possible users must be automatically logged off after 30 minutes of inactivity.

QUESTION 576:

In addition to providing an audit trail required by auditors, logging can be used to

A. provide backout and recovery information
B. prevent security violations
C. provide system performance statistics
D. identify fields changed on master files.

Answer: B

Auditing tools are technical controls that track activity within a network on a network device or on a specific computer. Even though auditing is not an activity that will deny an entity access to a network or computer, it will track activities so a network administrator can understand the types of access that took place, identify a security breach, or warn the administrator of suspicious activity. This can be used to point out weakness of their technical controls and help administrators understand where changes need to be made to preserve the necessary security level within the environment. . - Shon Harris All-in-one CISSP Certification Guide pg 179-180

QUESTION 577:

Which of the following should NOT be logged for performance problems?

A. CPU load.
B. Percentage of use.
C. Percentage of idle time.
D. None of the choices.

Answer: D

Explanation:
The level of logging will be according to your company requirements. Below is a list of items that could be logged, please note that some of the items may not be applicable to all operating systems. What is being logged depends on whether you are looking for performance problems or security problems. However you have to be careful about performance problems that could affect your security.

QUESTION 578:

Which of the following should be logged for security problems?

A. Use of mount command.
B. Percentage of idle time.
C. Percentage of use.
D. None of the choices.

Answer: A

Explanation:
The level of logging will be according to your company requirements. Below is a list of items that could be logged, please note that some of the items may not be applicable to all operating systems. What is being logged depends on whether you are looking for performance problems or security problems. However you have to be careful about performance problems that could affect your security.

QUESTION 579:

Which of the following services should be logged for security purpose?

A. bootp
B. All of the choices.
C. sunrpc
D. tftp

Answer: B

Explanation:
Request for the following services should be logged: systat, bootp, tftp, sunrpc, snmp, snmp-trap, nfs.

QUESTION 580:

The auditing method that assesses the extent of the system testing, and identifies specific program logic that has not
been tested is called

A. Decision process analysis
B. Mapping
C. Parallel simulation
D. Test data method

Answer: D
"Testing of software modules or unit testing should be addressed when the modules are being designed. Personnel
separate from the programmers should conduct this testing. The test data is part of the specifications. Testing should
not only check the modules using normal and valid input data, but it should also check for incorrect types, out-of-range values, and other bounds and/or conditions. Live or actual field data is not recommended for use in the
testing procedures because both data types might not cover out-of-range situations and the correct outputs of the test
are unknown. Special test suites of data that exercise all paths of the software to the fullest extent possible and whose corrected resulting outputs are known beforehand should be used." Pg. 345 Krutz: The CISSP Prep Guide:
Gold Edition.

QUESTION 581:

Who should NOT have access to the log files?

A. Security staff.
B. Internal audit staff.
C. System administration staff.

D. Manager's secretary.

Answer: D

Explanation:
Logs must be secured to prevent modification, deletion, and destruction. Only authorized persons should have access or permission to read logs. A person is authorized if he or she is a member of the internal audit staff, security staff, system administration staff, or he or she has a need for such access to perform regular duties.

QUESTION 582:

Which of the following correctly describe the use of the collected logs?

A. They are used in the passive monitoring process only.
B. They are used in the active monitoring process only.
C. They are used in the active and passive monitoring process.
D. They are used in the archiving process only.

Answer: C

Explanation:
All logs collected are used in the active and passive monitoring process. All logs are kept on archive for a period of time. This period of time will be determined by your company policies. This allows the use of logs for regular and annual audits if retention is longer then a year. Logs must be secured to prevent modification, deletion, and destruction.

QUESTION 583:

All logs are kept on archive for a period of time. What determines this period of time?

A. Administrator preferences.
B. MTTR
C. Retention polices
D. MTTF

Answer: C

Explanation:
All logs collected are used in the active and passive monitoring process. All logs are kept on archive for a period of time. This period of time will be determined by your company policies. This allows the use of logs for regular and annual audits if retention is longer then a year. Logs must be secured to prevent modification, deletion, and destruction.

QUESTION 584:

Logs must be secured to prevent:

A. Creation, modification, and destruction.
B. Modification, deletion, and initialization.
C. Modification, deletion, and destruction.
D. Modification, deletion, and inspection.

Answer: C

Explanation:
All logs collected are used in the active and passive monitoring process. All logs are kept on archive for a period of time. This period of time will be determined by your company policies. This allows the use of logs for regular and annual audits if retention is longer then a year. Logs must be secured to prevent modification, deletion, and destruction.

QUESTION 585:

To ensure dependable and secure logging, all computers must have their clock synchronized to:

A. A central timeserver.
B. The log time stamp.
C. The respective local times.
D. None of the choices.

Answer: A

Explanation:
The following pre-requisite must be met to ensure dependable and secure logging:
All computers must have their clock synchronized to a central timeserver to ensure accurate time on events being logged.
If possible all logs should be centralized for easy analysis and also to help detect patterns of abuse across servers.
Logging information traveling on the network must be encrypted if possible.
Log files are stored and protected on a machine that has a hardened shell.
Log files must not be modifiable without a trace or record of such modification.

QUESTION 586:

To ensure dependable and secure logging, logging information traveling on the network should be:

A. Stored

B. Encrypted
C. Isolated
D. Monitored

Answer: B

Explanation:
The following pre-requisite must be met to ensure dependable and secure logging:
All computers must have their clock synchronized to a central timeserver to ensure accurate time on events being logged.
If possible all logs should be centralized for easy analysis and also to help detect patterns of abuse across servers.
Logging information traveling on the network must be encrypted if possible.
Log files are stored and protected on a machine that has a hardened shell.
Log files must not be modifiable without a trace or record of such modification.

QUESTION 587:

The activity that consists of collecting information that will be used for monitoring is called:

A. Logging
B. Troubleshooting
C. Auditing
D. Inspecting

Answer: A

Explanation:
Logging is the activity that consists of collecting information that will be used for monitoring and auditing. Detailed logs combined with active monitoring allow detection of security issues before they negatively affect your systems.

QUESTION 588:

How often should logging be run?

A. Once every week.
B. Always
C. Once a day.
D. During maintenance.

Answer: B

Explanation:
Usually logging is done 24 hours per day, 7 days per week, on all available systems and

services except during the maintenance window where some of the systems and services may not be available while maintenance is being performed.

QUESTION 589:

Which of the following are security events on Unix that should be logged?

A. All of the choices.
B. Use of Setgid.
C. Change of permissions on system files.
D. Use of Setuid.

Answer: A

Explanation:
The following file changes, conditions, and events are logged:
.rhosts.
UNIX Kernel.
/etc/password.
rc directory structure.
bin files.
lib files.
Use of Setuid.
Use of Setgid.
Change of permission on system or critical files.

QUESTION 590:

Which of the following are potential firewall problems that should be logged?

A. Reboot
B. All of the choices.
C. Proxies restarted.
D. Changes to configuration file.

Answer: B

Explanation:
The following firewall configuration problem are logged:
Reboot of the firewall.
Proxies that cannot start (e.g. Within TIS firewall).
Proxies or other important services that have died or restarted.
Changes to firewall configuration file.
A configuration or system error while firewall is running.

QUESTION 591:

Which of the following is required in order to provide accountability?
A.) Authentication
B.) Integrity
C.) Confidentiality
D.) Audit trails

Answer: A
Reference: pg 5 Tittel: CISSP Study Guide

QUESTION 592:

The principle of accountability is a principle by which specific action can be traced back to:

A. A policy
B. An individual
C. A group
D. A manager

Answer: B

Explanation:
The principle of accountability has been described in many reference; it is a principle by which specific action can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a specific user. The definition of "Significant" is entirely dependant on your business circumstances and risk management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we must also be able to ascertain that this specific user was responsible for the uninitiated action.

QUESTION 593:

The principle of _____ is a principle by which specific action can be traced back to anyone of your users.

A. Security
B. Integrity
C. Accountability
D. Policy

Answer: C

Explanation:
The principle of accountability has been described in many reference; it is a

principle by which specific action can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a specific user. The definition of "Significant" is entirely dependant on your business circumstances and risk management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we must also be able to ascertain that this specific user was responsible for the uninitiated action.

QUESTION 594:

According to the principle of accountability, what action should be traceable to a specific user?

A. Material
B. Intangible
C. Tangible
D. Significant

Answer: D

Explanation:
The principle of accountability has been described in many reference; it is a principle by which specific action can be traced back to an individual. As mentioned by Idrach, any significant action should be traceable to a specific user. The definition of "Significant" is entirely dependant on your business circumstances and risk management model. It was also mentioned by Rino that tracing the actions of a specific user is fine but we must also be able to ascertain that this specific user was responsible for the uninitiated action.

QUESTION 595:

Which of the following best ensures accountability of users for actions taken within a system or domain?
A.) Identification
B.) Authentication
C.) Authorization
D.) Credentials

Answer: A
"Identification is the process by which a subject professes an identify and accountability is initiated." Pg 149 Tittel: CISSP Study Guide
"Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identify to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time." Pg 36 Krutz: The CISSP Prep Guide

---

QUESTION 596:

Individual accountability does not include which of the following?
A.) unique identifiers
B.) policies & procedures
C.) access rules
D.) audit trails

Answer: B

QUESTION 597:

Controls provide accountability for individuals who are accessing sensitive information.
This accountability is accomplished:
A.) through access control mechanisms that require identification and authentication and through the audit function.
B.) through logical or technical controls involving the restriction of access to systems and the protection of information
C.) through logical or technical controls but not involving the restriction of access to systems and the protection of information.
D.) through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Answer: A

QUESTION 598:

What types of computer attacks are most commonly reported by IDSs?

A. System penetration
B. Denial of service
C. System scanning
D. All of the choices

Answer: D

Explanation:
Three types of computer attacks are most commonly reported by IDSs: system scanning, denial of service (DOS), and system penetration. These attacks can be launched locally, on the attacked machine, or remotely, using a network to access the target. An IDS operator must understand the differences between these types of attacks, as each requires a different set of responses.

QUESTION 599:

Operation security requires the implementation of physical security to control which of the

following?
A.) unauthorized personnel access
B.) incoming hardware
C.) contingency conditions
D.) evacuation procedures

Answer: A

QUESTION 600:

Configuration Management is a requirement for the following level(s)?
A.) B3 and A1
B.) B1, B2 and B3
C.) A1
D.) B2, B3, and A1

Answer: D
Reference: pg 306 Krutz: CISSP Study Guide: Gold Edition

QUESTION 601:

Which of the following is not concerned with configuration management?
A.) Hardware
B.) Software
C.) Documentation
D.) They all are concerned with configuration management

Answer: D

QUESTION 602:

Configuration Management controls what?
A.) Auditing of changes to the Trusted Computing Base
B.) Control of changes to the Trusted Computing Base
C.) Changes in the configuration access to the Trusted Computing Base
D.) Auditing and controlling any changes to the Trusted Computing Base

Answer: D
"Official Definition of Configuration Management
Identifying, controlling, accounting for and auditing changes made to the baseline TCB, which includes changes to hardware, software, and firmware.
A System that will control changes and test documentation through the operational life cycle of a system." Pg 698 Shon Harris: All-in-One CISSP Certification
"[B3] The security administrator role is clearly defined, and the system must be able to recover from failures without its security level being compromised." Pg. 226 Shon Harris CISSP All-In-One Exam Guide

QUESTION 603:

In addition to ensuring that changes to the computer system take place in an identifiable and controlled environment, configuration management provides assurance that future changes:

A. The application software cannot bypass system security features.
B. Do not adversely affect implementation of the security policy.
C. To do the operating system are always subjected to independent validation and verification.
D. In technical documentation maintain an accurate description of the Trusted Computer Base.

Answer: B
"The primary security goal of configuration management is to ensure that changes to the system do not unintentionally diminish security." Pg 306 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 604:

Which set of principal tasks constitutes configuration management?

A. Program management, system engineering, and quality assurance.
B. Requirements verification, design, and system integration and testing.
C. Independent validation and verification of the initial and subsequent baseline.
D. Identification, control, status accounting, and auditing of changes.

Answer: D
Configuration management is the process of tracking and approving changes to a system. It involves identifying, controlling, and auditing all changes made to the system.
Pg. 223 Krutz: The CISSP Prep Guide

QUESTION 605:

If the computer system being used contains confidential information, users must not:

A. Leave their computer without first logging off.
B. Share their desks.
C. Encrypt their passwords.
D. Communicate

Answer: A

Explanation:
If the computer system being used or to which a user is connected contains sensitive or confidential information, users must not leave their computer, terminal, or workstation without first logging off. Users should be reminded frequently to follow this rule.

QUESTION 606:

Separation of duties is valuable in deterring:

A. DoS
B. external intruder
C. fraud
D. trojan house

Answer: C

Explanation:
Separation of duties is considered valuable in deterring fraud since fraud can occur if an opportunity exists for collaboration between various jobs related capabilities. Separation of duty requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set. The most commonly used examples are the separate transactions needed to initiate a payment and to authorize a payment. No single individual should be capable of executing both transactions.

QUESTION 607:

What principle requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set?

A. Use of rights
B. Balance of power
C. Separation of duties
D. Fair use

Answer: C

Explanation:
Separation of duties is considered valuable in deterring fraud since fraud can occur if an opportunity exists for collaboration between various jobs related capabilities. Separation of duty requires that for particular sets of transactions, no single individual be allowed to execute all transactions within the set. The most commonly used examples are the separate transactions needed to initiate a payment and to authorize a payment. No single individual should be capable of executing both transactions.

QUESTION 608:

Separation of duty can be:

A. Dynamic only

B. Encrypted
C. Static only
D. Static or dynamic

Answer: D

Explanation:
Separation of duty can be either static or dynamic. Compliance with static separation requirements can be determined simply by the assignment of individuals to roles and allocation of transactions to roles. The more difficult case is dynamic separation of duty where compliance with requirements can only be determined during system operation. The objective behind dynamic separation of duty is to allow more flexibility in operations.

QUESTION 609:

What is the company benefit, in terms of risk, for people taking a vacation of a specified minimum length?

A. Reduces stress levels, thereby lowering insurance claims.
B. Improves morale, thereby decreasing errors.
C. Increases potential for discovering frauds.
D. Reduces dependence on critical individuals.

Answer: C
Mandatory vacations are another type of administrative control that may sound a bit odd at first. Chapter 3 touches on reasons to make sure that employees take their vacations; this has to do with being able to identify fraudulent activities and enable job rotation to take place. - Shon Harris All-in-one CISSP Certification Guide pg 810

QUESTION 610:

Which of the following would be less likely to prevent an employee from reporting an incident?

A.) They are afraid of being pulled into something they don't want to be involved with
B.) The process of reporting incidents is centralized
C.) They are afraid of being accused of something they didn't do
D.) They are unaware of the company's security policies and procedures

Answer: A

Explanation:
Reference: ALL-IN-ONE CISSP Third Edition by Shon Harris Pg 783.

QUESTION 611:

Employee involuntary termination processing should include

A. A list of all passwords used by the individual.
B. A report on outstanding projects.
C. The surrender of any company identification.
D. Signing a non-disclosure agreement.

Answer: C
"Before the employee is released, all organization-specific identification, access, or security badges as well as cards, keys, and access tokens should be collected."
Pg. 173 Tittel: CISSP Study Guide

QUESTION 612:

Which trusted facility management concept implies that two operators must review and approve the work of each other?
A.) Two-man control
B.) Dual control
C.) Double control
D.) Segregation control

Answer: A

Explanation:
"In the concept of two-man control, two operators review and approve the work of each other. The purpose of two-man control is to provide accountability and to minimize fraud in highly sensitive or high-risk transactions. The concept of dual control means that both operators are needed to complete a sensitive task." Pg. 303 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 613:

When two operators review and approve the work of each other, this is known as?
A.) Dual control
B.) Two-man control
C.) Two-fold control
D.) Twin control

Answer: B

QUESTION 614:

What security procedure forces an operator into collusion with an operator of a different category to have access to unauthorized data?
A.) Enforcing regular password changes
B.) Management monitoring of audit logs
C.) Limiting the specific accesses of operations personnel

D.) Job rotation of people through different assignments

Answer: C

QUESTION 615:

Which of the following user items can be shared?

A. Password
B. Home directory
C. None of the choices.

Answer: C

Explanation:
Each user assigned directory (home directory) is not to be shared with others. None of the choices is correct.

QUESTION 616:

What should you do to the user accounts as soon as employment is terminated?

A. Disable the user accounts and erase immediately the data kept.
B. Disable the user accounts and have the data kept for a specific period of time.
C. None of the choices.
D. Maintain the user accounts and have the data kept for a specific period of time.

Answer: B

Explanation:
A record of user logins with time and date stamps must be kept. User accounts shall be disabled and data kept for a specified period of time as soon as employment is terminated. All users must log on to gain network access.

QUESTION 617:

What is the main objective of proper separation of duties?
A.) To prevent employees from disclosing sensitive information
B.) To ensure access controls are in place
C.) To ensure that no single individual can compromise a system
D.) To ensure that audit trails are not tampered with

Answer: C
"Separation of duties (also called segregation of duties) assigns parts of tasks to different personnel. Thus if no single person has total control of the system's security mechanisms, the

theory is that no single person can completely compromise the system."
Pg. 303 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 618:

What are the benefits of job rotation?

A. All of the choices.
B. Trained backup in case of emergencies.
C. Protect against fraud.
D. Cross training to employees.

Answer: A

Explanation:
Job assignments should be changed periodically so that it is more difficult for users to collaborate to exercise complete control of a transaction and subvert it for fraudulent purposes. This principle is effective when used in conjunction with a separation of duties. Problems in effectively rotating duties usually appear in organizations with limited staff resources and inadequate training programs. Rotation pf duties will protect you against fraud; provide cross training to you employees, as well as assuring trained backup in case of emergencies.

QUESTION 619:

Which of the following control pairing include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks in?
A.) Preventive/Administrative Pairing
B.) Preventive/Technical Pairing
C.) Preventive/Physical Pairing
D.) Detective/Administrative Pairing

Answer: A

QUESTION 620:

Which of the following are functions that are compatible in a properly segregated environment?
A.) Application programming and computer operation
B.) Systems programming and job control analysis
C.) Access authorization and database administration
D.) Systems development and systems maintenance

Answer: D

QUESTION 621:

Which of the following are functions that are compatible in a properly segregated environment?
A.) Security administration and quality assurance
B.) Security administration and data entry
C.) Security administration and application programming
D.) Application programming and data entry

Answer: A

Explanation:
Security Administration and Quality Assurance are the most similar tasks.
Administrative Management: Administrative management is a very important piece of operational security. One aspect of administrative management is dealing with personnel issues. This includes separation of duties and job rotation. The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. High-risk activities should be broken up into different parts and distributed to different individuals. This way the company does not need to put a dangerously high level of trust on certain individuals and if fraud were to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity.
Separation of duties also helps to prevent many different types of mistakes that can take place if one person is performing a task from the beginning to the end. For instance, a programmer should not be the one to test her own code. A different person with a different job and agenda should perform functionality and integrity testing on the programmer's code because the programmer may have a focused view of what the program is supposed to accomplish and only test certain functions, input values, and in certain environments.
Another example of separation of duties is the difference between the functions of a computer operator versus the functions of a system administrator. There must be clear cut lines drawn between system administrator duties and computer operator duties. This will vary from environment to environment and will depend on the level of security required within the environment. The system administrators usually have responsibility of performing backups and recovery procedures, setting permissions, adding and removing users, setting user clearance, and developing user profiles. The computer operator on the other hand, may be allowed to install software, set an initial password, alter desktop configurations, and modify certain system parameters. The computer operator should not be able to modify her own security profile, add and remove users globally, or set user security clearance. This would breach the concept of separation of duties.
Pg 808-809 Shon Harris: All-In-One CISSP Certification

QUESTION 622:

Which of the following are functions that are compatible in a properly segregated

environment?
A.) Data entry and job scheduling
B.) Database administration and systems security
C.) Systems analyst and application programming
D.) Security administration and systems programming

Answer: A
The two most similar jobs are Data Entry and Job Scheduling, so they need not be segregated.
Administrative Management: Administratative management is a very important piece of operational security. One aspect of administrative management is dealing with personnel issues. This includes separation of duties and job rotation. The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. High-risk activities should be broken up into different parts and distributed to different individuals. This way the company does not need to put a dangerously high level of trust on certain individuals and if fraud were to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity.
Separation of duties also helps to prevent many different types of mistakes that can take place if one person is performing a task from the beginning to the end. For instance, a programmer should not be the one to test her own code. A different person with a different job and agenda should perform functionality and integrity testing on the programmer's code because the programmer may have a focused view of what the program is supposed to accomplish and only test certain functions, input values, and in certain environments.
Another example of separation of duties is the difference between the functions of a computer operator versus the functions of a system administrator. There must be clear cut lines drawn between system administrator duties and computer operator duties. This will vary from environment to environment and will depend on the level of security required within the environment. The system administrators usually have responsibility of performing backups and recovery procedures, setting permissions, adding and removing users, setting user clearance, and developing user profiles. The computer operator on the other hand, may be allowed to install software, set an initial password, alter desktop configurations, and modify certain system parameters. The computer operator should not be able to modify her own security profile, add and remove users globally, or set user security clearance. This would breach the concept of separation of duties.
Pg 808-809 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 623:

Which of the following are functions that are compatible in a properly segregated environment?
A.) Application programming and computer operation
B.) Systems programming and job control analysis
C.) Access authorization and database administration
D.) System development and systems maintenance

Answer: C
Access Authorization and Database Administration are the most similar tasks of all the choices

so they need not be separated.
Administrative Management: Administratative management is a very important piece of operational security. One aspect of administrative management is dealing with personnel issues. This includes separation of duties and job rotation. The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. High-risk activities should be broken up into different parts and distributed to different individuals. This way the company does not need to put a dangerously high level of trust on certain individuals and if fraud were to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity.
Separation of duties also helps to prevent many different types of mistakes that can take place if one person is performing a task from the beginning to the end. For instance, a programmer should not be the one to test her own code. A different person with a different job and agenda should perform functionality and integrity testing on the programmer's code because the programmer may have a focused view of what the program is supposed to accomplish and only test certain functions, input values, and in certain environments.
Another example of separation of duties is the difference between the functions of a computer operator versus the functions of a system administrator. There must be clear cut lines drawn between system administrator duties and computer operator duties. This will vary from environment to environment and will depend on the level of security required within the environment. The system administrators usually have responsibility of performing backups and recovery procedures, setting permissions, adding and removing users, setting user clearance, and developing user profiles. The computer operator on the other hand, may be allowed to install software, set an initial password, alter desktop configurations, and modify certain system parameters. The computer operator should not be able to modify her own security profile, add and remove users globally, or set user security clearance. This would breach the concept of separation of duties.
Pg 808-809 Shon Harris: All-In-One CISSP Certification

QUESTION 624:

Controls are implemented to:
A.) eliminate risk and reduce potential for loss
B.) mitigate risk and eliminate the potential for loss
C.) mitigate risk and reduce the potential for loss
D.) eliminate risk and eliminate the potential for loss

Answer: C

QUESTION 625:

A timely review of system access audit records would be an example of which of the basic security functions?
A.) avoidance
B.) deterrence
C.) prevention
D.) detection

Answer: D

QUESTION 626:

A security control should

A. Allow for many exceptions.
B. Cover all contingencies.
C. Not rely on the security of its mechanism.
D. Change frequently.

Answer: C

QUESTION 627:

What set of principles is the basis for information systems controls?

A. Authentication, audit trails, and awareness briefings
B. Individual accountability, auditing, and separation of duties
C. Need to know, identification, and authenticity
D. Audit trails, limited tenure, and awareness briefings

Answer: C
"In addition to the CIA Triad, there is a plethora of other security-related concepts, principles, and tenants that should be considered and addressed when designing a security policy and deploying a security solution. This section discusses privacy, identification, authentication, authorization, accountability, nonrepudiation, and auditing." Pg. 133 Tittel: CISSP Study Guide

---

QUESTION 628:

An audit trail is a category of what control?

A. System, Manual
B. Detective, Technical
C. User, Technical
D. Detective, Manual

Answer: B

Explanation:
Detective Technical Controls warn of technical Access Control violations. Under this category you would find the following:
Audit trails
Violation reports

Intrusion detection system
Honeypot

QUESTION 629:

An IDS is a category of what control?

A. Detective, Manual
B. Detective, Technical
C. User, Technical
D. System, Manual

Answer: B

Explanation:
Detective Technical Controls warn of technical Access Control violations. Under this category you would find the following:
Audit trails
Violation reports
Intrusion detection system
Honeypot

QUESTION 630:

Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?
A.) Preventive/Administrative Pairing
B.) Preventive/Technical Pairing
C.) Preventive/Physical Pairing
D.) Detective/Technical Pairing

Answer: B

QUESTION 631:

Which one of the following can be identified when exceptions occur using operations security detective controls?

A. Unauthorized people seeing confidential reports.
B. Unauthorized people destroying confidential reports.
C. Authorized operations people performing unauthorized functions.
D. Authorized operations people not responding to important console messages.

Answer: C
C is the one that makes the most sence.

[Operation Security] Detective Controls are used to detect an error once it has occurred. Unlike preventative controls, these controls operate after the fact and can be used to track an unauthorized transaction for prosecution, or to lessen an error's impact on the system by identifying it quickly. An example of this type of control is an audit trail. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 299

QUESTION 632:

Which of the following is not an example of an operation control?
A.) backup and recovery
B.) audit trails
C.) contingency planning
D.) operations procedures

Answer: C
"Operation controls are the mechanisms and daily procedures that provide protection for systems."
When designing a protection scheme for resources, it is important to keep the following aspects or elements of the IT infrastructure in mind:
Communication hardware/software
Boundary devices
Processing equipment
Password files
Application program libraries
Application source code
Vendor software
Operating System
System Utilities
Directories and address tables
Proprietary packages
Main storage
Removable storage
Sensitive/critical data
System logs/audit trails
Violation reports
Backup files and media
Sensitive forms and printouts
Isolated devices, such as printers and faxes
Telephone network"
Pg 406-407 Tittel: CISSP Study Guide

QUESTION 633:

Which of the following is not an example of an operational control?
A.) backup and recovery
B.) audit trails

C.) contingency planning
D.) operations procedures

Answer: B
Audit Trails are under Operations Security Auditing opposed to Operations Security Operations Controls.
"Operations Controls embody the day-to-day procedures used to protect computer operations. The concepts of resource protection, hardware/software control, and privileged entity must be understood by the CISSP candidate." Pg. 311 Krutz: The CISSP Prep Guide: Gold Edition

---

QUESTION 634:

Access control allows you to exercise directing influence over which of the following aspects of a system?

A. Behavior, user, and content provider.
B. Behavior, use, and content.
C. User logs and content.
D. None of the choices.

Answer: B

Explanation:
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

QUESTION 635:

_____ is the means by which the ability to do something with a computer resource is explicitly enabled or restricted.

A. Access control
B. Type of access
C. System resource
D. Work permit

Answer: A

Explanation:
Access is the ability to do something with a computer resource (e.g., use, change, or view). Access control is the means by which the ability is explicitly enabled or restricted in some way (Usually through physical and system-based controls). Computer-based access controls can prescribe not only who or what process may have

access to a specific system resource, but also the type of access that is permitted.
These controls may be implemented in the computer system or in external devices.

QUESTION 636:

The ability to do something with a computer resource can be explicitly enabled or restricted through:

A. Physical and system-based controls.
B. Theoretical and system-based controls.
C. Mental and system-based controls.
D. Physical and trap-based controls.

Answer: A

Explanation:
Access is the ability to do something with a computer resource (e.g., use, change, or view). Access control is the means by which the ability is explicitly enabled or restricted in some way (Usually through physical and system-based controls).
Computer-based access controls can prescribe not only who or what process may have access to a specific system resource, but also the type of access that is permitted.
These controls may be implemented in the computer system or in external devices.

QUESTION 637:

The main categories of access control do NOT include:

A. Administrative Access Control
B. Logical Access Control
C. Random Access Control
D. Physical Access Control

Answer: C

Explanation:
There are several different categories of access control. The main categories are:
--Physical Access Control
--Administrative Access Control
--Logical Access Control
--Data Access Control

QUESTION 638:

You have very strict Physical Access controls. At the same time you have loose Logical Access Controls. What is true about this setting?

A. None of the choices.
B. It can 100% secure your environment.
C. It may secure your environment.
D. It may not secure your environment.

Answer: D

Explanation:
Access control is a bit like the four legs of a chair. Each of the legs must be equal or else an imbalance will be created. If you have very strict Physical Access controls but very poor Logical Access Controls then you may not succeed in securing your environment.

QUESTION 639:

Which of the following is not a detective technical control?

A. Intrusion detection system
B. Violation reports
C. Honeypot
D. None of the choices.

Answer: D

Explanation:
Detective Technical Controls warn of technical Access Control violations. Under this category you would find the following:
Audit trails
Violation reports
Intrusion detection system
Honeypot

QUESTION 640:

A business continuity plan is an example of which of the following?
A.) Corrective Control
B.) Detective Control
C.) Preventive Control
D.) Compensating Control

Answer: A

QUESTION 641:

_____ Technical Controls warn of technical Access Control violations.

A. Elusive
B. Descriptive
C. Corrective
D. Detective

Answer: D

Explanation:
Detective Technical Controls warn of technical Access Control violations. Under this category you would find the following:
Audit trails
Violation reports
Intrusion detection system
Honeypot

QUESTION 642:

A two factor authentication method is considered a:

A. Technical control
B. Patching control
C. Corrective control
D. Logical control

Answer: D

Explanation:
By technical controls we mean some or all of the following:
Access Control software
Antivirus Software
Passwords
Smart Cards
Encryption
Call-back systems
Two factor authentication

QUESTION 643:

Which of the following are NOT considered technical controls?

A. Access Control software
B. Man trap
C. Passwords
D. Antivirus Software

Answer: B

Explanation:
By technical controls we mean some or all of the following:
Access Control software
Antivirus Software
Passwords
Smart Cards
Encryption
Call-back systems
Two factor authentication

QUESTION 644:

_____ are the technical ways of restricting who or what can access system resources.

A. Preventive Manual Controls
B. Detective Technical Controls
C. Preventive Circuit Controls
D. Preventive Technical Controls

Answer: D

Explanation:
Preventive Technical Controls are the technical ways of restricting who or what can access system resources and what type of access is permitted. Its purpose is to protect the OS and other systems from unauthorized modification or manipulation. It is usually built into an operating system, or it can be a part of an application or program, or an add-on security package, or special components to regulate communication between computers. It also protects the integrity and availability by limiting the number of users and/or processes. These controls also protect confidential information from being disclosed to unauthorized persons.

QUESTION 645:

Which of the following is not a form of detective administrative control?
A.) Rotation of duties
B.) Required vacations
C.) Separation of duties
D.) Security reviews and audits

Answer: C

QUESTION 646:

Preventive Technical Controls are usually built:

A. By using MD5.
B. Into an operating system.
C. By security officer.
D. By security administrator.

Answer: B

Explanation:
Preventive Technical Controls are the technical ways of restricting who or what can access system resources and what type of access is permitted. Its purpose is to protect the OS and other systems from unauthorized modification or manipulation. It is usually built into an operating system, or it can be a part of an application or program, or an add-on security package, or special components to regulate communication between computers. It also protects the integrity and availability by limiting the number of users and/or processes. These controls also protect confidential information from being disclosed to unauthorized persons.

QUESTION 647:

Preventive Technical Controls cannot:

A. Protect the OS from unauthorized modification.
B. Protect confidential information from being disclosed to unauthorized persons.
C. Protect the OS from unauthorized manipulation.
D. Protect users from being monitored.

Answer: D

Explanation:
Preventive Technical Controls are the technical ways of restricting who or what can access system resources and what type of access is permitted. Its purpose is to protect the OS and other systems from unauthorized modification or manipulation. It is usually built into an operating system, or it can be a part of an application or program, or an add-on security package, or special components to regulate communication between computers. It also protects the integrity and availability by limiting the number of users and/or processes. These controls also protect confidential information from being disclosed to unauthorized persons.

QUESTION 648:

How do Preventive Technical Controls protect system integrity and availability?

A. By limiting the number of threads only.
B. By limiting the number of system variables.
C. By limiting the number of function calls only.

D. By limiting the number of users and/or processes.

Answer: D

Explanation:
Preventive Technical Controls are the technical ways of restricting who or what can access system resources and what type of access is permitted. Its purpose is to protect the OS and other systems from unauthorized modification or manipulation. It is usually built into an operating system, or it can be a part of an application or program, or an add-on security package, or special components to regulate communication between computers. It also protects the integrity and availability by limiting the number of users and/or processes. These controls also protect confidential information from being disclosed to unauthorized persons.

QUESTION 649:

Which of the following is NOT a type of access control?

A. Intrusive
B. Deterrent
C. Detective
D. Preventive

Answer: A

Explanation:
There are different types of access control. Access controls can be categorized as follows:
Preventive (in order to avoid occurrence)
Detective (in order to detect or identify occurrences)
Deterrent (in order to discourage occurrences)
Corrective (In order to correct or restore controls)
Recovery (in order to restore resources, capabilities, or losses)

QUESTION 650:

As a type of access control, which of the following asks for avoiding occurrence?

A. Preventive
B. Deterrent
C. Intrusive
D. Detective

Answer: A

Explanation:

There are different types of access control. Access controls can be categorized as follows:
Preventive (in order to avoid occurrence)
Detective (in order to detect or identify occurrences)
Deterrent (in order to discourage occurrences)
Corrective (In order to correct or restore controls)
Recovery (in order to restore resources, capabilities, or losses)

QUESTION 651:

As a type of access control, which of the following asks for identifying occurrences?

A. Deterrent
B. Preventive
C. Detective
D. Intrusive

Answer: C

Explanation:
There are different types of access control. Access controls can be categorized as follows:
Preventive (in order to avoid occurrence)
Detective (in order to detect or identify occurrences)
Deterrent (in order to discourage occurrences)
Corrective (In order to correct or restore controls)
Recovery (in order to restore resources, capabilities, or losses)

QUESTION 652:

As a type of access control, which of the following asks for discouraging occurrence?

A. Detective
B. Intrusive
C. Deterrent
D. Preventive

Answer: C

Explanation:
There are different types of access control. Access controls can be categorized as follows:
Preventive (in order to avoid occurrence)
Detective (in order to detect or identify occurrences)
Deterrent (in order to discourage occurrences)

Corrective (In order to correct or restore controls)
Recovery (in order to restore resources, capabilities, or losses)

QUESTION 653:

As a type of access control, which of the following asks for restoring controls?

A. Deterrent
B. Intrusive
C. Corrective
D. Preventive

Answer: C

Explanation:
There are different types of access control. Access controls can be categorized as follows:
Preventive (in order to avoid occurrence)
Detective (in order to detect or identify occurrences)
Deterrent (in order to discourage occurrences)
Corrective (In order to correct or restore controls)
Recovery (in order to restore resources, capabilities, or losses)

QUESTION 654:

What type of access control focuses on restoring resources?

A. Recovery
B. Preventive
C. Intrusive
D. Corrective

Answer: A

Explanation:
There are different types of access control. Access controls can be categorized as follows:
Preventive (in order to avoid occurrence)
Detective (in order to detect or identify occurrences)
Deterrent (in order to discourage occurrences)
Corrective (In order to correct or restore controls)
Recovery (in order to restore resources, capabilities, or losses)

QUESTION 655:

Access control is the collection of mechanisms that permits managers of a system to

exercise influence over the use of:

A. A man guard
B. An IS system
C. A threshold
D. A Trap

Answer: B

Explanation:
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

QUESTION 656:

What fencing height is likely to stop a determined intruder?
A.) 3' to 4' high
B.) 6' to 7' high
C.) 8' high and above with strands of barbed wire
D.) No fence can stop a determined intruder

Answer: C

QUESTION 657:

Lock picking is classified under which one of the following lock mechanism attacks?

A. Illicit key
B. Circumvention
C. Manipulation
D. Shimming

Answer: D

QUESTION 658:

The Physical Security domain addresses three areas that can be utilized to physically protect an enterprise's resources and sensitive information. Which of the following is not one of these areas?
A.) Threats
B.) Countermeasures
C.) Vulnerabilities
D.) Risks

Answer: D

QUESTION 659:

Which issue when selecting a facility site deals with the surrounding terrain, building markings and signs, and high or low population in the area?
A.) surrounding area and external entities
B.) natural disasters
C.) accessibility
D.) visibility

Answer: D

QUESTION 660:

Which of the following is not a physical control for physical security?
A.) lighting
B.) fences
C.) training
D.) facility construction materials

Answer: C

QUESTION 661:

The main risks that physical security components combat are all of the following EXCEPT:
A.) SYN flood
B.) physical damage
C.) theft
D.) availability

Answer: A

QUESTION 662:

What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?
A.) Central station alarm
B.) Proprietary alarm
C.) A remote station alarm
D.) An auxiliary station alarm

Answer: A

QUESTION 663:

Examples of types of physical access controls include all except which of the following?
A.) badges
B.) locks
C.) guards
D.) passwords

Answer: D

QUESTION 664:

Which of the following is the most costly countermeasures to reducing physical security risks?
A.) procedural controls
B.) hardware devices
C.) electronic systems
D.) personnel

Answer: D

QUESTION 665:

Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?
A.) Wave pattern motion detectors
B.) Capacitance detectors
C.) Field-powered devices
D.) Audio detectors

Answer: A

QUESTION 666:

Which of the following questions is less likely to help in assessing physical access controls?
A.) Does management regularly review the list of persons with physical access to sensitive facilities?
B.) Is the operating system configured to prevent circumvention of the security software and application controls?
C.) Are keys or other access devices needed to enter the computer room and media library?
D.) Are visitors to sensitive areas signed in and escorted?

Answer: B

QUESTION 667:

The concentric circle approach is used to

A. Evaluate environmental threats.
B. Assess the physical security facility,
C. Assess the communications network security.
D. Develop a personnel security program.

Answer: B
The original answer for this question was C (assess the communications network security) however I think the concentric circle is defining what in the krutz book is know as the security perimeter. To this end this is a reference
"A circular security perimeter that is under the access control defines the area or zone to be protected. Preventive/physical controls include fences, badges, multiple doors (man-traps that consists of two doors physically
separated so that an individual can be 'trapped' in the space between the doors after entering one of the doors), magnetic card entry systems, biometrics (for identification), guards, dogs, environmental control systems (temperature, humidity, and so forth), and building and access area layout." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 13
This is a standard concentric circle model shown in Figure 1 . If you've never seen this, you haven't had a security lecture.
On the outside is our perimeter. We are fortunate to have some defenses on our base. Although some bases don't have people guarding the gates and checking IDs any longer, there's still the perception that it's tougher to commit a crime on a Naval base than it would be at GM.
The point is: How much control do we have over fencing and guards? The answer: Not much.
The next circle, the red circle, contains your internal access controls. For our purposes, the heart of the red circle is the computer. That's what I want to zero in on. The internal controls are the things you can do to keep people out of your PCs and off your network.
http://www.chips.navy.mil/archives/96_oct/file5.htm

QUESTION 668:

The MAIN reason for developing closed-circuit television (CCTV) as part of your physical security program is to

A. Provide hard evidence for criminal prosecution.
B. Apprehend criminals.
C. Deter criminal activity.
D. Increase guard visibility.

Answer: D
A CCTV enables a guard to monitor many different areas at once from a centralized location.-
Shon Harris All-in-one CISSP Certification Guide pg 179-180

QUESTION 669:

Closed circuit TV is a feature of:

A. Detective Physical Controls
B. Corrective Physical Controls
C. Corrective Logical Controls
D. Logical Physical Controls

Answer: A

Explanation:
Detective Physical Controls would use the following: motion detectors, closed circuit TV, sensors, and alarms.

QUESTION 670:

Motion detector is a feature of:

A. Corrective Logical Controls.
B. Logical Physical Controls.
C. Corrective Physical Controls.
D. Detective Physical Controls.

Answer: D

Explanation:
Detective Physical Controls would use the following: motion detectors, closed circuit TV, sensors, and alarms.

QUESTION 671:

Which of the following is a physical control?
A.) Monitoring of system activity
B.) Environmental controls
C.) Identification and authentication methods
D.) Logical access control mechanisms

Answer: B

QUESTION 672:

Which of the following is a detective control?
A.) Segregation of duties
B.) Back-up procedures
C.) Audit trails

D.) Physical access control

Answer: C

QUESTION 673:

The basic Electronic Access Control (EAC) components required for access doors are an electromagnetic lock,

A. A credential reader, and a door closed sensor.
B. A card reader, and a door open sensor.
C. A biometric reader, and a door open sensor.
D. A card reader, and door motion detector.

Answer: A
We have not been able to find any reference to this question really. So we are going with A
"In addition to smart and dumb cards, proximity readers can be used to control physical access. A proximity reader can be passive device, a field-powered device, or a transponder." - Ed Tittle CISSP Study Guide (sybex) pg 650

QUESTION 674:

Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?
A.) Preventive/Technical Pairing
B.) Preventive/Administrative Pairing
C.) Preventive/Physical Pairing
D.) Detective/Administrative Pairing

Answer: B
"Preventive-Administrative
The following are the soft mechanisms that are put into place to enforce access control and protection for the company as a whole:
Policies and procedures
Effective hiring practices
Pre-employment background checks
Controlled termination processes
Data classification and labeling
Security awareness"
Pg. 157 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 675:

Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and the backing up of files are some of the examples of:

A.) Administrative controls
B.) Logical controls
C.) Technical controls
D.) Physical controls

Answer: D

QUESTION 676:

Which of the following is NOT a type of motion detector?
A.) photoelectric sensor
B.) wave pattern
C.) capacitance
D.) audio detector

Answer: D

Explanation: Audio detector detects sound not motion
Not A: A photoelectric sensor is a motion sensor that's what it was designed to do.

QUESTION 677:

Which of the following measures would be the BEST deterrent to the theft of corporate information from a laptop which was left in a hotel room?
A.) Store all data on disks and lock them in an in-room safe
B.) Remove the batteries and power supply from the laptop and store them separately from the computer
C.) Install a cable lock on the laptop when it is unattended
D.) Encrypt the data on the hard drive

Answer: D

QUESTION 678:

Guards are appropriate whenever the function required by the security program involves which of the following?
A.) The use of discriminating judgment
B.) The use of physical force
C.) The operation of access control devices
D.) The need to detect unauthorized access

Answer: A

QUESTION 679:

Which of the following floors would be most appropriate to locate information processing

facilities in a 6-stories building?
A.) Basement
B.) Ground floor
C.) Third floor
D.) Sixth floor

Answer: C

QUESTION 680:

Which of the following risk will most likely affect confidentiality, integrity and availability?
A.) Physical damage
B.) Unauthorized disclosure of information
C.) Loss of control over system
D.) Physical theft

Answer: D

QUESTION 681:

Which is the last line of defense in a physical security sense?
A.) people
B.) interior barriers
C.) exterior barriers
D.) perimeter barriers

Answer: A

QUESTION 682:

The recording of events with a closed-circuit TV camera is considered a:
A.) Preventative control
B.) Detective control
C.) Compensating control
D.) Corrective Control

Answer: B

QUESTION 683:

Sensor is:

A. Logical, Physical
B. Corrective, Logical
C. Detective, Physical
D. Corrective, Physical

Answer: C

Explanation:
Detective Physical Controls would use the following: motion detectors, closed circuit TV, sensors, and alarms.

QUESTION 684:

What fencing height is likely to stop a determined intruder?
A.) 3' to 4' high
B.) 6' to 7' high
C.) 8' high and above with strands of barbed wire
D.) No fence can stop a determined intruder

Answer: C
Reference: "2.4 meters/8 feet with top guard: Deters determined intruder". Pg 467 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 685:

A controlled light fixture mounted on a 5-meter pole can illuminate an area 30 meter in diameter. For security lighting purposes, what would be the proper distance between fixtures?

A. 25 meters
B. 30 meters
C. 35 meters
D. 40 meters

Answer: B
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and two feet out. (It is referred to as two-feet candles that reach eight feet in height) - Shon Harris All-in-one CISSP Certification Guide pg 325

QUESTION 686:

Critical areas should be lighted:
A.) Eight feet high and two feet out
B.) Eight feet high and four feet out
C.) Ten feet high and four feet out
D.) Ten feet high and six feet out

Answer: A

QUESTION 687:

Which of the following statements regarding an off-site information processing facility is TRUE?
A.) It should have the same amount of physical access restrictions as the primary processing unit
B.) It should be located in proximity to the originating site so that it can quicl be made operational
C.) It should be easily identified from the outside so in the event of an emergency it can be easily found
D.) Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive

Answer: A

QUESTION 688:

Which of the following is electromagnetic interference (EMI) that is noise from the radiation generated by the difference between the hot and ground wires?
A.) common-mode noise
B.) traverse-mode noise
C.) transversal-mode noise
D.) crossover-mode noise

Answer: A

QUESTION 689:

Which of the following is NOT a precaution you can take to reduce static electricity?
A.) power line conditioning
B.) anti-static sprays
C.) maintain proper humidity levels
D.) anti-static flooding

Answer: A

QUESTION 690:

Devices that supply power when the commercial utility power system fails are called which of the following?
A.) power conditioners
B.) uninterruptible power supplies
C.) power filters
D.) power dividers

Answer: B

QUESTION 691:

A prolonged high voltage is a:
A.) spike
B.) blackout
C.) surge
D.) fault

Answer: C

QUESTION 692:

A prolonged power supply that is below normal voltage is a:
A.) brownout
B.) blackout
C.) surge
D.) fault

Answer: A

QUESTION 693:

A prolonged power outage is a:
A.) brownout
B.) blackout
C.) surge
D.) fault

Answer: B

QUESTION 694:

A momentary power outage is a:
A.) spike
B.) blackout
C.) surge
D.) fault

Answer: D

QUESTION 695:

What can be defined as a momentary low voltage?
A.) Spike
B.) Sag
C.) Fault

D.) Brownout

Answer: B

QUESTION 696:

Electrical systems are the lifeblood of computer operations. The continued supply of clean, steady power is required to maintain the proper personnel environment as well as to sustain data operations. Which of the following is not an element that can threaten power systems?
A.) Noise
B.) Humidity
C.) Brownouts
D.) UPS

Answer: D

QUESTION 697:

Under what conditions would use of a "Class C" hand-held fire extinguisher be preferable to use of a "Class A" hand-held fire extinguisher?
A.) When the fire is in its incipient stage
B.) When the fire involves electrical equipment
C.) When the fire is located in an enclosed area
D.) When the fire is caused by flammable products

Answer: B

QUESTION 698:

Which of the following is a class C fire?
A.) electrical
B.) liquid
C.) common combustibles
D.) soda acid

Answer: A

QUESTION 699:

Which of the following is not a EPA-approved replacement for Halon?
A.) Water
B.) Argon
C.) NAF-S-III
D.) Bromine

Answer: D

QUESTION 700:

Which of the following suppresses combustion through a chemical reaction that kills the fire?
A.) Halon
B.) Co2
C.) water
D.) soda acid

Answer: A

QUESTION 701:

Which of the following is a class A fire?
A.) common combustibles
B.) liquid
C.) electrical
D.) Halon

Answer: A

QUESTION 702:

To be in compliance with the Montreal Protocol, which of the following options can be taken to refill a Halon flooding system in the event that Halon is fully discharged in the computer room?
A.) Order an immediate refill with Halon 1201 from the manufacture
B.) Contact a Halon recycling bank to make arrangements for a refill
C.) Order a different chlorofluorocarbon compound from the manufacture
D.) Order an immediate refill with Halon 1301 from the manufacture

Answer: B

QUESTION 703:

Under what conditions would the use of a Class C fire extinguisher be preferable to a Class A extinguisher?
A.) When the fire involves paper products
B.) When the fire is caused by flammable products
C.) When the fire involves electrical equipment
D.) When the fire is in an enclosed area

Answer: C

QUESTION 704:

Which of the following is true about a "dry pipe" sprinkler system?
A.) It is a substitute for carbon dioxide systems
B.) It maximizes chances of accidental discharge of water
C.) it minimizes chances of accidental discharge of water
D.) It uses less water than "wet pipe" systems

Answer: C

QUESTION 705:

Under what conditions would use of a "Class C" hand-held fire extinguisher be preferable to use of a "Class A" hand-held fire extinguisher?
A.) When the fire is in its incipient stage
B.) When the fire involves electrical equipment
C.) When the fire is located in an enclosed area
D.) When the fire is caused by flammable products

Answer: B

QUESTION 706:

Which fire class can water be most appropriate for?
A.) Class A fires
B.) Class B fires
C.) Class C fires
D.) Class D fires

Answer: A

QUESTION 707:

What category of water sprinkler system is currently the most recommended water system for a computer room?
A.) Dry Pipe sprinkler system
B.) Wet Pipe sprinkler system
C.) Pre-action sprinkler system
D.) Deluge sprinkler system

Answer: C

QUESTION 708:

Which of the following is currently the most recommended water system for a computer

room?
A.) pre-action
B.) wet pipe
C.) dry pipe
D.) deluge

Answer: A
Reference: pg 496 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 709:

According to the ISC2, what should be the fire rating for the walls of an information processing facility?
A.) All walls must have a one-hour minimum fire rating
B.) All walls must have a one-hour minimum fire rating, except for walls to adjacent rooms where records such as paper and media are stored, which should have a two-hour minimum fire rating
C.) All walls must have a two-hour minimum fire rating
D.) All walls must have a two-hour minimum fire rating, except for walls to adjacent rooms where records such as paper and media are stored, which should have a three-hour minimum fire rating.

Answer: C

QUESTION 710:

Which of the following suppresses the fuel supply of the fire?
A.) soda acid
B.) Co2
C.) Halon
D.) water

Answer: A

QUESTION 711:

Which of the following is true about a "dry pipe" sprinkler system?
A.) It is a substitute for carbon dioxide systems
B.) It maximizes chances of accidental discharge of water
C.) It minimizes chances of accidental discharge of water
D.) It uses less water than "wet pipe" systems

Answer: C

QUESTION 712:

The most prevalent cause of computer center fires is which of the following?
A.) AC equipment
B.) electrical distribution systems
C.) heating systems
D.) natural causes

Answer: B

QUESTION 713:

What fire suppression system can be used in computer rooms that will not damage computers and is safe for humans?
A.) Water
B.) FM200
C.) Halon
D.) CO2

Answer: B
Reference: http://www.fireline.com/fl_fm200firesuppression.html
FM-200 Systems
FM-200 Fire Suppression Systems - Halon Alternatives Fire Protection Systems
FM200 is a fire suppression system agent manufactured by Great Lakes Chemical.
How FM200 Suppresses Fire
FM200 suppresses fire by discharging as a gas onto the surface of combusting materials. Large amounts of heat energy are absorbed from the surface of the burning material, lowering it's temperature below the ignition point.
FM200 Fire Suppression Systems and the Environment
FM200 fire suppression systems have low atmospheric lifetimes, global warming, and ozone depletion potentials. Unlike Halon 1301 fire suppression systems, FM200 systems are environmentally friendly. They provide an effective, safe method of special hazards fire suppression where a non-residue producing clean agent is essential.

