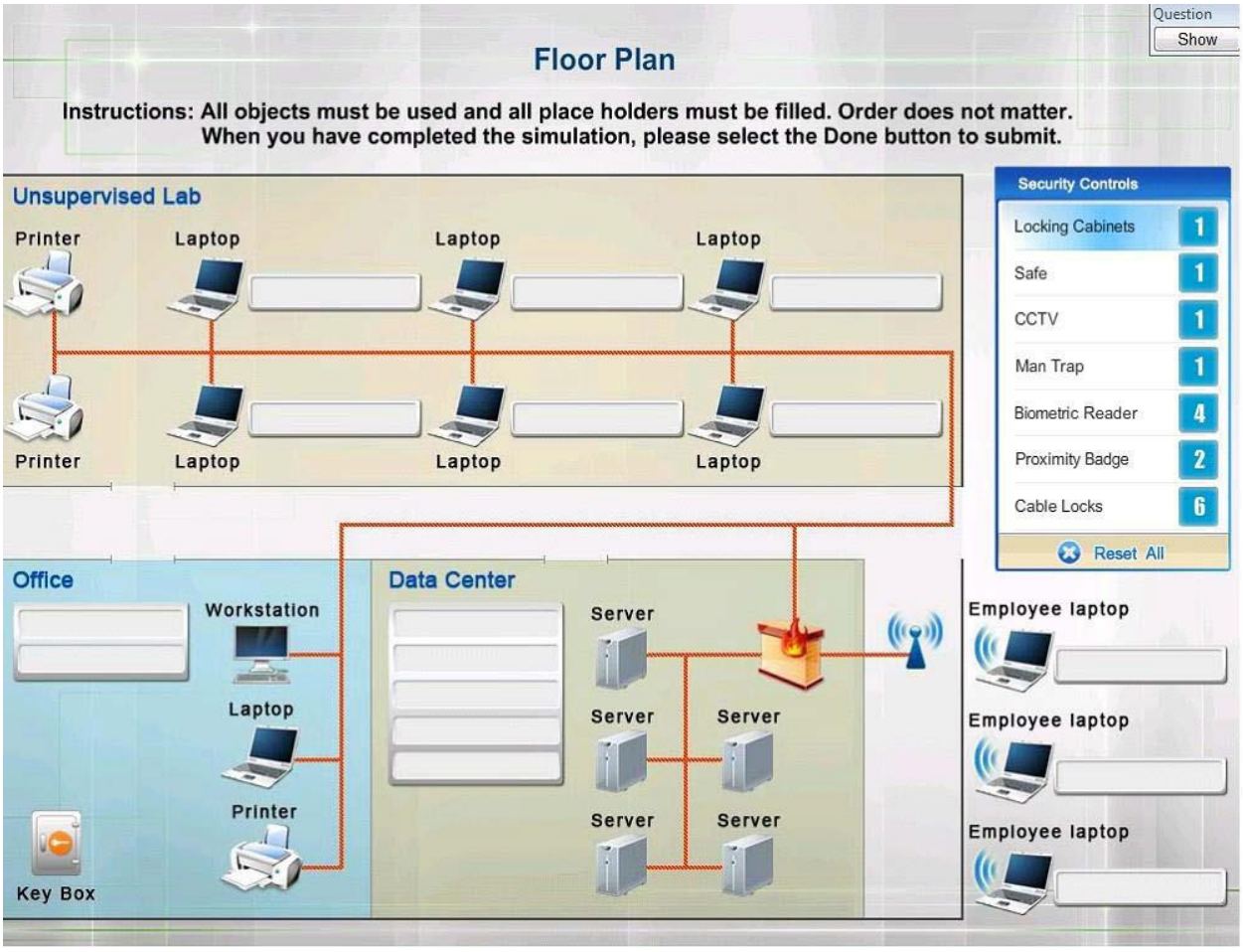
You have been tasked with designing a security plan for your company.

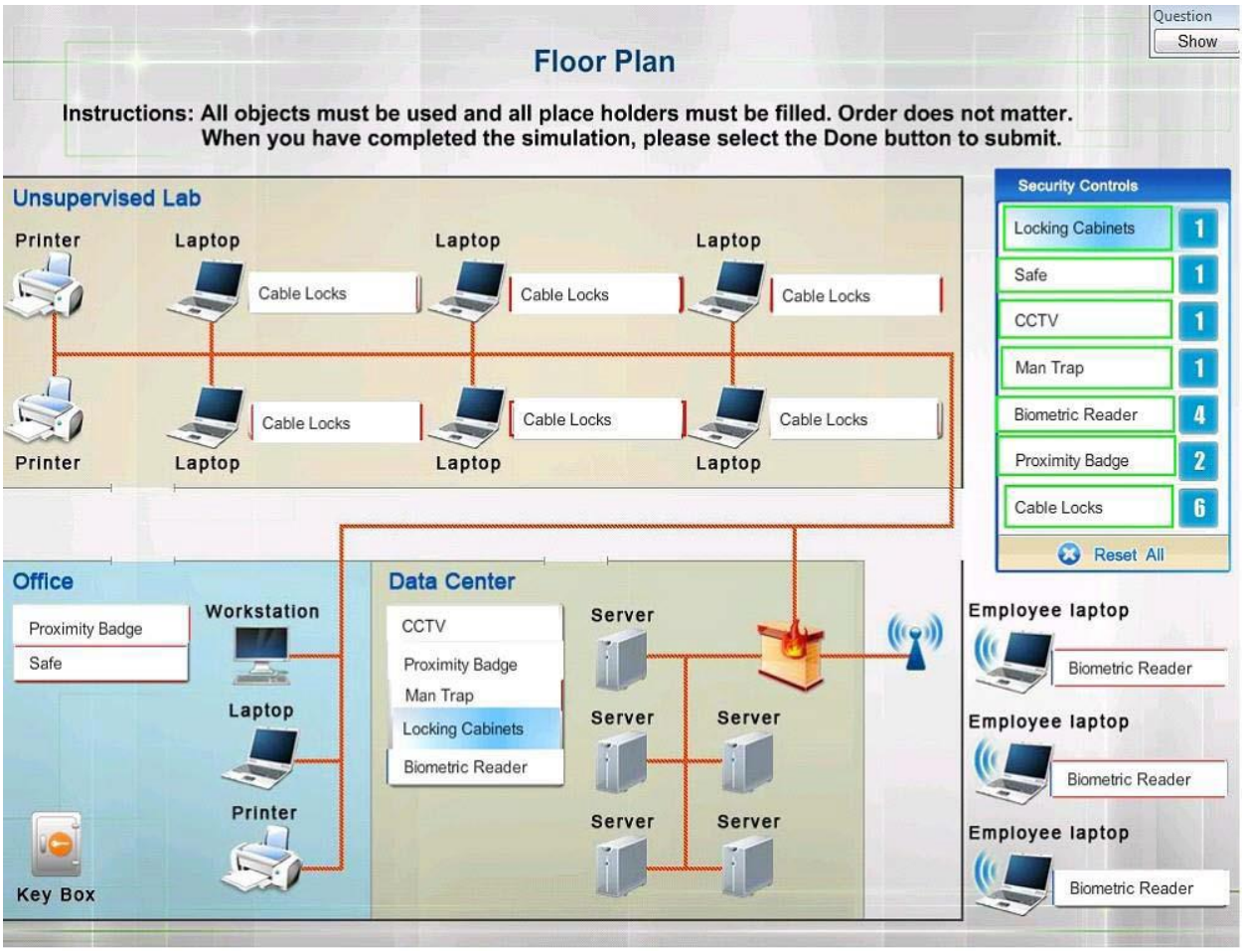
Drag and drop the appropriate security controls on the floor plan.

