Exam Topic Breakdown

Exam Topic	Number of Questions
Topic 1 : Exam Set 1	188
Topic 2 : Exam Set 2	195
Topic 3 : Exam Set 3	117
Topic 4 : Exam Set 4	77
TOTAL	577

Question #:111 - (Exam Topic 1)

Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft

B. Data loss

C. Data exfiltration

D. Reputation

Answer: D

Explanation

While the incident involves potential data loss (unfavorable pictures from the CEO's workstation), data exfiltration (hackers having access to the images), and a threat of blackmail (ransom demand), the most significant impact is on the reputation of the company. If the images were to be released to the press, it could result in serious damage to the company's reputation, which can have long-lasting and far-reaching consequences, including loss of trust from customers, partners, investors, and the public.

Reputation damage is a critical concern for organizations, as it can impact their credibility, customer loyalty, and overall business relationships. Therefore, it is often a top priority to protect and manage an organization's reputation in the face of security incidents like the one described.

Question #:112 - (Exam Topic 1)

An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

A. Apply a DLP solution.

B. Implement network segmentation

C. Utilize email content filtering,

D. isolate the infected attachment.

Answer: B

Explanation

Given that the target has already opened an attachment containing a worm, the immediate concern is to prevent further spread within the network. Implementing network segmentation is the best course of action in this scenario. Network segmentation involves dividing the network into isolated segments or zones, which can help contain the spread of the worm and limit its impact on other parts of the network.

While the other options mentioned (A. Apply a DLP solution, C. Utilize email content filtering, D. Isolate the infected attachment) are important security measures, they are generally more focused on preventing incidents or managing data, and may not be as effective in containing an already activated worm within the network.

Network segmentation is a cybersecurity practice that can be beneficial both as a precautionary measure before any incident happens and as a response strategy after an incident occurs.

Note: It's already open so isolation is difficult--segmentation first to stop whatever damage already happened

Question #:113 - (Exam Topic 1)

Which of the following biometric authentication methods is the MOST accurate?

A. Gait

B. Retina

C. Signature

D. Voice

Answer: B

Explanation

Retina scanning is one of the most accurate biometric authentication methods available. It involves capturing the unique patterns of blood vessels in the back of an individual's eye, which are highly distinctive and difficult to duplicate. Retina scans offer a high level of accuracy and security because they are not easily fooled by impersonation or replication, making them one of the most reliable biometric technologies for authentication.

While other biometric methods like voice, signature, and gait can be useful, they may have varying levels of accuracy and susceptibility to spoofing or false positives. Retina scanning, on the other hand, is exceptionally accurate and difficult to deceive, making it a strong choice for applications requiring the highest level of security.

Question #:114 - (Exam Topic 1)

Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:

• All users share workstations throughout the day.

• Endpoint protection was disabled on several workstations throughout the network.

• Travel times on logins from the affected users are impossible.

• Sensitive data is being uploaded to external sites.

• All user account passwords were forced to be reset and the issue continued.

Which of the following attacks is being used to compromise the user accounts?

A. Brute-force

B. Keylogger

C. Dictionary

D. Rainbow

Answer: B

Explanation

The indicators are pointing to Keylogger.

- All users sharing workstations could mean that the keylogger is capturing keystrokes across multiple user sessions.

- Endpoint protection being disabled on several workstations suggests that the attackers might have gained administrative access to the workstations, allowing them to disable security software without detection.

- Impossible travel times on logins from the affected users indicate that someone other than the legitimate user might be logging in using their credentials, possibly from a different location.

- Sensitive data being uploaded to external sites indicates unauthorized access to sensitive information, likely obtained through captured keystrokes.

A: Brute-force: trail and error attempts to guess login info

C: Dictionary: a form of brute force attack that uses common words, phrases and variations

D: Rainbow: uses tables of reversed hashes to crack passwords

Question #:115 - (Exam Topic 1)

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling

B. Spam

C. Invoice scam

D. Pharming

Answer: D

Explanation

In the scenario, the attack is more consistent with a "Pharming" attack because it involves the redirection of the

executive to a fake banking website where their credit card and account details are harvested. Pharming attacks focus on manipulating the DNS or other methods to redirect users to fraudulent websites, whereas whaling attacks are more about targeted, personalized phishing attempts against high-value individuals.

While the terminology can sometimes overlap, the details of the attack scenario provided align more closely with a Pharming attack.

"Whaling" is a specific form of phishing attack that targets high-profile individuals or executives within an organization. While it's true that executives are often the primary targets in whaling attacks, the scenario described doesn't fit the typical definition of a whaling attack.

In a whaling attack, the attacker often crafts personalized and convincing messages to deceive a high-ranking individual, such as a CEO or CFO, into taking a specific action, such as transferring funds or revealing sensitive information. The attack typically doesn't involve redirecting the victim to a fake website to harvest their information directly.

Question #:116 - (Exam Topic 1)

A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

A. Dictionary

B. Rainbow table

C. Spraying

D. Brute-force

Answer: C

Explanation

Password spraying is an attack where an attacker tries a small number of commonly used passwords against a large number of usernames. The goal of password spraying is to avoid detection by avoiding too many failed login attempts for any one user account. The fact that different usernames are being attacked from the same IP address is a strong indication that a password spraying attack is underway.