QUESTION 714:

The following are fire detector types EXCEPT:
A.) smoke activated
B.) flame actuated
C.) acoustical-seismic detection system
D.) heat activated

Answer: C

QUESTION 715:

Which fire class can water be most appropriate for?
A.) Class A fires
B.) Class B fires
C.) Class C fires
D.) Class D fires

Answer: A
"Fire Extinguisher Classes
Class Type Suppression Material
A Common combustibles Water, soda acid (dry powder)
B Liquids CO2 , Halon, soda acid
C Electrical CO2, Halon"
Pg. 578 Tittel: CISSP Study Guide

QUESTION 716:

Which one of the following actions should be taken FIRST after a fire has been detected?

A. Turn off power to the computers
B. Call the fire department
C. Notify management
D. Evacuate all personnel

Answer: D
Protection of life is of the utmost importance and should be dealt with first before looking to save material objects. . - Shon Harris All-in-one CISSP Certification Guide pg 625

QUESTION 717:

Which of the following provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat?
A.) Business continuity plan
B.) Incident response plan
C.) Disaster recovery plan
D.) Occupant emergency plan

Answer: D
"Occupant Emergency Plan (OEP). The OEP is a document providing coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat. It does not necessarily deal with business systems or IT system functionality, but rather focuses on personnel and property at a specific facility." Pg 666 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 718:

Disaster Recovery Plan emergency produces is a plan of action that commences immediately to prevent or minimize property damage and to:

A. Prevent interruption of service.
B. Minimize embarrassment.
C. Prevent loss of life.
D. Evacuate the facility.

Answer: C
Protection of life is of the utmost importance and should be dealt with first before looking to save material objects. - Shon Harris All-in-one CISSP Certification Guide pg 625

QUESTION 719:

What is the PRIMARY concern during a disaster?

A. Recover of the critical functions.
B. Availability of a hot site.
C. Acceptable outage duration.
D. Personnel safety.

Answer: D
Personal safety goes way above and beyond all other things, unless you're a rescue worker, and even then safety is still priority #1. Recovering critical functions and down time are not the MOST important concerns; Data can be recovered, a potential life loss cannote be Making Personal safety of the utmost important.

QUESTION 720:

Which of the following elements is not included in a Public Key Infrastructure (PKI)?
A.) Timestamping
B.) Lightweight Directory Access Protocol (LDAP)
C.) Certificate revocation
D.) Internet Key Exchange (IKE)

Answer: D

QUESTION 721:

In a Public Key Infrastructure (PKI) context, which of the following is a primary concern with LDAP servers?
A.) Availability
B.) Accountability
C.) Confidentiality

D.) Flexibility

Answer: A

QUESTION 722:

What is NOT true with pre shared key authentication within IKE/IPsec protocol:
A.) pre shared key authentication is normally based on simple passwords
B.) needs a PKI to work
C.) Only one preshared key for all VPN connections is needed
D.) Costly key management on large user groups

Answer: B

QUESTION 723:

What is the role of IKE within the IPsec protocol:
A.) peer authentication and key exchange
B.) data encryption
C.) data signature
D.) enforcing quality of service

Answer: A
"In order to set up and manage Sas on the Internet, a standard format called the Internet Security Association and Key Management Protocol (ISAKMP) was established. ISAKMP provides for secure key exchange and data authentication. However, ISAKMP is independent of the authentication protocols, security protocols, and encryption algorithms. Strictly speaking, a combination of three protocols is used to define key management for IPSEC. These protocols are ISAKMP, Secure Key Exchange Mechanism (SKEME) and Oakley. When combined and applied to IPSEC, these protocols are called the Internet Key Exchange (IKE) protocol." Pg. 222
Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 724:

In a Public Key Infrastructure, how are public keys published?
A.) They are sent via e-mail
B.) Through digital certificates
C.) They are sent by owners
D.) They are not published

Answer: B

QUESTION 725:

Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?

A.) Diffie-Hellman Key Exchange Protocol
B.) Internet Security Association and Key Management Protocol (ISAKMP)
C.) Simple Key-management for Internet Protocols (SKIP)
D.) OAKLEY

Answer: D

QUESTION 726:

Which of the following defines the key exchange for Internet Protocol Security (IPSEC)?

A. Internet Security Association Key Management Protocol (ISAKMP)
B. Internet Key Exchange (IKE)
C. Security Key Exchange (SKE)
D. Internet Communication Messaging Protocol (ICMP)

Answer: A
Because Ipsec is a framework, it does not dictate what hashing and encryption algorithms are to be used or how keys are to be exchanged between devices. Key management can be handled through manual process or automated a key management protocol. The Internet Security Association and Key management Protocol (ISAKMP) is an authentication and key exchange architecture that is independent of the type of keying mechanisms used.
Pg 577 Shon Harris All-In-One CISSP Certification Exam Guide

QUESTION 727:

A network of five nodes is using symmetrical keys to securely transmit data. How many new keys are required to re-establish secure communications to all nodes in the event there is a key compromise?

A. 5
B. 10
C. 20
D. 25

Answer: A
In a typical vpn using secret keys there would be one key at central office and the same key provided for each telecommuter, in this case 4. If the key was compromised, all 5 keys would have to be changed.
"Secret key cryptography is the type of encryption that is familiar to most people. In this type of cryptography, the sender and receiver both know a secret key. The sender encrypts the plaintext message with the secret key, and the receiver decrypts the message with the same secret key."
-Ronald Krutz The CISSP PREP Guide (gold edition) pg 194

QUESTION 728:

What is the effective key size of DES?
A.) 56 bits
B.) 64 bits
C.) 128 bits
D.) 1024 bits

Answer: A

QUESTION 729:

Matches between which of the following are important because they represent references from one relation to another and establish the connection among these relations?
A.) foreign key to primary key
B.) foreign key to candidate key
C.) candidate key to primary key
D.) primary key to secondary key

Answer: A

QUESTION 730:

Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets?
A.) Internet Security Association and Key Management Protocol (ISKAMP)
B.) Simple Key-Management for Internet Protocols (SKIP)
C.) Diffie-Hellman Key Distribution Protocol
D.) IPsec Key Exchange (IKE)

Answer: B
Reference: pg 117 Krutz

QUESTION 731:

What is the PRIMARY advantage of secret key encryption systems as compared with public key systems?

A. Faster speed encryption
B. Longer key lengths
C. Easier key management
D. Can be implemented in software

Answer: A
"The major strength of symmetric key cryptography is the great speed at which it can operate. By the nature of the mathematics involved, symmetric key cryptography also naturally lends itself to hardware implementations, creating the opportunity for even higher-speed operations."
Pg. 309 Tittel: CISSP Study Guide

QUESTION 732:

In a cryptographic key distribution system, the master key is used to exchange?

A. Session keys
B. Public keys
C. Secret keys
D. Private keys

Answer: A
"The Key Distribution Center (KDC) is the most import component within a Kerberos environment. The KDC holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The clients and services trust the integrity of the KDC, and this trust is the foundation of Kerberos security." Pg. 148 Shon Harris CISSP All-In-One Certification Exam Guide
'The basic principles of Kerberos operation are as follows:
1.) The KDC knows the secret keys of all clients and servers on the network.
2.) The KDC initially exchanges information with the client and server by using these secret keys.
3.) Kerberos authenticates a client to a requested service on a server through TGS, and by using temporary symmetric session keys for communications between the client and KDC, the server and the KDC, and the client and server.
4.) Communication then takes place between the client and the server using those temporary session keys."
Pg. 40 Krutz: The CISSP Prep Guide

QUESTION 733:

Which Application Layer security protocol requires two pair of asymmetric keys and two digital certificates?
A.) PEM
B.) S/HTTP
C.) SET
D.) SSL

Answer: C

QUESTION 734:

Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?
A.) foreign key
B.) candidate key
C.) Primary key
D.) Secondary key

Answer: A
Reference: pg 243 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 735:

What key size is used by the Clipper Chip?
A.) 40 bits
B.) 56 bits
C.) 64 bits
D.) 80 bits

Answer: D
"Each Clipper Chip has a unique serial number and an 80-bit unique unit or secret key. The unit key is divided into tow parts and is stored at two separate organizations with the serial number that uniquely identifies that particular Clipper Chip." Pg 166 Krutz: The CISSP Prep Guide

---

QUESTION 736:

What uses a key of the same length as the message?
A.) Running key cipher
B.) One-time pad
C.) Steganography
D.) Cipher block chaining

Answer: B
Reference:
"A one-time pad is an extremely powerful type of substitution cipher. One-time pads use a different alphabet for each letter of the plaintext message.
Normally, one-time pads are written as a very long series of numbers to be plugged into the function.
The great advantage to one-time pads is that, when used properly, they are an unbreakable encryption scheme. There is no repeating pattern of alphabetic substitution, redering cryptanalytic efforts useless. However, several requirements must be met to ensure the integrity of the algorithm:
The encryption key must be randomly generated. Using a phrase or a passage from a book would introduce the possibility of cryptanalysts breaking the code.
The one-time pad must be physically secured against disclosure. If the enemy has a copy of the pad, they can easily decrypt the enciphered messages.
Each one-time pad must be used only once. If pads are reused, cryptanalysts can compare similarities in multiple messages encrypted with the same pad and possibly determine the key values used.
The key must be at least as long as the message to be encrypted. This is because each key element is used to encode only one character of the message.
Pg. 304-305 Tittel: CISSP Study Guide

QUESTION 737:

Which of the following statements related to a private key cryptosystem is FALSE?
A.) The encryption key should be secure
B.) Data Encryption Standard (DES) is a typical private key cryptosystem
C.) The key used for decryption is known to the sender
D.) Two different keys are used for the encryption and decryption

Answer: D
"In symmetric key cryptography, a single secret key is used between entities, wheareas in public key systems, each entity has different keys, or asymmetric keys." Pg 476 Shon Harris CISSP Certification All-in-One Exam Guide

---

QUESTION 738:

Simple Key Management for Internet Protocols (SKIP) is similar to Secure Sockets Layer (SSL), except that it requires no prior communication in order to establish or exchange keys on a:
A.) Secure Private keyring basis
B.) response-by-session basis
C.) Remote Server basis
D.) session-by-session basis

Answer: D
Reference: pg 117 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 739:

A weak key of an encryption algorithm has which of the following properties?
A.) It is too short, and thus easily crackable
B.) It facilitates attacks against the algorithm
C.) It has much more zeroes than ones
D.) It can only be used as a public key

Answer: B

QUESTION 740:

Security measures that protect message traffic independently on each communication path are called:

A. Link oriented
B. Procedure oriented
C. Pass-through oriented
D. End-to-end oriented

Answer: A

Link encryption encrypts all the data along a specific communication path like a satellite link, T3 line, or telephone
circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data hat are part
of the packets are also encrypted. This provides extra protection against packet sniffers and eavesdroppers. - Shon
Harris All-in-one CISSP Certification Guide pg 560

QUESTION 741:

Who is responsible for the security and privacy of data during a transmission on a public communications link?

A. The carrier
B. The sending
C. The receiving party
D. The local service provider

Answer: B
The sender of an email is responsible for encryption if security is desired. A bank that sends data across web is responsible to utilize a secure protocol.

QUESTION 742:

Which of the following best provides e-mail message authenticity and confidentiality?
A.) Signing the message using the sender's public key and encrypting the message using the receiver's private key
B.) Signing the message using the sender's private key and encrypting the message using the receiver's public key
C.) Signing the message using the receiver's private key and encrypting the message using the sender's public key
D.) Signing the message using the receiver's public key and encrypting the message with the sender's private key

Answer: B

QUESTION 743:

Cryptography does not help in:
A.) Detecting fraudulent insertion
B.) Detecting fraudulent deletion
C.) Detecting fraudulent modifications
D.) Detecting fraudulent disclosure

Answer: D

QUESTION 744:

Which of the following is NOT a property of a one-way hash function?
A.) It converts a message of a fixed length into a message digest of arbitrary length
B.) It is computationally infeasible to construct two different messages with the same digest
C.) It converts a message of arbitrary length into a message digest of a fixed length
D.) Given a digest value, it is computationally infeasible to find the corresponding message

Answer: A

QUESTION 745:

How much more secure is 56 bit encryption opposed to 40 bit encryption?
A.) 16 times
B.) 256 times
C.) 32768 times
D.) 65,536 times

Answer: D
2 to the power of 40 = 1099511627776
2 to the power of 56 = 72057594037927936
72057594037927936 / 1099511627776 = 65,536

QUESTION 746:

Which of the following statements is true about data encryption as a method of protecting data?
A.) It should sometimes be used for password files
B.) It is usually easily administered
C.) It makes few demands on system resources
D.) It requires careful key Management

Answer: D
"Cryptography can be used as a security mechanism to provide confidentiality, integrity, and authentication, but not if the keys are compromised in any way. The keys can be captured, modified, corrupted, or disclosed to unauthorized individuals. Cryptography is based on a trust mode. Individuals trust each other to protect their own keys, they trust the administrator who is maintaining the keys, and they trust a server that holds, maintains and distributes the keys. Many administrators know that key management causes one of the biggest headaches in cryptographic implementation. There is more to key maintenance than using them to encrypt messages. The keys have to be distributed securely to the right entities and updated continuously. The keys need to be protected as they are being transmitted and while they are being stored on each workstation and server. The keys need to be generated, destroyed, and recovered properly, Key management can be handled through manual or automatic processes. Unfortunately, many companies use cryptographic keys, but rarely if ever change them. This is because of the hassle of key management and because the network administrator is already

overtaxed with other tasks or does not realize the task actually needs to take place. The frequency of use of a cryptographic key can have a direct correlation to often the key should be changed. The more a key is used, the more likely it is to be captured and compromised. If a key is used infrequently, then this risk drops dramatically. The necessary level of security and the frequency of use can dictate the frequency of the key updates.
Key management is the most challenging part of cryptography and also the most crucial. It is one thing to develop a very complicated and complex algorithm and key method, but if the keys are not securely stored and transmitted, it does not really matter how strong the algorithm is. Keeping keys secret is a challenging task." Pg 512-513 Shon Harris CISSP Certification All-In-One Exam Guide

---

QUESTION 747:

The primary purpose for using one-way encryption of user passwords within a system is which of the following?
A.) It prevents an unauthorized person from trying multiple passwords in one logon attempt
B.) It prevents an unauthorized person from reading or modifying the password list
C.) It minimizes the amount of storage required for user passwords
D.) It minimizes the amount of processing time used for encrypting password

Answer: B

QUESTION 748:

Which of the following is not a known type of Message Authentication Code (MAC)?
A.) Hash function-based MAC
B.) Block cipher-based MAC
C.) Signature-based MAC
D.) Stream cipher-based MAC

Answer: C

QUESTION 749:

Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT)?
A.) Secure Electronic Transaction (SET)
B.) Message Authentication Code (MAC)
C.) Cyclic Redundency Check (CRC)
D.) Secure Hash Standard (SHS)

Answer: B
Reference: pg 218 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 750:

Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use a hybrid encryption technique. What does this mean?
A.) Use of public key encryption to secure a secret key, and message encryption using the secret key
B.) Use of the recipient's public key for encryption and decryption based on the recipient's private key
C.) Use of software encryption assisted by a hardware encryption accelerator
D.) Use of elliptic curve encryption

Answer: A

QUESTION 751:

One-way hash provides:
A.) Confidentiality
B.) Availability
C.) Integrity
D.) Authentication

Answer: C
"Hash Functions
....how cryptosystems implement digital signatures to provide proof that a message originated from a particular user of a cryptosystem and to ensure that the message was not modified while in transit between the two parties."
Pg. 292 Tittel: CISSP Study Guide Second Edition
"integrity A state characterized by the assurance that modifications are not made by unauthorized users and authorized users do not make unauthorized modifications."
Pg. 616 Tittel: CISSP Study Guide Second Edition

QUESTION 752:

What size is an MD5 message digest (hash)?

A.) 128 bits
B.) 160 bits
C.) 256 bits
D.) 128 bytes

Answer: A
"MD4
MD4 is a one-way hash function designed by Ron Rivest. It produces 128-bit hash, or message digest, values. It is used for high-speed computation in software implementations and is optimized for microprocessors.
MD5
MD5 is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more

complex, which makes it harder to break. MD5 added a fourth round of operations to be performed during the hashing functions and makes several of it mathematical operations carry out more steps or more complexity to provide a higher level of security.
MD2
MD2 is also a 128-bit one-way hash designed by Ron Rivest. It is not necessarily any weaker than the previously mentioned hash functions, but is much slower.
SHA
SHA was designed by NIST and NSA to be used with DSS. The SHA was designed to be used with digital signatures and was developed when a more secure hashing algorithm was required for federal application.
SHA produces a 160-bit hash value, or message digest. This is then inputted into the DSA, which computes the signature for a message. The message digest is signed instead of the whole message because it is a much quicker process. The sender computes a 160-bit hash value, encrypts it with his private key (signs it), appends it to the message, and sends it. The receiver decrypts the value with the sender's public key, runs the same hashing function, and compares the two values. If the values are the same, the receiver can be sure that the message has not been tampered with in transit.
SHA is similar to MD4. It has some extra mathematical functions and produces a 160-bit hash instead of 128-bit, which makes it more resistant to brute force attacks, including birthday attacks.
HAVAL
HAVAL is a variable-length one-way hash function and is the modification of MD5. It processes message blocks twice the size of those used in MD5; thus it processes blocks of 1,024 bits.
Pg. 508-509 Shon Harris CISSP Certification All-In-One Exam Guide

---

QUESTION 753:

Which of the following is NOT a property of a one-way hash function?
A.) It converts a message of a fixed length into a message digest of arbitrary length.
B.) It is computationally infeasible to construct two different messages with the same digest
C.) It converts a message of arbitrary length into a message digest of a fixed length
D.) Given a digest value, it is computationally infeasible to find the corresponding message

Answer: A

QUESTION 754:

Which of the following would best describe a Concealment cipher?
A.) Permutation is used, meaning that letters are scrambled
B.) Every X number of words within a text, is a part of the real message
C.) Replaces bits, characters, or blocks of characters with different bits, characters, or blocks.
D.) Hiding data in another message so that the very existence of the data is concealed.

Answer: B
Reference: pg 468 Shon Harris: All-in-One CISSP Certification

---

QUESTION 755:

Which of the following ciphers is a subset of the Vignere polyalphabetic cipher?
A.) Caesar
B.) Jefferson
C.) Alberti
D.) SIGABA

Answer: A
"The Caesar Cipher,...., is a simple substitution cipher that involves shifting the alphabet three positions to the right. The Caesar Cipher is a subset of the Vigenere polyalphabetic cipher. In the Caesar cipher, the message's characters and repetitions of the key are added together, modulo 26. In modulo 26, the letters A to Z of the alphabet are given a value of 0 to 25, respectively."
Pg. 189 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 756:

Which of the following is not a property of the Rijndael block cipher algorithm?
A.) Resistance against all known attacks
B.) Design simplicity
C.) 512 bits maximum key size
D.) Code compactness on a wide variety of platforms

Answer: C

QUESTION 757:

What are two types of ciphers?
A.) Transposition and Permutation
B.) Transposition and Shift
C.) Transposition and Substitution
D.) Substitution and Replacement

Answer: C
"Classical Ciphers:
Substitution
Transposition (Permutation)
Vernam (One-Time Pad)
Book or Running Key
Codes
Steganography"
Pg 189-193 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 758:

Which one of the following, if embedded within the ciphertext, will decrease the likelihood

of a message being replayed?

A. Stop bit
B. Checksum
C. Timestamp
D. Digital signature

Answer: C
CBC is the CBC mode of some block cipher, HMAC is a keyed message digest, MD is a plain message digest, and timestamp is to protect against replay attacks. From the OpenSSL project http://www.mail-archive.com/openssl-users@openssl.org/msg23576.html

---

QUESTION 759:

Which of the following statements pertaining to block ciphers is incorrect?
A.) it operates on fixed-size blocks of plaintext
B.) it is more suitable for software than hardware implementation
C.) Plain text is encrypted with a public key and decrypted with a private key
D.) Block ciphers can be operated as a stream

Answer: C
"Strong and efficient block cryptosystems use random key values so an attacker cannot find a pattern as to which S-boxes are chosen and used." Pg. 481 Shon Harris CISSP Certification All-in-One Exam Guide
Not A:
"When a block cipher algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions, on block at a time." Pg. 480 Shon Harris CISSP Certification All-in-One Exam Guide
Not B:
"Block ciphers are easier to implement in software because they work with blocks of data that the software is used to work with." Pg 483 Shon Harris CISSP Certification All-in-One Exam Guide
Not D:
"This encryption continues until the plaintext is exhausted." Pg. 196 Krutz The CISSP Prep Guide.
Not A or D:
"When a block a block cipher algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions, one block at a time." Pg 480 Shon Harris: All-in-One CISSP Certification

---

QUESTION 760:

The repeated use of the algorithm to encipher a message consisting of many blocks is called

A. Cipher feedback
B. Elliptical curve
C. Cipher block chaining
D. Triple DES

Answer: C
"There are two main types of symmetric algorithms: stream and block ciphers. Like their names sound, block ciphers work on blocks of plaintext and ciphertext, whereas stream ciphers work on streams of plaintext and ciphertext, on bit or byte at a time. Pg 521. Shon Harris CISSP All-In-One Certification Exam Guide
Cipher Block Chaining (CBC) operates with plaintext blocks of 64 bits. ....Note that in this mode, errors propogate." Pg 149 Krutz: The CISSP Prep Guide

---

QUESTION 761:

When block chaining cryptography is used, what type of code is calculated and appended to the data to ensure authenticity?

A. Message authentication code.
B. Ciphertext authentication code
C. Cyclic redundancy check
D. Electronic digital signature

Answer: A
The original Answer was B. This is incorrect as cipthertext is the result not an authentication code.
"If meaningful plaintext is not automatically recognizable, a message authentication code (MAC) can be computed and appended to the message. The computation is a function of the entire message and a secret key; it is practically important to find another message with the same authenticator. The receiver checks the authenticity of the message by computing the MAC using the same secret key and then verifying that the computed value is the same as the one transmitted with the message. A MAC can be used to provide authenticity for unencrypted messages as well as for encrypted ones. The National Institute of Standards and Technology (NIST) has adopted a standard for computing a MAC. (It is found in Computer Data Authentication, Federal Information Processing Standards Publication (FIPS PUB) 113.)" http://www.cccure.org/Documents/HISM/637-639.html from the Handbook of Information Security Management by Micki Krause

---

QUESTION 762:

Which of the following statements pertaining to block ciphers is incorrect?
A.) It operates on fixed-size blocks of plaintext
B.) It is more suitable for software than hardware implementations
C.) Plain text is encrypted with a public key and decrypted with a private key
D.) Block ciphers can be operated as a stream

Answer: C
"Strong and efficient block cryptosystems use random key values so an attacker cannot find a pattern as to which S-boxes are chosen and used." Pg. 481 Shon Harris CISSP Certification All-in-One Exam Guide
Not A:
"When a block cipher algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions, on block at a time." Pg. 480 Shon Harris CISSP Certification All-in-One Exam Guide
Not B:
"Block ciphers are easier to implement in software because they work with blocks of data that the software is used to work with." Pg 483 Shon Harris CISSP Certification All-in-One Exam Guide
Not D:
"This encryption continues until the plaintext is exhausted." Pg. 196 Krutz The CISSP Prep Guide.

QUESTION 763:

Which of the following is a symmetric encryption algorithm?
A.) RSA
B.) Elliptic Curve
C.) RC5
D.) El Gamal

Answer: C

QUESTION 764:

How many bits is the effective length of the key of the Data Encryption Standard Algorithm?
A.) 16
B.) 32
C.) 56
D.) 64

Answer: C

QUESTION 765:

Compared to RSA, which of the following is true of elliptic curse cryptography?
A.) It has been mathematically proved to be the more secure
B.) It has been mathematically proved to be less secure
C.) It is believed to require longer keys for equivalent security
D.) It is believed to require shorter keys for equivalent security

Answer: D
CISSP All-In-One - page 491: "In most cases, the longer the key length, the more protection provided, but ECC can provide the same level of protection with a key size that is smaller than what RSA requires."
CISSP Prep Guide (not Gold edition) - page 158: "... smaller key sizes in the elliptic curve implementation can yield higher levels of security. For example, an elliptic curve key of 160 bits is equivalent to 1024-bit RSA key."

QUESTION 766:

Which of the following is not a one-way algorithm?
A.) MD2
B.) RC2
C.) SHA-1
D.) DSA

Answer: B
Not: A, C or D.
"Hash Functions
SHA
MD2
MD4
MD5"
Pg. 337- 340 Tittel: CISSP Study Guide
DSA, Digital Signature Algorithm, is a approved standard for Digital Signatures that utilizes SHA-1 hashing function.
Pg. 342-343 Tittel: CISSP Study Guide

QUESTION 767:

A public key algorithm that does both encryption and digital signature is which of the following?
A.) RSA
B.) DES
C.) IDEA
D.) DSS

Answer: A
"RSA, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a public key algorithm that is the most popular when it comes to asymmetric algorithms. RSA is a worldwide de facto standard and can be used for digital signatures, key exchange, and encryption."
Pg. 489 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 768:

Which of the following encryption algorithms does not deal with discrete logarithms?
A.) El Gamal

B.) Diffie-Hellman
C.) RSA
D.) Elliptic Curve

Answer: C

QUESTION 769:

The RSA algorithm is an example of what type of cryptography?
A.) Asymmetric key
B.) Symmetric key
C.) Secret Key
D.) Private Key

Answer: A

QUESTION 770:

How many rounds are used by DES?
A.) 16
B.) 32
C.) 64
D.) 48

Answer: A
"When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time. A block is made of 64 bits and is divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. The order and type of transposition and substitution function depend on the value of the key that is inputted into the algorithm. The result is the 64-bit block of ciphertext." Pg. 526 Shon Harris: CISSSP All-In-One Certification Guide

---

QUESTION 771:

Which of the following is the most secure form of triple-DES encryption?
A.) DES-EDE3
B.) DES-EDE1
C.) DES-EEE4
D.) DES-EDE2

Answer: A

QUESTION 772:

Which of the following algorithms does *NOT* provide hashing?
A.) SHA-1

B.) MD2
C.) RC4
D.) MD5

Answer: C
"Hashed Algorithms
SHA-1
HMAC-SHA-1
MD5
HMAC-MD5"
Pg 426 Hansche: Official (ISC)2 Guide to the CISSP Exam

QUESTION 773:

Which of the following is unlike the other three?
A.) El Gamal
B.) Teardrop
C.) Buffer Overflow
D.) Smurf

Answer: A

QUESTION 774:

Which of the following is not an encryption algorithm?
A.) Skipjack
B.) SHA-1
C.) Twofish
D.) DEA

Answer: B
SHA-1 is a hash algorithm opposed to encryption algorithm.
Reference: pg 293 Tittel: CISSP Study Guide

QUESTION 775:

Which one of the following is an asymmetric algorithm?

A. Data Encryption Algorithm.
B. Data Encryption Standard
C. Enigma
D. Knapsack

Answer: D
Merkle-Hellman Knapsack is a Public Key Algorithm Pg 206 Krutz: CISSP Prep Guide: Gold Edition.

Not A:
"DES describes the Data Encryption Algorithm (DEA) and is the name of the Federal Information Processing Standard (FIPS) 46-1 that was adopted in 1977..." pg 195 Krutz: CISSP Prep Guide: Gold Edition.
Not B:
"The best-known symmetric key system is probably the Data Encryption Standard (DES)." pg 195 Krutz: CISSP Prep Guide: Gold Edition.
Not C:
"The German military used a polyalphabetic substitution cipher machine called the Enigma as its principal encipherment system during World War II." Pg 185 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 776:

Which of the following is *NOT* a symmetric key algorithm?
A.) Blowfish
B.) Digital Signature Standard (DSS)
C.) Triple DES (3DES)
D.) RC5

Answer: B
Reference: pg 489 Shon Harris

QUESTION 777:

Which of the following layers is not used by the Rijndael algorithm?
A.) Non-linear layer
B.) Transposition layer
C.) Key addition layer
D.) The linear mixing layer

Answer: B
Reference: pg 201 Krutz: CISSP Prep Guide: Gold Edition

QUESTION 778:

What is the basis for the Rivest-Shamir-Adelman (RSA) algorithm scheme?

A. Permutations
B. Work factor
C. Factorability
D. Reversivibility

Answer: C
This algorithm is based on the difficulty of factoring a number, N, which is the product of two large prime numbers. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 204

QUESTION 779:

Which of the following encryption algorithms does not deal with discrete logarithms?
A.) El Gamal
B.) Diffie-Hellman
C.) RSA
D.) Elliptic Curve

Answer: C
Reference: pg 416 Hansche: Official (ISC)2 Guide to the CISSP Exam

QUESTION 780:

The RSA Algorithm uses which mathematical concept as the basis of its encryption?
A.) Geometry
B.) Irrational numbers
C.) PI (3.14159...)
D.) Large prime numbers

Answer: D

QUESTION 781:

PGP provides which of the following?(Choose three)

A. Confidentiality
B. Accountability
C. Accessibility
D. Integrity
E. Interest
F. Non-repudiation
G. Authenticity

Answer: A,D,G
PGP provides confidentiality, integrity, and authenticity.

QUESTION 782:

PGP uses which of the following to encrypt data?
A.) An asymmetric scheme
B.) A symmetric scheme
C.) a symmetric key distribution system
D.) An asymmetric key distribution

Answer: B

QUESTION 783:

Which of the following mail standards relies on a "Web of Trust"?
A.) Secure Multipurpose Internet Mail extensions (S/MIME)
B.) Pretty Good Privacy (PGP)
C.) MIME Object Security Services (MOSS)
D.) Privacy Enhanced Mail (PEM)

Answer: B
"PGP does not use a hierarchy of Cas, or any type of formal trust certificates, but relies on a "web of trust" in its key management approach. Each user generates and distributes his or her public key, and users sign each other's public keys, which creates a community of users who trust each other. This is different than the CA approach where no one trusts each other, they only trust the CA.

QUESTION 784:

Which of the following offers confidentiality to an e-mail message?
A.) The sender encrypting it with it's private key
B.) The sender encrypting it with it's public key
C.) The sender encrypting it with it's receiver's public key
D.) The sender encrypting it with the receiver's private key

Answer: C

QUESTION 785:

Which of the following items should not be retained in an E-mail directory?
A.) drafts of documents
B.) copies of documents
C.) permanent records
D.) temporary documents

Answer: C

QUESTION 786:

In a Secure Electronic Transaction (SET), how many certificates are required for a payment gateway to support multiple acquires?

A. Two certificates for the gateway only.
B. Two certificates for the gateway and two for the acquirers.
C. Two certificates for each acquirer.
D. Two certificates for the gateway and two for each acquirer.

Answer: B
I think it may be D two for each acquirer. Which unless I read it wrong it means each person must have 2 certificates exchanged with the gateway.
"SET uses a des symmetric key system for encryption of the payment information and uses rsa for the symmetric
key exchange and digital signatures. SET covers the end-to-end transaction from the cardholder to the financial institution". -Ronald Krutz The CISSP PREP Guide (gold edition) pg 219-220
In the SET environment, there exists a hierarchy of Certificate Authorities. The SET protocol specifies a method of entity authentication referred to as trust chaining. This method entails the exchange of digital certificates and verification of the public keys by validating the digital signatures of the issuing C
A. This trust chain method continues all the way up to the CA at the top of the hierarchy, which is referred to as the SET Root C
A. The SET Root CAis owned and maintained by SET Secure Electronic Transaction LLC. http://setco.org/certificates.html

---

QUESTION 787:

Which protocol makes use of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?
A.) SSH
B.) S/MIME
C.) SET
D.) SSL

Answer: C

QUESTION 788:

Which of the following best describes the Secure Electronic Transaction (SET) protocol?
A.) Originated by VISA and MasterCard as an Internet credit card protocol
B.) Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures
C.) Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer
D.) Originated by VISA and MasterCard as an Internet credit card protocol using SSL

Answer: B

QUESTION 789:

Which of the following would best define the "Wap Gap" security issue?
A.) The processing capability gap between wireless devices and PC's
B.) The fact that WTLS transmissions have to be decrypted at the carrier's WAP gateway to be re-encrypted with SSL for use over wired networks.

C.) The fact that Wireless communications are far easier to intercept than wired communications
D.) The inability of wireless devices to implement strong encryption

Answer: B

QUESTION 790:

What encryption algorithm is best suited for communication with handheld wireless devices?
A.) ECC
B.) RSA
C.) SHA
D.) RC4

Answer: A
"Eliptic curves are rich mathematical structures that have shown usefulness in many different types of applications. An Elliptic Curve Cryptosystem (ECC) provides much of the same functionality that RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. Some devices have limited processing capacity, storage, power supply, and bandwidth like wireless devices and cellular telephones. With these types of devices, efficiency of resource use is very important. ECC provides encryption functionality requiring a smaller percentage of resources required by RSA and other algorithms, so it is used in these types of devices. In most cases, the longer the key length, the protection provided, but ECC can provide the same level of protection with a key size that is smaller than what RSA requires. Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device." Pg. 491 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 791:

Which security measure BEST provides non-repudiation in electronic mail?

A. Digital signature
B. Double length Key Encrypting Key (KEK)
C. Message authentication
D. Triple Data Encryption Standard (DES)

Answer: A
A tool used to provide the authentication of the sender of a message. It can verify the origin of the message along with the identity of the sender. IT is unique for every transaction and created with a private key. - Shon Harris All-in-one CISSP Certification Guide pg 930
"Secure Multipurpose Internet Mail Extensions (S/MIME) offers authentication and privacy to e-mail through secured attachments. Authentication is provided through X.509 digital certificates. Privacy is provided through the use of Public Key Cryptography Standard (PKCS) Enryption. Two types of messages can be formed using S/MIME: signed messages and enveloped messages. A signed message provides integrity and sender authentication. An

enveloped message provides ntegrity, sender authentication, and confidentiality." Pg 123 Tittle: CISSP Study Guide

---

QUESTION 792:

Which of the following services is not provided by the digital signature standard (DSS)?
A.) Encryption
B.) Integrity
C.) Digital signature
D.) Authentication

Answer: A

QUESTION 793:

Public key cryptography provides integrity verification through the use of public key signature and?

A. Secure hashes
B. Zero knowledge
C. Private key signature
D. Session key

Answer: C
Pg 213 Krutz Gold Edition

QUESTION 794:

Electronic signatures can prevent messages from being:
A.) Erased
B.) Disclosed
C.) Repudiated
D.) Forwarded

Answer: C

QUESTION 795:

Why do vendors publish MD5 hash values when they provide software patches for their customers to download from the Internet?

A. Recipients can verify the software's integrity after downloading.
B. Recipients can confirm the authenticity of the site from which they are downloading the patch.
C. Recipients can request future updates to the software by using the assigned hash value.
D. Recipients need the hash value to successfully activate the new software.

Answer: A
If the two values are different, Maureen knows that the message was altered, either intentionally or unintentionally, and she discards the message...As stated in an earlier section, the goal of using a one-way hash function is to provide a fingerprint of the message. MD5 is the newer version of MD4. IT still produces a 128-bit hash, but the algorithm is a bit more complex to make it harder to break than MD4. The MD5 added a fourth round of operations to be performed during the hash functions and makes several of its mathematical operations carry steps or more complexity to provide a higher level of security . - Shon Harris All-in-one CISSP Certification Guide pg 182-185

QUESTION 796:

What attribute is included in a X.509-certificate?

A.) Distinguished name of subject
B.) Telephone number of the department
C.) secret key of the issuing CA
D.) the key pair of the certificate holder

Answer: A
The key word is 'In create the certificate.." Certificates that conform to X.509 contain the following data: Version of X.509 to which the certificate conforms; Serial number (from the certificate creator);Signature algorithm identifier (specifies the technique used by the certificate authority to digitally sign the contents of the certificate); Issuer name (identification of the certificate authority that issues the certificate) Validity period (specifies the dates and times - a starting date and time and an ending date and time - during which the certificate is valid); Subject's name (contains the distinguished name, or DN, of the entity that owns the public key contained in the certificate); Subject's key (the meat of the certificate - the actual public key of the certificate owner used to setup secure communications) pg 343-344 CISSP Study Guide byTittel

---

QUESTION 797:

What is used to bind a document to it's creation at a particular time?
A.) Network Time Protocol (NTP)
B.) Digital Signature
C.) Digital Timestamp
D.) Certification Authority (CA)

Answer: C

QUESTION 798:

What attribute is included in a X-509-certificate?
A.) Distinguished name of the subject

B.) Telephone number of the department
C.) Secret key of the issuing CA
D.) The key pair of the certificate holder

Answer: A
"Certificates that conform to X.509 contain the following data:
Version of X.509 to which the certificate conforms
Serial number
Signature algorithm identifier
Issuer name
Validity period
Subject's name (contains the distinguished name, or DN of the entity that owns the public key contained in the certificate)
Subjects Public Key"
Pg. 297 Tittel: CISSP Study Guide

QUESTION 799:

Which of the following standards concerns digital certificates?
A.) X.400
B.) X.25
C.) X.509
D.) X.75

Answer: C

QUESTION 800:

What level of assurance for a digital certificate only requires an e-mail address?
A.) Level 0
B.) Level 1
C.) Level 2
D.) Level 3

Answer: B

QUESTION 801:

The "revocation request grace period" is defined as:
A.) The period for to the user within he must make a revocation request upon a revocation reason
B.) Minimum response time for performing a revocation by the CA
C.) Maximum response time for performing a revocation by the CA
D.) Time period between the arrival of a revocation reason and the publication of the revocation information

Answer: C

QUESTION 802:

What enables users to validate each other's certificate when they are certified under different certification hierarchies?
A.) Cross-certification
B.) Multiple certificates
C.) Redundant certificate authorities
D.) Root certification authorities

Answer: A

QUESTION 803:

Digital signature users register their public keys with a certification authority, which distributes a certificate containing the user's public key and digital signature of the certification authority. In creating the certificate, the user's public key and the validity period are combined with what other information before computing the digital signature?

A. Certificate issuer and the Digital Signature Algorithm identifier
B. User's private key and the identifier of the master key code
C. Name of secure channel and the identifier of the protocol type
D. Key authorization and identifier of key distribution center

Answer: A
The key word is 'In create the certificate.." Certificates Certificates that conform to X.509 contain the following data: Version of X.509 to which the certificate conforms; Serial number (from the certificate cerator); Signature algorithm identifier (specifies the technique used by the certified authority to digitally sign the contents of the certificate); Issuer name (identification of the certificate authority that issues the certificate) Validity period (specifies the dates and times - a starting date and time and an ending date and time - during which the certificate is validated); Subject's name (contains the distinguished name, or DN, of the entity that owns the public key contained in teh certificate); Subject's public key (the meat of the certificate - the actual public key of the certificate owner used to setup secure communications) pg 343-344 CISSP Study Guide byTittel

QUESTION 804:

What level of assurance for digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?
A.) Level 1
B.) Level 2
C.) Level 3
D.) Level 4

Answer: B

QUESTION 805:

Which one of the following security technologies provides safeguards for authentication before securely sending information to a web server?

A. Secure/Multipurpose Internet Mail Extension (S/MIME)
B. Common Gateway Interface (CGI) scripts
C. Applets
D. Certificates

Answer: D
Digital certificates provide communicating parties with the assurance that they are communicating with people who truly are who they claim to be." Titel: CISSP Study Guide. pg 343. In this case, if the web server was a bank, you want to have a certificate confirming that they really are the bank before you authenticate with your username and password.

QUESTION 806:

The primary role of cross certification is:
A.) Creating trust between different PKIs
B.) Build an overall PKI hierarchy
C.) set up direct trust to a second root CA
D.) Prevent the nullification of user certifications by CA certificate revocation

Answer: A

QUESTION 807:

Windows 98 includes the ability to check the digitally signed hardware drivers. Which of the following are true?

A.) Drivers are the only files supplied with W98 that can checked for digital signatures and all drivers included with W98 have been digitally signed
B.) If a file on a windows W98 has been digitally signed it means that the file has passed quality testing by Microsoft.
C.) The level to which signature checking is implemented could only be changed by editing the registry
D.) All of the statements are true

Answer: B
Windows device drivers and operating system files have been digitally signed by Microsoft to ensure their quality. A Microsoft digital signature is your assurance that a particular file has met a certain level of testing, and that the file has not been altered or overwritten by another program's installation process.
Depending on how your administrator has configured your computer, Windows either ignores

device drivers that are not digitally signed, displays a warning when it detects device drivers that are not digitally signed (the default behavior), or prevents you from installing device drivers without digital signatures.
Windows includes the following features to ensure that your device drivers and system files remain in their original, digitally-signed state:
Window Files Protection
System File Checker
File Signature Verification
Windows XP help.
Not A: operating system files are included.
Not C: the setting can be changed in the GUI.

QUESTION 808:

What is the purpose of certification path validation?

A. Checks the legitimacy of the certificates in the certification path.
B. Checks that all certificates in the certification path refer to same certification practice statement.
C. Checks that no revoked certificates exist outside the certification path.
D. Checks that the names in the certification path are the same.

Answer: A
Not C. Revoked certificates are not checked outside the certification path.
"A Transaction with Digital Certificates
1.) Subscribing entity sends Digital Certificate Application to Certificate Authority.
2.) Certificate Authority issues Signed Digital Certificate to Subscribing Entity.
3.) Certificate Authority sends Certificate Transaction to Repository.
4.) Subscribing Entity Signs and sends to Party Transacting with Subscriber.
5.) Party Transacting with Subscriber queries Repository to verify Subscribers Public Key.
6.) Repository responds to Party Transacting with Subscriber the verification request."
Pg. 214 Krutz: The CISSP Prep Guide: Gold Edition.
"John needs to obtain a digital certificate for himself so that he can participate in a PKI, so he makes a request to the R
A. The RA requests certain identification from John, like a copy of his driver's licens, his phone number, address, and other identification information. Once the RA receives the required informoration from John and verifies it, the RA sends his certificate request to the C
A. The CA creates a certificate with John's public key and identify information embedded. (The private/public key pair is either generated by the CA or on John's machine, which depends on the systems' configurations. If it is created at the CA, his private key needs to be sent to him by secure means. In most cases the user generates this pair and sends in his public key during the registration process.) Now John is registered and can participate in PKI. John decides he wants to communicate with Diane, so he requests Diane's public key from a public directory. The directory, sometimes called a repository, sends Diane's public key, and John uses this to encrypt a session key that will be used to encrypt their messages. John sends the encrypted session key to Diane. Jon then sends his certificate, containing his public key, to

Diane. When Diane receives John's certificate, her browser looks to see if it trusts the CA that digitally signed this certificate. Diane's browser trusts this CA, and she makes a reques to the CA to see if this certificate is still valid. The CA responds that the certificate is valid, so Diane decrypts the session key with her private key. Now they can both communicate using encryption." Pg 499 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 809:

In what type of attack does an attacker try, from several encrypted messages, to figure out the key using the encryption process?
A.) Known-plaintext attack
B.) Ciphertext-only attack
C.) Chosen-Ciphertext attack
D.) Known Ciphertext attack

Answer: B
"Ciphertext-Only Attack
In this type of attack, the attacker has the ciphertext of several messages. Each of the messages has been encrypted using the same encryption algorithm. The attacker's goal is to discover the key that was used in the encryption process. Once the attacker figures out the key, she can decrypt all other messages encrypted with the same key.
A ciphertext-only attack is the most common because it is very easy to get ciphertext by sniffing someone's traffic, but it is the hardest attack to actually be successful at because the attacker has so little information about the encryption process." Pg 531 Shon Harris CISSP All-In-One Exam Guide

---

QUESTION 810:

When combined with unique session values, message authentication can protect against which of the following?

A. Reverse engineering, frequency analysis, factoring attacks, and ciphertext-only attack.
B. Masquerading, frequency analysis, sequence manipulation, and ciphertext-only attack.
C. Reverse engineering, content modification, factoring attacks, and submission notification.
D. Masquerading, content modification, sequence manipulation, and submission notification.

Answer: C
Unique session values: "IPSec: ....Each device will have one security association (SA) for each session that it uses. The SA is critical to the IPSec architecture and is a record of the configuration the device needs to support an IPSec connection. Pg 575 Shon Harris All-In-One CISSP Certification Exam Guide.
Message authentication and content modification: "Hashed Message Authentication Code (HMAC): An HMAC is a hashed alogrithim that uses a key to generate a Message Authentication Code (MAC). A MAC is a type of check sum that is a function of the information in the message. The MAC is generated before the message is sent, appended to the message, and then both are transmitted. At the receiving end, a MAC is generated from the message alone

using the same algorithm as used by the sender and this MAC is compared to the MAC sent with the message. If they are not identical, the message was modified en route. Hashing algorithms can be used to generate the MAC and hash algorithms using keys provide stronger protection than ordinary MAC generation.
Frequency analysis: Message authentication and session values do not protect against Frequency Analysis so A and B are eliminated.
"Simple substitution and transposition ciphers are vulnerable to attacks that perform frequency analysis. In every language, there are words and patters that are used more often than others. For instance, in the English language, the words "the.' "and," "that," and "is" are very frequent patters of letters used in messages and conversation. The beginning of messages usually starts "Hello" or "Dear" and ends with "Sincerely" or "Goodbye." These patterns help attackers figure out the transformation between plaintext to ciphertext, which enables them to figure out the key that was used to perform the transformation. It is important for cryptosystems to no reveal these patterns." Pg. 507 Shon Harris All-In-One CISSP Certification Exam Guide
Ciphertext-Only Attack: Message authentication and session values do not protect against Ciphertext so A and B are again eliminated.
"Ciphertext-Only Attack: In this type of an attack, an attacker has the ciphertext of several messages. Each of the messages has been encrypted using the same encryption algorithm. The attacker's goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. Once the attacker figures out the key, she can now decrypt all other messages encrypted with the same key." Pg 577 Shon Harris All-In-One CISSP Certification Exam Guide.
Birthday attack: "....refer to an attack against the hash function known as the birthday attack." Pg 162 Krutz: The CISSP Prep Guide. MAC utilizes a hashing function and is therefore susceptible to birthday attack.
Masguerading Attacks: Session values (IPSec) does protect against session hijacking but not spoofing so C is eliminated.
"Masguerading Attacks: ....we'll look at two common masquerading attacks - IP Spoofing and session hijacking." Pg 275 Tittel: CISSP Study Guide.
Session hijacking: "If session hijacking is a concern on a network, the administrator can implement a protocol that requires mutual authentication between users like IPSec. Because the attacker will not have the necessary credentials to authenticate to a user, she cannot act as an imposter and hijack sessions." Pg 834 Shon Harris All-In-One CISSP Certification Exam Guide
Reverse engineering: Message authentication protects against reverse engineering.
Reverse engineering: "The hash function is considered one-way because the original file cannot be created from the message digest." Pg. 160 Krutz: The CISSP Prep Guide
Content modification: Message authentication protects against content modification.
Factoring attacks: Message authentication protects against factoring attacks.

QUESTION 811:

The relative security of a commercial cryptographic system can be measured by the?

A. Rating value assigned by the government agencies that use the system.
B. Minimum number of cryptographic iterations required by the system.
C. Size of the key space and the available computational power.

D. Key change methodology used by the cryptographic system.

Answer: C
The strength of the encryption method comes from the algorithm, secrecy of the key, length of the key, initialization vectors, and how they all work together. - Shon Harris All-in-one CISSP Certification Guide pg 504

QUESTION 812:

Which one of the following describes Kerchoff's Assumption for cryptoanalytic attack?

A. Key is secret; algorithm is Known
B. Key is known; algorithm is Known
C. Key is secret; algorithm is secret
D. Key is known; algorithm is secret

Answer: A
Kerhkoff's laws were intended to formalize the real situation of ciphers in the field. Basically, the more we use any particular cipher system, the more likely it is that it will "escape" into enemy hands. So we start out assuming that our opponents know "all the details" of the cipher system, except the key. http://www.ciphersbyritter.com/NEWS4/LIMCRYPT.HTM

QUESTION 813:

Which of the following actions can make a cryptographic key more resistant to an exhaustive attack?

A. None of the choices.
B. Increase the length of a key.
C. Increase the age of a key.
D. Increase the history of a key.

Answer: B

Explanation:
Defenses against exhaustive attacks involve increasing the cost of the attack by increasing the number of possibilities to be exhausted. For example, increasing the length of a password will increase the cost of an exhaustive attack. Increasing the effective length of a cryptographic key variable will make it more resistant to an exhaustive attack.

QUESTION 814:

Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A.) Differential cryptanalysis
B.) Differential linear cryptanalysis
C.) Birthday attack
D.) Statistical attack

Answer: C
Attacks Against One-Way Hash Functions: A good hashing algorithm should not produce the same hash value for two different messages. If the algorithm does produce the same value for two distinctly different messages, this is referred to as a collision. If an attacker finds an instance of a collision, he has more information to use when trying to break the cryptographic methods used. A complex way of attacking a one-way hash function is called the birthday attack. Now hold on to your had while we go through this -- it is a bit tricky. In standard statistics, a birthday paradox exists. It goes something like this:
How many people must be in the same room for the chance to be greater than even that another person has the same birthday as you?

Answer: 253
How many people must be in the same room for the chance to be greater than even that at least two people share the same birthday?

