Exam Topic Breakdown

Exam Topic	Number of Questions
Topic 1 : Exam Set 1	180
Topic 2 : Exam Set 2	182
Topic 3 : Exam Set 3	111
Topic 4 : Exam Set 4	75
TOTAL	548

Topic 3, Exam Set 3

Question #:1 - (Exam Topic 3)

A web server has been compromised due to a ransomware attack. Further investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

A. The last incremental backup that was conducted 72 hours ago

B. The last known-good configuration stored by the operating system

C. The last full backup that was conducted seven days ago

D. The baseline OS configuration

Answer: A

Explanation

The last incremental backup that was conducted 72 hours ago would be the best option to restore the services to a secure state, as it would contain the most recent data before the ransomware infection. Incremental backups only store the changes made since the last backup, so they are faster and use less storage space than full backups. Restoring from an incremental backup would also minimize the data loss and downtime caused by the ransomware attack. References:

https://www.comptia.org/blog/mature-cybersecurity-response-to-ransomware

https://www.youtube.com/watch?v=HszU4nEAlFc

Question #:2 - (Exam Topic 3)

A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

A. User training

B. CASB

C. MDM

D. EDR

Answer: B

Explanation

The CASB serves as a policy enforcement center, consolidating multiple security policy enforcement functions and applying them to everything your business uses in the cloud—regardless of the kind of device attempting to access it, including unmanaged smartphones and personal laptops.

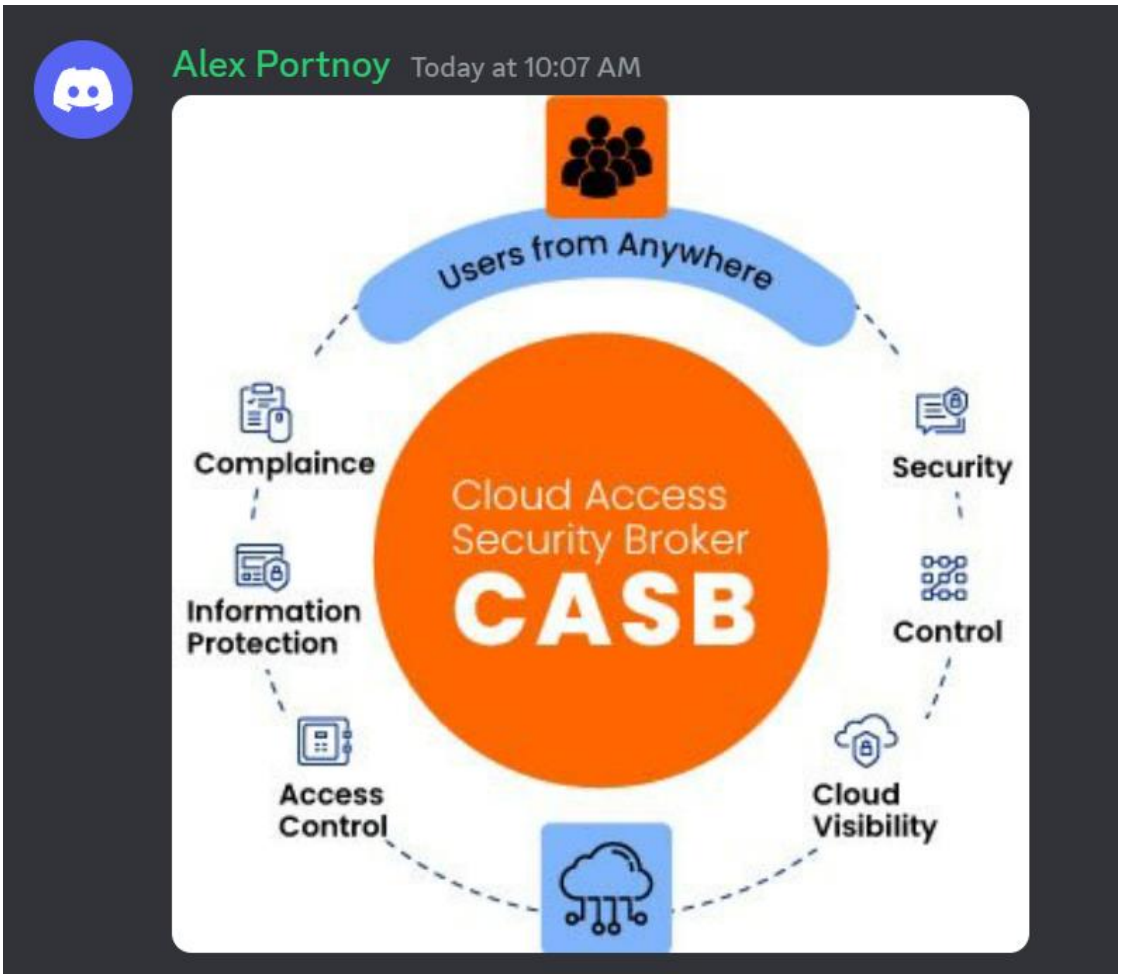
The company took special precautions by using proper labels for data. If you set such a CASB policy that restricts uploading those data that was labeled as sensitive, one cannot upload it to the cloud storage.

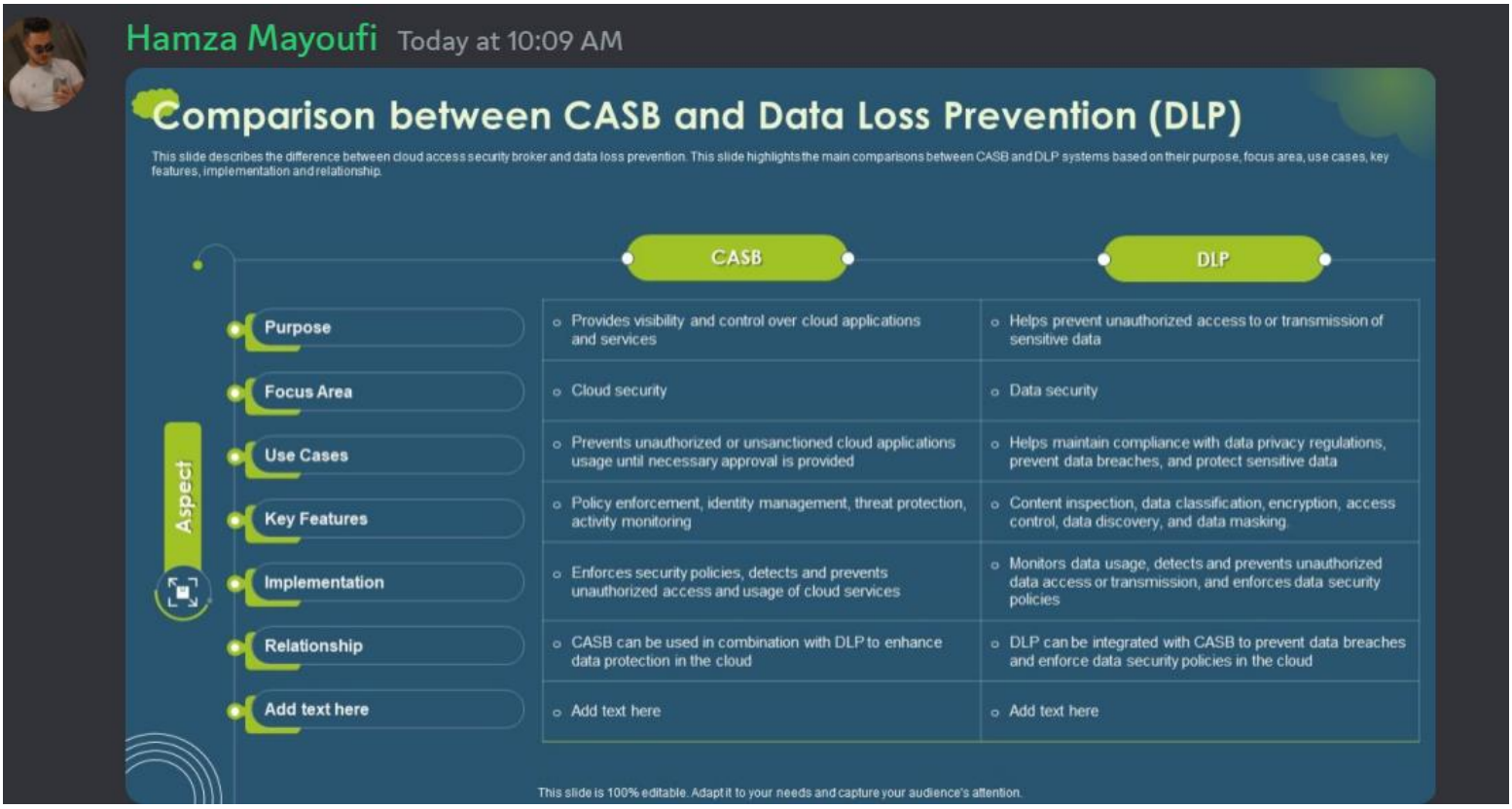
measures such as containerization or encryption. References:

https://www.blackberry.com/us/en/solutions/corporate-owned-personally-enabled

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mobile-device-management/

User training is essential for creating awareness and educating employees about security best practices. However, it may not be sufficient on its own to prevent sophisticated data breaches involving cloud storage.





Question #:3 - (Exam Topic 3)

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).

A. Application

B. Authentication

C. Error

D. Network

E. Firewall

F. System

Answer: D E

Explanation

Network and firewall logs should be analyzed to identify the impacted host in a cybersecurity incident involving a command-and-control server. A command-and-control server is a central server that communicates with and controls malware-infected devices or bots. A command-and-control server can send commands to the bots, such as downloading additional malware, stealing data, or launching attacks. Network logs can help to identify any suspicious or anomalous network traffic, such as connections to unknown or malicious domains, high-volume data transfers, or unusual protocols or ports. Firewall logs can help to identify any blocked or allowed traffic based on the firewall rules, such as connections to or from the command-and-control server, or any attempts to bypass the firewall. References:

https://cybersecurity.att.com/blogs/security-essentials/command-and-control-server-detection-methods-be

https://www.howtogeek.com/726136/what-is-a-command-and-control-server-for-malware/

While other types of logs, such as system logs and application logs, may contain valuable information about the incident, they may not provide direct evidence of communication with a C2 server.

Authentication logs, for instance, are more focused on user access and authentication activities and may not be the primary source for identifying C2 server communications.

Error logs and application logs may contain information about anomalies or suspicious activities, but they may not directly point to the C2 server's communication.

Question #:4 - (Exam Topic 3)

Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report

B. A risk register

C. A business impact analysis

D. An asset value register

E. A disaster recovery plan

Answer: B

Explanation

A risk register is a document or a tool that records and tracks information about the identified risks and their analysis, such as likelihood, impact, priority, mitigation strategies, residual risks, etc. It can contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented.

An RTO (Recovery Time Objective) report typically focuses on the time it takes to recover from a specific disaster or incident, not on ranking and ordering various types of risks.

A Business Impact Analysis (BIA) assesses the impact of various risks on business processes and systems but may not provide the same level of detail in terms of ranking and ordering risks.

An Asset Value Register typically contains information about the value of an organization's assets, which is important for risk assessment but doesn't provide the detailed information on risk likelihood, potential impact, and residual risks.

A Disaster Recovery Plan outlines the steps and procedures to follow in the event of a disaster or incident, including recovery strategies, but it does not necessarily contain the same comprehensive information about risk likelihood, impact, and controls as a Risk Register.

Risk Matrix		Severity				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	Very High	Very High	Very High
	Likely	Medium	High	High	Very High	Very High
	Possible	Low	Medium	High	High	Very High
	Unlikelyh	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

Petra Martina Vrancic — Today at 10:12 AM

A risk register is a document that systematically identifies, assesses, and prioritizes risks to a business. It typically includes information on the likelihood and potential impact of various risks, as well as the effectiveness of existing controls. Residual risks, which are the risks that remain after controls are implemented, are also commonly addressed in a risk register.

Question #:5 - (Exam Topic 3)

During an assessment, a systems administrator found several hosts running FTP and decided to immediately block FTP communications at the firewall. Which of the following describes the greatest risk associated with using FTP?

A. Private data can be leaked

B. FTP is prohibited by internal policy.

C. Users can upload personal files

D. Credentials are sent in cleartext.

Answer: D

Explanation

Credentials are sent in cleartext is the greatest risk associated with using FTP. FTP is an old protocol that does not encrypt the data or the credentials that are transmitted over the network. This means that anyone who can capture the network traffic can see the usernames and passwords of the FTP users, as well as the files they are transferring. This can lead to data breaches, identity theft, and unauthorized access. Private data can be leaked (Option A) is a possible consequence of using FTP, but not the root cause of the risk. FTP is prohibited by internal policy (Option B) is a compliance issue, but not a technical risk. Users can upload personal files (Option C) is a management issue, but not a security risk

https://www.infosectrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/

Petra Martina Vrancic — Today at 10:13 AM

lack of encryption means that sensitive credentials can be easily captured if the communication is not secured by additional means, like using FTPS (FTP Secure) or SFTP (SSH File Transfer Protocol).

Question #:6 - (Exam Topic 3)

Which of the following security concepts should an e-commerce organization apply for protection against erroneous purchases?

A. Privacy

B. Availability

C. Integrity

D. Confidentiality

Answer: C

Explanation

Integrity is a security concept that ensures that data is accurate, complete and consistent, and that it has not been tampered with or modified in an unauthorized or unintended way. Integrity is important for e-commerce organizations to protect against erroneous purchases, as it can prevent data corruption, duplication, loss or manipulation that could affect the transactions or the records of the customers. Integrity can be achieved by using methods such as hashing, digital signatures, checksums, encryption and access control. Verified References:

Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See What Skills Will You Learn?)

CompTIA Security+ 601 - Infosec https://www.infosecinstitute.com/wp-content/uploads/2021/03/CompTIA-Security-eBook.pdf (See Security+: 5 in-demand cybersecurity skills)

CompTIA Security+ SY0-601 Certification Study Guide https://www.comptia.org/training/books/security-sy0-601-study-guide (See Chapter 1: Threats, Attacks and Vulnerabilities, Section 1.4: Cryptography and PKI)

Availability relates to ensuring that the e-commerce platform is accessible and operational, but it doesn't directly address the prevention of erroneous purchases.

Privacy and Confidentiality are more focused on protecting sensitive customer information and data privacy. While these concepts are important for overall security, they are not specifically targeted at preventing erroneous purchases.

Nita Arapi — Today at 10:14 AM

Integrity data not modified

David Berrios — Today at 10:15 AM

proetction buy somethign intergirty that secure - data normal comes standerde

Petra Martina Vrancic — Today at 10:15 AM

Confidentiality is about protecting sensitive information from unauthorized access. While important, it may not be the primary

focus when dealing with preventing erroneous purchases.

volkan — Today at 10:15 AM

customers can be sur

Question #:7 - (Exam Topic 3)

A security professional wants to enhance the protection of a critical environment that is used to store and manage a company's encryption keys. The selected technology should be tamper resistant. Which of the following should the security professional implement to achieve the goal?

A. DLP

B. HSM

C. CA

D. FIM

Answer: B

Explanation

HSM stands for hardware security module, which is a physical device that is used to store and manage cryptographic keys in a secure and tamper-resistant manner. HSMs can provide high-performance encryption and decryption operations, as well as key generation, backup, and recovery. HSMs can also prevent unauthorized access or extraction of the keys, even by the cloud service provider or the HSM vendor. HSMs can enhance the protection of a critical environment that is used to store and manage encryption keys for a financial institution or any other organization that deals with sensitive data. References:

https://www.comptia.org/certifications/security

https://www.professormesser.com/security-plus/sy0-501/hardware-security-3/

Data Loss Prevention (DLP): DLP solutions focus on preventing data leakage and do not directly address the protection of encryption keys or the tamper resistance of key storage.

Certificate Authority (CA): CAs are used for issuing and managing digital certificates, which play a role in authentication and encryption, but they do not provide the physical security and tamper resistance needed to protect encryption keys.

File Integrity Monitoring (FIM): FIM tools are designed to monitor and detect changes to files and systems, ensuring their integrity. While important for security, FIM is not directly related to the specific goal of tamper-resistant protection of encryption keys.

David Berrios — Today at 10:16 AM

HSMs (Hardware Security Modules) are specifically designed to safeguard encryption keys and provide a high level of tamper resistance. They are physical devices that securely manage digital keys and perform cryptographic operations. HSMs ensure the confidentiality and integrity of sensitive data and cryptographic keys by storing them in a secure hardware environment, protecting them from

unauthorized access and tampering.

Question #:8 - (Exam Topic 3)

A security analyst discovers that one of the web APIs is being abused by an unknown third party. Logs indicate that the third party is attempting to manipulate the parameters being passed to the API endpoint. Which of the following solutions would best help to protect against the attack?

A. DLP

B. SIEM

C. NIDS

D. WAF

Answer: D

Explanation

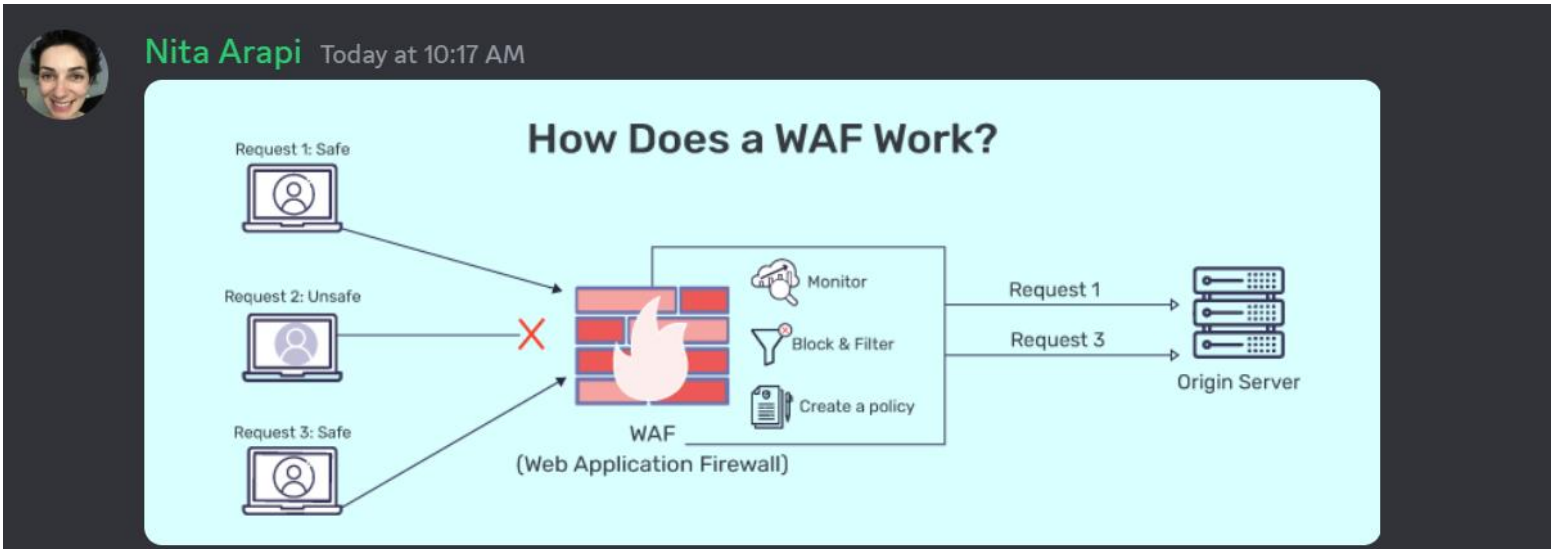
WAF stands for Web Application Firewall, which is a type of firewall that can monitor, filter and block web traffic to and from web applications. WAF can protect web applications from common attacks such as cross-site scripting (XSS), SQL injection, directory traversal, buffer overflow and more. WAF can also enforce security policies and rules that can prevent parameter manipulation or tampering by an unknown third party. WAF is the best solution to help protect against the attack on the web API, as it can inspect the HTTP requests and responses and block

any malicious or anomalous activity. Verified References:

Other Application Attacks – SY0-601 CompTIA Security+ : 1.3 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/other-application-attacks/ (See Web Application Firewall)

CompTIA Security+ SY0-601 Exam Cram
https://www.oreilly.com/library/view/comptia-security-sy0-601/9780136798767/ch03.xhtml (See Web Application Firewall)

Security+ domain #1: Attacks, threats, and vulnerabilities [updated 2021]
https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/ (See Web application firewall)



Question #:9 - (Exam Topic 3)

Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally?

A. Provisioning resources

B. Disabling access

C. APIs

D. Escalating permission requests

Answer: B

Explanation

Disabling access is an automation use case that can enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally. It can prevent unauthorized access and data leakage by revoking or modifying the access rights of employees based on their current status and role.

While provisioning resources and escalating permission requests are also important automation use cases, they are not as directly focused on enhancing security by promptly revoking access when it is no longer needed. APIs are a technology used to enable automation but are not a use case in themselves.

Question #:10 - (Exam Topic 3)

A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access points are up and running. One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

A. Someone near the building is jamming the signal

B. A user has set up a rogue access point near the building

C. Someone set up an evil twin access point in the affected area.

D. The APs in the affected area have been unplugged from the network

Answer: A

Explanation

Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

Wireless jamming is a way for an attacker to disrupt a wireless network and create a denial of ser-vice situation by decreasing the signal-to-noise ratio at the receiving device. The attacker would need to be relatively close to the wireless network to overwhelm the good signal. The other options are not likely to cause a wireless network outage for users near the parking lot.

Question #:11 - (Exam Topic 3)

Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical

Answer: A

Explanation

A turnstile is a physical security control that regulates the entry and exit of people into a facility or an area. It can prevent unauthorized access, tailgating, etc., by requiring valid credentials or tokens to pass through

Question #:12 - (Exam Topic 3)

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following best describes these systems?

A. DNS sinkholes

B. Honey pots

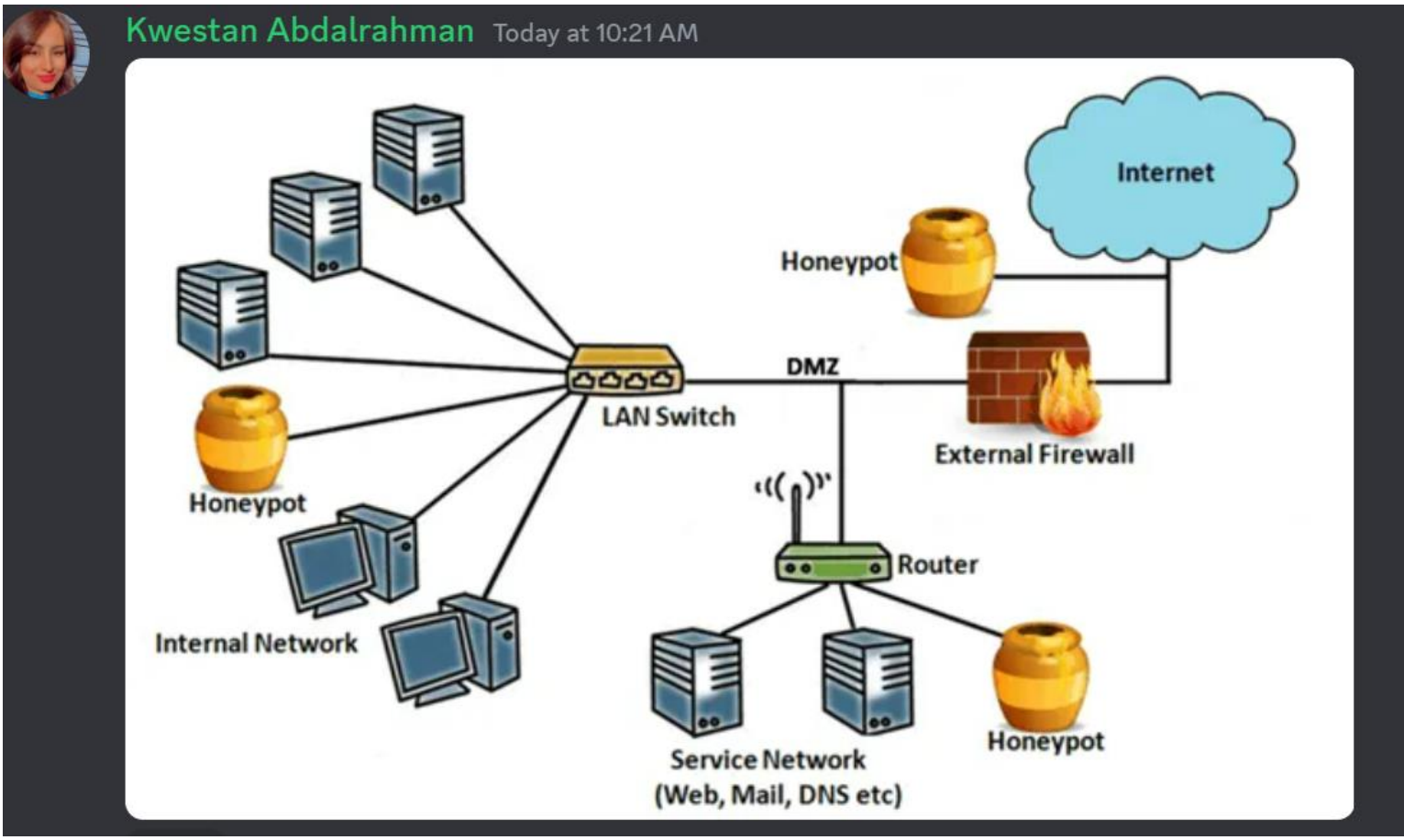
C. Virtual machines

D. Neural networks

Answer: B

Explanation

Honey pots are decoy systems or resources that are designed to attract and deceive threat actors and to learn more about their motives, techniques, etc. They can be deployed alongside production systems to create an illusion of a vulnerable target and divert attacks away from the real systems. They can also collect valuable information and evidence about the attackers and their activities for further analysis or prosecution.



Question #:13 - (Exam Topic 3)

A security analyst is hardening a network infrastructure. The analyst is given the following requirements:

• Preserve the use of public IP addresses assigned to equipment on the core router

• Enable "in transport" encryption protection to the web server with the strongest ciphers.

Which of the following should the analyst implement to meet these requirements? (Select two).

A. Configure VLANs on the core router

B. Configure NAT on the core router. //// Preserve the use of public IP addresses

C. Configure BGP on the core router

D. Enable AES encryption on the web server

E. Enable 3DES encryption on the web server

F. Enable TLSv2 encryption on the web server ///// "in transport" encryption protection

Answer: B F

Explanation

NAT (Network Address Translation) is a technique that allows a router to translate private IP addresses into public IP addresses and vice versa. It can preserve the use of public IP addresses assigned to equipment on the core router by allowing multiple devices to share a single public IP address. TLSv2 (Transport Layer Security version 2) is a cryptographic protocol that provides secure communication over the internet. It can enable “in transport” encryption protection to the web server with the strongest ciphers by encrypting the data transmitted between the web server and the clients using advanced algorithms and key exchange methods.

Question #:14 - (Exam Topic 3)

An organization is repairing damage after an incident. Which of the following controls is being implemented?

A. Detective

B. Preventive

C. Corrective

D. Compensating

Answer: C

Explanation

Corrective controls are security measures that are implemented after an incident to repair the damage and restore normal operations. They can include actions such as patching systems, restoring backups, removing malware, etc. An organization that is repairing damage after an incident is implementing corrective controls.

A corrective control is a type of security control that is designed to mitigate the damage caused by a security incident or to restore the normal operations after an incident. A corrective control can include actions such as restoring from backups, applying patches, isolating infected systems, or implementing new policies and procedures. A corrective control is different from a preventive control, which aims to stop an incident from happening, or a detective control, which aims to identify and record an incident. References:

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/security-controls-3/
https://www.oreilly.com/library/view/comptia-security-all-in-one/9781260464016/ch31.xhtml
https://www.professormesser.com/security-plus/sy0-501/security-controls-2/

Question #:15 - (Exam Topic 3)

Which of the following best ensures minimal downtime for organizations critical computing equipment located in earthquake-prone areas?

A. Generators and UPS

B. Off-site replication

C. Additional warm site

D. Local

Answer: B

Explanation

Off-site replication is a process of copying and storing data in a remote location that is geographically separate from the primary site. It can ensure minimal downtime for organizations with critical computing equipment located in earthquake-prone areas by providing a backup copy of data that can be accessed and restored in case of a disaster or disruption at the primary site.

Question #:16 - (Exam Topic 3)

An organization is building a new headquarters and has placed fake cameras around the building in an attempt to discourage potential intruders. Which of the following kinds of controls describes this security method?

A. Detective

B. Deterrent

C. Directive

D. Corrective

Answer: B

Explanation

A deterrent control is a type of security control that is designed to discourage potential intruders from attempting to access or harm a system or network. A deterrent control relies on the perception or fear of negative consequences rather than the actual enforcement of those consequences. A deterrent control can also be used to influence the behavior of authorized users by reminding them of their obligations and responsibilities. An example of a deterrent control is placing fake cameras around the building, as it can create the illusion of surveillance and deter potential intruders from trying to break in. Other examples of deterrent controls are warning signs, security guards, or audit trails. References:

https://www.ibm.com/topics/security-controls

https://www.f5.com/labs/learning-center/what-are-security-controls

Question #:17 - (Exam Topic 3)

Which of the following roles is responsible for defining the protection type and classification type for a given set of files?

A. General counsel

B. Data owner

C. Risk manager

D. Chief Information Officer

Answer: B

Explanation

Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk

manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and operations of the organization

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/

General counsel may provide legal guidance and oversee compliance, but they typically don't define the technical details of data protection and classification.

Risk manager focuses on identifying and managing risks across the organization but may not be directly responsible for classifying and protecting individual files.

Chief Information Officer (CIO) is responsible for the overall IT strategy and management but may delegate data classification and protection responsibilities to data owners and data stewards within the organization.

Petra Martina Vrancic — Today at 10:27 AM

The data owner is typically responsible for defining the protection and classification types for a given set of files.

Question #:18 - (Exam Topic 3)

A technician is setting up a new firewall on a network segment to allow web traffic to the internet while hardening the network. After the firewall is configured, users receive errors stating the website could not be located. Which of the following would best correct the issue?

A. Setting an explicit deny to all traffic using port 80 instead of 443

B. Moving the implicit deny from the bottom of the rule set to the top

C. Configuring the first line in the rule set to allow all traffic

D. Ensuring that port 53 has been explicitly allowed in the rule set

Answer: D

Explanation

Port 53 is the default port for DNS traffic. If the firewall is blocking port 53, then users will not be able to resolve domain names and will receive errors stating that the website could not be located.

The other options would not correct the issue. Setting an explicit deny to all traffic using port 80 instead of 443 would block all HTTP traffic, not just web traffic. Moving the implicit deny from the bottom of the rule set to the top would make the deny rule more restrictive, which would not solve the issue. Configuring the first line in the rule set to allow all traffic would allow all traffic, including malicious traffic, which is not a good security practice.

Therefore, the best way to correct the issue is to ensure that port 53 has been explicitly allowed in the rule set. Here are some additional information about DNS traffic:

DNS traffic is used to resolve domain names to IP addresses.

DNS traffic is typically unencrypted, which makes it vulnerable to eavesdropping.

There are a number of ways to secure DNS traffic, such as using DNS over HTTPS (DoH) or DNS over TLS (DoT).

David Berrios — Today at 10:29 AM

port 53 is used for DNS (Domain Name System) resolution, which is necessary for translating domain names into IP addresses. If users are receiving errors stating that websites could not be located, it could indicate a DNS resolution problem. By ensuring that port 53 is explicitly allowed in the firewall rule set, DNS queries will be able to pass through the firewall, allowing users to resolve domain names and

Question #:19 - (Exam Topic 3)

Which of the following would be the best resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP

B. Vulnerability scan results

C. NIST CSF

D. Third-party libraries

Answer: A

Explanation

OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for improving the security of web applications. It can be the best resource for a software developer who is looking to improve secure coding practices for web applications by offering various tools, frameworks, standards, cheat sheets, testing guides, etc., that cover various aspects of web application security development and testing.

Question #:20 - (Exam Topic 3)

An organization has hired a security analyst to perform a penetration test. The analyst captures 1GB worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap

B. CURL

C. Neat

D. Wireshark

Answer: D

Explanation

Wireshark is a tool that can analyze pcap files, which are files that capture network traffic. Wireshark can display the packets, protocols, and other details of the network traffic in a graphical user interface. Nmap is a tool that can scan networks and hosts for open ports and services. CURL is a tool that can transfer data from or to a server using various protocols. Neat is a tool that can test network performance and quality.