The reason for this is that the authentication failures are from different usernames that share the same source IP address, indicating that an attacker is attempting to log in to multiple user accounts. This is characteristic of a password spraying attack, in which an attacker uses common passwords against multiple usernames in the hopes of gaining access to one of them, rather than trying different passwords against a single user account, which is more typical of a brute-force attack.
\Petra Martina Vrancic — Today at 10:14 AM
yes
[10:15 AM]
Password spraying is a technique where attackers try a small number of commonly used passwords against many usernames or accounts. Since the authentication failures are from different usernames with the same source IP address, it's consistent with the behavior of a password spraying attack.

Question #:117 - (Exam Topic 1)

An information security manager for an organization is completing a PCI DSS self-assessment for the first time. Which of the following is the MOST likely reason for this type of assessment?

A. An international expansion project is currently underway.

B. Outside consultants utilize this tool to measure security maturity.

C. The organization is expecting to process credit card information.

D. A government regulator has requested this audit to be completed

Answer: C

Explanation

PCI DSS is a set of security standards designed to ensure that companies handling credit card transactions maintain a secure environment. If an organization plans to process credit card payments or already does so, it is typically required to comply with PCI DSS standards to safeguard sensitive cardholder data. Completing a PCI DSS self-assessment is a crucial step in assessing and documenting compliance with these standards.

While the other options may be related to security and compliance efforts:

International Expansion Project: Expanding internationally may involve various security and compliance considerations, but it doesn't directly necessitate a PCI DSS self-assessment.

Outside Consultants Measuring Security Maturity: This may involve security assessments, but PCI DSS compliance is specific to handling credit card data.

Government Regulator Requesting Audit: Government regulators may request audits for various reasons, but a PCI DSS self-assessment is typically initiated by organizations expecting to process credit card transactions.

If the organization is expecting to process credit card information, then it must demonstrate its compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Organizations that handle credit card information must demonstrate their compliance with PCI DSS on an annual basis, typically through a self-assessment questionnaire (SAQ) or an on-site assessment by a qualified security assessor (QSA).

PCI DSS = CREDIT CARD

Question #:118 - (Exam Topic 1)

A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

```
IPv4 Address ..... 10.0.0.87
Subnet Mask ..... 255.255.255.0
Default Gateway ..... 10.0.0.1
Internet Address      Physical Address
10.10.255.255         ff-ff-ff-ff-ff-ff
10.0.0.1              aa-aa-aa-aa-aa-aa
10.0.0.254            aa-aa-aa-aa-aa-aa
244.0.0.2             01-00-5e-00-00-02
```