Instructions:

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

When you have completed the simulation, please select the Done button to submit.





The security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication.

1. 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.

2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port

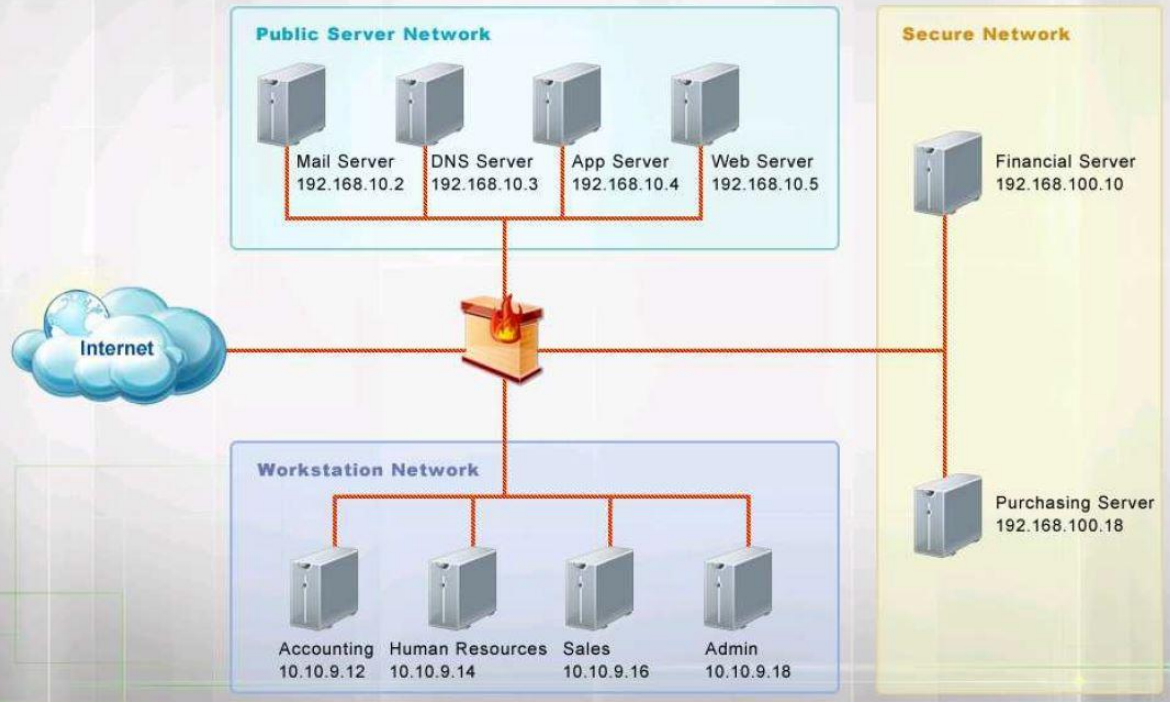
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: 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. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

Question
Show

Network Diagram

Instructions: 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. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny

Drag and Drop Question

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 updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.

Drag and Drop Question

An attack has occurred against a company.

INSTRUCTIONS

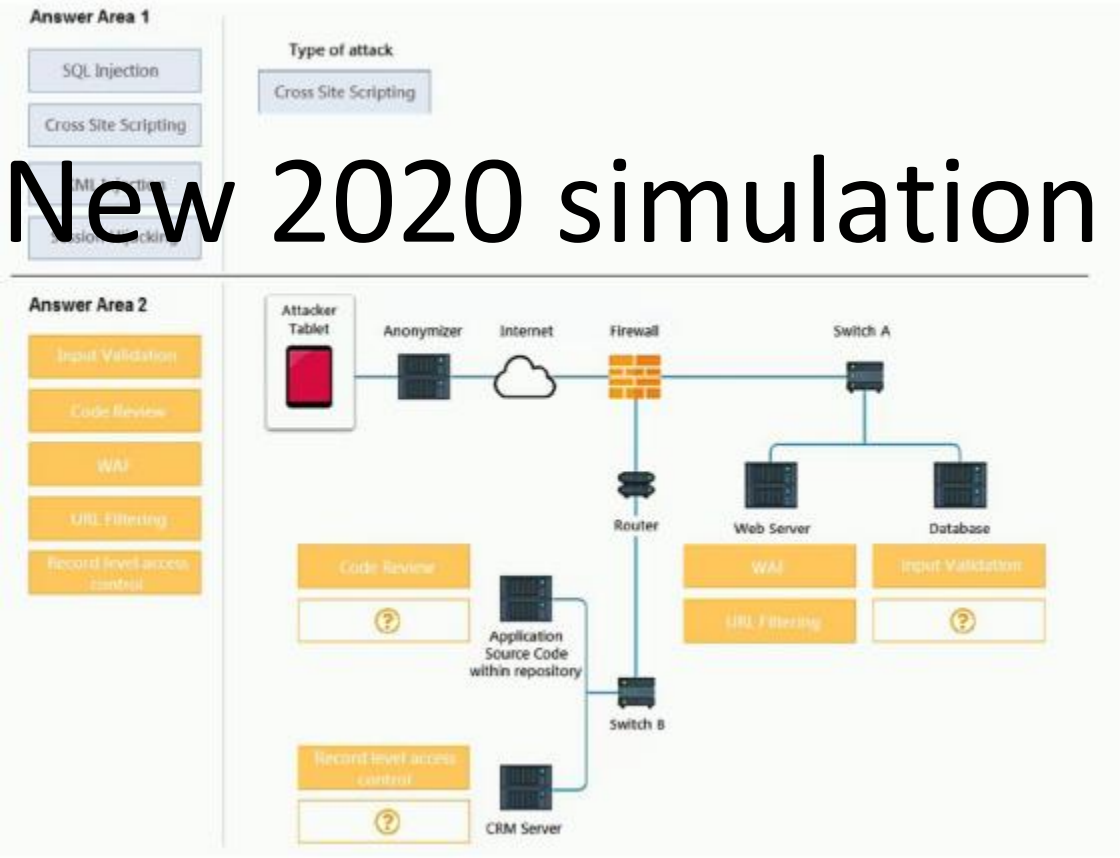
You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker1 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.