Question #:21 - (Exam Topic 3)

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported. The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy

B. RAID 1+5

C. Virtual machines

D. Full backups

Answer: C

Explanation

Virtual machines are software-based simulations of physical computers that run on a host system and share its resources. They can provide resiliency for legacy information systems that cannot be migrated to a newer OS due to software compatibility issues by allowing OS patches to be installed in a non-production environment without affecting the production environment. They can also create backups of the systems for recovery by taking snapshots or copies of the virtual machine files.

Question #:22 - (Exam Topic 3)

Which of the following is a primary security concern for a company setting up a BYOD program?

A. End of life

B. Buffer overflow

C. VM escape

D. Jailbreaking

Answer: D

Explanation

Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device's operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc.

David Berrios — Today at 10:36 AM

Jailbreaking refers to the process of removing software restrictions imposed on devices, allowing users to gain access to additional features and apps that are not available through the device's official app store. In a BYOD (Bring Your Own Device) program, where employees use their personal devices for work purposes, jailbreaking poses a significant security concern. Jailbroken devices are more vulnerable to malware, unauthorized software installations, and other security threats because they bypass the built-in security mechanisms. Companies need to implement policies and security measures to prevent employees from jailbreaking their devices to maintain a secure BYOD environment.

Question #:23 - (Exam Topic 3)

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

A. The business continuity plan

B. The risk management plan

C. The communication plan

D. The incident response plan

Answer: A

Explanation

A business continuity plan is a document or a process that outlines how an organization can continue its critical operations and functions in the event of a disruption or disaster. It can include strategies and procedures for recovering or relocating resources, personnel, data, etc., to ensure minimal downtime and impact. The organization will most likely consult the business continuity plan when setting up offices in a temporary work space after its corporate offices were destroyed due to a natural disaster.

Risk Management Plan: This plan typically outlines how an organization identifies, assesses, and mitigates risks. While risk management is an important component of disaster preparedness, it may not provide the specific strategies for maintaining business operations in a temporary workspace.

Communication Plan: Communication plans are vital during disasters for keeping stakeholders informed, but they are generally a subset of the broader BCP.

Incident Response Plan: An incident response plan is more focused on immediate actions to address a specific security incident or disaster when it occurs. While it may include aspects of recovery and continuity, its primary focus is on responding to the incident as it unfolds.

Question #:24 - (Exam Topic 3)

A company has installed badge readers for building access but is finding unauthorized individuals roaming the hallways. Which of the following is the most likely cause?

A. Shoulder surfing

B. Phishing

C. Tailgating

D. Identity fraud

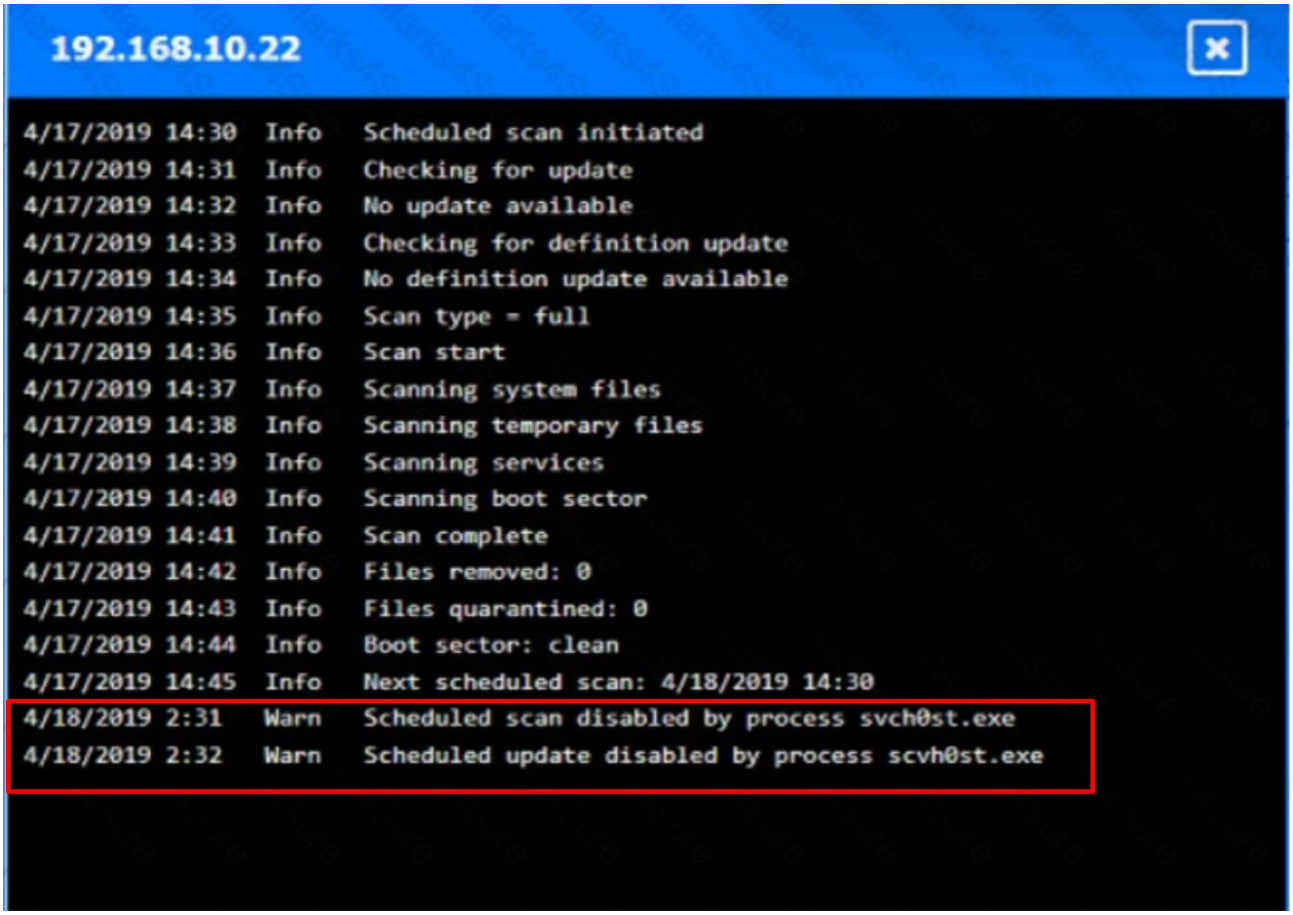
Answer: C

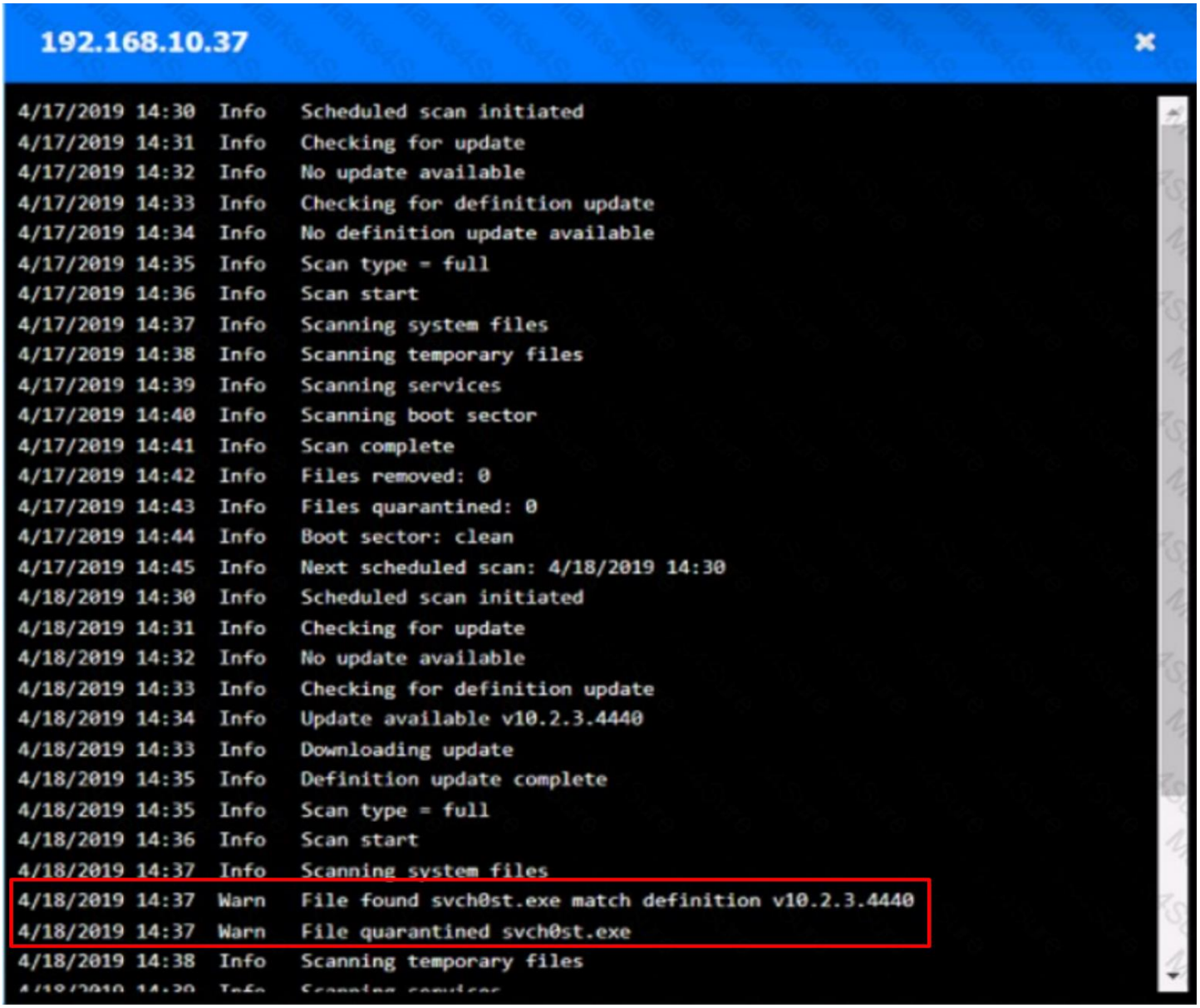
Explanation

Tailgating is a physical security threat that occurs when an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. It can cause unauthorized individuals to roam the hallways after gaining access through badge readers installed for building access.

Question #:25 - (Exam Topic 3)

You are security administrator investigating a potential infection on a network.
Click on each host and firewall. Review all logs to determine which host originated the infection and then deny each remaining hosts clean or infected.


192.168.10.22
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31 Warn Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32 Warn Scheduled update disabled by process scvh0st.exe