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

A. Denial of service

B. ARP poisoning

C. Command injection

D. MAC flooding

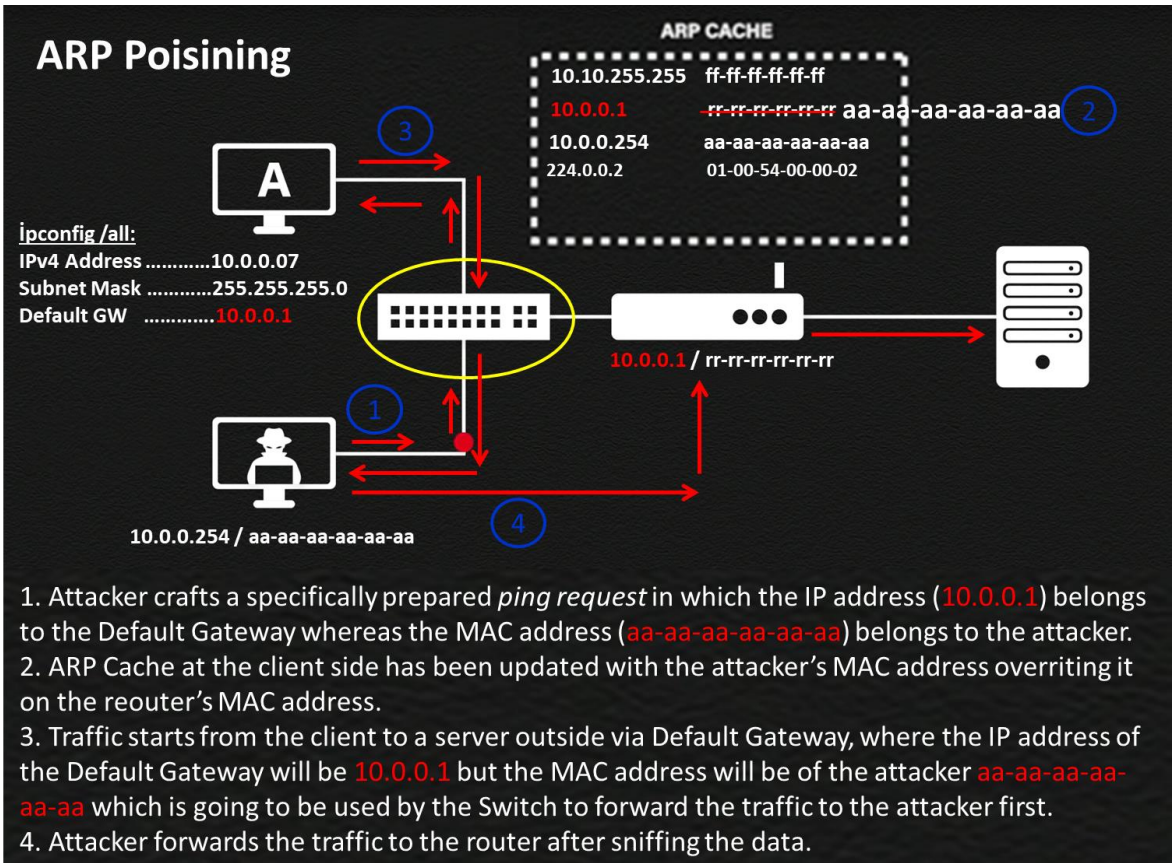
Answer: B

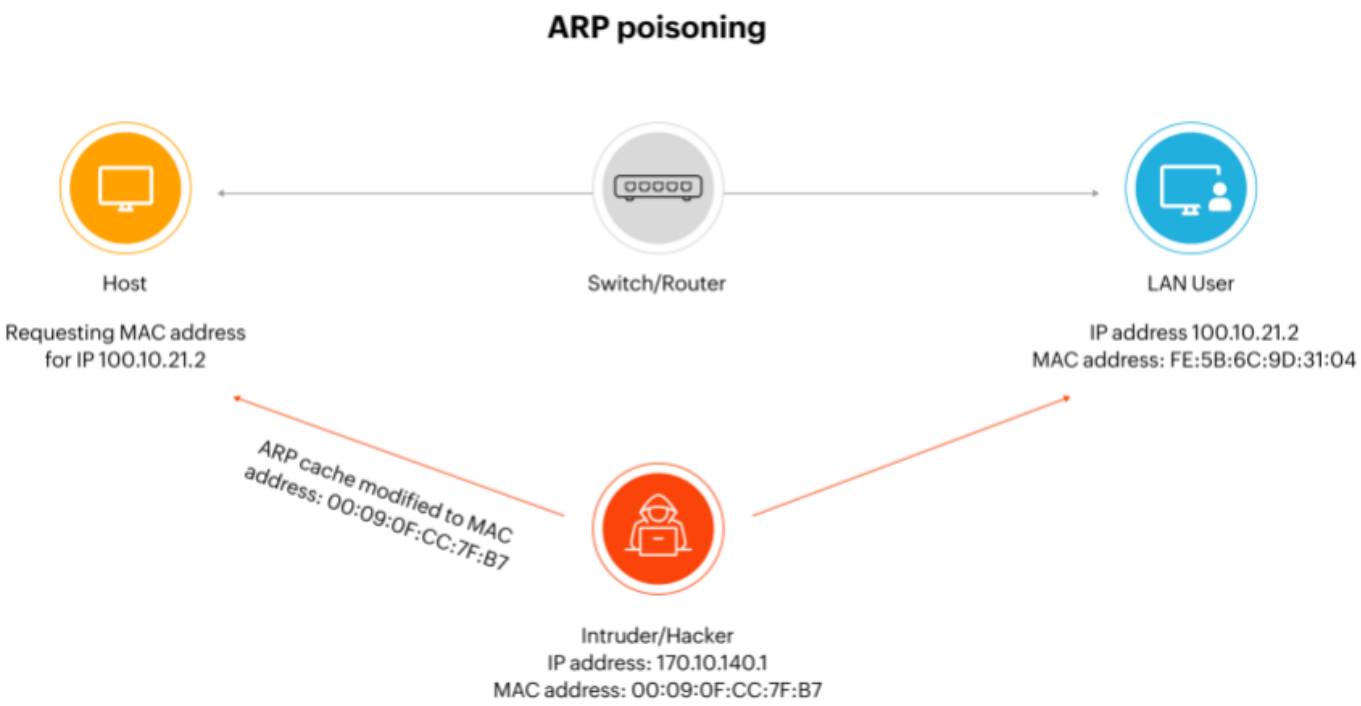
Explanation

ARP (Address Resolution Protocol) poisoning involves manipulating the ARP cache on a network to associate a rogue MAC address with a legitimate IP address. In the output you provided, you can see unusual ARP entries where IP addresses are mapped to MAC addresses that are not the expected hardware addresses.

The entry "10.0.0.1 aa-aa-aa-aa-aa-aa" suggests that the MAC address associated with the default gateway (10.0.0.1) has been changed to an unauthorized MAC address ("aa-aa-aa-aa-aa-aa"). This is a classic sign of ARP poisoning, where an attacker associates their MAC address with the gateway, intercepting traffic meant for the legitimate gateway.

Here the attacker has changed the MAC Address of the Default Gateway with his own MAC Address in the ARP Cache of a client to make the traffic to hit him first before going to a server outside. To do that, the attacker crafts a specifically prepared malicious ping request in which the IP address (10.0.0.1) belongs to the Default Gateway whereas the MAC address (aa-aa-aa-aa-aa-aa) belongs to the attacker. After that the ARP Cache at the client side has been updated (poisoned) with the new information. Whenever a traffic starts from the client to the Def.Gateway, the IP address will be 10.0.0.1 (Def.Gateway's IP) but the MAC address will be aa-aa-aa-aa-aa-aa (Attacker's MAC) which is going to be used by the Switch to forward the traffic to the attacker first.





Question #:119 - (Exam Topic 1)

Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.

Which of the following documents did Ann receive?

A. An annual privacy notice

B. A non-disclosure agreement

C. A privileged-user agreement

D. A memorandum of understanding

Answer: A

Explanation

An annual privacy notice is a document that organizations, including financial institutions, are required to provide to their customers under privacy regulations, such as the Gramm-Leach-Bliley Act (GLBA) in the United States. This notice informs customers about the company's privacy practices and how they handle the customers' Personally Identifiable Information (PII).