Attack Description	Target	Attack identified	Best Prevention or remediation
An attacker sends multiple SYN packets from multiple sources	Web server	SYN flood attack	
The attack establishes a connection, which allows remote commands to be executed	User	Remote code execution (RCE)	
The attack is self propagating and compromises a SQL database using well-know credentials as it moves through the network	Database server	Sql Injection	
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials	Executive	Keyloggers	
The attacker embeds hidden access in an internally developed application that bypasses account login	Application	Backdoor	

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

Answer: B

Explanation:

Encryption can be checked only with protocol analyzer

A company is experiencing an increasing number of systems that are locking upon 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

Answer: D

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 1AM 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

Answer: C.

Explanation:

SAML is the best solution to make safe SaaS federation

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

Answer: C.

Explanation:

Faraday cages help to prevent electro-magnetic interferences

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

Answer: A Explanation: Threat actors motivated by political goals are Hacktivists

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

Answer: A

Explanation:

Credentials using is the most significant difference

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

Answer: D

Explanation:

CRL has the same functionality

Which of the following provides PFS?

A. AES

B. RC4

C. DHE

D. HMAC

Answer: C

Explanation Diffie-Hellman protocol provides PFS

Staff members from a call center frequently use a conference room for meetings in the secured SOC. While walking through the SOC, the staff members can view sensitive materials displayed for monitoring purposes. The call center staff was emailed the PIN needed to open the SOC door by human resources. Which of the following access controls would prevent this situation from occurring? (Select TWO).

A. Change the entry system to one that uses proximity cards assigned to individual security staff members.

B. Create a security awareness program that educates all staff members on the risks involved with sharing the PIN for the SOC.

C. Install screen filters on all devices within the SOC and position monitors so they are not facing shared walkways.

D. Implement time-of-day restrictions that prevent access to the SOC using the shared PIN after hours.

E. Install CCTV monitors and a visitor log to control who is entering the SOC.

Answer: A D

Explanation:

The best controls - proximity cards and time-to-day restrictions

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 often passwords

C. Password length greater than ten characters

D. Complex passwords must be used

Answer: A Explanation: User can't change the password after the policy change

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

Answer: C

Explanation:

Technician should prevent all radio connections to the phone

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

Answer: C

Explanation:

443 is port for HTTPS (HTTP+SSL). However, HTTP itself uses 80 port.

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.

Answer: B Explanation: It is persistence

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.

Answer: B

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

Answer: A Explanation: It is acceptable use policy

Which of the following encryption algorithms require one encryption key? (Select TWO).

A. MD5

B. 3DES

C. BCRYPT

D. RC4

E. DSA

Answer: A D

Explanation:

These both are symmetric algorithms with single encryption key

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.

Answer: C

Explanation:

They don't have central password storage and user can use some compromised passwords

Using a one-time code that has been texted to a smartphone is an example of

A. something you have

B. something you are

C. something you know.

D. something you do

Answer: A

Explanation: It is one of the examples of what you have authentication factor

All account executives are being provided with COPE devices for their use. Which of the following mobile device security practices should be enabled for these devices to protect company data? (Select TWO)

A. Screen locks

B. Remote wipe

C. Containerization

D. Full device encryption

E. Push notification services

Answer: BC

Explanation:

Those two measures are the best for that situation (Company Owned Personally Enabled device)

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

Answer: D

Explanation: Buffer overflow (overrun) is a part of memory pointers dereferencing

A company recently purchased a new application and wants to enable LDAP-based authentication for all employees using the application. Which of the following should be set to connect the application to the company LDAP server in a secure manner? (Select TWO)

A. LDAP Path: ou-users,dc=company dc=com

B. LDAP Path: dc=com.dc=company, ou=users

C. Port 88

D. Port 636

E. Search filter: (cn=JoeAdmin)(ou=admins)(dc=company) dc-com)

F. Search filter (cn=dc01)(ou-computers) dc-com)(dc=company)

Answer: B D

Explanation:

First enables domain and second allows communication for LDAPS

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

Answer: D

Explanation:

Honeypot helps to gather information about attack and attacker

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.

Answer: B

Explanation:

Since the workstations are air-gapped the most common leakage channel is removable media

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

Answer: C

A security technician has identified an infected machine on a network. Which of the following should the technician do NEXT?

A. Power off the machine so it will not do any more damage.

B. Isolate the machine by disconnecting it from the network.

C. Escalate the issue to a senior security advisor.

D. Question the user as to what the user was doing before the machine became infected.

Answer: B

Explanation:

Isolate the machine is the first step after identification

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.

Answer: C Explanation: Certificate on the token - what you have. Secret passcode - what you know

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

Answer: B Explanation: Reporter (malicious actor) wants to use that information to gain something from the president

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

Answer: B

Explanation:

The cracks are made by humans with the help of trucks

An e-commerce company that sells sports equipment wants to partner with an e-commerce company that sells clothing by offering authenticated users access to the second company's products. Which of the following types of authentication would be BEST for the sports equipment company to use to connect to integrate the two environments?

A. SAML

B. LDAP

C. Kerberos

D. TACACS+

Answer: A

Explanation:

SAML is the best federation solution

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

Answer: A

Explanation:

The attacker first of all will use non-credentialed scan

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

Answer: A

Explanation:

To be more secure from electrical outage

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

Answer: C Explanation: Snapshot of the system is the first step

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. jax/script>

When 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

Answer: D Explanation: It is a stored XSS

Which of the following is a security consideration for loT devices?

A. loT 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.

Answer: B

Explanation: And in that case, they can't process a strong encryption

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

Answer: C

Explanation:

It will help to fill the gap in the process

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? (Select THREE)

A. S/MIME

B. TLS

C. HTTP-Digest

D. SAML

E. SIP

F. IPSec

G. Kerberos

Answer: A, C, F

Explanation:

Those 3 protocols use user-created certificates

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

Answer: A

Explanation:

It will send all the traffic to the IDS without interrupting the route.

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? (Select TWO).

A. DNS hijacking

B. Cross-site scripting

C. Domain hijacking

D. Man-in-the-browser

E. Session hijacking

Answer: AD

Explanation:

It is possible DNS poison and CSRF

Given the information below:|

MD5 HASH document.doc 049eab40 fd36caad1fab10b3cdf4a883 MD5 HASH image, jpg 049eab40fd36caad1fab0b3cdf4a883

Which of the following concepts are described above? (Select TWO)

A. Salting

B. Collision

C. Steganography

D. Hashing

E. Key stretching

Answer: BD

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: 443192. 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. RATD

D. Logic bomb

Answer: C

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? (Select TWO).

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.