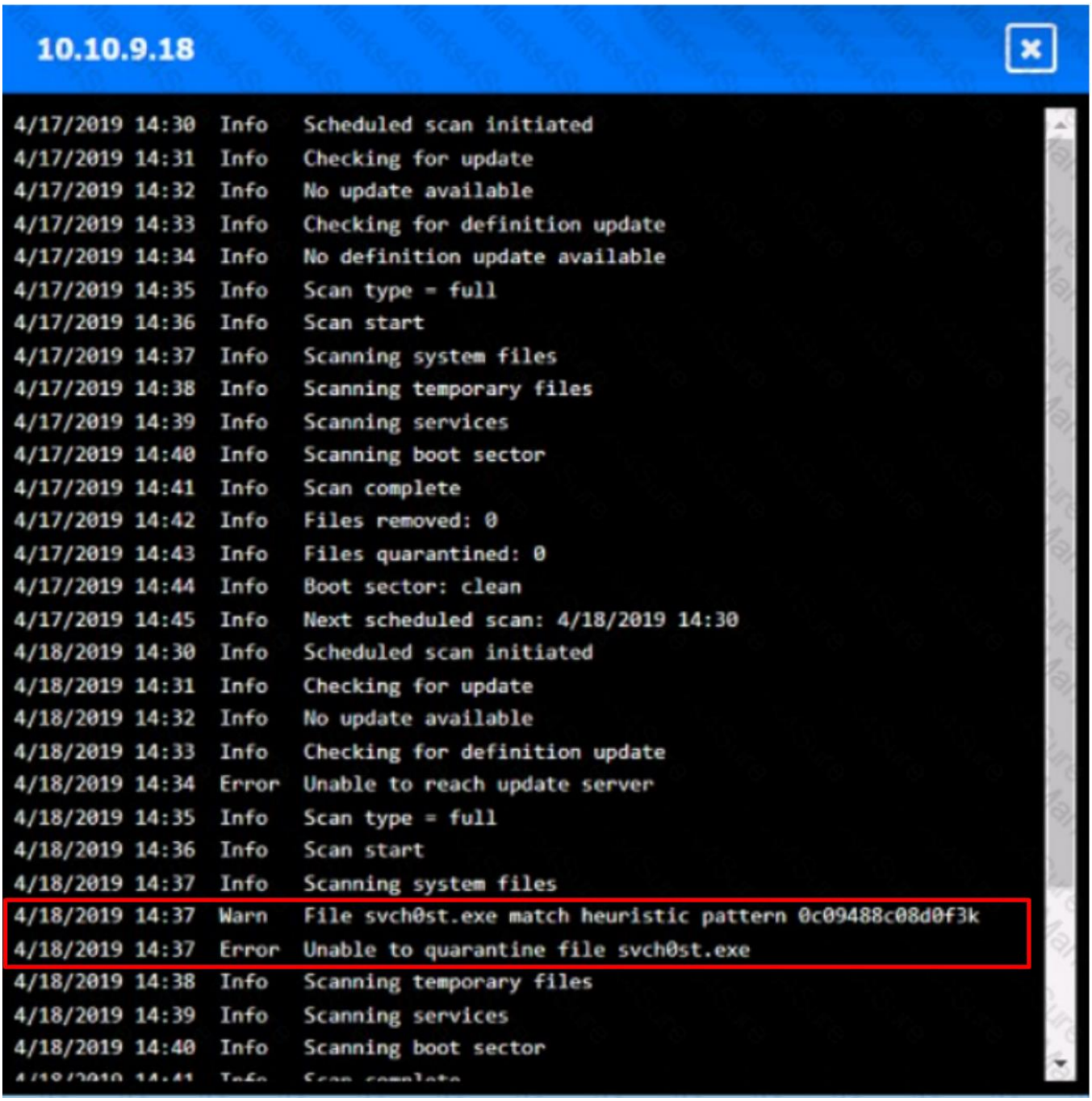

192.168.10.37
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files

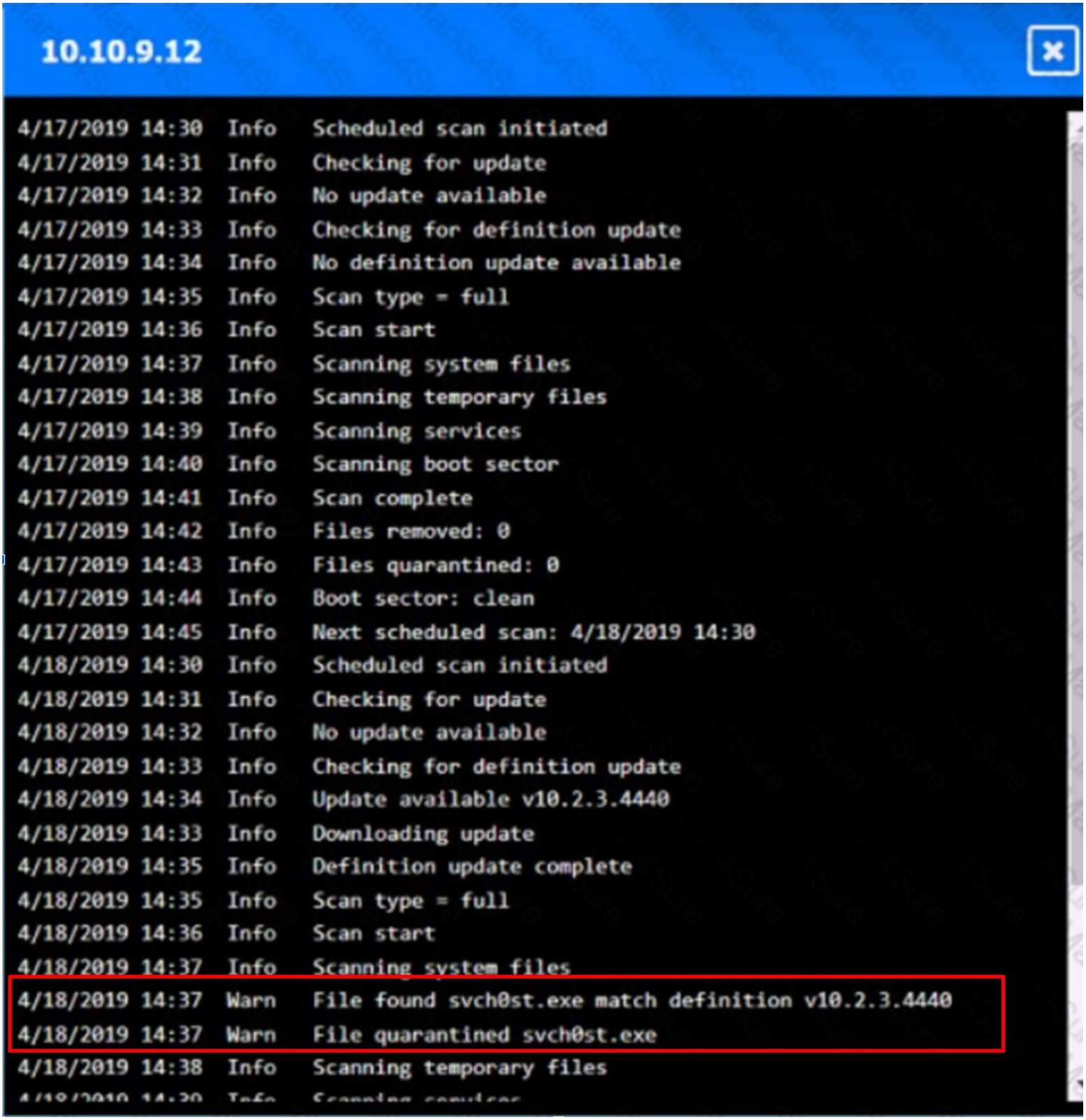
192.168.10.41

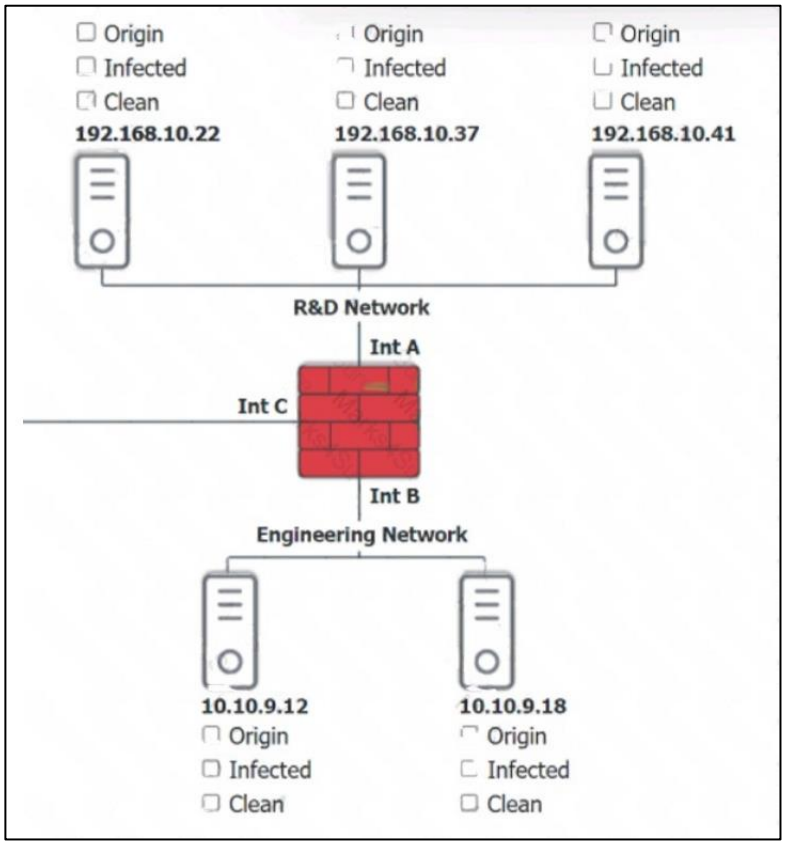
```
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

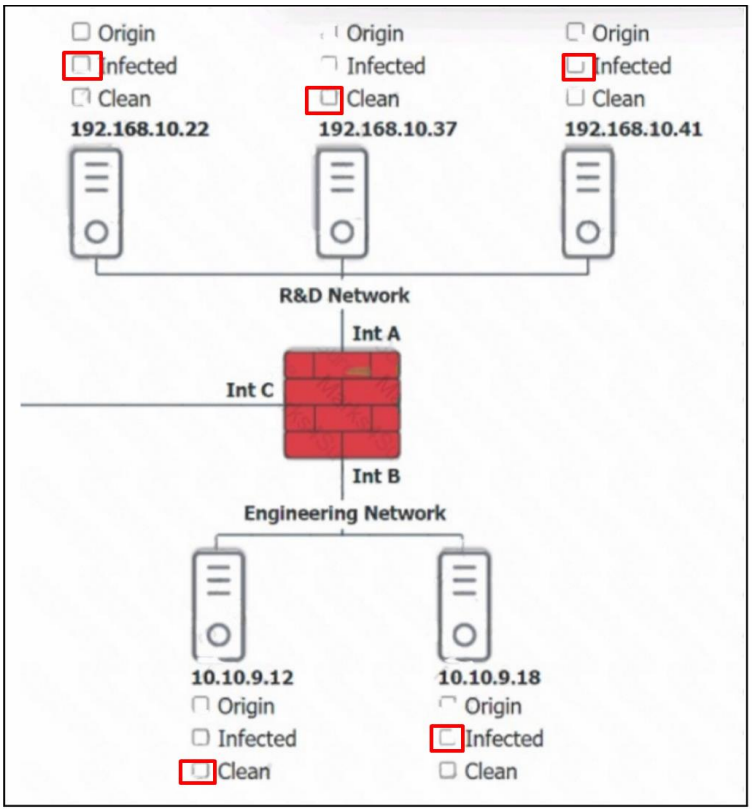
Firewall

Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938


10.10.9.18
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector


10.10.9.12
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files





Answer:

Explanation

Based on the logs, it seems that the host that originated the infection is **192.168.10.22**. This host has a suspicious

process named **svchost.exe** running on port 443, which is unusual for a Windows service. It also has a large number of outbound connections to different IP addresses on port 443, indicating that it is part of a botnet.

The firewall log shows that this host has been communicating with **10.10.9.18**, which is another infected host on the engineering network. This host also has a suspicious process named **svchost.exe** running on port 443, and a large number of outbound connections to different IP addresses on port 443.

The other hosts on the R&D network (**192.168.10.37**) are clean, as they do not have any suspicious processes or connections.

Question #:26 - (Exam Topic 3)

A systems administrator is required to enforce MFA for corporate email account access, relying on the possession factor. Which of the following authentication methods should the systems administrator choose? (Select two).

A. passphrase

B. Time-based one-time password

C. Facial recognition

D. Retina scan

E. Hardware token

F. Fingerprints

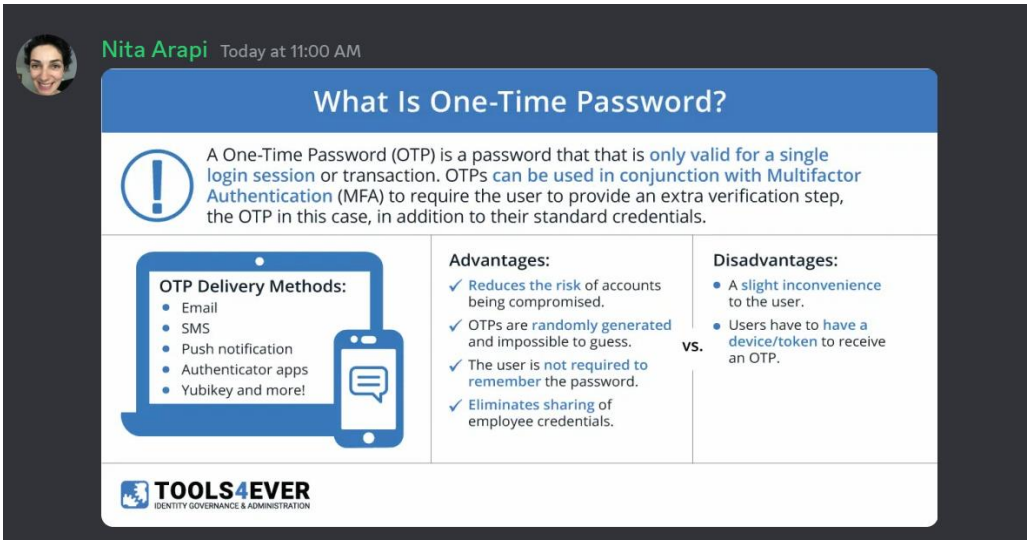
Answer: B E

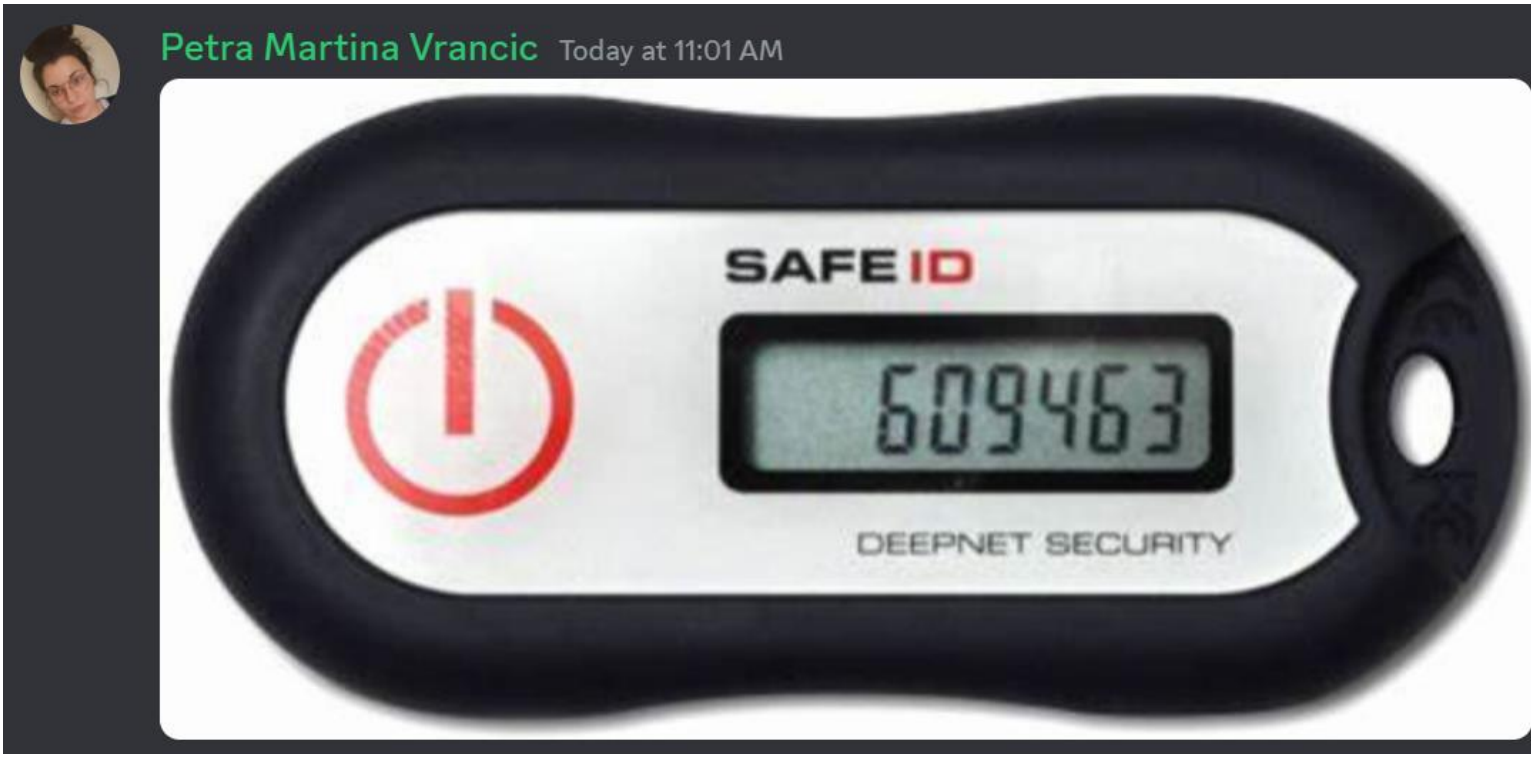
Explanation

Time-based one-time password (TOTP) and hardware token are authentication methods that rely on the possession factor, which means that the user must have a specific device or object in their possession to authenticate. A TOTP is a password that is valid for a short period of time and is generated by an app or a device that the user has. A hardware token is a physical device that displays a code or a password that the user can enter to authenticate. A passphrase (Option A) is a knowledge factor, while facial recognition (Option C), retina scan (Option D), and fingerprints (Option F) are all inherence factors.

https://ptgmedia.pearsoncmg.com/imprint_downloads/pearsonitcertification/bookreg/9780136798675/97801367

https://www.youtube.com/watch?v=yCJyPPvM-xg





Question #:27 - (Exam Topic 3)

An annual information security has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be best to use to update and reconfigure the OS-level security configurations?

A. CIS benchmarks

B. GDPR guidance

C. Regional regulations

D. ISO 27001 standards

Answer: A

Explanation

CIS benchmarks are best practices and standards for securing various operating systems, applications, cloud environments, etc. They are developed by a community of experts and updated regularly to reflect the latest threats and vulnerabilities. They can be used to update and reconfigure the OS-level security configurations to ensure compliance and reduce risks.

GDPR (General Data Protection Regulation) is a data protection regulation that focuses on the privacy of personal data. While GDPR is essential for data privacy compliance, it does not provide detailed guidance on configuring operating systems or hardening security settings.

Regional regulations may cover specific legal and compliance requirements for data protection, but they typically do not provide the level of technical detail needed to update OS-level security configurations.

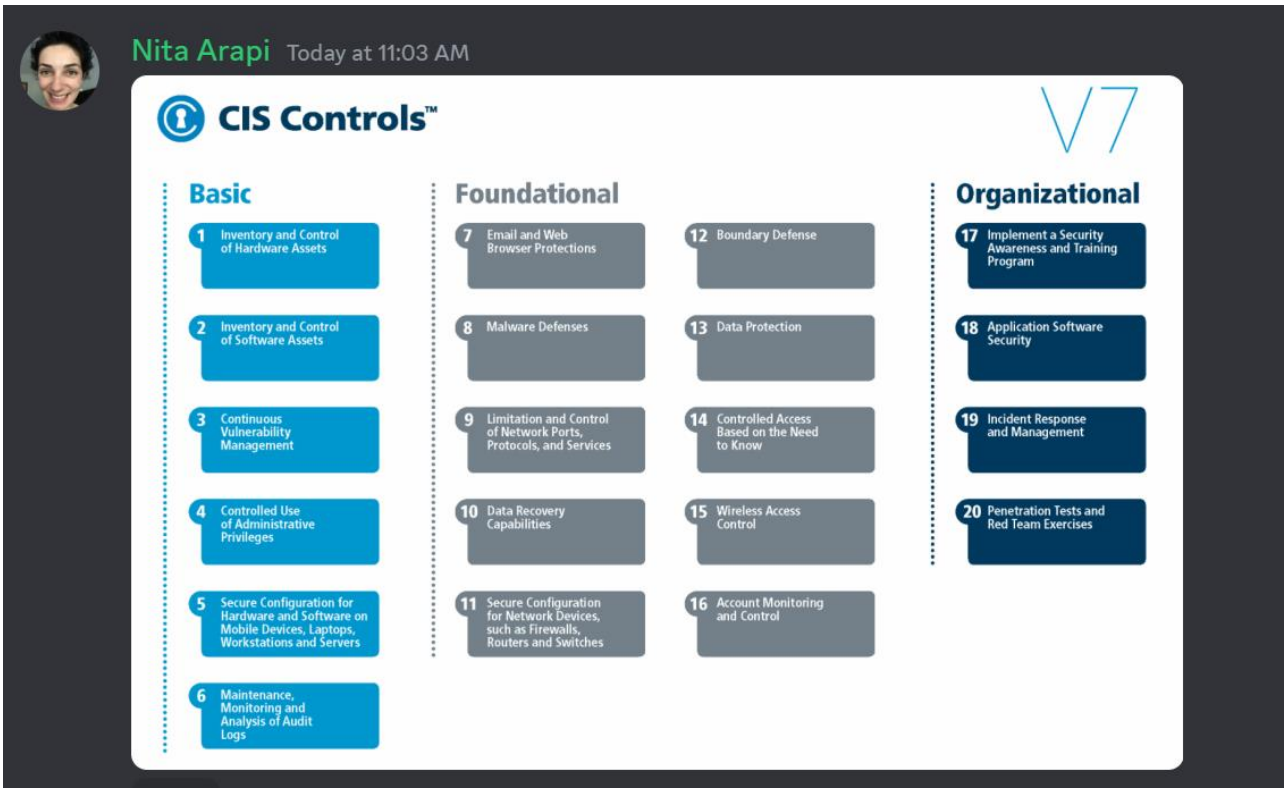
ISO 27001 is an international standard for information security management systems (ISMS). While it provides a framework for establishing and maintaining an ISMS, it does not offer the specific configuration guidance needed to update OS-level settings.

Oytun Azkanar

—

Today at 11:02 AM

CIS benchmarks refer to a set of best practice guidelines and recommendations developed by the Center for Internet Security (CIS) for enhancing the security of computer systems and networks. CIS is a nonprofit organization that focuses on improving the cybersecurity posture of both public and private sector organizations.



Question #:28 - (Exam Topic 3)

Which of the following supplies non-repudiation during a forensics investigation?

A. Dumping volatile memory contents first

B. Duplicating a drive with dd

C. Using a SHA-2 signature of a drive image

D. Logging everyone in contact with evidence

E. Encrypting sensitive data

Answer: C

Explanation

A SHA 2 signature is a cryptographic hash function that produces a unique and fixed-length output for any given input. It can provide non-repudiation during a forensics investigation by verifying the integrity and authenticity of a drive image and proving that it has not been altered or tampered with since it was created

Using a SHA-2 signature of a drive image is a way to supply non-repudiation during a forensics investigation, as it can verify the integrity and authenticity of the data captured in the image. SHA-2 is a family of secure hash algorithms that can produce a unique and fixed-length digest of any input data. By hashing the drive image and comparing the signature with the original hash, the investigator can prove that the image has not been altered or tampered with since the time of acquisition. This can also help to identify the source of the data and prevent any denial from the suspect. References:

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/managing-evidence/

https://www.skillsoft.com/course/comptia-security-incident-response-digital-forensics-supporting-investig

While other methods mentioned, such as duplicating a drive with dd, logging everyone in contact with evidence, and encrypting sensitive data, are important forensic practices, they do not directly provide non-repudiation in the same way that a cryptographic hash signature does.

Petra Martina Vrancic — Today at 11:04 AM

helps establish the integrity of the evidence and prevents parties from denying their involvement in the investigation.

Question #:29 - (Exam Topic 3)

A company is auditing the manner in which its European customers' personal information is handled. Which of the following should the company consult?

A. GDPR

B. ISO

C. NIST

D. PCI DSS

Answer: A

Explanation

GDPR stands for General Data Protection Regulation, which is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR also applies to organizations outside the EU that offer goods or services to, or monitor the behavior of, EU data subjects. GDPR aims to protect the privacy and rights of EU citizens and residents regarding their personal data. GDPR defines personal data as any information relating to an identified or identifiable natural person, such as name, identification number, location data, online identifiers, or any factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. A company that is auditing the manner in which its European customers' personal information is handled should consult GDPR to ensure compliance with its rules and obligations. References:

https://www.gdpreu.org/the-regulation/key-concepts/personal-data/

https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regula

Question #:30 - (Exam Topic 3)

A company recently suffered a breach in which an attacker was able to access the internal mail servers and directly access several user inboxes. A large number of email messages were later posted online. Which of the following would best prevent email contents from being released should another breach occur?

A. Implement S/MIME to encrypt the emails at rest.

B. Enable full disk encryption on the mail servers.

C. Use digital certificates when accessing email via the web.

D. Configure web traffic to only use TLS-enabled channels.

Answer: A

Explanation

S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which is a standard for encrypting and digitally signing email messages. S/MIME can provide confidentiality, integrity, authentication and non-repudiation for email communications. S/MIME can encrypt the emails at rest, which means that the email contents are protected even if they are stored on the mail servers or the user inboxes. S/MIME can prevent email contents from being released should another breach occur, as the attacker would not be able to decrypt or read the encrypted emails without the proper keys or certificates. Verified References:

Cryptography Concepts – SY0-601 CompTIA Security+ : 2.8 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/cryptography-concepts-2/ (See S/MIME)

Mail Encryption - CompTIA Security+ All-in-One Exam Guide (Exam SY0-301) https://www.oreilly.com/library/view/comptia-security-all-in-one/9780071771474/sec5_chap14.html (See S/MIME)

Symmetric and Asymmetric Encryption – CompTIA Security+ SY0-501 – 6.1 https://www.professormesser.com/security-plus/sy0-501/symmetric-and-asymmetric-encryption/ (See S/MIME)

Question #:31 - (Exam Topic 3)

A company wants the ability to restrict web access and monitor the websites that employees visit. Which of the following would best meet these requirements?

A. Internet Proxy

B. VPN

C. WAF

D. Firewall

Answer: A

Explanation

An internet proxy is a server that acts as an intermediary between a client and a destination server on the internet. It can restrict web access and monitor the websites that employees visit by filtering the requests and responses based on predefined rules and policies, and logging the traffic and activities for auditing purposes

If the company's primary goal is to restrict web access and monitor the websites that employees visit, an Internet Proxy is the most suitable choice as it offers the necessary features and granularity for this purpose.

VPN (Virtual Private Network): VPNs are primarily used to establish secure and encrypted connections between remote users and corporate networks. While VPNs can be used to restrict access to some extent, their primary purpose is security and privacy, not web content filtering or monitoring.

WAF (Web Application Firewall): A Web Application Firewall is designed to protect web applications from various online threats, such as hacking attempts and DDoS attacks. It is not primarily used for restricting web access or monitoring website usage.

Firewall: Firewalls are network security devices that filter traffic based on predefined rules. While firewalls can be used to restrict access to certain websites, they are not as granular or specialized as internet proxies for web content filtering and monitoring.

Question #:32 - (Exam Topic 3)

An attack has occurred against a company.

INSTRUCTIONS

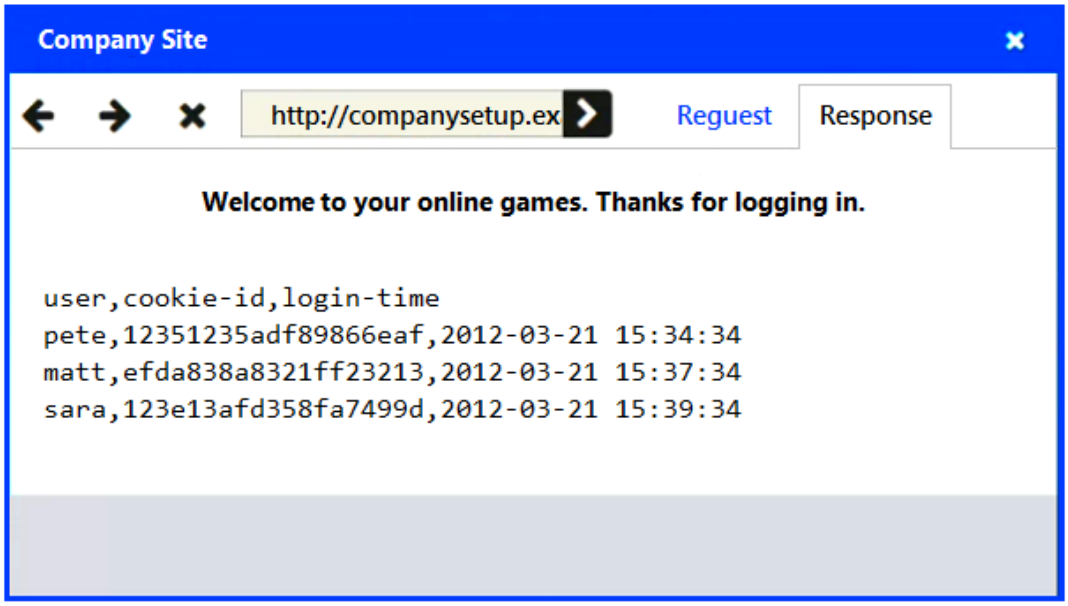
You have been tasked to do the following:

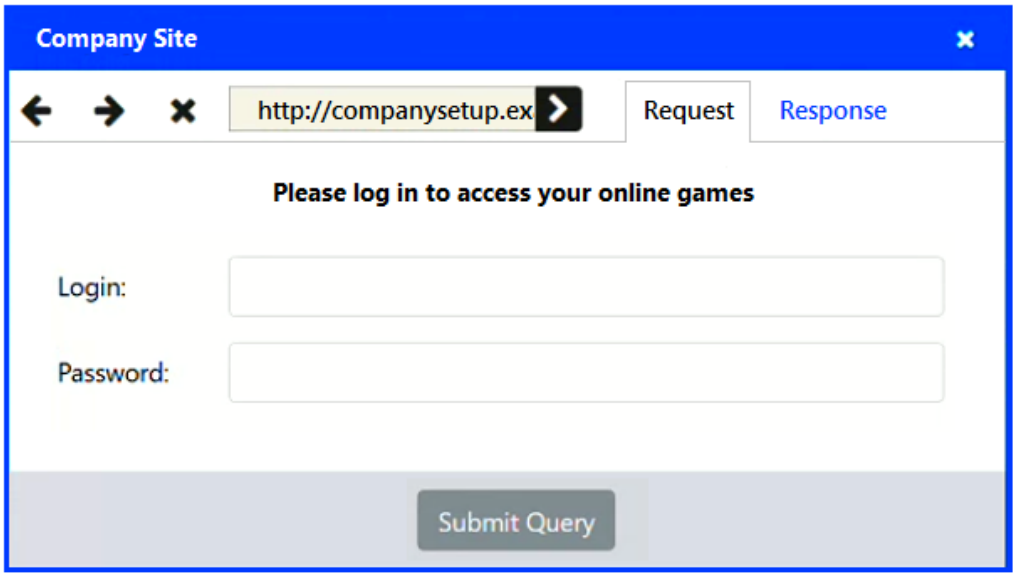
Identify the type of attack that is occurring on the network by clicking on the attacker’s tablet and reviewing the output. (Answer Area 1).

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.

(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

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


Company Site
http://companysetup.ex
Reguest
Response
Welcome to your online games. Thanks for logging in.
user,cookie-id,login-time
pete,12351235adf89866eaf,2012-03-21 15:34:34
matt,efda838a8321ff23213,2012-03-21 15:37:34
sara,123e13afd358fa7499d,2012-03-21 15:39:34


Company Site
http://companysetup.ex
Request
Response
Please log in to access your online games
Login:
Password:
Submit Query

Answer Area 1

SQL Injection

Cross Site Scripting

XML Injection

Session Hijacking

Type of attack

[?]

Answer Area 2

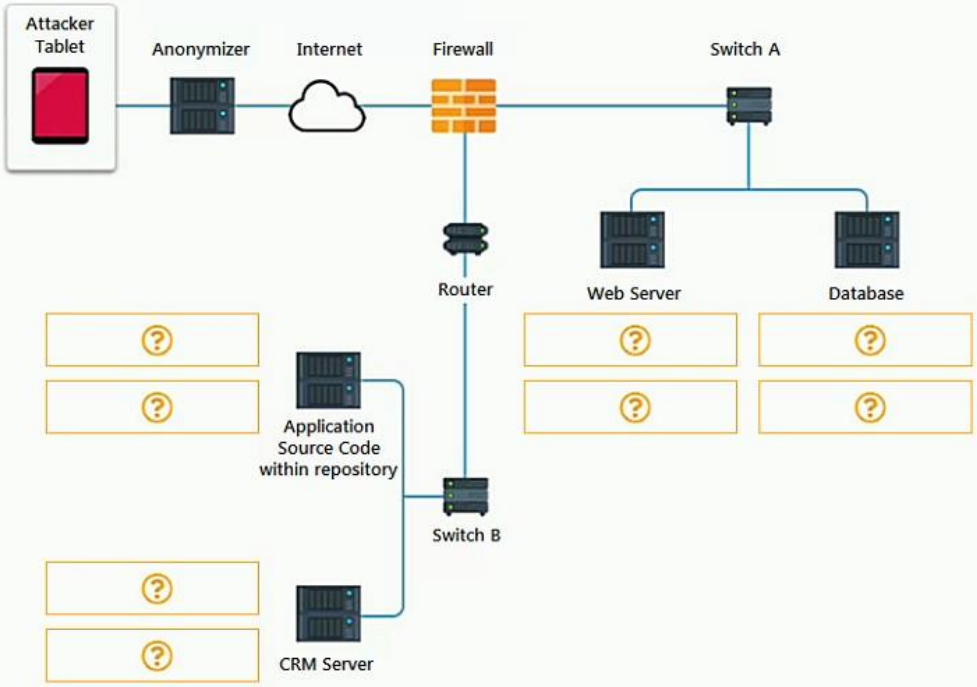
Input Validation

Code Review

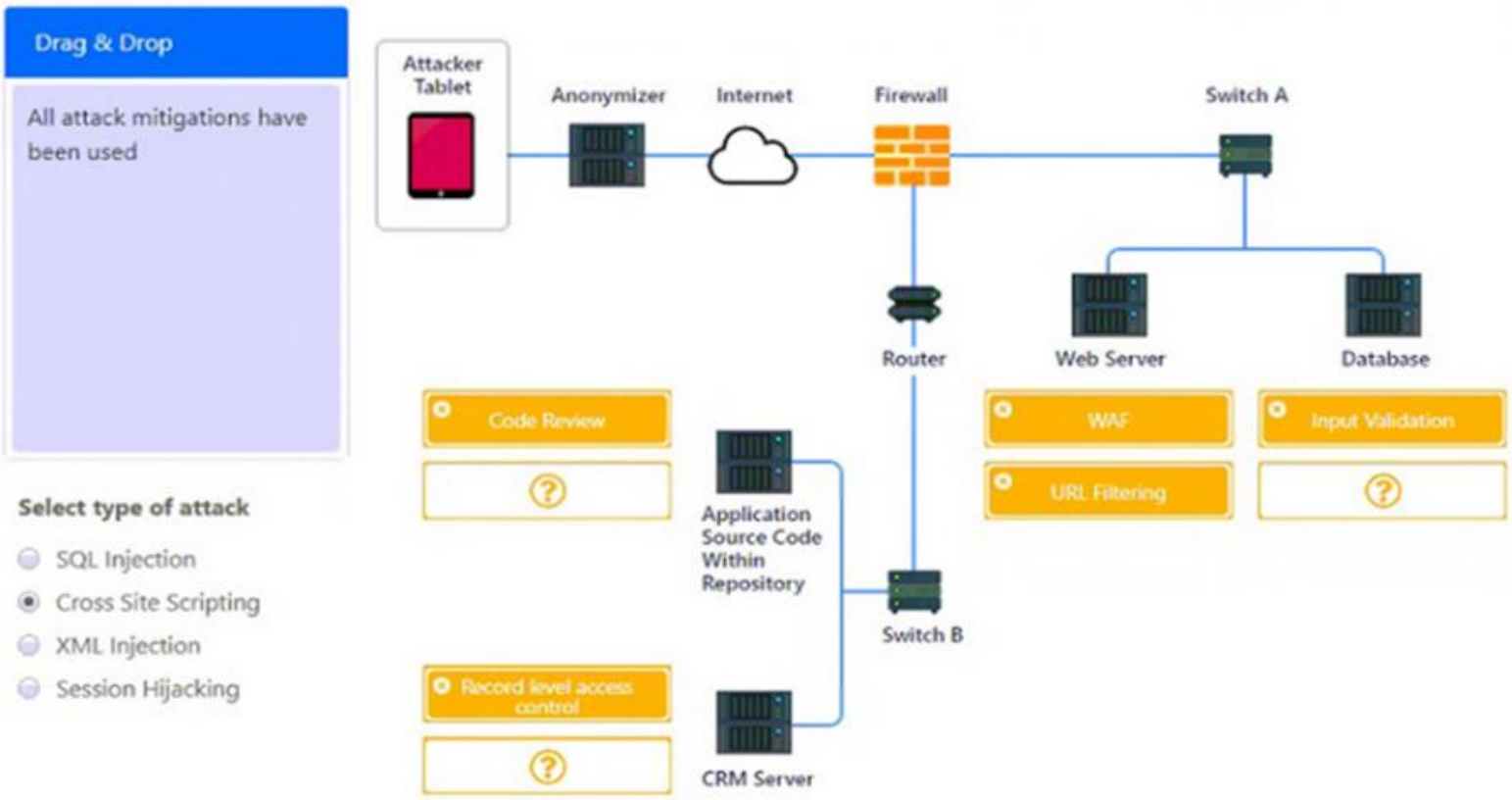
WAF

URL Filtering

Record level access control



Explanation



Application Source Code -> Code Review
CRM Server - > Record Level access Control
Web Server -> WAF and URL Filtering -
Database ->Input validation
Cookies are only on the client-side. Never in a database so it's not sql.

Q. A penetration tester has successfully exploited a vulnerability against your organization giving him access to the following data:

User, password, login-date, cookie-id
Homer, canipass, 2016-09-01 11:12, 286755fad04869ca523320acce0dc6a4
Bart, passican, 2016-09-01 11:15, 8edd7261c353c87a113269cd37635c68
Marge, icanpass, 2016-09-01 11:19, 26887fbd90ac0340e29ad62470270401

What type of attack does this represent?

A. SQL injection

B. XML injection

C. XSS

D. Session hijacking

Answer: C. Cross-site scripting (XSS) is the best choice of the available answers. You can see that the penetration tester is looking at cookies because the header includes ‘cookie-id’ and successful cross-site scripting (XSS) attacks allow attackers to capture user information such as cookies.

Question #:33 - (Exam Topic 3)

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software

B. Documentation of system classifications

C. A list of system owners and their departments

D. Third-party risk assessment documentation

Answer: A

Explanation

To accurately measure the overall risk to an organization when a new vulnerability is disclosed, having a full inventory of all hardware and software is essential. Here's why:

Full Inventory of Hardware and Software: When a new vulnerability is disclosed, security analysts need to assess the potential impact on the organization. To do this, they must know which systems are affected. Having a comprehensive inventory of all hardware and software within the organization enables analysts to identify which systems are vulnerable and need immediate attention.

While the other items mentioned (documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation) are important components of a comprehensive cybersecurity program, they are not as directly related to the initial step of identifying and measuring the risk posed by a new vulnerability. These other elements can be valuable for managing and mitigating risk but may come into play at later stages of the vulnerability management process.

References:

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/risk-analysis/

https://resources.infosecinstitute.com/certification/security-plus-risk-management-processes-and-concepts https://www.comptia.org/landing/securityplus/index.html

https://www.comptia.org/blog/complete-guide-to-risk-management

Question #:34 - (Exam Topic 3)

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS

B. PaaS

C. laaS

D. DaaS

Answer: C

Explanation

The cloud model that provides clients with servers, storage, and networks but nothing else is IaaS (Infrastructure as a Service).

In an IaaS model, clients can rent virtualized hardware resources such as virtual machines, storage, and networking infrastructure from a cloud service provider. Clients are responsible for managing the operating system, applications, and data running on the provided infrastructure. This gives clients more control over their computing environment compared to other cloud models like SaaS (Software as a Service) or PaaS (Platform as a Service), where the provider manages more aspects of the computing stack.

Here's a brief overview of the mentioned cloud service models:

SaaS (Software as a Service): In SaaS, clients are provided with access to software applications that are hosted and maintained by the cloud service provider. Clients typically don't manage the underlying infrastructure, operating system, or application code.

PaaS (Platform as a Service): PaaS provides clients with a platform and environment for developing, deploying, and managing applications. It abstracts the underlying infrastructure but still requires clients to manage their application code.

DaaS (Desktop as a Service): DaaS delivers virtual desktop environments from the cloud to end-users. It's focused on providing desktop computing resources rather than just servers, storage, and networks.

So, if you're looking for a cloud model that offers servers, storage, and networks without managing the software stack, IaaS is the appropriate choice.

Question #:35 - (Exam Topic 3)

A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would best meet this need?

A. CVE

B. SIEM

C. SOAR

D. CVSS /// Vulnerability scoring

Answer: D

Explanation

To communicate the severity levels of an organization's vulnerabilities to the leadership team, the best option among the provided choices is CVSS (Common Vulnerability Scoring System).

Here's why CVSS is the most appropriate choice:

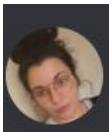
CVE (Common Vulnerabilities and Exposures): CVE is a database of known vulnerabilities, and it provides unique identifiers for each vulnerability. While CVEs are essential for tracking vulnerabilities, they do not provide a severity score or a comprehensive assessment of how critical a vulnerability is to an organization.

SIEM (Security Information and Event Management): SIEM systems are used for collecting, analyzing, and correlating security event data. They are valuable for monitoring and managing security incidents but do not directly provide vulnerability severity assessments.

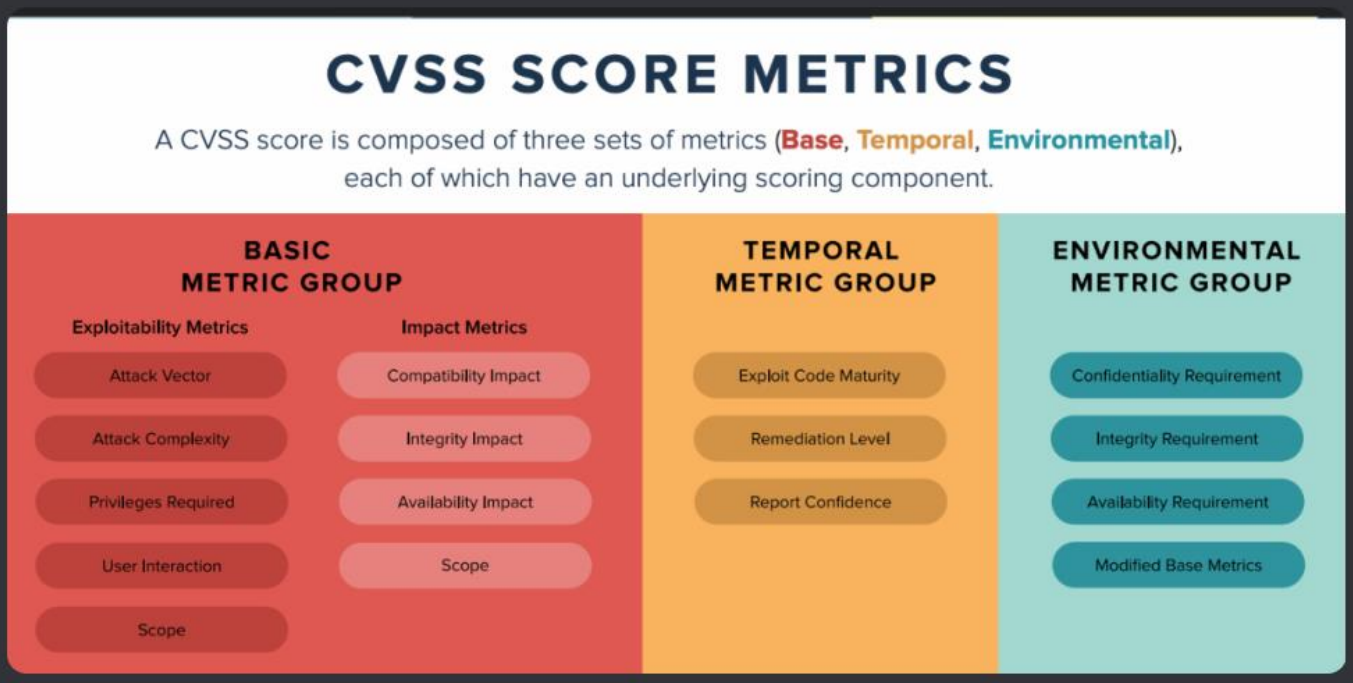
SOAR (Security Orchestration, Automation, and Response): SOAR platforms focus on automating and orchestrating security processes and incident response. While they can help in managing vulnerabilities, their primary purpose is automation and orchestration, not vulnerability severity assessment.

CVSS (Common Vulnerability Scoring System): CVSS is specifically designed to assess and communicate the severity of vulnerabilities. It provides a numerical score based on a range of factors, including the impact and exploitability of a vulnerability. This score can be easily communicated to the leadership team to help them understand the risk associated with different vulnerabilities and prioritize mitigation efforts accordingly.

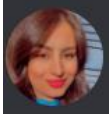
In summary, CVSS is the most suitable choice for communicating vulnerability severity levels to the leadership team, as it provides a standardized and easily understandable way to assess and prioritize vulnerabilities based on their potential impact on the organization's security.



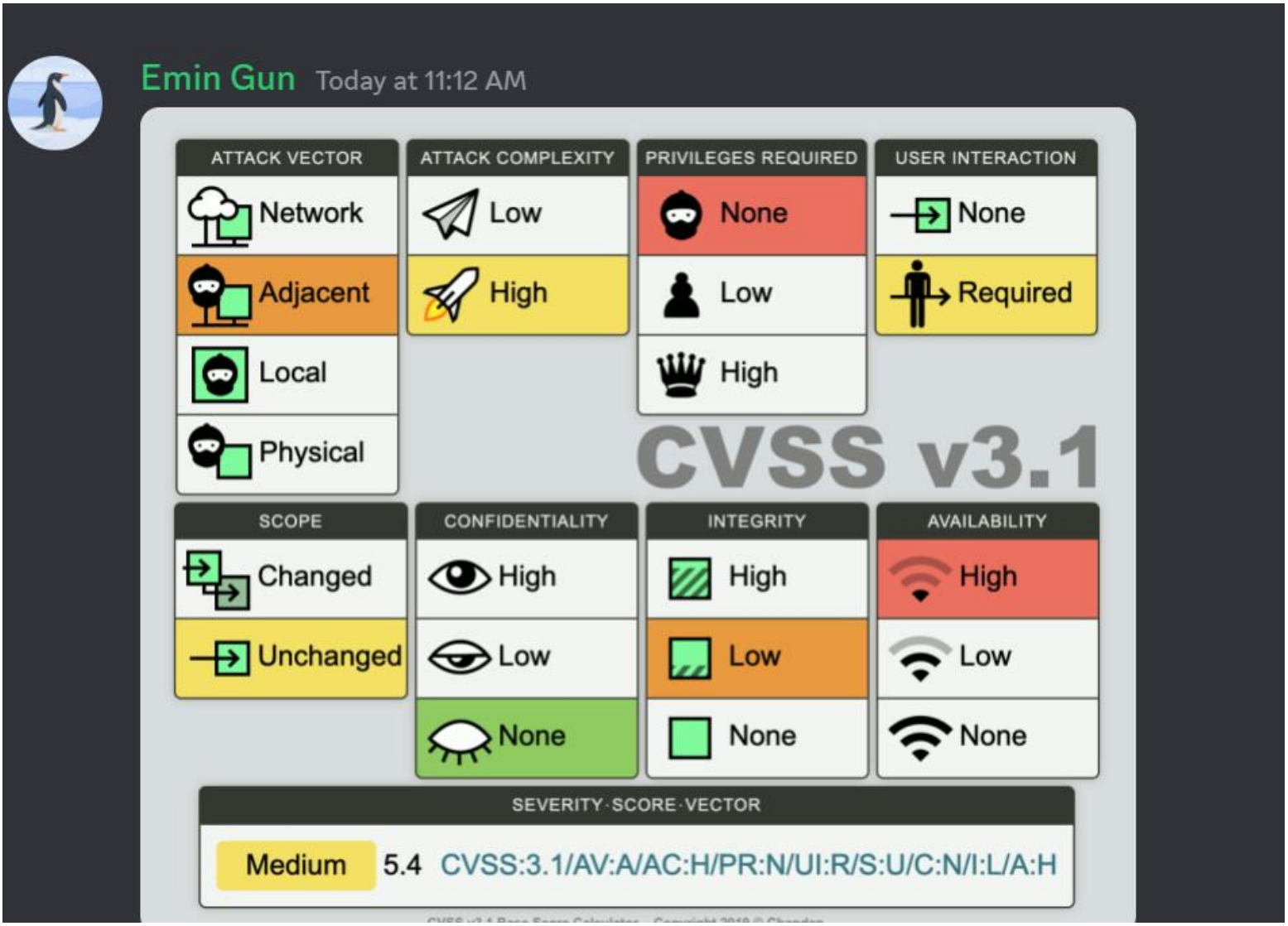
Petra Martina Vrancic Today at 11:12 AM



Emin Gun Today at 11:12 AM



Kwestan Abdalrahman Today at 11:12 AM



Question #:36 - (Exam Topic 3)

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software

C. Performing static code analysis on the software

D. Ensuring secure cookies are used

Answer: B

Explanation

To ensure the authenticity of the code created by the company, the most appropriate option is performing code signing on company-developed software.

Code Signing: Code signing is a process where a digital signature is applied to software or code to verify its authenticity and integrity. It ensures that the software has not been tampered with or altered by unauthorized parties since it was signed. When users or systems encounter signed code, they can check the digital signature to confirm that the software comes from a trusted source and has not been modified. This helps in establishing the authenticity of the code.

Testing input validation on the user input fields is important for preventing malicious code from being entered into a system. However, it does not address the authenticity of the code itself.

Performing static code analysis on the software can help to identify security vulnerabilities. However, it cannot guarantee that the code has not been tampered with.

Ensuring secure cookies are used is important for preventing unauthorized access to user data. However, it does not address the authenticity of the code itself.

Therefore, the most appropriate option to ensure the authenticity of the code created by the company is to perform code signing on the software.

Here are some additional benefits of code signing:

It can help to prevent malware from being installed on users' computers. It can

help to protect intellectual property.

It can help to improve user trust.

Question #:37 - (Exam Topic 3)

During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following best describes this type of vulnerability?

A. Legacy operating system

B. Weak configuration

C. Zero day

D. Supply chain

Answer: C

Explanation

The type of vulnerability described, where a security flaw is discovered in a common operating system, but the vendor is unaware and has not yet released a patch, is typically referred to as a "Zero Day Vulnerability." It's called "zero-day" because there are zero days of protection from the time the vulnerability is discovered until the vendor releases a patch. Attackers may exploit zero-day vulnerabilities before a fix is available.

Here's a brief explanation of other terms mentioned for clarity:

Legacy Operating System: A legacy operating system is an older, outdated operating system that may no longer receive regular updates or support from the vendor. Vulnerabilities in legacy operating systems can persist for a long time, but they are not necessarily unknown to the vendor.

Weak Configuration: Weak configuration refers to security weaknesses resulting from misconfigured settings, which can be exploited by attackers. These vulnerabilities are generally not related to the vendor's awareness or patching schedule.

Supply Chain: Supply chain vulnerabilities relate to security risks introduced through the software supply chain, such as malicious actors compromising the development or distribution process. This term is not directly related to the scenario described.

References:

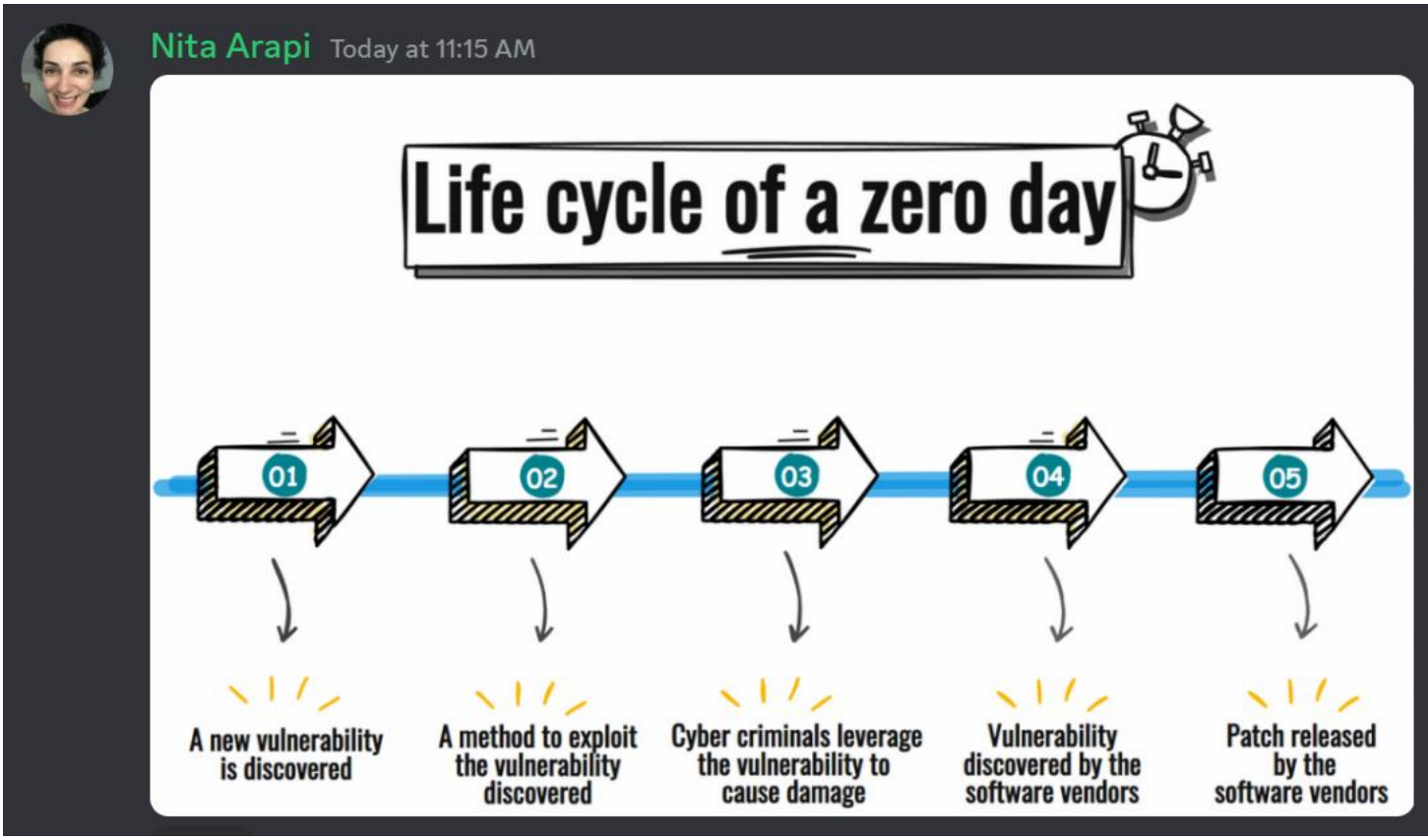
https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/

https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-1-threats-attacks-and-vulnera

https://www.professormesser.com/security-plus/sy0-501/zero-day-attacks-4/

Emin Gun — Today at 11:14 AM

A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched.



Question #:38 - (Exam Topic 3)

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the most effective across heterogeneous platforms?

A. Enforcing encryption

B. Deploying GPOs

C. Removing administrative permissions

D. Applying MDM software

Answer: D

Explanation

MDM stands for Mobile Device Management, which is a software solution that can manage and secure smartphones, laptops, tablets and other mobile devices across heterogeneous platforms. MDM can enforce security features such as

encryption, password policies, remote wipe, device tracking, app control and more. MDM can also monitor and update the devices remotely and provide reports and alerts on their status. MDM is the most effective solution to implement security features across heterogeneous platforms, as it can provide centralized and consistent management of various types of devices. Verified References:

Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.4: Given a scenario, implement secure systems design.)

CompTIA Security+ 601 - Infosec https://www.infosecinstitute.com/wp-content/uploads/2021/03/CompTIA-Security-eBook.pdf (See Security+: 5 in-demand cybersecurity skills, Implementation)

Certification Security+ | CompTIA https://www.comptia.org/landing/securityplus/index.html (See Exam Objectives)

Question #:39 - (Exam Topic 3)

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

A. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 67 -Allow: Any Any 68 -Allow: Any Any 22 -Deny: Any Any 21 -Deny: Any Any

B. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 67 -Allow: Any Any 68 -Deny: Any Any 22 -Allow: Any Any 21 -Deny: Any Any

C. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 22 -Deny: Any Any 67 -Deny: Any Any 68 -Deny: Any Any 21 -Allow: Any Any

D. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Deny: Any Any 67 -Allow: Any Any 68 -Allow: Any Any 22 -Allow: Any Any 21 -Allow: Any Any

Answer: A

Explanation

This firewall rule set allows a subnet to only access DHCP, web pages, and SFTP, and specifically blocks FTP by allowing or denying traffic based on the source, destination, and port. The rule set is as follows:

Allow any source and any destination on port 80 (HTTP)

Allow any source and any destination on port 443 (HTTPS)

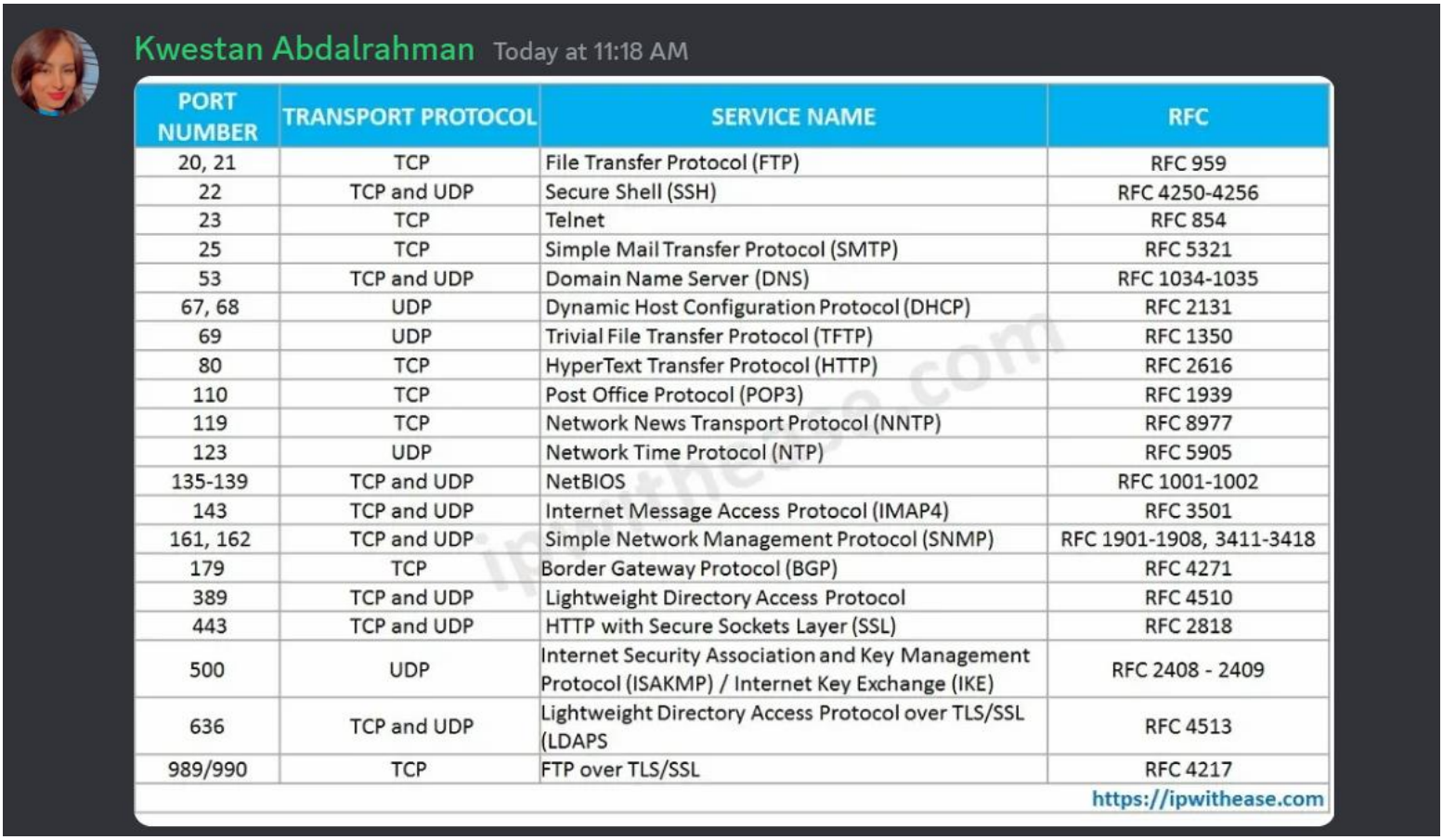
Allow any source and any destination on port 67 (DHCP server) Allow

any source and any destination on port 68 (DHCP client) Allow any

source and any destination on port 22 (SFTP)

Deny any source and any destination on port 21 (FTP)

Deny any source and any destination on any other port



PORT NUMBER	TRANSPORT PROTOCOL	SERVICE NAME	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217

Question #:40 - (Exam Topic 3)

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A. Compensating control

B. Network segmentation

C. Transfer of risk

D. SNMP traps

Answer: A

Explanation

A compensating control is a type of security control that is implemented in lieu of a recommended security measure that is deemed too difficult or impractical to implement at the present time. A compensating control must provide equivalent or comparable protection for the system or network and meet the intent and rigor of the original security requirement. An example of a compensating control is using a host-based firewall on a legacy Linux system to allow connections from only specific internal IP addresses, as it can provide a similar level of defense as a network firewall that may not be compatible with the system. When it comes to A-Compensating control, the given explanation under the question is quite explanatory actually.

"A compensating control is a type of security control that is implemented in lieu of a recommended security measure (e.g. network-based firewalls, routers, VLANs, etc.) that is deemed too difficult or impractical to implement at the present time. A compensating control must provide equivalent or comparable protection for the system or network and meet the intent and rigor of the original security requirement. An example of a compensating control is using a host-based firewall on a legacy Linux system to allow connections from only specific internal IP addresses, as it can provide a similar level of defense as a network firewall that may not be compatible with the system."

Now, the keyword in the question is "legacy". Suppose that you have a legacy Linux server which is not compatible with those network-based firewalls, routers and multi-layer switches which is preventing you not just from building VLANs (Network Segmentation), but also from applying white-listing ACL technique against malicious IP addresses. So, what you're going to do is you are going to use host-based firewalls as a compensation for network appliances to be able to accomplish the similar end-result

Network Segmentation: Network segmentation involves dividing a network into separate segments or subnetworks.

Transfer of Risk: Transfer of risk typically involves shifting the financial burden or liability for a specific risk to another party, often through insurance or contractual arrangements. It is not directly related to firewall rules.

SNMP Traps: SNMP (Simple Network Management Protocol) traps are notifications sent by network devices to a management system to report specific events or conditions. SNMP traps are used for network monitoring and management but are not directly related to firewall access control.

References:

> https://www.techtarget.com/whatis/definition/compensating-control https://reciprocity.com/resources/whats-the-difference-between-compensating-controls-and-mitigating-co
>
> Petra Martina Vrancic — Today at 11:21 AM
>
> Using a host-based firewall to allow connections only from specific internal IP addresses is an example of a compensating control. Compensating controls are security measures that are put in place to offset or compensate for vulnerabilities or weaknesses in an organization's systems or processes. In this case, the host-based firewall is compensating for the lack of network segmentation by restricting connections to specific internal IP addresses
>
> Emin Gun — Today at 11:21 AM
>
> What are Compensating Controls? In cybersecurity, compensating controls are measures taken to address any weaknesses of existing controls or to compensate for the inability to meet specific security requirements due to various different constraints.
>
> Osman Ceylan — Today at 11:21 AM
>
> spesific ip

Question #:41 - (Exam Topic 3)

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.

Which of the following best describes this step?

A. Capacity planning

B. Redundancy

C. Geographic dispersion

D. Tabletop exercise

Answer: A

Explanation

The step that best describes determining how many staff members would be required to sustain the business in the case of a disruption is Capacity Planning.

Here's a brief explanation of each term:

Capacity Planning: Capacity planning involves assessing the resources, including staff, that an organization needs to meet its operational requirements, especially during times of disruption or increased demand. In this context, it would involve calculating the necessary staffing levels to ensure that essential business functions can continue in the event of a disruption.

Redundancy: Redundancy refers to the practice of having backup systems, resources, or personnel in place to maintain critical operations in case of a disruption. While staffing levels may be part of redundancy planning, it doesn't specifically address the determination of the required staff numbers.

Geographic Dispersion: Geographic dispersion is a strategy where an organization spreads its operations across multiple locations to reduce the risk of disruption caused by a localized event (e.g., natural disaster). While this strategy may affect staffing decisions, it doesn't directly involve determining the required staff numbers.

Tabletop Exercise: A tabletop exercise is a simulated scenario in which key stakeholders gather to discuss and practice their response to a hypothetical disaster or disruption. It helps organizations test their continuity plans and identify areas that may need adjustment. It doesn't directly address the step of determining staffing levels.

In summary, capacity planning is the step that focuses on assessing and determining the necessary staffing levels to sustain the business during a disruption, ensuring that the right personnel are available to maintain essential operations.

Question #:42 - (Exam Topic 3)

A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.

B. remove the single point of failure.

C. cut down the mean time to repair

D. reduce the recovery time objective

Answer: B

Explanation

A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and

provide redundancy and failover capabilities.