In this case, the notice states that the mortgage company may share Ann's PII with partners, affiliates, and associates for day-to-day business operations. This is a common disclosure found in annual privacy notices, informing customers about how their information may be shared and used by the organization and its partners while ensuring compliance with privacy regulations.

Non-Disclosure Agreement (NDA): An NDA is a legal contract that outlines confidentiality obligations between parties. It is typically used when two or more parties need to share confidential information and want to ensure that the information remains confidential. NDAs are commonly used in business dealings, partnerships, and when sharing sensitive information with employees or contractors. They are not related to privacy notices sent to customers.

Privileged-User Agreement: A privileged-user agreement is a document that outlines the terms and conditions associated with privileged access to computer systems, networks, or sensitive data. It is often used within organizations to define the responsibilities and restrictions of users who have elevated privileges, such as system administrators or network administrators. This agreement helps ensure that privileged users understand their responsibilities for safeguarding data and systems.

Memorandum of Understanding (MOU): An MOU is a written agreement between two or more parties that outlines the terms and conditions of their relationship or cooperation on a particular project or initiative. MOUs are commonly used in business, government, and nonprofit organizations to formalize agreements on shared goals, responsibilities, and resources. They are not typically related to privacy notifications sent to customers.

In the context of the question, the annual privacy notice is the document specifically related to informing customers about the mortgage company's privacy practices and the sharing of Personally Identifiable Information (PII) with partners, affiliates, and associates, as required by privacy regulations.

Question #:120 - (Exam Topic 1)

When planning to build a virtual environment, an administrator need to achieve the following,

• Establish policies to limit who can create new VMs

• Allocate resources according to actual utilization‘

• Require justification for requests outside of the standard requirements.

• Create standardized categories based on size and resource requirements

Which of the following is the administrator MOST likely trying to do?

A. Implement IaaS replication

B. Product against VM escape

C. Deploy a PaaS

D. Avoid VM sprawl

Answer: D

Explanation

VM sprawl occurs when virtual machines (VMs) are created but not properly managed, leading to an uncontrolled proliferation of VMs that consume resources and complicate management.

VM sprawl occurs when an organization has many VMs that aren't managed properly.

The administrator is most likely trying to avoid VM sprawl, which occurs when virtual machines are created without proper management or oversight, resulting in an uncontrolled proliferation of VMs that consume resources and increase management overhead. The policies to limit who can create new VMs and require justification for requests outside of the standard requirements help to control the creation of new VMs and ensure that they are only created when necessary. This can help prevent VM sprawl by ensuring that VMs are created in a controlled and deliberate manner. Allocating

resources according to actual utilizations and creating standardized categories based on size and resource requirements also help to prevent VM sprawl by ensuring that VMs are sized appropriately and that resources are allocated efficiently.

A: is a technique used to ensure high availability and disaster recovery for virtual machines in a cloud environment. It is not related to the goals listed by the administrator in this scenario.

B: is a security technique used to prevent attackers from breaking out of a virtual machine and accessing the underlying host. It is not related to the goals listed by the administrator in this scenario.

D: involves providing a platform for developing, deploying, and managing applications in a cloud environment. It is not related to the goals listed by the administrator in this scenario.

Question #:121 - (Exam Topic 1)

The help desk has received calls from users in multiple locations who are unable to access core network services. The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?

A. Disconnect all external network connections from the firewall

B. Send response teams to the network switch locations to perform updates

C. Turn on all the network switches by using the centralized management software

D. Initiate the organization's incident response plan.

Answer: D

Explanation

An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned.

The situation described in the question is indicative of a potential cyber attack, as multiple locations are experiencing issues with accessing core network services. The network team has already taken initial steps to address the issue by turning off the network switches remotely. However, the incident response plan should be initiated to ensure that the incident is contained, assessed, and addressed properly. This will involve coordinating with various stakeholders, including security, IT, management, and potentially law enforcement.

If the help desk has received calls from users in multiple locations who are unable to access core network services, it could indicate that a network outage or a denial-of-service attack has occurred.

The next action that the network team should take is to initiate the organization's incident response plan, which would involve notifying the appropriate stakeholders, such as management, security team, legal team, etc., and following the predefined steps to investigate, analyze, document, and resolve the incident.

The other options are not correct because:

A. Disconnect all external network connections from the firewall. This could be another containment measure to prevent external attackers from accessing the network, but it would also disrupt legitimate network traffic and

services. This action should be taken only if it is part of the incident response plan and after notifying the relevant parties.

B. Send response teams to the network switch locations to perform updates. This could be a recovery measure to restore normal network operations and apply patches or updates to prevent future incidents, but it should be done only after the incident has been properly identified, contained, and eradicated.

C. Turn on all the network switches by using the centralized management software. This could be a recovery measure to restore normal network operations, but it should be done only after the incident has been properly identified, contained, and eradicated.

According to CompTIA Security+ SY0-601 Exam Objectives 1.5 Given a scenario, analyze indicators of compromise and determine the type of malware:

"An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned."

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

Question #:122 - (Exam Topic 1)

A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities

B. Install a sandbox to run the malicious payload in a safe environment

C. Perform a traceroute to identify the communication path

D. Use netstat to check whether communication has been made with a remote host

Answer: B

Explanation

By installing a sandbox, the analyst can isolate the malicious payload and run it in a controlled environment, which can help identify the behavior of the payload and any potential threats it may pose. This can help to determine if the document is part of a larger attack campaign, and if so, what other systems or users may be at risk.