Answer: 23
This seems a bit backwards, but the difference is that in the first instance, you are looking for someone with a specific birthday date, which matches yours. In the second instance, you are looking for any two people who share the same birthday. There is a higher probability of finding two people who share a birthday than you finding another person sharing your birthday -- thus, the birthday paradox.
....This means that if an attacker has one hash value and wants to find a message that hashes to the same hash value, this process could take him years. However, if he just wants to find any two messages with the same hashing value, it could take him only a couple hours. .....The main point of this paradox and this section is to show how important longer hashing values truly are. A hashing algorithm that has a larger bit output is stronger and less vulnerable to brute force attacks like a birthday attack.
Pg 554-555 Shon Harris: All-In-One Certification Exam Guide

QUESTION 815:

Frame-relay uses a public switched network to provide:
A.) Local Area Network (LAN) connectivity
B.) Metropolitan Area Network (MAN) connectivity
C.) Wide Area Network (WAN) connectivity
D.) World Area Network (WAN) connectivity

Answer: C

QUESTION 816:

Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?
A.) ISDN
B.) SLIP
C.) xDSL
D.) T1

Answer: B

QUESTION 817:

Which of the following provide network redundancy in a local network environment?
A.) Mirroring
B.) Shadowing
C.) Dual backbones
D.) Duplexing

Answer: C

QUESTION 818:

Which of the following is a Wide Area Network that was originally funded by the Department of Defense, which uses TCP/IP for data interchange?
A.) the Internet
B.) the Intranet
C.) the Extranet
D.) The Ethernet

Answer: A

QUESTION 819:

Internet specifically refers to the global network of:
A.) public networks and Internet Service Providers (ISPs) throughout the world
B.) private networks and Internet Services Providers (ISPs) through the world
C.) limited networks and Internet Service Providers (ISPs) throughout the world
D.) point networks and Internet Service Providers (ISPs) throughout the world

Answer: A

QUESTION 820:

To improve the integrity of asynchronous communications in the realm of personal computers, the Microcom Networking Protocol (MNP) uses a highly effective communications error-control technique known as

A. Cyclic redundancy check.
B. Vertical redundancy check.
C. Checksum.
D. Echoplex.

Answer: D

QUESTION 821:

Organizations should consider which of the following first before connecting their LANs to the Internet?
A.) plan for implementing W/S locking mechanisms
B.) plan for protecting the modem pool
C.) plan for providing the user with his account usage information
D.) plan for considering all authentication options

Answer: D

QUESTION 822:

Which xDSL flavour delivers both downstream and upstream speeds of 1.544 MBps over two copper twisted pairs?
A.) HDSL
B.) SDSL
C.) ADSL
D.) VDSL

Answer: A

QUESTION 823:

Which of the following statements pertaining to Asynchronous Transfer Mode (ATM) is false?
A.) It can be used for voice
B.) It can be used for data
C.) It carries various sizes of packets
D.) It can be used for video

Answer: C
"Asynchronous transfer mode (ATM) is a cell-switching technology, as opposed to a packet-switching technology like Frame Relay. ATM uses virtual circuits much like Frame Relay, but because it uses fixed-size frames or cells, it can guarantee throughput. This makes ATM an excellent WAN technology for voice and video conferencing." Pg 87 Tittel: CISSP Study Guide

---

QUESTION 824:

Satellite communications are easily intercepted because__

A. transmissions are continuous 24 hours per day.
B. a satellite footprint is narrowly focused.
C. a satellite footprint is very large.
D. a satellite footprint does not change.

Answer: C
I think it may have to do with the footprint of the satellite.
Footprint - The area of Earth with sufficient antenna gain to receive a signal from a satellite. - http://www.aero.org/publications/crosslink/winter2002/backpage.html
Not A: Granted Satellites transmit but they may not do it 24x7 as it could be only when traffic is sent.

QUESTION 825:

Which one of the following protocols CANNOT be used for full duplex Wide Area Network (WAN) communications?

A. Synchronous Data Link Control (SDLC)
B. Serial Line Internet Protocol (SLIP)
C. Point-to-Point Protocol (PPP)
D. High-Level Data Link Control (HDLC)

Answer: A
"SDLC was developed to enable mainframes to communicate with remote locations." Pg 456 Shon Harris CISSP Certification Exam Guide. This is a WAN protocol.
Not B
"Serial Line Internet Protocol (SLIP) is an older technology developed to support TCP/IP communications over asynchronous serial connections, such as serial cables or modem dial-up." Pg 96. Tittel: CISSP Study Guide. SLIP is serial protocol opposed to WAN protocol. This could be correct answer but SDLC is more correct.
Not C.
"PPP is a full-duplex protocol that provides bi-directional links over synchronous, asynchronous, ISDN, frame relay and SONET connections." Pg. 472 Shon Harris CISSP All-In-One Certification Exam Guide. PPP is full-duplex.
Not D.
"HDLC is an extension of SDLC, which is mainly used in SNA environments. HDLC provides high throughput because it supports full-duplex transmissions and is used in point-to-point and multipoint connections." Pg 456 Shon Harris CISSP All-In-One Certification Exam Guide. PPP is full-duplex.

QUESTION 826:

Fast ethernet operates at which of the following?
A.) 10 MBps
B.) 100 MBps
C.) 1000 MBps
D.) All of the above

Answer: B
"Fast Ethernet 100bps - IEE 802.3u" pg 810 Shon Harris CISSP All-In-One Exam Guide

---

QUESTION 827:

Which of the following statements about the "Intranet" is NOT true?
A.) It is an add-on to a local area network.
B.) It is unrestricted and publicly available.
C.) It is usually restricted to a community of users
D.) t can work with MANS or WANS

Answer: B

Explanation:
"An intranet is a 'private' network that uses Internet technologies, such as TCP/IP. The company has Web servers and client machines using Web browsers, and it uses the TCP/IP protocol suite. The Web pages are written in Hypertext Markup Language (HTML) or Extensible Markup Language (XML) and are accessed via HTTP." Pg 395 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 828:

Frame relay and X.25 networks are part of which of the following?
A.) Circuit-switched services
B.) Cell-switched services
C.) Packet-switched services
D.) Dedicated digital services

Answer: C
Packet-Switched Technologies:
X.25
Link Access Procedure-Balanced (LAPB)
Frame Relay
Switched Multimegabit Data Service (SMDS)
Asynchronous Transfer Mode (ATM)
Voice over IP (VoIP)

QUESTION 829:

A Wide Area Network (WAN) may be privately operated for a specific user community,

may support multiple communication protocols, or may provide network connectivity and services via:
A.) interconnected network segments (extranets, intranets, and Virtual Private Networks)
B.) interconnected network segments (extranets, internets, and Virtual Private Networks)
C.) interconnected netBIOS segments (extranets, intranets, and Virtual Private Networks)
D.) interconnected NetBIOS segments (extranets, interest, and Virtual Private Networks)

Answer: A

QUESTION 830:

What is the proper term to refer to a single unit of Ethernet data?
A.) Ethernet segment
B.) Ethernet datagram
C.) Ethernet frame
D.) Ethernet packet

Answer: C
When the Ethernet software receives a datagram from the Internet layer, it performs the following steps: 1.) Breaks IP layer data into smaller chunks if necessary which will be in the data field of ethernet frames. Pg. 40 Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 831:

Which of the following is a LAN transmission protocol?
A.) Ethernet
B.) Ring Topology
C.) Unicast
D.) Polling

Answer: C
Reference: "LAN Transmission Methods. LAN data is transmitted from the sender to one or more receiving stations using either a unicast, multicast, or broadcast transmission." pg 528 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 832:

Which of the following access methods is used by Ethernet?
A.) CSMA/CD
B.) CSU/DSU
C.) TCP/IP
D.) FIFO

Answer: A
"Under the Ethernet CSMA/CD media-access process, any computer on a CSMA/CD LAN can access the network at any time." Pg. 103 Krutz: The CISSP Prep Guide.

QUESTION 833:

Which one of the following data transmission technologies is NOT packet-switch based?

A. X.25
B. ATM (Asynchronous Transfer Mode)
C. CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
D. Frame Relay

Answer: C
"Examples of packet-switching networks are X.25, Link Access Procedure-Balanced (LAPB), Frame Relay, Switched Multimegabit Data Systems (SMDS), Asynchronous Transfer Mode (ATM), and Voice over IP (VoIP)." Pg 146 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 834:

Unshielded (UTP) does not require the fixed spacing between connections that is:
A.) necessary with telephone-type connections
B.) necessary with coaxial-type connections
C.) necessary with twisted pair-type connections
D.) necessary with fiber optic-type connections

Answer: B

QUESTION 835:

What type of cable is used with 100Base-TX Fast Ethernet?
A.) Fiber-optic cable
B.) Four pairs of Category 3, 4, or 5 unshielded twisted-pair (UTP) wires.
C.) Two pairs of Category 5 unshielded twisted-pair (UTP) or Category 1 shielded twisted-pair (STP) wires
D.) RG-58 Cable

Answer: C

QUESTION 836:

Which cable technology refers to the CAT 3 and Cat5 Categories?
A.) Coaxial cables
B.) Fiber Optic cables
C.) Axial cables
D.) Twisted Pair cables

Answer: D

QUESTION 837:

On which Open System Interconnection (OSI) Reference Model layer are repeaters used as communications transfer devices?

A. Data-link
B. Physical
C. Network
D. Transport

Answer: B
This original answer is wrong (network) repeater is physical layer. Repeaters just regenerates the signal
"Hubs are multi port repeaters, and as such they obey the same rules as repeaters (See previous section OSI Operating Layer). They operate at the OSI Model Physical Layer."
http://www.thelinuxreview.com/howto/intro_to_networking/c5434.htm

---

QUESTION 838:

In the OSI/ISO model, at what layer are some of the SLIP, CSLIP, PPP, control functions are provided?
A.) Link
B.) Transport
C.) Presentation
D.) Application

Answer: A

QUESTION 839:

In the OSI/ISO model, at what level are TCP and UDP provided?
A.) Transport
B.) Network
C.) Presentation
D.) Application

Answer: A
Transport Layer. .... TCP and UDP operate on this layer.' Pg 82. Krutz: The CISSP Prep Guide.

QUESTION 840:

DNS, FTP, TFTP, SNMP are provided at what level of the OSI/ISO model?
A.) Application
B.) Network
C.) Presentation
D.) Transport

Answer: A

QUESTION 841:

Which of the following OSI layers does not provide confidentiality?
A.) Presentation
B.) Network
C.) Transport
D.) Session

Answer: C
Reference: "[Network Layer] The routing protocols are located at this layer and include the following: .....Internet Protocol Security (IPSec)". "The following protocols operate within the Session layer: Secure Sockets Layer (SSL)". "The Presentation layer is also responsible for encryption and compression." Pg 61-62 Tittel: CISSP Study Guide

---

QUESTION 842:

Which of the following OSI layers provides routing and related services?
A.) Network
B.) Presentation
C.) Session
C.) Physical

Answer: A

QUESTION 843:

The International Standards Organization/Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?
A.) Standard model for network communications
B.) Used to gain information from network devices such as count of packets received and routing tables
C.) Allows dissimilar networks to communicate
D.) Defines 7 protocol layers (a.k.a. protocol stacks)

Answer: B
Not A.
"The Open System Interconnect (OSI) is a worldwide federation that works to provide international standards. "
Not C.
"A protocol is a standard set of rules that determine how systems will communicate across networks. Two different systems can communicate and understand each other because they use the same protocols in spite of their differences."
Pg. 343-344 Shon Harris: CISSP All-In-One Certification Exam Guide

---

QUESTION 844:

Which of the following layers supervises the control rate of packet transfers in an Open Systems Interconnections (OSI) implementation?

A. Physical
B. Session
C. Transport
D. Network

Answer: C
The transport layer defines how to address the physical locations and /or devices on the network, how to make connections between nodes, and how to handle the networking of messages. It is responsible for maintaining the end-to-end integrity and control of the session. Services located in the transport layer both segment and reassemble
the data from upper-layer applications and unite it onto the same data stream, which provides end-to-end data transport services and establishes a logical connection between the sending host and destination host on a network.
The transport layer is also responsible for providing mechanisms for multiplexing upper-layer applications, session
establishment, and the teardown of virtual circuits. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 275-276
"Transport Layer The agreement on these issues before transferring data helps provide more reliable data transfer, error detection and correction, and flow control and it optimizes network services needed to perform these tasks." Pg. 318 - 319 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 845:

Which Open Systems Interconnect (OSI) layers provide Transport Control Protocol/Internet Protocol (TCP/IP) end-to-end security?

A. Application and presentation
B. Presentation and session
C. Network and application
D. Application and transport

Answer: B
"The Session layer (layer 5) is responsible for establishing, maintaining, and terminating communication sessions between two computers. The primary technology within layer 5 is a gateway. The following protocols operate within the Session layer:
Secure Sockets Layer (SSL)
Network File System (NFS)
Structured Query Language (SQL)
Remote Procedure Call (RPC)

The presentation layer (layer 6) is responsible for transforming data received from the application layer into a format that any system following the OSI model can understand. It imposes common or standardized structure and formatting rules onto the data. The Presentation layer is also responsible for encryption and compression." Pg. 79-80 Tittel: CISSP Study Guide.

QUESTION 846:

Which one of the following is a TRUE statement about the bottom three layers of the Open Systems Interconnection (OSI) Reference Model?

A. They generally pertain to the characteristics of the communicating end systems.
B. They cover synchronization and error control of network data transmissions.
C. They support and manage file transfer and distribute process resources.
D. They support components necessary to transmit network messages.

Answer: D
By exclusion:
Not A.
"The Session layer (layer 5) is responsible for establish, maintaining, and terminating communication sessions between two computers." Pg 79 Tittel: CISSP Study Guide.
Not B.
"The Transport layer (layer 4) ....This layer includes mechanisms for segmentation, sequencing, error checking, controlling the flow of data, error correction and network service optimization." Pg 79 Tittel: CISSP Study Guide.
Not C.
"The Application itself it is not located within this layer [Application]; rather the protocols and services required to transmit files, exchange messages, connect to remote terminals, and so on are here." Pg. 80 Tittel: CISSP Study Guide.

QUESTION 847:

ICMP and IGMP belong to which layer of the OSI model?
A.) Datagram
B.) Network
C.) Transport
D.) Link

Answer: B
The Network layer (layer 3) is responsible for adding routing information to the data. The Network layer accepts the segment from the Transport layer and adds information to it to create a packet. The packet includes the source and destination IP addresses. T
The routing protocols are located at this layer and include the following:
Internet Control Message Protocol (ICMP)
Routing Information Protocol (RIP)
Open Shortest Path First (OSPF)
Border Gateway Protocol (BGP)

Internet Group Management Protocol (IGMP)
Internet Protocol (IP)
Internet Packet Exchange (IPX)
Pg. 78 Tittel: CISSP Study Guide

QUESTION 848:

The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers 6 is which of the following?
A.) Application Layer
B.) Presentation Layer
C.) Data Link Layer
D.) Network Layer

Answer: B
"Presentation Layer (Layer 6)." Pg 81 Krutz The CISSP Prep Guide.

QUESTION 849:

Which OSI/ISO layer is IP implemented at?
A.) Session layer
B.) Transport layer
C.) Network layer
D.) Data link layer

Answer: C

QUESTION 850:

Which of the following security-focused protocols operates at a layer different from the others?
A.) Secure HTTP
B.) Secure shell (SSH-2)
C.) Secure socket layer (SSL)
D.) Simple Key Management for Internet Protocols (SKIP)

Answer: A

QUESTION 851:

In the OSI/ISO model, at what layer are some of the SLIP, CSLIP, PPP control functions are provided?
A.) Link
B.) Transport
C.) Presentation
D.) Application

Answer: A

QUESTION 852:

ICMP and IGMP belong to which layer of the OSI Model? (Fill in the blank)

Answer: Network

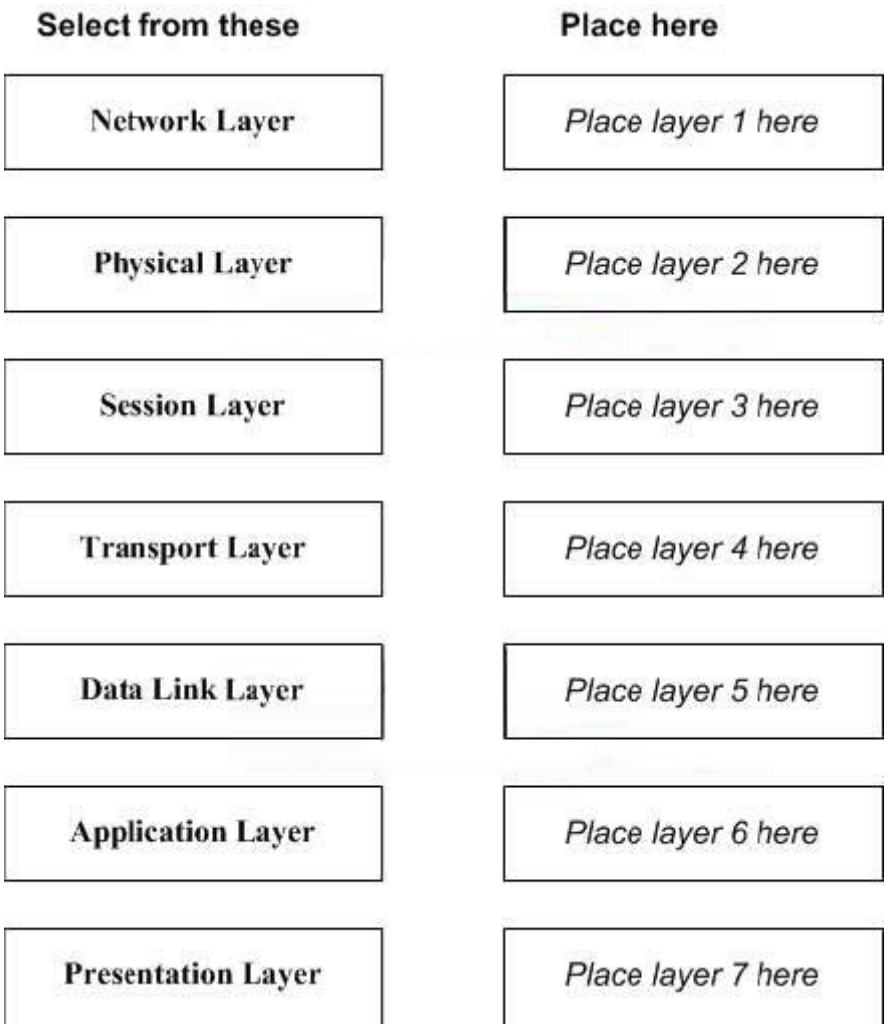
QUESTION 853:

The International Standards Organization / Open Systems Interconnection (ISO/OSI)
Layers 6 is which of the following? (Fill in the blank)

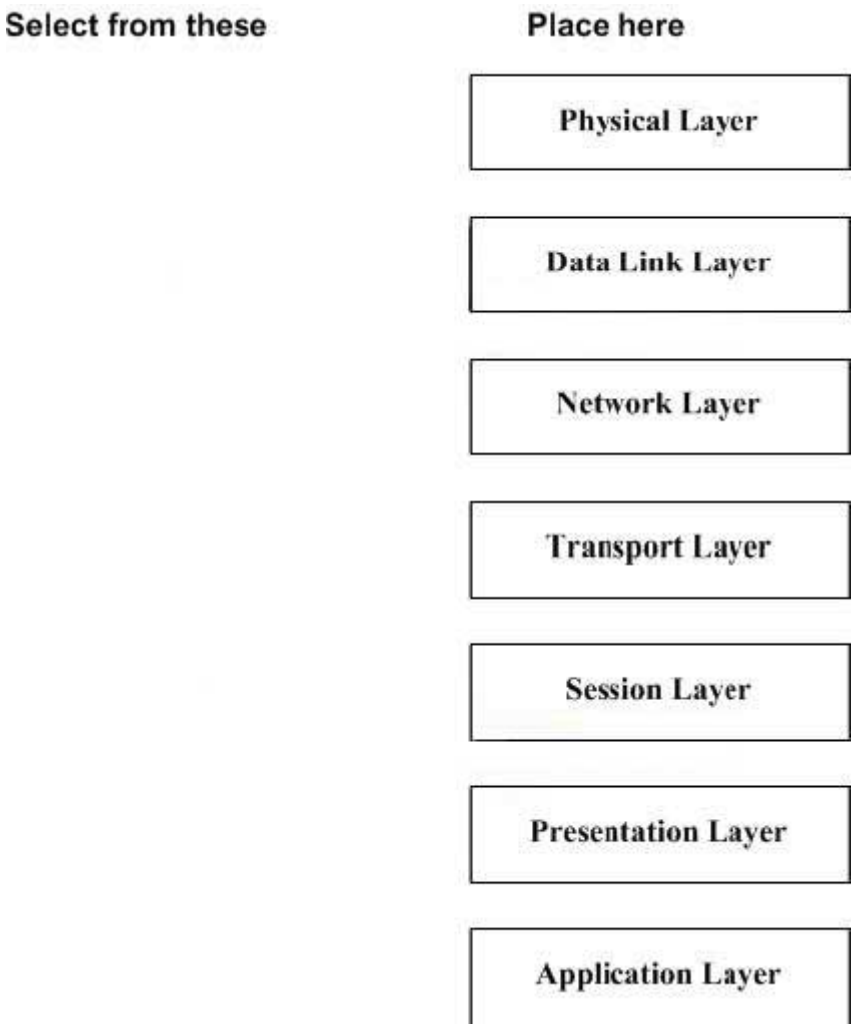
Answer: Presentation

QUESTION 854:

The International Standards Organization / Open Systems Interconnection (ISO/OSI)
Layers are in which of the following order (1 to 7). (Fill in the blank)


Select from these
Place here
Network Layer
Physical Layer
Session Layer
Transport Layer
Data Link Layer
Application Layer
Presentation Layer
Place layer 1 here
Place layer 2 here
Place layer 3 here
Place layer 4 here
Place layer 5 here
Place layer 6 here
Place layer 7 here

Answer:



Explanation:
Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer

---

QUESTION 855:

Which of the following OSI layers provides non-repudiation services? (Fill in the blank)

Answer: Application

QUESTION 856:

The OSI model contains seven layers. TCP/IP is generally accepted as having how many layers?
A.) four
B.) five
C.) six
D.) eight

Answer: A
The TCP/IP Protocol Model is similar to the OSI model, but it defines only the following four layers instead of seven: Application Layer, Host-to-Host Transport Layer, Internet Layer, Network Access or Link Layer.
Pg. 84 Krutz: The CISSP Prep Guide.

QUESTION 857:

Which of the following layers provides end-to-end service?
A.) Network Layer
B.) Link Layer
C.) Transport Layer
D.) Presentation Layer

Answer: C
Session services located in the Transport Layer both segment and reassemble the data from upper-layer applications and unite it onto the same data stream, which provides end-to-end data transport services and establishes a logical connection between the sending host and destination host on a network.
Pg. 82 Krutz: The CISSP Prep Guide.

QUESTION 858:

Both TCP and UDP use port numbers of what length?
A.) 32 bits
B.) 16 bits
C.) 8 bits
D.) 4 bits

Answer: B

QUESTION 859:

Which one of the following is an effective communications error-control technique usually implemented in software?

A. Redundancy check
B. Packet filtering
C. Packet checksum
D. Bit stuffing

Answer: C

QUESTION 860:

What is the proper term to refer to a single unit of IP data? (Fill in the blank)

Answer: Datagram
"When the Ethernet software receives a datagram from the Internet layer, it performs the following steps: 1.) Breaks IP layer data into smaller chunks if necessary which will be in the data field of ethernet frames." Pg. 40 Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 861:

What is the proper term to refer to a single unit of TCP data at the transport layer?
A.) TCP segment
B.) TCP datagram
C.) TCP frame
D.) TCP packet

Answer: A
The data package created at the transport layer, which encapsulates the Application layer message is called a segment if it comes from TCP/IP." Pg. 27 Pg. 55 Casad: Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 862:

Each data packet is assigned the IP address of the sender and the IP address of the:
A.) recipient
B.) host
C.) node
D.) network

Answer: A

QUESTION 863:

Both TCP and UDP use port numbers of what length?
A.) 32 bits
B.) 16 bits
C.) 8 bits
D.) 4 bits

Answer: B
2 to 16th power = 65,536
"TCP and UDP each have 65,536 ports". Pg 75 Tittel: CISSP Study Guide

---

QUESTION 864:

Which of the following type of packets can *easily* be denied with a stateful packet filter?
A.) ICMP

B.) TCP
C.) UDP
D.) IP

Answer: B

QUESTION 865:

Which ports are the "Register ports", registered by the IANA?
A.) Ports 128 to 255
B.) Ports 1024 to 49151
C.) Ports 1023 to 65535
D.) Ports 1024 to 32767

Answer: B
"The User (Registered) Ports are those from 1024 through 49151."
http://www.iana.org/numbers.htm#P

QUESTION 866:

What protocol was UDP based and mainly intended to provide validation of dial up user login passwords?

A. PPTP
B. L2TP
C. IPSec
D. TACACS

Answer: D

Explanation:
The original TACACS protocol was developed by BBN for MILNET. It was UDP based and mainly intended to provide validation of dial up user login passwords. The TACACS protocol was formally specified, but the spec is not generally available.

QUESTION 867:

On which port is POP3 usually run?
A.) 110
B.) 109
C.) 139
D.) 119

Answer: A

QUESTION 868:

The primary function of this protocol is to send messages between network devices regarding the health of the network:
A.) Internet Control Message Protocol (ICMP)
B.) Reverse Address Resolution Protocol (RARP)
C.) Address Resolution Protocol (AR)
D.) Internet Protocol (IP)

Answer: A

QUESTION 869:

Telnet and rlogin use which protocol?
A.) UDP
B.) SNMP
C.) TCP
D.) IGP

Answer: C

QUESTION 870:

The IP header contains a protocol field. If this file contains the value of 2, what type of data is contained within the IP datagram?
A.) TCP
B.) ICMP
C.) UDP
D.) IGMP

Answer: D

QUESTION 871:

The IP header contains a protocol field. If this field contains the value of 17, what type of data is contained within the ip datagram?
A.) TCP
B.) ICMP
C.) UDP
D.) IGMP

Answer: C
ICMP = 1
TCP = 6
UDP = 17
Pg. 55 Casad: Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 872:

Why do some sites choose not to implement Trivial File Transfer Protocol (TFTP)?
A.) list restrictions
B.) inherent security risks
C.) user authentication requirement
D.) directory restriction

Answer: B

QUESTION 873:

The IP header contains a protocol field. If this field contains the value of 6, what type of data is contained within the ip datagram?
A.) TCP
B.) ICMP
C.) UDP
D.) IGMP

Answer: A
ICMP = 1
TCP = 6
UDP = 17
Pg. 55 Casad: Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 874:

Which of the following is not a basic security service defined by the OSI?
A.) Routing control
B.) Authentication
C.) Data Confidentiality
D.) Logging and monitoring

Answer: A

QUESTION 875:

Which of the following is not an OSI architecture-defined broad category of security standards?
A.) Security techniques standards
B.) Layer security protocol standards
C.) Application-specific security
D.) Firewall security standards

Answer: D

QUESTION 876:

Which one of the following is the Open Systems Interconnection (OSI) protocol for message handling?

A. X.25
B. X.400
C. X.500
D. X.509

Answer: B
An ISO and ITU standard for addressing and transporting e-mail messages. It conforms to layer 7 of the OSI model and supports several types of transport mechanisms, including Ethernet, X.25, TCP/IP, and dial-up lines. - http://www.webopedia.com/TERM/X/X_400.html

QUESTION 877:

The IP header contains a protocol field. If this field contains the value of 1, what type of data is contained within the IP datagram?
A.) TCP
B.) ICMP
C.) UDP
D.) IGMP

Answer: B
ICMP = 1
TCP = 6
UDP = 17
Pg. 55 Casad: Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 878:

Which of the following is true?
A.) TCP is connection-oriented. UDP is not
B.) UDP provides for Error Correction. TCP does not.
C.) UDP is useful for longer messages
D.) UDP guarantees delivers of data. TCP does not guarantee delivery of data.

Answer: A

QUESTION 879:

What works as an E-mail message transfer agent?
A.) SMTP
B.) SNMP

C.) S-RPC
D.) S/MIME

Answer: A

QUESTION 880:

A common way to create fault tolerance with leased lines is to group several T-1's together with an inverse multiplexer placed:
A.) at one end of the connection
B.) at both ends of the connection
C.) somewhere between both end points
D.) in the middle of the connection

Answer: B

QUESTION 881:

Several methods provide telecommunications continuity, which of the following is a method of routing traffic through split cable or duplicate cable facilities?
A.) diverse routing
B.) alternative routing
C.) last mile circuit protection
D.) long haul network diversity

Answer: A

QUESTION 882:

Which of the following is the primary security feature of a proxy server?
A.) Client hiding
B.) URL blocking
C.) Route blocking
D.) Content filtering

Answer: A

QUESTION 883:

Which of the following Common Data Network Services is used to send and receive email internally or externally through an email gateway device?
A.) File services
B.) Mail services
C.) Print Services
D.) Client/Server services

Answer: B

QUESTION 884:

Which one of the following is a technical solution for the quality of service, speed, and security problems facing the Internet?

A. Random Early Detection (RED) queuing
B. Multi-protocol label-switching (MPLS)
C. Public Key Cryptography Standard (PKCS)
D. Resource Reservation Protocol (RSVP)

Answer: B
The original answer to this question was RED however I think this is incorrect because of this reason. Both Red and
MPLS deal with qos/cos issues, there by increasing speed. Mpls more so the RED. However I have not been able to
find any documents that state RED is a security implementation while MPLS is heavy used in the ISP VPN market.
See this link for MPLS security http://www.nwfusion.com/research/2001/0521feat2.html
Below are the link that are formation of the ration for this answer of B (MPLS)
Congestion avoidance algorithm in which a small percentage of packets are dropped when congestion is detected and before the queue in question overflows completely
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/r12.htm
Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/m12.htm
Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/r12.htm
Random Early Detection (RED) is the recommended approach for queue congestion management in routers (Braden et al., 1998). Although in its basic form RED can be implemented in a relatively short C program, as the speed of ports and the number of queues per port increase, the implementation moves more and more into hardware. Different vendors choose different ways to implement and support RED in their silicon implementations. The degree of programmability, the number of queues, the granularity among queues, and the calculation methods of the RED parameters all vary from implementation to implementation. Some of these differences are irrelevant to the behavior of the algorithm-and hence to the resulting network behavior. Some of the differences, however, may result in a very different behavior of the RED algorithm-and hence of the network efficiency.
http://www.cisco.com/en/US/products/hw/routers/ps167/products_white_paper09186a0080091fe4.shtml
Based on label swapping, a single forwarding mechanism provides opportunities for new control

paradigms and applications. MPLS Label Forwarding is performed with a label lookup for an incoming label, which is then swapped with the outgoing label and finally sent to the next hop. Labels are imposed on the packets only once at the edge of the MPLS network and removed at the other end. These labels are assigned to packets based on groupings or forwarding equivalence classes (FECs). Packets belonging to the same FEC get similar treatment. The label is added between the Layer 2 and the Layer 3 header (in a packet environment) or in the virtual path identifier/virtual channel identifier (VPI/VCI) field (in ATM networks). The core network merely reads labels, applies appropriate services, and forwards packets based on the labels. This MPLS lookup and forwarding scheme offers the ability to explicitly control routing based on destination and source addresses, allowing easier introduction of new IP services.
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/xlsw_ds.htm

---

QUESTION 885:

How do you distinguish between a bridge and a router?

A. The router connects two networks at the data-link layer, while bridge connects two networks at the network layer
B. The bridge connects two networks at the data-link layer, while router connects two networks at the network layer
C. It is not possible to distinguish them. They have the same funcationality.

Answer: B

QUESTION 886:

Why should you avoid having two routers connect your trusted internal LAN to your demilitarized zone?
A.) Network congestion might cause the routers to pass data from your private network through the demilitarized zone
B.) This provides attackers with multiple paths to access your trusted network
C.) There is a substantial increase in cost with only a nominal increase in security
D.) You may overlook an attack on one of your routers because your data still teaches the outside world from your other router

Answer: C

QUESTION 887:

In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class B network?
A.) The first bit of the ip address would be set to zero
B.) The first bit of the ip address would be set to one and the second bit set to zero
C.) The first two bits of an ip address would be set to one, and the third bit set to zero
D.) The first three bits of the ip address would be set to one

Answer: B

QUESTION 888:

Which of the following is an ip address that is private (i.e. reserved for internal networks, and not a valid address to use on the internet)?
A.) 172.5.42.5
B.) 172.76.42.5
C.) 172.90.42.5
D.) 172.16.42.5

Answer: D
The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets - 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255- that are known as "global non-routable addresses."" Pg. 94 Krutz: The CISSP Prep Guide.

QUESTION 889:

Which of the following is an ip address that is private (i.e. reserved for internal networks, and not a valid address to use on the internet)?
A.) 10.0.42.5
B.) 11.0.42.5
C.) 12.0.42.5
D.) 13.0.42.5

Answer: A
The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets - 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255- that are known as "global non-routable addresses."" Pg. 94 Krutz: The CISSP Prep Guide.

QUESTION 890:

Which of the following is an ip address that is private (i.e. reserved for internal networks, and not a valid address to use on the internet)?
A.) 172.12.42.5
B.) 172.140.42.5
C.) 172.31.42.5
D.) 172.15.45.5

Answer: C
The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets - 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255,

and 192.168.0.0 to 192.168.255.255- that are known as "global non-routable addresses."" Pg. 94
Krutz: The CISSP Prep Guide.

QUESTION 891:

In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class C network?
A.) The first bit of the ip address would be set to zero
B.) The first bit of the ip address would be set to one and the second bit set to zero
C.) The first two bits of the ip address would be set to one, and the third bit set to zero
D.) The first three bits of the ip address would be set to one

Answer: C
Pg. 80 Sams Teach Yourself TCP/IP in 24 hrs.

QUESTION 892:

Which of the following is an ip address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?
A.) 192.168.42.5
B.) 192.166.42.5
C.) 192.175.42.5
D.) 172.1.42.5

Answer: A

QUESTION 893:

How long are IPv4 addresses:

A.) 32 bits long
B.) 64 bits long
C.) 128 bits long
D.) 16 bits long

Answer: A
"Ipv4 user 32 bits for addresses, and Ipv6 user 128 bits; thus v6 provide more possible addresses to work with." Pg 331 Shon Harris: All-in-One CISSP Certification

---

QUESTION 894:

ARP and RARP map between which of the following?
A.) DNS addresses and IP addresses
B.) 32-bit hardware addresses and 48-bit IPv6 addresses
C.) 32-bit hardware addresses and 48-bit IPv4 addresses
D.) 32-bit addresses in IPv4 and 48-bit hardware addresses

Answer: D
An Ethernet address is a 48-bit address that is hard-wired into the NIC of the network node. ARP matches up the 32-bit IP address with this hardware address, which is technically referred to as the Media Access Control (MAC) address or the physical address. Pg. 87 Krutz: The CISSP Prep Guide.

QUESTION 895:

Which protocol matches an Ethernet address to an Internet Protocol (IP) address?
A.) Address Resolution Protocol (ARP)
B.) Reverse Address Resolution Protocol (RARP)
C.) Internet Control Message Protocol (ICMP)
D.) User Datagram Protocol (UDP)

Answer: B
"As with ARP, Reverse Address Resolution Protocol (RARP) frames go to all systems on the subnet, but only the RARP server responds. Once the RARP server receives this request, it looks in its table to see which IP address matches the broadcast hardware address. The server then sends a message back to the requesting computer that contains its IP address. The system now has an IP address and can function on the network." Pg 357 Shon Harris: All-in-One CISSP Certification

---

QUESTION 896:

In a typical firewall configuration, what is the central host in organization's network security?

A. Stateful
B. Screen
C. Gateway
D. Bastion

Answer: D
Bastion Host: A system that has been hardened to resist attack at some critical point of entry, and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be 'outside" Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (e.g., LNIX, VMS, WNT, etC.) rather than a ROM-based or firmware operating system.
http://www.securesynergy.com/library/articles/it_glossary/glossary_b.php

---

QUESTION 897:

Which one of the following describes a bastion host?

A. A physically shielded computer located in a data center or vault.

B. A computer which maintains important data about the network.
C. A computer which plays a critical role in a firewall configuration.
D. A computer used to monitor the vulnerability of a network.

Answer: C
A bastion host or screened host is just a firewall system logically positioned between a private network and an untrusted network. - Ed Tittle CISSP Study Guide (sybex) pg 93

QUESTION 898:

Which of the following statements pertaining to firewalls is incorrect?
A.) Firewalls should not run NIS (Network Information Systems)
B.) Firewalls should mount files systems via NFS
C.) All system logs on the firewall should log to a separate host
D.) Compilers should be deleted from the firewall

Answer: B

QUESTION 899:

Which is the MAIN advantage of having an application gateway?

A. To perform change control procedures for applications.
B. To provide a means for applications to move into production.
C. To log and control incoming and outgoing traffic.
D. To audit and approve changes to applications.

Answer: C
"An application-level gateway firewall is also called a proxy firewall. A proxy is a mechanism that copies packets from one network into another; the copy process also changes the sources and destination address to protect the identity of the internal or private network. An application-level gateway firewall filters traffic based on the Internet service (i.e., application) used to transmit or receive the data." - Shon Harris All-in-one CISSP Certification Guide pg 92

QUESTION 900:

Which process on a firewall makes permit/deny forwarding decisions based solely on address and service port information?

A. Circuit Proxy
B. Stateful Packet Inspection Proxy
C. Application Proxy
D. Transparency Proxy

Answer: A
Circuit-level proxy creates a circuit between the client computer and the server. It does not

understand or care about the higher-level issues that an application-level proxy deals with. It knows the source and destinations addresses and makes access decisions based on this information...IT looks at the data within the packet header versus the data within the payload of the packet. It does not know if the contents within the packet are actually safe or not. - Shon Harris All-in-one CISSP Certification Guide pg 419-420

QUESTION 901:

A proxy based firewall has which one of the following advantages over a firewall employing stateful packet inspection?

A. It has a greater throughput.
B. It detects intrusion faster.
C. It has greater network isolation.
D. It automatically configures the rule set.

Answer: C

QUESTION 902:

Firewalls filter incoming traffic according to

A. The packet composition.
B. A security policy.
C. Stateful packet rules.
D. A security process.

Answer: B

QUESTION 903:

Application Level Firewalls create:
A.) a real circuit between the workstation client and the server
B.) a virtual circuit between the workstation client and the server
C.) a imaginary circuit between the workstation guest and the server
D.) a temporary circuit between the workstation host and the server

Answer: B

QUESTION 904:

Which of the following is the biggest concern with firewall security?
A.) Internal hackers
B.) Complex configuration rules leading to misconfiguration
C.) Buffer overflows
D.) Distributed denial of service (DDOS) attacks

Answer: B

QUESTION 905:

Which of the following is true of network security?
A.) A firewall is not a necessity in today's connected world
B.) A firewall is a necessity in today's connected world
C.) A whitewall is a necessity in today's connected world
D.) A black firewall is a necessity in today's connected world

Answer: B

QUESTION 906:

Which of the following statements pertaining to firewalls is incorrect?
A.) Firewall create bottlenecks between the internal and external network
B.) Firewalls allow for centralization of security services in machines optimized and dedicated to the task
C.) Strong firewalls can protect a network at all layers of the OSI models
D.) Firewalls are used to create security checkpoints at the boundaries of private networks

Answer: C

QUESTION 907:

Which of the following is the least important security service provided by a firewall?
A.) Packet filtering
B.) Encrypted tunnels
C.) Network Address Translation
D.) Proxy services

Answer: B

QUESTION 908:

Which of the following firewall rules is less likely to be found on a firewall installed between an organization's internal network and internet?
A.) Permit all traffic to and from local host
B.) Permit all inbound ssh traffic
C.) Permit all inbound tcp connections
D.) Permit all syslog traffic to log-server.abc.org

Answer: C

QUESTION 909:

Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?
A.) Inbound packets with Source Routing option set
B.) Router information exchange protocols
C.) Inbound packets with an internal source IP address
D.) Outbound packets with an external destination IP address

Answer: D

QUESTION 910:

By examining the "state" and "context" of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC). This type of firewall system is used in:
A.) first generation firewall systems
B.) second generation firewall systems
C.) third generation firewall systems
D.) fourth generation firewall systems

Answer: C
"Stateful Inspection Characteristics
The firewall maintains a state table that tracks each and every communication channel.
Frames are analyzed at all communication layers.
It provides a high degree of security and does not introduce the performance hit that proxy firewalls introduce.
It is scaleable and transparent to users
It provides data tracking for tracking connectionless protocols such as UDP and ICMP
The stat and context of the data within the packets are stored and updated continuously.
It is considered a third-generation firewall." Pg. 375 Shon Harris: All-in-One CISSP Certification
Not A:
"Packet filtering is the first generation firewall-that is, it was the first type that was created and used, and other types were developed fall into different generations." Pg 373 Shon Harris: All-in-One CISSP Certification

---

QUESTION 911:

Which of the following statements pertaining to packet filtering is incorrect?
A.) It is based on ACLs
B.) It is not application dependant
C.) It operates at the network layer
D.) It keeps track of the state of a connection

Answer: D

QUESTION 912:

A screening router can perform packet filtering based upon what data?

A. Translated source destination addresses.
B. Inverse address resolution.
C. Source and destination port number.
D. Source and destination addresses and application data.

Answer: C
The original answer was A (translated source destination address). I did not come across this term in my reading.
Screening router
A screening router is one of the simplest firewall strategies to implement. This is a popular design because most companies already have the hardware in place to implement it. A screening router is an excellent first line of defense in the creation of your firewall strategy. It's just a router that has filters associated with it to screen outbound and inbound traffic based on IP address and UDP and TCP ports.
http://www.zdnet.co.uk/news/specials/2000/10/enterprise/techrepublic/2002/10/article002c.html

---

QUESTION 913:

Why are hardware security features preferred over software security features?

A. They lock in a particular implementation.
B. They have a lower meantime to failure.
C. Firmware has fever software bugs.
D. They permit higher performance.

Answer: D
This is a sort of iffy question. Hardware allows faster performance then software and does not need to utilize an underlying OS to make the security software operate. (An example is PIX firewall vs checkpoint). The meantime to failure answer to me is ok but the hardware that the software security also has a MTFF. A few people looked over this question and had no problem with the answer of B (meantime to failure question) but as I looked into it I have picked D. MTTF is typical the time to failure. "MTFF is the expected typical functional lifetime of the device given a specific operating environment" (- Ed Tittle CISSP Study Guide (sybex) pg 657). This leads me to think that this question says hardware has a SHORTER lifespan then software. Thus I am going to have
to go with D (higher performance). This can be because of ASICs. As always uses your best judgment, knowledge
and experience on this question. Below are some points of view.
Few things to consider when deploying software based firewall:
Patching OS or firewall software could bring down firewall or open additional holes
OS Expertise vs. firewall expertise (you may need two administrators).

Support contract (One for hardware, one for OS, one for firewall), who do you call?
Administration (One for OS and one for firewall). If your not an expert in both then forget it.
High-availability (Stateful failover) (usually requires additional software and costs a lot of money). As a result it adds to support costs.
Is software firewalls a bad idea it depends. Every situation is different. -Bob
http://www.securityfocus.com/archive/105/322401/2003-05-22/2003-05-28/2
A software firewall application is designed to be installed onto an existing operating system running on generic server or desktop hardware. The application may or may not 'harden' the underlying operating system by replacing core components. Typical host operating systems include Windows NT, 2000 server or Solaris.
Software firewall applications all suffer from the following key disadvantages:
They run on a generic operating system that may or may not be hardened by the Firewall installation itself.
A generic operating system is non-specialized and more complex than is necessary to operate the firewall. This leads to reliability problems and hacking opportunities were peripheral/unnecessary services are kept running.
Generic operating systems have their own CPU and memory overheads making software based firewalls slower than their dedicated hardware counterparts.
If the software firewalls uses PC hardware as the host platform, then there may be additional reliability problems with the hardware itself. Sub-optimal performance of generic hardware also affects software applications bundled with their own operating systems.
There is no physical or topological separation of the firewalling activity.
A dedicated hardware firewall is a software firewall application and operating system running on dedicated hardware. This means the hardware used is optimized for the task, perhaps including digital signal processors (DSPs) and several network interfaces. There may also be special hardware used to accelerate the encryption/decryption of VPN data. It may be rack mounted for easy installation into a comms' cabinet.
We recommend dedicated hardware firewalls as they offer several key advantages over software applications:
Dedicated hardware is typically more reliable.
Hardware firewalls are simpler, hence more secure.
Hardware firewalls are more efficient and offer superior performance, especially in support of VPNs.
The firewalling activity is physically and topologically distinct.
http://www.zensecurity.co.uk/default.asp?URL=hardware%20software%20firewall

---

QUESTION 914:

Firewalls can be used to

A. Enforce security policy.
B. Protect data confidentiality.
C. Protect against protocol redirects.
D. Enforce Secure Network Interface addressing.

Answer: A

A firewall is a device that supports and enforces the company's network security policy. - Shon Harris All-in-one CISSP Certification Guide pg 412

QUESTION 915:

Which one of the following operations of a secure communication session cannot be protected?

A. Session initialization
B. Session support
C. Session termination
D. Session control

Answer: C
I did not find the answer to this question in any of the texts sources I read for the cissp. However, Network Intrusion
Detection (3rd edition) gives some hints. I am basing this off of the 3 way hand shake and looking for the termination of the session and who does it. Was it a RESET or FIN in the packet. So based off this concept I am concluding that Session Termination is really not controllable. Use your best judgment on this question based off of
experience and knowledge.

QUESTION 916:

The general philosophy for DMZ's are that:
A.) any system on the DMZ can be compromised because it's accessible from the Internet
B.) any system on the DMZ cannot be compromised because it's not accessible from the Internet
C.) some systems on the DMZ can be compromised because they are accessible from the Internet
D.) any system on the DMZ cannot be compromised because it's by definition 100% safe and not accessible from the Internet

Answer: A

QUESTION 917:

What is NOT an authentication method within IKE and IPsec:
A.) CHAP
B.) Pre-shared Key
C.) certificate based authentication
D.) Public Key authentication

Answer: A

QUESTION 918:

In IPSec, if the communication mode is gateway-gateway or host-gateway:
A.) Only tunnel mode can be used

B.) Only transport mode can be used
C.) Encapsulating Security Payload (ESP) authentication must be used
D.) Both tunnel and transport mode can be used

Answer: D
"IPSec can work in one of two modes: transport mode, where the payload of the message is protected, and tunnel mode, where the payload and the routing and header information is protected." Pg 527 Shon Harris: All-in-One CISSP Certification
Not: C
"IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to be used, but it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology. IPSec uses two basic security protocols: Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity." Pg 527 Shon Harris: All-in-One CISSP Certification

---

QUESTION 919:

Internet Protocol Security (IPSec) provides security service within the Internet Protocol (IP) by doing all of the following EXCEPT

A. Enabling a system to select required security protocols.
B. Providing traffic analysis protection.
C. Determining the algorithm(s) to use for the IPsec services.
D. Putting in place any cryptographic keys required to provide the requested services.

Answer: A
Pg 527 Shon Harris CISSP All-In-One Certification Exam Guide

QUESTION 920:

Which of the following Internet Protocol (IP) security headers are defined by the Security Architecture for IP (IPSEC)?

A. The IPv4 and IPv5 Authentication Headers
B. The Authentication Header Encapsulating Security Payload
C. The Authentication Header and Digital Signature Tag
D. The Authentication Header and Message Authentication Code

Answer: B
"IPSec uses two basic security protocols: Authentication Header (AH) and the Encapsulating Security Payload (ESP)." pg 575 Shon Harris CISSP All-In-One Certification Exam Guide

---

QUESTION 921:

Which of the following statements is not true of IPSec Transport mode?
A.) It is required for gateways providing access to internal systems
B.) Set-up when end-point is host or communications terminates at end-points
C.) If used in gateway-to-host communication, gateway must act as host
D.)Detective/Administrative Pairing

Answer: A

QUESTION 922:

What is called the standard format that was established to set up and manage Security Associations (SA) on the Internet in IPSec?
A.) Internet Key Exchange
B.) Secure Key Exchange Mechanism
C.) Oakley
D.) Internet Security Association and Key Management Protocol

Answer: D
Reference: pg 221 Krutz

QUESTION 923:

What is the purpose of the Encapsulation Security Payload (ESP) in the Internet Protocol (IP) Security Architecture for Internet Protocol Security?

A. To provide non-repudiation and confidentiality for IP transmission.
B. To provide integrity and confidentiality for IP transmissions.
C. To provide integrity and authentication for IP transmissions.
D. To provide key management and key distribution for IP transmissions.

Answer: B
"Encapsulating Security Payload (ESP). AH is the authenticating protocol and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity." Pg 575 Shon Harris CISSP All-In-One Certification Exam Guide

---

QUESTION 924:

Which one of the following is a circuit level application gateway and works independent of any supported TCP/IP application protocol?

A. SOCK-et-S (SOCKS)
B. Common Information Model (CIM)
C. Secure Multipurpose Internet Mail Extension (S/MIME)
D. Generic Security Service Application Programming Interface (GSS-API)

Answer: A
"Socks Proxy Server Characteristics
Circuit-level proxy server
Requires clients to be SOCKS-fied with SOCKS client software
Mainly used for outbound Internet access and virtual private network (VPN) functionality
Can be resource-intensive
Provides authentication and encryption features to other VPN protocols, but not considered a traditional VPN protocol"
Pg. 422 Shon Harris CISSP All-In-One Certification Exam Guide
Reference:
The SOCKS is an example of a circuit-level proxy gateway that provides a secure channel between two computers. pg. 379 Shon Harris CISSP

QUESTION 925:

How does the SOCKS protocol secure Internet Protocol (IP) connections?

A. By negotiating encryption keys during the connection setup.
B. By attaching Authentication Headers (AH) to each packet.
C. By distributing encryption keys to SOCKS enabled applications.
D. By acting as a connection proxy.

Answer: D
"SOCKS is an example of a circuit-level proxy gateway that provides a secure channel between two computers. When a SOCKS-enabled client sends a request to a computer on the Internet, this request actually goes to the network's SOCKS proxy server..." pg 379 Shon Harris: All-in-One CISSP Certification

---

QUESTION 926:

In the TCP/IP protocol stack, at what level is the SSL (Secure Sockets Layer) protocol provided?
A.) Application
B.) Network
C.) Presentation
D.) Session

Answer: B

QUESTION 927:

SSL (Secure Sockets Layer) has two possible 'session key' lengths, what are they?
A.) 40 bit & 54 bit
B.) 40 bit & 128 bit
C.) 64 bit & 128 bit
D.) 128 bit & 256 bit

Answer: B

QUESTION 928:

Which of the following is NOT true of SSL?
A.) By convention is uses 's-http://' instead of 'http://'.
B.) It stands for Secure Sockets Layer
C.) It was developed by Netscape
D.) IT is used for transmitting private documents over the internet

Answer: A

QUESTION 929:

Which SSL version offers client-side authentication
A.) SSL v1
B.) SSL v2
C.) SSL v3
D.) SSL v4

Answer: B
"Client Authentication using Digital IDs
Enable access by certificates1. Choose Encryption|Security Preferences in the Server Manager.
2. Specify which versions of SSL your server can communication with. The latest and most secure version is SSL version 3, but many older clients use only SSL version 2. You will probably want to enable your server to use both versions.
3. Refuse access to any client that does not have a client certificate from a trusted CA by choosing the Yes box under Require client certificates (regardless of access control):
4. Click the OK button and confirm your changes."
http://www.verisign.com/repository/clientauth/ent_ig.htm#clientauth

---

QUESTION 930:

In which way does a Secure Socket Layer (SSL) server prevent a "man-in-the-middle" attack?