E. Install antivirus on mobile endpoints.

F. Patch critical vulnerabilities at least daily.

Answer: A D

Explanation:

Remote wiping and biometrical login will prevent the unauthorized access to data

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.

Answer: B

Explanation:

It will not eradicate but give more information

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

Answer: A

Explanation:

Sandbox is the safe environment

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

Answer: B

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

Answer: A

Explanation:

It can be as a result of SQL injection attack

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 model

D. BYOD model

Answer: B

Explanation:

Company allows to choose the device from the list

A technician wants to add wireless guest capabilities to an enterprise wireless network that is currently implementing 802.IX EAP-TLS. The guest network must.

- Support client isolation
- Issue a unique encryption key to each client.
- Allow guests to register using their personal email addresses

Which of the following should the technician implement? (Select TWO).

A. RADIUS Federation

B. Captive portal

C. EAP-PEAP

D. WPA2-PSK

E. A separate guest SSID

F. P12 certificate format

Answer: B C

Explanation:

First allows register with email and the second - isolation and encryption

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.

Answer: C

Explanation:

Because the other measures described will not prevent password reuse

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

Answer: D

Explanation:

Preventive control mitigate the risk

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

Answer: D

Explanation:

This will be the best solution for that

A company recently implemented a new security system.

In the course of configuration, the security administrator adds the following entry:

#Whitelist

USB\VID13FE&PID_4127&REV_0100

Which of the following security technologies is MOST likely being configured?

A. Application white listing

B. HIDS

C. Data execution prevention

D. Removable media control

Answer: D

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's certificate pair must be installed on the web servers.

C. The web servers' private certificate must be installed on the UTM.

0. The UTM and web servers must use the same certificate authority.

Answer: A

Explanation:

This is the best solution

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 Answer: D Explanation:

They can check if hashes match the passwords

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.

Answer: C

Explanation:

It will allow complexity and disable older clients.

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

Answer: C

Explanation:

It is supply chain issue

A sensitive manufacturing facility has recently noticed an abnormal number of assembly-line robot failures. Upon intensive investigation, the facility discovers many of the SCADA controllers have been infected by a new strain of malware that uses a zero day flaw in the operating system Which of the following types of malicious actors is MOST likely behind this attack?

A. A nation-state

B. A political hacktivist

C. An insider threats

D. A competitor

Answer: D

Explanation:

Because they affected the work process

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

Answer: C Explanation: It will meet all requirements

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.

Answer: C

Explanation:

It is fairly cheap and will make secure certificates with chain of authority

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

Answer: C Explanation: SAML allow the identification federation

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.

Answer: D

Explanation:

Account without interactive login will prevent a misuse 64.

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

Answer: B

Explanation:

To gain more information about the malicious actors and their methods

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

Answer: B

Explanation:

They want to be noticed

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

Answer: B

Explanation:

Agile teams should deploy the releases fast

.

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

Answer: B

Explanation:

The secure configuration should allow baseline

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.IX

B. SSH

C. Shared secret

D. SNMPv3

E. CHAP Answer: C

Explanation:

TACACS+ is authenticated with switch using the shared key

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/AC

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 it 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

Answer: C

A security analyst is checking log files and finds the following entries:

C:l\>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,

Answer: C

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 in 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

Answer: A

Explanation:

Insurance it is risk transition technique

Which of the following implements two-factor authentication on a VPN?

A. Username, password, and source IP

B. Public and private key

C. HOTP token and logon credentials 0. Source and destination IP addresses

Answer: C

Explanation:

Logon credentials - 1$I authentication factor, HOTP token - 2nd

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

Answer: D

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.

Answer: C

A forensic analyst is creating a report of findings for litigation purposes. The analyst must ensure data preserved using all elements of the CIA triad. Given this scenario, which of the following should the analyst use to BEST meet these requirements?

A. Hashing for confidentiality, full backups for integrity, and encryption for availability

B. Full backups for confidentiality, encryption for integrity, and hashing for availability

C. Hashing for confidentiality, encryption for integrity, and full backups for availability

D. Encryption for confidentiality, hashing for integrity, and full backups for availability

Answer: D

Explanation:

Only this answer has Encryption for confidentiality as a first factor in this triad

Which of the following controls is implemented in lieu of the primary security controls?

A. Compensating

B. Corrective

C. Detective

D. Deterrent

Answer: B

Explanation:

This control helps to improve the primary control.

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

Answer: A Explanation:

It is false rejection rate

During the incident handling process, an analyst ran the following command:

PS c: \>get.-filehash c: \windows\sysre:n32\cmd.exe

SHA1 cmd.exe cda52a0faca4ac7df32cffc6c3fa05acf42ad5cb7

The original file hash for cmd.exe was: ab5d7c8faca4ac7df32cfb6c8fa09acf42ad5fl2

Which of the following is MOST associated with this indicator of compromise?

A. Virus

B. Rootkit

C. Backdoor

D. Keylogger

Answer: C Explanation: It is utility for remote malicious access.

A company is deploying MFDs in its office to improve employee productivity when dealing with paperwork. Which of the following concerns is MOST likely to be raised as a possible security issue in relation to these devices?

A. Sensitive scanned materials being saved on the local hard drive

B. Faulty printer drivers causing PC performance degradation

C. Improperly configured NIC settings interfering with network security

D. Excessive disk space consumption due to storing large documents Answer: A

Explanation:

The answers B and C have incorrect conclusions. D is not security issue.

Which of the following algorithms would be used to provide non-repudiation of a file transmission?

A. AES

B. RSA

C. MD5

D. SHA

Answer: B

Explanation:

This algorithm is used for digital signature.

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

Answer: A

Explanation:

OCSP is the best replacement for the CRL.

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.

Answer: C

Explanation:

It is used for encryption of the data that is currently used.

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.

Answer: C

Explanation:

This answer meets the both goals

A company is implementing an authentication system for its wireless network. The system will be for public use and must be able to track how long a person is connected to the WiFi system for billing purposes. Which of the following would be BEST to implement in this situation?

A. Captive portal

B. Pre-shared key

C. WPS

D. 802.IX Answer: A

Explanation:

It allows the goals, the other answers are for security purposes

The Chief Information Security Officer (CISO) at a large company tasks a security administrator to provide additional validation for website customers. Which of the following should the security administrator implement?

A. HTTP

B. DNSSEC

C. 802.IX

D. Captive portal

Answer: B Explanation:

This answer is for web-site security.

A service provider recently upgraded one of the storage clusters that houses non-confidential data for clients. The storage provider wants the hard drives back in working condition. Which of the following is the BEST method for sanitizing the data given the circumstances?

A. Hashing

B. Wiping

C. Purging

D. Degaussing

Answer: B

Explanation:

Only this answer will not destroy the disk itself instead of A - this answer will not clean the disk.

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

Answer: C

Explanation:

The authorities are described in role model.

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

Answer: C

Explanation:

It is the hash-algorithm to validate the integrity

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.