Running a vulnerability scan against the CEO's computer (option A) is not necessary in this situation, as it may disrupt the CEO's work and may not provide useful information about the phishing email.

Performing a traceroute (option C) and using netstat (option D) can provide information about the communication path and potential connections to remote hosts, but may not reveal much about the payload itself.

Question #:123 - (Exam Topic 1)

An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

A. SOAP

B. SAML

C. SSO

D. Kerberos

Answer: C

Explanation

Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials.

SSO is a method of authentication that enables users to authenticate once and access multiple applications without having to re-enter their credentials. It eliminates the need for users to remember multiple sets of credentials for different applications, which can improve security and reduce the burden on users.

SOAP (Simple Object Access Protocol) is a messaging protocol used for exchanging structured data between applications over the internet. While it can be used for authentication, it is not a specific authentication protocol and does not provide seamless authentication.

SAML (Security Assertion Markup Language) is an XML-based authentication protocol used for exchanging authentication and authorization data between parties, typically between an identity provider (IdP) and a service provider (SP). While it can be used for SSO, it is not the only SSO protocol available.

Kerberos is a network authentication protocol used to provide secure authentication between clients and servers over a network. While it can be used for authentication, it is not a specific SSO protocol and does not provide seamless authentication to multiple applications.

References: CompTIA Security+ Study Guide 601, Chapter 6

Question #:124 - (Exam Topic 1)

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).