A. It uses signed certificates to authenticate the server's public key.
B. A 128 bit value is used during the handshake protocol that is unique to the connection.
C. It uses only 40 bits of secret key within a 128 bit key length.
D. Every message sent by the SSL includes a sequence number within the message contents.

Answer: A
Secure Sockets Layer (SSL). An encryption technology that is used to provide secure transactions such as the exchange of credit card numbers. SSL is a socket layer security protocol and is a two-layered protocol that contains the SSL Record Protocol and the SSL Handshake Protocol. Similiar to SSH, SSL uses symmetric encryption for private connections and

asymmetric or public key cryptography (certificates) for peer authentication. It also uses a Message Authentication Code for message integrity checking.
Krutz: The CISSP Prep Guide pg. 89. It prevents a man in the middle attack by confirming that you are authenticating with the server desired prior entering your user name and password. If the server was not authenticated, a man-in-the-middle could retrieve the username and password then use it to login.
The SSL protocol has been known to be vulnerable to some man-in-the-middle attacks. The attacker injects herself right at the beginning of the authentication phase so that she obtains both parties' keys. This enables her to decrypt and view messages that were not intended for her. Using digital signatures during the session-key exchange can circumvent the man-in-the-middle attack. If using kerberos, when Lance and Tanya obtain each other's public keys from the KDC, the public keys are signed by the KDC. Because Tanya and Lanace have the public key of the KDC, they both can decrypt and verify the signature on each other's public key and be sure that it came from the KDC itself. Because David does not have the private key of the KDC, he cannot substitute his pubic key during this type of transmission. Shon Harris All-In-One CISSP Certification pg. 579.
One of the most important pieces a PKI is its public key certificate. A certificate is the mechanism used to associate a public key with a collection of components sufficient to uniquely authenticate the claimed owner. Shon Harris All-In-One CISSP Certification pg. 540.

QUESTION 931:

Secure Shell (SSH) and Secure Sockets Layer (SSL) are very heavily used for protecting
A.) Internet transactions
B.) Ethernet transactions
C.) Telnet transactions
D.) Electronic Payment transactions

Answer: A

QUESTION 932:

Which one of the following CANNOT be prevented by the Secure Shell (SSH) program?

A. Internet Protocol (IP) spoofing.
B. Data manipulation during transmissions.
C. Network based birthday attack.
D. Compromise of the source/destination host.

Answer: D
This is a question that I disagreed with. The premises that SSH does use RSA and 3DES, thus susceptible to cryptographic attack (namely birthday attach) has merit but I think the answer is more simple, in that you SSH cant protect against a compromised source/destination. You can safely rule out spoofing and manipulation (that is the job of ssh to protect the transmission). Original answer was C birthday attack. Use your best judgment based on knowledge and experience.

The use of ssh helps to correct these vulnerabilities. Specifically, ssh protects against these attacks: IP spoofing (where the spoofer is on either a remote or local host), IP source routing, DNS spoofing, interception of cleartext passwords/data and attacks based on listening to X authentication data and spoofed connections to an X11 server.
http://www-arc.com/sara/cve/SSH_vulnerabilities.html
Birthday attack - Usually applied to the probability of two different messages using the same hash fucntion that produces a common message digest; or given a message and its corresponding message digest, finding another message that when passed through the same hash function generates the same specific message digest. The term "birthday" comes from the fact that in a room with 23 people, the probability of two people having the same birthday is great than 50 percent. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 212

QUESTION 933:

Another name for a VPN is a:
A.) tunnel
B.) one-time password
C.) pipeline
D.) bypass

Answer: A

QUESTION 934:

Which one of the following attacks is MOST effective against an Internet Protocol Security (IPSEC) based virtual private network (VPN)?

A. Brute force
B. Man-in-the-middle
C. Traffic analysis
D. Replay

Answer: B
Active attacks find identities by being a man-in-the-middle or by replacing the responder in the negotiation. The attacker proceeds through the key negotiation with the attackee until the attackee has revealed its identity. In a well-designed system, the negotiation will fail after the attackee has revealed its identity because the attacker cannot spoof the identity of the originally-intended system.
The attackee might then suspect that there was an attack because the other side failed before it gave its identity. Therefore, an active attack cannot be persistent because it would prevent all legitimate
access to the desired IPsec system.
http://msgs.securepoint.com/cgi-bin/get/ipsec-0201/18.html
Not C: Traffic analysis is a good attack but not the most effective as it is passive in nature, while Man in the middle is active.

QUESTION 935:

Which of the following is NOT an essential component of a VPN?
A.) VPN Server
B.) NAT Server
C.) authentication
D.) encryption

Answer: B

QUESTION 936:

Virtual Private Network software typically encrypts all of the following EXCEPT

A. File transfer protocol
B. Data link messaging
C. HTTP protocol
D. Session information

Answer: B

QUESTION 937:

Which of the following is less likely to be used in creating a Virtual Private Network?
A.) L2TP
B.) PPTP
C.) IPSec
D.) L2F

Answer: D
"The following are the three most common VPN communications protocol standards:
Point-to-Point Tunneling Protocol(PPTP). PPTP works at the Data Link Layer of the OSI model. Designed for individual client to server connections, it enables only a single point-to-point connection per session. This standard is very common with asynchronous connections that use Win9x or NT clients. PPTP uses native Point-to-Point Protocol (PPP) authentication and encryption services.
Layer 2 Tunneling Protocol (L2TP). L2TP is a combination of PPTP and the earlier Layer 2 Forwarding (L2F) Protocol that works at the Data Link Layer like PPTP. It has become an accepted tunneling standard for VPN's. In fact, dial-up VPNs use this standard quite frequently. Like PPTP, this standard was designed for single point-to-point client to server connections. Not that multiple protocols can be encapsulated within the L2TP tunnel, but do not use encryption like PPTP. Also, L2TP supports TACACS+ and RADIUS, but PPTP does not.
IPSEC. IPSec operates at the Network Layer and it enables multiple and simultaneous tunnels, unlike the single connection of the previous standards. IPSec has the functionality to encrypt and authenticate IP data. It is built into the new Ipv6 standard, and is used as an add-on to the current

Ipv4. While PPTP and L2TP are aimed more at dial-up VPNs, IPSec focuses more on network-to-network connectivity." Pg. 123-125 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 938:

Which one of the following instigates a SYN flood attack?

A. Generating excessive broadcast packets.
B. Creating a high number of half-open connections.
C. Inserting repetitive Internet Relay Chat (IRC) messages.
D. A large number of Internet Control Message Protocol (ICMP) traces.

Answer: B
A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol
(TCP) session initialization handshake. The attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target
system to time out while waiting for the proper response, which makes the system crash or become unusable. - Ronald Krutz The CISSP PREP Guide (gold edition) pg 103
"In a SYN flood attack, hackers use special software that sends a large number of fake packets with the SYN flag set to the targeted system. The victim then reserves space in memory for the connection and attempts to send the standard SYN/ACK reply but never hears back from the originator. This process repeats hundreds or even thousands of times, and the targeted computer eventually becomes overwhelmed and runs out of available resources for the half-opened connections. At that time, it either crashes or simply ignores all inbound connection requests because it can't possibly handle any more half-open connections." Pg 266 Tittel: CISSP Study Guide.

QUESTION 939:

Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing
B. Domain Name Server (DNS) poisoning
C. Reverse Address Resolution Protocol (ARP)
D. Port scanning

Answer: B
This reference is close to the one listed DNS poisoning is the correct answer however, Harris does not say the name
when describing the attack but later on the page she state the following.
This is how DNS DOS attack can occur. If the actual DNS records are unattainable to the attacker for him to alter in
this fashion, which they should be, the attacker can insert this data into the cache of there server instead of

replacing
the actual records, which is referred to as cache poisoning. - Shon Harris All-in-one CISSP Certification Guide pg 795

QUESTION 940:

A Packet containing a long string of NOP's followed by a command is usually indicative of what?
A.) A syn scan
B.) A half-port scan
C.) A buffer overflow
D.) A packet destined for the network's broadcast address

Answer: C
Reference "This paper is for those who want a practical approach to writing buffer overflow exploits. As the title says, this text will teach you how to write these exploits in Perl.
.....
There are reasons why we construct the buffer this way. First we have a lot of NOPs, then the shellcode (which in this example will execute /bin/sh), and at last the ESP + offset values." http://hackersplayground.org/papers/perl-buffer.txt

---

QUESTION 941:

You are running a packet sniffer on a network and see a packet with a long string of long string of "90 90 90 90...." in the middle of it traveling to an x86-based machine. This could be indicative of what?
A.) Over-subscription of the traffic on a backbone
B.) A source quench packet
C.) a FIN scan
D.) A buffer overflow

Answer: D
Reference: "TCP Port 5000 Buffer Overflow Attack
The attack on Port 5000 was part of this scan pattern
Mar 14, 2004 15:58:17.837 - (TCP) 68.144.13.102 : 2282 >>> 192.168.1.36 : 2745
Mar 14, 2004 15:58:17.857 - (TCP) 68.144.13.102 : 2283 >>> 68.144.193.246 : 135
Mar 14, 2004 15:58:17.887 - (TCP) 68.144.13.102 : 2284 >>> 192.168.1.38 : 1025
Mar 14, 2004 15:58:17.907 - (TCP) 68.144.13.102 : 2285 >>> 68.144.193.246 : 445
Mar 14, 2004 15:58:17.938 - (TCP) 68.144.13.102 : 2286 >>> 192.168.1.36 : 3127
Mar 14, 2004 15:58:17.958 - (TCP) 68.144.13.102 : 2287 >>> 68.144.193.246 : 6129
Mar 14, 2004 15:58:17.988 - (TCP) 68.144.13.102 : 2288 >>> 68.144.193.246 : 139
Mar 14, 2004 15:58:18.008 - (TCP) 68.144.13.102 : 2289 >>> 192.168.1.36 : 5000
Mar 14, 2004 15:58:29.164 - (TCP) 68.144.13.102 : 1442 >>> 68.144.193.246 : 1981
Mar 14, 2004 15:58:33.470 - (TCP) 68.144.13.102 : 1442 >>> 68.144.193.246 : 1981
Mar 14, 2004 15:58:39.288 - (TCP) 68.144.13.102 : 1442 >>> 68.144.193.246 : 1981

The attack appears to be a buffer overfull attack on the Plug and Play service on TCP Port 5000, which likely contains instructions to
download and execute the rest of the worm.
TCP Connection Request
---- 14/03/2004 15:40:57.910
68.144.193.124 : 4560 TCP Connected ID = 1
---- 14/03/2004 15:40:57.910
Status Code: 0 OK
68.144.193.124 : 4560 TCP Data In Length 697 bytes
MD5 = 19323C2EA6F5FCEE2382690100455C17
---- 14/03/2004 15:40:57.920
0000 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0010 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0020 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0030 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0040 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0050 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0060 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0070 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0080 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0090 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
00A0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
00B0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
00C0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
00D0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
00E0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
00F0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0100 90 90 90 90 90 90 90 90 90 90 90 90 4D 3F E3 77 ....M?.w
0110 90 90 90 90 FF 63 64 90 90 90 90 90 90 90 90 90 .....cd.........
0120 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....
0130 90 90 90 90 90 90 90 90 EB 10 5A 4A 33 C9 66 B9 ....ZJ3.f.
0140 66 01 80 34 0A 99 E2 FA EB 05 E8 EB FF FF FF 70 f..4...........p
0150 99 98 99 99 C3 21 95 69 64 E6 12 99 12 E9 85 34 .....!.id......4
0160 12 D9 91 12 41 12 EA A5 9A 6A 12 EF E1 9A 6A 12 ....A....j....j.
0170 E7 B9 9A 62 12 D7 8D AA 74 CF CE C8 12 A6 9A 62 ...b....t......b
0180 12 6B F3 97 C0 6A 3F ED 91 C0 C6 1A 5E 9D DC 7B .k...j?.....^..{
0190 70 C0 C6 C7 12 54 12 DF BD 9A 5A 48 78 9A 58 AA p....T....ZHx.X.
01A0 50 FF 12 91 12 DF 85 9A 5A 58 78 9B 9A 58 12 99 P.......ZXx..X..
01B0 9A 5A 12 63 12 6E 1A 5F 97 12 49 F3 9A C0 71 E5 .Z.c.n._..I...q.
01C0 99 99 99 1A 5F 94 CB CF 66 CE 65 C3 12 41 F3 9D ...._...f.e..A..
01D0 C0 71 F0 99 99 99 C9 C9 C9 C9 F3 98 F3 9B 66 CE .q............f.
01E0 69 12 41 5E 9E 9B 99 9E 24 AA 59 10 DE 9D F3 89 i.A^....$.Y.....
01F0 CE CA 66 CE 6D F3 98 CA 66 CE 61 C9 C9 CA 66 CE ..f.m...f.a...f.
0200 65 1A 75 DD 12 6D AA 42 F3 89 C0 10 85 17 7B 62 e.u..m.B......{b
0210 10 DF A1 10 DF A5 10 DF D9 5E DF B5 98 98 99 99 ....^......
0220 14 DE 89 C9 CF CA CA CA F3 98 CA CA 5E DE A5 FA ....^...

0230 F4 FD 99 14 DE A5 C9 CA 66 CE 7D C9 66 CE 71 AA .....f.}.f.q.
0240 59 35 1C 59 EC 60 C8 CB CF CA 66 4B C3 C0 32 7B Y5.Y.`....fK..2{
0250 77 AA 59 5A 71 62 67 66 66 DE FC ED C9 EB F6 FA w.YZqbgff.....
0260 D8 FD FD EB FC EA EA 99 DA EB FC F8 ED FC C9 EB .....
0270 F6 FA FC EA EA D8 99 DC E1 F0 ED C9 EB F6 FA FC .....
0280 EA EA 99 D5 F6 F8 FD D5 F0 FB EB F8 EB E0 D8 99 .....
0290 EE EA AB C6 AA AB 99 CE CA D8 CA F6 FA F2 FC ED .....
02A0 D8 99 FB F0 F7 FD 99 F5 F0 EA ED FC F7 99 F8 FA .....
02B0 FA FC E9 ED 99 0D 0A 0D 0A ..... " http://www.linklogger.com/TCP5000_Overflow.htm

---

QUESTION 942:

Which of the following is true related to network sniffing?
A.) Sniffers allow an attacker to monitor data passing across a network.
B.) Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
C.) Sniffers take over network connections
D.) Sniffers send IP fragments to a system that overlap with each other.

Answer: A

Explanation: Sniffing is the action of capture / monitor the traffic going over the network. Because, in a normal networking environment, account and password information is passed along Ethernet in clear-text, it is not hard for an intruder to put a machine into promiscuous mode and by sniffing, compromise all the machines on the net by capturing password in an illegal fashion.

QUESTION 943:

Which one of the following threats does NOT rely on packet size or large volumes of data?

A. SYN flood
B. Spam
C. Ping of death
D. Macro virus

Answer: D
SPAM - The term describing unwanted email, newsgroup, or discussion forum messages. Spam can be innocuous as an advertisement from a well-meaning vendor or as malignant as floods or unrequested messages with viruses or Trojan horses attached
SYN Flood Attack - A type of DoS. A Syn flood attack is waged by not sending the final ACK packet, which breaks the standard three-way handshake used by TCP/IP to initiate communication sessions.
Ping of death attack - A type of DoS. A ping of death attack employs an oversized ping packet. Using special tools, an attacker can send numerous oversized ping packets to a victim. In many cases, when the victimized system attempts to process the packets, an error occurs causing the

system to freeze, crash, or reboot.
Macro Viruses - A virus that utilizes crude technologies to infect documents created in the Microsoft Word environment.
- Ed Tittle CISSP Study Guide (sybex) pg 550 740, 743, 723, 713

QUESTION 944:

A TCP SYN Attack:
A.) requires a synchronized effort by multiple attackers
B.) takes advantage of the way a TCP session is established
C.) may result in elevation of privileges.
D.) is not something system users would notice

Answer: B
"[SYN Flood] Attackers can take advantage of this design flaw by continually sending the victim SYN messages with spoofed packets. The victim will commit the necessary resources to setup this communication socket, and it will send its SYN/ACK message waiting for the ACK message in return. However, the victim will never receive the ACK message, because the packet is spoofed, and victim system sent the SYN/ACK message to a computer that does not exist. So the victim system receives a SYN message, add it dutifully commits the necessary resources to setup a connection with another computer. This connection is queued waiting for the ACK message, and the attacker sends another SYN message. The victim system does what is supposed to can commits more resources, sends the SYN/ACK message, and queues this connection. This may only need to happen a dozen times before the victim system no longer has the necessary resources to open up another connection. This makes the victim computer unreachable from legitimate computers, denying other systems service from the victim computer." Pg. 735 Shon Harris CISSP All-In-One Exam Guide

---

QUESTION 945:

What attack is typically used for identifying the topology of the target network?

A. Spoofing
B. Brute force
C. Teardrop
D. Scanning

Answer: D

Explanation:
Flaw exploitation attacks exploit a flaw in the target system's software in order to cause a processing failure or to cause it to exhaust system resources. An example of such a processing failure is the 'ping of death' attack. This attack involved sending an unexpectedly large ping packet to certain Windows systems. The target system could not handle this abnormal packet, and a system crash resulted. With respect to resource exhaustion attacks, the resources targeted include CPU time, memory, disk space, space

in a special buffer, or network bandwidth. In many cases, simply patching the software can circumvent this type of DOS attack.

QUESTION 946:

Which one of the following is the reason for why hyperlink spoofing attacks are usually successful?

A. Most users requesting DNS name service do not follow hyperlinks.
B. The attack performs user authentication with audit logs.
C. The attack relies on modifications to server software.
D. Most users do not make a request to connect to a DNS names, they follow hyperlinks.

Answer: D

Explanation:
The problem is that most users do not request to connect to DNS names or even URLs, they follow hyperlinks... But, whereas DNS names are subject to "DNS spoofing" (whereby a DNS server lies about the internet address of a server) so too are URLs subject to what I call "hyperlink spoofing" or "Trojan HTML", whereby a page lies about an URLs DNS name. Both forms of spoofing have the same effect of steering you to the wrong internet site, however hyperlink spoofing is technically much easier than DNS spoofing.
http://www.brd.ie/papers/sslpaper/sslpaper.html

QUESTION 947:

Which of the following identifies the first phase of a Distributed Denial of Service attack?

A. Establishing communications between the handler and agent.
B. Disrupting the normal traffic to the host.
C. Disabling the router so it cannot filter traffic.
D. Compromising as many machines as possible.

Answer: D
Another form of attack is called the distributed denial of service (DDOS). A distributed denial of service occurs when the attacker compromises several systems and uses them as launching platforms against on or more victims. - Ed Tittle CISSP Study Guide (sybex) pg 51

QUESTION 948:

This type of vulnerability enables the intruder to re-route data traffic from a network device to a personal machine? This diversion enables the intruder to capture data traffic to and from the devices for analysis or modification, or to steal the password file from the server and gain access to user accounts.
A.) Network Address Translation
B.) Network Address Hijacking

C.) Network Address Supernetting
D.) Network Address Sniffing

Answer: B
"Network Address Hijacking. It might be possible for an intruder to reroute data traffic from a server or network device to a personal machine, either by device address modification or network address "hijacking." This diversion enables the intruder to capture traffic to and from the devices for data analysis or modification or to steal the password file from the server and gain access to user accounts. By rerouting the data output, the intruder can obtain supervisory terminal functions and bypass the system logs."
Pg. 324 Krutz: The CISSP Prep Guide: Gold Edition

QUESTION 949:

Which one of the following is an example of hyperlink spoofing?

A. Compromising a web server Domain Name Service reference.
B. Connecting the user to a different web server.
C. Executing Hypertext Transport Protocol Secure GET commands.
D. Starting the user's browser on a secured page.

Answer: B
The problem is that most users do not request to connect to DNS names or even URLs, they follow hyperlinks... But, whereas DNS names are subject to "DNS spoofing" (whereby a DNS server lies about the internet address of a server) so too are URLs subject to what I call "hyperlink spoofing" or "Trojan HTML", whereby a page lies about an URLs DNS name. Both forms of spoofing have the same effect of steering you to the wrong internet site, however hyperlink spoofing is technically much easier than DNS spoofing.
http://www.brd.ie/papers/sslpaper/sslpaper.html

QUESTION 950:

Why are packet filtering routers NOT effective against mail bomb attacks?

A. The bomb code is obscured by the message encoding algorithm.
B. Mail bombs are polymorphic and present no consistent signature to filter on.
C. Filters do not examine the data portion of a packet.
D. The bomb code is hidden in the header and appears as a normal routing information.

Answer: C

QUESTION 951:

Which one of the following correctly identifies the components of a Distributed Denial of Service Attack?

A. Node, server, hacker, destination

B. Client, handler, agent, target
C. Source, destination, client, server
D. Attacker, proxy, handler, agent

Answer: B
Another form of DoS. A distributed denial of service occurs when the attacker compromises several systems to be used as launching platforms against one or more victims. The compromised systems used in the attacks are often called claves or zombies. A DDoS attack results in the victims being flooded with data from numerous sources. - Ed Tittle CISSP Study Guide (sybex) pg 693

QUESTION 952:

Which one of the following attacks will pass through a network layer intrusion detection system undetected?

A. A teardrop attack
B. A SYN flood attack
C. A DNS spoofing attack
D. A test.cgi attack

Answer: D

Explanation:
"Because a network-based IDS reviews packets and headers, it can also detect denial of service (DoS) attacks." Pg. 64 Krutz: The CISSP Prep Guide
Not A or B:
"The following sections discuss some of the possible DoS attacks available.
Smurf
Fraggle
SYN Flood
Teardrop
DNS DoS Attacks"
Pg. 732-737 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 953:

Which one of the following is a passive network attack?

A. Spoofing
B. Traffic Analysis
C. Playback
D. Masquerading

Answer: B

Explanation:

"Traffic analysis and trend analysis are forms of monitoring that examine the flow of packets rather than the actual content of packets. Traffic and trend analysis can be used to infer a large amount of information, such as primary communication routes, sources of encrypted traffic, location of primary servers, primary and backup communication pathways, amount of traffic supported by the network, typical direction of traffic flow, frequency of communications, and much more." Pg 429 Tittel: CISSP Study Guide

---

QUESTION 954:

Which one of the following can NOT typically be accomplished using a Man-in-the-middle attack?

A. DNS spoofing
B. Session hijacking
C. Denial of service flooding
D. Digital signature spoofing

Answer: D

QUESTION 955:

What is called an attach where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?
A.) SYN flood attack
B.) Smurf attack
C.) Ping of Dead Attack
D.) Denial of Service (DOS) Attack

Answer: B
Reference: pg 158 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 956:

Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?
A.) TCP sequence number attack
B.) IP spoofing attack
C.) Piggybacking attack
D.) Teardrop attack

Answer: B

QUESTION 957:

How does a teardrop attack work?

Answer:
Reference: Another attack that relies on poor TCP/IP implementation is Teardrop < http://www.rage.mircx.com/knowledge/tcpip-teardrop.htm> , which exploits defects in the way systems reassemble IP packet fragments. On their way from hither to you on the Internet, an IP packet may be broken up into smaller pieces. Each of these still has the original IP packet's header, as well as an offset field that identifies which bytes of the original packet it contains. With this information, an ordinary broken packet is reassembled at its destination and network continues uninterrupted. When a Teardrop attack hits, your server is bombarded with IP fragments that have overlapping offset fields. If your server or router can't disregard these fragments and attempts to reassemble them, your box will go castors up quickly. If your systems are up-to-date, or if you have a firewall that blocks Teardrop packets, you shouldn't have any trouble.

QUESTION 958:

What attack takes advantage of operating system buffer overflows?

A. Spoofing
B. Brute force
C. DoS
D. Exhaustive

Answer: C

Explanation:
Denial of Service is an attack on the operating system or software using buffer overflows. The result is that the target is unable to reply to service requests. This is too a large an area of information to try to cover here, so I will limit my discussion to the types of denial of service (DoS) attacks:

QUESTION 959:

What attack is primarily based on the fragmentation implementation of IP and large ICMP packet size?

A. Exhaustive
B. Brute force
C. Ping of Death
D. Spoofing

Answer: C

Explanation:
Ping of Death -- This exploit is based on the fragmentation implementation of IP whereby large packets are reassembled and can cause machines to crash. 'Ping of Death

takes advantage of the fact that it is possible to send an illegal ICMP Echo packet with more than the allowable 65, 507 octets of data because of the way fragmentation is performed. A temporary fix is block ping packets. Ideally, an engineer should secure TCP/IP from overflow when reconstructing IP fragments.

QUESTION 960:

Land attack attacks a target by:

A. Producing large volume of ICMP echos.
B. Producing fragmented IP packets.
C. Attacking an established TCP connection.
D. None of the choices.

Answer: C

Explanation:
Land.c. attack -- Attacks an established TCP connection. A program sends a TCP SYN packet giving the target host address as both the sender and destination using the same port causing the OS to hang.

QUESTION 961:

What attack is primarily based on the fragmentation implementation of IP?

A. Teardrop
B. Exhaustive
C. Spoofing
D. Brute force

Answer: A

Explanation:
Teardrop attack - This is based on the fragmentation implementation of IP whereby reassembly problems can cause machines to crash. The attack uses a reassembly bug with overlapping fragments and causes systems to hang or crash. It works for any Internet Protocol type because it hits the IP layer itself. Engineers should turn off directed broadcast capability.

QUESTION 962:

What attack floods networks with broadcast traffic so that the network is congested?

A. Spoofing
B. Teardrop
C. Brute force

D. SMURF

Answer: D

Explanation:
SMURF attack -- This attack floods networks with broadcast traffic so that the network is congested. The perpetrator sends a large number of spoofed ICMP (Internet Control Message Protocol) echo requests to broadcast addresses hoping packets will be sent to the spoofed addresses. You need to understand the OSI model and how protocols are transferred between layer 3 and layer 2 to understand this attack. The layer 2 will respond to the ICMP echo request with an ICMP echo reply each time, multiplying the traffic by the number of hosts involved. Engineers should turn off broadcast capability (if possible in your environment) to deter this kind of attack.

QUESTION 963:

What attack involves repeatedly sending identical e-message to a particular address?

A. SMURF
B. Brute force
C. Teardrop
D. Spamming

Answer: D

Explanation:
Spamming -- Involves repeatedly sending identical e-message to a particular address. It is a variant of bombing, and is made worse when the recipient replies -- i.e. recent cases where viruses or worms were attached to the e-mail message and ran a program that forwarded the message from the reader to any one on the user's distribution lists. This attack cannot be prevented, but you should ensure that entrance and exit of such mail is only through central mail hubs.

QUESTION 964:

A stack overflow attack that "crashes" a Transmission Control Protocol/Internet Protocol (TCP/IP) service daemon
can result in a serious security breach because the

A. Process does not implement proper object reuse.
B. Process is executed by a privileged entity.
C. Network interface becomes promiscuous.
D. Daemon can be replaced by a trojan horse.

Answer: B

QUESTION 965:

The intrusion detection system at your site has detected Internet Protocol (IP) packets where the IP source address is
the same as the destination address.
This situation indicates

A. Misdirected traffic jammed to the internal network.
B. A denial of service attack.
C. An error in the internal address matrix.
D. A hyper overflow in the IP stack.

Answer: B
"The Land denial of service attack causes many older operating systems (such as Windows NT 4, Windows 95, and SunOS 4.1.4) to freeze and behave in an unpredictable manner. It works by creating an artificial TCP packet that has the SYN flag set. The attacker set the destination IP address to the address of the victim machine and the destination port to an open port on that machine. Next, the attacker set the source IP address and source port to the same values as the destination IP address and port. When the targeted host receives this unusual packet, the operating system doesn't know how to process it and freezes, crashes, or behaves in an unusual manner as a result." Pg 237 Tittel: CISSP Study Guide

---

QUESTION 966:

What type of attacks occurs when a rogue application has been planted on an unsuspecting user's workstation?

A. Physical attacks
B. Logical attacks
C. Trojan Horse attacks
D. Social Engineering attacks

Answer: C

Explanation:
Trojan Horse attacks - This attack involves a rogue, Trojan horse application that has been planted on an unsuspecting user's workstation. The Trojan horse waits until the user submits a valid PIN from a trusted application, thus enabling usage of the private key, and then asks the smartcard to digitally sign some rogue data. The operation completes but the user never knows that their private key was just used against their will.

QUESTION 967:

Man-in-the-middle attacks are a real threat to what type of communication?

A. Communication based on random challenge.
B. Communication based on face to face contact.
C. Communication based on token.
D. Communication based on asymmetric encryption.

Answer: D

Explanation:
The weakest point in the communication based on asymmetric encryption is the knowledge about the real owners of keys. Somebody evil could generate a key pair, give the public key away and tell everybody, that it belongs to somebody else. Now, everyone believing it will use this key for encryption, resulting in the evil man being able to read the messages. If he encrypts the messages again with the public key of the real recipient, he will not be easily recognized. This sort of attack is called ``man-in-the-middle'' attack and can only be prevented by making sure, public keys really belong to the one being designated as owner.

QUESTION 968:

Which of the following threats is not addressed by digital signature and token technologies?
A.) Spoofing
B.) replay attacks
C.) password compromise
D.) denial-of-service

Answer: D

QUESTION 969:

Which one of the following is concerned with masking the frequency, length, and origin-destination patterns of the communications between protocol entities?

A. Masking analysis
B. Protocol analysis
C. Traffic analysis
D. Pattern analysis

Answer: C
Traffic analysis, which is sometimes called trend analysis, is a technique employed by an intruder that involves analyzing data characteristics (message length, message frequency, and so forth) and the patterns of transmissions (rather than any knowledge of the actual information transmitted) to infer information that is useful to an intruder) . -Ronald Krutz The CISSP PREP Guide (gold edition) pg 323

QUESTION 970:

Which of the following would NOT be considered a Denial of Service Attack?
A.) Zone Transfer
B.) Smurf
C.) Syn Flood
D.) TearDrop

Answer: A
Zone transfer is method that DNS uses to transfer zone information between servers. In some un-secure DNS installations zone transfers are allowed to un-trusted DNS servers. This allows the hacker to determine internal host names and ip addresses to provide additional information for an attack.

QUESTION 971:

The connection using fiber optics from a phone company's branch office to local customers is which of the following?
A.) new loop
B.) local loop
C.) loopback
D.) indigenous loop

Answer: B
In telecommunications Telecommunication the local loop is the wiring between the central office and the customer's premises demarcation point. The telephony local loop connection is typically a copper twisted pair carrying current from the central office to the customer premises and back again. Individual local loop telephone lines are connected to the local central office or to a remote concentrator.
Local loop connections can be used to carry a range of technologies, including:
Analog Voice
ISDN
DSL

QUESTION 972:

Which step ensures the confidentiality of a facsimile transmission?

A. Pre-schedule the transmission of the information.
B. Locate the facsimile equipment in a private area.
C. Encrypt the transmission.
D. Phone ahead to the intended recipient.

Answer: C

QUESTION 973:

Which one of the following could a company implement to help reduce PBX fraud?

A. Call vectoring
B. Direct Inward System Access (DISA)
C. Teleconferencing bridges
D. Remote maintenance ports

Answer: B
The potential for fraud to occur in voice telecommunications equipment is a serious threat. PBX's (Private Branch
Exchange) are telephone switches used within state agencies to allow employees to make out-going and receive incoming
phone calls. These PBX's can also provide connections for communications between personal computers
and local and wide area networks. Security measures must be taken to avoid the possibility of theft of either phone
service or information through the telephone systems.
Direct Inward System Access (DISA) is the ability to call into a PBX, either on an 800 number or a local dial-in,
and by using an authorization code, gain access to the long distance lines and place long distance calls through the
PBX
http://www.all.net/books/Texas/chap10.html

QUESTION 974:

Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud
manipulates the line voltage to receive a toll-free call?
A.) Red boxes
B.) Blue boxes
C.) White boxes
D.) Black boxes

Answer: D

QUESTION 975:

Which one of the following devices might be used to commit telecommunications fraud
using the "shoulder surfing" technique?

A. Magnetic stripe copier
B. Tone generator
C. Tone recorder
D. Video recorder

Answer: C

QUESTION 976:

What technique is used to prevent eavesdropping of digital cellular telephone conversations?

A. Encryption
B. Authentication
C. Call detail suppression
D. Time-division multiplexing

Answer: D
The name "TDMA" is also used to refer to a specific second generation mobile phone standard - more properly referred to as IS-136, which uses the TDMA technique to timeshare the bandwidth of the carrier wave. It provides between 3 to 6 times the capacity of its predecessor AMPS, and also improved security and privacy. In the United States, for example, AT&T Wireless uses the IS-136 TDMA standard. Prior to the introduction of IS-136, there was another TDMA North American digital cellular standard called IS-54(which was also referred to just as "TDMA").

QUESTION 977:

Which of the following is a telecommunication device that translates data from digital to analog form and back to digital?

A.) Multiplexer
B.) Modem
C.) Protocol converter
D.) Concentrator

Answer: B

QUESTION 978:

Which of the following could lead to the conclusion that a disaster recovery plan may not be operational within the timeframe the business needs to recover?
A.)The alternate site is a warm site
B.) Critical recovery priority levels are not defined
C.) Offsite backups are located away from the alternate site
D.) The alternate site is located 70 miles away from the primary site

Answer: B

QUESTION 979:

What are the four domains of communication in the disaster planning and recovery process?

A. Plan manual, plan communication, primer for survival, warning and alarms
B. Plan communication, primer for survival, escalation, declaration
C. Plan manual, warning and alarm, declaration, primer for survival
D. Primer for survival, escalation, plan communication, warning and alarm

Answer: C

QUESTION 980:

The underlying reason for creating a disaster planning and recover strategy is to

A. Mitigate risks associated with disaster.
B. Enable a business to continue functioning without impact.
C. Protect the organization's people, place and processes.
D. Minimize financial profile.

Answer: A
"Disaster recovery has the goal of minimizing the effects of a disaster and taking the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner." Pg 550 Shon Harris: All-in-One CISSP Certification

---

QUESTION 981:

Which of the following is not a direct benefit of successful Disaster Recovery Planning?
A.) Maintain Nance of Business Continuity
B.) Protection of Critical Data
C.) Increase in IS performance
D.) Minimized Impact of a disaster

Answer: C

QUESTION 982:

Organizations should not view disaster recovery as which of the following?
A.) committed expense
B.) discretionary expense
C.) enforcement of legal statues
D.) compliance with regulations

Answer: B

QUESTION 983:

Which of the following statements pertaining to disaster recovery is incorrect?
A.) A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
B.) A salvage team's task is to ensure that the primary site returns to normal processing conditions
C.) The disaster recovery plan should include how the company will return from the alternate site to the primary site
D.) When returning to the primary site, the most critical applications should be brought back first

Answer: D

QUESTION 984:

Which of the following statements pertaining to dealing with the media after a disaster occurred and disturbed the organization's activities is incorrect?
A.) The CEO should always be the spokesperson for the company during a disaster
B.) The disaster recovery plan must include how the media is to be handled during the disaster
C.) The organization's spokesperson should report bad news before the press gets ahold of it through another channel
D.) An emergency press conference site should be planned ahead

Answer: A

QUESTION 985:

What is a disaster recovery plan for a company's computer system usually focused on?
A.) Alternative procedures to process transactions
B.) The probability that a disaster will occur
C.) Strategic long-range planning
D.) Availability of compatible equipment at a hot site

Answer: A

QUESTION 986:

What is the most critical piece to disaster recovery and continuity planning?
A.) Security Policy
B.) Management Support
C.) Availability of backup information processing facilities
D.) Staff training

Answer: B

QUESTION 987:

Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?
A.) it is unlikely to be affected by the same contingency
B.) it is close enough to become operation quickly
C.) is it close enough to serve it's users
D.) it is convenient to airports and hotels

Answer: A

QUESTION 988:

Which of the following are PRIMARY elements that are required when designing a Disaster Recovery Plan (DRP)?

A. Back-up procedures, off-site storage, and data recover.
B. Steering committee, emergency response team, and reconstruction team.
C. Impact assessment, recover strategy, and testing.
D. Insurance coverage, alternate site, and manual procedures.

Answer: C
The most critical piece to disaster recovery and continuity planning is management support. They must be convinced of its necessity. Therefore, a business case must be made to obtain this support. The business case can include current vulnerabilities, regulatory and legal obligations, current status of recovery plans, and recommendations. Management will mostly concerned with cost/benefit issues, so several preliminary numbers will need to be gathered and potential losses estimated. - Shon Harris All-in-one CISSP Certification Guide pg 595
There are four major elements of the BCP process
Scope and Plan Initiation - this phase marks the beginning of the BCP process. IT entails creating the scope and other elements needed to define the parameters of the plan.
Business Impact Assessment - A BIA is a process used to help business units understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment
Business Continuity Plan Development - This term refers to using the information collection in the BIA to develop the actual business continuity plan. This process includes the areas of plan implementation, plan testing, and ongoing plan maintenance.
Plan Approval and Implementation - This process involves getting the final senior management signoff, creating enterprise-wide awareness of the plan, and implementing a maintenance procedure for updating the plan as needed. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 380-381

QUESTION 989:

Emergency actions are taken at the incipient stage of a disaster with the objectives of preventing injuries or loss of life and of:
A.) determining the extent of property damage

B.) protecting evidence
C.) preventing looting and further damage
D.) mitigating the damage to avoid the need for recovery

Answer: D

QUESTION 990:

Who should direct short-term recovery actions immediately following a disaster?
A.) Chief Information Officer
B.) Chief Operating Officer
C.) Disaster Recovery Manager
D.) Chief Executive Officer

Answer: C

QUESTION 991:

The environment that must be protected includes all personnel, equipment, data, communication devices, power supply and wiring. The necessary level of protection depends on the value of data, the computer systems, and the company assets within the facility. The value of these items can be determined by what type of analysis?
A.) Critical-channel analysis
B.) Critical-route analysis
C.) Critical-path analysis
D.) Critical-conduit analysis

Answer: C
"The environment that must be protected through physical security controls includes all personnel, equipment, data, communication devices, power supplies, and wiring. The necessary level of protection depends on the value of the data, the computer systems, and the company assets within the facility. The value of these items can be determined by a critical-path analysis, which lists each piece of the infrastructure and what is necessary to keep those pieces healthy and operational." Pg 255 Shon Harris: All-in-One CISSP Certification

---

QUESTION 992:

Which of the following steps should be performed first in a business impact analysis (BIA)?
A.) Identify all business units within the organization
B.) Evaluate the impact of the disruptive events
C.) Estimate the Recovery Time Objectives (RTO)
D.) Evaluate the criticality of business functions

Answer: A

QUESTION 993:

Which of the following steps it NOT one of the four steps of a Business Impact Analysis (BIA)?
A.) Notifying senior management
B.) Gathering the needed assessment materials
C.) Performing the vulnerability assessment
D.) Analyzing the information compiled

Answer: A
"A BIA generally takes the form of these four steps:
1.) Gathering the needed assessment materials
2.) Performing the vulnerability assessment
3.) Analyzing the information compiled
4.) Documenting the results and presenting recommendations"
Pg. 383 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 994:

What methodology is commonly used in Business Continuity Program?

A. Work Group Recovery
B. Business Impact Analysis
C. Qualitative Risk Analysis
D. Quantitative Risk Analysis

Answer: B
A BIA is performed at the beginning of disaster recovery and continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of disaster or disruption. - Shon Harris All-in-one CISSP Certification Guide pg 597

QUESTION 995:

Which of the following steps should be performed first in a business impact analysis (BIA)?
A.) Identify all business units within an organization
B.) Evaluate the impact of disruptive events
C.) Estimate the Recovery Time Objectives (RTO)
D.) Evaluate the criticality of business functions

Answer: A
"The initial step of the BIA is identifying which business units are critical to continuing an acceptable level of operations." Pg 383 Krutz: CISSP Prep Guide: Gold Edition.

QUESTION 996:

Which is not one of the primary goals of BIA?
A.) Criticality Prioritization
B.) Down time estimation
C.) Determining requirements for critical business functions
D.) Deciding on various test to be performed to validate Business Continuity Plan

Answer: D

QUESTION 997:

Which of the following is used to help business units understand the impact of a disruptive event?
A.) A risk analysis
B.) A Business Impact assessment
C.) A Vulnerability assessment
D.) A disaster recovery plan

Answer: B
Reference: "The purpose of a BIA is to create a document to be used to help understand what impact a disruptive event would have on the business." Pg 383 Krutz : CISSP Prep Guide: Gold Edition

---

QUESTION 998:

A Business Impact Analysis (BIA) does not:
A.) Recommend the appropriate recovery solution
B.) Determine critical and necessary business functions and their resource dependencies
C.) Identify critical computer applications and the associated outage tolerance
D.) Estimate the financial and operation impact of a disruption

Answer: A

QUESTION 999:

What assesses potential loss that could be caused by a disaster?
A.) The Business Assessment (BA)
B.) The Business Impact Analysis (BIA)
C.) The Risk Assessment (RA)
D.) The Business Continuity Plan (BCP)

Answer: B

QUESTION 1000:

During the course of a Business Impact Analysis (BIA) you will less likely:
A.) Estimate the financial and operational impact of a disruption
B.) Identify regulatory exposure
C.) Determine if functions Recovery Time Objective (RTO)
D.) Determine the impact upon the organizations market share and corporate image

Answer: C

QUESTION 1001:

Which of the following tasks is not usually part of a Business Impact Analysis (BIA)?
A.) Identify the type and quantity of resources required for recovery
B.) Identify the critical processes and the dependencies between them
C.) Identify organizational risks
D.) Develop a mission statement

Answer: D

QUESTION 1002:

Which of the following will a Business Impact Analysis (BIA) NOT identify?
A.) Areas that would suffer the greatest financial or operation loss in the event of a disaster
B.) Systems critical to the survival of the enterprise
C.) The names of individuals to be contacted during a disaster
D.) The outage time that can be tolerated by the enterprise as a result of a disaster

Answer: C

QUESTION 1003:

Which one the following is the primary goal of Business Continuity Planning?

A. Sustain the organization.
B. Recover from a major data center outage.
C. Test the ability to prevent major outages.
D. Satisfy audit requirements.

Answer: A
Simply put, business continuity plans are created to prevent interruptions to normal business activity.-Ronald Krutz The CISSP PREP Guide (gold edition) pg 378

QUESTION 1004:

Most of unplanned downtime of information systems is attributed to which of the following?
A.) Hardware failure

B.) Natural disaster
C.) Human error
D.) Software failure

Answer: A

QUESTION 1005:

System reliability s increased by:
A.) A lower MTBF and a lower MTTR
B.) A higher MTBF and a lower MTTR
C.) A lower MTBF and a higher MTTR
D.) A higher MTBF and a higher MTTR

Answer: B
One prefers to have a higher MTBF and a lower MTTR.
"Each device has a mean time between failure (MTBF) and a mean time to repair (MTTR). The MTBF estimate is used to determine the expected lifetime of a device or when an element within that device is expected to give out. The MTTR value is used to estimate the time it will take to repair the device and get it back into production." Pg 267 Shon Harris: All-in-One CISSP Certification

---

QUESTION 1006:

Which of the following is NOT a major element of Business Continuity Planning?
A.) Creation of a BCP committee
B.) Business Impact Assessment (BIA)
C.) Business Continuity Plan Development
D.) Scope plan initiation

Answer: A

QUESTION 1007:

Which one of the following is a core infrastructure and service element of Business Continuity Planning (BCP) required to effectively support the business processes of an organization?

A. Internal and external support functions.
B. The change management process.
C. The risk management process.
D. Backup and restoration functions.

Answer: C
Pg 383 Krutz Gold Edition. Backup is not BCP.

QUESTION 1008:

A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern?
A.) Marketing/Public relations
B.) Data/Telecomm/IS facilities
C.) IS Operations
D.) Facilities security

Answer: B

QUESTION 1009:

When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?
A.) Executive management staff
B.) Senior business unit management
C.) BCP committee
D.) Functional business units

Answer: B

QUESTION 1010:

Classification of information systems is essential in business continuity planning. Which of the following system types can not be replaced by manual methods?
A.) Critical System
B.) Vital System
C.) Sensitive System
D.) Non-critical system

Answer: A

QUESTION 1011:

A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern?
A.) Marketing/Public Relations
B.) Data/Telecomm/IS facilities
C.) IS Operations
D.) Facilities security

Answer: B

QUESTION 1012:

Business Continuity Plan development depends most on:
A.) Directives of Senior Management
B.) Business Impact Analysis (BIA)
C.) Scope and Plan Initiation
D.) Skills of BCP committee

Answer: B

QUESTION 1013:

Which primary element of BCP includes carrying out vulnerability analysis?
A.) Scope and Plan Initiation
B.) Business Impact Assessment
C.) Business Continuity Plan Development
D.) Plan Approval and Implementation

Answer: B

QUESTION 1014:

To mitigate the impact of a software vendor going out of business, a company that uses vendor software should require which one of the following?

A. Detailed credit investigation prior to acquisition.
B. Source code held in escrow.
C. Standby contracts with other vendors.
D. Substantial penalties for breech of contract.'

Answer: B
The original answer was C however this is incorrect for this case. SLA and standby are good ideas but in this case B
is right.
"A software escrow arrangement is a unique tool used to protect a company against the failure of a software developer to provide adequate support for its products or against the possibility that the developer will go out of business and no technical support will be available for the product....Under a software escrow agreement, the developer provides copies of the application source code to an independent third-party organization. The third party
then maintains updated backup copies of the source code in a secure fashion. The agreement between the end user
and the developer specifies "trigger events", such as the failure of the developer to meet terms of a service level agreement (SLA) or the liquidation of the developer's firm." - Ed Tittle CISSP Study Guide (sybex) pg 550

QUESTION 1015:

Similarity between all recovery plans is:
A.) They need extensive testing
B.) They need to be developed by business continuity experts
C.) They become obsolete quickly
D.) The create employment opportunities

Answer: C

QUESTION 1016:

Which of the following focuses on sustaining an organizations business functions during and after a disruption?
A.) Business continuity plan
B.) Business recovery plan
C.) Continuity of operations plan
D.) Disaster recovery plan

Answer: A

QUESTION 1017:

What is not one of the drawbacks of a hot site?
A.) Need Security controls, as it usually contain mirror copies of live production data
B.) Full redundancy in hardware, software, communication lines, and applications lines is very expensive
C.) The hot sites are available immediately or within maximum allowable downtime (MTD)
D.) They are administratively resource intensive, as transaction redundancy controls need to be implemented to keep data up-to-date

Answer: C

QUESTION 1018:

Which one of the following processing alternatives involves a ready-to-use computing facility with telecommunications equipment, but not computers?

A. Company-owned hot site
B. Commercial hot site
C. Cold site
D. Warm site

Answer: D
"Warm Site - These facilities are usually partially configured with some equipment, but not the actual computers." - Shon Harris All-in-one CISSP Certification Guide pg 613

QUESTION 1019:

What is a hot-site facility?
A.) A site with pre-installed computers, raised flooring, air conditioning, telecommunications, and networking equipment, and UPS
B.) A site is which space is reserved with pre-installed wiring and raised floors
C.) A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS
D.) A site with ready made work space with telecommunications equipment, LANs, PCs, and terminals with work groups

Answer: A

QUESTION 1020:

Contracts and agreements are unenforceable in which of the following alternate back facilities?
A.) hot site
B.) warm site
C.) cold site
D.) reciprocal agreement

Answer: D

QUESTION 1021:

Which of the following computer recovery sites is the least expensive and the most difficulty to test?
A.) non-mobile hot site
B.) mobile hot site
C.) warm site
D.) cold site

Answer: D

QUESTION 1022:

Which of the following is an advantage of the use of hot sites as a backup alternative?
A.) The costs associated with hot sites are low
B.) Hot sites can be made ready for operation within a short period of time
C.) Hot sites can be used for an extended amount of time
D.) Hot sites do not require that equipment and systems software be compatible with the primary installation being backed up

Answer: B

QUESTION 1023:

What is not a benefit of Cold Sites?
A.) No resource contention with other organization
B.) Quick Recovery
C.) Geographical location that is not affected by the same disaster
D.) low cost

Answer: B

QUESTION 1024:

What is the PRIMARY reason that reciprocal agreements between independent organizations for backup processing
capability are seldom used?

A. Lack of successful recoveries using reciprocal agreements.
B. Legal liability of the host site in the event that the recovery fails.
C. Dissimilar equipment used by disaster recovery organization members.
D. Difficulty in enforcing the reciprocal agreement.

Answer: D
"Reciprocal agreements are at best a secondary option for disaster protection. The agreements are not enforceable, so there is no guarantee that this facility will really be available to the company in a time of need." Pg 615 Shon Harris CISSP All-In-One Certification Exam Guide

---

QUESTION 1025:

Which of the following alternative business recovery strategies would be LEAST appropriate in a large database and on-line communications network environment where the critical business continuity period is 7 days?
A.) Hot site
B.) Warm site
C.) Duplicate information processing facilities
D.) Reciprocal agreement

Answer: D

QUESTION 1026:

A contingency plan should address:
A.) Potential risks
B.) Residual risks
C.) Identified risks
D.) All of the above

Answer: B

QUESTION 1027:

Prior to a live disaster test, which of the following is most important?
A.) Restore all files in preparation for the test
B.) Document expected findings
C.) Arrange physical security for the test site
D.) Conduct a successful structured walk-through

Answer: D

QUESTION 1028:

Which of the following business continuity stages ensures the continuity strategy remains visible?

A. Backup, Recover and Restoration
B. Testing Strategy Development
C. Post Recovery Transition Data Development
D. Implementation, Testing and Maintenance

Answer: D
Once the strategies have been decided upon, they need to be documented and put into place. This moves the efforts from a purely planning stage to an actual implementation and action phase...The disaster recovery and continuity plan should be tested periodically because an environment continually changes and each time it is tested, more improvements may be uncovered...The plan's maintenance can be incorporated into change management procedures so that any changes in the environment will be sure to be reflected in the plan itself. - Shon Harris All-in-one CISSP Certification Guide pg 611

QUESTION 1029:

During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?
A.) Measurement of accuracy
B.) Elapsed time for completion of critical tasks
C.) Quantitatively measuring the results of the test
D.) Evaluation of the observed test results

Answer: C

QUESTION 1030:

Which of the following recovery plan test results would be most useful to management?