Answer: A Explanation: Malware should be inspected only in isolated environment.

A systems administrator wants to disable the use of usernames and passwords for SSH authentication and enforce key-based authentication. Which of the following should the administrator do NEXT to enforce this new configuration?

A. Issue a public/private key pair for each user and securely distribute a private key to each employee

B. Instruct users on how to create a public/private key pair and install users' public keys on the server

C. Disable the username and password authentication and enable TOTP in the sshd.conf file.

D. Change the default SSH port, enable TCP tunneling, and provide a pre-configured SSH client.

Answer: B Explanation: Users should create their keys by themselves

An administrator is beginning an authorized penetration test of a corporate network. Which of the following tools would BEST assist in identifying potential attacks?

A. Netstat

B. Honeypot

C. Company directory

D. Nmap

Answer: D

Explanation:

Nmap is the best tool for identifying attacks

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

Answer: B

Explanation:

Default port for NetBIOS is 137

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

Answer: B

Explanation:

It is organized crime hacker bands, usually they are demanding money and using ransomware

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

Answer: A

Explanation:

Is designed for low power consumption

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

Answer: B

Explanation:

VM escape is the vulnerability when user or process from the one VM can affect the others, or host system

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

Answer: B

Explanation:

Administrator eradicated the weak services

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? (Select TWO).

A. Vishing

B. Whaling

C. Spear phishing

D. Pharming

E. War dialing

F. Hoaxing

Answer: C F

Explanation:

Those are two most possible security concerns for that case

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? (Select TWO).

A. Vishing

B. Whaling

C. Spear phishing

D. Pharming

E. War dialing

F. Hoaxing

Answer: C F

Explanation:

Those are two most possible security concerns for that case

Chat White Board 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 Answer: D

Explanation:

Swap space is gaining data from all processes are running in the memory

Some call center representatives' workstations were recently updated by a contractor, who was able to collect customer information from the call center workstations. Which of the following types of malware was installed on the call center users' systems?

A. Adware

B. Logic bomb

C. Trojan

D. Spyware

Answer: D

Explanation:

Malware for covert information collection

Which of the following is unique to a stream cipher?

A. It encrypts 128 bytes at a time.

B. It uses AES encryption.

C. It performs bit-level encryption.

D. It is used in HTTPS.

Answer: C Explanation: Stream cipher encrypting bits in blocks

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.

Answer: A

Explanation:

Single point of failure is always a problem

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

Answer: D

Explanation:

ARP spoofing is when attacker sends the other MAC address to the network device

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

Answer: C

Explanation:

Is best set of measures for password protection

A security administrator is enhancing the security controls in an organization with respect to the allowed devices policy. The administrator wrote a .reg file with the code below:

HKE Y__LOCAL_M^CHINE\System\Current control set\Services \USBTOR "Start = dword : 00000004

Which of the following BEST represents what the administrator is doing?

A. Changing the name of the USB port

B. Requiring USB device encryption

C. Upgrading the system to USB 3.0

D. Blocking the use of USB devices

Answer: D

Explanation: This string blocks the use of USB devices

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 I rpm	1. 8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 RPM (RASA-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

Answer: D

Explanation:

This ID has the highest risk score

A small contracting company's IT infrastructure enables the processing of various levels of sensitive data for which not all employees have access. However, the employees share physical office space. Which of the following controls would help reduce the risk of accidental spillage of sensitive data?

A. Install screen filters.

B. Install cable locks for computers.

C. Use an IDS within the employees' offices.

D. Segment the network into VLANs.

E. Implement a DLP solution.

Answer: A

Explanation:

It will protect physically data from shoulder surfing

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

Answer: B

Explanation:

Air gapping is the best solution to prevent outside network attacks

Which of the following is one of the fundamental differences between the Agile and waterfall development models?

A. Agile development sprints do not end until all tasks assigned to a sprint are completed.

B. Waterfall models account for schedule slippage by moving individual tasks to later phases.

C. Waterfall development takes place in well-defined linear cycles planned in advance of the entire project.

D. Agile development plans all sprints in advance of the initial project kickoff.

Answer: C

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 5 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.

Answer: A

Explanation:

The most possible issue is other system password reuse.

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

Answer: B

A security administrator receives a request from a customer for certificates to access servers securely. The customer would like a single encrypted file that supports PKCS and contains the private key. Which of the following formats should the technician use?

A. PEM

B. DER

C. P12

D. PFX

Answer: A

Explanation:

It contains all the user need

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 Pll or PHI.

Answer: A Explanation: The better step is to check the contract about data retention policies

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? (Select TWO).

A. tcpdump

B. nc

C. nmap

D. nslookup

E. tail

F. traced

Answer: AB

Explanation:

tcpdump to check traffic to the listener and nc - to check services

Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Select TWO).

A. Accounting

B. Authentication

C. Auditing

D. Authorization

E. Non-repudiation

Answer: AC

Explanation:

It gives rights (accounting) and check the state (auditing)

A security engineer is looking to purchase a fingerprint scanner to improve the security of a datacenter. Which of the following scanner characteristics is the MOST critical to successful implementation?

A. Low false rejection rate

B. High false rejection rate

C. High false acceptance rate

D. Low crossover error rate

Answer: C

Explanation:

High false acceptance rate is most critical characteristic. It allows the unauthorized personnel to access the datacenter

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

Answer: A

Explanation:

This attack is fully mitigated by data retention policy

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

Answer: B

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. Identify mission-critical applications and systems.

C. Identify the single point of failure in the system.

D. Identify the impact on safety of the property

Answer: D

Explanation:

Natural disasters affects property safety first

A user wants to send a confidential message to a customer to ensure unauthorized users cannot access the information. Which of the following can be used to ensure the security of the document while in transit and at rest?

A. BCRYPT

B. PGP

C. FTPS

D. S/MIME

Answer: B

Explanation:

It is most common encryption in that case

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

Answer: B

Explanation:

The range of addresses is exhausted

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

Answer: C

Explanation:

File is encrypted with ransomware

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.

Answer: C

Explanation:

21 port is for FTP that uses unencrypted communication

A security administrator is researching ways to improve the security of a manufacturing company's systems within the next three to six months. Which of the following would provide the security administrator with the MOST diverse perspective?

A. Platform-specific security benchmark for the company’s specific systems

B. Manufacturing security auditing requirements

C. Academic security research on emerging technologies

D. Security regulations from other industry verticals

Answer: B

An organization has decided to implement biometric controls for improved access management. However, a significant number of authorized users are being denied access to networked resources. Which of the following is the MAIN biometric factor that requires attention?

A. False acceptance

B. False rejection

C. True negative

D. True positive

Answer: B

Explanation:

It is false rejection problem

A security technician must prevent unauthorized external access from stolen passwords. Which of the following authentication methods would allow users to use their current passwords while enhancing security?