A. HIDS

B. NIPS

C. HSM

D. WAF

E. NAC

F. NIDS

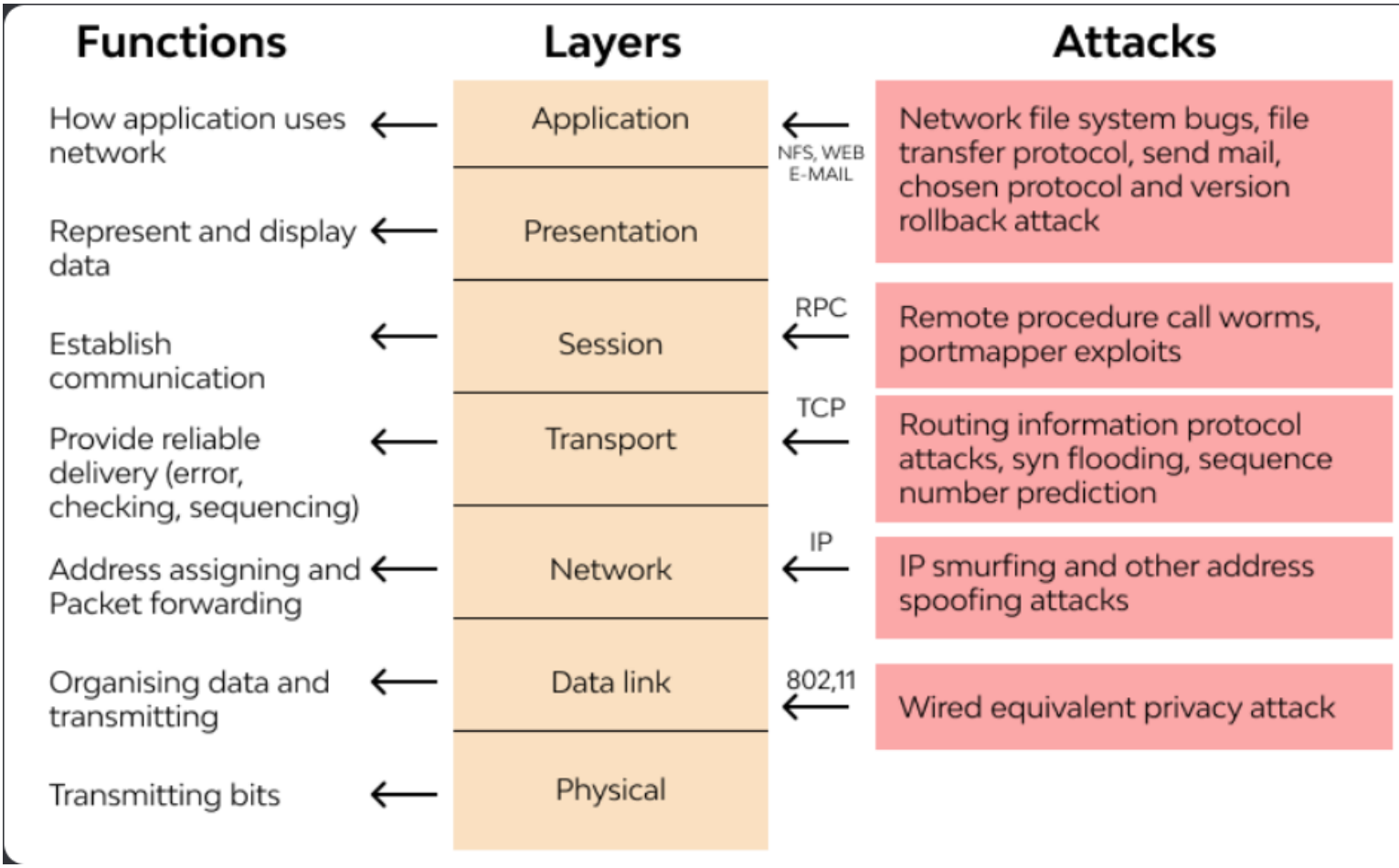
G. Stateless firewall

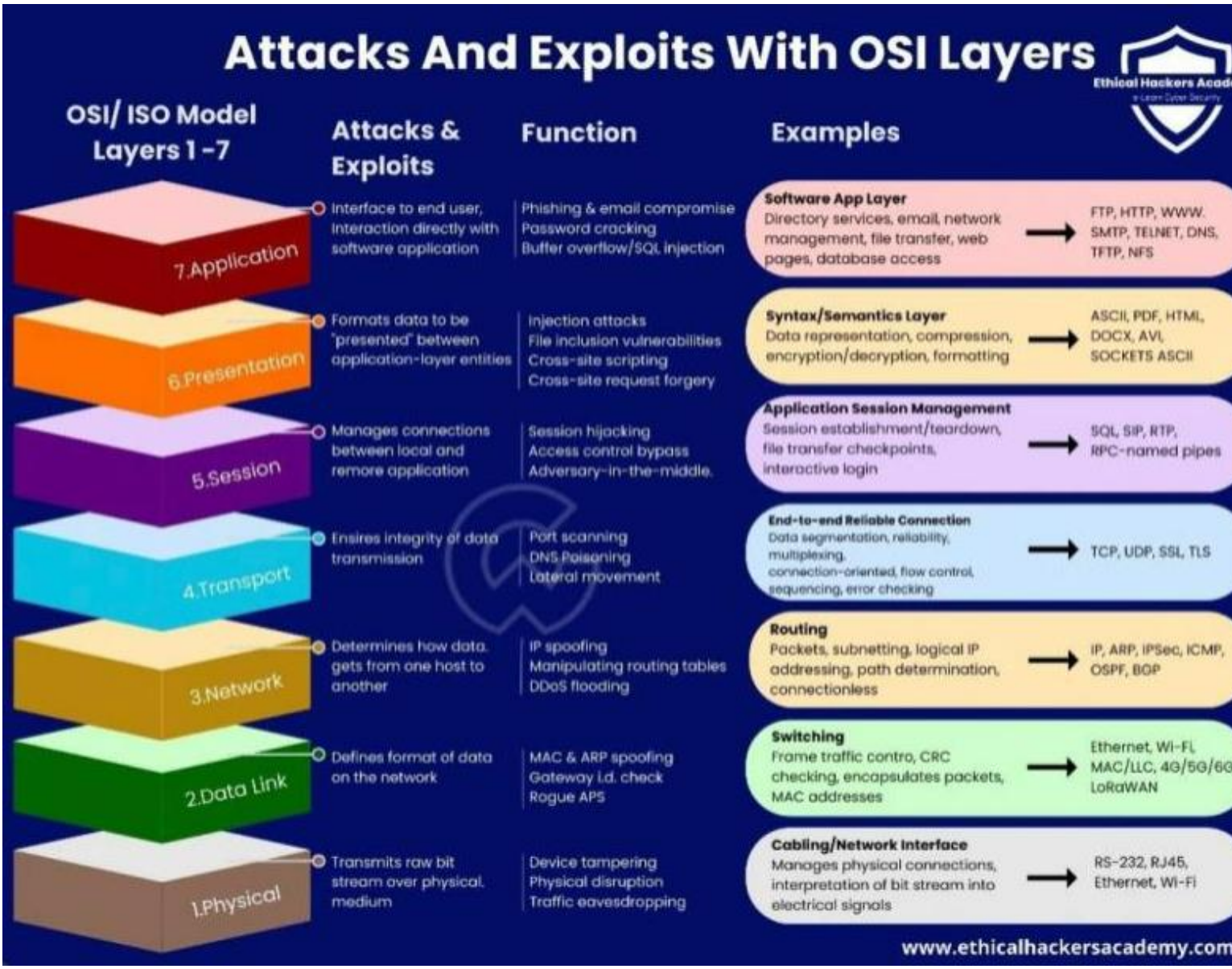
Answer: B D

Explanation

A WAF (Web Application Firewall) and NIPS (Network Intrusion Prevention System) are both examples of Layer 7 security controls. A WAF can block attacks at the application layer (Layer 7) of the OSI model by filtering traffic to and from a web server. NIPS can also block attacks at Layer 7 by monitoring network traffic for suspicious patterns and behaviors. References: CompTIA Security+ Study Guide, pages 94-95, 116-118

A network-based intrusion prevention system (NIPS) has as its core an intrusion detection system. However, whereas a NIDS can only alert when network traffic matches a defined set of rules, a NIPS can take further actions. A NIPS can take direct action to block an attack, with its actions governed by rules. By automating the response, a NIPS significantly shortens the response time between detection and action.