A.) elapsed time to perform various activities
B.) list of successful and unsuccessful activities
C.) amount of work completed
D.) description of each activity

Answer: B

QUESTION 1031:

Failure of a contingency plan is usually:
A.) A technical failure
B.) A management failure
C.) Because of a lack of awareness
D.) Because of a lack of training

Answer: B

QUESTION 1032:

The first step in contingency planning is to perform:
A.) A hardware backup
B.) A data backup
C.) An operating system software backup
D.) An application software backup

Answer: B

QUESTION 1033:

Which of the following server contingency solutions offers the highest availability?
A.) System backups
B.) Electronic vaulting/remote journaling
C.) Redundant arrays of independent disks (RAID)
D.) Load balancing/disk replication

Answer: D

QUESTION 1034:

Which of the following statement pertaining to the maintenance of an IT contingency plan is incorrect?
A.) The plan should be reviewed at least once a year for accuracy and completeness
B.) The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan
C.) Strict version control should be maintained
D.) Copies of the plan should be provided to recovery personnel for storage at home and office

Answer: B

QUESTION 1035:

Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?
A.) Simulation test
B.) Checklist test
C.) Parallel test
D.) Structured walkthrough test

Answer: D
"Structured walk-through:
1. Functional representatives meet to review the plan in detail
2. Strategy involves a thorough look at each of the plan steps and the procedures that are invoked at that point in the plan
3. This ensures that the actual planned activities are accurately described in the plan.
Pg 699 Hansche: Official (ISC)2 Guide to the CISSP Exam

QUESTION 1036:

What is the MAIN purpose of periodically testing off-site hardware backup facilities?
A.) To eliminate the need to develop detailed contingency plans
B.) To ensure that program and system documentation remains current
C.) To ensure the integrity of the data in the database
D.) To ensure the continued compatibility of the contingency facilities

Answer: D

QUESTION 1037:

Scheduled tests of application contingency plans should be based on the

A. Size and complexity of the application.
B. Number of changes to the application.
C. Criticality of the application.
D. Reliability of the application.

Answer: C
All though not directly answering the question a little inference lead to this
"Priorities - It is extremely important to know what is critical versus nice to have... It is necessary to know which department must come online first, which second, and so on...It maybe more necessary to ensure that the database is up and running before working to bring the file server online." - Shon Harris All-in-one CISSP Certification Guide pg 604

QUESTION 1038:

Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?
A.) Contact information for all personnel
B.) Vendor contract information, including offsite storage and alternate site
C.) Equipment ad system requirements lists of hardware, software, firmware, and other resources required to support system operations
D.) The Business Impact Analysis

Answer: D

Explanation: You use the BIA as a guideline to create the contingency plan.

QUESTION 1039:

The first step in contingency planning is to perform:
A.) A hardware backup
B.) A data backup
C.) An operating system software backup
D.) An application software backup

Answer: B

QUESTION 1040:

Which of the following teams should not be included in an organization's contingency plan?
A.) Damage assessment team
B.) Hardware salvage team
C.) Tiger team
D.) Legal affairs team

Answer: C

QUESTION 1041:

In the public sector, as opposed to the private sector, due care is usually determined by

A. Minimum standard requirements.
B. Legislative requirements.
C. Insurance rates.
D. Potential for litigation.

Answer: B

QUESTION 1042:

What is the minimum and customary practice of responsible protection of assets that affects a community or societal norm?

A. Due diligence
B. Risk mitigation
C. Asset protection
D. Due care

Answer: D
"Due care and due diligence are terms that are used throughout this book. Due diligence is the act of investigating and understanding the risks the company faces. A company practices due care by developing security policies, procedures, and standards. Due care shows that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees from possible risks. So due diligence is understanding the current threats and risks and due care is implementing countermeasures to provide protection from those threats. If a company does not practice due care and due diligence pertaining to the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence." Pg. 85 Shon Harris: All-in-One CISSP Certification
"The following list describes some of the actions required to show that due care is being properly practiced in a corporation:
1. Adequate physical and logical access controls
2. Adequate telecommunication security, which could require encryption
3. Proper information, application, and hardware backups
4. Disaster recovery and business continuity plans
5. Periodic review, drills, tests, and improvement in disaster recovery and business continuity plans
6. Properly informing employees of expected behavior and ramifications of not following these expectations
7. Developing a security policy, standards, procedures, and guidelines
8. Performing security awareness training
9. Running updated antivirus software
10. Periodically performing penetration tests from outside and inside the network
11. Implementing dial-back or preset dialing features on remote access applications
12. Abiding by and updating external service level agreements (SLAs)
13. Ensuring that downstream security responsibilities are being met
14. Implementing measures that ensure that software piracy is not taking place
15. Ensuring the proper auditing and reviewing of those audit logs are taking place
16. Conducting background checks on potential employees"
Pg. 616 Shon Harris: All-in-One CISSP Certification

QUESTION 1043:

Under the standard of due care, failure to achieve the minimum standards would be

considered

A. Negligent
B. Unethical
C. Abusive
D. Illegal

Answer: A
Due Care: care which an ordinary prudent person would have exercised under the same or similar circumstances. "Due Care" and "Reasonable Care" are used interchangeably. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 896

QUESTION 1044:

Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:
A.) the company is not a multi-national company
B.) they have not exercised due care protecting computing resources
C.) they have failed to properly insure computer resources against loss
D.) the company does not prosecute the hacker that caused the breach

Answer: B

QUESTION 1045:

The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (C) of instituting the protection versus the estimated loss (L) resulting from the exploitation f the corresponding vulnerability. Therefore, a legal liability exists when?
A.) C < L
B.) C < L - (residual risk)
C.) C > L
D.) C > L - (residual risk)

Answer: A

QUESTION 1046:

When companies come together to work in an integrated manner such as extranets, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability and responsibility. These aspects should be defined in the contracts that each party signs. What describes this type of liability?
A.) Cascade liabilities
B.) Downstream liabilities
C.) Down-flow liabilities
D.) Down-set liabilities

Answer: B
"When companies come together to work in an integrated manner, such as extranets and VANs, special care must be taken to ensure that teach party promises to provide the necessary level of protection, liability, and responsibility needed, which should be clearly defined in the contracts that each party signs. Auditing and testing should be performed to ensure that each party is indeed holding up its side of the bargain and that its technology integrates properly with all other parties. Interoperability can become a large, frustrating, and expensive issue in these types of arrangements.
If one of the companies does no provide the necessary level of protection and their negligence affects a partner they are working with, the affected company can sue the upstream company. For example, let's say company A and company B have constructed an extranet. Company A does not put in controls to detect and del with viruses. Company A gets infected with a destructive virus and it is spread to company B through the extranet. The virus corrupts critical data and causes massive disruption to company B's production. Company B can sue company A for being negligent. Both companies need to make sure that they are doing their part to ensure that their activities, or lack of them, will not negatively affect another company, which is referred to as downstream liability." Pg 616 Shon Harris: All-in-One CISSP Certification

---

QUESTION 1047:

The typical computer felons are usually persons with which of the following characteristics?
A.) The have had previous contact with law enforcement
B.) The conspire with others
C.) They hold a position of trust
D.) They deviate from the accepted norms of security

Answer: D

QUESTION 1048:

Which of the following is responsible for the most security issues?
A.) Outside espionage
B.) Hackers
C.) Personnel
D.) Equipment Failure

Answer: C

QUESTION 1049:

Hackers are most often interested in:
A.) Helping the community in securing their networks
B.) Seeing how far their skills wll take them
C.) Getting recognition for their actions

D.) Money

Answer: B

QUESTION 1050:

Which of the following categories of hackers poses the greatest threat?
A.) Disgruntled employees
B.) Student hackers
C.) Criminal hackers
D.) Corporate spies

Answer: A

QUESTION 1051:

Individuals who have their sole aim as breaking into a computer system are being referred to as:

A. Crackers
B. Sniffers
C. Hackers
D. None of the choices.

Answer: A

Explanation:
Crackers are individuals who try to break into a computer system. The term was coined in the mid-80s by hackers who wanted to differentiate themselves from individuals whose sole purpose is to sneak through security systems. Whereas crackers sole aim is to break into secure systems, hackers are more interested in gaining knowledge about computer systems and possibly using this knowledge for playful pranks. Although hackers still argue that there's a big difference between what they do and what crackers do, the mass media has failed to understand the distinction, so the two terms -- hack and crack -- are often used interchangeably.

QUESTION 1052:

Which of the following tools is less likely to be used by a hacker?
A.) l0phtcrack
B.) Tripwire
C.) Crack
D.) John the ripper

Answer: B
"Other security packages, such as the popular Tripwire data integrity assurance packages, also provide a secondary antivirus functionality. Tripwire is designed to alert administrators of

unauthorized file modifications. It's often used to detect web server defacements and similar attacks, but it also may provide some warning of virus infections if critical system executable files, such as COMMAND.COM, are modified unexpectedly. These systems work by maintaining a database of hash values for all files stored on the system. These archive hash values are then compared to current computed values to detect any files that were modified between the two periods." Pg. 224 Tittel: CISSP Study Guide

---

QUESTION 1053:

Which of the following tools is not likely to be used by a hacker?
A.) Nessus
B.) Saint
C.) Tripwire
D.) Nmap

Answer: C

QUESTION 1054:

Supporting evidence used to help prove an idea of point is described as? It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence:
A.) Circumstantial evidence
B.) Corroborative evidence
C.) Opinion evidence
D.) Secondary evidence

Answer: B

QUESTION 1055:

Which of the following would best describe secondary evidence?
A.) Oral testimony by a non-expert witness
B.) Oral testimony by an expert witness
C.) A copy of a piece of evidence
D.) Evidence that proves a specific act

Answer: C

QUESTION 1056:

Which of the following exceptions is less likely to make hearsay evidence admissible in court?
A.) Records are collected during the regular conduct of business
B.) Records are collected by senior or executive management
C.) Records are collected at or near the time of occurrence of the act being investigated
D.) Records are in the custody of the witness on a regular basis

Answer: B

QUESTION 1057:

Once evidence is seized, a law enforcement officer should emphasize which of the following?
A.) chain of command
B.) chain of custody
C.) chain of control
D.) chain of communications

Answer: B

QUESTION 1058:

Which of the following rules is less likely to allow computer evidence to be admissible in court?
A.) It must prove a fact that is material to the case
B.) Its reliability must be proven
C.) The process for producing it must be documented
D.) The chain of custody of evidence must show who collected, security, controlled, handled, transported, and tampered with the evidence

Answer: C

QUESTION 1059:

A copy of evidence or oral description of this contents; not reliable as best evidence is what type of evidence?
A.) Direct evidence
B.) Circumstantial evidence
C.) Hearsay evidence
D.) Secondary evidence

Answer: D

QUESTION 1060:

What is defined as inference of information from other, intermediate, relevant facts?
A.) Secondary evidence
B.) Conclusive evidence
C.) Hearsay evidence
D.) Circumstantial evidence

Answer: D

QUESTION 1061:

In order to be able to successfully prosecute an intruder:
A.) A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B.) A proper chain of custody of evidence has to be preserved
C.) Collection of evidence has to be done following predefined procedures
D.) Whenever possible, analyze, a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence

Answer: B

QUESTION 1062:

Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?
A.) direct evidence
B.) best evidence
C.) conclusive evidence
D.) hearsay evidence

Answer: A

QUESTION 1063:

In order to preserver a proper chain of custody of evidence?
A.) Evidence has to be collected following predefined procedures in accordance with all laws and legal regulations
B.) Law enforcement officials should be contacted for advice on how and when to collect critical information
C.) Verifiable documentation indicating the sequence of individuals who have handled a piece of evidence should be available.
D.) Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.

Answer: A

QUESTION 1064:

What is the primary reason for the chain of custody of evidence?
A.) To ensure that no evidence is lost
B.) To ensure that all possible evidence is gathered
C.) To ensure that it will be admissible in court
D.) To ensure that incidents were handled with due care and due diligence

Answer: C

QUESTION 1065:

Which element must computer evidence have to be admissible in court?
A.) It must be relevant
B.) It must be annotated
C.) It must be printed
D.) t must contain source code

Answer: A

QUESTION 1066:

Which kind of evidence would printed business records, manuals, and, printouts classify as?
A.) Direct evidence
B.) Real evidence
C.) Documentary evidence
D.) Demonstrative evidence

Answer: B

QUESTION 1067:

Since disks and other magnetic media are only copies of the actual or original evidence, what type of evidence are they are often considered to represent?
A.) Hearsay
B.) Irrelevant
C.) Incomplete
D.) Secondary

Answer: A

QUESTION 1068:

Which of the following is LEAST necessary when creating evidence tags detailing the chain of custody for electronic evidence?

A. The mode and means of transportation.
B. Notifying the person who owns the information being seized.
C. Complete description of the evidence, including quality if necessary.
D. Who received the evidence.

Answer: B

The references indicate that transportation is important.
Each piece of evidence should be marked in some way with the date, time, initials of the collector, and a case number if one has been assigned...The pieces of evidence should then be sealed in a container and the container should be marked with the same information. The container should be sealed with evidence tape and if possible, the
writing should be on the tape so a broken seal can be detected. - Shon Harris All-in-one CISSP Certification Guide pg 673
In many cases, it is not possible for a witness to uniquely identify an object in court. In those cases, a chain of evidence must be established. This involves everyone who handles evidence - including the police who originally collect it, the evidence technicians who process it, and the lawyers who use it in court. The location of the evidence must be fully documented from the moment it was collected to the moment it appears in court to ensure that it is indeed the same item. This requires thorough labeling of evidence and comprehensive logs noting who had access to the evidence at specific times and the reasons they required such access." Pg. 593 Tittel: CISSP Study Guide.
The evidence life cycle covers the evidence gathering and application process. This life cycle has the following components:
Discovery and recognition
Protection
Recording
Collection
Collect all relevant storage media
Make image of hard disk before removing power
Print out screen
Avoid degaussing equipment
Identification
Preservation
Protect magnetic media from erasure
Store in proper environment
Transportation
Presentation in a court of law
Return of evidence to owner
Pg. 309 Krutz: The CISSP Prep Guide
The life cycle of evidence includes
* Collection and identification
* Storage, preservation, and transportation
* Presentation in court
* Being returned to victim or owner
Pg 677 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 1069:

To be admissible in court, computer evidence must be which of the following?
A.) relevant
B.) decrypted
C.) edited

D.) incriminating

Answer: A

QUESTION 1070:

Computer-generated evidence is considered:
A.) Best evidence
B.) Second hand evidence
C.) Demonstrative evidence
D.) Direct evidence

Answer: B
"Most of the time, computer-related documents are considered hearsay, meaning the evidence is secondhand evidence. Hearsay evidence is not normally admissible in court unless it has firsthand evidence that can be used to prove the evidence's accuracy, trustworthiness, and reliability, such as a businessperson who generated the computer logs and collected them." Pg. 630 Shon Harris: All-in-One CISSP Certification

---

QUESTION 1071:

Why would a memory dump be admissible as evidence in court?
A.) Because it is used to demonstrate the truth of the contents
B.) Because it is used to identify the state of the system
C.) Because the state of the memory cannot be used as avidence
D.) Because of the exclusionary rule

Answer: B

QUESTION 1072:

Evidence corroboration is achieved by

A. Creating multiple logs using more than one utility.
B. Establishing secure procedures for authenticating users.
C. Maintaining all evidence under the control of an independent source.
D. Implementing disk mirroring on all devices where log files are stored.

Answer: C
Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is
used as a supplementary tool to help prove a primary piece of evidence. - Shon Harris All-in-one CISSP Certification Guide pg 678

QUESTION 1073:

You are documenting a possible computer attack.
Which one of the following methods is NOT appropriate for legal record keeping?

A. A bound paper notebook.
B. An electronic mail document.
C. A personal computer in "capture" mode that prints immediately.
D. Microcassette recorder for verbal notes

Answer: D

QUESTION 1074:

Which one of the following is NOT a requirement before a search warrant can be issued?

A. There is a probable cause that a crime has been committed.
B. There is an expectation that evidence exists of the crime.
C. There is probable cause to enter someone's home or business.
D. There is a written document detailing the anticipated evidence.

Answer: D
"If a computer crime is suspected, it is important not to alert the suspect. A preliminary investigation should be conducted to determine weather a crime has been committed by examining the audit records and system logs, interviewing witnesses, and assessing the damage incurred....Search warrants are issued when there is a probable cause for the search and provide legal authorization to search a location for specific evidence." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 436

QUESTION 1075:

Once a decision is made to further investigate a computer crime incident, which one of the following is NOT employed?

A. Identifying what type of system is to be seized.
B. Identifying the search and seizure team members.
C. Identifying the cost of damage and plan for their recover.
D. Determining the risk that the suspect will destroy evidence.

Answer: C
Costs and how to recover are not considered in a computer crime scene incident.

QUESTION 1076:

From a legal perspective, which of the following rules must be addressed when investigating a computer crime?

A. Search and seizure

B. Data protection
C. Engagement
D. Evidence

Answer: D
"The gathering, control, storage and preservation of evidence are extremely critical in any legal investigation." Pg
432 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 1077:

Which of the following is not a problem regarding computer investigation issues?
A.) Information is intangible
B.) Evidence is difficult to gather
C.) Computer-generated records are only considered secondary evidence, thus are no as reliable as best evidence
D.) In many instances, an expert or specialist is required

Answer: D

QUESTION 1078:

Why is the investigation of computer crime involving malicious damage especially challenging?

A. Information stored in a computer is intangible evidence.
B. Evidence may be destroyed in an attempt to restore the system.
C. Isolating criminal activity in a detailed audit log is difficult.
D. Reports resulting from common user error often obscure the actual violation.

Answer: B
The gathering, control, storage, and preservation of evidence are extremely critical in any legal investigation. Because evidence involved in a computer crime might be intangible and subject to easy modification without a trace, evidence must be carefully handled and controlled throughout its entire life cycle. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 432

QUESTION 1079:

After law enforcement is informed of a computer crime, the organization's investigators constraints are

A. removed.
B. reduced.
C. increased.
D. unchanged.

Answer: C
"On the other hand, there are also two major factors that may cause a company to shy away from calling in the authorities. First, the investigation will more than likely become public and may embarrass the company. Second, law enforcement authorities are bound to conduct an investigation that complies with the Fourth Amendment and other legal requirements that may not apply to a private investigation." Pg. 529 Tittel: CISSP Study Guide

---

QUESTION 1080:

To understand the "whys" in crime, many times it is necessary to understand MOM.
Which of the following is not a component of MOM?
A.)Opportunities
B.) Methods
C.) Motivation
D.) Means

Answer: B
Reference: pg 600 Shon Harris: All-in-One CISSP Certification

---

QUESTION 1081:

What category of law deals with regulatory standards that regulate performance and conduct? Government agencies create these standards, which are usually applied to companies and individuals within those companies.
A.) Standards law
B.) Conduct law
C.) Compliance law
D.) Administrative law

Answer: D

QUESTION 1082:

Something that is proprietary to that company and importance for its survival and profitability is what type of intellectual property law?
A.) Trade Property
B.) Trade Asset
C.) Patent
D.) Trade Secret

Answer: D

QUESTION 1083:

Which of the following statements regarding trade secrets is false?
A.) For a company to have a resource qualify as a trade secret, it must provide the company with

some type of competitive value or advantage
B.) The Trade Secret Law normally protects the expression of the idea of the resource.
C.) Many companies require their employees to sign nondisclosure agreements regarding the protection of their trade secrets
D.) A resource can be protected by law if it is not generally known and if it requires special skill, ingenuity, and/or expenditure of money and effort to develop it

Answer: B

QUESTION 1084:

Which category of law is also referenced as a Tort law?
A.) Civil law
B.) Criminal law
C.) Administrative law
D.) Public law

Answer: A

QUESTION 1085:

Which of the following European Union (EU) principles pertaining to the protection of information on private individuals is incorrect?
A.) Data collected by an organization can be used for any purpose and for as long as necessary, as long as it is never communicated outside of the organization by which it was collected
B.) Individuals have the right to correct errors contained in their personal data
C.) Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited.
D.) Records kept on an individual should be accurate and up to date

Answer: B

QUESTION 1086:

A country that fails to legally protect personal data in order to attract companies engaged in collection of such data is referred to as a

A. data pirate
B. data haven
C. country of convenience
D. sanctional nation

Answer: B
Correct answer is B. Data Haven.
Data Haven
A place where data that cannot legally be kept can be stashed for later use; an offshore web host.

This is an interesting topic; companies often need information that they are not legally allowed to know. For example, some hospitals are not allowed to mark patients as HIV positive (because it stigmatizes patients); staff members create codes or other ways so can take the necessary steps to protect themselves.
http://www.technovelgy.com/ct/content.asp?Bnum=279
DATA HAVEN
This phrase has been around for at least 15 years, but only in a specialist way. One sense is that of a place of safety and security for electronic information, for example where encrypted copies of crucial data can be stored as a backup away from one's place of business. But it can also mean a site in which data can be stored outside the jurisdiction of regulatory authorities. This sense has come to wider public notice recently as a result of Neal Stephenson's book Cryptonomicon, in which the establishment of such a haven in South East Asia is part of the plot. In a classic case of life imitating art, there is now a proposal to set up a data haven on one of the old World War Two forts off the east coast of Britain, which declared independence under the name of Sealand back in 1967 (it issues its own stamps and money, for example). The idea is to get round a proposed British law-the Regulation of Investigatory Powers Bill (RIP)-that would force firms to hand over decryption keys if a crime is suspected and make Internet providers install equipment to allow interception of e-mails by the security services.
The Privacy Act doesn't protect information from being transferred from New Zealand to data havens-countries that don't have adequate privacy protection.
[Computerworld, May 1999]
The government last night poured cold water on a plan by a group of entrepreneurs to establish a "data haven" on a rusting iron fortress in the North Sea in an attempt to circumvent new anti-cryptography laws.
[Guardian, June 2000]
World Wide Words is copyright (c) Michael Quinion, 1996-2004.
All rights reserved. Contact the author for reproduction requests.
Comments and feedback are always welcome.
Page created 17 June 2000; last updated October 2002.
http://www.worldwidewords.org/turnsofphrase/tp-dat2.htm
Not C: The majority google searches for 'Country of Convenience' relate to those countries supporting terrorism.
Not D: the meaning of sanctioned is listed below. This would mean that countries that DON'T protect privacy are APPROVED
Main Entry: 2sanction
Function: transitive verb
Inflected Form(s): sanc*tioned; sanc*tion*ing
Date: 1778
1 to make valid or binding usually by a formal procedure (as ratification)
2 to give effective or authoritative approval or consent

QUESTION 1087:

Which of the following requires all communications carriers to make wiretaps possible?
A.) 1994 U.S. Communications Assistance for Law Enforcement Act
B.) 1996 U.S. Economic and Protection of Property Information Act

C.) 1996 U.S. National Information Infrastructure Protection Act
D.) 1986 U.S. Computer Security Act

Answer: A

QUESTION 1088:

Which of the following U.S. federal government laws/regulations was the first to require the development of computer security plan?
A.) Privacy Act of 1974
B.) Computer Security Act of 1987
C.) Federal Information Resources Management Regulations
D.) Office of Management & Budget Circular A-130

Answer: B
Reference: pg 722 Hansche: Official (ISC)2 Guide to the CISSP Exam

---

QUESTION 1089:

Which U.S. act places responsibility on senior organizational management for prevention and detection programs with fines of up to $290 million for nonperformance?
A.) The 1987 U.S. Computer Security Act
B.) The 1986 U.S. Computer Fraud and Abuse Act
C.) The 1991 U.S. Federal Sentencing Guidelines
D.) The 1996 U.S. National Information Infrastructure Protection Act

Answer: C
Reference: pg 615 Shon Harris: All-in-One CISSP Certification

---

QUESTION 1090:

What document made theft no longer restricted to physical constraints?
A.) The Electronic Espionage Act of 1996
B.) The Gramm Leach Bliley Act of 1999
C.) The Computer Security Act of 1987
D.) The Federal Privacy Act of 1974

Answer: A

QUESTION 1091:

In the US, HIPPA addresses which of the following?
A.) Availability and Accountability
B.) Accuracy and Privacy
C.) Security and Availability
D.) Security and Privacy

Answer: D

QUESTION 1092:

Which of the following placed requirements of federal government agencies to conduct security-related training, to identify sensitive systems, and to develop a security plan for those sensitive systems?
A.) 1987 U.S. Computer Security Act
B.) 1996 U.S. Economic and Protection of Proprietary Information Act
C.) 1994 U.S. Computer Abuse Amendments Act
D.) 1986 (Amended in 1996) U.S. Computer Fraud and Abuse Act

Answer: A

QUESTION 1093:

Which of the following cannot be undertaken in conjunction with computer incident handling?
A.) system development activity
B.) help-desk function
C.) system backup function
D.) risk management process

Answer: A

QUESTION 1094:

What is the primary goal of incident handling?

A.) Successfully retrieve all evidence that can be used to prosecute
B.) Improve the company's ability to be prepared for threats and disasters
C.) Improve the company's disaster recovery plan
D.) Contain and repair any damage caused by an event

Answer: D
Reference: Page 629 of Shon Harris's All in One Exam Guide, Second Ed.

QUESTION 1095:

Which one of the following is NOT a factor to consider when establishing a core incident response team?

A. Technical knowledge
B. Communication skills
C. The recovery capability

D. Understanding business policy

Answer: C
The team should have someone from senior management, the network administrator, security officer, possibly a network engineer and /or programmer, and liaison for public affairs...The incident response team should have the following basic items
List of outside agencies and resources to contact or report to
List of computer or forensics experts to contact
Steps on how to secure and preserve evidence
Steps on how to search for evidence
List of items that should be included on the report
A list that indicates how the different systems should be treated in this type of situation (removed from internet, removed from the network, and powered down) - Shon Harris
All-in-one CISSP Certification Guide pg 671-672
..an investigation should involve management, corporate security, human resources, the legal department, and other appropriate staff members. The act of investigating may also affect critical operations...Thus it is important to prepare a plan beforehand on how to handle reports of suspected computer crimes. A committee of appropriate personnel should be set up beforehand to address the following issues
Establishing a prior liaison with law enforcement
Deciding when and whether to bring in law enforcement...
Setting up means of reporting computer crimes
Establishing procedures for handling and processing reports of computer crime
Planning for and conducting investigations
Involving senior management and the appropriate departments, such as legal, internal audit, information systems, and human resources
Ensuring the proper collection of evidence, which includes identification and protection of the various storage media. -Ronald Krutz The CISSP PREP Guide (gold edition) pg 435-436

QUESTION 1096:

Which of the following specifically addresses cyber attacks against an organization's IT systems?
A.) Continuity of support plan
B.) Business continuity plan
C.) Incident response plan
D.) Continuity of operations plan

Answer: C

QUESTION 1097:

When should a post-mortem review meeting be held after an intrusion has been properly taken care of?
A.) Within the first three months after the investigation of the intrusion is completed
B.) Within the first week after prosecution of intruders have taken place, weather successful or

not
C.) Within the first month after the investigation of the intrusion is completed
D.) Within the first week of completing the investigation of the intrusion

Answer: D

QUESTION 1098:

During a review of system logs of the enterprise, a security manager discovers that a colleague working on an exercise ran a job to collect confidential information on the company's clients. The colleague who ran the job has since left the company to work for a competitor. Based on the (ISC) Code of Ethics, which one of the following statements is MOST correct?

A. The manager should call the colleague and explain what has been discovered.
The manager should then ask for the return of the information in exchange for silence.
B. The manager should warn the competitor that a potential crime has been committed that could put their company
at risk.
C. The manager should inform his or her appropriate company management, and secure the results of the recover
exercise for future review.
D. The manager should call the colleague and ask the purpose of running the job prior to informing his or her company management of the situation.

Answer: C
In the references I have not found out anything that directly relates to this but It would be logical to assume the answer of going to necessary management.
"ISC2 Code of Ethics....
...Not commit or be party to any unlawful or unethical act that may negatively affect their professional reputation or the reputation of their profession.
...Appropriately report activity related to the profession that they believe to be unlawful and shall cooperate with the resulting investigations." -Ronald Krutz The CISSP PREP Guide (gold edition) pg 440

QUESTION 1099:

In what way could the use of "cookies" violate a person's privacy?

A. When they are used to tie together a set of unconnected requests for web pages to cause an electronic map of where one has been.
B. When they are used to keep logs of who is using an anonymizer to access a site instead of their regular userid.
C. When the e-mail addresses of users that have registered to access the web site are sold to marketing firms.

Answer: A
Both A and C are correct in that they are true but from a CISSP viewpoint looking into a PC the cookies

show a map of where the user has been. Therefore I think A is the better choice.
"Any web site that knows your identity and has cookie for you could set up procedures to exchange their data with
the companies that buy advertising space from them, synchronizing the cookies they both have on your computer.
This possibility means that once your identity becomes known to a single company listed in your cookies file, any
of the others might know who you are every time you visit their sites.
The result is that a web site about gardening that you never told your name could sell not only your name to mail-order companies, but also the fact that you spent a lot of time one Saturday night last June reading about how
to fertilize roses. More disturbing scenarios along the same lines could be imagined."
http://www.junkbusters.com/cookies.html

QUESTION 1100:

Which of the following is the BEST way to prevent software license violations?
A.) Implementing a corporate policy on copyright infringements and software use
B.) Requiring that all PC's be diskless workstations
C.) Installing metering software on the LAN so applications can be accessed through the metered software
D.) Regularly scanning used PC's to ensure that unauthorized copies of software have not been loaded on the PC

Answer: D

QUESTION 1101:

The ISC2 Code of Ethics does not include which of the following behaviors for a CISSP:
A.) moral
B.) ethical
C.) legal
D.) control

Answer: D

QUESTION 1102:

Where can the phrase "Discourage unsafe practice" be found?
A.) Computer Ethics Institute commandments
B.) (ISC)2 Code of Ethics
C.) Internet Activities Board's Ethics and the Internet (RFC1087)
D.) CIAC Guidelines

Answer: B

QUESTION 1103:

One of the offences an individual or company can commit is decompiling vendor code. This is usually done in the hopes of understanding the intricate details of its functionality. What best describes this type of non-ethical engineering?
A.) Inverse Engineering
B.) Backward Engineering
C.) Subvert Engineering
D.) Reverse Engineering

Answer: D

QUESTION 1104:

Which one of the following is an ethical consideration of computer technology?

A. Ownership of proprietary software.
B. Information resource management.
C. Service level agreements.
D. System implementation and design.

Answer: A
can only assume that they mean piracy or something.

QUESTION 1105:

The Internet Activities Board characterizes which of the following as unethical behavior for Internet users?
A.) Writing computer viruses
B.) Monitoring data traffic
C.) Westing computer resources
D.) Concealing unauthorized accesses

Answer: D

QUESTION 1106:

Which of the following is a potential problem when creating a message digest for forensic purposes?

A. The process if very slow.
B. The file's last access time is changed.
C. The message digest is almost as long as the data string.
D. One-way hashing technology invalidates message digest processing.

Answer: D

Not C.
"To generate a digital signature, the digital signal program passes the file to be sent through a one-way hash function. This hash function produces a fixed size output from a variable size input." Pg. 208 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 1107:

A forensic examination should inspect slack space because it

A. Contains system level access control kernel.
B. Can contain a hidden file or data.
C. Can contain vital system information.
D. Can be defeted to avoid detection.

Answer: B

QUESTION 1108:

Forensic imaging of a workstation is initiated by

A. Booting the machine with the installed operating system.
B. Booting the machine with an operating system diskette.
C. Removing the hard drive to view the output of the forensic imaging software.
D. Directing the output of the forensic imaging software to the small computer system interface (SCSI).

Answer: D
"It is very important that the person, or people, conducting the forensics investigation is skilled in this trade and knows what to look out for. If a person reboots the attacked system or goes around looking at different files, it could corrupt viable evidence, change timestamps on key files, and erase footprints the criminal may have left. One very good first step is to make a sound image of the attacked system and perform forensic analysis on this copy. This will ensure that the evidence stays unharmed on the original system in case some steps in the investigation actually corrupt or destroy data. Also the memory of the system should be dumped to a file before doing any work on the system or powering it down." - Shon Harris All-in-one CISSP Certification Guide pg 672-673
PCMCIA to SCSI and parallel to SCSI forensic products can be found at the following vendor.
http://www.icsforensic.com/products_cat_fr.cfm

QUESTION 1109:

A disk image backup is used for forensic investigation because it

A. Is based on secured hardware technology.
B. Creates a bit level copy of the entire disk.
C. Time stamps the files with the date and time of the copy operation.
D. Excludes areas that have never been used to store data.

Answer: B
Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident. - Ed Tittle CISSP Study Guide (sybex) pg 595

QUESTION 1110:

When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
A.) Clearing completely erases the media whereas purging only remoes file headers, allowing the recovery of files
B.) Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack
C.) They both involve rewriting the media
D.) Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack

Answer: B
Reference: pg 405 Tittel: CISSP Study Guide

QUESTION 1111:

What is HIPPA?
A.) The Home Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act.
B.) The Public Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act.
C.)The Health Insurance Privacy & Accountability Act of 1996 (August 2), public law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act.
D.) The Health Insurance Privacy & Accountability Act of 1996 (August 2), Public Law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act.

Answer: B

Explanation:
"The United States Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPPA-Public Law 104-191), effective August 21, 1996, addresses the issues of health care privacy, security, transactions and code sets, unique identifies, electronic signatures, and plan portability in the United States." Pg 499-500 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 1112:

The privacy provisions of the federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPPA),
A.) apply to certain types of critical health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses.
B.) apply to health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses.
C.) apply to health information created or maintained by some large health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses.
D.) apply to health information created or maintained by health care providers regardless of whether they engage in certain electronic transactions, health plans, and health care clearinghouses.

Answer: B

QUESTION 1113:

Gap analysis does not apply to
A.) Transactions
B.) availability
C.) Privacy
D.) Security

Answer: B

QUESTION 1114:

A gap analysis for Privacy refers
A.) to the practice of identifying the policies and procedures you currently have in place regarding the availability of protected health information.
B.) to the practice of identifying the policies and procedures you currently have in place regarding the confidentiality of protected health information.
C.) to the practice of identifying the policies and procedures you currently have in place regarding the authenticity of protected health information.
D.) to the practices of identifying the legislation you currently have in place regarding the confidentiality of protected health information.

Answer: B

QUESTION 1115:

A gap analysis for Privacy
A.) includes a comparison of your proposed policies and procedures and the requirements established in the Security and Privacy Regulation in order to identify any necessary

modifications in existing policies to satisfy HIPPA regulations when they are stricter than state privacy laws.
B.) includes a comparison of your current policies and procedures and the requirements established in the Security and Privacy Regulation in order to identify any necessary modifications in existing policies to satisfy HIPPA regulations when they are stricter than state privacy laws
C.) includes a comparison of your ideal policies and procedures and the requirements established in the Security and Privacy Regulation in order to identify any necessary modifications in existing policies to satisfy HIPPA regulations when they are stricter than state privacy laws.
D.) includes a comparison of your exceptional policies and procedures and the requirements established in the Security and Privacy Regulation in order to identify any necessary modifications in existing policies to satisfy HIPPA regulations when they are stricter than state privacy laws

Answer: B

QUESTION 1116:

What is a gap analysis in relationship to HIPPA?
A.) In terms of HIPPA, a gap analysis cannot be defined.
B.) In terms of HIPPA, a gap analysis defines what an organization currently is doing in a specific area of their organization and compares current operations to other requirements mandated by ethical standards.
C.) In terms of HIPPA, a gap analysis defines what an organization currently is doing in a specific area of their organization and compares current operations to other requirements mandated by state or federal law
D.) In terms of HIPPA, a gap analysis defines what an organization proposes to be doing in a specific area of their organization and compares proposed operations to other requirements mandated by state or federal law.

Answer: C

QUESTION 1117:

The privacy provisions of the federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPPA), apply to certain types of health information created or maintained by health care providers
A.) who engage in certain electronic transactions, health plans, and health care clearinghouses
B.) who do not engage in certain electronic transactions, health plans, and health care clearinghouses
C.) regardless of whether they engage in certain electronic transactions, health plans, and health care clearinghouses
D.) if they engage for a majority of days in a year in certain electronic transactions, health plans, and health care clearinghouses.

Answer: A

QUESTION 1118:

HIPPA preempts state laws
A.) except to the extent that the state law is less stringent
B.) regardless of the extent that the state law is more stringent
C.) except to the extent that the state law more stringent
D.) except to the extent that the state law is legislated later than HIPPA

Answer: C

QUESTION 1119:

The Implementation Guides
A.) are referred to in the Static Rule
B.) are referred to in the Transaction Rule
C.) are referred to in the Transitional Rule
D.) are referred to in the Acquision Rule

Answer: B

QUESTION 1120:

The HIPPA task force must first
A.) inventory the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient care and central to the organization's business
B.) inventory the organization's systems, processes, policies, procedures and data to determine which elements are non critical to patient care and central to the organization's business
C.) inventory the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient complaints and central to the organization's peripheral businesses
D.) modify the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient care and central to the organization's business

Answer: A

QUESTION 1121:

A covered healthcare provider which a direct treatment relationship with an individual need not:
A.) provide the notice no later than the date of the first service delivery, including service delivered electronically
B.) have the notice available at the service delivery site for individuals to request and keep
C.) get a acknowledgement of the notice from each individual on stamped paper
D.) post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered healthcare provider to be able to read it

Answer: C

QUESTION 1122:

A health plan may conduct its covered transactions through a clearinghouse, and may require a provider to conduct covered transactions with it through a clearinghouse. The incremental cost of doing so must be borne
A.) by the HIPPA authorities
B.) by the health plan
C.) by any other entity but the health plan
D.) by insurance companies

Answer: B

QUESTION 1123:

Covered entities (certain health care providers, health plans, and health care clearinghouses) are not required to comply with the HIPPA Privacy Rule until the compliance date. Covered entities may, of course, decide to:
A.) unvoluntarily protect patient health information before this date
B.) voluntarily protect patient health information before this date
C.) after taking permission, voluntarily protect patient health information before this date
D.) compulsorily protect patient health information before this date

Answer: B

QUESTION 1124:

The confidentiality of alcohol and drug abuse patient records maintained by this program is protected by federal law and regulations. Generally, the program may not say to a person outside the program that a patient attends the program, or disclose any information identifying a patient as an alcohol or drug abuser even if:
A.)The person outside the program gives a written request for the information
B.) the patient consent in writing
C.) the disclosure is allowed by a court order
D.) the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation.

Answer: D

Explanation:
Incident handling is not related to disaster recovery, it is related to security incidents.

QUESTION 1125:

What is a Covered Entity? The term "Covered Entity" is defined in 160.103 of the regulation.
A.) The definition is complicate and long.
B.) The definition is referred to in the Secure Computing Act
C.) The definition is very detailed.
D.) The definition is deceptively simple and short

Answer: D

QUESTION 1126:

Are employers required to submit enrollments by the standard transactions?
A.) Though Employers are not CEs and they have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards
B.) Employers are not CEs and do not have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards.
C.) Employers are CEs and have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards.
D.) Employers are CEs and do not have to send enrollment using HIPPA standard transactions. Further, the employer health plan IS also a CE and must be able to conduct applicable transactions using the HIPPA standards.

Answer: B

QUESTION 1127:

Employers
A.) often advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to the health plan, and generally help them navigate their health benefits.
B.) sometimes advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to the health plan, and generally help them navigate their health benefits.
C.) never advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to health plan, and generally help them navigate their health benefits.
D.) are prohibited by plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plan.

Answer: A

QUESTION 1128:

Employers
A.) are covered entities if they do not use encryption
B.) are covered entities

C.) are not legal entities
D.) are not covered entities

Answer: D

QUESTION 1129:

The HIPPA task force must inventory the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient care and central to the organizations business. All must be inventoried and listed by
A.) by priority as well as encryption levels, authenticity, storage-devices, availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused and carefully document all the criteria used.
B.) by priority and cost as well as availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused and carefully document all the criteria used.
C.) by priority as well availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused but need not document all the criteria used.
D.) by priority as well as availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused and carefully document all the criteria used.

Answer: D

QUESTION 1130:

Are there penalties under HIPPA?
A.) No penalties
B.) HIPPA calls for severe civil and criminal penalties for noncompliance, including: -- fines up to $25k for multiple violations of the same standard in a calendar year -- fines up to $250k and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.
C.) HIPPA calls for severe civil and criminal penalties for noncompliance, includes: -- fines up to 50k for multiple violations of the same standard in a calendar year -- fines up to $500k and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information
D.) HIPPA calls for severe civil and criminal penalties for noncompliance, including: -- fines up to $100 for multiple violations of the same standard in a calendar year -- fines up to $750k and/or imprisonment up to 20 years for knowing misuse of individually identifiable health information

Answer: B

QUESTION 1131:

HIPPA gave the option to adopt other financial and administrative transactions standards, "consistent with the goals of improving the operation of health care system and reducing administrative costs" to
A.) ASCA prohibits HHS from paying Medicare claims that are not submitted electronically

after October 16, 2003.
B.) ASCA prohibits HHS from paying Medicare claims that are not submitted on paper after October 16, 2003
C.) ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement
D.) No

Answer: C

QUESTION 1132:

May a health plan require a provider to use a health care clearinghouse to conduct a HIPPA-covered transaction, or must the health plan acquire the ability to conduct the transaction directly with those providers capable of conducting direct transactions?
A.) A health plan may conduct its covered transactions through a clearinghouse, and may require a provider to conduct covered transactions with it through a clearinghouse. But the incremental cost of doing so must be borne by the health plan. It is a cost-benefit decision on the part of the health plan whether to acquire the ability to conduct HIPPA transactions directly with other entities, or to require use of a clearinghouse.
B.) A health plan may not conduct it's covered transactions through a clearinghouse
C.) A health plan may after taking specific permission from HIPPA authorities conduct its covered transactions through a clearinghouse
D.) is not as per HIPPA allowed to require provider to conduct covered transactions with it through a clearinghouse

Answer: A

QUESTION 1133:

Business Associate Agreements are required by the regulation whenever a business associate relationship exists. This is true even when the business associates are both covered entities.
A.) There are no specific elements which must be included in a Business Associate Agreement. However some recommended but not compulsory elements are listed in 164.504(e) (2)
B.) There are specific elements which must be included in a Business Associate Agreement. These elements are listed Privacy Legislation
C.) There are no specific elements which must be included in a Business Associate Agreement.
D.) There are specific elements which must be included in a Business Associate Agreement. These elements are listed in 164.504(e) (2)

Answer: D

QUESTION 1134:

The implementation Guides
A.) are referred to in the Transaction Rule

B.) are not referred to in the Transaction Rule
C.) are referred to in the Compliance Rules
D.) are referred to in the Confidentiality Rule

Answer: A

QUESTION 1135:

Business Associates
A.) are entities that perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity
B.) are entities that do not perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity
C.) are entities that perform services that require the use of Encrypted Insurance Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity
D.) are entities that perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity cannot be a business partner of another covered entity.

Answer: A

QUESTION 1136:

Health Care Providers, however,
A.) become the business associates of health plans even without joining a network
B.) become the business associates of health plans by simply joining a network
C.) do not become the business associates of health plans by simply joining a network
D.) do not become the HIPPA associates of health plans by simply joining a network

Answer: C

QUESTION 1137:

In terms of HIPPA what an organization currently is doing in a specific area of their organization and compared current operations to other requirements mandated by state or federal law is called
A.) HIPPA status analysis
B.) gap analysis
C.) comparison analysis
D.) stop-gap analysis

Answer: B

QUESTION 1138:

Group Health Plans sponsored or maintained by employers, however,
A.) ARE SOMETIMES covered entities.
B.) ARE NOT covered entities.
C.) ARE covered entities
D.) ARE called uncovered entities

Answer: C

QUESTION 1139:

Employers often advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to the health plan, and generally help them navigate their health benefits. Is this type of assistance allowed under the regulation?
A.) The final rule does nothing to hinder or prohibit plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plans.
B.) The final rule prohibits plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plans
C.) The final rule does hinder but does not prohibit plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plans
D.) The final rule does no advocating on behalf of group health plan participants or provide assistance in understanding their health plan.

Answer: A

QUESTION 1140:

HIPPA does not call for:
A.) Standardization of electronic patient health, administrative and financial data
B.) Unique health identifiers for individuals, employers, health plans, and health care providers.
C.) Common health identifiers for individuals, employers, health plans and health care providers.
D.) Security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future.

Answer: C

QUESTION 1141:

A gap analysis for the Transactions set refer to the practice of identifying the data content you currently have available
A.) through your medical software
B.) through your accounting software
C.) through competing unit medical software
D.) based on the statutory authorities report

Answer: A

QUESTION 1142:

A gap analysis for the Transactions set does not refer to
A.) the practice of identifying the data content you currently have available through your medical software
B.) the practice of and comparing that content to what is required by HIPPA, and ensuring there is a match.
C.) and requires that you study the specific format of a regulated transaction to ensure that the order of the information when sent electronically matches the order that is mandated in the Implementation Guides.
D.) but does not require that you study the specific format of a regulated transaction to ensure that the order of information when sent electronically matches the order that is mandated in the Implementation Guides.

Answer: D

QUESTION 1143:

Health Information Rights although your health record is the physical property of the healthcare practitioner or facility that compiled it, the information belongs to you. You do not have the right to:
A.) obtain a paper copy of the notice of information practices upon request inspect and obtain a copy of your health record as provided for in 45 CFR 164.524
B.) request a restriction on certain uses and disclosures of your information outside the terms as provided by 45 CFR 164.522
C.) amend your health record as provided in 45 CFR 164.528 obtain an accounting of disclosures of your health information as provided in 45 CFR 164.528
D.) revoke your authorization to use or disclose health information except to the extent that action has already been taken

Answer: B

QUESTION 1144:

Employers often advocate on behalf of their employees in benefit disputes and appeals, answer questions with regard to the health plan, and generally help them navigate their health benefits. Is individual consent required?
A.) No
B.) Sometimes
C.) Yes
D.) The answer is indeterminate

Answer: C

QUESTION 1145:

Who enforces HIPPA?
A.) The Office of Civil Rights of the Department of Confidentiality Services is responsible for enforcement of these rules
B.) The Office of Civil Rights of the Department of Health and Human Services is responsible for enforcement of these rules
C.) The Office of Health Workers Rights of the Department of Health and Human Services in responsible for enforcement of these rules
D.) The Department of Civil Rights of the Office of Health and Human Services is responsible for enforcement of these rules

Answer: B

QUESTION 1146:

Gap analysis does not apply to
A.) Transactions
B.) availability
C.) Privacy
D.) Security

Answer: B

QUESTION 1147:

A gap analysis for Security
A.) refers to the practice of trusting the security policies and practices currently in place in your organization designed to protect all your data from unauthorized access, alternation or inadvertent disclose.
B.) refers to the practice of modifying the security policies and practices currently in place in your organization designed to protect all your data from unauthorized access, alteration or inadvertent disclosure.
C.) refers to the practice of identifying the security policies and practices currently in place in your organization designed to protect all your data from unauthorized access, alteration or inadvertent disclosure.
D.) refers to the practice of improving the security policies and practices currently in place in your organization designed to protect all your data from unauthorized access alteration or inadvertent disclosure.

Answer: C

QUESTION 1148:

The Implementation Guides are referred to in the Transaction Rule. The manuals are

A.) non-technical in nature and do not specifically state what the data content should be for each HIPPA transaction. They also do not state the order in which this data must appear when transmitted electronically.
B.) theoretical in nature and specifically state what the data content should be for each HIPPA transaction. They also state the order in which this data must appear when transmitted electronically.
C.) technical in nature and specifically state what the data content should be for each HIPPA transaction. They do not state the order in which this data must appear when transmitted electronically.
D.) technical in nature and specifically state what the data content should be for each HIPPA transaction. They also state the order in which this data must appear when transmitted electronically.

Answer: D

QUESTION 1149:

Title II of HIPPA includes a section, Administrative Simplification, not requiring:
A.) Improved efficiency in healthcare delivery by standardizing electronic data interchange
B.) Protection of confidentiality of health data through setting and enforcing standards
C.) Protection of security of health data through setting and enforcing standards
D.) Protection of availability of health data through setting and enforcing standards

Answer: D

QUESTION 1150:

Who is not affected by HIPPA?
A.) clearing houses
B.) banks
C.) universities
D.) billing agencies

Answer: B

QUESTION 1151:

HIPPA results in

A.) sweeping changed in some healthcare transaction and administrative information systems
B.) sweeping changes in most healthcare transaction and administrative information systems
C.) minor changes in most healthcare transaction and administrative information systems
D.) no changes in most healthcare transaction and minor changes in administrative information systems

Answer: B

QUESTION 1152:

Which one is an example of a man-in-the-middle attack?

A. Buffer overflow
B. DoS attack
C. All of the above
D. None of the above

Answer: D

Explanation: Wrong: Both A and B could be the result of a man-in-the-middle attack, but neither are man-in-the-middle attacks. For example someone who uses a packet capturing device, such as a "sniffer" to obtain an unencrypted user ID and password to one or more PCs or servers and then the platforms to launch a DOS attach or create a Buffer Overflow by exploiting an application flaw or OS Vulnerability.

QUESTION 1153:

Which one of these is a basic firewall?

A. Packet Filtering Firewalls
B. Proxy Firewalls
C. All of the above
D. None of the above

Answer: A

Explanation: Packet Filtering Firewall - only examines an IP packet based on Source IP (SIP), Destination IP (DIP), Source Port and Destination Port for both UDP and TCP by subjecting each IP packet to an Access Control List.

QUESTION 1154:

Why is there an exception area in a policy?

A. Policy isn't valid without it
B. Management has to deal with various issues that may require exceptions
C. All of the above
D. None of the above

Answer: B

Explanation: Polices are ever evolving process that requires updating. Polices must change as the goals, functions and responsibilities of a company, government or employee changes. A simple policy exception could be - No unauthorized person or persons can enter the computer room. The Exception would be - Unless cleared by management and escorted by an authorized individual. In some cases there are NO exceptions - An example: Military TOP Secret information can ONLY be handled by someone with a TOP secret Clearanve;thus answer A is incorrect.

QUESTION 1155:

Which is a characteristic of IDEA?

A. 56 bytes
B. 64 bits
C. 64 bytes
D. All of the above
E. None of the above

Answer: B

Explanation: From Wikipedia: International Data Encryption Algorithm (IDEA) operates on 64-bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a round, see the illustration) and an output transformation (the half-round). The processes for encryption and decryption are similar. IDEA derives much of its security by interleaving operations from different groups - modular addition and multiplication, and bitwise eXclusive OR (XOR) - which are algebraically "incompatible" in some sense.

QUESTION 1156:

Which of the following can be used to raise awareness of the importance of security and risk?