A. Biometrics

B. Cognitive passwords

C. Trusted platform module

D. One-time password

Answer: A

Explanation:

It will allow users to use current passwords with second factor

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.

Answer: B

Explanation:

It will fully destroy data and the drive itself

A company has a backup site with equipment on site without any data. This is an example of

A. a hot site

B. a cold site.

C. a hot standby

D. a warm site.

Answer: D

Explanation:

With data it will be hot site, without equipment - cold

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.

Answer: B

Explanation:

This protocol using secure transfer

Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?

A. Memory leak

B. SQL injection

C. Resource exhaustion

D. Buffer overflow

Answer: A, Explanation: This type of attack affect memory that is pointed to the application

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.

Answer: B

Explanation: This is SQL port

A security administrator's review of network logs indicates unauthorized network access, the source of which appears to be wired data jacks in the lobby area. Which of the following represents the BEST course of action to prohibit this access?

A. Enabling BDPU guard

B. Enabling loop prevention

C. Enabling port security

D. Enabling anti-spoofing

Answer: C

Explanation:

Port security will prevent the physical intrusion in the network

A company notices that at 10a.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

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

A. Rootkit

B. Backdoor

C. Logic bomb

D. RAT

Answer: C

Explanation:

If some file exists (c:\file.txt) it will recursively delete the subcategory

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 configure 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.

Answer: A

Explanation:

It is the best solution to monitor all traffic in that case

Which of the following attacks is used to capture the WPA2 handshake?

A. Replay

B. IV

C. Evil twin

D. Disassociation

Answer: A

Explanation:

WPA2 handshakes are capturing with replay attack

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

Answer: D

Explanation:

SSL Pinning is the best solution to prevent MITM attack

A security administrator found the following piece of code referenced on a domain controller's task scheduler

Svar = GetDomainAdmins If Svar != 'fabio'

Set DomainAdmins = NULL

With which of the following types of malware is the code associated?

A. RAT

B. Backdoor

C. Logic bomb

D. Crypto-malware

Answer: C

Explanation:

It will delete domain admins if there is no admin equal Fabio

An authorized user is conducting a penetration scan of a system for an organization. The tester has a set of network diagrams, source code, version numbers of applications, and other information about the system, including hostnames and network addresses. Which of the following BEST describes this type of penetration test?

A. Gray-box testing

B. Black-box testing

C. White-box testing

D. Blue team exercise

E. Red team exercise

Answer: C

Explanation:

It is white-box because tester has all the information about the system

In order to prevent the possibility of a thermal shutdown, which of the following physical controls should be implemented in a datacenter?

A. Hot and cold aisles

B. Air-gapped servers

C. Infrared detection

D. Halon suppression

Answer: A

Explanation:

The best control will be to separate hot and cold streams

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.

Answer: C

A security analyst is responsible for assessing the security posture of a new high-stakes application that is currently in the production environment but has not yet been made available to system users. Which of the following would provide the security analyst with the MOST comprehensive assessment of the application’s ability to withstand unauthorized access attempts?

A. Dynamic analysis

B. Vulnerability scanning

C. Static code scanning

D. Stress testing

Answer: A

Explanation:

The application is deployed

A security administrator is implementing a SIEM and needs to ensure events can be compared against each other based on when the events occurred and were collected. Which of the following does the administrator need to implement to ensure this can be accomplished?

A. TOTP

B. TKIP

C. NTP

D. HOTP

Answer: C

Explanation:

It is network time protocol

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. RAIDI

C. RAID 2

D. RAID 3

Answer: B

Explanation:

It is data mirroring between 2 disks

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

Answer: B Explanation:

SIEM will help with the task to identify malicious actors and deeds

A network technician identified a web server that has high network utilization and crashes during peak business hours. After making a duplicate of the server, which of the following should be installed to reduce the business impact caused by these outages?

A. Load balancer

B. Layer 3 switch

C. Traffic shaper

D. Application proxy

Answer: A

Explanation:

Load balancer will balance traffic load between two servers

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? (Select 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.

Answer: A D

Explanation:

It will the best practice. Service account does not have interactive logon possibility and least privileges will reduce the risk

An organization utilizes network devices that only support a remote administration protocol that sends credentials in cleartext over the network. Which of the following should the organization do to improve the security of the remote administration sessions?

A. Upgrade the devices to models that support SSH.

B. Enforce PPTP with CHAP for network devices.

C. Implement TACACS on the organization's network.

D. Replace SNMPvl with SNMPv2c on network devices.

Answer: A

Explanation:

The only way is to use secure shell protocol

A systems administrator wants to determine if two DNS servers are configured to have the same record for IP address 192.168.1.10. The systems administrator has verified the record on Serverl and now needs to verify the record on Server2. Which of the following commands should the systems administrator run?

A. nslookup server2 192.168.1.10

B. ne-1-P 53 192.168.1.10-eserver2

C. tcpdump -Inv host 192.168.1.10 or host server2

D. dig -x 192.168.1.10 @server2

Answer: A

Explanation:

This command will return the name for IP address from the server2 record

157.

A security analyst was performing a BIA for a web commerce company and identified that one server in the entire network is responsible for the front-end site. Which of the following BEST describes the potential impact this poses to the organization? (Select TWO).

A. Privacy non-compliance

B. Single point of failure

C. Application overload

D. Low recovery point objective

E. Short MTTR metrics

Answer: B C

Explanation:

The problem is that this server will receive the most load

An organization is considering utilizing a third-party web-hosting service for a human resources application. The organization's Chief Information Officer (CIO) is concerned the web-hosting service may not have a sufficient level of security. The sales representative for the web hosting service suggests that the CIO use banner grabbing to test the security levels of an existing website hosted by the company www.example.com). Which of the following commands should the CIO use? (Select TWO)

A. no

B. telnet

C. ifoonfig

D. traced

E. netstat

F. nslookup

Answer: AB

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.

Answer: A

Explanation:

It is the most possible

Which of the following BEST identifies repeated exploitation of different network hosts after mitigation has occurred?

A. Privilege escalation

B. Pivoting

C. Persistence

D. Zero day

Answer: C

Explanation:

Persistence means how to stay in system after mitigation

During routine maintenance, a security engineer discovers many photos on a company issued laptop. Several of the photos appear to be the same, except the file sizes are noticeably different and the image resolution is lower. The security engineer confiscates the user's laptop. Which of the following threats is the security engineer MOST likely concerned about?

A. The security engineer suspects the photos contain viruses.

B. The photos are taking up too much space on the user's hard drive.

C. The security engineer suspects the photos contain rootkits.

D. The security engineer suspects steganography is being used.

Answer: D

Explanation:

Steganography it is when someone hides files inside pictures, audio or video files

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.

Answer: B

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

Answer: B

Explanation:

Implementing controls is risk mitigation

A forensic analyst needs to collect physical evidence that may be used in legal proceedings. Which of the following should be used to ensure the evidence remains admissible in court?