Remove the single point of failure: Implementing a high availability (HA) pair of firewalls means that if one firewall goes offline or experiences a failure, the other firewall can take over seamlessly. This eliminates the single point of failure and ensures continuous network security even if one firewall becomes unavailable.

The Mean Time to Repair (MTTR) is a metric used in reliability engineering and maintenance to measure the average time it takes to repair a failed system or component and restore it to normal functioning.The RTO is the maximum acceptable downtime for a system or service. MTBF is a metric that quantifies the average time elapsed between failures of a system or component.

Question #:43 - (Exam Topic 3)

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

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 Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Attack Identified options: Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

BEST Preventative or Remediation Action options: Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

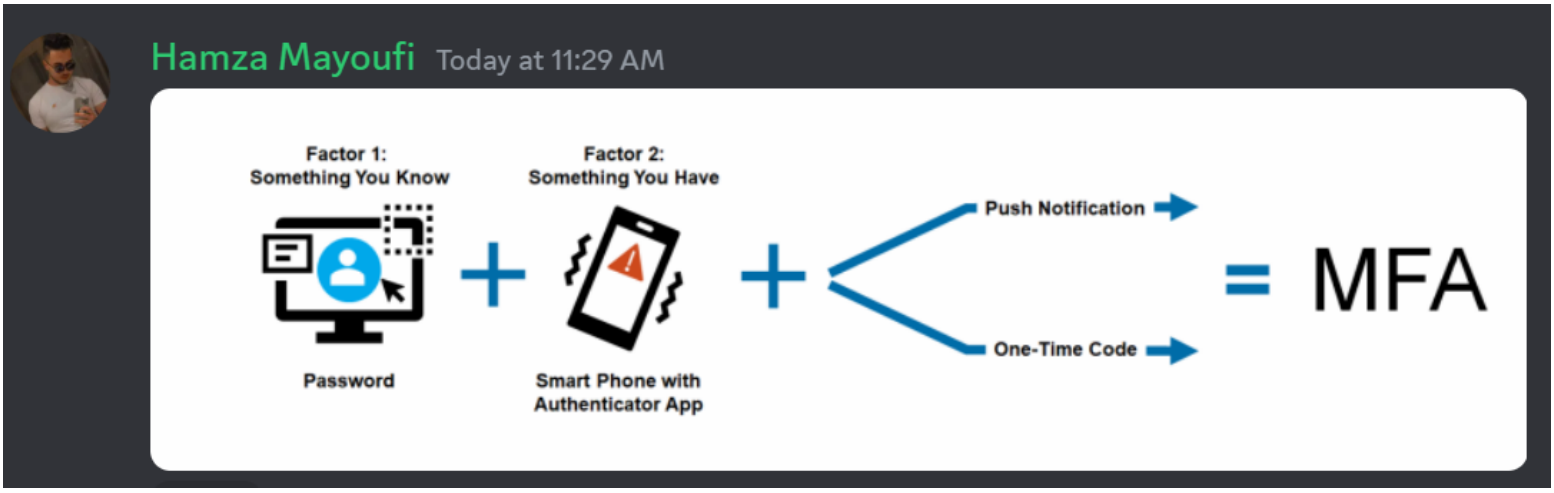
Explanation

Web server Botnet Enable DDoS protection**User** RAT Implement a host-based IPS**Database server** Worm Change the default application password**Executive** KeyloggerDisable vulnerable services**Application** Backdoor Implement 2FA using push notification

A screenshot of a computer program Description automatically generated with low confidence

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Emin Gun — Today at 11:29 AM
A push notification is a message that pops up on a mobile device, such as a sports score, an invitation to a flash sale or a coupon for downloading.



Question #:44 - (Exam Topic 3)

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's Pll?

A. SCAP

B. NetFlow

C. Antivirus

D. DLP

Answer: D

Explanation

DLP stands for Data Loss Prevention, which is a technology that can monitor, detect and prevent the unauthorized transmission of sensitive data, such as PII (Personally Identifiable Information). DLP can be implemented on endpoints, networks, servers or cloud services to protect data in motion, in use or at rest. DLP can also block or alert on data transfers that violate predefined policies or rules. DLP is the best tool to assist with detecting an employee who has accidentally emailed a file containing a customer's PII, as it can scan the email content and attachments for any data that matches the criteria of PII and prevent the email from being sent or notify the administrator of the incident.

The other options, SCAP, NetFlow, and Antivirus, are valuable security tools but are not specifically designed for detecting and preventing accidental data leaks involving PII in emails:

SCAP (Security Content Automation Protocol) is a framework used for automating security-related tasks such as vulnerability management and compliance checking but does not focus on email content inspection or data loss prevention.

NetFlow is a network monitoring and traffic analysis tool that provides insights into network traffic patterns and can help identify suspicious network behavior but is not designed for email content inspection or data loss prevention.

Antivirus software primarily focuses on identifying and removing malware from files and systems, rather than preventing the unintentional sharing of customer PII through email.

For PII protection, especially in email communication, organizations should invest in DLP solutions and create policies and rules that align with their data security needs and compliance requirements.

Verified References:

Data Loss Prevention Guide to Blocking Leaks - CompTIA https://www.comptia.org/content/guides/data-loss-prevention-a-step-by-step-guide-to-blocking-leaks

Data Loss Prevention – SY0-601 CompTIA Security+ : 2.1 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-loss-prevention-4/

Data Loss Prevention – CompTIA Security+ SY0-501 – 2.1 https://www.professormesser.com/security-plus/sy0-501/data-loss-prevention-3/

Petra Martina Vrancic — Today at 11:31 AM

It's like the guardian angel of sensitive information, making sure it doesn't wander off where it shouldn't

Question #:45 - (Exam Topic 3)

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop.A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

No	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst most likely see in this packet capture?

A. Session replay

B. Evil twin

C. Bluejacking

D. ARP poisoning

Answer: B

Explanation

One of the main purposes of deauthentication used in the hacking community is to force clients to connect to an evil twin access point, which then can be used to capture network packets transferred between the client and the access point. The Wireshark capture provided shows multiple deauthentication frames being sent by the source "Sagemcom_87:9f:a3" to the broadcast address, indicating that devices in the wireless network are being forcibly disconnected or deauthenticated.

An evil twin is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. In this packet capture, the analyst can see that there are two access points with the same SSID (CoffeeShop) but different MAC addresses (00:0c:41:82:9c:4f and 00:0c:41:82:9c:4e). This indicates that one of them is an evil twin that is trying to impersonate the other one.

Session Replay: Session replay attacks involve capturing and replaying network traffic to impersonate a user's session. This attack doesn't typically involve sending deauthentication frames as shown in the capture. Deauthentication frames are more commonly associated with disrupting network connections.

Bluejacking: Bluejacking is an attack related to Bluetooth devices, not Wi-Fi. It doesn't involve deauthentication frames in a Wi-Fi network.

ARP Poisoning (ARP Spoofing): ARP poisoning is a technique where an attacker sends malicious ARP packets to associate their MAC address with the IP address of another device on the network. While ARP poisoning can lead to various network attacks, it's not directly related to the deauthentication frames shown in the capture.

Question #:46 - (Exam Topic 3)

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will

grant the employee access to other company-owned websites based on the intranet profile.
Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation

B. Identity proofing

C. Password complexity

D. Default password changes

E. Password manager

F. Open authentication

Answer: A C

Explanation

Federation: The company's approach of granting access to multiple company-owned websites based on the intranet profile suggests a form of identity federation. Federation allows a user to access multiple systems or services with a single set of credentials (in this case, the intranet account). It enables single sign-on (SSO) capabilities, where the user logs in once and gains access to various resources without needing to authenticate separately for each one.

Password Complexity: The requirement for a password to include ten characters, numbers, letters, and two special characters is an example of enforcing password complexity. Password complexity rules enhance security by ensuring that passwords are not easily guessable or susceptible to brute-force attacks.

Identity proofing typically involves verifying an individual's identity through various means, which may include presenting physical identification documents or answering security questions. It is not mentioned as a part of the password creation process.

Default password changes refer to changing default passwords provided by systems or devices. This is not the primary focus in the scenario.

Password manager is a tool or software used by individuals to store and manage their passwords securely. While it can be a good practice for users, it is not the primary mechanism by which access is managed in this scenario.

Open authentication (assuming you mean OpenID or OAuth) is a protocol for authentication and authorization but is not directly mentioned as the method for granting access in this scenario. Federation is a more specific concept related to the scenario.

References:

https://www.keycloak.org/

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-fed

Question #:47 - (Exam Topic 3)

A security administrator needs to inspect in-transit files on the enterprise network to search for PII credit card data, and classification words .Which of the following would be the best to use?

A. IDS solution

B. EDR solution

C. HIPS software solution

D. Network DLP solution

Answer: D

Explanation

A network DLP (Data Loss Prevention) solution is a tool that monitors and controls the data that is transmitted over a network. It can inspect in-transit files on the enterprise network to search for PII (Personally Identifiable Information), credit card data, and classification words by using predefined rules and policies, and then block, encrypt, quarantine, or alert on any sensitive data that is detected or leaked.

Question #:48 - (Exam Topic 3)

A network penetration tester has successfully gained access to a target machine. Which of the following should the penetration tester do next?

A. Clear the log files of all evidence

B. Move laterally to another machine.

C. Establish persistence for future use.

D. Exploit a zero-day vulnerability.

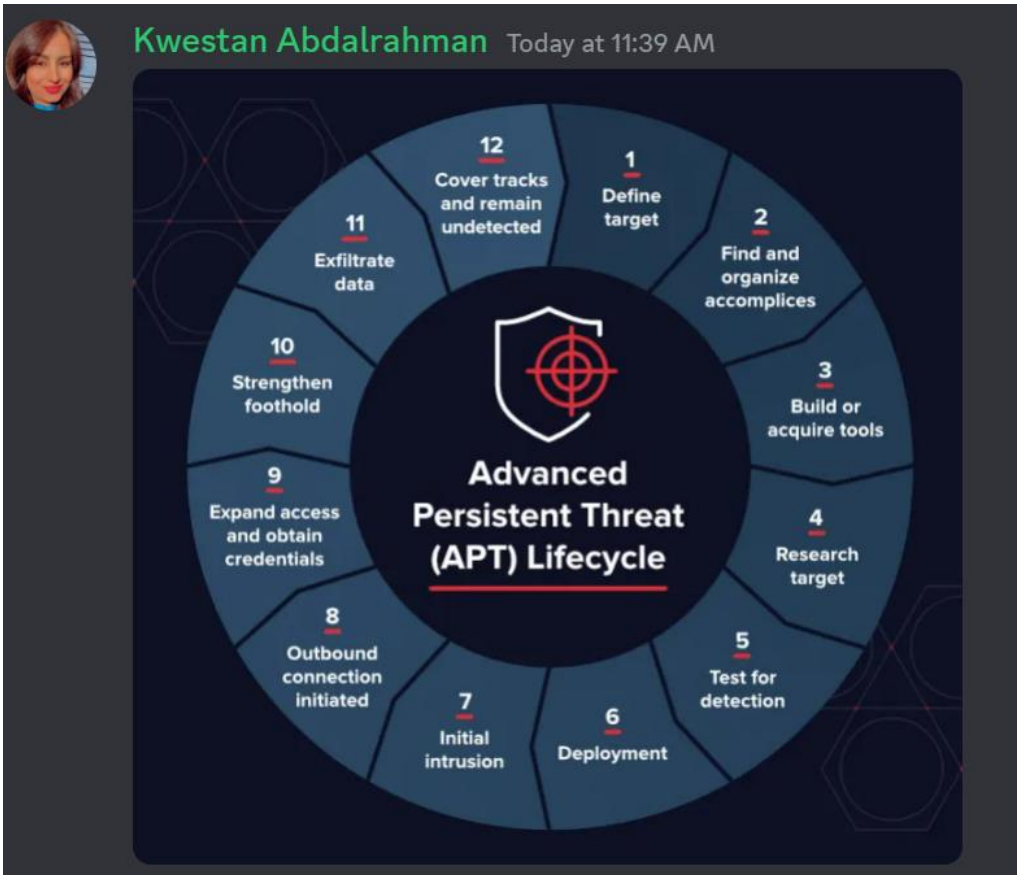
Answer: C

Explanation

APT

Establishing persistence for future use is the next step that a network penetration tester should do after gaining access to a target machine. Persistence means creating a backdoor or a covert channel that allows the penetration tester to maintain access to the target machine even if the initial exploit is patched or the connection is lost. Persistence can be achieved by installing malware, creating hidden user accounts, modifying registry keys, or setting up remote access tools. Establishing persistence can help the penetration tester to perform further reconnaissance, move laterally to other machines, or exfiltrate data from the target network.

The other options mentioned, such as clearing log files or exploiting a zero-day vulnerability, would typically be considered unethical and potentially illegal if done without proper authorization. Ethical penetration testing focuses on identifying and mitigating security weaknesses, not causing harm or attempting unauthorized actions.



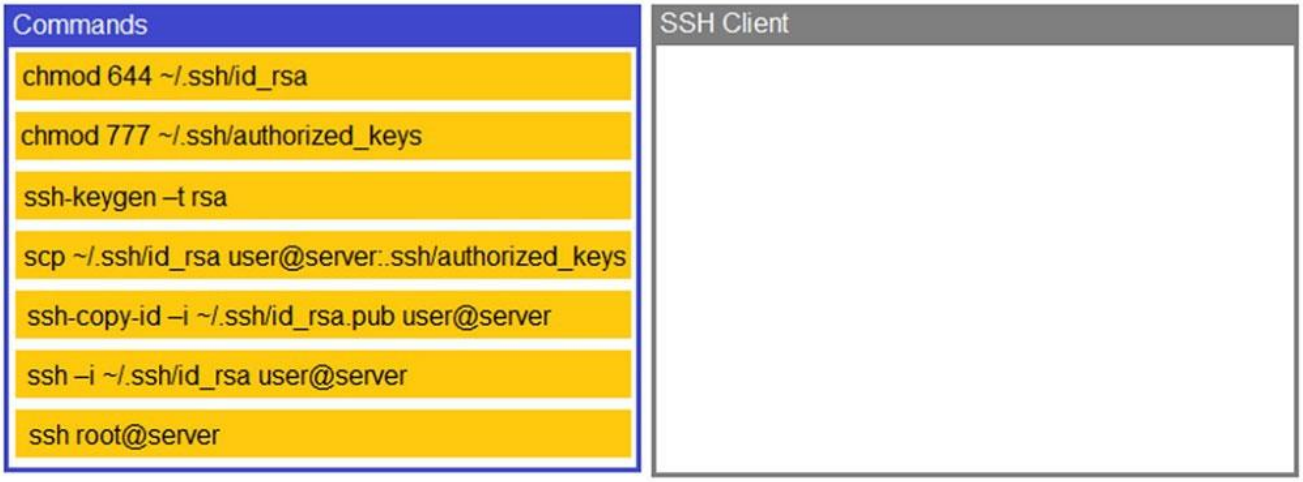
Question #:49 - (Exam Topic 3)

A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

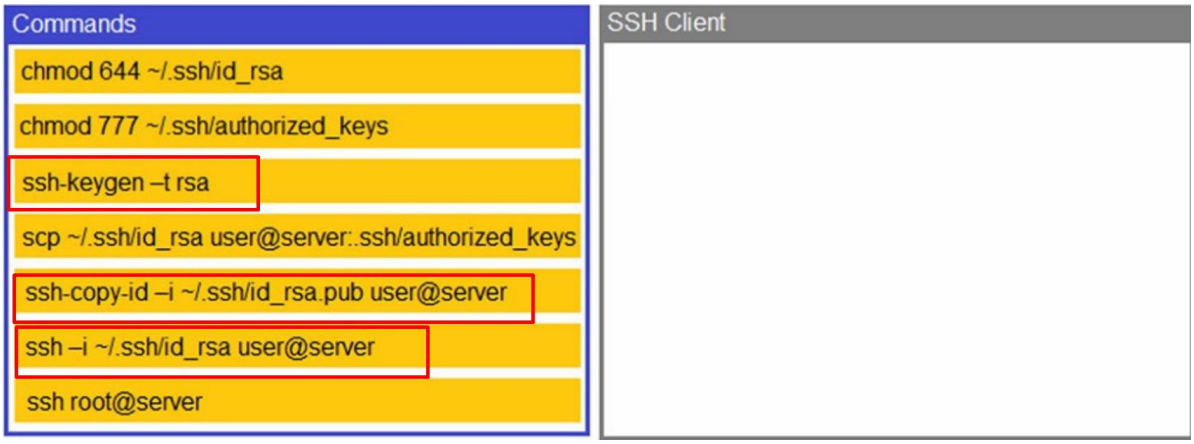
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

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



Answer:

The task requires only the minimum set of commands.
1. ssh-keygen -t rsa (creating the key-pair)
2. ssh-copy-id -i /.ssh/id_rsa.pub user@server (copy the public-key to user@server)
3. ssh -i ~/.ssh/id_rsa user@server (login to remote host with private-key)



Explanation

ssh-keygen -t rsa (creating the key pair):

- This command generates a new SSH key pair, consisting of a private key (id_rsa) and a public key (id_rsa.pub). The -t option specifies the key type (RSA in this case). These keys will be used for authentication.

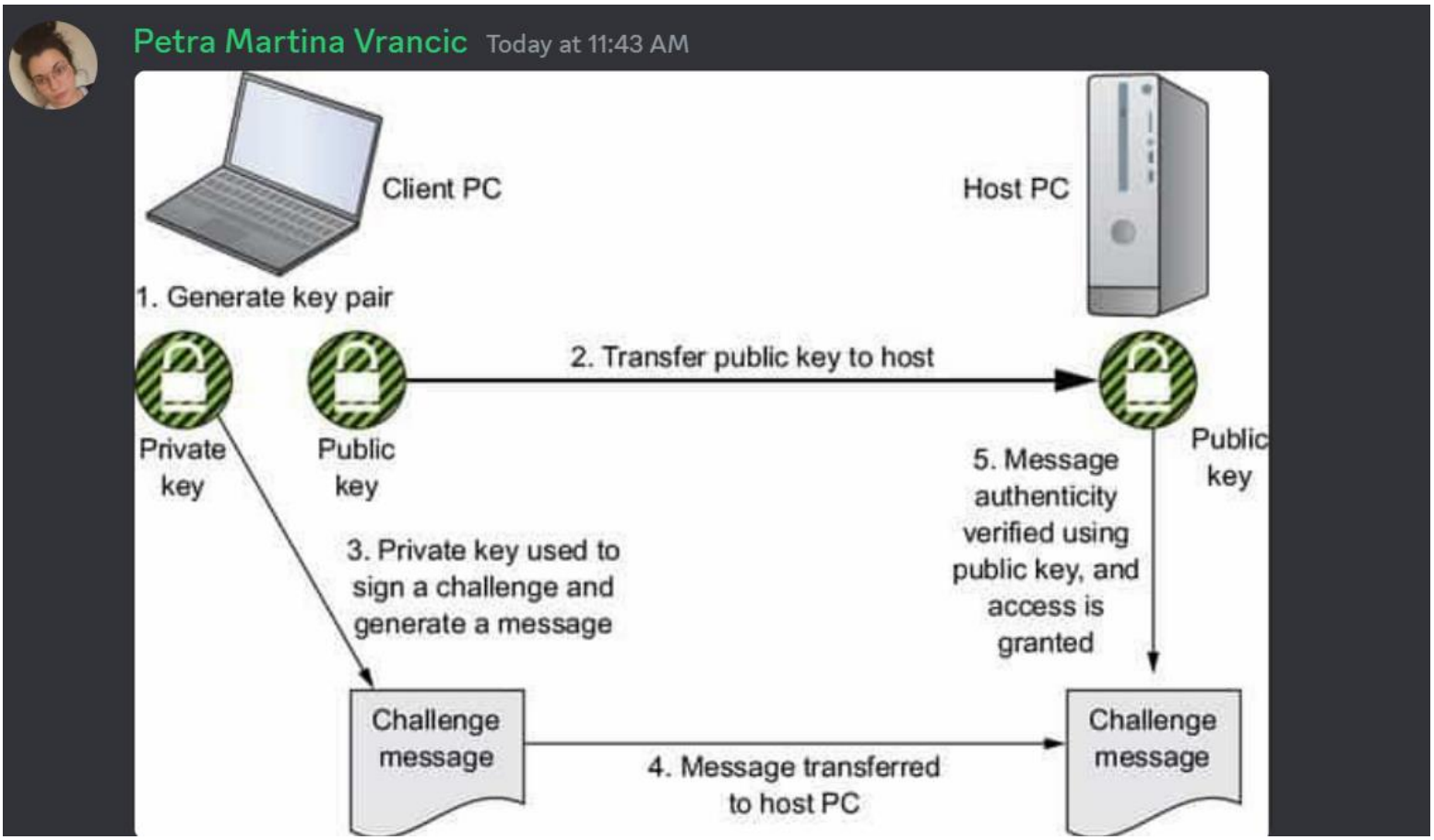
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server (copy the public key to user@server):

- This command is used to copy the public key to a remote server so that you can use key-based authentication.
- The -i option specifies the path to the public key file (~/.ssh/id_rsa.pub), and user@server represents the remote

username and server address. This command appends the public key to the ~/.ssh/authorized_keys file on the remote server, allowing you to log in without a password.

ssh -i ~/.ssh/id_rsa user@server (login to the remote host with the private key):

- This command establishes an SSH connection to the remote server (server) as the specified user (user) using the private key (~/.ssh/id_rsa) for authentication. By specifying the private key file with the -i option, you can log in without needing a password, provided that the public key corresponding to this private key has been added to the remote server's ~/.ssh/authorized_keys file.



Question #:50 - (Exam Topic 3)

A large retail store's network was breached recently and this news was made public. The store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the store lost revenue after the breach. Which of the following is the most likely reason for this issue?

A. Employee training

B. Leadership changes

C. Reputation

D. Identity theft

Answer: C

Explanation

Reputation is the perception or opinion that customers, partners, investors, etc., have about a company or its products and services. It can affect the revenue and profitability of a company after a network breach, even if no intellectual property or customer information was stolen, because it can damage the trust and confidence of the stakeholders and reduce their willingness to do business with the company

Question #:51 - (Exam Topic 3)

A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account
- One of the websites the manager used recently experienced a data breach.
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.

Which of the following attacks has most likely been used to compromise the manager's corporate account?

A. Remote access Trojan

B. Brute-force

C. Dictionary

D. Credential stuffing

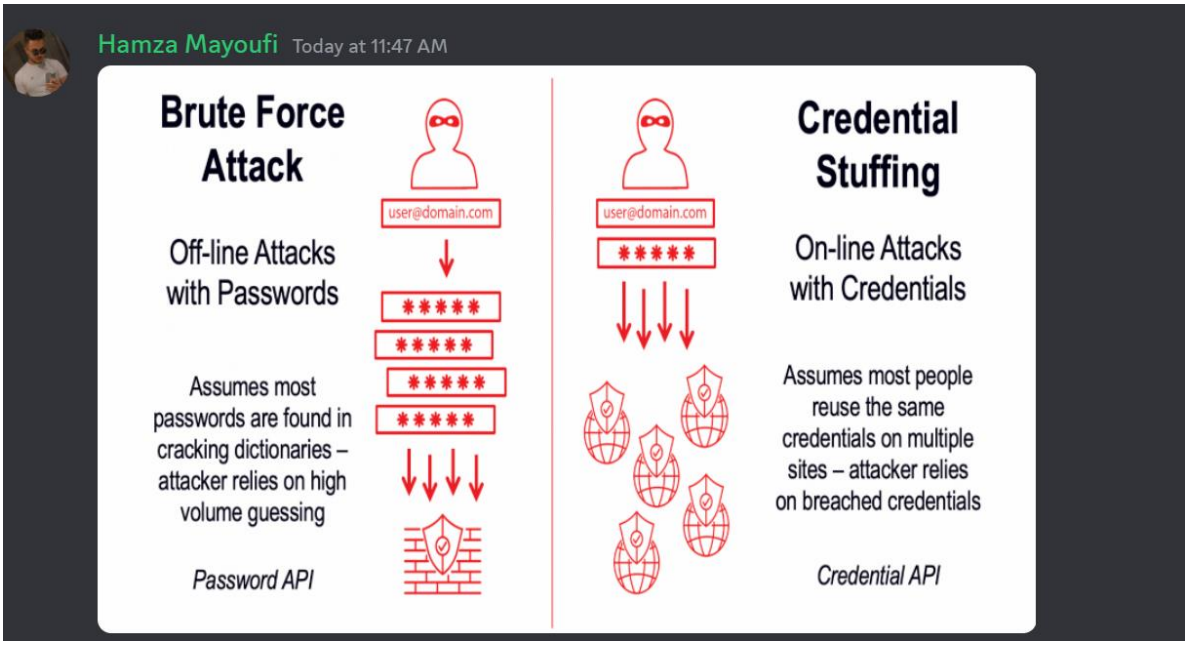
E. Password spraying

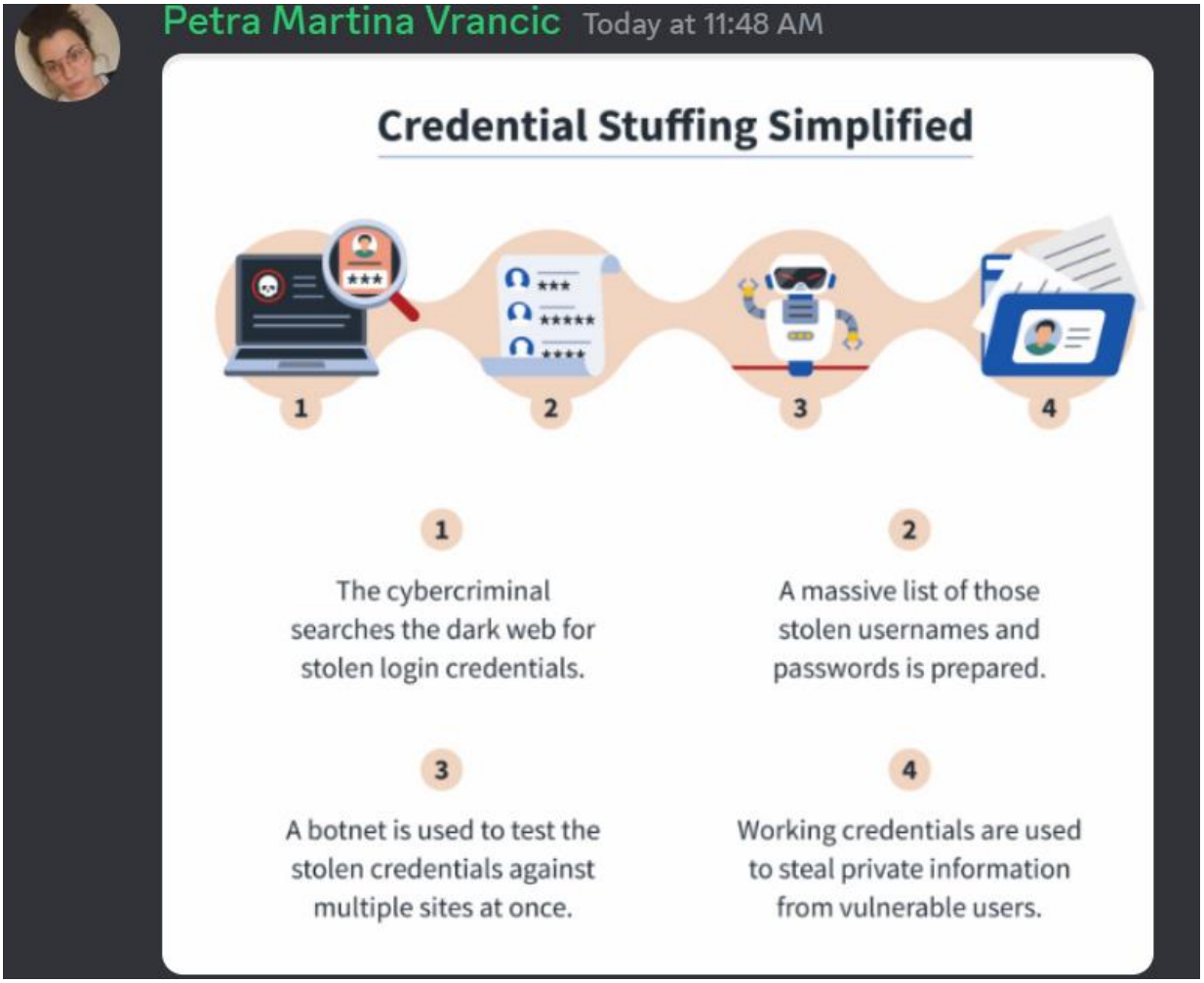
Answer: D

Explanation

Credential stuffing is the most likely attack that has been used to compromise the manager's corporate account. Credential stuffing is a type of cyber attack that involves using lists of stolen username and password combinations to gain unauthorized access to multiple accounts.

In this case, it is likely that the manager's password was obtained during the data breach of one of the external websites the manager used, and then used in a credential stuffing attack to access the manager's corporate email account. The fact that the manager was using the same password across multiple websites and the corporate account made it easier for the attacker to carry out the attack and compromise the corporate account.





Oytun Azkanar — Today at 11:47 AM

Credential stuffing is a cyberattack method in which an attacker uses a large list of stolen username and password combinations (credentials) to gain unauthorized access to user accounts on various online platforms, services, or websites. This type of attack relies on the fact that many people reuse passwords across multiple accounts, and the attacker capitalizes on this behavior.

Question #:52 - (Exam Topic 3)

An audit identified PII being utilized in the development environment of a critical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed: however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to best satisfy both the CPOs and the development team's requirements?

A. Data purge

B. Data encryption

C. Data masking

D. Data tokenization

Answer: C

Explanation

Tokenization

Typical uses: Payment processing systems; structured data

Tokenization, like encryption, is a reversible process that replaces sensitive data with data that can't be used by unauthorized parties. While encryption uses algorithms to generate ciphertext from plaintext, tokenization replaces the original data with randomly-generated characters in the same format (token values). Relationships between the original values and token values are stored on a token server. When a user or application needs the correct data, the tokenization system looks up the token value and retrieves the original value.

Tokenization is often used to protect credit card numbers or other sensitive information in payment processing systems, customer service databases, and other structured data environments. However, length-and-format-preserving encryption can address the same use cases, often with less complexity.

Masking

Typical uses: Test environments; structured data

Masking is essentially permanent tokenization. Sensitive information is replaced by random characters in the same format as the original data, but without a mechanism for retrieving the original values. This is a common practice in test environments, which require realistic-looking data but cannot be populated with actual customer or employee data.

Masking can also be used to control access to sensitive data based on entitlements. This approach, known as dynamic data masking, allows authorized users and applications to retrieve unmasked data from a database, while providing masked data to users who are not authorized to view the sensitive information.

To satisfy both the Chief Privacy Officer (CPO) and the development team's requirements, the best approach is to implement Data Masking.

Data Masking involves replacing sensitive or personally identifiable information (PII) with fictional or obfuscated data while maintaining the format and structure of the original data. This allows developers to perform functionality tests and search for specific data while ensuring that real PII is not exposed in the development environment.

Here's why Data Masking is the most suitable choice in this scenario:

Protecting PII: Data Masking ensures that sensitive PII is not exposed to developers in the development environment, addressing the CPO's concerns about data privacy and compliance.

Functional Testing: Developers can still perform functionality tests and search for specific data with masked data, as long as the data retains the same format and structure as the original. This allows them to test the application's functionality effectively.

Realistic Testing: Data masking provides a realistic testing environment because it maintains the data's appearance and relationships while protecting the actual PII. This helps ensure that the application behaves as expected with real-world data scenarios.

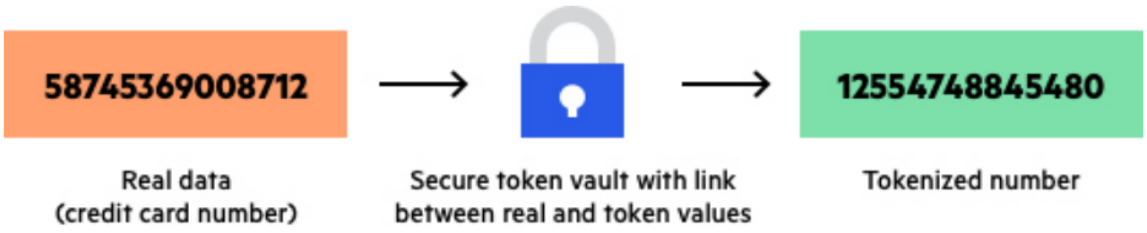
While other options like Data Purge, Data Encryption, and Data Tokenization have their use cases, they may not be as suitable for this scenario:

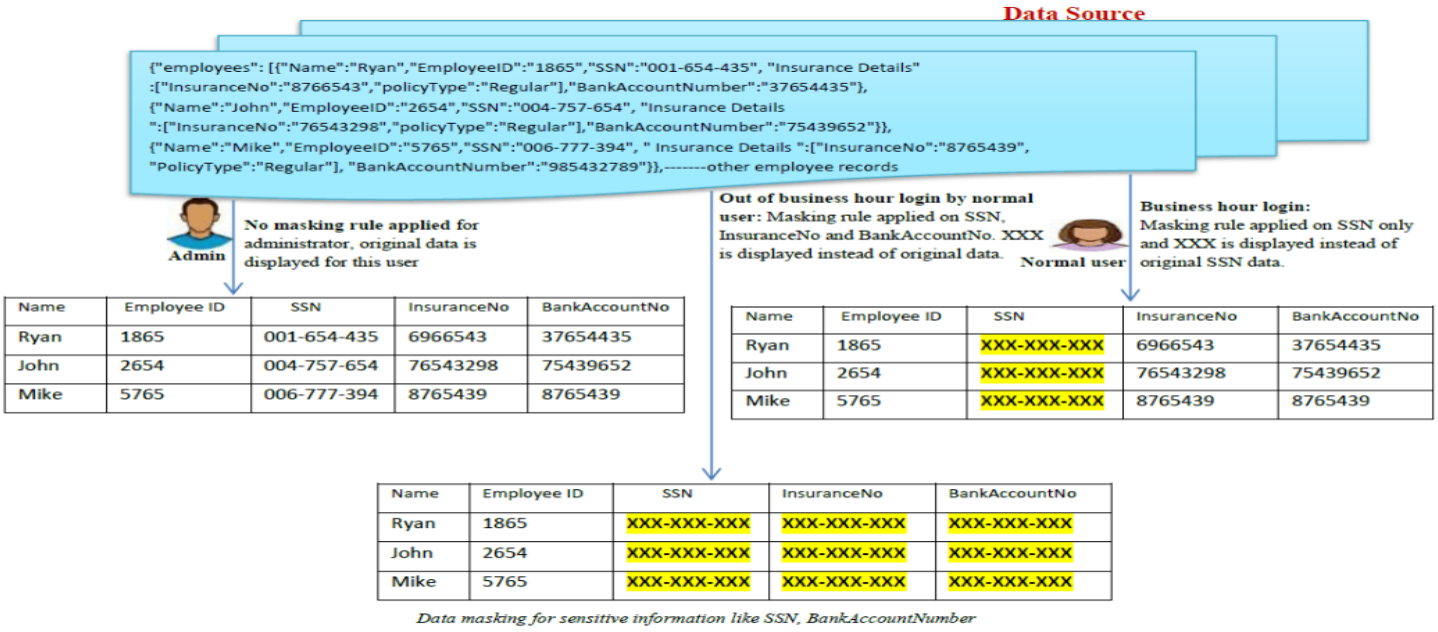
Data Purge: Purging all data would not allow for effective functionality testing and searching for specific data.

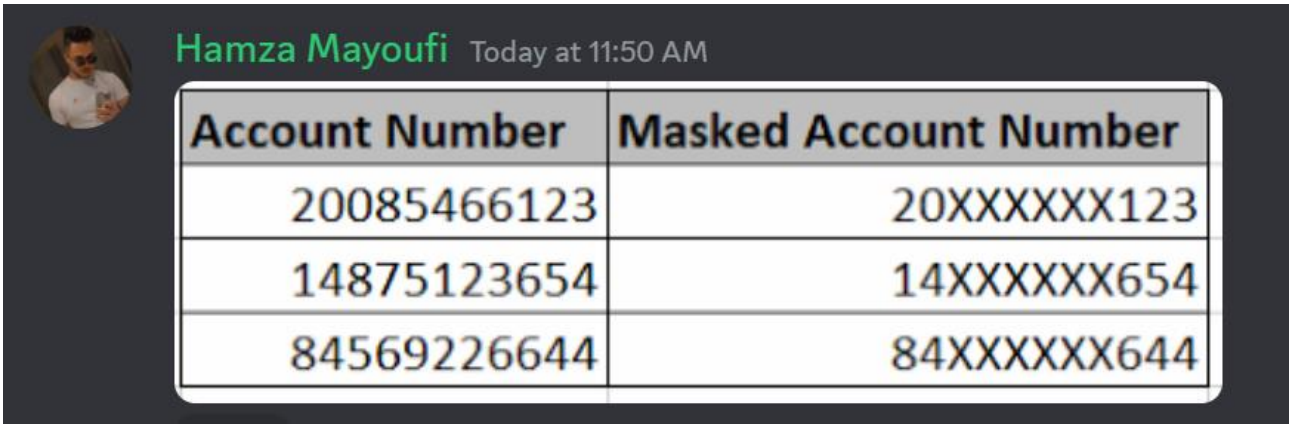
Data Encryption: While encryption can protect data, it doesn't necessarily address the developers' need for realistic data for testing and functionality purposes.

Data Tokenization: Tokenization replaces sensitive data with unique tokens, but it may not provide the realistic data scenarios needed for functional testing.

Data Masking strikes a balance between data privacy and the development team's requirements, making it the most appropriate choice.







Question #:53 - (Exam Topic 3)

A company wants to deploy PKI on its internet-facing website.The applications that are currently deployed are

• www company.com (main website)

• contact us company com (for locating a nearby location)

• quotes company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com Which of the following certificate types would best meet the requirements?

A. SAN

B. Wildcard

C. Extended validation

D. Self-signed

Answer: B

Explanation

A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (*) as a placeholder for any subdomain name. For example, *.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

Question #:54 - (Exam Topic 3) ///// Duplicate

An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be best to use to update and reconfigure the OS-level security configurations?

A. CIS benchmarks

B. GDPR guidance

C. Regional regulations

D. ISO 27001 standards

Answer: A

Explanation

To update and reconfigure OS-level security configurations to bring them into compliance, the best reference to use is CIS benchmarks (Center for Internet Security benchmarks).

CIS benchmarks provide detailed guidance and best practices for securing various operating systems, applications, and network devices. They are specifically designed to help organizations improve their security posture by aligning with industry-accepted security standards and best practices.

In this scenario, the outdated hardening standards need to be updated and reconfigured to ensure compliance. CIS benchmarks are widely recognized and respected in the cybersecurity community for providing comprehensive, up-to-date, and practical recommendations for securing various IT components, including operating systems.

The other options mentioned, such as GDPR guidance, regional regulations, and ISO 27001 standards, focus on different aspects of information security, data protection, and compliance but do not provide the detailed and specific guidance needed for updating and reconfiguring OS-level security settings. CIS benchmarks are more tailored to this specific task and would be the most appropriate choice.

Question #:55 - (Exam Topic 3)

Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall

B. System isolation

C. Least privilege

D. Application allow list

Answer: C

Explanation

Least privilege is a security principle that states that users should only be granted the permissions they need to do their job. This helps to protect against malware infections by preventing users from installing unauthorized software.

A host-based firewall can help to protect against malware infections by blocking malicious traffic from reaching a computer. However, it cannot prevent a user from installing malware if they have the necessary permissions.

System isolation is the practice of isolating systems from each other to prevent malware from spreading. This can be done by using virtual machines or network segmentation. However, system isolation can be complex and expensive to implement.

An application allow list is a list of applications that are allowed to run on a computer. This can help to prevent malware infections by preventing users from running unauthorized applications. However, an application allow list can be difficult to maintain and can block legitimate applications.

Therefore, the best way to protect against an employee inadvertently installing malware on a company system is to use the principle of least privilege. This will help to ensure that users only have the permissions they need to do their job, which will reduce the risk of malware infections.

Here are some additional benefits of least privilege:

It can help to improve security by reducing the attack surface.

It can help to simplify security management by reducing the number of permissions that need to be managed.

It can help to improve compliance by reducing the risk of data breaches.

Petra Martina Vrancic — Today at 11:54 AM

Limiting the access and permissions of employees helps minimize the potential damage they can cause, whether intentional or accidental.

Nita Arapi — Today at 11:54 AM

Least privilege restricts user or system access to the minimum necessary, while an application allow list controls which software is allowed to run.

Question #:56 - (Exam Topic 3)

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

A. MFA

B. Lockout

C. Time-based logins

D. Password history

Answer: A

Explanation

MFA stands for multi-factor authentication, which is a method of verifying a user's identity using two or more factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident.

Lockout Policy: A lockout policy can help prevent unauthorized access by temporarily locking out user accounts after a certain number of unsuccessful login attempts. This can thwart brute-force attacks and deter attackers who have obtained credentials but are trying to guess the password.

Password History: Implementing a password history policy enforces the use of unique passwords over time. Users cannot reuse their previous passwords when changing their credentials. This prevents users from simply reverting to old passwords, which might be known to attackers who have exfiltrated credentials.

Time-based Logins: Time-based logins or session timeouts automatically log users out after a specified period of inactivity. This reduces the risk of unauthorized access in case a user leaves their session open on a shared computer or if their credentials are compromised and someone tries to use them later.

In summary, while all of these policies are important for security, implementing MFA is the most effective measure to prevent unauthorized access using exfiltrated credentials. It adds an additional layer of security beyond passwords, making it significantly more difficult for attackers to gain access even if they have obtained login credentials. However, a combination of these policies can provide a robust defense against credential-based attacks.

References:

https://www.comptia.org/certifications/security

https://www.youtube.com/watch?v=yCJyPPvM-xg

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/

Petra Martina Vrancic — Today at 11:55 AM

adds an extra layer of security by requiring users to provide multiple forms of identification before granting access. Even if credentials are exfiltrated, an additional authentication step would still be needed, preventing unauthorized access.

Question #:57 - (Exam Topic 3)

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would best support the new office?

A. Always-on

B. Remote access

C. Site-to-site

D. Full tunnel

Answer: C

Explanation

Site-to-site VPN allows secure communication between two networks, typically the main office network and the remote office network. This type of VPN provides a direct, secure connection between the two networks, allowing users in the remote office to access resources in the main office, and vice versa. Site-to-site VPN is ideal for connecting two networks that need to communicate with each other on a regular basis, and it can handle a large number of users at the remote site.

Option A, Always On VPN, is a type of VPN that is always active and provides an always-on connection for remote users. This type of VPN is best suited for mobile or remote workers who need to access corporate resources from different locations.

Option B, Remote Access VPN, is a type of VPN that provides secure access for remote users to a corporate network over the internet. This type of VPN is best suited for users who need to access the corporate network from outside the organization's premises.

Option D, Full Tunnel VPN, is a type of VPN that routes all network traffic from the remote user's device through the VPN connection. This type of VPN provides enhanced security, but it can be slow and may not be suitable for a large number of users.

Verified References:

Virtual Private Networks – SY0-601 CompTIA Security+ : 3.3 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/virtual-private-networks-sy0-601- (See Site-to-Site VPN)

VPN Technologies – CompTIA Security+ SY0-501 – 3.2 https://www.professormesser.com/security-plus/sy0-501/vpn-technologies/ (See Site-to-Site VPN)

Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.3: Given a scenario, implement secure network architecture concepts.)

Question #:58 - (Exam Topic 3)

A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192 168 34.26 The Chief Information Security Officer asks the analyst to block the originating source. Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192 168.34 26. Which of the following describes this type of alert?

A. True positive

B. True negative

C. False positive

D. False negative

Answer: C

Explanation

In this scenario, the alert about the IP address 192.168.34.26 being blocked and later reported as a problem with vulnerability scans not being performed properly represents a False Positive.

Here's why:

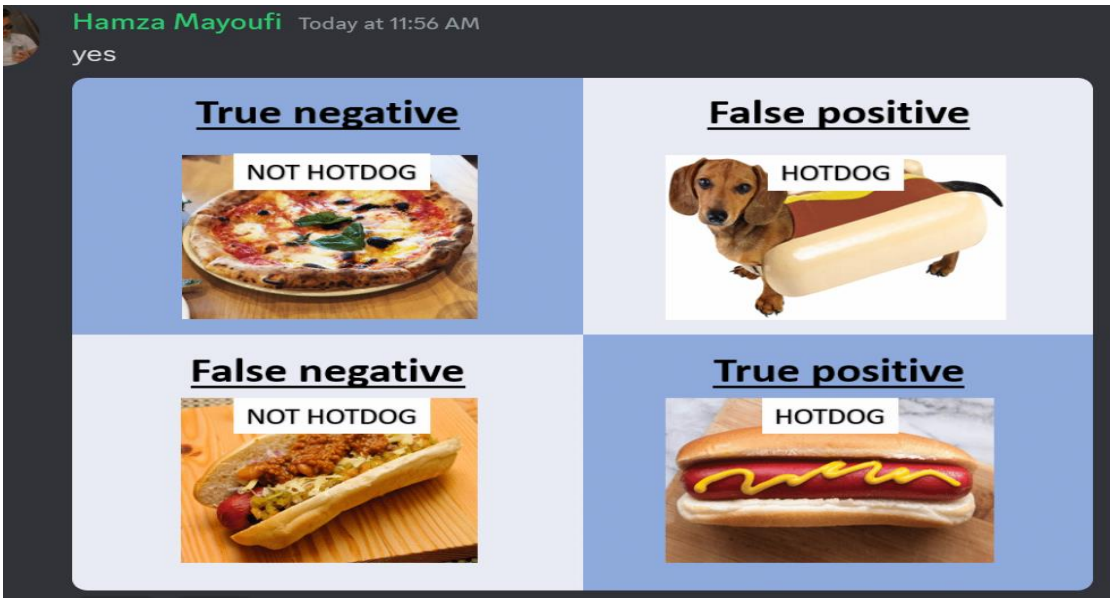
False Positive: A false positive occurs when a security system or alert wrongly identifies normal or benign activity as a security threat. In this case, the initial alert led to blocking the IP address 192.168.34.26, but it turns out that this IP address was being used for legitimate activities (vulnerability scans) within the organization. Therefore, the initial alert was incorrect, making it a false positive.

True Positive: A true positive occurs when a security system correctly identifies and alerts on actual security threats. For example, if the alert correctly detected malicious activity and led to appropriate action, it would be a true positive.

False Negative: A false negative occurs when a security system fails to detect an actual security threat. If the system did not detect the malicious activity but should have, it would be a false negative.

True Negative: A true negative occurs when a security system correctly does not identify a security threat when there is none. It means the system correctly identifies benign or legitimate activity as such.

In this case, the initial alert incorrectly identified benign activity as malicious, leading to the blocking of a legitimate source IP address. This is why it is considered a false positive.



Question #:59 - (Exam Topic 3)

Which Of the following will provide the best physical security countermeasures to Stop intruders? (Select two).

A. Alarm

B. Signage

C. Lighting

D. Access control vestibules

E. Fencing

F. Sensors

Suggested Answer: D E

Explanation

Alarms=deterrent, Signage=deterrent, Lighting=deterrent, Mantraps=physical countermeasure, Fencing=physical

countermeasure and Sensors are either reactive or technical. https://www.professormesser.com/security-plus/sy0-501/physical-security-controls-2/

D: physical security measure that provides a secure entrance to a building by creating an intermediate area between the outside and the inside of the building. This area can be used to control access to the building by requiring visitors to pass through a secure checkpoint before gaining entry. Access control vestibules can prevent unauthorized access and deter intruders from attempting to enter the building.

E: physical security measure that creates a physical barrier around a property, preventing unauthorized access and creating a clear boundary for the property. Fencing can be used to deter intruders from attempting to gain access to the property, and it can also provide a physical barrier that makes it more difficult to breach.

Question #:60 - (Exam Topic 3)

Two organizations are discussing a possible merger. Both organizations' Chief Financial Officers would like to safely share payroll data with each other to determine if the pay scales for different roles are similar at both organizations. Which of the following techniques would be best to protect employee data while allowing the companies to successfully share this information?

A. Pseudo-anonymization

B. Tokenization

C. Data masking

D. Encryption

Answer: C

Explanation

In a situation where two organizations are considering a merger and want to share payroll data while protecting employee data, the best technique to use is C. Data masking.

Here's why:

Pseudo-anonymization involves replacing identifying information with pseudonyms or fake identifiers, but it may not be suitable for this scenario because the CFOs want to compare pay scales for different roles. Pseudo-anonymization might make it challenging to accurately compare data.

Tokenization replaces sensitive data with tokens (random values) but retains a mapping table to convert tokens back to the original data. While it's a useful technique for security, it may not be the best choice here because the CFOs need to perform direct data comparisons, and tokenization can add complexity.

Data masking involves replacing sensitive data with fictitious or scrambled information while preserving the data's format and relationships. This technique allows for data comparisons while protecting sensitive employee information. It's a suitable choice for sharing data in a merger scenario without exposing sensitive details.

Encryption is a security measure that converts data into a coded form that can only be decrypted with the appropriate keys. While encryption is excellent for data security, it might not be ideal for this scenario because it doesn't allow direct data comparisons without decryption, which could introduce complexity and risk.

Question #:61 - (Exam Topic 3)

A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors of real-world events in order to improve the incident response team's process. Which of the following is the analyst most likely participating in?

A. MITRE ATT&CK

B. Walk-through

C. Red team

D. Purple team-I

E. TAXI

Answer: A

Explanation

MITRE ATT&CK is a knowledge base and framework that analyzes and categorizes threat actors and real-world events based on their tactics, techniques and procedures. It can help improve the incident response team's process by providing a common language and reference for identifying, understanding and mitigating threats

The security analyst is most likely participating in an evaluation process related to MITRE ATT&CK.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base and framework that categorizes and describes various tactics, techniques, and procedures (TTPs) used by threat actors during cyberattacks. It is a valuable resource for understanding and analyzing real-world threat actor behavior and tactics.

In the context of incident response and cybersecurity, organizations often use MITRE ATT&CK to:

Improve Incident Response: By understanding how threat actors operate and the techniques they use, incident response teams can better prepare for and respond to security incidents.

Enhance Security Posture: Organizations can use MITRE ATT&CK to identify potential weaknesses in their defenses and take proactive measures to mitigate risks.

Evaluate Security Solutions: MITRE ATT&CK can be used to test and evaluate security tools and solutions by simulating attack scenarios based on real-world threat actor behavior.

While other activities like red teaming and purple teaming involve testing and evaluating security defenses, MITRE ATT&CK specifically focuses on cataloging and categorizing threat actor behavior and techniques, making it a valuable resource for incident response and cybersecurity improvement efforts.

Question #:62 - (Exam Topic 3)

A local server recently crashed, and the team is attempting to restore the server from a backup. During the restore process, the team notices the file size of each daily backup is large and will run out of space at the current rate.

The current solution appears to do a full backup every night. Which of the following would use the least amount of storage space for backups?

A. A weekly, incremental backup with daily differential backups

B. A weekly, full backup with daily snapshot backups

C. A weekly, full backup with daily differential backups

D. A weekly, full backup with daily incremental backups

Answer: D

Explanation

A weekly, full backup with daily incremental backups would use the least amount of storage space for backups, as it would only store the changes made since the last backup, whether it is a full or incremental backup. Incremental backups are faster and use less storage space than full or differential backups, but they require more time and media to restore data. A full backup is a complete copy of all data, which requires more time and storage space to perform, but allows a faster and easier recovery. A differential backup is a copy of the data that changed since the last full backup, which requires less time and storage space than a full backup, but more than an incremental backup. A differential backup allows a faster recovery than an incremental backup, but slower than a full backup. References:

https://www.techtarget.com/searchdatabackup/feature/Full-incremental-or-differential-How-to-choose-the

https://www.nakivo.com/blog/backup-types-explained/

	Full	Incremental	Differential
Storage Consumption	Max	Significantly lower	Min
Data Integrity	Max	Min	Average
Time Consumption	Max	Significantly lower	Min
Recovering Time	Average	Max	Min
Database Friendly	Yes	No	Yes
Preferred Frequency	Moderate	Up to max	Significantly higher

Question #:63 - (Exam Topic 3)

Which of the following is the best method for ensuring non-repudiation?

A. SSO

B. Digital certificate

C. Token

D. SSH key

Answer: B

Explanation

Digital certificates, especially in the context of public key infrastructure (PKI), are specifically designed to provide non-repudiation. Digital certificates are issued by trusted certificate authorities and bind a user's or device's identity to a public key. When a user or device signs a document or message using their private key (which corresponds to the public key in their certificate), it provides strong evidence of their identity. The recipient can verify the signature using the public key in the sender's certificate and be assured of the sender's identity. This makes it difficult for the sender to deny that they sent the message or signed the document, ensuring non-repudiation.

Single Sign-On (SSO): SSO is primarily used for providing convenient and secure access to multiple services with a single set of credentials. While it can enhance security, it is not primarily designed for ensuring non-repudiation. SSO focuses more on authentication and access control.

Token: Tokens are often used in multi-factor authentication (MFA) systems to enhance security by requiring something the user knows (password) and something the user has (token). While tokens can improve security, they don't inherently provide non-repudiation on their own.

SSH key: SSH keys are used for secure authentication and encrypted communication between devices but do not

inherently provide non-repudiation. They focus more on authentication and data protection.

In summary, while the other methods listed have their uses in enhancing security, digital certificates, especially in the context of PKI, are specifically designed to provide non-repudiation and are widely used for this purpose in various applications, including digital signatures and secure communication

Petra Martina Vrancic

—

Today at 12:39 PM

Digital signatures, which are often based on digital certificates, play a crucial role in non-repudiation by providing proof of the origin and integrity of a message or transaction

Question #:64 - (Exam Topic 3)

A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would best support the policy?

A. Mobile device management ///MDM

B. Full device encryption

C. Remote wipe

D. Biometrics

Answer: A

Explanation

For a comprehensive solution to protect company information on user devices in a BYOD (Bring Your Own Device) policy, the best approach is to implement a combination of these security measures, but if you had to choose one solution that best supports the policy, it would be Mobile Device Management (MDM).

Here's why:

Mobile Device Management (MDM): MDM solutions are designed to manage and secure mobile devices, including smartphones, tablets, and sometimes laptops. They provide a centralized platform for IT administrators to enforce security policies, control access, and manage devices remotely. MDM allows you to:

Enforce device encryption: Many MDM solutions enable you to enforce full device encryption as part of your security policy.

Implement remote wipe: MDM allows for remote wiping of company data from devices that are lost, stolen, or when an employee leaves the company, ensuring that sensitive information doesn't fall into the wrong hands.

Enforce security policies: MDM lets you enforce policies such as password requirements, app whitelisting/blacklisting, and device patch management.

Monitor device health: It allows IT teams to monitor the health and security status of devices, including detecting and responding to potential threats.

Full Device Encryption: Full device encryption is an essential component of mobile security, but it is typically just one aspect of what an MDM solution can provide. MDM allows you to enforce encryption and manage it across a fleet of devices.

Remote Wipe: Remote wipe is an important feature, and it can be implemented through MDM solutions. However, MDM offers a broader range of security features beyond just remote wipe.

Biometrics: Biometrics like fingerprint recognition or facial recognition can enhance device security, but they are typically used in conjunction with other security measures, such as device encryption and MDM.

In a BYOD policy, where employees use their own devices, MDM is crucial because it provides comprehensive control and management capabilities over these devices, ensuring that company information is protected, security policies are enforced, and the company can take action in case of device loss or compromise. It complements other security measures like full device encryption and remote wipe, making it the best choice to support the policy.

Question #:65 - (Exam Topic 3)

A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

A. SFTP

B. AIS

C. Tor ///// The Onion Router

D. loC

Answer: C

Explanation

The network that the security analyst should monitor for traffic initiated to the dark web is Tor (The Onion Router).

Tor (The Onion Router): Tor is a network that anonymizes internet traffic by routing it through a series of volunteer-operated servers, making it difficult to trace the source and destination of the traffic. The dark web often relies on Tor to provide anonymity to users and websites. Monitoring Tor traffic is essential for organizations to detect and prevent potentially malicious activities related to the dark web.

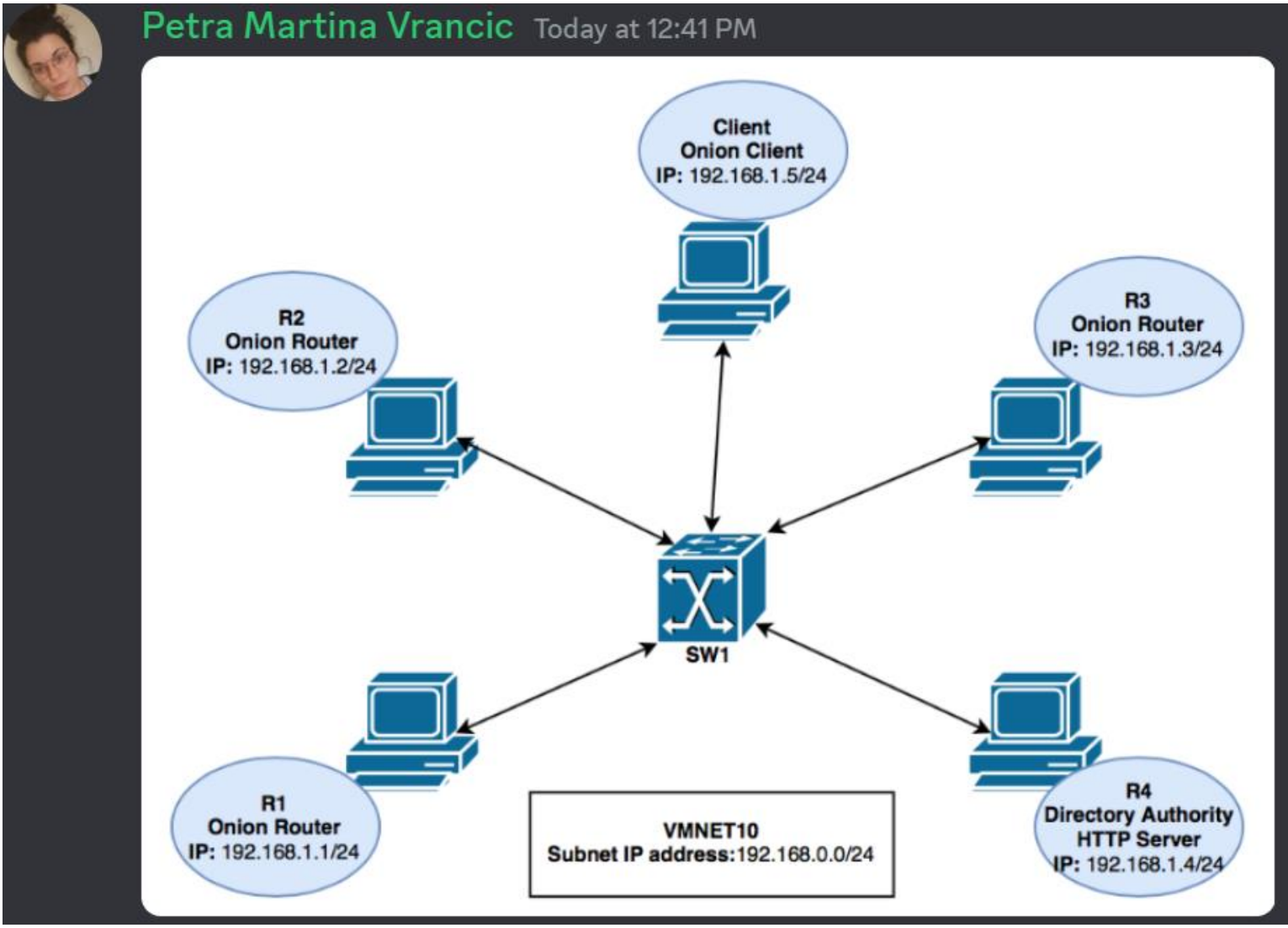
SFTP (Secure File Transfer Protocol): SFTP is a secure method for transferring files, typically over SSH (Secure Shell). It is not a network but a protocol used for securely transferring files. While it is important to monitor file transfer activities for security purposes, it is not directly related to dark web monitoring.

AIS (Automatic Identification System): AIS is a tracking system used for identifying and tracking ships at sea. It is not related to monitoring the dark web from a corporate LAN.

IoC (Indicators of Compromise): IoC refers to specific pieces of information that may indicate a security breach or compromise, such as IP addresses, domains, or file hashes. While monitoring IoCs is important for detecting security incidents, it does not directly relate to monitoring traffic to the dark web.

In summary, the analyst should monitor Tor traffic to identify and investigate any attempts to access the dark web from the corporate LAN, as this is the network commonly used for anonymous access to such hidden online resources.

tor (The Onion Router) is a network that enables anonymous communication on the internet. It's often used to access websites on the dark web. If a security analyst is concerned about traffic initiated to the dark web from the corporate LAN, they should monitor the Tor network to detect any Tor-related traffic originating from within the corporate network. Monitoring Tor traffic can help organizations identify potential security risks or policy violations associated with accessing the dark web.



Question #:66 - (Exam Topic 3)

An audit report indicates multiple suspicious attempts to access company resources were made. These attempts were not detected by the company. Which of the following would be the best solution to implement on the company's network?

A. Intrusion prevention system// IPS

B. Proxy server

C. Jump server

D. Security zones

Answer: A

Explanation

The best solution to implement on the company's network to address the issue of multiple suspicious attempts to access company resources that were not detected is an Intrusion Prevention System (IPS).

Here's why an IPS is the most appropriate choice:

Intrusion Prevention System (IPS): An IPS is a network security appliance or software that actively monitors network traffic for malicious activity or policy violations. It can detect and block suspicious or unauthorized access attempts in real-time. When it identifies such activity, it can take automated actions to prevent the intrusion, such as blocking the IP address or signature associated with the attack.

Benefits:

Real-time detection and prevention: An IPS actively inspects network traffic and can block suspicious attempts as they happen, minimizing potential damage.

Signature-based and behavioral analysis: IPS systems use a combination of known attack signatures and behavioral analysis to detect both known and unknown threats.

Policy enforcement: IPS can enforce network security policies and rules to ensure compliance and prevent unauthorized access.

Granular control: It can provide detailed logs and reports for post-incident analysis and reporting.

Proxy Server: While a proxy server can provide some security benefits by acting as an intermediary between internal users and external resources, it may not be as effective as an IPS at detecting and preventing suspicious access attempts. Proxy servers are often used for content filtering and caching but may not have the same level of real-time intrusion detection and prevention capabilities as an IPS.

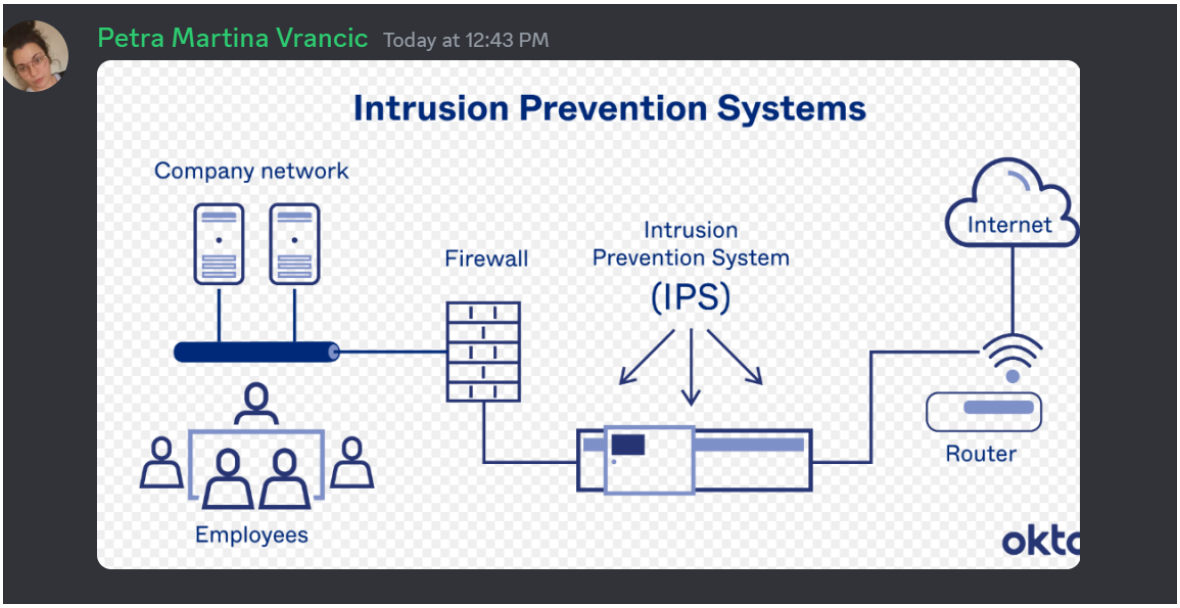
Jump Server: A jump server (also known as a bastion host) is used to secure remote access to internal resources. While it can enhance security by limiting direct access to critical systems, it may not be sufficient for monitoring and preventing suspicious access attempts across the entire network.

Security Zones: Security zones are a network segmentation technique used to isolate different parts of the network based on security requirements. While they are important for controlling and limiting access, they may not provide real-time intrusion detection and prevention capabilities on their own.

In summary, an Intrusion Prevention System (IPS) is the most suitable solution for detecting and preventing suspicious access attempts in real-time, making it an essential component of a comprehensive network security strategy to address the issue described in the audit report.

https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips



Question #:67 - (Exam Topic 3)

A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avoid managing a password for authentication and additional software installation. Which of the following should the architect recommend?

A. Soft token

B. Smart card

C. CSR

D. SSH key

Answer: D

Explanation

For a remote access solution to a Linux server where the business partner wants to avoid managing a password for authentication and additional software installation, the security architect should recommend using an SSH key.

Here's why SSH key authentication is a suitable recommendation:

SSH Key: SSH (Secure Shell) key pairs consist of a private key and a public key. The public key is placed on the server, and the private key is kept secure by the user. When the business partner tries to access the Linux server, the server checks if the presented public key matches the corresponding private key. If they match, authentication is successful, and access is granted.

Advantages:

No password management: Since SSH key authentication doesn't require a password, the business partner doesn't need to remember or manage a password for authentication.

Secure: SSH key authentication is considered highly secure because it relies on strong asymmetric cryptography.

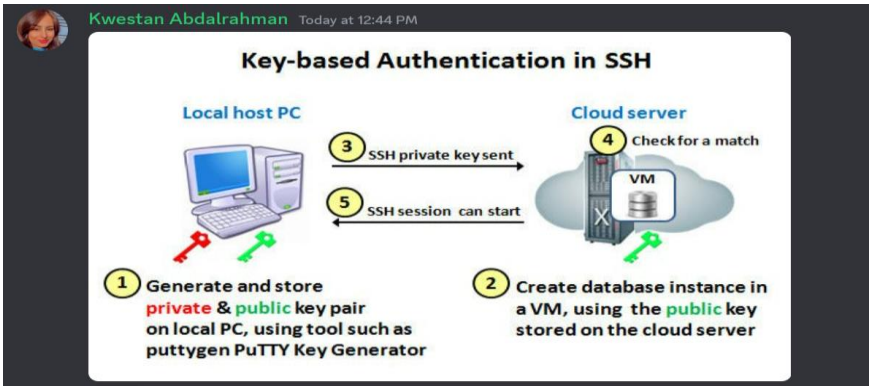
Minimal software installation: SSH key pairs are typically supported by default on most Linux distributions and do not require additional software installation on the client side.

Strong access control: You can control which public keys are allowed to access the server, providing fine-grained access control.

Soft Token and Smart Card: Soft tokens and smart cards are also used for secure authentication, but they often require additional software installation and may involve some level of password management or PIN entry. While they can be secure authentication methods, they might not align with the partner's preference to avoid additional software installation and password management.

CSR (Certificate Signing Request): A CSR is a request for a digital certificate, typically used in the context of SSL/TLS certificates for securing web services. It is not directly related to SSH key authentication for remote access to a Linux server.

In summary, SSH key authentication is a straightforward and secure solution that aligns with the business partner's requirements of avoiding password management and additional software installation. It is a widely accepted and used method for securing remote access to Linux servers.



Question #:68 - (Exam Topic 3)

Which of the following threat actors is most likely to be motivated by ideology?

A. Business competitor

B. Hacktivist

C. Criminal syndicate

D. Script kiddie

E. Disgruntled employee

Answer: B

Explanation

A hacktivist is a threat actor who is most likely to be motivated by ideology. A hacktivist is a person or group who uses hacking skills and techniques to promote a political or social cause. Hacktivists may target government, corporate, or religious entities that they disagree with or oppose. Hacktivists may use various methods to achieve their goals, such as defacing websites, leaking sensitive data, launching denial-of-service attacks, or spreading propaganda. Hacktivists are not motivated by financial gain or personal benefit, but rather by their beliefs and values. References:

https://www.uscybersecurity.net/hacktivist/

https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

Question #:69 - (Exam Topic 3)

A building manager is concerned about people going in and out of the office during non-working hours.

Which of the following physical security controls would provide the best solution?

A. Cameras

B. Badges

C. Locks

D. Bollards

Answer: B

Explanation

Badges are physical security controls that provide a way to identify and authenticate authorized individuals who need to access a building or a restricted area. Badges can also be used to track the entry and exit times of people and monitor their movements within the premises. Badges can help deter unauthorized access by requiring people to present a valid credential before entering or leaving the office. Badges can also help prevent tailgating, which is when an unauthorized person follows an authorized person through a door or gate. Badges can be integrated with other security systems, such as locks, alarms, cameras, or biometrics, to enhance the level of protection.

Question #:70 - (Exam Topic 3)

A cyber-security administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive. All connections are being dropped by the firewall. Which of the following would be the best option to remove the rules?

A. # iptables -t mangle -X

B. # iptables -F

C. # iptables -2

D. # iptables -P INPUT -j DROP

Answer: B

Explanation

iptables is a command-line tool that allows an administrator to configure firewall rules for a Linux system.

The -F option flushes or deletes all the existing rules in the selected chain or in all chains if none is given. It can be used to remove the rules that caused the network to be unresponsive and restore the default firewall behavior.

-F — Flushes the selected chain, which effectively deletes every rule in the chain. If no chain is specified, this command flushes every rule from every chain.

Z — Zeros the byte and packet counters in all chains for a table.

-t — Specifies a table name.

-X — Deletes a user-specified chain. Deleting a built-in chain for any table is not allowed.

-p — Sets the IP protocol for the rule, which can be either icmp, tcp, udp, or all, to match every supported protocol. In addition, any protocols listed in /etc/protocols may also be used. If this option is omitted when creating a rule, the all option is the default.

-j — Jumps to the specified target when a packet matches a particular rule. Valid targets to use after the -j option include standard options (ACCEPT, DROP, QUEUE, and RETURN) as well as extended options that are available through modules loaded by default with the Red Hat Enterprise Linux iptables RPM package, such as LOG, MARK, and REJECT, among others. Refer to the iptables man page for more information about these and other targets.

Petra Martina Vrancic — Today at 12:47 PM

This command flushes all the rules in the filter table, which is typically used for managing packet filtering rules. It's a quick way to reset the firewall rules without removing the tables or chains.

Question #:71 - (Exam Topic 3)

A web architect would like to move a company's website presence to the cloud. One of the management team's key concerns is resiliency in case a cloud provider's data center or network connection goes down. Which of the following should the web architect consider to address this concern?

A. Containers

B. Virtual private cloud

C. Segmentation

D. Availability zones

Answer: D

Explanation

Availability zones are the most appropriate cloud feature to address the concern of resiliency in case a cloud provider's data center or network connection goes down. Availability zones are physically separate locations within an Azure region that have independent power, cooling, and networking. Each availability zone is made up of one or more data centers and houses infrastructure to support highly available, mission-critical applications. Availability zones are connected with high-speed, private fiber-optic networks. Azure services that support availability zones fall into two categories: Zonal services – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses), or Zone-redundant services – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database). To achieve comprehensive business continuity on Azure, build your application architecture using the combination of availability zones with Azure region pairs. You can synchronously replicate your applications and data using availability zones within an Azure region for high-availability and asynchronously replicate across Azure regions for disaster recovery protection.

Question #:72 - (Exam Topic 3)

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

A. Security information and event management /////SIEM

B. A web application firewall

C. A vulnerability scanner

D. A next-generation firewall

Answer: A

Explanation

Security information and event management (SIEM) is a solution that collects, analyzes, and correlates logs and events from various sources such as firewalls, servers, applications, etc., within an organization's network. It can centralize logs to create a baseline and have visibility on security events by providing a unified dashboard and reporting system for log management and security monitoring.

Question #:73 - (Exam Topic 3)

A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash. Which of the following is the next step according to the incident response process?

A. Recovery

B. Lessons learned

C. Containment

D. Preparation

Answer: C

Explanation

Containment is the next step according to the incident response process after identifying affected devices that are running a malicious application with a unique hash. Containment involves isolating the compromised devices or systems from the rest of the network to prevent the spread of the attack and limit its impact.
Containment can be done by disconnecting the devices from the network, blocking network traffic to or from them, or applying firewall rules or access control lists. Containment is a critical step in incident response because it helps to preserve evidence for further analysis and remediation, and reduces the risk of data loss or exfiltration

https://www.fortinet.com/resources/cyberglossary/incident-response

https://www.ibm.com/topics/incident-response

Question #:74 - (Exam Topic 3)

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy

Which of the following is The router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion

Answer: D

Explanation

The router is experiencing a resource exhaustion issue. The output from the command indicates that the CPU is consistently busy, with a 1-second average of 99 percent busy and a 1-minute average of 83 percent busy. This indicates that the router is struggling to keep up with the demands placed on it, potentially due to a high volume of traffic or other factors. As a result, web pages are experiencing long load times. This is an example of resource exhaustion, where the router's resources are being overwhelmed and are unable to meet the demands placed on them. A DDoS attack, memory

leak, or buffer overflow would not typically cause the symptoms described in the scenario.

Question #:75 - (Exam Topic 3)

Which of the following is constantly scanned by internet bots and has the highest risk of attack in the case of the default configurations?

A. Wearable sensors

B. Raspberry Pi

C. Surveillance systems

D. Real-time operating systems

Answer: C

Explanation

Surveillance systems are constantly scanned by internet bots and have the highest risk of attack in the case of the default configurations because they are often connected to the internet and use weak or default passwords that can be easily guessed or cracked by malicious bots. Internet bots are software applications that run automated tasks over the internet, usually with the intent to imitate human activity or exploit vulnerabilities.

Some bots are used for legitimate purposes, such as web crawling or indexing, but others are used for malicious purposes, such as spamming, phishing, denial-of-service attacks, or credential stuffing. Security misconfigurations are one of the most common gaps that criminal hackers look to exploit. Therefore, it is important to secure the configuration of surveillance systems by changing the default passwords, updating the firmware, disabling unnecessary services, and enabling encryption and authentication.

https://www.cctvcameraworld.com/setup-ip-camera-system-on-network/

What is the meaning of surveillance system?

Surveillance system means a system of video cameras, monitors, recorders, and other equipment used for surveillance

Question #:76 - (Exam Topic 3)

A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The file share is located in a local data center. Which of the following should the security architect recommend to best meet the requirement?

A. Fog computing and KVMs ///Keyboard, Video, Mouse switches

B. VDI and thin clients

C. Private cloud and DLP

D. Full drive encryption and thick clients

Answer: B

Explanation

VDI and thin clients are the best solution to deploy to conference rooms for displaying sensitive data on large screens. VDI stands for virtual desktop infrastructure, which is a technology that hosts the desktop operating systems and applications on a central server or cloud and allows users to access them remotely. Thin clients are devices that have minimal hardware and software components and rely on a network connection to the VDI system. By using VDI and thin clients, the security architect can ensure that the sensitive data is not stored in the conference rooms, but rather in a secure data center or cloud. The thin clients can also be easily managed and updated centrally, reducing the maintenance costs and risks.

Fog computing and KVMs (Keyboard, Video, Mouse switches): While KVMs can help switch between local and remote systems, fog computing typically involves processing data at the edge of the network. It doesn't inherently centralize data storage, which is a requirement in this scenario.

Private cloud and DLP (Data Loss Prevention): While a private cloud could provide centralized computing resources, it doesn't inherently solve the problem of sensitive data storage in the conference rooms. DLP is a data protection measure but is not a replacement for data centralization.

Full drive encryption and thick clients: Full drive encryption can help protect data on local devices, but it doesn't centralize data storage. Thick clients typically store data locally, which would not meet the requirement of not storing sensitive data in the conference rooms.

References:

https://www.acecloudhosting.com/blog/what-is-vdi-thin-client/

https://www.parallels.com/blogs/ras/vdi-thin-client/

Question #:77 - (Exam Topic 3)

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the most acceptable?

A. SED

B. HSM

C. DLP

D. TPM

Answer: A

Explanation

SED stands for Self-Encrypting Drive, which is a type of hard drive that automatically encrypts and decrypts data using a built-in hardware encryption engine. SEDs do not require any additional software or configuration, and they do not affect the performance or usability of the laptop2. SEDs also have a feature called Instant Secure Erase, which allows the user to quickly and securely wipe the data on the drive by deleting the encryption key1.

HSM (Hardware Security Module): HSMs are used for secure key management and cryptographic operations. While they enhance security, they may not directly address data protection on laptop hard drives or reduce user inconvenience.

DLP (Data Loss Prevention): DLP solutions are designed to monitor and prevent the unauthorized transfer or sharing of sensitive data. They are more focused on data leakage prevention and may not provide the same level of protection for data on laptop hard drives.

TPM (Trusted Platform Module): TPM is a hardware component that provides secure storage for cryptographic keys and performs various security functions. While it can enhance overall system security, it may not provide the same level of data encryption and protection as SEDs for laptop hard drives.

Question #:78 - (Exam Topic 3)

Which of the following vulnerabilities is exploited by an attacker to overwrite a register with a malicious address that changes the execution path?

A. VM escape

B. SQL injection

C. Buffer overflow

D. Race condition

Answer: C

Explanation