A. Money
B. All of the above
C. None of the above

Answer: C

Explanation: C is the only logical choice. Awareness and the importance of security and risk can not be improved or awareness be increased with only money. Awareness is produced by providing employees with education and training. Reference the Training and Education Triad. Exam Cram 2 CISSP Page 52

QUESTION 1157:

Which mechanism complements an IDS?

A. Activating the built in VPN capabilities
B. Configuring built in alerts
C. All of the above
D. None of the above

Answer: B

Explanation: A network security engineer or other security personal must configure the IDS to detect alerts for specified security events, so the IDS will log the threat event. An IDS can either be a Network or Host based. Both have default settings and allow the administrator to configure triggers for alerts.

QUESTION 1158:

A programmer creates a virus producing tool in order to test the performance of a new virus diction product.

A. This is ethical because it was created to test and enhance the performance of a virus protection tool
B. It's unethical because the virus creating tool may become available to the public.
C. All of the above
D. None of the above

Answer: B

Explanation: As a CISSP, one needs to discourage unsafe practices and/or bad practices, and preserve and strengthen the integrity of the public infrastructures. See "All-in-One Exam Guide" Third Edition by Shon Harris page 753 or www.isc2.org.

QUESTION 1159:

A product cost $20,000. The cost to restore information is $1,000,000. The product is 60% effective. What is the value of the product in 2 years?

Answer:
Explanation: This question makes no sense. There are some questions on the actual CISSP exam that are not used for research only purposes and are not used to grade the exam.. This problem is not a SLE, because SLE pertains to a one year period of time. Based on the information provided the value of the product could be lower or higher due to market demands. This question has more to do with economics then SLE.

QUESTION 1160:

What is the SLE?

Answer:
Explanation: Single Loss Expectancy (SLE)
Estimate potential losses (SLE)-this step involves determining the single loss expectancy (SLE). SLE is calculated as follows:
Single loss expectancy x Asset value = Exposure factor
Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

QUESTION 1161:

What is the ALE?

Answer:

Explanation:
Determine annual loss expectancy (ALE)-This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:
Annualized loss expectancy (ALE) x Single loss expectancy (SLE) = Annualized rate of occurrence (ARO)

QUESTION 1162:

In a discretionary mode, which of the following entities is authorized to grant information access to other people?

A. Manager
B. Group leader
C. Security manager
D. User

Answer: D

Explanation: Discretionary control is the most common type of access control mechanism implemented in computer systems today. The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. Discretionary security differs from mandatory security in that it implements the access control decisions of the user. Mandatory controls are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

QUESTION 1163:

Which DES mode of operation is best suited for database encryption?

A. Cipher Block Chaining (CBC) mode
B. Cycling Redundancy Checking (CRC) mode
C. Electronic Code Book (ECB) mode
D. Cipher Feedback (CFB) mode

Answer: C

Explanation: The DES algorithm in Electronic Codebook (ECB) mode is used for DEK and MIC encryption when symmetric key management is employed. The character string "DES-ECB" within an encapsulated PEM header field indicates use of this algorithm/mode combination.
A compliant PEM implementation supporting symmetric key management shall support this algorithm/mode combination. This mode of DES encryption is the best suited for database encryption because of its low overhead.
ECB Mode has some weakness, here they are:
1. ECB Mode encrypts a 64-bit block independently of all other 64-bit blocks
2. Given the same key, identical plaintext will encrypt the same way
3. Data compression prior to ECB can help (as with any mode)
4. Fixed block size of 64 bits therefore incomplete block must be padded

QUESTION 1164:

Within the realm of IT security, which of the following combinations best defines risk?

A. Threat coupled with a breach.
B. Threat coupled with a vulnerability.
C. Vulnerability coupled with an attack.
D. Threat coupled with a breach of security.

Answer: B

Explanation: This is the main concept, when we talk about a possible risk we always have a possible vulnerability in the system attacked. This vulnerability can make a threat to be successful. We can say that the level of risk can be measures through the level of vulnerabilities in our current systems and the ability of the attackers to exploit them to make a threat successful.

QUESTION 1165:

Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.

Answer: B

Explanation: This is the right answer, with a separation of the two environments (Test and development), we can get a more stable and more "in control" environment, Since we are making tests in the development environment, we don't want our production processes there, we don't want to experiment things in our production processes. With a separation of the environments we can get a more risk free production environment and more control and flexibility over the test environment for the developers.

QUESTION 1166:

Which of the following statements pertaining to dealing with the media after a disaster occurred and disturbed the organizations activities is incorrect?

A. The CEO should always be the spokesperson for the company during a disaster.
B. The disaster recover plan must include how the media is to be handled during the disaster.
C. The organization's spokesperson should report bad news before the press gets a hold of it through another channel.
D. An emergency press conference site should be planned ahead.

Answer: A

Explanation: This is not a good practice, we cannot involves the CEO of the company to deal with the media in every case we have a disaster, depending on the severity of the disaster we can make the CEO talk, but the best practice in the real world is to have a well-known person with that role, with special speaking capabilities and knowledge about press methods. In general, the CEO always gets news of what happened, and he decides the company politics, then another designed employee (Usually from the disaster recovery team) deals with the media.

QUESTION 1167:

Which Orange book security rating introduces security labels?

A. C2
B. B1
C. B2
D. B3

Answer: B

Explanation: Class (B1) or "Labeled Security Protection" systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

QUESTION 1168:

A Business Impact Analysis (BIA) does not:

A. Recommend the appropriate recovery solution.
B. Determine critical and necessary business functions and their resource dependencies.
C. Identify critical computer applications and the associated outage tolerance.
D. Estimate the financial impact of a disruption.

Answer: A

Explanation: Remember that when we talk about a BIA (Business Impact Analysis), we are analyzing and identifying possible issues about our infrastructure, in this kind of analysis we don't make suggestions about what to do to recover from them. This is not an action plan, It's an analysis about the business, the process that it relays on, the level of the systems and a estimative of the financial impact, or in other words, how much many we loose with our systems down.

QUESTION 1169:

Which access control model enables the owner of the resource to specify what subjects can access specific resources?

A. Discretionary Access Control
B. Mandatory Access Control
C. Sensitive Access Control
D. Role-based Access Control

Answer: A

Explanation: Discretionary Access Control (DAC) is used to control access by restricting a subject's access to an object. It is generally used to limit a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file. Using a DAC mechanism allows users control over access rights to their files. When these rights are managed correctly, only those users specified by the owner may have some combination of read, write, execute, etc. permissions to the file.

QUESTION 1170:

What type of cable is used with 100Base-TX Fast Ethernet?

A. Fiber-optic cable
B. Four pairs of Category 3, 4 or 5 unshielded twisted-par (UTP) wires.
C. Two pairs of Category 5 unshielded twisted-pair (UTP) or Category 1 shielded twisted-pair (STP) wires.
D. RG.58 cable.

Answer: C

Explanation: 100BaseTX is a 100-Mbps baseband Fast Ethernet specification using two pairs of either UTP or STP wiring. The first pair of wires is used to receive data; the second is used to transmit. To guarantee proper signal timing, a 100BaseTX segment cannot exceed 100 meters in length. This specification of Ethernet is based on the IEEE 802.3 standard.

QUESTION 1171:

Which of the following best describes the Secure Electronic Transaction (SET) protocol?

A. Originated by VISA and MasterCard as an Internet credit card protocol.
B. Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures.
C. Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer.
D. Originated by VISA and MasterCard as an Internet credit card protocol using SSL.

Answer: B

Explanation: This protocol was created by VISA and MasterCard as a common effort to make the buying process over the Internet secure through the distribution line of those companies. It is located in layer 7 of the OSI model.
SET uses a system of locks and keys along with certified account IDs for both consumers and merchants. Then, through a unique process of "encrypting" or scrambling the information exchanged between the shopper and the online store, SET ensures a payment process that is convenient, private and most of all secure. Specifically, SET:
1. Establishes industry standards to keep your order and payment information confidential.
2. Increases integrity for all transmitted data through encryption.
3. Provides authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provides authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Allows the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
The SET process relies strongly on the use of certificates and digital signatures for the process of authentication and integrity of the information.

QUESTION 1172:

At which of the following phases of a software development life cycle are security and access controls normally designed?

A. Coding
B. Product design
C. Software plans and requirements
D. Detailed design

Answer: D

Explanation: Security controls and access controls are normally designed in the "Detailed" phase of design. In this phase you have the design of many of the security features of your development like authentication, confidentiality functionality, non repudiation capabilities. In this phase you can also define what is going to be the access control method for the software, we can make it discretionary (less restrictive), mandatory (more restrictive), role based and others.

QUESTION 1173:

Which type of control would password management classify as?

A. Compensating control
B. Detective control
C. Preventive control
D. Technical control

Answer: C

Explanation: Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:
Access control software.
Antivirus software.
Library control systems.
Password and Password management
Smart cards.
Encryption.
Dial-up access control and callback sytems
About Passwords: Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system.
Fixed passwords that are used for a defined period of time are often easy for hackers to compromise; therefore, great care must be exercised to ensure that these passwords do not

appear in any dictionary. Fixed passwords are often used to control access to specific data bases. In this use, however, all persons who have authorized access to the data base use the same password; therefore, no accountability can be achieved.
Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords. Dynamic passwords are created by a token that is programmed to generate passwords randomly.
The management of those passwords is part of Preventive control.

QUESTION 1174:

Due are is not related to:

A. Good faith
B. Prudent man
C. Profit
D. Best interest

Answer: C

Explanation: This is obviously a term not related to Profit, a "due" is not going to give us profit, its going to give us the opposite. Its always a good practice to pay your due. This can be learned in the real life. A Prudent man always pays its due, also a Good faith men pays them. This term is not related to profit.

QUESTION 1175:

Which of the following is not an Orange Book-defined life cycle assurance requirement?

A. Security testing
B. Design specification and testing
C. Trusted distribution
D. System integrity

Answer: D

Explanation: Life cycle assurance is more than configuration management.
Reference: "Operational assurance focuses on the basic features and architecture of a system that lend themselves to supporting security. There are five requirements or elements of operation assurance:
* System architecture
* System integrity
* Covert channel analysis
* Trusted facility management
* Trusted Recovery
Life cycle assurance focuses on the controls and standards that are necessary for designing, building, and maintaining a system. The following are the four requirements or elements of life

cycle assurance:
* Security testing
* Design specification and testing
* Configuration Management
* Trusted distribution"
Pg 398 Tittel

QUESTION 1176:

What is another name for the Orange Book?

A. The Trusted Computer System Evaluation Criteria (TCSEC)
B. The Trusted Computing Base (TCB)
C. The Information Technology Security Evaluation Criteria (ITSEC)
D. The Common Criteria

Answer: A

Explanation:
The Trusted Computer System Evaluation Criteria (TCSEC) is a collection of criteria used to grade or rate the security offered by a computer system product. The TCSEC is sometimes referred to as "the Orange Book" because of its orange cover. The current version is dated 1985 (DOD 5200.28-STD, Library No.S225,711) The TCSEC, its interpretations and guidelines all have different color covers, and are sometimes known as the "Rainbow Series".

QUESTION 1177:

A password that is the same for each log-on session is called a?

A. "one-time password"
B. "two-time password"
C. static password
D. dynamic password

Answer: C

Explanation: A Static password is one that remains the same until its changed. Its like the password that we use in the operating systems, you set it, and then you always use the same password to logon to the system for the time of the session. This password will give us access to the system and will be the vehicle to create our access token in a successful way to get our privileges. A one-time password is only valid for one use, dynamic ones change every certain condition is met, and two-time passwords can only be used two times. We can provide certain times of access with this kind of passwords.

QUESTION 1178:

Which of the following backup methods is most appropriate for off-site archiving?

A. Incremental backup method.
B. Off-site backup method.
C. Full backup method.
D. Differential backup method.

Answer: C

Explanation:
Since we want to maintain the backups offsite, its always better to send FULL-Backups because they contain a consistent base of the system. We perform the beginning of a restore through a full backup. Remember that the backups stored offsite are in most cases in a secure place, full backup in there are a best practice for any network administrator. With incremental or differential backups we don't have all we need to restore a system to a consistent state. We need to start from the full backup. "Offsite Backup" is not a valid backup method.

QUESTION 1179:

Which of the following is not a weakness of symmetric cryptography?

A. Limited security
B. Key distribution
C. Speed
D. Scalability

Answer: C

Explanation: In secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.
With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver ; that in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.
Symmetric encryption is around 1000 times faster than Asymmetric encryption, the second is commonly used just to encrypt the keys for Symmetric Cryptography.

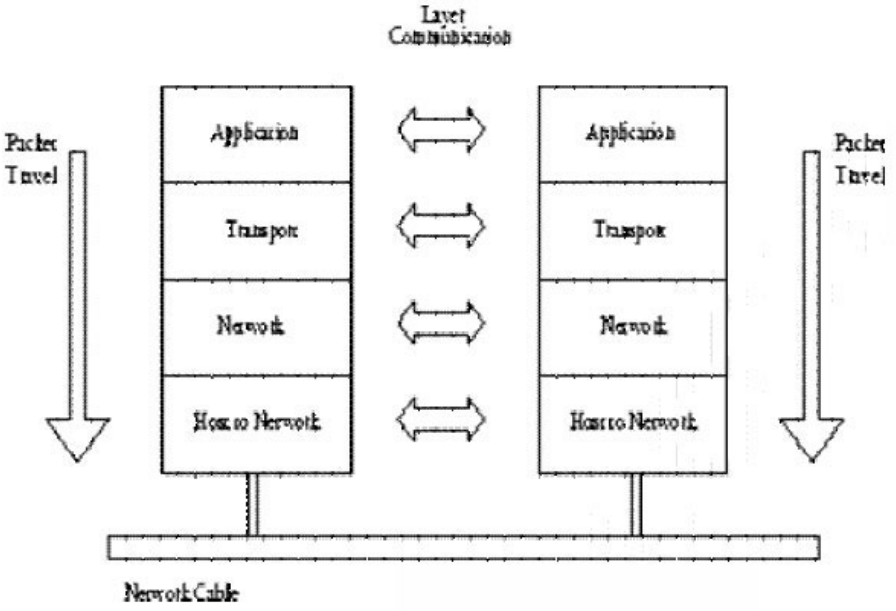
QUESTION 1180:

Which of the following is not a defined layer in the TCP/IP protocol model?

A. Application layer
B. Session layer
C. Internet layer
D. Network access layer

Answer: B

Explanation: The TCP/IP reference model is the network model used in the current Internet architecture. It has its origins back in the 1960's with the grandfather of the Internet, the ARPANET. This was a research network sponsored by the Department of Defense in the United States.
The reference model was named after two of its main protocols, TCP (Transmission Control Protocol) and IP (Internet Protocol). They choose to build a packet-switched network based on a connectionless internet layer. Here is a representation of it:



"The TCP/IP Protocol Model is similar to the OSI model, but it defines only the following four layers instead of seven:
Application Layer. Consists of the applications and processes that use the network.

Host-to-Host Transport Layer. Provides end-to-end data delivery service to the Application Layer.
Internet Layer. Defines the IP datagram and handles the routing of data across networks.
Network Access or Link Layer. Consists of routines for accessing physical networks and the electrical connection."
Pg 112 Krutz: The CISSP Prep Guide: Gold Edition.

QUESTION 1181:

Rewritable and erasable (CDR/W) optical disk are sometimes used for backups that require short time storage for changeable data, but require?

A. Faster file access than tape.
B. Slower file access than tape.
C. Slower file access than drive.
D. Slower file access than scale.

Answer: A

Explanation: This is true, when we use optical media like CD´s to make our backups we need a constant throughput on the file access and data transfer inside the disk because of the risk to get a buffer overrun error in the CD writer. If the buffer user by the CD burner is empty and the Hard disk does not provide data for that time, the Backup will be unsuccessful. This can be solved with a Technology known as "Burn Proof".

QUESTION 1182:

Which one of the following is not a primary component or aspect of firewall systems?

A. Protocol filtering
B. Packet switching
C. Rule enforcement engine
D. Extended logging capability

Answer: B

Explanation: This is not a main function of a firewall, packet switching is a main feature of a Switch (working only in the layer 2 of the OSI model). Firewall are network security devices that can function through layer 2 to layer 7 of the OSI model. They usually include rule engine that enforce the enterprise security policy of the company. They provide protocol filtering to enforce our requirements through the forwarded or deny of traffic. They also provide logging capabilities so we can analyze what is happening in a very low level in our network.

QUESTION 1183:

What are database views used for?

A. To ensure referential integrity.
B. To allow easier access to data in a database.
C. To restrict user access to data in a database.
D. To provide audit trails.

Answer: C

Explanation: Through the use of a view we can provide security for the organization restricting users access to certain data or to the real tables containing the information in

our database. For example, we can create a view that brings data from 3 tables, only showing 2 of the 4 columns in each. Instead of giving access to the tables that contain the information, we give access to the view, so the user can access this fixed information but does not have privileges over the tables containing it. This provides security.

QUESTION 1184:

Which of the following Common Data Network Services is used to send and receive email internally or externally through an email gateway device?

A. File services
B. Mail services
C. Print services
D. Client/Server services

Answer: B

Explanation: This functionality is provided through mail services, this service permits collaboration between users in an internal and external level. We usually use two protocols, "SMTP" in port TCP 25 to send the emails and "POP3" in port TCP 110 to receive them. Currently there is another protocol that is gaining popularity, it is "IMAP4". Print services are used for printing documents and file services are used to share and access files and folders inside the infrastructure.

QUESTION 1185:

Intrusion detection has which of the following sets of characteristics.

A. It is adaptive rather than preventive.
B. It is administrative rather than preventive.
C. It is disruptive rather than preventative.
D. It is detective rather than preventative.

Answer: D

Explanation: This is one of the features of intrusion detections, instead of being pro-active, it has a reactive behavior. When we set an IDS system inside of our network or hosts, the IDS agent is constantly monitoring in real time what activities are being performed in the infrastructure. If the IDS founds a malicious activity taking place it can take actions against it like disabling interfaces, alerting the administrators or sending network attacks to the source to put it out of service.
As a difference to the detective behavior of IDS, we can also increase the security with practices like hardening our systems ,this is considered a preventive practice.

QUESTION 1186:

Which type of password provides maximum security because a new password is required for each now log-on is defined to as?

A. One-time or dynamic password
B. Cognitive password
C. Static password
D. Pass phrase

Answer: A

Explanation: "One-time" or "dynamic" password technology concept is having your remote host already know a password that is not going to go over insecure channels and when you connect, you get a challenge. You take the challenge information and password and plug it into an algorithm which generates the response that should get the same answer if the password is the same on the both sides. Therefore the password never goes over the network, nor is the same challenge used twice. Unlike SecurID or SNK, with S/key you do not share a secret with the host.
Other one time password technology is card systems where each user gets a card that generates numbers that allow access to their account. Without the card, it is improbable to guess the numbers.

QUESTION 1187:

They in form of credit card-size memory cards or smart cards, or those resembling small calculators, are used to supply static and dynamic passwords are called?

A. Token Ring
B. Tokens
C. Token passing networks
D. Coupons

Answer: B

Explanation: Tokens are usually used to provide authentication through "What we have", is most commonly implemented to provide two-factor authentication. For example, SecurID requires two pieces of information, a password and a token. The token is usually generated by the SecurID token - a small electronic device that users keep with them that display a new number every 60 seconds. Combining this number with the users password allows the SecurID server to determine whatever or not the user should be granted access.

QUESTION 1188:

Which of the following uses a directed graph to specify the rights that a subject can transfer to an object, or that a subject can take from another subject?

A. Take-Grant model

B. Access Matrix model
C. Biba model
D. Bell-Lapadula model

Answer: A

Explanation: The Take-Grant System is a model that helps in determining the protection rights (e.g., read or write) in a computer system. The Take-Grant system was introduced by Jones, Lipton, and Snyder to show that it is possible to decide on the safety of a computer system even when the number of subjects and objects are very large, or unbound. This can be accomplished in linear time based on the initial size of the system. The take-grant system models a protection system which consists of a set of states and state transitions. A directed graph shows the connections between the nodes of this system. These nodes are representative of the subjects or objects of the model. The directed edges between the nodes represent the rights that one node has over the linked node.

QUESTION 1189:

Which of the following is the BEST way to prevent software license violations?

A. Implementing a corporate policy on copyright infringements and software use.
B. Requiring that all PCs be diskless workstations.
C. Installing metering software on the LAN so applications can be accessed through the metered software.
D. Regularly scanning used PCs to ensure that unauthorized copies of software have not been loaded on the PC.

Answer: D

Explanation: Since its impossible to control all the efforts of the users to install software without the proper licenses in their PC´s (Specially downloaded from the Internet), the best way to prevent licenses violations is through regular audit to every single user PC to see what's the installed programs are and what's the nature of them (Shareware, freeware, licensed). We cant use LAN monitoring software because not all the applications are network enabled, also, there is usually a policy about software installation, but the users do not rely on them many times. It also a very nice practice to punish the users making software license violations.

QUESTION 1190:

Zip/Jaz drives, SyQuest, and Bemoulli boxes are very transportable and are often the standard for?

A. Data exchange in many businesses.
B. Data change in many businesses.
C. Data compression in many businesses.

D. Data interchange in many businesses.

Answer: A

Explanation: This is the primary use of this kind of devices, since they are very portable (a medium-size external box) and they provide standard interfaces to the PC, they are usually used in data exchange because of their high capacity in comparison to the 3.5 floppy diskettes. We can make changes in the media used by this devices, but is not their primary use. Compression is not the best feature of this devices, their usually depend on File system compression. Absolutely, the best use of this boxes is for data exchange.

QUESTION 1191:

What are two types of system assurance?

A. Operational Assurance and Architecture Assurance.
B. Design Assurance and Implementation Assurance.
C. Architecture Assurance and Implementation Assurance.
D. Operational Assurance and Life-Cycle Assurance.

Answer: D

Explanation:
Software Systems Quality Assurance (SQA) is defined as a planned and systematic approach to the evaluation of the quality of and adherence to software product standards, processes, andprocedures. SQA includes the process of assuring that standards and procedures are established and are followed throughout the software acquisition life cycle. Compliance with agreed-upon standards and procedures is evaluated through process monitoring, product evaluation, and audits. Software development and control processes should include quality assurance approval points, where an SQA evaluation of the product may be done in relation to the applicable standards. The 2 types available are : Operational assurance (that specified that the operation compiles with the required) and Life-Cycle assurance (that specifies that the system has passed through all the Software life-cycle).

QUESTION 1192:

Why does compiled code pose more risk than interpreted code?

A. Because malicious code can be embedded in the compiled code and can be difficult to detect.
B. Because the browser can safely execute all interpreted applets.
C. Because compilers are not reliable.
D. It does not. Interpreted code poses more risk than compiled code.

Answer: A

Explanation: Since the compiled code has already been translated to binary language (the

language understanded natively by the computers), its very difficult for us (the humans) to detect malicious code inside an application, this is because its not apparently visible, you have to find that malicious code through the behavior of the program. Instead, when we talk about Interpreted code, we use a language interpreter, that is a piece of software that allows the end-user to write a program in some human-readable language, and have this program executed directly by the interpreter.
This is in contrast to language compilers, that translate the human-readable code into machine-readable code, so that the end-user can execute the machine-readable code at a later time.This is far more easier to detect malicious code inside the programs, you just need to see what piece of code produced the undesired action.

QUESTION 1193:

Which model, based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes, introduced five levels with which the maturity of an organization involved in the software process is evaluated?

A. The Total Quality Model (TQM)
B. The IDEAL Model
C. The Software Capability Maturity Model
D. The Spiral Model

Answer: C

Explanation: The Capability Maturity Model for Software describes the principles and practices underlying software process maturity and is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. The CMM is organized into five maturity levels:1) Initial. The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.2) Repeatable. Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.3)Defined. The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.4) Managed. Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.5) Optimizing. Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

QUESTION 1194:

Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud simulates the tones of coins being deposited into a payphone?

A. Red Boxes
B. Blue Boxes
C. White Boxes
D. Black Boxes

Answer: A

Explanation:
The Red box basically simulates the sounds of coins being dropped into the coin slot of a payphone. The traditional Red Box consisting of a pair of Wien-bridge oscillators with the timing controlled by 555 timer chips.The Blue Box, The mother of all boxes, The first box in history, which started the whole phreaking scene. Invented by John Draper (aka "Captain Crunch") in the early 60s, who discovered that by sending a tone of 2600Hz over the telephone lines of AT&T, it was possible to make free calls.A Black Box is a device that is hooked up to your phone that fixes your phone so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to 1/2 hour, after 1/2 hour the Phone Co. gets suspicious, and then you can guess what happens.The White Box turns a normal touch tone keypad into a portable unit. This kind of box can be commonly found in a phone shop.

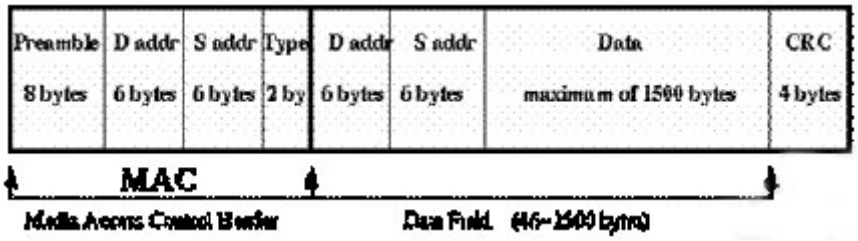
QUESTION 1195:

What is the proper term to refer to a single unit of Ethernet data?

A. Ethernet segment
B. Ethernet datagram
C. Ethernet frame
D. Ethernet packet

Answer: C

Explanation: Ethernet traffic is transported in units of a frame, where each frame has a definite beginning and end. Here is an Ethernet frame:



In this picture we define:
1. Preamble Field used for synchronization, 64-bits
2. Destination Address Ethernet address of the destination host, 48-bits
3. Source Address Ethernet address of the source host, 48-bits
4. Type of data encapsulated, e.g. IP, ARP, RARP, etc, 16-bits.
5. Data Field Data area, 46-1500 bytes, which has

Destination Address Internet address of destination host
Source Address Internet address of source host
6. CRC Cyclical Redundancy Check, used for error detection

QUESTION 1196:

Which of the following represents an ALE calculation?

A. Singe loss expectancy x annualized rate of occurrence.
B. Gross loss expectancy x loss frequency.
C. Actual replacement cost - proceeds of salvage.
D. Asset value x loss expectancy.

Answer: A

Explanation: ALE (Annualized Loss Expectancy) calculations are a component of every risk analysis process. ALE calculations when done properly portray risk accurately. ALE calculations provide meaningful cost/benefit analysis. ALE calculations are used to:
1. Identify risks
2. Plan budgets for information risk management
3. Calculate loss expectancy in annualized terms
SLE x ARO = ALE

QUESTION 1197:

IF an operating system permits executable objects to be used simultaneously by multiple users without a refresh of the objects, what security problem is most likely to exist?

A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Data leakage through covert channels.
D. Denial of service through a deadly embrace.

Answer: A

Explanation: This is a well known issue knew by many programmers, since the operating system is allowing the executables to be used by many users in different sessions at the same time, and there is not refreshing every certain time, there will be a disclosure of residual data. To fix this we need to get sure that objects are refreshed frequently, for added security its better an OS that does not allow the use of an executable object by many users at the same time.

QUESTION 1198:

Tape arrays use a large device with multiple (sometimes 32 or 64) tapes that are configured as a?

A. Single array
B. Dual array
C. Triple array
D. Quadruple array

Answer: A

Explanation: This is the function of a tape robot/changer working on a media library / jukebox. We can get as many as 32 / 64 or even more tapes action as a single logical unit. You can have a robot that changes and retrieves the different tapes when they are needed, so you see the whole bunch of tapes as it's a single logical storage solution for you. This kind of solutions are very expensive.

QUESTION 1199:

Why would anomaly detection IDSs often generate a large number of false positives?

A. Because they can only identify correctly attacks they already know about.
B. Because they are application-based are more subject to attacks.
C. Because they cant identify abnormal behavior.
D. Because normal patterns of user and system behavior can vary wildly.

Answer: D

Explanation: One of the most obvious reasons why false alarms occur is because tools are stateless. To detect an intrusion, simple pattern matching of signatures is often insufficient. However, that's what most tools do. Then, if the signature is not carefully designed, there will be lots of matches. For example, tools detect attacks in sendmail by looking for the words "DEBUG" or "WIZARD" as the first word of a line. If this is in the body of the message, it's in fact innocuous, but if the tool doesn't differentiate between the header and the body of the mail, then a false alarm is generated.
Finally, there are many events happening in the course of the normal life of any system or network that can be mistaken for attacks. A lot of sysadmin activity can be catalogued as anomalous. Therefore, a clear correlation between attack data and administrative data should be established to cross-check that everything happening on a system is actually desired.
Normal patterns and user activities are usually confused with attacks by IDS devices, its expected that the 2nd generations IDS systems will decrease the percent of false positives.

QUESTION 1200:

According to private sector data classification levels, how would salary levels and medical information be classified?

A. Public
B. Sensitive

C. Private
D. Confidential

Answer: C

Explanation: According to the classification levels of the private sector, this information is classified as Private because this information is from a personal nature. There is no need for other employees to see details about your health or you salary range, this can lead to internal problems inside the company, problems like jealous employees.

QUESTION 1201:

Which of the following is used in database information security to hide information?

A. Inheritance
B. Polyinstantiation
C. Polymorphism
D. Delegation

Answer: B

Explanation: Polyinstantiation represents an environment characterized by information stored in more than one location in the database. This permits a security model with multiple levels-of-view and authorization. The current problem with polyinstantiation is ensuring the integrity of the information in the database. Without an effective method for the simultaneous updating of all occurrences of the same data element - integrity cannot be guaranteed.

QUESTION 1202:

Which of the following evaluates the product against the specification?

A. Verification
B. Validation
C. Concurrence
D. Accuracy

Answer: A

Explanation: This is the proper term, "Verification", this term is used when we are making a comparison of a product against a specification. For example, you can have a product that is build on open standards, you can have a proof of that by making a "verification" of it against the standards or specifications included in those.

QUESTION 1203:

Application Level Firewalls are commonly a host computer running proxy server software, which makes a?

A. Proxy Client
B. Proxy Session
C. Proxy System
D. Proxy Server

Answer: D

Explanation: A proxy server is a server that sits between a client and server application, such as a Web browser and a source web server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the original source web server. Firewalls usually provides this kind of services to have more control over user request and allow / deny the traffic of those through the gateway. At this time the most common Proxy server is for HTTP protocol, we can also have proxies for SMTP and FTP.

QUESTION 1204:

What attack involves the perpetrator sending spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening?

A. Bonk attack
B. Land attack
C. Teardrop attack
D. Smurf attack

Answer: B

Explanation: The Land attack involves the perpetrator sending spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening. If the packet(s) contain the same destination and source IP address as the host, the victim's machine could hang or reboot.
In addition, most systems experience a total freeze up, where as CTRL-ALT-DELETE fails to work, the mouse and keyboard become non operational and the only method of correction is to reboot via a reset button on the system or by turning the machine off.
Vulnerable Systems:
This will affect almost all Windows 95, Windows NT, Windows for Workgroups systems that are not properly patched and allow Net Bios over TCP/IP.
In addition, machines running services such as HTTP, FTP, Identd, etc that do not filter packet(s), that contain the same source / destination IP address, can still be vulnerable to attack through those ports.
Prevention:
This attack can be prevented for open / listening ports by filtering inbound packets containing the same source / destination IP address at the router or firewall level.
For most home users not running a lot of services, and for those who use IRC, disabling the

Identd server within their client will stop most attacks since the identd service (113) is becoming the most attacked service/port.

QUESTION 1205:

The beginning and the end of each transfer during asynchronous communication data transfer are marked by?

A. Start and Stop bits.
B. Start and End bits.
C. Begin and Stop bits.
D. Start and Finish bits.

Answer: A

Explanation: The ASYNCHRONOUS (ASYNC) format for data transmission is a procedure or protocol in which each information CHARACTER or BYTE is individually synchronized or FRAMED by the use of Start and Stop Elements, also referred to as START BITS and STOP BITS. The Asynchronous Transmission Format is also known as START-STOP mode or CHARACTER mode. Each character or byte is framed as a separate and independent unit of DATA that may be transmitted and received at irregular and independent time intervals. The characters or bytes may also be transmitted as a contiguous stream or series of characters.

QUESTION 1206:

Most of unplanned downtime of information systems is attributed to which of the following?

A. Hardware failure
B. Natural disaster
C. Human error
D. Software failure

Answer: A

Explanation:
This is what the static's says. Most of the downtime is cause of unexpected hardware failure. Commonly you just replace the FRU (Field replazable unit) when they fail. Usually a well written software does not fail if the hardware is running correctly. The human errors are controllable and natural disasters are not very often. Hardware failure is very common, it's a good practice to have spare disks, NIC and any other hardware FRU´s in your company to minimize the downtime with quick replacements.

QUESTION 1207:

Raid that functions as part of the operating system on the file server

A. Software implementation
B. Hardware implementation
C. Network implementation
D. Netware implementation

Answer: A

Explanation: This kind of RAID is totally depended on the operating system, this is because the server does not have any special hardware - RAID controller in the board. This kind of RAID implementation usually degrades performance because it takes many CPU cycles. A very common example of software RAID is the support for it on Windows 2000 Server, where you can create RAID 0,1 and 5 through heterogeneous disks, you can even make a RAID between one SCSI and one EIDE disk. The software implementation is hardware independent always that the disks are recognized by the Operating System.

QUESTION 1208:

During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Development
D. Implementation

Answer: C

Explanation:
The System Development Life Cycle is the process of developing information systems through investigation, analysis, design, implementation, and maintenance. The System Development Life Cycle (SDLC) is also known as Information Systems Development or Application Development. If you take a look at the standard IT system life cycle chart, you will see that everything that deals with security requirements is done at the "development" stage. In this stage you can create the access controls, the form of authentication to use and all the other security requirements.

QUESTION 1209:

Ensuring that printed reports reach proper users and that receipts are signed before releasing sensitive documents are examples of?

A. Deterrent controls
B. Output controls
C. Information flow controls
D. Asset controls

Answer: B

Explanation: Since we want to deal with printer reports, we are talking about output controls, Why, because printer produce output, and we can control it. As a best practice you can have people dedicated in the company to receive the different print jobs in the printing center, and people that takes care of the confidential information requiring a signature from the sender stating that the document was delivered to the owner in a timely and secure fashion.

QUESTION 1210:

Non-Discretionary Access Control. A central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on?

A. The societies role in the organization.
B. The individual's role in the organization.
C. The group-dynamics as they relate to the individual's role in the organization.
D. The group-dynamics as they relate to the master-slave role in the organization.

Answer: B

Explanation: An access control model defines a computer and/or network system's rules for user access to information resources. Access control models provide confidentiality, integrity and also provide accountability through audit trails. An audit trail documents the access of an object by a subject with a record of what operations were performed. Operations include: read, write, execute and own.
Non-Discretionary Access Control is usually role-based, centrally administered with authorization decisions based on the roles individuals have within an organization (e.g. bank teller, loan officer, etc. in a banking model). A system's security administrator grants and/or revokes system privileges based on a user's role. This model works well for corporations with a large turnover of personnel.

QUESTION 1211:

An effective information security policy should not have which of the following characteristics?

A. Include separation of duties.
B. Be designed with a short-to mid-term focus.
C. Be understandable and supported by all stakeholders.
D. Specify areas of responsibility and authority.

Answer: B

Explanation: This is not a very good practice, specially for the CISSP examination, when

you plan and develop the security policy for your enterprise you should always plan it with a long term focus. The policy should be created to be there for a long time, and you should only make revisions of it every certain time to comply with changes or things that could have changed.
In a security policy the duties should be well specified, be understandable by the people involved in it, and specify areas of responsibility.

QUESTION 1212:

Which of the following statements pertaining to secure information processing facilities is incorrect?

A. Walls should have an acceptable fire rating.
B. Windows should be protected by bars.
C. Doors must resist forcible entry.
D. Location and type of fire suppression systems should be known.

Answer: B

Explanation: The correct answer can be determined through elimination. We need to have an acceptable fire rating for the walls, this is well known for any CISSP aspirant, its like that because we need to contain the fire as much as we can. We also need resistant doors so unauthorized people do not enter easily using the force. The people also need to know about fire suppression systems to be able to deal with a fire situation inside the facilities. As you can see, We should not protect windows with bars, this is a bad practice because, in the case of a fire, the people cannot get out of the building through the windows.

QUESTION 1213:

Making sure that the data is accessible when and where it is needed is which of the following?

A. Confidentiality
B. Integrity
C. Acceptability
D. Availability

Answer: D

Explanation: This is one of the pillars of network security. We can say that the data is available if we can access to it when we need it. This what is referred in the question, Availability refers to get access to data when and where you need it. Confidentiality deals with encryption and data protection against third party interception. Integrity deals with digital signatures and assures that the data has not changed. Acceptability is not a related term.

QUESTION 1214:

Business continuity plan development depends most on?

A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee

Answer: B

Explanation: Business continuity is of course a vital activity. However, prior to the creation of a business continuity plan, it is essential to consider the potential impacts of disaster and to understand the underlying risks. It is now widely accepted that both business impact analysis and risk analysis are vital components of the business continuity process. However, many organizations are unsure of how to approach these important disciplines. BIA is important because it provides management level analysis by which an organization assesses the quantitative (financial) and qualitative (non-financial) impacts, effects and loss that might result if the organization were to suffer a Business Continuity E/I/C. The findings from a BIA are used to make decisions concerning Business Continuity Management strategy and solutions.

QUESTION 1215:

Which layer defines the X.25, V.35, X,21 and HSSI standard interfaces?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Answer: D

Explanation: The Physical Layer is the layer that is concerned with the signaling of the message and the interface between the sender or receiver and the medium. The physical layer is generally defined by one of the standards bodies and carries a designation that indicates the characteristics of the connection. Among frequently used physical layers standards are EIA-232-D, ITU V.35, and some of the X series (X.21/X.21bis, for example).

QUESTION 1216:

Related to information security, availability is the opposite of which of the following?

A. Delegation
B. Distribution
C. Documentation

D. Destruction

Answer: D

Explanation: This is the correct term, remember that Availability refers to get access to data when and where you need it. When we talk about destruction, we are saying the opposite, if your information is destroyed, you cant access to it neither when or where you want it. Delegation deals with permissions, distribution deals with deployment and documentation deals with information and how to´s. The term we are looking here is definitively "destruction".

QUESTION 1217:

Which of the following is a disadvantage of a behavior-based ID system?

A. The activity and behavior of the users while in the networked system may not be static enough to effectively implement a behavior-based ID system.
B. The activity and behavior of the users while in the networked system may be dynamic enough to effectively implement a behavior-based ID system.
C. The activity and behavior of the users while in the networked system may not be dynamic enough to effectively implement a behavior-based ID system.
D. The system is characterized by high false negative rates where intrusions are missed.

Answer: A

Explanation: Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. The high false alarm rate is generally cited as the main drawback of behavior-based techniques because the entire scope of the behavior of an information system may not be covered during the learning phase. Also, behavior can change over time, introducing the need for periodic online retraining of the behavior profile, resulting either in unavailability of the intrusion detection system or in additional false alarms. To get the most out of this kind of IDS you need to have very static behavior on your network and the user actions, this is because any new thing is considered dangerous, providing many false-positives but increased security. If you are in a very "dynamic" environment these kind of IDS system is not recommended.

QUESTION 1218:

Which of the following statements pertaining to VPN protocol standards is false?

A. L2TP is a combination of PPTP and L2F.

B. L2TP and PPTP were designed for single point-to-point client to server communication.
C. L2TP operates at the network layer.
D. PPTP uses native PPP authentication and encryption services.

Answer: C

Explanation: The Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability.
PPTP and L2TP are Layer 2 tunneling protocols; both encapsulate the payload in a Point-to-Point Protocol (PPP) frame to be sent across an intermediate network.

QUESTION 1219:

What is the most critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements
C. Accuracy
D. Reliability

Answer: C

Explanation: The principle of biometrics is to use some unique characteristic to identify whether the person is who they say they are. Biometrics works by matching or verifying a person's unique traits with stored data in two categories: physiological characteristics and those that are behavioral. Physical indicators include iris, fingerprint, facial, or hand geometry. Behavior types are usually voiceprints, keystroke dynamics and handwritten signatures. Most biometric technologies require special hardware to convert analog measurements of signatures, voices, or patterns of fingerprints and palm prints, to digital measurement, which computers can read.
The biggest characteristic and problem of biometric implementations today is the accuracy, we must see the level of accuracy before buying a solution, because the technology is not perfect at this time and it can be erroneous sometimes.

QUESTION 1220:

RAID Software can run faster in the operating system because neither use the hardware-level parity drives by?

A. Simple striping or mirroring.
B. Hard striping or mirroring.
C. Simple hamming code parity or mirroring.
D. Simple striping or hamming code parity.

Answer: A

Explanation:
This is true, if we do not use parity in our RAID implementation, like RAID 1 (Mirroring) or RAID 0 (Stripping) we can improve performance because the CPU does not need waste cycles to make the parity calculations. For example this can be achieved in Windows 2000 server through the use of RAID 0 (No fault tolerance, just stripping in 64kb chunks) or RAID 1 (Mirroring through a file system driver). This is not the case of RAID 5 that actually use parity to provide fault tolerance.

QUESTION 1221:

The guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered is?

A. Integrity
B. Confidentiality
C. Availability
D. Identity

Answer: A

Explanation: Here are 2 definitions for Data Integrity:
1. The condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
2. The condition in which data are identically maintained during any operation, such as transfer, storage, and retrieval.
Availability refers to get access to data when and where you need it. Confidentiality deals with encryption and data protection against third party interception. Identity deals with authentication.

QUESTION 1222:

Which of the following is a preventive control?

A. Motion detectors
B. Guard dogs
C. Audit logs
D. Intrusion detection systems

Answer: B

Explanation: This is very obvious. Since we want to prevent something from happening, we can go out and buy some Guard dogs to make the job. You are buying them because you want to prevent something from happening. The intruder will see the dogs and will maybe go back, this prevents an attack, this dogs are a form of preventive control. Motion Detectors and IDS are real-time, Audit Logs are passive.

QUESTION 1223:

What uses a key of the same length as the message?

A. Running key cipher
B. One-time pad
C. Steganography
D. Cipher block chaining

Answer: B

Explanation: The one time pad is the most secure, and one of the simplest of all cryptographic methods. It was invented and patented just after World War I by Gilbert Vernam (of AT&T) and Joseph Mauborgne (USA, later chief of the Signal Corps). The fundamental features are that the sender and receiver each have a copy of an encryption key, which is as long as the message to be encrypted, and each key is used for only one message and then discarded. That key must be random, that is without pattern, and must remain unknown to any attacker. In addition, the key must never be reused, otherwise the cipher becomes trivially breakable. One of its features it's the key length, it's the same as the message.

QUESTION 1224:

Which of the following protocols operates at the session layer (layer 5)?

A. RPC
B. IGMP
C. LDP
D. SPX

Answer: A

Explanation: The socket method of network use is a message-based system, in which one process writes a message to another. This is a long way from the procedural model.
The remote procedure call is intended to act like a procedure call, but to act across the network transparently. The process makes a remote procedure call by pushing its parameters and a return address onto the stack, and jumping to the start of the procedure. The procedure itself is responsible for accessing and using the network. After the remote execution is over, the procedure jumps back to the return address. The calling process then continues. RPC works at the Session layer of the OSI model.

QUESTION 1225:

Which of the following are NOT a countermeasure to traffic analysis?

A. Padding messages
B. Eavesdropping
C. Sending noise
D. Covert channel analysis

Answer: B

Explanation: Lets do this with a elimination process. With padding messages you can countermeasure traffic analysis because you add garbage information to the message to let in end in a fixed length, this can confuse the analyzer. Sending noise on the communication line could also countermeasure analysis because the analyzer don't now how to differentiate between real information and noise. You can also covert channel analysis. Eavesdropping does not apply in this situation, its not considered a counter measure to traffic analysis.

QUESTION 1226:

Which of the following layers of the ISO/OSI model do packet filtering firewalls operate at?

A. Application layer
B. Session layer
C. Network layer
D. Presentation layer

Answer: C

Explanation: Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. These firewalls are normally part of a router, which is a device that receives and forwards packets to networks. "In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator." The criteria used to evaluate a packet include source, destination IP address, destination port, and protocol used. These types of firewalls are low in cost and don't have much of an impact on the network's performance.

QUESTION 1227:

A prolonged high voltage is?

A. Spike

B. Blackout
C. Surge
D. Fault

Answer: C

Explanation: A surge is a prolonged spike, it occur when the power level rises above normal levels and then drop back to normal in less than one second. A Spike occurs when the power level rises above normal levels and stays there for more than 1 or 2 seconds.. A blackout is the total loss of power and a fault is the opposite of a Spike, it's a lowering in the voltage, its usually around one second. The surge is the most dangerous from the listed above.

QUESTION 1228:

How do the Information Labels of Compartmented Mode Workstation differ from the Sensitivity Levels of B3 evaluated systems?

A. Information Labels in CMW are homologous to Sensitivity Labels, but a different term was chosen to emphasize that CMW's are not described in the Orange Book.
B. Information Labels contain more information than Sensitivity Labels, thus allowing more granular access decisions to be made.
C. Sensitivity Labels contain more information than Information Labels because B3+ systems should store more sensitive data than workstations.
D. Information Labels contain more information than Sensitivity Labels, but are not used by the Reference Monitor to determine access permissions.

Answer: D

Explanation: The primary goal of the compartmented mode workstation (CMW) project was to articulate the security requirements that workstations must meet to process highly classified intelligence data. As a basis for the validity of the requirements developed, a prototype was implemented which demonstrated that workstations could meet the requirements in an operationally useful manner while still remaining binary compatible with off-the-shelf software. The security requirements not only addressed traditional security concerns but also introduced concepts in areas such as labeling and the use of a trusted window management system. The CMW labeling paradigm is based on associating two types of security labels with objects: sensitivity levels and information labels. Sensitivity levels describe the levels at which objects must be protected. Information labels are used to prevent data over classification and also provide a mechanism for associating with data those markings that are required for accurate data labeling, but which play no role in access control decisions. The use of a trusted window manager allows users to easily operate at multiple sensitivity levels and provides a convenient mechanism for communicating security information to users in a relatively unobtrusive manner. Information labels are not used by reference monitor, permissions are referenced in Sensibility labels.

QUESTION 1229:

In what security mode can a system be operating if all users have the clearance or authorization and need-to-know to all data processed within the system?

A. Dedicated security mode.
B. System-high security mode.
C. Compartmented security mode.
D. Multilevel security mode.

Answer: A

Explanation: An information-system (IS) security mode of operation wherein each user with direct or indirect
access to the system, its peripherals, remote terminals, or remote hosts, has all of the Following: (a) a valid security clearance for all information within the system; (b) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments, and/or special access programs); and (c) a valid need_to_know for all information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

QUESTION 1230:

What are the three conditions that must be met by the reference monitor?

A. Confidentiality, availability and integrity.
B. Policy, mechanism and assurance.
C. Isolation, layering and abstraction.
D. Isolation, completeness and verifiability.

Answer: D

Explanation: These are three of the main characteristics of a Reference Monitor. You need Isolation, because it cant be of public access, the less access the better. It must have a sense of completeness to provide the whole information and process cycles. It must be verifiable, to provide security, audit and accounting functions.

QUESTION 1231:

While referring to Physical Security, what does Positive pressurization means?

A. The pressure inside your sprinkler system is greater than zero.
B. The air goes out of a room when a door is opened and outside air does not go into the room.

C. Causes the sprinkler system to go off.
D. A series of measures that increase pressure on employees in order to make them more productive.

Answer: B

Explanation:
Positive Pressurization is a condition that exists when more air is supplied to a space than is exhausted, so the air pressure within that space is greater than that in surrounding areas. This condition can cause the situation mentioned above in the answer B, you can make air go out of a room but not enter to it from the outside.

QUESTION 1232:

The baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level

Answer: C

Explanation: According to CISSP documentation, this is the proper term, The Clipping level is used to determine suspicious occurrences that are a production of errors or mistakes. Checkpoint level is not a related term. Ceiling level is not related to baselines. Threshold level is attractive, but is not the correct term. Take a look at your CISSP documentation.

QUESTION 1233:

The most prevalent cause of computer center fires is which of the following?

A. AC equipment
B. Electrical distribution systems.
C. Heating systems
D. Natural causes

Answer: B

Explanation: According to static's, this is the greatest cause, Electrical distribution systems, specially those not installed through standards are very prone to fail and make fire inside places. AC equipment its not very prone to make fire. Natural causes it's a possibility but is definitively not the most prevalent cause. Heating systems are a very rare case of Fire beginners.

QUESTION 1234:

An offsite backup facility intended to operate an information processing facility, having no computer or communications equipment, but having flooring, electrical writing, air conditioning, etc. Is better known as a?

A. Hot site
B. Duplicate processing facility
C. Cold site
D. Warm site

Answer: C

Explanation: A cold site has all the appropriate power requirements, and floor space to install the hardware and to enable you to recreate your computer environment, but does not provide the actual equipment. Many of the companies that provide hot sites also provide cold sites. It may be reasonable for your company to consider creating its won cold site if your company has floor space available in another location than the home site. They require much more outage than Hot sites before operations can be restored.

QUESTION 1235:

Which of the following are necessary components of a Multi-Level Security Policy?

A. Sensitivity Labels and a "system high" evaluation.
B. Sensitivity Labels and Discretionary Access Control.
C. Sensitivity Labels and Mandatory Access Control.
D. Object Labels and a "system high" evaluation.

Answer: C

Explanation: First implemented in Military organizations (and I think even today it's implemented there only), this model was a significant improvement in terms of security policy implementation. This model made implementation of complex security policies very simple. It's specifications are present in the orange book from DoD. In this model, every object is assigned a sensitivity label. Also, every user is assigned a sensitivity label. If a user's sensitivity label is greater than or equal to the sensitivity label, he is allowed access to the object, otherwise, he is denied access. This methodology is used for creating a hierarchy of access. We can say that this method is used for partitioning the organization hierarchy horizontally.
Multi-Level Security is considered a Mandatory Access Control method.

QUESTION 1236:

Which of the following, used to extend a network, has a storage capacity to store frames

and act as a store-and-forward device?

A. Bridge
B. Router
C. Repeater
D. Gateway

Answer: A

Explanation: A bridge is a network device that connects two similar network segments together. The primary function of a bridge is to keep traffic separated on both sites of the bridge. Traffic is allowed to pass through the bridge only if the transmission is intended for a station in the opposite side. Bridges operate at the data link layer of the OSI model an provides two different collision domains in Ethernet, but they only provide one broadcast domain for layer 3 an up of the OSI model. The bridge can store frames and forward them in many forms like Cut-through and Store and Forward.