Question #:125 - (Exam Topic 1)

The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO

B. MFA

C. PKI

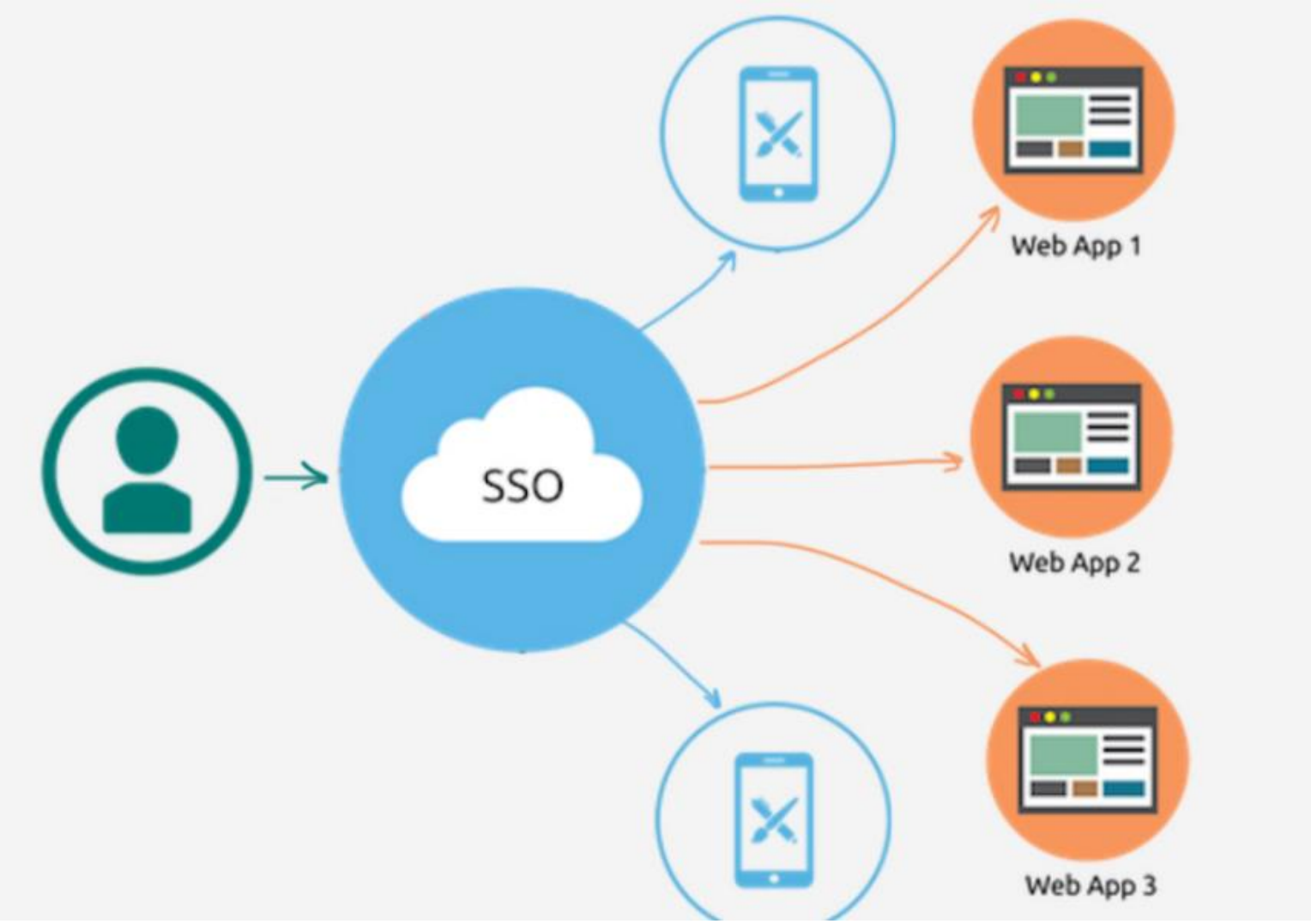
D. OLP

Answer: A

Explanation

Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one.

B: MFA (Multi-Factor Authentication): SAML alone doesn't directly enable MFA, although it can be used in conjunction with MFA to provide an additional layer of security after the initial authentication.
C: PKI (Public Key Infrastructure): SAML and PKI serve different purposes. PKI is a system for managing digital keys and certificates, whereas SAML is primarily used for identity and authentication purposes.
D: OLP (Online Payment): SAML is not directly related to online payment systems. Online payment systems typically use other protocols and security measures like HTTPS, TLS, and payment gateways.



References:

CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls. CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

Question #:126 - (Exam Topic 1)

A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

http://comptia.org/../../../etc/passwd

Which ol the following types of attacks is being attempted and how can it be mitigated?

A. XSS. implement a SIEM

B. CSRF. implement an IPS

C. Directory traversal implement a WAF

D. SQL infection, implement an IDS

Answer: C

Explanation

Detailed Explanation: The attack being attempted is directory traversal, which is a web application attack that allows an attacker to access files and directories outside of the web root directory. A WAF can help mitigate this attack by detecting and blocking attempts to access files outside of the web root directory.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4: Securing Application Development and Deployment, p. 191

http://comptia.org/../../../etc/passwd

In this malicious payload, http://comptia.org/ is the base URL.

../../ is used to traverse two levels up from the web root directory.

etc/passwd is an attempt to access the /etc/passwd file, which is a common target in Directory Traversal attacks as it can contain sensitive system information, including user account details.

This type of attack is a security vulnerability because it can allow an attacker to view or potentially manipulate files and data that they should not have access to. Web applications should be configured to validate and sanitize user input to prevent such attacks. Security measures like input validation, output encoding, and proper file access controls can help mitigate Directory Traversal vulnerabilities.

What about the security solution for mitigation and prevention of a directory traversal attack? Now, a Web Application Firewall (WAF) can help mitigate Directory Traversal attacks. WAFs are specifically designed to protect web applications from various types of attacks, including those that exploit vulnerabilities like Directory Traversal.