A buffer overflow is a type of vulnerability that occurs when an attacker sends more data than a buffer can hold, causing the excess data to overwrite adjacent memory locations such as registers. It can allow an attacker to overwrite a register with a malicious address that changes the execution path and executes arbitrary code on the target system

Question #:79 - (Exam Topic 3)

A government organization is developing an advanced AI defense system. Developers are using information collected from third-party providers. Analysts are noticing inconsistencies in the expected performance of the system and attribute the outcome to a recent attack on one of the suppliers. Which of the following IS the most likely reason for the inaccuracy of the system?

A. Improper algorithms security

B. Tainted training data

C. Virus

D. Crypto Malware

Answer: B

Explanation

Tainted training data is a type of data poisoning attack that involves modifying or injecting malicious data into the training dataset of a machine learning or artificial intelligence system. It can cause the system to learn incorrect or biased patterns and produce inaccurate or malicious outcomes. It is the most likely reason for the inaccuracy of the system that is using information collected from third-party providers that have been compromised by an attacker.

Petra Martina Vrancic — Today at 12:59 PM

If the training data used to develop the AI system is compromised or manipulated, it can introduce biases or inaccuracies that impact the system's performance. This could be a result of an attack on one of the suppliers, leading to tainted or malicious data being used in the training process.

Question #:80 - (Exam Topic 3)

Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

A. Persistence

B. Port scanning

C. Privilege escalation

D. Pharming

Answer: C

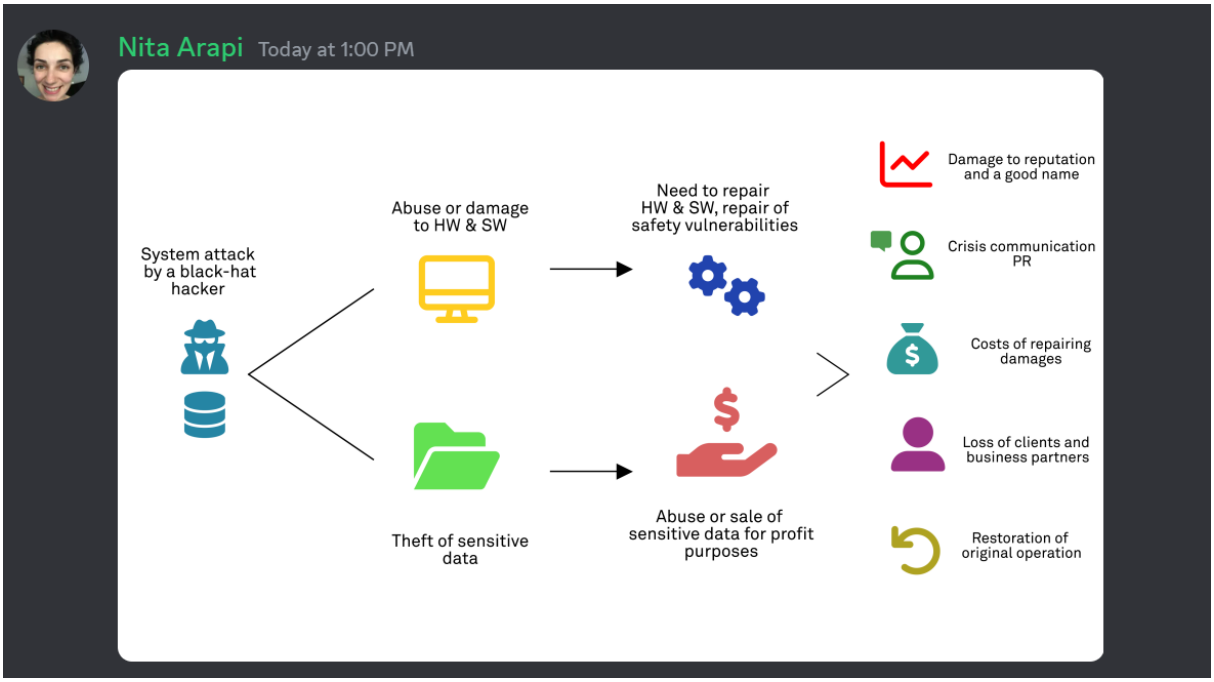
Explanation

Privilege escalation describes the exploitation of an interactive process to gain access to restricted areas. It is a type of attack that allows a normal user to obtain higher privileges or access rights on a system or network, such as administrative or root access. Privilege escalation can be achieved by exploiting a vulnerability, design flaw, or misconfiguration in the system or application. Privilege escalation can allow an attacker to perform unauthorized actions, such as accessing sensitive data, installing malware, or compromising other systems.

References:

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/privilege-escalation-3/

https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-2-secure-code-design-and-im



Question #:81 - (Exam Topic 3)

After multiple on-premises security solutions were migrated to the cloud, the incident response time increased. The analysts are spending a long time trying to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

A. CASB

B. VPC

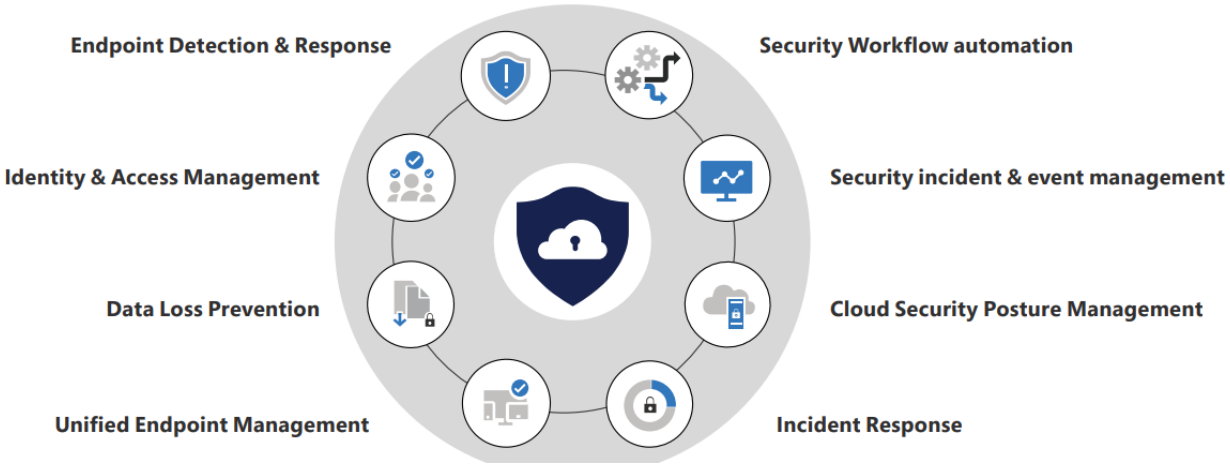
C. SWG

D. CMS

Answer: A

Explanation

4 pillars of CASB security, which are Compliance, Deep Visibility, Data Protection, and Threat Detection. All 4 of these Pillars are required to build a CASB and keep your business data secure.



A content management system (CMS) is software that helps users create, manage, and modify content on a website without the need for technical knowledge. In other words, a CMS lets you build a website without needing to write code from scratch (or even know how to code at all)

Cloud management is the organized management of cloud computing products and services that operate in the cloud. It refers to the processes, strategies, policies, and technology used to help control and maintain public and private cloud, hybrid cloud, or multi cloud environments.

Question #:82 - (Exam Topic 3)

Cloud security engineers are planning to allow and deny access to specific features in order to increase data security. Which of the following cloud features is the most appropriate to ensure access is granted properly?

A. API integrations

B. Auditing

C. Resource policies

D. Virtual networks

Answer: C

Explanation

Resource policies are cloud features that allow and deny access to specific features in order to increase data security. Resource policies are rules or statements that define what actions can be performed on a particular resource by which entities under what conditions. Resource policies can be attached to cloud resources such as virtual machines, storage accounts, databases, or functions. Resource policies can help enforce security best practices, compliance requirements, and cost management. Resource policies can also help implement the principle of least privilege, which grants users only the minimum level of access they need to perform their tasks.

Question #:83 - (Exam Topic 3)

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following best describes this kind of attack?

A. Directory traversal

B. SQL injection

C. API

D. Request forgery

Answer: A

Explanation

Directory traversal is a type of web application attack that involves exploiting a vulnerability in the web server or application to access files or directories that are outside the intended scope or root directory. It can allow an attacker to read, modify, or execute files on the target system by using special characters such as …/ or %2e%2e/ to manipulate the path or URL. In this case, the attacker used …/ to access the /etc/passwd file, which contains user account information on Linux systems.

Question #:84 - (Exam Topic 3)

Which of the following will increase cryptographic security?

A. High data entropy

B. Algorithms that require less computing power

C. Longer key longevity

D. Hashing

Answer: A

Explanation

Data entropy is a measure of the randomness or unpredictability of data. High data entropy means that the data has more variation and less repetition, making it harder to guess or crack. It can increase cryptographic security by making the encryption keys and ciphertext more complex and resistant to brute-force attacks, frequency analysis, etc

Question #:85 - (Exam Topic 3)

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (select two).

A. Something you know

B. Something you have

C. Somewhere you are

D. Someone you know

E. Something you are

F. Something you can do

Answer: A B

Explanation

MFA (Multi-Factor Authentication) is a method of verifying a user's identity by requiring two or more factors or attributes that belong to different categories. The categories are something you know (such as a password or a PIN), something you have (such as a token or a smart card), something you are (such as a fingerprint or an iris scan), something you do (such as a gesture or a voice command), and somewhere you are (such as a location or an IP address). In this case, the user enters a password (something you know) and then receives an authentication code (something you have) to log in to a workstation.

Question #:86 - (Exam Topic 3)

During a security incident, the security operations team identified a sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32

B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0

C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

Explanation

This command creates an inbound access list that denies any IP traffic from the source IP address of 10.1.4.9/32 to any destination IP address (0.0.0.0/0). It blocks the originating source of malicious traffic from accessing the organization's network.

Petra Martina Vrancic

—

Today at 1:08 PM

access-list inbound: This specifies that we are creating an access list named "inbound." deny: This indicates that the rule is designed to deny traffic. ip: This specifies that the rule is for IP traffic. source 10.1.4.9/32: This defines the source IP address as 10.1.4.9 with a subnet mask of /32, meaning a single IP address. destination 0.0.0.0/0: This sets the destination IP address range as 0.0.0.0/0, meaning any destination IP address. So, putting it all together, the rule access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0 says: deny any IP traffic coming from the source IP address 10.1.4.9 to any destination IP address. This effectively blocks traffic from the specified malicious IP address.

Question #:87 - (Exam Topic 3)

A security analyst discovers that a company's username and password database were posted on an internet forum. The usernames and passwords are stored in plaintext. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network.

B. Implement salting and hashing.

C. Configure the web content filter to block access to the forum.

D. Increase password complexity requirements.

Answer: B

Explanation

Salting and hashing are techniques that can improve the security of passwords stored in a database by making them harder to crack or reverse-engineer by hackers who might access the database.

Salting is the process of adding a unique, random string of characters known only to the site to each password before it is hashed2. Hashing is the process of converting a password into a fixed-length string of characters, which cannot be reversed3. Salting and hashing ensure that the encryption process results in a different hash value, even when two passwords are the same1. This makes it more difficult for an attacker to use precomputed tables or dictionaries to guess the passwords, or to exploit duplicate hashes in the database4.

Question #:88 - (Exam Topic 3)

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is most likely the cause?

A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage

B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.

C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.

D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

Explanation

Mimikatz is a tool that can extract plaintext credentials from memory on Windows systems. A malicious flash drive can bypass the GPO blocking the flash drives by using techniques such as autorun.inf or HID spoofing to execute Mimikatz on the target system without user interaction or consent. This can cause AV alerts indicating Mimikatz attempted to run on the remote systems and also reduce the storage capacity of the flash drives to only 512KB by creating hidden partitions or files on them.

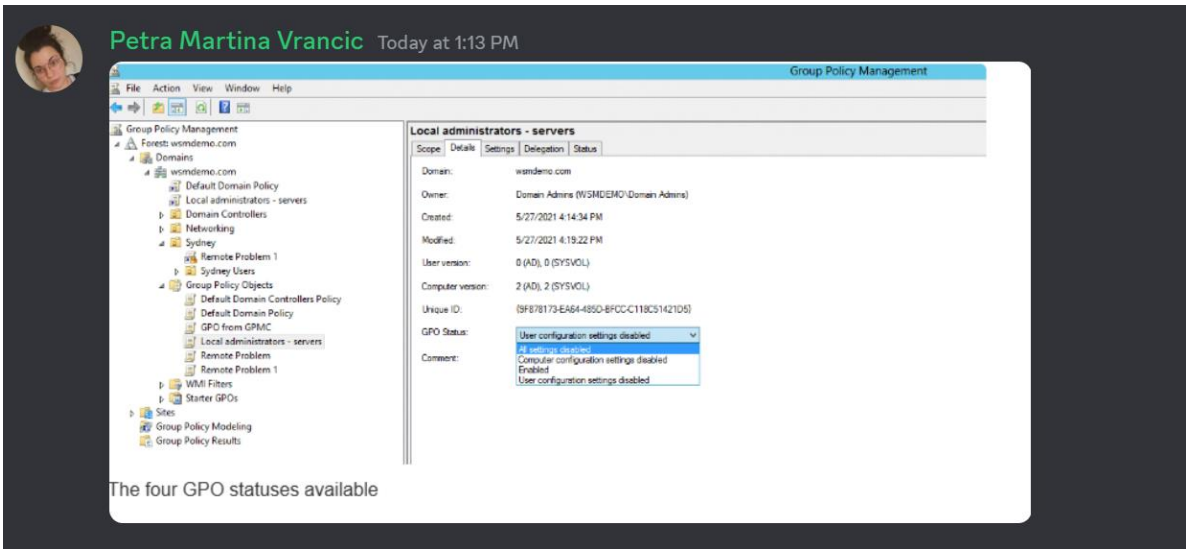
This scenario is the most likely cause of the reported issues, as it explains the AV alerts related to Mimikatz and the limited storage capacity of the new flash drives. It is possible that the malicious flash drive is using Mimikatz to extract credentials from the memory of the remote systems, which would explain the AV alerts.

Additionally, the limited storage capacity of the new flash drives could be a deliberate attempt to make the malicious flash drive less noticeable.

mimikatz gets windows secure pass hash

it is used to pass the hash attack

we can use code signing policy to stop execute Mimikatz



Question #:89 - (Exam Topic 3)

A user received an SMS on a mobile phone that asked for bank details. Which of the following social engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Answer: D

Explanation

Smishing is a type of social engineering technique that involves sending fraudulent or malicious text messages (SMS) to a user's mobile phone. It can trick the user into providing personal or financial information, clicking on malicious links, downloading malware, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity.

Question #:90 - (Exam Topic 3)

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate data center that houses confidential information. There is a firewall at the internet border, followed by a DLP appliance, the VPN server and the data center itself. Which of the following is the weakest design element?

A. The DLP appliance should be integrated into a NGFW.

B. Split-tunnel connections can negatively impact the DLP appliance's performance.

C. Encrypted VPN traffic will not be inspected when entering or leaving the network.

D. Adding two hops in the VPN tunnel may slow down remote connections

Answer: C

Explanation

VPN (Virtual Private Network) traffic is encrypted to protect its confidentiality and integrity over the internet. However, this also means that it cannot be inspected by security devices or tools when entering or leaving the network, unless it is decrypted first. This can create a blind spot or a vulnerability for the network security posture, as malicious traffic or data could bypass detection or prevention mechanisms by using VPN encryption.

- Encrypted Traffic Bypass: If the VPN traffic is encrypted and not being inspected, it creates a potential blind spot for security. Encrypted traffic could contain malicious content or could be used for data exfiltration, and without inspection, the organization may not detect these threats.
- Security Risks: Not inspecting encrypted traffic is a security risk as it bypasses the Data Loss Prevention (DLP) appliance and other security measures. Attackers can take advantage of this to hide their activities.
- Data Protection: In environments with confidential information, it's essential to inspect all traffic, including encrypted traffic, to ensure that sensitive data is not leaving the network without proper authorization.

A: The DLP appliance should be integrated into a NGFW (Next-Generation Firewall):

Integrating DLP into a NGFW is generally a good security practice. It allows for deeper inspection of network traffic and can enhance data loss prevention capabilities. This is not a design weakness but rather a security enhancement.

B: Split-tunnel connections can negatively impact the DLP appliance's performance:

Split-tunneling refers to a configuration where only specific traffic is sent through the VPN, while other traffic goes directly to the internet. While split-tunneling can impact DLP performance, it is often necessary to avoid routing all internet traffic through the VPN, which can lead to performance issues and increase the load on the VPN server. It's more of a trade-off between security and performance rather than a design weakness.

D:Adding two hops in the VPN tunnel may slow down remote connections

Adding hops in the VPN tunnel, such as multiple VPN gateways or intermediate nodes, can indeed introduce additional latency and potentially slow down remote connections. However, this is not necessarily a design weakness, but rather a consideration that needs to be balanced with the need for security and network optimization. The trade-off between security and performance should be carefully evaluated.

Question #:91 - (Exam Topic 3)

To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would best accommodate the request?

A. laaS

B. PaaS

C. DaaS

D. SaaS

Answer: D

Explanation

SaaS (Software as a Service) is a cloud service model that allows organizations to access and use software applications over the internet, without having to maintain or support the underlying infrastructure. SaaS providers are responsible for maintaining and updating the software and infrastructure, which can help to reduce and limit software and infrastructure costs. In the case of email services, a SaaS provider would host and manage the email system, including security controls to protect sensitive data.
IaaS (Infrastructure as a Service) provides virtualized computing resources over the internet, it doesn't cover email services.
PaaS (Platform as a Service) provides a platform for the development, running and management of applications, it doesn't cover email services.
DaaS (Desktop as a Service) provides virtualized desktop environments, it doesn't cover email services.

Question #:92 - (Exam Topic 3)

Which of the following would be used to find the most common web-application vulnerabilities?

A. OWASP

B. MITRE ATT&CK

C. Cyber Kill Chain

D. SDLC

Answer: A

Explanation

OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for

improving the security of web applications. It publishes a list of the most common web application vulnerabilities, such as injection, broken authentication, cross-site scripting, etc., and provides recommendations and best practices for preventing and mitigating them

Question #:93 - (Exam Topic 3)

A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security team has been instructed to resolve the problem as quickly as possible causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?

A. Update the host firewalls to block outbound SMB.
B. Place the machines with the unapproved software in containment.
C. Place the unauthorized application in a blocklist.
D. Implement a content filter to block the unauthorized software communication.

Answer: B

B: Placing the machines with the unauthorized software in containment is the best course of action in this scenario, as it will prevent the software from communicating with other machines in the lab and on the Internet, while minimizing disruption to the researchers.

This can be done by disconnecting the affected machines from the network, or by using software-based containment solutions that restrict the software's access to network resources.

A: helps to block the app from accessing the internet, so it can help, but doesn't resolve the issue.

C: does not resolve the problem, it just hopefully prevents it in the future.

D: doesn't really apply

It allows the security team to investigate and remediate the issue without causing disruption to the entire network.

Question #:94 - (Exam Topic 3)

Which of the following are common VoIP-associated vulnerabilities? (Select two).

A. SPIM
B. Vishing
C. VLAN hopping
D. Phishing
E. DHCP snooping
F. Tailgating

Answer: A B

Explanation

SPIM (Spam over Internet Messaging) is a type of VoIP-associated vulnerability that involves sending unsolicited or fraudulent messages over an internet messaging service, such as Skype or WhatsApp. It can trick users into clicking on malicious links, downloading malware, providing personal or financial information, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity. Vishing (Voice Phishing) is a type of VoIP-associated vulnerability that involves making unsolicited or fraudulent phone calls over an internet telephony service, such as Google Voice or Vonage. It can trick users into disclosing personal or financial information, following malicious instructions, transferring money, etc., by using voice spoofing, caller ID spoofing, or interactive voice response systems.

Question #:95 - (Exam Topic 3)

Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

A. A right-to-audit clause allowing for annual security audits

B. Requirements for event logs to be kept for minimum of 30 days

C. Integration of threat intelligence in the company's AV

D. A data-breach clause requiring disclosure of significant data loss

Answer: A

Explanation

Including a right-to-audit clause in a contract would allow the company to monitor the ongoing security maturity of a new vendor. This clause would grant the company the right to conduct annual security audits of the vendor's security controls and procedures to ensure they meet the company's requirements. By having this clause in the contract, the company can ensure that the vendor maintains a minimum level of security and compliance with relevant regulations and standards.

B: Requirements for event logs to be kept for a minimum of 30 days would be more appropriate for ensuring the vendor's compliance with data retention policies and for forensic investigations after a security incident.

C: Integration of threat intelligence in the company's AV and

D: A data-breach clause requiring disclosure of significant data loss are also important for a comprehensive security program, but they do not directly relate to monitoring the ongoing security maturity of a new vendor.

Question #:96 - (Exam Topic 3)

An organization has hired a red team to simulate attacks on its security posture. Which of the following will the blue team do after detecting an IOC?

A. Reimage the impacted workstations.

B. Activate runbooks for incident response.

C. Conduct forensics on the compromised system,

D. Conduct passive reconnaissance to gather information

Answer: B

The purpose of runbooks is to have a systematic, documented, and repeatable process to respond to security incidents.

A runbook is a set of predefined procedures and steps that guide an incident response team through the process of handling a security incident. It can help the blue team respond quickly and effectively to an indicator of compromise (IOC) by following the best practices and predefined actions for containment, eradication, recovery and lessons learned.

After detecting an Indicator of Compromise (IoC), the blue team will activate runbooks for incident response.

The blue team will use the runbooks to assess the scope of the attack, contain it, and minimize damage. The runbooks will also help the blue team collect and preserve evidence, perform root cause analysis, and restore normal operations. The blue team will take the information gathered from the runbooks and use it to improve the organization's security posture.

Question #:97 - (Exam Topic 3)

A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send the file to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

A. SMIME

B. LDAPS

C. SSH

D. SRTP

Answer: C

Explanation

SSH: is a protocol that enables two computers to communicate securely by encrypting the connection. Since the question is looking to transfer files over the internet to a specific directory, the FTP protocol can be used for the file transfer itself. As SSH can be used with the FTP protocol, this allows for secure(SSH) file transfer(FTP) over the internet.

S/MIME (Secure/Multipurpose internet Mail Extensions) - Digitally signs and encrypts the contents of email messages.

LDAPS(Lightweight Directory Access Protocol) - Provides authentication for directory-based traffic

SRTP (Secure Real-time Transport Protocol) - Provides authentication/encryption for transmitted audio and video traffic.

Question #:98 - (Exam Topic 3)

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705 "http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705 "http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705 "http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705 "http://www.example.com/login.php"

106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705 "http://umw.example.com/login.php"

Which of the following password attacks is taking place?

A. Dictionary

B. Brute-force

C. Rainbow table

D. Spraying

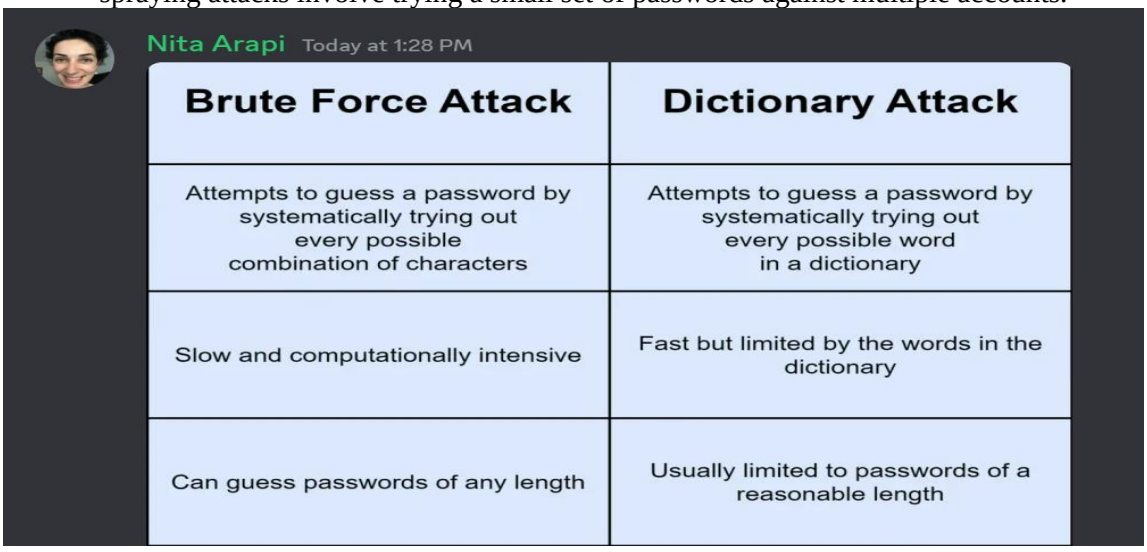
Answer: B

Explanation

Brute-force:

- Sequential PIN Attempts: In each log entry, the attacker is making sequential requests to the login page with a username of "admin" and a different PIN number (e.g., "0000," "0001," "0002," etc.). This pattern suggests that the attacker is systematically trying a range of possible PINs in a sequential manner.
- No Patterns or Reuse: Unlike a dictionary attack where commonly used passwords or words are tried, or a rainbow table attack where precomputed hashes are used to find corresponding passwords, this attack involves trying all possible PIN combinations, which is characteristic of a brute-force attack.
- Repetitive Access: The attacker is repeatedly making requests to the login page with different PINs for the same username, "admin." This behavior aligns with the brute-force attack method of trying all possible combinations until the correct one is found.

- Dictionary Attack: In a dictionary attack, an attacker tries a large number of passwords from a predefined list (dictionary).
- Rainbow Table Attack: In a rainbow table attack, an attacker uses precomputed tables (rainbow tables) to look up password hashes and find corresponding passwords. It's efficient for cracking hashed passwords but does not involve sequentially trying different values like the log entries show.
- Spraying Attack: A spraying attack is when an attacker attempts to access multiple accounts using a few common passwords or PINs. Unlike the log entries, where the attacker is trying sequential PINs for the same account ("admin"), spraying attacks involve trying a small set of passwords against multiple accounts.



Question #:99 - (Exam Topic 3)

A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.
INSTRUCTIONS

Please click on the below items on the network diagram and configure them accordingly:

WAP

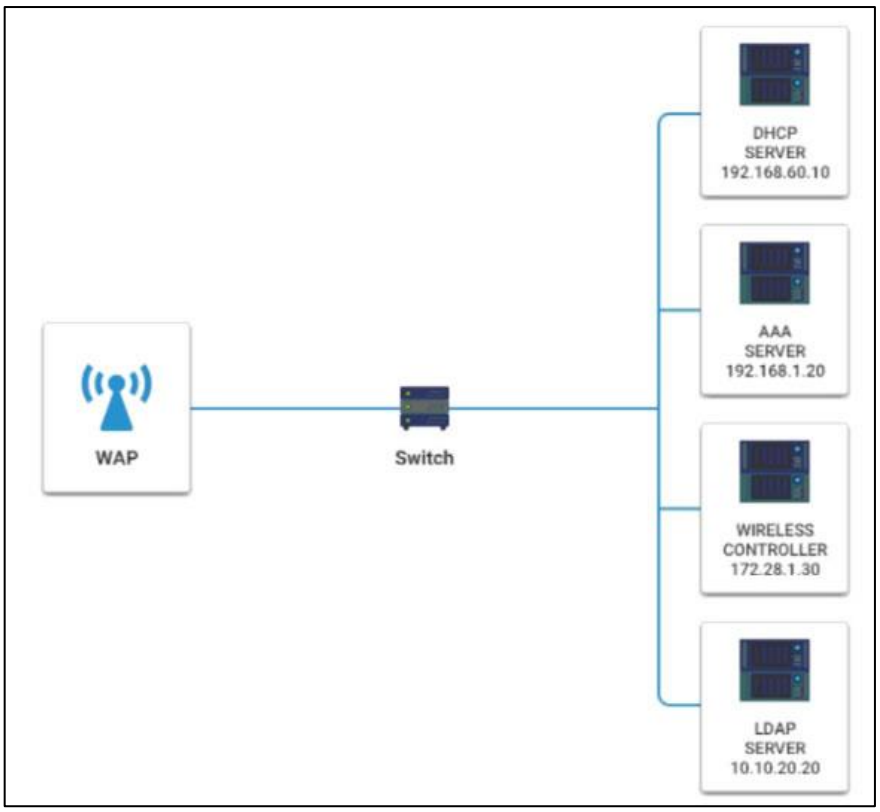
DHCP Server

AAA Server

Wireless Controller

LDAP Server

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



DHCP SERVER

IP	192.168.60.10
NETMASK	255.255.255.0
DG	192.168.60.1
Range	10.50.7.0-10.50.8.255
DNS Servers	192.168.30.4, 192.168.40.4
Reserved	A1-27-CA-23-45-76-E3 10.50.7.5
Reserved	B3-47-A3-18-E7-7D-E2 10.50.7.6
Domain	corporatenet
Port	67

AAA SERVER

IP	192.1681.20
NETMASK	255.255.255.0
DG	192.168.1.1
Secret	corporatenet
Realm	wirelessnet
Port	1812

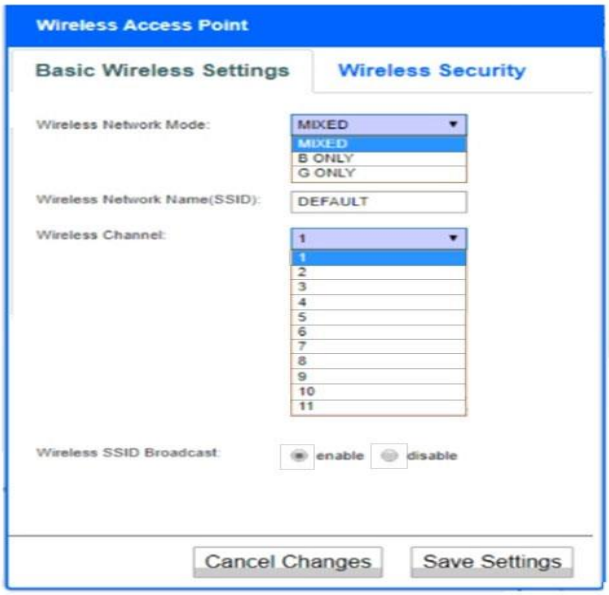
WIRELESS CONTROLLER

IP	172.28.1.30
NETMASK	255.255.255.0
DG	172.28.1.1
Admin User	root
Admin Password	corporatenet
WAP Key	supersecret
Port	1212

LDAP SERVER

IP	10.10.20.20
NETMASK	255.255.255.0
DG	10.10.20.1
Domain	corporatenet
Tree Name	wirelessnet
Bind Password	secretpass
Port	389

Hot Area:



Answer:

Explanation

Wireless Access Point

Network Mode – G only

Wireless Channel – 11

Wireless SSID Broadcast – disable

Security settings – WPA2 Professional

Question #:100 - (Exam Topic 3)

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management

B. Testing the policy in a non-production environment before enabling the policy in the production network

C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy

D. Including an "allow any" policy above the "deny any" policy

Answer: B

Explanation

Testing the policy in a non-production environment before enabling the policy in the production network would prevent the issue of making several company servers unreachable. A non-production environment is a replica of the production network that is used for testing, development, or training purposes. By testing the policy in a non-production environment, the technician can verify the functionality and impact of the policy without affecting the real network or users. This can help to identify and resolve any errors or conflicts before applying the policy to the production network. Testing the policy

in a non-production environment can also help to ensure compliance with security standards and best practices.

A: Documenting the new policy in a change request and submitting the request to change management: While documentation and change management are essential steps in maintaining a well-organized and controlled network environment, simply documenting and submitting the change request may not prevent the issue. Change management ensures that changes are tracked, reviewed, and authorized but does not inherently address the risk of the new policy causing service disruptions.

C: Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy: Disabling intrusion prevention signatures may provide temporary relief from security-related issues but does not address the core problem of the new policy causing servers to become unreachable. It also potentially weakens security controls, which is not advisable.

D: Including an "allow any" policy above the "deny any" policy: Adding an "allow any" policy above the "deny any" policy essentially negates the purpose of the "deny any" policy. This can pose significant security risks as it allows all traffic, which is not a recommended practice. It does not address the issue; instead, it creates a potential security vulnerability.

Question #:101 - (Exam Topic 3)

A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large number of different source IP addresses. Which of the following describes this type of attack?

A. DDoS

B. Privilege escalation

C. DNS poisoning

D. Buffer overflow

Answer: A

Explanation

A distributed denial-of-service (DDoS) attack is an attempt to make a computer or network resource unavailable to its intended users. This is accomplished by overwhelming the target with a flood of traffic from multiple sources.

In the scenario described, the security analyst identified a source IP address and blocked it from communicating with the network. However, the attack was still ongoing and coming from a large number of different source IP addresses. This indicates that the attack was a DDoS attack.

Privilege escalation is an attack that allows an attacker to gain unauthorized access to a system or network. DNS poisoning is an attack that modifies the DNS records for a domain name, causing users to be redirected to a malicious website. A buffer overflow is an attack that occurs when a program attempts to store more data in a buffer than it is designed to hold.

Therefore, the most likely type of attack in the scenario described is a DDoS attack.

Question #:102 - (Exam Topic 3)

Which of the following best reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

A. Implement proper network access restrictions.

B. Initiate a bug bounty program.

C. Classify the system as shadow IT.

D. Increase the frequency of vulnerability scans.

Answer: A

Explanation

Network access restrictions can limit the exposure of systems that have expired vendor support and lack an immediate replacement, as they can prevent unauthorized or unnecessary access to those systems from other devices or networks. Network access restrictions can include firewalls, network segmentation, VPNs, access control lists, and other methods that can filter or block traffic based on predefined rules or policies. Network access restrictions can reduce the security risks introduced by running systems that have expired vendor support, as they can mitigate the impact of potential vulnerabilities or exploits that may affect those systems. Verified References:

CompTIA Security+ Certification Exam Objectives Version 3.0
https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf (See Domain 2.1: Given a scenario, implement secure protocols.)

CompTIA Security+ SY0-501 Study Guide
https://www.certblaster.com/wp-content/uploads/2017/10/CompTIA-Security-SY0-501-Study-Guide.pdf (See Chapter 2: Technologies and Tools, Section 2.5: Firewall and Network Security Appliances.)

Question #:103 - (Exam Topic 3)

A company wants to build a new website to sell products online. The website will host a storefront application that allows visitors to add products to a shopping cart and pay for products using a credit card. Which of the following protocols would be most secure to implement?

A. SSL

B. SFTP

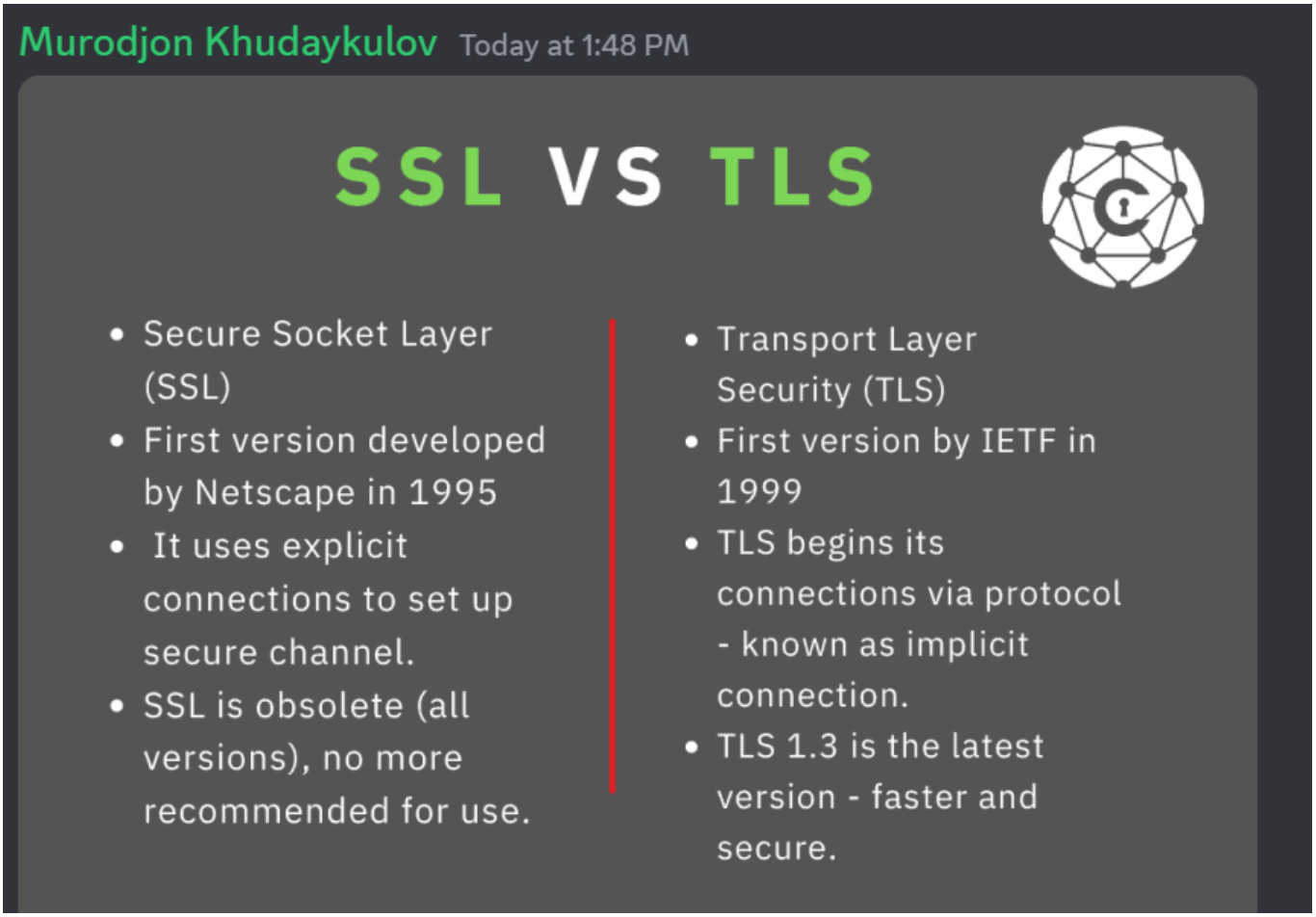
C. SNMP

D. TLS

Answer: D

Explanation

TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet. It can protect the data transmitted between the website and the visitors from eavesdropping, tampering, etc. It is the most secure protocol to implement for a website that sells products online using a credit card.



Question #:104 - (Exam Topic 3)

A user downloaded an extension for a browser, and the user's device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:

```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -
DriveLetter C - FileSystemLabel "New"-FileSystem NTFS - Full -Force -Confirm:$false |
```

Which of the following is the malware using to execute the attack?

A. PowerShell

B. Python

C. Bash

D. Macros

Answer: A

Explanation

PowerShell is a scripting language and command-line shell that can be used to automate tasks and manage systems. PowerShell can also be used by malware to execute malicious commands and evade detection. The code snippet in the question is a PowerShell command that creates a new partition on disk 2, formats it with NTFS file system, and assigns it a drive letter C. This could be part of an attack that wipes out the original data on the disk or creates a hidden partition for storing malware or stolen data.

Petra Martina Vrancic — Today at 1:48 PM

The given command involves creating a new partition on Disk 2, assigning it the drive letter C, and formatting it with the NTFS file system, which could be part of an attempt to hide or obscure malicious activity

References:

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/scripting-and-automation/

https://learn.microsoft.com/en-us/powershell/module/storage/new-partition?view=windowsserver2022-ps

Question #:105 - (Exam Topic 3)

A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the most likely cause of this issue?

A. An external access point is engaging in an evil-Twin attack

B. The signal on the WAP needs to be increased in that section of the building

C. The certificates have expired on the devices and need to be reinstalled

D. The users in that section of the building are on a VLAN that is being blocked by the firewall

Answer: A

Explanation

An evil-Twin attack is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. It is the most likely cause of the issue that users are experiencing slow speeds, unable to connect to network drives, and required to enter their credentials on web pages when working in the section of the building that is closest to the parking lot, where an external access point could be placed nearby.

Question #:106 - (Exam Topic 3)

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: C

Explanation

Push notifications are a type of technology that allows an application or a service to send messages or alerts to a user's device without requiring the user to open the application or the service. They can be used for multi-factor authentication (MFA) by sending a prompt or a code to the user's device that the user has to approve or enter to verify their identity. They can be non-disruptive and user friendly because they do not require the user to remember or type anything, and they can be delivered instantly and securely.

Question #:107 - (Exam Topic 3)

Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification

B. Accountability

C. Legal hold

D. Chain of custody

Answer: C

Explanation

A legal hold is a process that requires an organization to preserve electronically stored information and paper documents that are relevant to a pending or anticipated litigation or investigation. It suspends the normal retention and destruction policies and procedures for such information and documents until the legal hold is lifted or released.

https://www.exterro.com/basics-of-e-discovery/legal-hold

Nita Arapi — Today at 1:54 PM

A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated. Chain-of-Custody: This refers to maintaining a log or documentation for all data gathered throughout the life of a case.

Question #:108 - (Exam Topic 3)

Which of the following best describes configuring devices to log to a centralized, off-site location for possible future reference?

A. Log aggregation

B. DLP

C. Archiving

D. SCAP

Answer: C

Explanation

Archiving is the process of storing data for long-term preservation. In the context of IT security, archiving logs is the process of collecting and storing log files from devices in a centralized location. This allows organizations to access and analyze log data for troubleshooting, compliance, and security auditing purposes.

Log aggregation is the process of collecting log data from multiple sources and storing it in a single location. This can be done for performance or security reasons. However, log aggregation does not necessarily involve storing the logs in

an off-site location.

DLP (Data Loss Prevention) is a set of technologies and processes that are used to protect sensitive data from unauthorized access, use, disclosure, alteration, or destruction. DLP can be used to prevent data from being exfiltrated from an organization's network, but it does not typically involve storing logs in an off-site location.

SCAP (Security Content Automation Protocol) is a set of standards and tools that are used to automate the assessment and remediation of security vulnerabilities. SCAP can be used to collect log data from devices, but it does not typically involve storing the logs in an off-site location.

Therefore, the best answer to the question is archiving. https://sleeknote.com/advanced/ecommerce-glossary/what-is-email-archiving-and-how-does-it-work

David Berrios — Today at 1:55 PM

Archiving generally refers to the process of storing historical data, including logs, documents, emails, and other records, in a secure and organized manner for long-term retention and future reference. While archiving can involve storing logs, the term "log aggregation" specifically refers to the process of collecting and centralizing log data from various sources in real-time or near real-time. Archiving, on the other hand, focuses on preserving historical data for compliance, legal, or business purposes, and it may include logs among other types of information

Question #:109 - (Exam Topic 3)

A malicious actor recently penetrated a company's network and moved laterally to the data center. 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

A dump file is a file that contains the contents of memory at a specific point in time. It can be used for debugging or forensic analysis of a system or an application. It can reveal what was in the memory on the compromised server, such as processes, variables, passwords, encryption keys, etc.

https://www.varonis.com/blog/memory-forensics

Question #:110 - (Exam Topic 3)

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls' (Select two).

A. ISO

B. PCI DSS

C. SOC

D. GDPR

E. CSA

F. NIST

Answer: B D

Explanation

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards and requirements for organizations that store, process, or transmit payment card data. It aims to protect cardholder data and prevent fraud and data breaches. GDPR (General Data Protection Regulation) is a regulation that governs the collection, processing, and transfer of personal data of individuals in the European Union. It aims to protect the privacy and rights of data subjects and impose obligations and penalties on data controllers and processors. These are the frameworks that the security officer should map the existing controls to, as they are relevant for a credit card transaction company that has a new office in Europe

https://www.pcisecuritystandards.org/standards/

https://gdpr-info.eu/

Question #:111 - (Exam Topic 3)

Security analysts notice a server login from a user who has been on vacation for two weeks, The analysts confirm that the user did not log in to the system while on vacation. After reviewing packet capture the analysts notice the following:

```
username: ....smithJA.....
Password: 944d3697d8880ed401b5ba2c77811
```

Which of the following occurred?

A. A buffer overflow was exploited to gain unauthorized access.

B. The user's account was compromised, and an attacker changed the login credentials.

C. An attacker used a pass-the-hash attack to gain access.

D. An insider threat with username logged in to the account.

Answer: C

Explanation

A pass-the-hash attack is a type of replay attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is possible because some authentication protocols send hashes over the network instead of plain text passwords. The packet capture shows that the attacker used NTLM authentication, which is vulnerable to pass-the-hash attacks

The username appears to be suspicious with extra characters before and after "smithJA," which suggests potential tampering or manipulation of the username.
The password is not a plain text password but rather a hash value ("944d3697d880ed401b5ba2c77811"). This suggests that the attacker did not need the actual password but used a hashed version of it.
A "pass-the-hash" attack is a method where an attacker obtains hashed passwords (often through various means) and uses those hashes to authenticate to a system or service, bypassing the need for the actual plaintext password. In this case, it appears that an

attacker used a hashed password to log in as the user "smithJA," which indicates that the user's credentials or password hashes may have been compromised.

A: buffer overflow is unlikely based on the provided information as there is no evidence of a buffer overflow attack.
B: account compromise is also possible, but the fact that a hashed password was used suggests a different attack method.
D: insider threat is possible, but the evidence does not clearly indicate that an insider threat was involved. Pass-the-hash attacks can also be carried out by external attackers who have obtained password hashes through various means.

https://www.netwrix.com/pass_the_hash_attack_explained.html#:~:text=Pass%2Dthe%2DHash%20is%20a,obtaining%20the%20account's%20plaintext%20password.

Topic 4, Exam Set 4

Question #:1 - (Exam Topic 4)

A security analyst is creating baselines for the server team to follow when hardening new devices for deployment. Which of the following best describes what the analyst is creating?

A. Change management procedure

B. Information security policy

C. Cybersecurity framework

D. Secure configuration guide

Answer: D

Explanation

A secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies. A security analyst can create baselines for the server team to follow when hardening new devices for deployment based on a secure configuration guide.

A. Change management procedure. This is not the correct answer, because a change management procedure is a document that describes the steps and processes for implementing, reviewing, and approving changes to an IT system or environment. A change management procedure helps to minimize the risks and impacts of changes on the system performance, availability, and security.

B. Information security policy. This is not the correct answer, because an information security policy is a document that defines the rules and principles for protecting the confidentiality, integrity, and availability of information assets within an organization. An information security policy helps to establish the roles and responsibilities of employees, managers, and stakeholders regarding information security.

C. Cybersecurity framework. This is not the correct answer, because a cybersecurity framework is a document that provides a set of standards, guidelines, and best practices for managing cybersecurity risks and improving resilience. A cybersecurity framework helps to align the business objectives and priorities with the security requirements and capabilities.

D. Secure configuration guide. This is the correct answer, because a secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies.

Reference: Secure Configuration Guide, Security Technical Implementation Guide - Wikipedia.

https://core.vmware.com/security-configuration-guide

Question #:2 - (Exam Topic 4)

An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF, MDM. HIPS, and CASB systems. Which of the following is the best way to improve the situation?

A. Remove expensive systems that generate few alerts.

B. Modify the systems to alert only on critical issues.

C. Utilize a SIEM to centralize logs and dashboards.

D. Implement a new syslog/NetFlow appliance.

Answer: C

Explanation

A SIEM (Security Information and Event Management) is a system that collects, analyzes, and correlates data from multiple sources, such as AV (antivirus), EDR (endpoint detection and response), DLP (data loss prevention), SWG (secure web gateway), WAF (web application firewall), MDM (mobile device management), HIPS (host intrusion prevention system), and CASB (cloud access security broker). A SIEM can help improve the situation by providing a centralized view of the security posture, alerts, and incidents across the organization.

https://blog.logcraft.io/posts/2023/what-logs-to-collect-in-a-siem.html

Question #:3 - (Exam Topic 4)

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicate a directory traversal attack has occurred. Which of the following is the analyst most likely seeing?

A. http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>

B. http://sample.url.com/someotherpageonsite/../../../etc/shadow

C. http://sample.url.com/select-from-database-where-password-null

D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect

Answer: B

Explanation

The log files show that the attacker was able to access files and directories that were not intended to be accessible by web users, such as "/etc/passwd" and "/var/log". This indicates that the attacker was able to exploit a vulnerability in the web server or application that allowed them to manipulate the file path and access arbitrary files on the server. This is a type of attack known as directory traversal, which can lead to information disclosure, privilege escalation, or remote code execution3.

https://brightsec.com/blog/directory-traversal/#:~:text=Simple%20Directory%20Traversal%20(dot%2Ddot%2Dslash%20Attack),-The%20simplest%20example&text=If%20the%20application%20does%20not,access%20the%20protected%20passwd%20file.

A: appears to be an attempt to inject a script tag into a URL, potentially for a different type of attack, like Cross-Site Scripting (XSS).
C: This URL appears to be related to a database query. While it doesn't specifically indicate an attack, it may potentially be related to SQL injection, a common type of attack on web applications.
D: This URL appears to be related to a DNS redirect. While it includes the term "malicious," the URL itself does not provide enough information to determine the nature of the atta
Bilal Lamharti — Today at 2:02 PM

../../../'
directory traversalck. DNS-based attacks can involve various tactics, including DNS cache poisoning, DNS spoofing, or domain hijacking.

Question #:4 - (Exam Topic 4)

A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works best until a proper fix is released?

A. Detective

B. Compensating

C. Deterrent

D. Corrective

Answer: B

Explanation

Compensating controls are alternative or additional controls that are implemented when the primary or preferred controls are not feasible or effective. Compensating controls can provide a similar level of protection or reduce the risk to an acceptable level until a proper fix is released. For example, if a vulnerability exists in a web server that allows remote code execution, a compensating control could be to restrict access to the web server by using a firewall or an IPS.

https://pathlock.com/learn/what-are-compensating-controls-and-why-you-need-them/

Question #:5 - (Exam Topic 4)

Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.//// transference
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.///// risk reduction
C. A security control objective cannot be met through a technical change, so the company changes as a method of operation. //// Detection Change management
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk. /////////// Acceptance

Answer: B

A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation**.**

https://www.buildings.com/industry-news/article/10193773/managing-risk-through-employee-training

Petra Martina Vrancic — Today at 2:05 PM

Training users is a form of risk reduction because knowledgeable and informed employees are less likely to engage in risky behaviors or fall victim to security threats. It's a proactive measure to enhance the human element of security and create a more resilient overall security posture for the company.

Question #:6 - (Exam Topic 4)

An analyst is concerned about data leaks and wants to restrict access to internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service. Which of the following would be the best technology for the analyst to consider implementing?

A. DLP

B. VPC

C. CASB

D. Content filtering

Answer: C

Explanation

A cloud access security broker (CASB) is a technology that can restrict access to internet services to authorized users only and control the actions each user can perform on each service. A CASB is a type of software or service that acts as an intermediary between users and cloud service providers. A CASB can enforce security policies, monitor user activity, detect and prevent data leaks, encrypt data, and provide visibility and auditability of cloud usage. References:

https://www.netskope.com/security-defined/what-is-casb

https://www.comptia.org/blog/what-is-a-cloud-access-security-broker

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:7 - (Exam Topic 4)

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

A. Accept

B. Transfer

C. Mitigate

D. Avoid

Answer: B

Explanation

A company purchased cyber insurance to address items listed on the risk register. This represents a transfer strategy. A transfer strategy involves transferring or sharing some or all of the responsibility or impact of a risk to another party, such as an insurer, a supplier, or a partner. A transfer strategy can help to reduce the financial liability or exposure of the company in case of a security incident or breach. References: https://www.comptia.org/blog/what-is-cyber-insurance

https://foundershield.com/blog/risk-management/

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:8 - (Exam Topic 4) -

A security analyst is investigating an incident to determine what an attacker was able to do on a compromised Laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionpolicies	C:\asdf234\asdf234.exe was Policies blocked by Group Policy
PC1	4688	Microsoft-Windows-Security Auditing	A new process has been created. New Process Name: powershell.exe Creator Process Name: outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name: lat.ps1 Creator Process Name: powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name: PC1 Authentication Package Name: NTLM

Which of the following describes the method that was used to compromise the laptop?

A. An attacker was able to move laterally from PC 1 to PC2 using a pass-the-hash attack

B. An attacker was able to bypass the application approval list by emailing a spreadsheet. attachment with an embedded PowerShell in the file.

C. An attacker was able to install malware to the C:\asdf234 folder and use it to gain administrator rights and launch Outlook

D. An attacker was able to phish user credentials successfully from an Outlook user profile

Answer: B

Explanation

The first event says that .exe file was blocked. The second event says that PowerShell process started and initiated by outlook. So an email attachment is most likely the case. Among all available options B is talking about attachment.The SIEM log shows that a new process named "powershell.exe" was created by "outlook.exe" and later by "powershell.exe" on the compromised laptop, which suggests that the attacker used a method that involved PowerShell. The fact that the "SoftwareRestrictionpolicies" blocked "C:\asdf234\asd£234.exe" indicates that some type of application whitelisting or software restriction policy was in place, but the attacker was able to bypass it by using PowerShell.

A: is not supported by the provided SIEM log.

C: shows that the malware was blocked by a software restriction policy.

D:does not show any evidence of successful credential theft.

Question #:9 - (Exam Topic 4)

A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website. The malicious actor posted an entry in an attempt to trick users into clicking the following:

https://www.c0mptia.com/contact-us/%3Fname%3D%3Cscript%Ealert(document.cookie)%3C%2Fscript%3E

Which of the following was most likely observed?

A. DLL injection

B. Session replay

C. SQLi

D. xss

Answer: D

Explanation

The code is URL encoded. If we decode the entry it gives us: https://www.c0mptia.com/contact-us/?name=<scriptlert(document.cookie)</script>. This is clearly a sign of XSS attack. Cross-site scripting is a type of web application attack that involves injecting malicious code or scripts into a trusted website or application. The malicious code or script can execute in the browser of the victim who visits the website or application, and can perform actions such as stealing cookies, redirecting to malicious sites, displaying fake content, or compromising the system. References:

https://www.comptia.org/blog/what-is-cross-site-scripting

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Option A (DLL injection) typically involves injecting malicious Dynamic Link Library (DLL) files into processes, not web applications.

Option B (Session replay) is a different type of attack where an attacker captures and replays a user's session, which is unrelated to

the content of the provided URL.

Option C (SQLi or SQL Injection) is another type of attack that targets vulnerabilities in database queries, but the URL does not exhibit characteristics of SQL injection; it's more in line with XSS.

Question #:10 - (Exam Topic 4)

A systems administrator set up an automated process that checks for vulnerabilities across the entire environment every morning. Which of the following activities is the systems administrator conducting?

A. Scanning

B. Alerting

C. Reporting

D. Archiving

Answer: A

Explanation

Scanning is the activity of checking for vulnerabilities across the network, systems, or applications. It can be done manually or automatically using tools such as vulnerability scanners, port scanners, or network mappers. Scanning can help identify and remediate potential security issues before they are exploited.

https://purplesec.us/learn/what-is-vulnerability-scanning/

Question #:11 - (Exam Topic 4)

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

A. Open-source intelligence

B. Bug bounty

C. Red team

D. Penetration testing

Answer: B

Explanation

A program that allows individuals to security test the company’s internet-facing application and compensates researchers based on the vulnerabilities discovered is best described as a bug bounty program. A bug bounty program is an incentive-based program that rewards ethical hackers for finding and reporting security flaws in software or systems.

https://www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples

Question #:12 - (Exam Topic 4) -

A security analyst is reviewing SIEM logs during an ongoing attack and notices the following:

http://company.com/get php? f=/etc/passwd

http://company.com/..%2F..%2F..%2F..%2Fetc%2Fshadow

http: //company.com/../../../ ../etc/passwd

Which of the following best describes the type of attack?

A. SQLi

B. CSRF

C. API attacks

D. Directory traversal

Answer: D

Explanation

Directory traversal (also known as file path traversal) is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files1. In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server1.

Directory traversal in its simplest form uses the …/ pattern, which means to step up one level in the directory structure. By repeating this pattern, an attacker can traverse to the root directory and then access any file or folder on the server. For example, the following request attempts to read the Unix password file /etc/passwd from the server:

http://company.com/get.php?f=/etc/passwd

Some web applications may implement some defenses against directory traversal attacks, such as filtering out ../ patterns or percent-decoding the user input before validating it. However, these defenses can often be bypassed by using variations or encoding techniques. For example, the following requests use different ways to represent …/ or / characters:

http://company.com/…%2F…%2F…%2Fetc%2Fpasswd

http://company.com/…/…/…/%2Fetc%2Fpasswd

http://company.com/%2E%2E/%2E%2E/%2E%2E/etc/passwd

These requests may still result in directory traversal attacks if the web application does not properly handle them12.

A. SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application's database layer, where malicious SQL statements are inserted into an entry field for execution3. The requests in the question do not contain any SQL statements or commands.

B. CSRF. This is not the correct answer, because CSRF stands for Cross-Site Request Forgery, which is an attack that exploits the trust a web server has in a user's browser, where malicious requests are sent to the web server using the user's credentials. The requests in the question do not indicate that they are forged or sent by another website.

C. API attacks. This is not the correct answer, because API stands for Application Programming Interface, which is a set of rules and specifications that allow software components to communicate and exchange data. API attacks are attacks that target the vulnerabilities or weaknesses of APIs, such as authentication, authorization, encryption, rate limiting, or input validation5. The requests in the question do not target any specific API functionality or feature.

D. Directory traversal. This is the correct answer, because directory traversal is an attack that exploits insufficient security validation or sanitization of user-supplied file names, such that characters representing “traverse to parent directory” are passed through to the operating system’s file system API12. The requests in the question contain various patterns of …/ or / characters that attempt to access restricted files and directories on the server.

Reference: What is directory traversal, and how to prevent it? - PortSwigger, Directory traversal attack - Wikipedia, What Is SQL Injection (SQLi) and How To Prevent It, What Is Cross-Site Request Forgery (CSRF)? | Acunetix, API Security Testing – How to Hack an API and Get Away with It (Part 1 of 3).

Question #:13 - (Exam Topic 4)

A security analyst has been reading about a newly discovered cyberattack from a known threat actor. Which of the following would best support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

A. Security research publications

B. The MITRE ATT&CK framework

C. The Diamond Model of Intrusion Analysis

D. The Cyber Kill Cham

Answer: B

Explanation

The MITRE ATT&CK framework would best support the analyst’s review of the tactics, techniques, and procedures (TTPs) the threat actor was observed using in previous campaigns. The MITRE ATT&CK framework is a knowledge base that describes the common TTPs used by various threat actors across different stages of an attack lifecycle. The framework can help security analysts understand how adversaries operate, what tools they use, what vulnerabilities they exploit, what indicators they leave behind, etc. The framework can also help security analysts improve their detection and response capabilities by providing recommendations and best practices.

Reference: https://attack.mitre.org/

Question #:14 - (Exam Topic 4)

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat

B. Hacktivist

C. Nation-state

D. Organized crime

Answer: D

Explanation

Organized crime is a term that describes groups of criminals who operate in a coordinated and systematic manner to

pursue illicit activities for profit. Organized crime groups often use sophisticated tools and techniques to evade law enforcement and exploit vulnerabilities in various sectors, such as finance, transportation, or healthcare. Organized crime groups may also collaborate with other criminal groups or actors to share resources, information, or expertise.

Ransomware as a service (RaaS) is an example of a business model used by organized crime groups to conduct ransomware and extortion attacks. RaaS is an arrangement between an operator, who develops and maintains the tools to power extortion operations, and an affiliate, who deploys the ransomware payload.
When the affiliate conducts a successful ransomware and extortion attack, both parties profit. The RaaS model lowers the barrier to entry for attackers who may not have the skill or technical wherewithal to develop their own tools but can manage ready-made penetration testing and sysadmin tools to perform attacks12.

Insider threat is a term that describes individuals who have legitimate access to an organization's systems or data and use it for malicious purposes, such as theft, sabotage, or espionage. Insider threats may be motivated by various factors, such as greed, revenge, ideology, or coercion. Insider threats may also be unintentional, such as when an employee falls victim to phishing or social engineering.

Hacktivist is a term that describes individuals or groups who use hacking or cyberattacks to promote a political or social cause. Hacktivists may target governments, corporations, or other entities that they perceive as oppressive, corrupt, or unethical. Hacktivists may also use cyberattacks to expose information, disrupt services, or deface websites.

Nation-state is a term that describes a sovereign state that has a centralized government and a defined territory. Nation-state actors are individuals or groups who conduct cyberattacks on behalf of or with the support of a nation-state. Nation-state actors may target other states, organizations, or individuals for various reasons, such as espionage, sabotage, influence, or retaliation.

Reference: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/ransomware-as-a-service#:~:text=Ransomware%2Das%2Da%2DService%20(RaaS)%20is%20a,then%20extorting%20payments%E2%80%94to%20affiliates.

Question #:15 - (Exam Topic 4)

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain the chain of custody?

A. Document the collection and require a sign-off when possession changes.

B. Lock the device in a safe or other secure location to prevent theft or alteration.

C. Place the device in a Faraday cage to prevent corruption of the data.

D. Record the collection in a block chain-protected public ledger.

Answer: A

Explanation

Documenting the collection and requiring a sign-off when possession changes are essential steps for maintaining chain of custody during an investigation. Chain of custody is the process of documenting and preserving the integrity and authenticity of evidence from the time it is collected until it is presented in court. Documenting the collection involves recording information such as date, time, location, description, serial number, etc., of the evidence. Requiring a sign-off when possession changes involves obtaining signatures from every person who handles or transfers the evidence.

Question #:16 - (Exam Topic 4)

A security analyst discovers several jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of

the images if all the metadata is still intact?

A. The GPS location

B. When the file was deleted

C. The total number of print jobs

D. The number of copies made

Answer: A

Explanation

The GPS location would be part of the images if all the metadata is still intact. Metadata is data that describes other data, such as file name, size, date, author, etc. Some metadata can also contain information about the device, software, or location that created or modified the data. For example, some digital cameras and smartphones can embed GPS coordinates into the metadata of photos, which can reveal the location where the photos were taken. This can be useful for forensic analysis, but also pose privacy risks.

Reference: https://christianespinosa.com/blog/2-simple-ways-to-extract-gps-coordinates-from-images/

Question #:17 - (Exam Topic 4)

The application development teams have been asked to answer the following questions:

Does this application receive patches from an external source?

Does this application contain open-source code?

Is this application accessible by external users?

Does this application meet the corporate password standard?

Which of the following are these questions part of?

A. Risk control self-assessment

B. Risk management strategy

C. Risk acceptance

D. Risk matrix

Answer: A

Explanation

A risk control self-assessment (RCSA) is a process that allows an organization to identify, evaluate, and mitigate the risks associated with its activities, processes, systems, and products. A RCSA involves asking relevant questions to assess the effectiveness of existing controls and identify any gaps or weaknesses that need improvement. A RCSA also helps to align the risk appetite and tolerance of the organization with its strategic objectives and performance.

The application development teams have been asked to answer questions related to their applications' security posture, such as whether they receive patches from an external source, contain open-source code, are accessible by external users, or meet the corporate password standard. These questions are part of a RCSA process that aims to evaluate the potential risks and vulnerabilities associated with each application and determine how well they are managed and

mitigated.

Reference: https://broadleaf.com.au/resource-material/controls-3-conducting-a-simple-control-self-assessment/

Question #:18 - (Exam Topic 4)

During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will best assist the analyst?

A. A vulnerability scanner

B. A NGFW

C. The Windows Event Viewer

D. A SIEM

Answer: D

Explanation

A security information and event management (SIEM) system will best assist the analyst to review the correlated logs to find the source of the incident. A SIEM system is a type of software or service that collects, analyzes, and correlates logs and events from multiple sources, such as firewalls, EDR systems, servers, or applications. A SIEM system can help to detect and respond to security incidents, provide alerts and reports, support investigations and forensics, and comply with regulations. References: https://www.comptia.org/blog/what-is-a-siem https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:19 - (Exam Topic 4)

A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would most likely show where the malware originated?

A. The DNS logs

B. The web server logs

C. The SIP traffic logs

D. The SNMP logs

Answer: A

Explanation

Most network software, including malware, relies on it to resolve domains to IP addresses before it can establish connections over protocols such as HTTP(S), SMTP, and many others. This means that DNS logging will contain a more complete record, not limited to HTTP(S) traffic, of domain access by endpoints in the environment, making it a valuable log source for defenders.

Host is been infected

Question #:20 - (Exam Topic 4)

An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding a credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack

B. Protocol poisoning

C. Domain hijacking

D. Bluejacking

Answer: A

Explanation

An on-path attack is an attack that took place when an attacker was eavesdropping on a user who was shopping online and was able to spoof the IP address associated with the shopping site. An on-path attack is a type of network attack that involves intercepting or modifying traffic between two parties by placing oneself in the communication path. An on-path attack can also be called a man-in-the-middle attack or a session hijacking attack. An on-path attacker can steal sensitive information, such as credit card details, or redirect the user to a malicious website. References:

https://www.cloudflare.com/learning/security/threats/on-path-attack/#:~:text=On%2Dpath%20attackers%20place%20themselves,either%20of%20the%20two%20agents.

https://www.comptia.org/blog/what-is-a-man-in-the-middle-attack

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

Question #:21 - (Exam Topic 4)

Historically, a company has had issues with users plugging in personally owned removable media devices into corporate computers. As a result, the threat of malware incidents is almost constant. Which of the following would best help prevent the malware from being installed on the computers?

A. AUP

B. NGFW

C. DLP

D. EDR

Answer: D

Explanation

EDR stands for Endpoint Detection and Response, which is a technology that monitors, detects, and responds to cyber threats on endpoint devices, such as laptops, desktops, servers, or mobile devices. EDR collects and analyzes data from endpoints to identify suspicious or malicious activities, such as malware installation, file modification, registry changes, network connections, or user actions. EDR also provides tools and capabilities to respond to threats, such as isolating infected devices, blocking malicious processes, removing malware, or restoring files.

An EDR solution provides visibility into endpoint activities and can detect when removable media is connected, scan it for malware, and prevent malicious files from being installed. By alerting on and blocking risky actions at the endpoint, EDR provides the strongest protection against malware from user's personal media devices.

Question #:22 - (Exam Topic 4)

Server administrators want to configure a cloud solution so that computing memory and processor usage are maximized most efficiently across a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation

B. High availability

C. Segmentation

D. Container security

Answer: A

Explanation

Dynamic resource allocation is a technique that allows cloud providers to adjust the amount and distribution of computing resources according to the changing demand and capacity of the cloud environment1. Dynamic resource allocation can improve the efficiency and utilization of available computing power, as well as reduce the cost and energy consumption of the cloud infrastructure1. Dynamic resource allocation can also enhance the system availability and reliability by avoiding potential denial-of-service situations caused by overloading or under-provisioning of resources.

Reference: https://ieeexplore.ieee.org/document/8212723

Question #:23 - (Exam Topic 4)

An organization suffered numerous multi day power outages at its current location. The Chief Executive Officer wants to create a disaster recovery strategy to resolve this issue. Which of the following options offer low-cost solutions? (Select two).

A. Warm site

B. Generator

C. Hot site

D. Cold site

E. Cloud backups

F. UPS

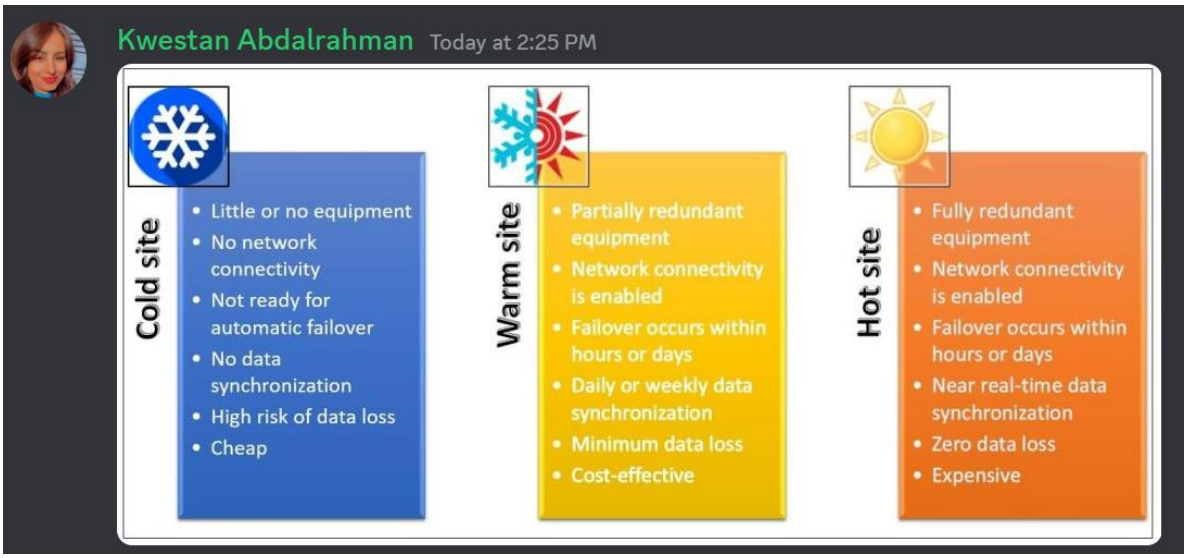
Answer: D F

Explanation

A UPS (uninterruptible power supply) is a low-cost solution that can provide backup power to an organization in case of a power outage. It is a device that provides battery power to a system when the main power source fails. UPS is cheaper compared to generators. Cold site provides power, cooling, and/or office space which waits in the event of a significant outage to the main work site or datacenter. The cold site will require extensive support from engineering and IT personnel to get all necessary servers and equipment migrated and functional. Cold sites are the cheapest cost-recovery option for businesses to utilize.

Reference: https://www.seguetech.com/three-stages-disaster-recovery-sites/

https://www.dalepowersolutions.com/knowledge-base/the-differences-between-ups-systems-and-generators#:~:text=A%20UPS%20system%20means%20that,short%20term%20standby%20power%20solution.



Question #:24 - (Exam Topic 4) -

Which of the following is an example of risk avoidance?

A. Installing security updates directly in production to expedite vulnerability fixes

B. Buying insurance to prepare for financial loss associated with exploits

C. Not installing new software to prevent compatibility errors

D. Not taking preventive measures to stop the theft of equipment

Answer: C

Explanation

Risk avoidance is the strategy of eliminating or minimizing exposure to risk by not engaging in an activity or process that may result in a negative outcome. Not installing new software to prevent compatibility errors is an example of risk avoidance, as it avoids the possibility of introducing new vulnerabilities or disrupting existing functionality.

Not installing new software to prevent compatibility errors.

In this scenario, by choosing not to install new software, an organization is actively avoiding the risk associated with potential compatibility errors that could arise from the introduction of new software into their existing environment. This is a proactive approach to eliminating the risk altogether.

A: Installing security updates directly in production to expedite vulnerability fixes is an example of risk mitigation or risk reduction, where steps are taken to reduce the impact or likelihood of a risk rather than avoiding it altogether.

B: Buying insurance to prepare for financial loss associated with exploits is an example of risk transfer, where the organization shifts the financial burden of the risk to an insurance provider rather than avoiding the risk itself.

D: Not taking preventive measures to stop the theft of equipment is an example of risk acceptance, where the organization acknowledges the risk but chooses not to take any action to mitigate, avoid, or transfer it.

Question #:25 - (Exam Topic 4)

An organization wants to ensure that proprietary information is not inadvertently exposed during facility tours. Which of the following would the organization implement to mitigate this risk?

A. Clean desk policy

B. Background checks

C. Non-disclosure agreements

D. Social media analysis

Answer: A

Explanation

A clean desk policy is a set of rules that require employees to clear their desks of any documents, papers, or devices that contain sensitive or confidential information when they leave their workstations. This policy helps to prevent unauthorized access, theft, or disclosure of proprietary information during facility tours or other situations where outsiders may visit the premises.

A. Clean desk policy. This is the correct answer, because a clean desk policy is a simple and effective way to mitigate the risk of exposing proprietary information during facility tours.

Reference: https://www.schellman.com/blog/cybersecurity/benefits-of-a-clean-desk-policy

Similar question

The president of a regional bank likes to frequently provide SOC tours to potential investors. Which of the following policies BEST reduces the risk of malicious activity occurring after a tour?

A. Password complexity

B. Acceptable use

C. Access control

D. Clean desk

Answer: D

A malicious investor would not be able to take advantage of anything gained until after the tour if the swiped a USB, looked at or stole documents. If their was a clean desk policy then that would prevent issues after a tour

lowing only necessary communication between them.