QUESTION 1237:

Which of the following is addressed by Kerberos?

A. Authorization and authentication.
B. Validation and integrity.
C. Confidentiality and integrity.

Answer: C

Explanation: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well. Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt (confidentiality) all of their communications to assure privacy and data integrity as they go about their business.

QUESTION 1238:

Access Control techniques do not include which of the following choices?

A. Relevant Access Controls
B. Discretionary Access Control
C. Mandatory Access Control
D. Lattice Based Access Control

Answer: A

Explanation: Relevant Access Controls are not included as a Access Control Technique. Lattice-based access control models were developed in the early 1970s to deal with the confidentiality of military information. In the late 1970s and early 1980s, researchers applied these models to certain integrity concerns. Later, application of the models to the Chinese Wall policy, a confidentiality policy unique to the commercial sector, was demonstrated. Discretionary control is the most common type of access control mechanism implemented in computer systems today. The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. Discretionary Access control security differs from mandatory access control security in that it implements the access control decisions of the user. Mandatory controls are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

QUESTION 1239:

Why is public key cryptography recommended for use in the process of securing facsimiles during transmission?

A. Keys are never transmitted over the network.
B. Data compression decreases key change frequency.
C. Key data is not recognizable from facsimile data.
D. The key is securely passed to the receiving machine.

Answer: D

Explanation: In this method of cryptography we use 2 keys, one to encrypt the data, and another to decrypt it. In Public Key Cryptography, the users have a public and a private key, the public key is of free distribution and is usually published in a directory, while the private keys must be keep secure. This allows the keys to pass in a secure fashion to the receiving machine, its because the public key is not confidential and can be send through a secure channel. You need to use a certification authority to make this kind of cryptography work.

QUESTION 1240:

Database views are not used to:

A. Implement referential integrity.
B. Implement least privilege.
C. To implement content-dependent access restrictions.
D. Implement need-to-know.

Answer: A

Explanation: A View is a display of one or more table shows that shows the table data. You can even retrieve part of the table and display the same to the user. Before a user is able to use a view, they must have both, permission on the view and all dependent objects. Views can also be used to implement security, for example you can create a view that only shows 3 of 5 columns contained in a table. Views are not used to provide integrity you can use constraints, rule or other components of database systems.

QUESTION 1241:

Which of the following is most concerned with personnel security?

A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls.

Answer: B

Explanation: Personnel security always have to deal more with Operational controls, Operational controls provide the guidelines and the correct procedures to implement the different operations. Management controls are usually used only by managers. Human resources and Technical Controls are not related to personal security as the question states. See the different control definitions in your CISSP documentation.

QUESTION 1242:

Which of the following statements pertaining to the Trusted Computer System Evaluation Criteria (TCSEC) is incorrect?

A. With TCSEC, functionality and assurance are evaluated separately.
B. TCSEC provides a means to evaluate the trustworthiness of an information system.
C. The Orange book does not cover networks and communications.
D. Data base management systems are not covered by the TCSEC.

Answer: A

Explanation: TCSEC does not separate functionality and assurance from evaluation. It makes them a combined criteria. Just to remember, The Trusted Computer System Evaluation Criteria (TCSEC) is a collection of criteria used to grade or rate the security offered by a computer system product. The TCSEC is sometimes referred to as "the Orange Book" because of its orange cover (Orange Book deals with networks and communications). The current version is dated 1985 (DOD 5200.28-STD, Library No.S225,711) The TCSEC, its interpretations and guidelines all have different color covers, and are sometimes known as the "Rainbow Series". Database management is also covered in TCSEC.

The Orange Book is used to evaluate whether a product contains the security properties the vendor claims it does and whether the product is appropriate for a specific application or function. The Orange Book is used to review the functionality, effectiveness, and assurance of a product during its evaluation, and it uses classes that were devised to address typical patterns of security requirements.
- Shon Harris, "CISSP All-in-One Exam Guide", 3rd Ed, p 302.

QUESTION 1243:

Which of the following could illegally capture network user passwords?

A. Data diddling
B. Sniffing
C. Spoofing
D. Smurfing

Answer: B

Explanation: Sniffing is the action of capture the information going over the network. Most popular way of connecting computers is through Ethernet. Ethernet protocol works by sending packet information to all the hosts on the same circuit. The packet header contains the proper address of the destination machine. Only the machine with the matching address is suppose to accept the packet. A machine that is accepting all packets, no matter what the packet header says, is said to be in promiscuous mode. Because, in a normal networking environment, account and password information is passed along Ethernet in clear-text, it is not hard for an intruder to put a machine into promiscuous mode and by sniffing, compromise all the machines on the net by capturing password in an illegal fashion.

QUESTION 1244:

Which trusted facility management concept implies that two operators must review and approve the work of each other?

A. Two-man control
B. Dual control
C. Double control
D. Segregation control

Answer: A

Explanation: The proper term for this trusted facility management concept is "Two-man Control", it means that two people must work and approve each others work to provide increased security and eliminate the possibility of one of them to hurt the company. For example they can only make changes to the system if both of them authenticate with their retina at the same time at the data center and enter their secret password This kind of work fashion is only used in highly secure environments, its not very common.

QUESTION 1245:

There are more than 20 books in the Rainbow Series. Which of the following covers password management guidelines?

A. Orange Book
B. Green Book
C. Red Book
D. Lavender Book

Answer: B

Explanation: The DoD Password Management Guideline was published at 12 April 1985, it is also called the "Green Book" because of the color of its cover. Here is the password definition according to it: "A character string used to authenticate an identity. Knowledge of the password that is associated with a user ID is considered proof of authorization to use the capabilities associated with that user ID."

QUESTION 1246:

Which of the following is an ip address that is private? (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

A. 172.5.42.5
B. 172.76.42.5
C. 172.90.42.5
D. 172.16.42.5

Answer: D

Explanation: The IP address 172.16.42.5 is contained in a class B reserved network, IANA reserved the 172.16.0.0 through 172.31.255.255 networks for internal use, this network its not routable in Internet and its commonly used in intranets. Class B networks are used in medium-sized networks. In class B networks, the two high order bits are always 10, and then remaining bits are used to define 16.384 networks, each with as many as 65.534 hosts attached. Examples of valid Class B networks include Microsoft and Exxon.

QUESTION 1247:

How fast is private key cryptography compared to public key cryptography?

A. 10 to 100 times faster.
B. 100 to 1000 times faster.
C. 1000 to 10000 times faster.
D. 10000 to 20000 times faster.

Answer: C

Explanation: Since Private Key encryption (Symmetric) only has one key for encrypt-decrypt, you need to use an alternative way to pass the shared secret in a secure manner, in our days, it's usually done by telephone or some secure methods that not involve the channel you are trying to secure. Also, since you need one different key to encrypt-decrypt every connection, the number of keys gets huge in a little time, for example, if we have 10 users trying to communicate between themselves, we have 100 different encryption keys to manage. There is an advantage for Private key encryption, the encryption is very fast, about 1000 / 10000 times faster than asymmetric encryption.

QUESTION 1248:

The continual effort of making sure that the correct policies, procedures and standards are in place and being followed is described as what?

A. Due care
B. Due concern
C. Due diligence
D. Due practice

Answer: A

Explanation: "Due care means that a company did all that it could have reasonable done to try and prevent security breaches, and also took the necessary steps to ensure that if a security breach did take place, the damages were reduced because of the controls or countermeasures that existed. Due care means that a company practiced common sense and prudent management practices with responsible actions. Due diligence meants that the company properly investigated all of their possible weaknesses and vulnerabilities before carrying out any due care practices.
The following list describes some of the actions required to show that due care is being properly practiced in a corporation:
Adequate physical and logical access controls
Adequate telecommunication security, which could require encryption
Proper information, application, and hardware backups
Disaster recovery and business continuity plans
Periodic review, drills, tests, and improvement in disaster recovery and business continuity plans
Properly informing employees of expected behavior and ramifications of not following these expectations
Developing a security policy, standards, procedures, and guidelines
Performing security awareness training
Running updated antivirus software
Periodically performing penetration test from outside and inside the network
Implementing dial-back or preset dialing features on remote access applications
Abiding by and updating external service level agreements (SLAs)

Ensuring that downstream security responsibilities are being met
Implementing measure that ensure software piracy is not taking place
Ensuring that proper auditing and reviewing of those audit logs are taking place
Conducting background checks on potential employees"
Pg. 616 Shon Harris: CISSP Certification All-in-One Exam Guide

---

QUESTION 1249:

Which tape format type is mostly used for home/small office backups?

A. Quarter Inch Cartridge drives (QIC)
B. Digital Linear Tapes (DLT)
C. 8mm tape
D. Digital Audio Tape (DAT)

Answer: A

Explanation: QIC technology utilizates belt-driven dual-hub cartridges containing integral tape motion and guidance mechanisms, providing a rich spectrum of compatible solutions across a wide range of PC system platforms. QIC reliability is unsurpassed by any other removable storage technology. Reliability can be measured both in mean-time-between failure (MTBF) and, more practically, as a function of drive duty cycles. QIC has a worldwide installed base in excess of 15 million drives -- more than twice that of any alternate removable storage technology -- a level of acceptance that would have been unachievable without rock-solid reliability. QIC is the most common tape solution for SOHO.

QUESTION 1250:

In an organization, an Information Technology security function should:

A. Be a function within the information systems function of an organization.
B. Report directly to a specialized business unit such as legal, corporate security or insurance.
C. Be lead by a Chief Security Officer and report directly to the CEO.
D. Be independent but report to the Information Systems function.

Answer: C

Explanation: This is one of the best practices because its not good to be lead and report to the same person, in that case, that person could take possession of everything that is happening and hurt the enterprise, we can't let that to happen with security concerns. The best practice is to always be lead by a different person that the one you report to, this can be checked in real life. An advice, always try to report to the highest person you can inside the company.

QUESTION 1251:

Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

A. Business and functional managers.
B. IT Security practitioners.
C. System and information owners.
D. Chief information officer.

Answer: C

Explanation: This is true, the people who own the information and the equipment are the ones who need to ensure they are making everything to get integrity, confidentiality and availability. The security professionals can develop policies and show how to keep the environment secure, but it depends on the owners of the actual data to achieve the security.

QUESTION 1252:

The act of requiring two of the three factors to be used in the authentication process refers to?

A. Two-Factor Authentication
B. One-Factor Authentication
C. Bi-Factor Authentication
D. Double Authentication

Answer: A

Explanation: Two-Factor Authentication is a security process that confirms user identities using two distinctive factors-something you know, such as a Personal Identification Number (PIN), and something you have, such as a smart card or token.
The overall strength of Two-Factor Authentication lies in the combination of both factors, something you know and something you have.

QUESTION 1253:

This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes", similar to WORMs, (Write Once, Read Many)

A. Hierarchical Storage Management (HSM).
B. Hierarchical Resource Management (HRM).
C. Hierarchical Access Management (HAM).
D. Hierarchical Instance Management (HIM).

Answer: A

Explanation: Hierarchical Storage Management originated in the mainframe world where it was used to minimize storage costs. The HSM name signifies that the software has the intelligence to move files along a hierarchy of storage devices that are ranked in terms of cost per megabyte of storage, speed of storage and retrieval, and overall capacity limits. Files are migrated along the hierarchy to less expensive forms of storage based on rules tied to the frequency of data access. File migration and retrieval is transparent to users. Two major factors, data access response time and storage costs determine the appropriate combination of storage devices used in HSM. A typical three tier strategy may be composed of hard drives as primary storage on the file servers, rewritable optical as the secondary storage type, and tape as the final tertiary storage location. If faster access is required, a hard drive can be considered as an alternative to optical for secondary storage, and WORM (Write Once, Read Many) optical can also be implemented, in place of tape, as the final storage destination.

QUESTION 1254:

Which of the following elements is not included in a Public Key Infrastructure (PKI)?

A. Timestamping
B. Lightweight Directory Access Protocol (LDAP)
C. Certificate revocation
D. Internet Key Exchange (IKE)

Answer: D

Explanation: Public key cryptography is one mechanism that is often used to fulfill the security requirements necessary to conduct electronic transactions over public networks. PKI (public key infrastructure) and cryptography based solutions are taking the lead in secure e-commerce. PKI addresses nonrepudiation of identity using a dual-key encryption system that allows users to uniquely sign documents with a digital signature. Public key cryptography uses pairs of keys, each pair consisting of one public key and one private key. Information encrypted with one key in the pair can only be decrypted with the other key. LDAP is issued to bring user information and Timestamping to track changes over time. PKI also relies on certificated and CRL (Certificate Revocation list) to discard compromised, expired digital certificates.

QUESTION 1255:

Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?

A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing

Answer: B

Explanation: An addressing mode found in many processors' instruction sets where the instruction contains the address of a memory location which contains the address of the operand (the "effective address") or specifies a register which contains the effective address. Indirect addressing is often combined with pre- or post- increment or decrement addressing, allowing the address of the operand to be increased or decreased by one (or some specified number) either before or after using it.

QUESTION 1256:

Creation and maintenance of intrusion detection systems and processes for the following is one of them identify it:

A. Event nonrepudiation
B. Event notification
C. Netware monitoring
D. Guest access

Answer: B

Explanation: There is not much to explain or comment in here, when you administer an IDS system you have to deal with the maintenance and creation of event notification processes, this have to be reviewed every certain time. This is a well known topic for any Intrusion detection system administrator. This notifications will save your life when your network is being attacked and you get real time notifications that will allow you to shut down your external interface before the attacker gets what he was looking for.

QUESTION 1257:

Which of the following is true related to network sniffing?

A. Sniffers allow an attacker to monitor data passing across a network.
B. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods,
C. Sniffers take over network connections.
D. Sniffers send IP fragments to a system that overlap with each other.

Answer: A

Explanation: Sniffing is the action of capture / monitor the traffic going over the network. Because, in a normal networking environment, account and password information is passed along Ethernet in clear-text, it is not hard for an intruder to put a machine into promiscuous mode and by sniffing, compromise all the machines on the net by capturing password in an illegal fashion.

QUESTION 1258:

Which of the following protocols is not implemented at the Internet layer of the TCP/IP protocol model?

A. User datagram protocol (UDP)
B. Internet protocol (IP)
C. Address resolution protocol (ARP)
D. Internet control message protocol (ICMP)

Answer: A

Explanation: UDP (User Datagram Protocol) is a communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. UDP is implemented at the Transport layer of the TCP/IP protocol model.

QUESTION 1259:

Which of the following is used to help business units understand the impact of a disruptive event?

A. A risk analysis.
B. A business impact assessment.
C. A vulnerability assessment.
D. A disaster recovery plan.

Answer: B

Explanation: A Business impact assessment can provide information in combination with the BIA to the different business units about how can an attack impact or disrupt the business. Every disaster recovery plan should include an study containing a BIA and a Business impact assessment to better understand how is going to be in the case that a business continuity disruptive event takes place.

QUESTION 1260:

A contingency plan should address?

A. Potential risks
B. Residual risks

C. Identified risks
D. All of the above

Answer: B

Explanation: This is true, as stated in CISSP documentation, you should address any possible "Residual Risk" at your contingency plan to minimize business impact when you are in a downtime situation. The identified Risks and the Potential Risks are not identified there, they are identified earlier.

QUESTION 1261:

In the OSI/ISO model, at what level is SET (SECURE ELECTRONIC TRANSACTION PROTOCOL) provided?

A. Application
B. Network
C. Presentation
D. Session

Answer: A

Explanation: This protocol was created by VISA and MasterCard as a common effort to make the buying process over the Internet secure through the distribution line of those companies. It is located in layer 7 of the OSI model, the application layer. SET uses a system of locks and keys along with certified account IDs for both consumers and merchants. Then, through a unique process of "encrypting" or scrambling the information exchanged between the shopper and the online store, SET ensures a payment process that is convenient, private and most of all secure.

QUESTION 1262:

A packet filtering firewall looks at the data packet to get information about the source and destination addresses of an incoming packet, the session's communications protocol (TCP, UDP or ICMP), and the source destination application port for the?

A. Desired service
B. Dedicated service
C. Delayed service
D. Distributed service.

Answer: A

Explanation: This is true, the packets filters show the desired service port (Remember that they are layer 3 devices), this is because you can have many different referenced port number in the destination port field of the different packets. You have to look for the

well-known port numbers of the service desired. For example, look in port 80 for HTTP and port 21 for FTP. This is the correct terminology, see the features of Packet Filters in your CISSP documentation.

QUESTION 1263:

Packet Filtering Firewalls system is considered a?

A. First generation firewall.
B. Second generation firewall.
C. Third generation firewall.
D. Fourth generation firewall.

Answer: A

Explanation: Firewall technology is a young but quickly maturing industry. The first generation of firewall architectures has been around almost as long as routers, first appearing around 1985 and coming out of Cisco's IOSsoftware division. These firewalls are called packet filter firewalls. However, the first paper describing the screening process used by packet filter firewalls did not appear until 1988, when Jeff Mogul from Digital Equipment Corporation published his studies. At this time we are in the Fourth generation of firewall devices and software.

QUESTION 1264:

When should a post-mortem review meeting be held after an intrusion has been properly taken care of?

A. Within the first three months after the investigation of the intrusion is completed.
B. Within the first week after prosecution of intruders have taken place, whether successful or not.
C. Within the first month after the investigation of the intrusion is completed.
D. Within the first week of completing the investigation of the intrusion.

Answer: D

Explanation: As stated in CISSP documentation, you should make post mortem review meetings after taking care of the intrusion, and no more than one week after the facts. Its not a good practice to wait more than this time, it's a matter of common sense too, three months, one month, 2 weeks, its too much time.

QUESTION 1265:

Which of the following can be used as a covert channel?

A. Storage and timing.

B. Storage and low bits.
C. Storage and permissions.
D. Storage and classification.

Answer: A

Explanation: Those are the proper elements, you can use these two to achieve a covert channel. Low bits is not a term related to covert channels. Permissions are related to authentication, they do not achieve what the question wants. Also, classification is could not selected as a correct choice.
Check your official CISSP documentation to see what can be used as a covert channel.
"An active variation on eavesdropping is called Covert Channel eavesdropping, which consists of using a hidden unauthorized network connection to communicate unauthorized information. A Covert Storage Channel operates by writing information to storage by one process and then reading by using another process from a different security level. A Covert Timing Channel signals information to another process by modulating its own resource use to affect the response time of another." Pg. 101 Krutz: The CISSP Prep Guide: Gold Edition

---

QUESTION 1266:

Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model.
B. The modified Waterfall model.
C. The Spiral model.
D. The Critical Patch Model (CPM).

Answer: C

Explanation:
The spiral model for software engineering has evolved to encompass the best features of the classic waterfall model, while at the same time adding an element known as risk analysis. The spiral model is more appropriate for large, industrial software projects and has four main blocks/quadrants. Each release or version of the software requires going through new planning, risk analysis, engineering and customer evaluation phases and this is illustrated in the model by the spiral evolution outwards from the center. For each new release of a software product, a risk analysis audit should be performed to decide whether the new objectives can be completed within budget (time and costs), and decisions have to be made about whether to proceed. The level of planning and customer evaluation is missing from the waterfall model which is mainly concerned with small software programs. The spiral model also illustrated the evolutionary development of software where a solution may be initially proposed which is very basic (first time round the loop) and then later releases add new features and possibly a more elaborate GUI.

QUESTION 1267:

What is not true with pre-shared key authentication within IKE / IPsec protocol:

A. Pre-shared key authentication is normally based on simple passwords.
B. Needs a PKI to work.
C. Only one preshared key for all VPN connections is needed.
D. Costly key management on large user groups.

Answer: B

Explanation: Pre-Shared Secret is usually used when both ends of the VPN lacks access to a compatible certificate server. Once you have defined all the endpoints in your VPN, you can establish a password that is used to authenticate the other end of the connection, this is the Pre-Shared secret. Since you are using Pre-Shared key because you don't have an available / compatible certificate server, IPSEC and IKE do not need to use PKI in this case (that actually provides the certificate server infrastructure).

QUESTION 1268:

Which question is NOT true concerning Application Control?

A. It limits end users of applications in such a way that only particular screens are visible.
B. Only specific records can be requested choice.
C. Particular uses of the application can be recorded for audit purposes.
D. Is non-transparent to the endpoint applications so changes are needed to the applications involved.

Answer: D

Explanation: Application control provides a transparent feeling to endpoint applications when changes are needed, this is one of the features of it. With application control you can audit certain use of the applications involved and only specify record of your choice. There is also the possibility to limit the end users applications to provide access to only certain screens. Check your CISSP documentation about Application Control.

QUESTION 1269:

In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use?

A. Screened subnets
B. Digital certificates
C. Encrypted Virtual Private Networks
D. Encryption

Answer: C

Explanation: This is the correct answer, since firewall does not mean "VPN" we have to select "Encrypted Virtual Private Networks". With a VPN and encryption we can provide secure communication in a transparent way for the users between the endpoints achieving "Confidentiality". This confidentiality is achieved through encryption, and this encryption relies on encryption algorithms like AES, DES, CAST and others. Screened Subnet are not related to secure data over public networks, it's a place to put our network services accessible from the outside. Digital certificates do not provide confidentiality, they only provide integrity.

QUESTION 1270:

What is necessary for a subject to have write access to an object in a Multi-Level Security Policy?

A. The subject's sensitivity label must dominate the object's sensitivity label.
B. The subject's sensitivity label subordinates the object's sensitivity label.
C. The subject's sensitivity label is subordinated by the object's sensitivity label.
D. The subject's sensitivity label is dominated by the object's sensitivity label.

Answer: A

QUESTION 1271:

What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own ban account?

A. Data fiddling
B. Data diddling
C. Data hiding
D. Data masking

Answer: B

Explanation: This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed. This kind of attack was used in the past to make what is stated in the question, steal small quantities of money and transfer them to the attackers account. See "Data deddling crimes" on the Web.
The most correct answer is 'Salami', but since that is not an option the most correct answer is data diddling.
"A salami attack is committing several small crimes with the hope that the overall larger crime will go unnoticed. ....An example would be if an employee altered a banking software program to subtract 5 cents from each of the bank's customers' accounts once a month and moved this amount to the employee's bank account. If this happened to all of the bank's 50,000 customer

accounts, the intruder could make up to $ 30,000 a year.
Data diddling refers to the alteration of existing data. Many times this modification happens before it is entered into an application or as soon as it completes processing and is outputted from an application.
There was an incident in 1997, in Maryland, where a Taco Bell employee was sentenced to ten years in jail because he reprogrammed the drive-up window cash register to ring up ever 42.99 order as one penny. He collected the full amount from the customer, put the penny in the till, and pocketed the other $2.98. He made $3600 before his arrest."
Pg. 602-603 Shon Harris: All-In-One CISSP Certification Exam Guide

---

QUESTION 1272:

Which of the following is unlike the other three?

A. El Gamal
B. Teardrop
C. Buffer Overflow
D. Smurf

Answer: A

Explanation: Options B, C and D are all Denial of Service attacks. El Gamal is the Diffie-Hellman key exchange algorithm and is usually described as an active exchange of keys by two parties. The buffer overflow attack objective is consume the available memory for the TCP/IP protocol stack to make the machine crash. Teardrop and Smurf are DoS attacks that make use of spoofing.

QUESTION 1273:

Phreakers are hackers who specialize in telephone fraud. What type of telephone fraud manipulates the line voltage to receive a tool-free call?

A. Red Boxes
B. Blue Boxes
C. White Boxes
D. Black Boxes

Answer: D

Explanation: A Black Box is a device that is hooked up to your phone that fixes your phone so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to 1/2 hour, after 1/2 hour the Phone Co. gets suspicious, and then you can guess what happens.
The Red box basically simulates the sounds of coins being dropped into the coin slot of a payphone. The traditional Red Box consisting of a pair of Wien-bridge oscillators with the timing controlled by 555 timer chips. The Blue Box, The mother of all boxes, The first box in

history, which started the whole phreaking scene. Invented by John Draper (aka "Captain Crunch") in the early 60s, who discovered that by sending a tone of 2600Hz over the telephone lines of AT&T, it was possible to make free calls.
The White Box turns a normal touch tone keypad into a portable unit. This kind of box can be commonly found in a phone shop.

QUESTION 1274:

Which of the following groups represents the leading source of computer crime losses?

A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees

Answer: D

Explanation: This can be checked at the computer crime static's on the web. Most of the attacks, actually 70% of them, come from inside the company, and 80% of them from employees of it. This is a reality, when we protect our infrastructure be sure to give great importance to internal security, we don't when is one of the company employees going to make a strike. Hackers are also important, but less than our own employees.

QUESTION 1275:

Which of the following steps should be performed first in a business impact analysis (BIA)?

A. Identify all business units within the organization.
B. Evaluate the impact of disruptive events.
C. Estimate the Recovery Time Objectives (RTO).
D. Evaluate the criticality of business functions.

Answer: A

Explanation: Remember that when we talk about a BIA (Business Impact Analysis), we are analyzing and identifying possible issues about our infrastructure. It's an analysis about the business, the process that it relays on, the level of the systems and a estimative of the financial impact, or in other words, how much many we loose with our systems down. The first step on it should always be the identifying of the business units in the company. You can then go to other requirements like estimate losses and downtime costs.

QUESTION 1276:

Which of the following embodies all the detailed actions that personnel are required to follow?

A. Standards

B. Guidelines
C. Procedures
D. Baselines

Answer: C

Explanation: As stated in the dictionary, here are 3 definitions of procedure:
1. A manner of proceeding; a way of performing or effecting something: standard procedure.
2. A series od steps taken to accomplish an end: a medical procedure; evacuation procedures.
3. A set of established forms or methods for conducting the affairs of an organized body such as a business, club, or government.
Its pretty visible that this is the term we are looking for as stated in the questions, you can check your CISSP documentation too.

QUESTION 1277:

Immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases) is?

A. Coaxial cable
B. Twisted Pair cable
C. Axial cable
D. Fiber Optic cable

Answer: D

Explanation: Since fiber optics does not use electrical signals to transmit the information (it uses lights that goes through the mirrored silvered cable from source to end), its not affected by EMI (Electro Magnetic Interference) like other copper transmission methods like 10base5 and 10base2, therefore EMI does not affect the possible transmission distance. Fiber optics can have a great distance between end points, much greater than the copper transmission methods. Examples of Fiber optics standards are: 100BaseFX and 1000BaseFX.

QUESTION 1278:

Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or cassette?

A. Degaussing
B. Parity Bit Manipulation
C. Certification
D. Buffer overflow

Answer: A

Explanation: An alternating current (AC) bulk eraser (degausser) is used for complete erasure of data and other signal on magnetic media. Degaussing is a process where magnetic media is exposed to a powerful, alternating magnetic field. Degaussing removes any previously written data, leaving the media in a magnetically randomized (blank) state. The degausser must subject the media to an alternating magnetic field of sufficient intensity to saturate the media and then by slowly withdrawing or reducing the field leaves the magnetic media in a magnetically neutral state.

QUESTION 1279:

Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Answer: A

Explanation: The Prototype Phase is also called the "Proof of Concept" Phase. Whether it's called one or the other depends on what the creator is trying to "prove." If the main deliverable of the Phase includes a working version of the product's technical features, it's a "prototype." If the main deliverable just looks like it has the product's technical features, then it's a "proof of concept."
Prototypes can save time and money because you can test some functionality earlier in the process. You don't have to make the whole final product to begin testing it.

QUESTION 1280:

The IS security analyst's participation in which of the following system development life cycle phases provides maximum benefit to the organization?

A. System requirements definition.
B. System design.
C. Program development.
D. Program testing.

Answer: B

QUESTION 1281:

Controls are implemented to?

A. Eliminate risk and reduce the potential for loss.
B. Mitigate risk and eliminate the potential for loss.
C. Mitigate risk and reduce the potential for loss.

D. Eliminate risk and eliminate the potential for loss.

Answer: C

Explanation: That's the essence of Controls, you put them in your environment to minimize the impact of a potential loss, with them you can also mitigate the risk and obtain the first through this.
Controls are a very good practice to secure an environment, they should be considered by any security professional, CISSP or not, the risk should be minimized as much as you can.

QUESTION 1282:

A circuit level gateway is _____ when compared to an application level firewall.

A. Easier to maintain.
B. More difficult to maintain.
C. More secure.
D. Slower

Answer: A

Explanation: Since circuit level gateways are not as high in the OSI model for the inspection as Application level firewalls, they are easier to maintain and configure. Application layer firewalls are up to layer 7 of the OSI model and provide a great bunch of options and complex configurations. Application layer firewalls are more secure than circuit level gateway because they can track and analyze information up to layer 7, a drawback to this, is that this functionality makes them slower.

QUESTION 1283:

In IPSec, if the communication mode is gateway-gateway or host-gateway:

A. Only tunnel mode can be used.
B. Only transport mode can be used.
C. Encapsulating Security Payload (ESP) authentication must be used.
D. Both tunnel and transport mode can be used.

Answer: C

Explanation: ESP or Encrypted Security Payload, is a header that when its added to an IP datagram, protects the confidentiality, integrity and authenticity of the data. AH and ESP can be used separately or together. As defined by the IETF, IPSec transport mode can only be used when both the source and destination systems understand IPSEC. In most cases you deploy IPSEC in tunnel mode. In this transport mode (gateway to gateway and gateway to host) you must use ESP for authentication.

QUESTION 1284:

Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model

Answer: C

Explanation: The Clark-Wilson model was developed to address security issues in commercial environments. The model uses two categories of mechanisms to realize integrity: well-formed transactions and separation of duty. It defines a constraint data item, a integrity verification and a transformation of that object. A possible way to represent a constraint that only certain trusted programs can modify objects is using application:checksum condition, where the checksum ensures authenticity of the application. Another way is using application:endorser condition, which indicates that a valid certificate, stating that the application has been endorsed by the specified endorser, must be presented. Static separation of duty is enforced by the security administrator when assigning group membership. Dynamic separation of duty enforces control over how permissions are used at the access time

---

QUESTION 1285:

Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?

A. In order to facilitate recover, a single plan should cover all locations.
B. There should be requirements for to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
C. In its procedures and tasks, the plan should refer to functions, not specific individuals.
D. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.

Answer: A

Explanation: This is not the best practice, even more for the CISSP exam. Continuity / recovery plans should be make for every location in separate. This is because when there is a disaster, Its not usually in all the different locations, its better to have one plan for each of it so you can use and follow only the plan of the affected site and don't bother the other ones.

QUESTION 1286:

What are suitable protocols for securing VPN connections?

A. S/MIME and SSH
B. TLS and SSL
C. IPsec and L2TP
D. PKCS# and X.509

Answer: C

Explanation: Both of them can be used to create and secure VPN's. The Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. IPSec is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies ways for securing private information transmitted over public networks. Services supported by IPSec include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering) and replay protection (defense against unauthorized re-sending of data). It work on layer 3 of the OSI model and is the most common protocols used to create VPNs.

QUESTION 1287:

Which of the following questions is less likely to help in assessing identification and authentication controls?

A. Is a current list maintained and approved of authorized users and their access?
B. Are passwords changed at least every ninety days or earlier if needed?
C. Are inactive user identifications disabled after a specified period of time?
D. Is there a process for reporting incidents?

Answer: D

Explanation: We just some common sense to answer this question correctly, why are we going to ask about process reporting for incidents?, does is help relating to identification and authentication?, I don't think so. There are other more interesting questions, password deal with authentication, inactive user Ids are also related to identification. But the most important to me, know if there is a list with authorized users and their current access, this can help you to identify unauthorized activities.

QUESTION 1288:

The primary purpose for using one-way encryption of user passwords within a system is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
B. It prevents an unauthorized person from reading or modifying the password list.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting passwords.

Answer: B

Explanation: This kind of encryption flavor increases security for passwords, if you use a one way encryption algorithm, you know that the encryption is not reversible, you cannot get the original value that you provided as a password from the resulting hash with any key or algorithm. This increase security in the way that when a person see the password list, it will only see the hash values and cannot read the original password or modify them without getting corruption.

QUESTION 1289:

The security of a computer application is most effective and economical in which of the following cases?

A. The system is optimized prior to the addition of security.
B. The system is procured off-the-shelf.
C. The system is customized to meet the specific security threat.
D. The system is designed originally to provide the necessary security.

Answer: D

Explanation: This is very obvious, if your system is designed from the ground up to provide security, its going to be cheaper and more effective at the end, because you don't need re-analysis, re-coding, and re-structure of the internal code of the computer application. If you don't address security at the beginning you will also need to spend time and money reviewing the code to try to put the security infrastructure in some place of it.

QUESTION 1290:

In the following choices there is one that is a typical biometric characteristics that is not used to uniquely authenticate an individual's identity?

A. Retina scans
B. Iris scans
C. Palm scans
D. Skin scans

Answer: D

Explanation: Answer A, B and C can be used to uniquely identify a person, but in the case of the Skin, there are no unique characteristics that can differentiate two distinct

individuals in an acceptable accurate way. In the case of the IRIS and the Retina, there are not two of them equal. In the case of the palm, every person has different marks on it. The skin is common to all and does not have specific textures or marks to make it unique in comparison to another individual.

QUESTION 1291:

Which of the following proves or disproves a specific act though oral testimony based on information gathered through the witness's five senses?

A. Direct evidence
B. Circumstantial evidence
C. Conclusive evidence
D. Corroborative evidence

Answer: A

Explanation: As stated in the CISSP documentation, "If you want to make achieve the validation or revalidation of the oral testimony of a witness, you need to provide physical, direct evidence to backup your statements and override the five senses of an oral testimony". Circumstantial or Corroborative evidence is not enough in this case, we need direct, relevant evidence backing up the facts.

QUESTION 1292:

Which of the following would be defined as an absence of safeguard that could be exploited?

A. A threat
B. A vulnerability
C. A risk
D. An exposure

Answer: B

Explanation: In IT, a vulnerability is the weakness of a System to be exploited and corrupted by a security hole. There is always a risk that our systems been vulnerable, with security we cannot make the risk to be 0%, but we can decrease the possibility of a threat becoming in a successful attack through one of those vulnerabilities. There is no system without vulnerabilities, we need to patch our systems frequently to reduce the risk of a threat through a vulnerability of one of our systems.

QUESTION 1293:

Which of the following is a LAN transmission protocol?

A. Ethernet

B. Ring topology
C. Unicast
D. Polling

Answer: C
Reference: "LAN Transmission Methods. LAN data is transmitted from the sender to one or more receiving stations using either a unicast, multicast, or broadcast transmission." pg 528
Hansche: Official (ISC)2 Guide to the CISSP Exam

QUESTION 1294:

Why would a database be denormalized?

A. To ensure data integrity.
B. To increase processing efficiency.
C. To prevent duplication of data.
D. To save storage space.

Answer: B

Explanation: Denormalization is the process of attempting to optimize the performance of data storage by adding redundant data. It is necessary because current DBMSs are not fully relational. A fully relational DBMS would be able to preserve full normalization at the logical level, while allowing it to be mapped to performance-tuned physical level. Database designers often justify denormalization on performance issues, but they should note that logical denormalization can easily break the consistency of the database, one of the all-important ACID properties. However, a designer can achieve the performance benefits while retraining consistency by performing denormalization at a physical level; such denormalization is often called caching.

QUESTION 1295:

Under "Named Perils" form of Property insurance

A. Burden of proof that particular loss is covered is on Insurer.
B. Burden of proof that particular loss is not covered is on Insurer.
C. Burden of proof that particular loss is covered is on Insured.
D. Burden of proof that particular loss is not covered is on Insured.

Answer: C

Explanation:
Here is something on "Named Perils" for your understanding: "Named Perils is a formal and specific listing of perils covered in a policy providing property insurance. A policy covering for damage by fire is said to cover for "the named peril" of fire". As you can see, Answer C is correct.

QUESTION 1296:

The following is not true:

A. Since the early days of mankind humans have struggled with the problems of protecting assets.
B. The addition of a PIN keypad to the card reader was a solution to unreported card or lost card problem.
C. There has never been of problem of lost keys.
D. Human guard is an inefficient and sometimes ineffective method of protecting resources.

Answer: C

Explanation: This is absolutely false, this problem can be seen almost anywhere. There have always been trouble with the lost of keys. Some of those looses are more important than others, its not the same to lost the key of the company safe box, that lost the key of you locker with that contains your shoes.
This is obviously an incorrect statement, answer C is the one in here.
"Unfortunately, using security guards is not a perfect solution. There are numerous disadvantages to deploying, maintaining, and relying upon security guards. Not all environments and facilities support security guards. This may be due actual human incompatibility with the layout, design, location, and construction of the facility. Not all security guards are themselves reliable. Prescreening, bonding, and training does not guarantee that you won't end up with an ineffective and unreliable security guard." Pg 646 Tittel: CISSP Guide.

QUESTION 1297:

Which of the following statements pertaining to software testing approaches is correct?

A. A bottom-up approach allows interface errors to be detected earlier.
B. A top-down approach allows errors in critical modules to be detected earlier.
C. The test plan and results should be retained as part of the system's permanent documentation.
D. Black box testing is predicted on a close examination of procedural detail.

Answer: C

Explanation: This is an absolute best practice in the software testing field, you should always have to keep all your testing approaches with the results as part of the product documentation. This can help you in the case you have problems with some tasks or components of the software in the future, you can check back your testing and results and see if the system was making the tasks correctly and if anything changed from that environment.

QUESTION 1298:

Which Orange Book evaluation level is described as "Structured Protection"?

A. A1
B. B3
C. B2
D. B1

Answer: C

Explanation: Class B2 corresponds to Structured Protection.
Division B - Mandatory Protection
Mandatory access is enforced by the use of security labels. The architecture is based on the Bell-LaPadula security model and evidence of the reference monitor enforcement must be available.
B1: Labeled Security Each data object must contain a classification label and each subject must have a clearance label. When a subject attempts to access an object, the system must compare the subject and the object's security labels to ensure the requested actions are acceptable. Data leaving the system must also contain an accurate security label. The security policy is based on an informal statement and the design specifications are reviewed and verified. It is intended for environments that handle classified data.
B2: Structured Protection The security policy is clearly defined and documented and the system design and implementation is subjected to more thorough review and testing procedures. This class requires more stringent authentication mechanisms and well-defined interfaces between layers. Subject and devices require labels, and the system must not allow covert channels. A trusted path for logon and authentication processes must be in place, which means there are no trapdoors. There is a separation of operator and administration functions within the system to provide more trusted and protected operational functionality. Distinct address spaces must be provided to isolated processes, and a covert channel analysis is conducted. This class adds assurance by adding requirements to the design of the system. The environment that would require B2 systems could process sensitive data that requires a higher degree of security. This environment would require systems that are relatively resistant to penetration and compromise.
B3 Security Domains In this class, more granularity is provided in each protects mechanism and the programming code that is not necessary to support the security is excluded. The design and implementation should not provide too much complexity because as the complexity of a system increases, the ability of the individuals who need to test, maintain, and configure it reduces; thus, the overall security can be threatened. The reference monitor components must be small enough to test properly and be tamperproof. The security administrator role is clearly defined and the system must be able to recover from failures without its security level being compromised. When the system starts up and loads its operating system and components, it must be done in an initial secure state to ensure any weakness of the system cannon be taken advantage of in this slice of time. An environment that requires B3 systems is a highly secured environment that processes very sensitive information. It requires systems that are highly resistant to penetration.
Note: In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into

protection-critical and non-protection-critical elements. Class B corresponds to "Structured Protection" inside the Orange Book.

QUESTION 1299:

Which of the following questions should any user not be able to answer regarding their organization information security policy?

A. Who is involved in establishing the security policy?
B. Where is the organization security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization security policy?

Answer: C

Explanation: According to CISSP documentation, the actual definition and procedures defined inside an organization disaster recovery policy are of private nature. Only people working in the company and with a role inside it should know about those procedures. Its not a good practice to be divulgating Disaster recovery procedures to external people. Many times external people need to know who is involved in it, and who is responsible. This could be the case of a vendor providing replacement equipment in case of disaster.

QUESTION 1300:

RAID Level 1 mirrors the data from one disk to set of disks using which of the following techniques?

A. Copying the data onto another disk or set of disks.
B. Moving the data onto another disk or set of disks.
C. Establishing dual connectivity to another disk or set of disks.
D. Establishing dual addressing to another disk or set of disks.

Answer: A

Explanation: RAID 1 or Mirroring is a technique in which data is written to two duplicate disks simultaneously through a copy process. This way if one of the disk drives fails, the system can instantly switch to the other disk without any loss of data or service. Disk mirroring is used commonly in on-line database systems where it's critical that the data be accessible at all times. RAID means "Redundant Array of Inexpensive Disks".

QUESTION 1301:

Which type of firewall can be used to track connectionless protocols such as UDP and RPC?

A. Statefull inspection firewalls
B. Packet filtering firewalls

C. Application level firewalls
D. Circuit level firewalls

Answer: A

Explanation: Here are some characteristics of Statefull Inspection technology on Firewalls:
1. Scan information from all layers in the packet.
2. Save state information derived from previous communications, such as the outgoing Port command of an FTP session, so that incoming data communication can be verified against it.
3. Provides tracking support for connectionless protocols through the use of session state databases.
4. Allow state information derived from other applications access through the firewall for authorized services only, such as previously authenticated users.
5. Evaluate and manipulate flexible expressions based on communication and application derived state information.

QUESTION 1302:

Which of the following items should not be retained in an E-mail directory?

A. Drafts of documents.
B. Copies of documents.
C. Permanent records.
D. Temporary documents.

Answer: C

Explanation: This is another matter of common sense, the CISSP exam has many situations like this. Its not a good practice to have Permanent documents in your e-mail, this is because you don't know if your -mail is always backed up, and maybe the document must be available in a corporate repository. There is not problem to have Copies, draft or temporary documents in your e-mail. The important ones for the company are the Permanent documents.

QUESTION 1303:

Which of the following department managers would be best suited to oversee the development of an information security policy?

A. Information systems
B. Human resources
C. Business operations
D. Security administration

Answer: C

Explanation: He is the most appropriate manager, this is because he know the inns and outs of the business processes inside the company. Remember that he manages the business operations, and are those operations the ones that make the company live and generate the revenue. He knows who should access what and when. Security administrators develop the policy with the information provided by persons like the Business operations manager. Human Resources is not appropriate in this case, and the Information systems manager know about the technology, but not the business needs of the company.

QUESTION 1304:

Which of the following countermeasures is not appropriate for war dialing attacks?

A. Monitoring and auditing for such activity.
B. Disabling call forwarding.
C. Making sure only necessary phone numbers are made public.
D. Using completely different numbers for voice and data accesses.

Answer: B

Explanation: War dialing, or scanning, has been a common activity in the computer underground and computer security industry for decades. Hollywood made war dialing popular with the 1983 movie, War Games, in which a teenager searching for a videogame company ultimately uncovers a government nuclear war warning system. The act of war dialing is extremely simple - a host computer dials a given range of telephone numbers using a modem. Every telephone number that answers with a modem and successfully connects to the host is stored in a log. Disabling call forwarding is not a useful countermeasure because it's the attacker machine the one who connects to the attacked system and forwarding is not an issue inside the attack. Answer A, C and D can be used as countermeasures to harder the war dial attack.

QUESTION 1305:

Which of the following tools is less likely to be used by a hacker?

A. I0phtcrack
B. Tripwire
C. Crack
D. John the Ripper

Answer: B

Explanation: Tripwire is a tool that checks to see what has changed on your system. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc. The hard part is doing it the right way, balancing security, maintenance, and functionality. This tool is not usually used by hackers

to attack, its usually used to defend against hackers attacks. L0phtcrack is a hacker utility to get passwords, Crack and John the Ripper are also password crackers.

QUESTION 1306:

Which of the following logical access exposures involves changing data before, or as it is entered into the computer?

A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses

Answer: A

Explanation: This kind of attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed. This kind of attack was used in the past to steal small quantities of money and transfer them to the attackers account, there are many other uses too. Trojan horses open ports without the user knowledge to permit remote control and a Virus is a malicious piece of code that executed inside your computer.

QUESTION 1307:

Which of the following computer aided software engineering (CASE) products is used for developing detailed designs, such as screen and report layouts?

A. Lower CASE
B. Middle CASE
C. Upper CASE
D. I-CASE

Answer: B

Explanation: This is the proper name, you can search for "Middle CASE" on the Internet. "Middle CASE" its a CASE flavor and UML design tool that provides the required functionality like screen and report layouts and detailed designs. There are many well known vendors providing this kind of tools for the development process of Software.

QUESTION 1308:

What is called the number of columns in a table?

A. Schema
B. Relation
C. Degree

D. Cardinality

Answer: C

Explanation: In database terminology, is the same to say that the number of Degrees is "X" and that the number of columns is "X" inside a Table. This question is just trying to test our knowledge of rare, difficult to fin terminology. You can check this in the knowledgebase of Oracle. When we talk about degrees, we are just talking about columns. The schema is the structure of the database, and the relations are the way each table relates to others.

QUESTION 1309:

Which of the following is the most reliable authentication device?

A. Variable callback system
B. Smart Card system
C. Fixed callback system
D. Combination of variable and fixed callback system.

Answer: B

Explanation: The smart card, an intelligent token, is a credit card sized plastic card embedded with an integrated circuit chip. It provides not only memory capacity, but computational capability as well. The self-containment of smart card makes it resistant to attack as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications which require strong security protection and authentication. Option B is the most correct option, this is because Callback systems are not considered very reliable in the CISSP examination, Smart cards can also provide 2 mode authentication.
"Caller ID and callback options are great, but they are usually not practical because they require users to call in from a static phone number each time they access the network. Most users are accessing the network remotely because they are on the road and moving from place to place." Pg. 428 Shon Harris: All-In-One CISSP Certification Guide.

QUESTION 1310:

Which of the following firewall rules is less likely to be found on a firewall installed between and organization internal network and the Internet?

A. Permit all traffic to and from local host.
B. Permit all inbound ssh traffic
C. Permit all inbound tcp connections.
D. Permit all syslog traffic to log-server.abc.org.

Answer: C

Explanation: Option "C" is a very bad practice in a firewall connecting one of its interfaces to a public network like Internet. Since in that rule you are allowing all inbound TCP traffic, the hackers can send all the attacks they want to any TCP port, they can make port scanning, Syn Attacks, and many other dangerous DoS activities to our private network. Permit the traffic from local host is a best practice, our firewall is the local host. Permit SSH (Secure Shell) is also good because this protocol use cryptography.

QUESTION 1311:

The Internet can be utilized by either?

A. Public or private networks (with a Virtual Private Networks).
B. Private or public networks (with a Virtual Private Networks).
C. Home or private networks (with a Virtual Private Networks).
D. Public or home networks (with a Virtual Private Networks).

Answer: B

Explanation: This is true, you can utilize Internet from a Private network and get access through an access translation method that gives you a valid IP address to make the request. Or you can access the Internet directly from a routable, public IP address contained in a public network. To increase security, you can create VPN´s to pass information between two endpoints with confidentiality through the Internet.

QUESTION 1312:

This backup method must be made regardless of whether Differential or Incremental methods are used.

A. Full Backup Method
B. Incremental backup method
C. Differential backup method
D. Tape backup method

Answer: A

Explanation: Since the "Full" backup method provides a baseline for our systems for Restore, the full backup must be done at least once regardless of the method you are using. Its very common to use full backups in combination with incremental or differential ones to decrease the backup time (however you increment the restore time), but there is no way to maintain a system only with incremental or differential backups. You always need to begin from your restore baseline, the Full Backup.

QUESTION 1313:

Why do buffer overflows happen?

A. Because buffers can only hold so much data.
B. Because input data is not checked for appropriate length at time of input.
C. Because they are an easy weakness to exploit.
D. Because of insufficient system memory.

Answer: B

QUESTION 1314:

Which of the following should not be performed by an operator?

A. Mounting disk or tape
B. Backup and recovery
C. Data entry
D. Handling hardware

Answer: C

Explanation: This is very obvious, the operators are responsible of making operative tasks that deals with the hardware and software implementations, they can handle the hardware and put t in condition for the user, be in charge of the backup and restore procedures and Mounting the disk or tapes for the backup. Those are all common tasks. When we talk about the data entry, is the user who has to make does, If the operator do that too, what is the user going to do?

QUESTION 1315:

What security model is dependant on security labels?

A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control

Answer: C

Explanation:
With mandatory controls, only administrators and not owners of resources may make decisions that bear on or derive from policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy. This kind of access control method is based on Security labels. It is important to note that mandatory controls are prohibitive (i.e., all that is not expressly permitted is forbidden).

QUESTION 1316:

Detection capabilities of Host-based ID systems are limited by the incompleteness of which of the following?

A. Audit log capabilities
B. Event capture capabilities
C. Event triage capabilities
D. Audit notification capabilities

Answer: A

Explanation: This is one of the weakest point of IDS systems installed on the individual hosts. Since much of the malicious activity could be circulating through the network, and this kind of IDS usually have small logging capabilities and of local nature. So any activity happening in the network could go unnoticed, and intrusions can't be tracked as in depth as we could with an enterprise IDS solution providing centralized logging capabilities.

QUESTION 1317:

Computer crime is generally made possible by which of the following?

A. The perpetrator obtaining training & special knowledge.
B. Victim carelessness.
C. Collusion with others in information processing
D. System design flaws.

Answer: B

Explanation:
This is a real problem, nobody thinks that can be victim of a computer crime until it is. There is a big problem relating to the people thinking about this kind of attacks. Computer crimes can be very important and can make great damage to enterprises. Computer Crime will decrease once people begin to think about the Risks and begin to protect their systems from the most common attacks.

QUESTION 1318:

The structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media includes?

A. The Telecommunications and Network Security domain.
B. The Telecommunications and Netware Security domain.
C. The Technical communications and Network Security domain.
D. The Telnet and Network Security domain.

Answer: A

Explanation: This is pretty straight forward. The four principal pillars of computer security: integrity, authentication, confidentiality and availability are all part of the network security and telecommunication domain. Why? Because those pillars deal with that. We provide integrity through digital signatures, authentication through passwords, confidentiality through encryption and availability by fault tolerance and disaster recovery. All of those are networking and telecommunication components.

QUESTION 1319:

Which of the following is the lowest TCSEC class where in the system must protected against covert storage channels (but not necessarily covert timing channels)?

A. B2
B. B1
C. B3
D. A1

Answer: A

Explanation: The B2 class referenced in the orange book is the formal security policy model based on device labels that can use DAC (Discretionary access controls) and MAC (Mandatory Access Controls). It provides functionality about covert channel control. It does not require covert timing channels. You can review the B2 section of the Orange Book.

QUESTION 1320:

Which type of control is concerned with avoiding occurrences of risks?