A. Bit-level image

B. Chain of custody

C. Log capture

D. Incident response plan

Answer: B

Explanation:

Chain of custody is very important for evidence

Which of the following ready resources is a cold site MOST likely to have?

A. Servers

B. Workstations

C. Internet access

D. Electricity

Answer: D

Explanation:

The main facility for cold site is electricity

A user has lost access to all organization resources on a mobile device but can still get to personal email, the Internet, and other applications. The organization uses MDM on company devices. The user contacts the service desk for assistance, but there are no other issues reported or outages of company email or mobile applications. Which of the following has MOST likely occurred to cause this issue?

A. Allowable authentication methods were set to pattern, but the user changed it to a complex password.

B. The organization enabled encryption for the devices through the MDM.

C. The user changed the password for the mobile device's lock screen.

D. The user rooted the mobile device, which caused the MDM software to disable all company access

Answer: D

Explanation:

The most possible cause is rooting the device

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.

Answer: D

Explanation:

Credentialed scan sees the system as logged user

A security technician is reviewing packet captures. The technician is aware that there is unencrypted traffic on the network, so sensitive information may be present. Which of the following physical security controls should the technician use?

A. Key management

B. Air gap

C. Faraday cage

D. Screen filter

Answer: B

Explanation:

It will prevent the threats from outer network

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

Answer: D

Explanation:

It prevents fraud because each transaction need 2 pairs of eyes to confirm

Which of the following can be used to obfuscate malicious code without the need to use a key to reverse the encryption process?

A. ROT13

B. MD4

C. ECDHE

D. HMAC

Answer: A

Explanation:

Only ROTI3 does not need any key (it is switch for 13 symbols)

A company is deploying a file-sharing protocol across 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

Answer: C

Explanation:

Kerberos is allowing SSO and mutual authentication

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.

Answer: A.

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

Answer: B.

Explanation: It will secure the website transactions

A human resources manager needs to be able to view all employees' salary and annual increase information, but the payroll manager needs view and edit access to the employees' salary and benefits selections. Which of the following is the BEST access control method to implement?

A. Mandatory access control

B. Rule-based access control

C. Role-based access control

D. Discretionary access control

Answer: C.

Explanation: Role-based access will give different access level for different roles

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

Answer: C.

Explanation: Only this protocol is for that purpose

A technician is recommending preventive physical security controls for a server room. Which of the following would the technician MOST likely recommend? (Select TWO).

A. GEO fencing

B. Video surveillance

C. Protected cabinets

D. Mantrap

E. Key exchange

F. Authorized personnel signage

Answer: BD.

Explanation: It is both physical measures related for the server room

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

Answer: A Full tunnel VPN will meet all requirements

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

Answer: C

Captive portal actually is made for that

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

Answer: B

RAM is most volatile

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

Answer: D

It will show all active and waiting connections

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

Answer: D

MSCHAP provides mutual authentication

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.

Answer: D

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 P the following configurations should the engineer choose?

A. EAP-TLS

B. EAP-TTLS

C. EAP-FAST

D. EAP-MD5

E. PEAP

Answer: A

Allows mutual authentication

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.

Answer: D

For classified government data trusted OS is a must

An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the helpdesk 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 maar is MOST Bely responsible for producing the SIEM alerts?

A. Ransomware

B. Logic bomb

C. Rootkit

D. Adware

Answer: B

It seems being logic bomb in firmware

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? (Select TWO).

A. Poorly trained users

B. Misconfigured WAP settings

C. Undocumented assets

D. Improperly configured accounts

E. Vulnerable business processes

Answer: A D

Poor account configuration with poor training makes that things happens

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

Answer: A

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

Answer: A

Most possible that files were encrypted with ransomware

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 mom and external customers. W 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.

Answer: B

Mail and Webserver can be placed into DMZ and be accessible securely from both sides

Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES

B. SSL

C. TLS

D. RSA

Answer: A

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.

Answer: A

Configuration exam will minimize the system interaction

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

Answer: D

Which of the following are used to substantially increase the computation time required to crack a password? (Select TWO)

A. BCRYPT

B. Substitution cipher

C. ECDHE

D. PBKDF2

E. Diffie-Hellman

Answer: A D

Those two are made for increasing computation time

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 BE control to address this audit finding?

A. Faraday cage

B. Mantrap

C. Biometrics

D. Proximity cards

Answer: B

Mantrap could not allow access of multiple people in the same location at the same time

A security analyst, who is analyzing the security of the company s web server, receives the following output:

POST http://www.acme.com/AuthenticationServlet HTTP/1.1 Hos t: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=LvzZRJJXgwyWPWEQMhS49vtWlyJdvn78CGKp5jTwChDyPkrun4tl
Content=type:application/x-www-form-urlencoded Content-lenghth:64

delegate service=l314user=acmel&pass=test&submit=SUBMIT

Which of the following is the issue?

A. Code signing

B. Stored procedures.

C. Access violations.

D. Unencrypted credentials.

Answer: D

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

Answer: D

It will make the snapshot of the RAM and it will fasten the restoration

Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrators and help desk staff?

A. Passive reconnaissance

B. Initial exploitation

C. Vulnerability scanning

D. Social engineering

Answer: A

It is a part of OSINT

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

Answer: D

The next step will be containment. Then will be eradication.

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. One-time passwords

B. Email tokens

C. Push notifications

D. Hardware authentication

Answer: D

It will not demand additional user interaction

An employee to test the function before recommending implementation. An employee takes the plain text 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 to different documents. Which of the flowing BEST describes this cryptographic attack?

A. Brute force

B. Known plaintext

C. Replay

D. Collision Answer: D

It is description of cryptographic collision

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.

Answer: B

Which of the following is the BEST way for home users to mitigate vulnerabilities associated with loT devices on their home networks?

A. Power off the devices when they are not in use.

B. Prevent loT devices from contacting the Internet directly.

C. Apply firmware and software updates upon availability

D. Deploy a bastion host on the home network.

Answer: B

To close them from direct external connection is the best way to secure

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 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.

Answer: A

If HDD shouldn’t be operable after that

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.

Answer: A

The help desk can wipe them securely

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.

Answer: A

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

Answer: D

DHCP snooping prevent DHCP starvation

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

Answer: A

Server suffers denial of service attack from distributed malicious actors

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

Answer: D

Restricted data will be stored on-premise and the other - in cloud

Users are attempting to access a company's website but are transparently redirected to another website. 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

Answer: A

It seems to be the DNS poisoning attack.

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:

click here to unsubscribe

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection

B. CSRF

C. XSS

D. XSRF

Answer: B

It is the most common example of cross-site request forgery

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.

Answer: A.

Encryption will give confidentiality and digital sign - integrity

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? (Select TWO).

A. Containerization

B. FDE

C. Remote wipe capability

D. MDM

E. MFA

F. OTA updates

Answer: AD

Actually only those two measures can allow all needed functionality.

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.

Answer: A

It has the well-known initial configuration

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.

Answer: A

WAF is made for public web-services defense

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 the 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.

Answer: B

It will prevent the new infestation

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

Answer: B

While checking the traffic administrator can find the unwanted services

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.IX utilizing the current PKI infrastructure

B. SSO to authenticate corporate users

C. MAC address filtering with ACLs on the router

D. PAM for user account management

Answer: A

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. CR

D. CSR

Answer: B

This technology allows fast certificate state check

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.

Answer: A

It is the only reasonable explanation

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

Answer: D Explanation:

EAP protocol is modern version of TKIP

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon investigation a security analyst identifies the following:

- The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to this IP.
- The forged website's IP address appears to be 10.2.12.99, based on NetFlow records.
- All three of the organization's DNS servers show the website correctly resolves to the legitimate IP.

- DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.

Which of the following MOST likely occurred?

A. A reverse proxy was used to redirect network traffic.

B. An SSL strip MITM attack was performed.

C. An attacker temporarily poisoned a name server.

D. An ARP poisoning attack was successfully executed.

Answer: D Explanation:

It looks like ARP poisoning, because DNS has cached web-site with forged IP

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

Answer: D Explanation:

Secure Real-time Transport Protocol

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

Answer: C.

Explanation:

It is context-aware authentication, because it should use geofencing, AV version and authentication target.

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 micro-segmentation rules

C. Emulate the malware in a heavily monitored DMZ segment.

D. Apply network blacklisting rules for the adversary domain.

Answer: D Explanation:

Better will be to block access to C&C server

232.

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

Answer: D Explanation:

Is the weakest authentication wireless protocol

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

Answer: D

A security analyst is reviewing the following attack log output.

user comptia\john.smith attempted login with the password password123

user comptia\jane.dco attempted login with the password password123

user comptia\user.one attempted login with the password password123

user comptia\user.two attempted login with the password password123

user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234

user comptia\jane.dco attempted login with the password password234

user comptia\user.one attempted login with the password password234

user comptia\user.two attempted login with the password password234

user comptia\user.three attempted login with the password password234

Which of the following types of attacks does this MOST likely represent?

A. Rainbow table

B. Brute Force

C. Password-spraying

D. Dictionary

Answer: C

Explanation:

It is called password-spraying when someone tries one or several passwords on the different usernames

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

Answer: C

Explanation:

He protects the application from buffer overflow

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 constant recommend?

A. S/MIME

B. DNSSEC

C. RADIUS

D. 802.11X

Answer: A Explanation:

It allows the message integrity check with digital sign

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

A. Corrective

B. Physical

C. Detective

D. Administrative

Answer: C Explanation:

IDS detecting the threats

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

Answer: D

Explanation:

It is passive method

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

Answer: B Explanation:

The best is purging for HDD

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.

Answer: C

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 to communicate back to central server. 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

Answer: D

Explanation:

Network segmentation without routes between segments

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 storage 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 failing and the files are being corrupted.

B. The computer has been infected with crypto-malware.

C. A reply attack has occurred.

D. A keylogger has been installed.

Answer: A Explanation:

It is not crypto-malware because there were no messages on boot-up or login

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.

Answer: D Explanation:

It is the best method for risk correction on both system/application layer

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

Answer: C Explanation:

Memory dump should be given to forensic firm

A company is planning to build an internal website that allows for access to outside contractors 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

Answer: A Explanation:

Better is to use VPN by the external contractors to access internal web-site.

A technician who is managing a secure B2B connection, noticed the connection broke last night All networking equipment and media functioning as expected, which leads the technician to question certain PKI components. Which of the following should the technician use to validate this assumption?

(Select two)

A. PEM

B. CER

C. SCEP

D. CRL

E. OCSP

F. PFX

Answer: DE

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. ApplyaGPO

C. Conduct use awareness training

D. Enforce the AUP

Answer: D

Explanation:

It is the most effective

Which of the following is a random value appended to a credential that makes the credential less susceptible to compromise when hashed?

A. None

B. Salt

C. OTP

D. Block cipher

E. IV

Answer: B

Explanation:

It makes the hash more random

A security operation 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

Answer: C Explanation:

To teach the employees password rules

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

Answer: D Explanation:

It is made for accessing the multiple applications after first logon

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 DP controls and prevent the use of USB drives on devices.

D. Configure the WAP's to use NAC and refuse connections that do not pass the health check.
Answer: A

Explanation:

Only this control can prevent undocumented and unpatched devices

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.

Answer: B Explanation:

It should be configured on endpoint

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

Answer: D Explanation:

Credentialed scan can determine needed patches to be installed

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

Answer: B Explanation:

It looks like B Smith shared his account with colleagues 255.

A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or Wifi network are not impacted, but all WAN and VoIP services are affected. Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads.

Which of the following BEST describe this type of attack? (Select TWO)

A. DoS

B. SSL stripping

C. Memory leak

D. Race condition

E. Shimming

F. Refactoring

Answer: AD

Which of the following is a team of people dedicated to testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

A. Red team

B. White team

C. Blue team

D. Purple team

Answer: A Explanation:

It is work for red team

A forensics analysis 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.

Answer: A

Explanation:

Hash is needed to provide integrity of data

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

Answer: D Explanation:

Backup is not older than 60 minutes

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 file and return the device to the user.

D. Wipe and reimage the device.

Answer: A Explanation:

First of all, analyst should be sure that he is doing it legally

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

Answer: A

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 company does not support DNSSEC.

D. The HTTP response is susceptible to sniffing.

Answer: D

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

Answer: C Explanation:

The application can return the error in fuzzing stage

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. Blackbox

B. Gray box

C. White box

D. Red team

E. Blue team

Answer: C Explanation:

It is white box

A security analysis 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 the scene, 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

Answer: A Explanation: All that parts are contained in .pfx

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 system has the attacker compromised?

A. DMZ

B. RTOS

C. SCADA

D. IoT

Answer: C Explanation:

It is Supervisory Control And Data Acquisition system

Which of the following is used to encrypt web application data?

A. MD5

B. AES

C. SHA

D. DHA

Answer: B Explanation:

AES is used for TLS tunnel

Joe, a user reports to the help desk that he can no longer access any documents on this PC. He states that he saw a window appear on the screen earlier but he closed it without reading it. Upon the investigation, the technician sees high disk activity on Joe's PC. Which of the following types of malware MOST likely indicated by these findings?

A. Keylogger

B. Trojan

C. Rootkit

D. Crypto-malware

Answer: D Explanation:

It is typical crypto-malware behavior

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

Answer: A Explanation:

It is strong algorithm and it is reversible

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

Answer: B Explanation:

It helps find improper input handling

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

Answer: D Explanation:

Containerization will keep al sensitive data in separate part of device

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.

Answer: E