A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls

Answer: C

Explanation: Preventive controls deals with the avoidance of risk through the diminution of probabilities. Is like the example we read earlier about the dogs. Just to remember, Since we want to prevent something from happening, we can go out and buy some Guard dogs to make the job. You are buying them because you want to prevent something from happening. The intruder will see the dogs and will maybe go back, this prevents an attack, this dogs are a form of preventive control.

QUESTION 1321:

The basic function of an FRDS is to?

A. Protect file servers from data loss and a loss of availability due to disk failure.
B. Persistent file servers from data gain and a gain of availability due to disk failure.
C. Prudent file servers from data loss and a loss of acceptability due to disk failure.
D. Packet file servers from data loss and a loss of accountability due to disk failure.

Answer: A

Explanation:
FRDS systems will give us the functionality to protect our servers from disk failure an allow us to have highly available file services in our production servers. FRDS provides high availability against many types of disk failures and well known problems, if one disk goes down, the others still work providing no downtime. FRDS solutions are the preferred way to protect file servers against data corruption and loss. You can see more about FRDS in the Internet, search "FRDS System".

QUESTION 1322:

Which of the following protocols does not operate at the data link layer (layer 2)?

A. PPP
B. RARP
C. L2F
D. ICMP

Answer: D

Explanation: Internet Control Message Protocol. ICMP is used for diagnostics in the network. The Unix program, ping, uses ICMP messages to detect the status of other hosts in the net. ICMP messages can either be queries (in the case of ping) or error reports, such as when a network is unreachable. This protocol resides in layer 3 of the OSI model (Network layer).

QUESTION 1323:

This tape format can be used to backup data systems in addition to its original intended audio used by:

A. Digital Audio tape (DAT)
B. Digital video tape (DVT)
C. Digital Casio Tape (DCT)
D. Digital Voice Tape (DVT)

Answer: A

Explanation: Digital Audio Tape (DAT or R-DAT) is a signal recording and playback medium introduced by Sony in 1987. In appearance it is similar to a compact audio cassette, using 1/8" magnetic tape enclosed in a protective shell, but is roughly half the size at 73 mm x 54 mm x 10.5 mm. As the name suggests the recording is digital rather than analog, DAT converting and recording at the same rate as a CD (44.1 kHz sampling rate and 16 bits quantization) without data compression. This means that the entire input signal is retained. If a digital source is copied then the DAT will produce an exact clone.
The format was designed for audio use, but through an ISO standard it has been adopted for general data storage, storing from 4 to 40 GB on a 120 meter tape depending on the standard and compression (DDS-1 to DDS-4). It is, naturally, sequential-access media and is commonly used for backups. Due to the higher requirements for integrity in data backups a computer-grade DAT was introduced.

QUESTION 1324:

By examining the "state" and "context" of the incoming data packets, it helps to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC). This type of firewall system is used in?

A. First generation firewall systems.
B. Second generation firewall systems.
C. Third generation firewall systems.
D. Fourth generation firewall systems.

Answer: C

Explanation: Statefull inspection is a third generation firewall technology designed to be aware of, and inspect, not only the information being received, but the dynamic connection and transmission state of the information being received. Control decisions are made by analyzing and utilizing the following: Communication Information, Communication derived state, Application derived state and information manipulation. Here are some characteristics of Statefull Inspection technology on Firewalls:
1. Scan information from all layers in the packet.
2. Save state information derived from previous communications, such as the outgoing Port command of an FTP session, so that incoming data communication can be verified against it.
3. Provides tracking support for connectionless protocols through the use of session state databases.
4. Allow state information derived from other applications access through the firewall for authorized services only, such as previously authenticated users.
5. Evaluate and manipulate flexible expressions based on communication and application derived state information.

QUESTION 1325:

Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment.
B. The use of physical force.
C. The operation of access control devices.
D. The need to detect unauthorized access.

Answer: A

Explanation: This is the correct answer, we don't have guards only to use physical force, that is not the real functionality of them if your security policy is well oriented. They are not only there to operate control devices and to detect unauthorized access, as stated in CISSP documentation, the appropriate function of a guard inside a security program is the use of discriminating judgment.

QUESTION 1326:

A server cluster looks like a?

A. Single server from the user's point of view.
B. Dual server from the user's point of view.
C. Tripe server from the user's point of view.
D. Quardle server from the user's point of view.

Answer: A

Explanation: A "Cluster" is a grouping of machines running certain services providing high availability and fault tolerance fro them. In other words, they are grouped together as a means of fail over support. From the users view, a cluster is a single server, but its only a logical one, you can have an array of 4 server in cluster all with the same IP address (/achieving correct resolution through ARP), there is no difference for the client.

QUESTION 1327:

Which of the following are functions that are compatible in a properly segregated environment?

A. Application programming and computer operation.
B. System programming and job control analysis.
C. Access authorization and database administration.
D. System development and systems maintenance.

Answer: D

Explanation: If you think about it, System development and system maintenance are perfectly compatible, you can develop in the systems for certain time, and when it time for a maintenance, you stop the development process an make the maintenance. It's a pretty straight forward process. The other answer do not provide the simplicity and freedom of this option.

QUESTION 1328:

Encryption is applicable to all of the following OSI/ISO layers except:

A. Network layer
B. Physical layer
C. Session layer
D. Data link layer

Answer: B

Explanation: The Physical Layer describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. Ex: this layer defines the size of Ethernet coaxial cable, the type of BNC connector used, and the termination method. You cannot encrypt nothing at this layer because its physical, it is not protocol / software based. Network, Data link and transport layer supports encryption.

QUESTION 1329:

The Computer Security Policy Model the Orange Book is based on is which of the following?

A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest

Answer: A

Explanation: Following the publication of the Anderson report, considerable research was initiated into formal models of security policy requirements and of the mechanisms that would implement and enforce those policy models as a security kernel. Prominent among these efforts was the ESD-sponsored development of the Bell and LaPadula model, an abstract formal treatment of DoD security policy.[2] Using mathematics and set theory, the model precisely defines the notion of secure state, fundamental modes of access, and the rules for granting subjects specific modes of access to objects. Finally, a theorem is proven to demonstrate that the rules are security-preserving operations, so that the application of any sequence of the rules to a system that is in a secure state will result in the system

entering a new state that is also secure. This theorem is known as the Basic Security Theorem.

QUESTION 1330:

Which type of attack would a competitive intelligence attack best classify as?

A. Business attack
B. Intelligence attack
C. Financial attack
D. Grudge attack

Answer: A

Explanation: Since we are talking about a competitive intelligence attack, we can classify it as a Business attack because it is disrupting business activities. Intelligence attacks are one of the most commonly used to hurt a company where more it hurts, in its information. To see more about competitive intelligence attacks you can take a look at some CISSP study guide. It could be the CISSP gold edition guide.
"Military and intelligence attacks are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources.
Business attacks focus on illegally obtaining an organization's confidential information.
Financial attacks are carried out to unlawfully obtain money or services.
Grudge attacks are attacks that are carried out to damage an organization or a person."
Pg. 616 Tittel: CISSP Study Guide

QUESTION 1331:

Which of the following is responsible for the most security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Answer: C

Explanation: As I stated earlier in the comments, the great part of the attacks to companies comes from the personnel. Hackers are out there and attack some targets, but should never forget that your worst enemy can be inside of your company. Is for that that we usually implement IDS and profundity security. It's a very good practice to install Host based IDS to limit the ability of internal attackers through the machines.
Another problem with personal is the ignorance, there are time that they just don't know what they are doing, and certainly are violating the security policy.

QUESTION 1332:

Which of the following goals is NOT a goal of Problem Management?

A. To eliminate all problems.
B. To reduce failures to a manageable level.
C. To prevent the occurrence or re-occurrence of a problem.
D. To mitigate the negative impact of problems on computing services and resources.

Answer: A

Explanation: This is not possible, nobody can eliminate all problems, only god can, this is a reality and Problem Management Gurus know that. With problem management we can reduce failures, prevent reoccurrence of problems and mitigate negative impact as much as we can, but we cannot eliminate all problems, this is not a perfect world.

QUESTION 1333:

Examples of types of physical access controls include all except which of the following?

A. badges
B. locks
C. guards
D. passwords

Answer: D

Explanation: A password is not a physical thing, it's a logical one. You can control physical access with armed guards, by locking doors and using badges to open doors, but you can't relate password to a physical environment. Just to remember, Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system. They are related to software, not to hardware.

QUESTION 1334:

Which of the following statements pertaining to the (ISC)2 Code of Ethics is incorrect?

A. All information systems security professionals who are certified by (ISC)2 recognize that such a certification is a privilege that must be both earned and maintained.
B. All information systems security professionals who are certified by (ISC)2 shall provide diligent and competent service to principals.
C. All information systems security professionals who are certified by (ISC)2 shall discourage such behavior as associating or preparing to associate with criminals or criminal behavior.
D. All information systems security professionals who are certified by (ISC)2 shall promote the understanding and acceptance of prudent information security measures.

Answer: C

Explanation: This is not one of the statements of the ISC2 code of Ethics, ISC2 certified people is free to get in association with any person and any party they want. ISC2 thinks that their certified people must have liberty of choice in their associations. However ISC2 ask the certified professionals to promote the certification and the understanding and acceptance of security measures, they also ask the certified people to provide competent services and be proud of their exclusive ISC2 certified professional status.
I think is very fair, you are free to who where you want, with the people you want, but always be proud of your certification and your skills as a security professional.
Code from ISC web site.
"All information systems security professionals who are certified by (ISC)2 recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all Certified Information Systems Security Professionals (CISSPs) commit to fully support this Code of Ethics. CISSPs who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification.
There are only four mandatory canons in the code. By necessity such high-level guidance is not intended to substitute for the ethical judgment of the professional.
Additional guidance is provided for each of the canons. While this guidance may be considered by the Board in judging behavior, it is advisory rather than mandatory. It is intended to help the professional in identifying and resolving the inevitable ethical dilemmas that will confront him/her.
Code of Ethics Preamble:
* Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
* Therefore, strict adherence to this code is a condition of certification.
Code of Ethics Canons:
* Protect society, the commonwealth, and the infrastructure.
* Act honorably, honestly, justly, responsibly, and legally.
* Provide diligent and competent service to principals.
* Advance and protect the profession.
The following additional guidance is given in furtherance of these goals.
Objectives for Guidance
In arriving at the following guidance, the committee is mindful of its responsibility to:
* Give guidance for resolving good v. good and bad v. bad dilemmas.
* To encourage right behavior such as:
* Research
* Teaching
* Identifying, mentoring, and sponsoring candidates for the profession
* Valuing the certificate
* To discourage such behavior as:
* Raising unnecessary alarm, fear, uncertainty, or doubt
* Giving unwarranted comfort or reassurance
* Consenting to bad practice
* Attaching weak systems to the public net

* Professional association with non-professionals
* Professional recognition of or association with amateurs
* Associating or appearing to associate with criminals or criminal behavior

However, these objecttives are provided for information only; the professional is not required or expected to agree with them.

In resolving the choices that confront him, the professional should keep in mind that the following guidance is advisory only. Compliance with the guidance is neither necessary nor sufficient for ethical conduct.

Compliance with the preamble and canons is mandatory. Conflicts between the canons should be resolved in the order of the canons. The canons are not equal and conflicts between them are not intended to create ethical binds.

Protect society, the commonwealth, and the infrastructure

* Promote and preserve public trust and confidence in information and systems.
* Promote the understanding and acceptance of prudent information security measures.
* Preserve and strengthen the integrity of the public infrastructure.
* Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally

* Tell the truth; make all stakeholders aware of your actions on a timely basis.
* Observe all contracts and agreements, express or implied.
* Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
* Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
* When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service to principals

* Preserve the value of their systems, applications, and information.
* Respect their trust and the privileges that they grant you.
* Avoid conflicts of interest or the appearance thereof.
* Render only those services for which you are fully competent and qualified.

Advance and protect the profession

* Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
* Take care not to injure the reputation of other professionals through malice or indifference.

Maintain your competence; Keep your skills and Knowledge current. Give generously of your time and knowledge in training others.

QUESTION 1335:

Which DES modes can best be used for authentication?

A. Cipher Block Chaining and Electronic Code Book.
B. Cipher Block Chaining and Output Feedback.
C. Cipher Block Chaining and Cipher Feedback.
D. Output Feedback and Electronic Code Book.

Answer: C

Explanation: Cipher Block Chaining (CBC) uses feedback to feed the result of encryption back into the encryption of the next block. The plain-text is XOR'ed with the previous cipher-text block before it is encrypted. The encryption of each block depends on all the previous blocks. This requires that the decryption side processes all encrypted blocks sequentially. This mode requires a random initialization vector which is XOR'ed with the first data block before it is encrypted. The initialization vector does not have to be kept secret. The initialization vector should be a random number (or a serial number), to ensure that each message is encrypted uniquely. In the Cipher Feedback Mode (CFB) is data encrypted in units smaller than the block size. This mode can be used to encrypt any number of bits e.g. single bits or single characters (bytes) before sending across an insecure data link.
Both of those method can be best used to provide user authentication capabilities.

QUESTION 1336:

In the OSI / ISO model, at what layer are some of the SLIP, CSLIP, PPP control functions are provided?

A. Link
B. Transport
C. Presentation
D. Application

Answer: A

Explanation: The Data Link layer takes raw data from the physical layer and gives it logical structure. This logic includes information about where the data is meant to go, which computer sends the data, and the overall validity of the bytes sent. The Data Link layer also controls functions of logical network topologies and physical addressing as well as data transmission synchronization and corrections. SLIP, CSLIP and PPP provide control functions at the Data Link Layer (layer 2 of the OSI model).

QUESTION 1337:

Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment.

Answer: B

Explanation: A bug is a coding error in a computer program. The process of finding bugs before program final users is called debugging. Debugging starts after the code is first written and continues in successive stage as code is combined with other units of programming to form a software product, such as an operating system or application. The main reason to debug is to detect and correct errors in the program.

QUESTION 1338:

With RAID Level 5 the spare drives that replace the failed drives are usually hot swappable, meaning the can be replaced on the server while the?

A. System is up and running.
B. System is down and running.
C. System is in-between and running.
D. System is centre and running.

Answer: A

Explanation: This is true, since RAID 5 uses parity to provide fault tolerance through the array, once of the disk in it can become corrupted, and you usually can just take it out without turning off the system (Hot SWAP) and plug a spare disk on the bay. Then the array will automatically begin to reconstruct the information in the new disk with the parity contained through the other disks in the array. This Hot Swap capability is usually present in enterprise servers that require high availability.

QUESTION 1339:

What is the process that RAID Level 0 uses as it creates one large disk by using several disks?

A. Striping
B. Mirroring
C. Integrating
D. Clustering

Answer: A

Explanation: This is the correct term, with stripping RAID 0 can evenly distribute the information through the disk that form the array in a transparent way for the final user. With RAID 0 you can be writing to 12 disk simultaneously and you see them as only one large logical partition. This level of RAID does not provide fault tolerance but provides an increase in performance because you are writing and reading from many disks and heads. An example of this stripping is the software version that comes with Windows 2000, it supports up to 32 disks.

QUESTION 1340:

Which of the following is used to create and delete views and relations within tables?

A. SQL Data Definition Language
B. SQL Data Manipulation Language
C. SQL Data Relational Language
D. SQL Data Identification Language

Answer: A

Explanation: SQL supports the data definition language (DDL) for creating, altering, and deleting tables and indexes. SQL does not permit metadata object names to be represented by parameters in DDL statements. With this language you can create many of the objects used in SQL, this language is standard and is supported by most database vendors in its standard form. Many of them also extends its functionality for proprietary products.

QUESTION 1341:

Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D
B. C
C. B
D. A

Answer: B

Explanation: The C division of the Orange Book deals discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.
This information can be checked in the orange book. Just make a search online through it with the words "discretionary protection".

QUESTION 1342:

The Diffie-Hellman algorithm is used for?

A. Encryption
B. Digital signature
C. Key exchange
D. Non-repudiation

Answer: C

Explanation:

Diffie Hellman is a Key exchange algorithm, its strength its in the difficulty of computing discrete logarithms in a finite field generated by a large primary number. Although RSA and Diffie Hellman are similar in mathematical theory, their implementation is somewhat different. This algorithm has been released to the public. It's the primary alternative to the RSA algorithm for key exchange.

QUESTION 1343:

Primary run when time and tape space permits, and is used for the system archive or baselined tape sets is the?

A. Full backup method.
B. Incremental backup method.
C. Differential backup method.
D. Tape backup method.

Answer: A

Explanation: "Full" backup method provides a baseline for our systems for Restore; the full backup must be done at least once regardless of the method you are using to make backups. It's very common to use full backups in combination with incremental or differential ones to decrease the backup time (however you increment the restore time with incremental and differential) because it takes the largest time to complete. You always need to begin a system restoration from your baseline, and this baseline is the Full Backup.

QUESTION 1344:

Which of the following teams should not be included in an organization's contingency plan?

A. Damage assessment team.
B. Hardware salvage team.
C. Tiger team.
D. Legal affairs team.

Answer: C

Explanation: In the computer industry, a tiger team is a group of programmers or users who volunteer or are hired to expose errors or security holes in new software or to find out why a computer network's security is being broken. In hiring or recruiting volunteers for a tiger team, some software developers advise others to be sure that tiger team members don't include crackers, who might use their special knowledge of the software to disable or compromise it in the future. We don't need a tiger team inside our contingency plan, however, we do need someone to assest the damage, the hardware and legal affairs.

QUESTION 1345:

When an organization takes reasonable measures to ensure that it took precautions to protect its network and resources is called:

A. Reasonable Action
B. Security Mandate
C. Due Care
D. Prudent Countermeasures

Answer: C

Explanation: Due care are the steps taken to show it has taken responsibility for its actions.

QUESTION 1346:

What two things below are associated with security policy?(Choose Two)

A. Support of upper management
B. Support of department managers
C. Are tactical in nature
D. Are strategic in nature
E. Must be developed after procedures
F. Must be developed after guidelines

Answer: A,D

Explanation: Policies are written as a broad overview and require the support of upper management. After the development and approval of policies, guidelines and procedures may be written.

QUESTION 1347:

Total risk is equal to:(Choose All That Apply)

A. Threat
B. Vulnerability
C. Frequency
D. Asset value
E. Asset loss

Answer: A,B,D

Explanation: Total risk = asset value * vulnerability * threats

---

QUESTION 1348:

Government data classifications include which of the following:(Choose three)

A. Open
B. Unclassified
C. Confidential
D. Private
E. Secret
F. Top Secret

Answer: B,C,F

Explanation: One of the most common systems used to classify information is the one developed within the US Department of Defense. These include: unclassified, sensitive, confidential, secret, and top secret.

QUESTION 1349:

Job rotation is important because:

A. It insures your employees are cross-trained.
B. It increases job satisfaction.
C. It reduces the opportunity for fraud

Answer: C

Explanation: Job rotation is tightly tied to the principle of least privilege. It is an effective security control.

QUESTION 1350:

Your co-worker is studying for the CISSP exam and has come to you with a question. What is ARP poisoning?

A. Flooding of a switched network
B. A denial of service that uses the DNS death ping
C. Turning of IP to MAC resolution
D. Inserting a bogus IP and MAC address in the ARP table
E. Modifying a DNS record

Answer: D

Explanation: ARP poisoning is a masquerading attack where the attacker inserts a bogus IP and MAC address in a victims ARP table or into the table of a switch. This has the effect of redirecting traffic to the attacker and not to the intended computer.

QUESTION 1351:

What is the best description for CHAP Challenge Handshake Authentication Protocol?

A. Passwords are sent in clear text
B. Passwords are not sent in clear text
C. Passwords are not used, a digital signature is sent
D. It is substandard to PAP
E. It was used with PS2's and has been discontinued

Answer: B

Explanation: Passwords are not sent in clear text. The server performing the authentication sends a challenge value and the user types in the password. The password is used to encrypt the challenge value then is sent back to the authentication server.

QUESTION 1352:

CSMA/CD computers cannot communicate without a token.(True/False)

A. True
B. False

Answer: B

Explanation: CSMA/CD computers do not use a token. It is the media access method used in Ethernet.

QUESTION 1353:

_____ sends out a message to all other computers indicating it is going to send out data.

A. CSMA/CD
B. CSMA/CA
C. CSMA/HB
D. PPP
E. SLIP

Answer: B

Explanation: CSMA/CA sends out a message to all other computers indicating it is going to send out data. CSMA/CA or token ring networking uses this approach to reduce the amount of data collisions.
Note: When computers use the carrier sense multiple access with collision detection

(CSMA/CD) protocols, they monitor the transmission activity, or carrier activity, on the wire so that they can determine when would be the best time to transmit data.
Carrier sense multiple access with collision avoidance (CSMA/CA) is an access method where each computer signals its intent to transmit data before it actually does so.
pg 390-391 Shon Harris All-In-One CISSP Certification

QUESTION 1354:

Which of the following best describes ISDN BRI(Choose two)

A. 2 B channels
B. 4 B channels
C. 23 B channels
D. 1 D channel
E. 2 D channels

Answer: A,D

Explanation: ISDN BRI has 2 B and 1 D channels

QUESTION 1355:

The top speed of ISDN BRI is 256 KBS.(True/False)

A. True
B. False

Answer: B

Explanation: The top speed of ISDN BRI is 128 KBS. Its two primary channels are each capable of carrying 64 KBS so the combined top speed is 128 KBS.

QUESTION 1356:

Which of the following should NOT be implemented to protect PBX's?(Choose all that apply)

A. Change default passwords and configurations
B. Make sure that maintenance modems are on 24/7
C. Review telephone bill regularly
D. Block remote calling after business hours
E. Post PBX configuration and specs on the company website

Answer: B,E

Explanation: Many vendors have maintenance modems that vendors can use to

troubleshoot systems and provide updates. They should normally be turned off. Also information about the system should not be posted on the website and should be closely guarded.

QUESTION 1357:

Which of the following best describes the difference between a circuit based and application based firewall?

A. Application based is more flexible and handles more protocols
B. Circuit based provides more security
C. Application based builds a state table
D. Circuit based looks at IP addresses and ports
E. Circuit based firewalls are only found in Cisco routers

Answer: D

Explanation: Circuit based look only at IP address and ports, whereas application based dig much deeper into the packet. This makes it more secure.

QUESTION 1358:

_____ is the fraudulent use of telephone services.

A. Rolling
B. Warzing
C. Wardriving
D. Wardialing
E. Phreaking

Answer: E

Explanation: Phreaking is the fraudulent use of telephone services.

QUESTION 1359:

What is another name for a VPN?

A. Firewall
B. Tunnel
C. Packet switching
D. Pipeline
E. Circuit switching

Answer: B

Explanation: A VPN creates a secure tunnel through an insecure network.

QUESTION 1360:

Which of the following is a connection-orientated protocol?

A. IP
B. UDP
C. TCP
D. ICMP
E. SNMP
F. TFTP

Answer: C

Explanation: TCP is a connection-orientated protocol.

QUESTION 1361:

Which of the following is not considered firewall technology?

A. Screened subnet
B. Screened host
C. Duel gateway host
D. Dual homed host

Answer: C

Explanation: Duel gateway host is not considered firewall technology.

QUESTION 1362:

Which type of network topology passes all traffic through all active nodes?

A. Broadband
B. Star
C. Baseband
D. Token Ring

Answer: D
Token ring passes all traffic through nodes.

QUESTION 1363:

The act of validating a user with a unique and specific identifier is called what?

A. Validation
B. Registration
C. Authentication
D. Authorization
E. Identification

Answer: C
Authentication is the act of validating a user with a unique and specific identifier.

QUESTION 1364:

Why is fiber the most secure means of transmission?

A. High speed multiplexing
B. Interception of traffic is more difficult because it is optically based
C. Higher data rates make it more secure
D. Multiplexing prevents traffic analysis
E. Built-in fault tolerance

Answer: B
Fiber is more secure because it is hard to tap into and gives off no EMI such as copper cabling.

QUESTION 1365:

The IAB defines which of the following as a violation of ethics?

A. Performing a DoS
B. Downloading an active control
C. Performing a penetration test
D. Creating a virus
E. Disrupting Internet communications

Answer: E
The IAAB considers the Internet a privilege, not a right, and as such considers it unethical to purposely disrupt communications.

QUESTION 1366:

A chain of custody shows who _____ _____ and _____.(Choose three)

A. Who controlled the evidence
B. Who transcribed the evidence
C. Who validated the evidence
D. Who presented the evidence
E. Secured the evidence

F. Obtained the evidence

Answer: A,E,F
The chain of evidence shows who obtained the evidence, who secured the evidence, and who controlled the evidence.

QUESTION 1367:

Good forensics requires the use of a bit level copy?(True/False)

A. True
B. False

Answer: A
Good forensics requires the use of a bit level copy. A bit level copy duplicates all information on the suspect's disk. This includes slack space and free space.

QUESTION 1368:

Which agency shares the task of investigating computer crime along with the FBI?

A. Secret Service
B. CIA
C. Department of justice
D. Police force
E. NSA

Answer: A
Along with the FBI, the Secret Service has been given the authority to investigate computer crime.

QUESTION 1369:

This type of password recovery is considered more difficult and must work through all possible combinations of numbers and characters.

A. Passive
B. Active
C. Dictionary
D. Brute force
E. Hybrid

Answer: D
Brute force cracking is considered more difficult and must work through all possible combinations of numbers and characters.

QUESTION 1370:

_____ are added to Linux passwords to increase their randomness.

A. Salts
B. Pepper
C. Grains
D. MD5 hashes
E. Asymmetric algorithms

Answer: A
Salts are added to Linux passwords to increase their randomness. They are used to help insure that no two users have the same, hashed password.

QUESTION 1371:

The Linux root user password is typically kept in where?(Choose two)

A. etc/shadow
B. cmd/passwd
C. etc/passwd
D. windows/system32
E. var/sys
F. var/password

Answer: A,C
The Linux root user password is typically kept in /etc/passwd or etc/shadow.

QUESTION 1372:

The goal of cryptanalysis is to _____.

A. Determine the number of encryption permutations required
B. Reduce the system overhead for a crypto-system
C. Choose the correct algorithm for a specified purpose
D. Forge coded signals that will be accepted as authentic
E. Develop secure crypto-systems

Answer: D
The goal of cryptanalysis is to forge coded signals that will be accepted as authentic.

QUESTION 1373:

If an employee is suspected of computer crime and evidence need to be collected, which of the following departments must be involved with the procedure?

A. Public relations
B. Law enforcement
C. Computer security
D. Auditing
E. HR

Answer: E
Human Resources always needs to be involved if an employee is suspected of wrongdoing. They know what rules apply to protect and prosecute employees.

QUESTION 1374:

What is it called when a system has apparent flaws that were deliberately available for penetration and exploitation?

A. A jail
B. Investigation
C. Enticement
D. Data manipulation
E. Trapping

Answer: C
Administrators that leave systems with apparent flaws are performing an act of enticement. This is sometimes called a honeypot.

QUESTION 1375:

Why are computer generated documents not considered reliable?

A. Difficult to detect electron tampering
B. Stored in volatile media
C. Unable to capture and reproduce
D. Too delicate
E. Because of US law, Section 7 paragraph 154

Answer: A
Because it is difficult to detect electron tampering and can be easily modified.

QUESTION 1376:

What is the name of the software that prevents users from seeing all items or directories on a computer and is most commonly found in the UNIX/Linux environment?

A. Shell Kits
B. Root Kits
C. Ethereal

D. Shadow data
E. Netbus

Answer: D
Shadowing, used for Unix password files hides the password hash.
IF SHAWDOWING IS ACTIVE:

If the shawdowing is active the /etc/passwd would look like this:
root:x:0:1:0000:/:
sysadm:x:0:0:administration:/usr/admin:/bin/rsh
The password filed is substituted by "x".
The /etc/shawdow file only readable by root will look similar to
this:
root:D943/sys34:5288::
:
super user accounts
:
Cathy:masai1:5055:7:120
:
all other users
:
The first field contains users id:the second contains the password(The pw will be NONE if logining in remotely is deactivated):the third contains a code of when the password was last changed:the fourth and the fifth contains the minimum and the maximum numbers of days for pw changes(Its rare that you will find this in the super user logins due to there hard to guess passwords)

QUESTION 1377:

What is a commercial application of steganography that is used to identify pictures or verify their authenticity?

A. A MAC
B. A digital checksum
C. A MD5 hash
D. A digital signature
E. A watermark

Answer: E
A watermark is a commercial application of steganography that is used to identify pictures or verify its authenticity.

QUESTION 1378:

What are the basic questions that must be asked at the beginning of any investigation?(Choose all that apply)

A. Who
B. Cost
C. What
D. When
E. Where
F. How
G. Time frame
H. Budget

Answer: A,C,D,E,F
At the beginning of any investigation, an investigator must ask who, what, when, where, and how. Answering the questions will lead to the successful conclusion of the case.

QUESTION 1379:

Risk can be eliminated.(True/False)

A. True
B. False

Answer: B
Risk can never be eliminated. It may be reduced or transferred to a third party through insurance, but will always remain in some form.

QUESTION 1380:

Employees are a greater risk to employers than outsiders. T/F(True/False)

A. True
B. False

Answer: A
Employees are a greater risk to employers than outsiders, because they possess two of the three items required to commit a crime: means and opportunity.

QUESTION 1381:

When an organization takes reasonable measures to ensure that it took precautions to protect its network and resources is called:

A. Reasonable Action
B. Security Mandate
C. Due Care
D. Prudent Countermeasures

Answer: C
Due care are the steps taken to show it has taken responsibility for its actions.

QUESTION 1382:

What two things below are associated with security policy?(Choose Two)

A. Support of upper management
B. Support of department managers
C. Are tactical in nature
D. Are strategic in nature
E. Must be developed after procedures
F. Must be developed after guidelines

Answer: A,D
Policies are written as a broad overview and require the support of upper management. After the development and approval of policies, guidelines and procedures may be written.

QUESTION 1383:

Total risk is equal to:(Choose All That Apply)

A. Threat
B. Vulnerability
C. Frequency
D. Asset value
E. Asset loss

Answer: A,B,D
Total risk = asset value * vulnerability * threats

QUESTION 1384:

Government data classifications include which of the following:(Choose three)

A. Open
B. Unclassified
C. Confidential
D. Private
E. Secret
F. Top Secret

Answer: B,C,F
One of the most common systems used to classify information is the one developed within the US Department of Defense. These include: unclassified, sensitive, confidential, secret, and top secret.

QUESTION 1385:

Job rotation is important because:

A. It insures your employees are cross-trained.
B. It increases job satisfaction.
C. It reduces the opportunity for fraud

Answer: C
Job rotation is tightly tied to the principle of least privilege. It is an effective security control.

QUESTION 1386:

Your co-worker is studying for the CISSP exam and has come to you with a question. What is ARP poisoning?

A. Flooding of a switched network
B. A denial of service that uses the DNS death ping
C. Turning of IP to MAC resolution
D. Inserting a bogus IP and MAC address in the ARP table
E. Modifying a DNS record

Answer: D
ARP poisoning is a masquerading attack where the attacker inserts a bogus IP and MAC address in a victims ARP table or into the table of a switch. This has the effect of redirecting traffic to the attacker and not to the intended computer.

QUESTION 1387:

What is the best description for CHAP Challenge Handshake Authentication Protocol?

A. Passwords are sent in clear text
B. Passwords are not sent in clear text
C. Passwords are not used, a digital signature is sent
D. It is substandard to PAP
E. It was used with PS2's and has been discontinued

Answer: B
Passwords are not sent in clear text. The server performing the authentication sends a challenge value and the user types in the password. The password is used to encrypt the challenge value then is sent back to the authentication server.

QUESTION 1388:

CSMA/CD computers cannot communicate without a token.(True/False)

A. True
B. False

Answer: B
CSMA/CD computers do not use a token. It is the media access method used in Ethernet.

QUESTION 1389:

_____ sends out a message to all other computers indicating it is going to send out data.

A. CSMA/CD
B. CSMA/CA
C. CSMA/HB
D. PPP
E. SLIP

Answer: B
CSMA/CA sends out a message to all other computers indicating it is going to send out data. CSMA/CA or token ring networking uses this approach to reduce the amount of data collisions.

QUESTION 1390:

Which of the following best describes ISDN BRI(Choose two)

A. 2 B channels
B. 4 B channels
C. 23 B channels
D. 1 D channel
E. 2 D channels

Answer: A,D
ISDN BRI has 2 B and 1 D channels

QUESTION 1391:

The top speed of ISDN BRI is 256 KBS.(True/False)

A. True
B. False

Answer: B
The top speed of ISDN BRI is 128 KBS. Its two primary channels are each capable of carrying 64 KBS so the combined top speed is 128 KBS.

QUESTION 1392:

Which of the following should NOT be implemented to protect PBX's?(Choose all that apply)

A. Change default passwords and configurations
B. Make sure that maintenance modems are on 24/7
C. Review telephone bill regularly
D. Block remote calling after business hours
E. Post PBX configuration and specs on the company website

Answer: B,E
Many vendors have maintenance modems that vendors can use to troubleshoot systems and provide updates. They should normally be turned off. Also information about the system should not be posted on the website and should be closely guarded.

QUESTION 1393:

Which of the following best describes the difference between a circuit based and application based firewall?

A. Application based is more flexible and handles more protocols
B. Circuit based provides more security
C. Application based builds a state table
D. Circuit based looks at IP addresses and ports
E. Circuit based firewalls are only found in Cisco routers

Answer: D
Circuit based look only at IP address and ports, whereas application based dig much deeper into the packet. This makes it more secure.

QUESTION 1394:

_____ is the fraudulent use of telephone services.

A. Rolling
B. Warzing
C. Wardriving
D. Wardialing
E. Phreaking

Answer: E
Phreaking is the fraudulent use of telephone services.

QUESTION 1395:

What is another name for a VPN?

A. Firewall
B. Tunnel
C. Packet switching
D. Pipeline
E. Circuit switching

Answer: B
A VPN creates a secure tunnel through an insecure network.

QUESTION 1396:

Which of the following is a connection-orientated protocol?

A. IP
B. UDP
C. TCP
D. ICMP
E. SNMP
F. TFTP

Answer: C
TCP is a connection-orientated protocol.

QUESTION 1397:

Which of the following is not considered firewall technology?

A. Screened subnet
B. Screened host
C. Duel gateway host
D. Dual homed host

Answer: C
Duel gateway host is not considered firewall technology.

QUESTION 1398:

Which of the following can be used to defeat a call-back security system?

A. Call waiting
B. Passive wiretapping
C. Active wiretapping
D. Brute force password attacks
E. Call forwarding

Answer: E
Call forwarding can be used to bypass the call back feature and is considered a security risk.

QUESTION 1399:

Which type of network topology passes all traffic through all active nodes?

A. Broadband
B. Star
C. Baseband
D. Token Ring

Answer: D
Token ring passes all traffic through nodes.

QUESTION 1400:

The act of validating a user with a unique and specific identifier is called what?

A. Validation
B. Registration
C. Authentication
D. Authorization
E. Identification

Answer: C
Authentication is the act of validating a user with a unique and specific identifier.

QUESTION 1401:

Why is fiber the most secure means of transmission?

A. High speed multiplexing
B. Interception of traffic is more difficult because it is optically based
C. Higher data rates make it more secure
D. Multiplexing prevents traffic analysis
E. Built-in fault tolerance

Answer: B
Fiber is more secure because it is hard to tap into and gives off no EMI such as copper cabling.

QUESTION 1402:

The IAB defines which of the following as a violation of ethics?

A. Performing a DoS
B. Downloading an active control
C. Performing a penetration test
D. Creating a virus
E. Disrupting Internet communications

Answer: E
The IAAB considers the Internet a privilege, not a right, and as such considers it unethical to purposely disrupt communications.

QUESTION 1403:

A chain of custody shows who _____ _____ and _____.(Choose three)

A. Who controlled the evidence
B. Who transcribed the evidence
C. Who validated the evidence
D. Who presented the evidence
E. Secured the evidence
F. Obtained the evidence

Answer: A,E,F
The chain of evidence shows who obtained the evidence, who secured the evidence, and who controlled the evidence.

QUESTION 1404:

Good forensics requires the use of a bit level copy?(True/False)

A. True
B. False

Answer: A
Good forensics requires the use of a bit level copy. A bit level copy duplicates all information on the suspect's disk. This includes slack space and free space.

QUESTION 1405:

Which agency shares the task of investigating computer crime along with the FBI?

A. Secret Service
B. CIA
C. Department of justice
D. Police force
E. NSA

Answer: A
Along with the FBI, the Secret Service has been given the authority to investigate computer crime.

QUESTION 1406:

This type of password recovery is considered more difficult and must work through all possible combinations of numbers and characters.

A. Passive
B. Active
C. Dictionary
D. Brute force
E. Hybrid

Answer: D
Brute force cracking is considered more difficult and must work through all possible combinations of numbers and characters.

QUESTION 1407:

_____ are added to Linux passwords to increase their randomness.

A. Salts
B. Pepper
C. Grains
D. MD5 hashes
E. Asymmetric algorithms

Answer: A
Salts are added to Linux passwords to increase their randomness. They are used to help insure that no two users have the same, hashed password.

QUESTION 1408:

The Linux root user password is typically kept in where?(Choose two)

A. etc/shadow
B. cmd/passwd
C. etc/passwd
D. windows/system32
E. var/sys
F. var/password

Answer: A,C
The Linux root user password is typically kept in /etc/passwd or etc/shadow.

QUESTION 1409:

The goal of cryptanalysis is to _____.

A. Determine the number of encryption permutations required
B. Reduce the system overhead for a crypto-system
C. Choose the correct algorithm for a specified purpose
D. Forge coded signals that will be accepted as authentic
E. Develop secure crypto-systems

Answer: D
The goal of cryptanalysis is to forge coded signals that will be accepted as authentic.

QUESTION 1410:

If an employee is suspected of computer crime and evidence need to be collected, which of the following departments must be involved with the procedure?

A. Public relations
B. Law enforcement
C. Computer security
D. Auditing
E. HR

Answer: E
Human Resources always needs to be involved if an employee is suspected of wrongdoing. They know what rules apply to protect and prosecute employees.

QUESTION 1411:

What is it called when a system has apparent flaws that were deliberately available for penetration and exploitation?

A. A jail
B. Investigation
C. Enticement
D. Data manipulation
E. Trapping

Answer: C
Administrators that leave systems with apparent flaws are performing an act of enticement. This is sometimes called a honeypot.

QUESTION 1412:

Why are computer generated documents not considered reliable?

A. Difficult to detect electron tampering
B. Stored in volatile media
C. Unable to capture and reproduce
D. Too delicate
E. Because of US law, Section 7 paragraph 154

Answer: A
Because it is difficult to detect electron tampering and can be easily modified.

QUESTION 1413:

What is the name of the software that prevents users from seeing all items or directories on a computer and is most commonly found in the UNIX/Linux environment?

A. Shell Kits
B. Root Kits
C. Ethereal
D. Shadow data
E. Netbus

Answer: D

QUESTION 1414:

What is a commercial application of steganography that is used to identify pictures or verify their authenticity?

A. A MAC
B. A digital checksum
C. A MD5 hash
D. A digital signature
E. A watermark

Answer: E
A watermark is a commercial application of steganography that is used to identify pictures or verify its authenticity.

QUESTION 1415:

What are the basic questions that must be asked at the beginning of any investigation?(Choose all that apply)

A. Who
B. Cost

C. What
D. When
E. Where
F. How
G. Time frame
H. Budget

Answer: A,C,D,E,F
At the beginning of any investigation, an investigator must ask who, what, when, where, and how. Answering the questions will lead to the successful conclusion of the case.

QUESTION 1416:

Risk can be eliminated.(True/False)

A. True
B. False

Answer: B
Risk can never be eliminated. It may be reduced or transferred to a third party through insurance, but will always remain in some form.

QUESTION 1417:

Employees are a greater risk to employers than outsiders. T/F(True/False)

A. True
B. False

Answer: A
Employees are a greater risk to employers than outsiders, because they possess two of the three items required to commit a crime: means and opportunity.

QUESTION 1418:

What does the term "red boxing" mean?

A. Denial of Service
B. Telephone voltage manipulation
C. Sounds of coins dropping
D. Tone manipulation
E. A salami attack

Answer: C
Red boxing was used by phone phreakers to record the sound off coins dropping in pay phones and play it back to gain free phone access.

QUESTION 1419:

Which of the following is the proper lifecycle of evidence?

A. A Collection, storage, present in court, destroy
B. Collection, transportation, storage, return to owner
C. Collection, present in court, transportation, return to owner
D. Collection, analysis, storage, present in court, return to owner
E. Collection, storage, transportation, present in court, return to owner

Answer: D
The life cycle of evidence includes: collection, analysis, storage, present in court, and return to owner

QUESTION 1420:

A copy of a computer disk would be what type of evidence?

A. Secondary
B. Best
C. Hearsay
D. Direct
E. Indirect

Answer: C
A copy of a computer disk is considered hearsay, because unless it has been copied in a forensically approved manner, it is not credible evidence.

QUESTION 1421:

A copyright protects _____.

A. The trade secrets of a company
B. A persons private papers
C. An invention
D. An expression or an idea
E. Distinguishing or unique characters, colors, or words

Answer: D
A copyright protects the expression of a resource, not the resource directly.

QUESTION 1422:

_____ is a _____ attack that eavesdrops on communication. (Choose two)

A. Passive
B. Active
C. Brute force
D. Wiretapping
E. Password cracking

Answer: A,D
Wiretapping is a passive attack that eavesdrops on communication. It is only legal with prior consent or a warrant.

QUESTION 1423:

What types of laws are considered standards of performance or conduct expected by government agencies from companies, industries, and certain officials.(Chose all that apply)

A. Civil
B. Criminal
C. Administrative
D. Regulatory
E. Tort

Answer: C,D
Administrative or regulatory laws are considered standards of performance or conduct expected by government agencies from companies, industries, and certain officials.

QUESTION 1424:

Sandra's employer is considering placing login banners on all company computers to indicate to the users about the permitted use of company computers. What is this called?

A. Employee privacy law
B. Employee policies
C. Employee regulations
D. User policies
E. Acceptable use policy

Answer: E
Acceptable use policies provide the company with legal protection. Logon banners should be used to inform users what will happen if they do not follow company rules.

QUESTION 1425:

_____ deemed proprietary to a company and can be information that provides a competitive edge.

A. Trade secrets are
B. Copyrights are
C. Restricted information is
D. Information marked strictly private is

Answer: A
Trade secrets are deemed proprietary to a company and can be information that provides a competitive edge. This information is protected as long as the owner takes the necessary security actions.

QUESTION 1426:

Sandra is studying for her CISSP exam. Sandra has come to you for help and wants to know what the last step in the change control process is?

A. Validated and approved
B. Test and implement
C. Review and approve
D. Report change to management
E. Inform user of change

Answer: D
Reporting the change to management is the last step in the process.

QUESTION 1427:

Who is ultimately responsible for the security of an organization?

A. Management
B. Senior management
C. The chief security officer
D. Department heads
E. Employees

Answer: B
Senior management is ultimately responsible for the security of an organization. Policy flows from the top down.

QUESTION 1428:

Which of the following falls under the categories of configuration management?(Choose three)

A. Operating system configuration
B. Software configuration
C. Hardware configuration

D. Logical configuration
E. Physical configuration

Answer: A,B,C
Configuration management controls the changes that take place in hardware, software, and operating systems.

QUESTION 1429:

Macro viruses infect what type of files.

A. Microsoft office files
B. Mail servers
C. E-mail messages
D. Web browsers
E. Linux Kernel files

Answer: A
Macro viruses infect Microsoft office files. There are many macro viruses because the macro language is easy to use and because Microsoft Office is prolific.

QUESTION 1430:

What is another name for rows and columns within relational databases?(Choose two)

A. Attributes
B. Keys
C. Tuples
D. Views
E. Attributes

Answer: C,E
Within a relational database, the rows of a table are called tuples and the columns are called attributes.

QUESTION 1431:

Which of the following can reproduce itself without the help of system applications or resources?

A. Trojan
B. Logic bomb
C. Virus
D. Worm
E. Backdoor

Answer: D
Worms can reproduce themselves without the help of system applications or resources.

QUESTION 1432:

What is the final stage of the system development life cycle?

A. Certification
B. Validation
C. Evaluation
D. Implementation
E. Maintenance
F. Installation

Answer: E
Maintenance is the final stage of the system development life cycle.

QUESTION 1433:

A polymorphic virus is _____.

A. A virus that makes copies of itself and then makes changes to those copies
B. A virus that can make itself stealth
C. A virus that is written in a macro language
D. A virus that is written in visual basic
E. A virus that infects the boot sector of a hard drive

Answer: A
A polymorphic virus is a virus that makes copies of itself, then makes changes to those copies. It does this in hopes of avoiding detection of anti-virus software.

QUESTION 1434:

Which one of the following is identified by a business impact analysis?(Choose three)

A. Determining regulatory requirements
B. Analyzing the threats associated with each functional area
C. Determining the risk associated with each threat
D. Identifying the major functional areas of information
E. Determining the team members that will be associated with disaster planning

Answer: B,C,D
The following identifies a business impact analysis: analyzing the threats associated with each functional area, determining the risk associated with each threat, and identifying the major functional areas of information.

QUESTION 1435:

_____ are the step-by-step instructions used to satisfy control requirements.

A. Policy
B. Procedure
C. Guideline
D. Standard
E. Outline

Answer: B
Procedures are the step-by-step instructions used to satisfy control requirements.

QUESTION 1436:

Which of the following are controls that can be used to secure faxing of sensitive data?(Choose all that apply)

A. Disable automatic printing
B. Print "sensitive document banner" on each page
C. Fax encryptor
D. Send to email boxes instead of printing
E. Restrict the use of fax machines that use a ribbon or duplication cartridge

Answer: A,C,D,E
All of the items listed can help secure faxes except printing a sensitive document banner, which actually encourages people to look at the document.

QUESTION 1437:

Which of the following are considered administrative controls?(Choose all that apply)

A. Rotation of duties
B. Separation of duties
C. Implementation of WEP keys
D. Enforcing mandatory vacations

Answer: A,B,D
Rotation of duties, separation of duties, and mandatory vacations are all administrative controls, enforcing WEP is a technical control

---

QUESTION 1438:

Why should organizations enforce separation of duties?

A. It ensures compliance with federal union rules

B. It helps verify that all employees know their job tasks
C. It provides for a better work environment
D. It encourages collusion
E. It is considered valuable in deterring fraud

Answer: E
Separation of duties is considered valuable in deterring fraud since fraud can occur if an opportunity exists for collaboration between various job related capabilities. The most commonly used examples are the separate transactions needed to initiate a payment and to authorize a payment. No single individual should be capable of executing both transactions.

QUESTION 1439:

What is the most secure way to dispose of data held on a CD?

A. Reformatting
B. Sanitizing
C. Physical destruction
D. Degaussing

Answer: C
Since CD's cannot be sanitized in a way to remove all data, they should be physically destroyed. There are many products that con do this. Some actually shred the CD!

QUESTION 1440:

What is the most accepted way to dispose data held on a floppy disk?

A. Reformatting
B. Sanitizing
C. Physical destruction
D. Degaussing

Answer: D
Degaussing is the most accepted way of disposing data held on a floppy disk.

QUESTION 1441:

Which of the following is NOT an attack against operations?

A. Morris Worm
B. SYN Denial of Service
C. Buffer Overflow
D. Brute force
E. Known plain text attack

Answer: E
A known plain text attack is an attack against the organization's cryptosystem, not a direct attack against operations.

QUESTION 1442:

Which one of the following tools can be used to launch a Distributed Denial of service attack against a network?

A. Satan
B. Saint
C. Trinoo
D. Nmap
E. Netcat

Answer: C
Trinoo and the Tribal Flood Network (TFN) are the two most commonly used distributed denial of service attacks. The other four tools mentioned are reconnaissance techniques used to map networks and scan for known vulnerabilities.

QUESTION 1443:

Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. Smurf
C. Ping of Death
D. SYN flood
E. SNMP Attack

Answer: A
The teardrop attack uses overlapping packet fragments to confuse a target system and cause the system to reboot or crash.

QUESTION 1444:

What are the elements of the CIA triad?(Choose three)

A. Confidentiality
B. Accountability
C. Accessibility
D. Integrity
E. Interest
F. Control
G. Availability

Answer: A,D,G
The essential security principles of confidentiality, integrity, and availability are referred to as the CIA Triad.

QUESTION 1445:

_____ is the first step of access control.

A. Identification
B. Authorization
C. Validation
D. Interrogation
E. Accountability logging

Answer: A
The first step in the access control process is identifying who the subject is.

QUESTION 1446:

What is a Type 2 authentication factor?

A. Something you know
B. Something you are
C. Something you have

Answer: C
A Type 2 authentication factor is something you have, such as a smart card, ATM card, token device, memory card, etc.

QUESTION 1447:

_____ requires that two entities work together to complete a task?

A. Rotation of duties
B. Separation of duties
C. Dual controls
D. Enforced mandatory vacations
E. Workplace rules

Answer: C
Dual controls require that two entities work together to complete a task. This is used to reduce the possibility of fraud.

QUESTION 1448:

PGP provides which of the following?(Choose three)

A. Confidentiality
B. Accountability
C. Accessibility
D. Integrity
E. Interest
F. Non-repudiation
G. Authenticity

Answer: A,D,G
PGP provides confidentiality, integrity, and authenticity.

QUESTION 1449:

Computer security is generally considered the responsibility of everyone in the organization.(True/False)

A. True
B. False

Answer: A
Everyone is responsible for security.

QUESTION 1450:

Which aspect of security was the Bell-LaPadula access control model designed to protect?

A. Authenticity
B. Accountability
C. Accessibility
D. Integrity
E. Interest
F. Non-repudiation
G. Confidentiality

Answer: G
The Bell-LaPadula model is focused on maintaining confidentiality.

QUESTION 1451:

Which access control method uses security policies and security awareness training to stop or deter an unauthorized activity from occurring?

A. Administrative
B. Preventative

C. Detective
D. Authoritative
E. Corrective

Answer: B
Preventative access control is deployed to stop an unauthorized activity from occurring.

QUESTION 1452:

The Secure Hash Algorithm (SHA) is specified in?

A. Digital Encryption Standard
B. Digital Signature Standard
C. Digital Encryption Standard
D. Advanced Encryption Standard
E. NSA 1403

Answer: A
The Secure Hash Algorithm (SHA) is specified in the Digital Encryption Standard. This is the most widely used encryption to date. It is used to encrypt millions of files ranging from matters of national security, to bank accounts, and electronic funds transfers.

QUESTION 1453:

Which of the following is an example of a symmetric key algorithm?(Choose all that apply)

A. Rijndael
B. RSA
C. Diffie-Hellman
D. Knapsack
E. IDEA

Answer: A,E
All the others except Rijndael and IDEA are examples of asymmetric key algorithms.