Here's how a WAF can contribute to mitigating Directory Traversal attacks:

Input Validation and Sanitization: WAFs can inspect incoming HTTP requests and analyze the URL parameters and request payloads. They can be configured to detect patterns consistent with Directory Traversal attempts, such as sequences of "../" or known traversal patterns. If such patterns are detected, the WAF can block or sanitize the malicious input.

Signature-Based Detection: WAFs often use signature-based detection to identify known attack patterns, including Directory Traversal. They maintain a database of attack signatures and patterns and can block requests that match these signatures.

Behavioral Analysis: Advanced WAFs can employ behavioral analysis to detect anomalies in request patterns. If a request exhibits unusual navigation of directories or access to sensitive files, the WAF may flag it as suspicious and take action to block or alert on the request.

Custom Rules: Security administrators can create custom rules in the WAF to specifically target and mitigate Directory Traversal vulnerabilities in their web applications. These rules can be tailored to the application's specific needs and known vulnerabilities.

Logging and Alerting: WAFs provide detailed logging and alerting capabilities. When a Directory Traversal attempt is detected, the WAF can log the event and send alerts to administrators for further investigation and response.

Positive Security Model: Some WAFs use a positive security model, where they define what is considered valid input and block everything else. This approach helps protect against not only known attack patterns but also unknown threats, including Directory Traversal.

It's important to note that while a WAF can be a valuable layer of defense against Directory Traversal attacks, it should not be the sole security measure. A comprehensive security strategy should also include secure coding practices, input validation within the application code, and regular security assessments to identify and remediate vulnerabilities.

Question #:127 - (Exam Topic 1)

A company would like to set up a secure way to transfer data between users via their mobile phones. The company's top priority is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

A. Cellular

B. NFC

C. Wi-Fi

D. Bluetooth

Answer: B

Explanation

Near Field Communication (NFC): NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimeters. This makes it the most secure connection method for the company's data transfer requirements.

To fulfill the requirement of transferring data between users via mobile phones with the condition that users need to be in as close proximity as possible to each other, the best choice would be Near Field Communication (NFC).

NFC is a short-range wireless communication technology that operates over very short distances, typically within a few centimeters or inches. It requires devices to be in very close proximity to each other for communication to occur, making it an ideal choice for secure data transfer in situations where physical proximity is a priority. NFC is commonly used for contactless payments, sharing small amounts of data, pairing devices, and other applications that require close-range, secure communication.

In contrast, the other options have different characteristics:

Cellular: Cellular connections provide broader coverage and are not limited to close proximity. They are designed for long-range communication and may not meet the requirement of being in close proximity.

Wi-Fi: Wi-Fi typically operates over a longer range, making it less suitable for scenarios where users need to be physically close to each other.

Bluetooth: Bluetooth is designed for short-range communication but can still have a range of several meters, which may not fulfill the requirement of users being in very close proximity.

Therefore, NFC is the most suitable technology for the company's specific need for secure data transfer between mobile phones with users being as close as possible to each other.

Question #:128 - (Exam Topic 1)

Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

A. File integrity monitoring

B. Honeynets

C. Tcpreplay

D. Data loss prevention

Answer: D

Explanation

Data loss prevention (DLP) technology is used to actively monitor for specific file types being transmitted on the network. DLP solutions can detect and prevent the unauthorized transmission of sensitive data, such as confidential documents, financial records, or personal information. They typically use a combination of content analysis, network monitoring, and policy enforcement to detect and block the transmission of sensitive data.

File integrity monitoring (FIM) is a security technology used to monitor and detect changes to files and file systems. It is used to ensure the integrity and security of critical files and systems by monitoring for unauthorized modifications, deletions, or additions.

Honeynets are a type of security technology used to detect and analyze network attacks. They involve setting up a network of decoy systems that are designed to attract attackers, allowing security researchers to observe and study their tactics and techniques.

Tcpreplay is a tool used to replay network traffic for testing, training, and troubleshooting purposes. It is not specifically designed to monitor or detect specific file types being transmitted on the network.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 99-102.

Question #:129 - (Exam Topic 1)

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption

B. Network usage rules

C. Geofencing

D. Containerization

E. Application whitelisting

F. Remote control

Correct Answer: D F

Explanation

MDM solutions, where Containerization and Remote Control are two methods, emerged to solve problems created by BYOD. With MDM, IT teams can remotely wipe devices clean if they are lost or stolen. MDM also makes the life of an IT administrator a lot easier as it allows them to enforce corporate policies, apply software updates, and even ensure that password protection is used on each device.

Containerization is a technique that creates a separate and secure space on the device for work-related data and applications. This way, personal and corporate data are isolated from each other, and IT admins can manage only the work container without affecting the user's privacy. Containerization also allows IT admins to remotely wipe only the work container if needed, leaving the personal data intact.

Remote Control: Remote control or remote management capabilities are essential for managing BYOD devices. This includes the ability to remotely wipe company data, including emails, from the device if it's lost or stolen. It also allows for enforcing security policies, such as password requirements and encryption, on the device to protect company data.

Containerization is a technique that creates a separate and secure space on the device for work-related data and applications. This way, personal and corporate data are isolated from each other, and IT admins can manage only the work container without affecting the user's privacy. Containerization also allows IT admins to remotely wipe only the work container if needed, leaving the personal data intact.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.office1.com/blog/byod-vs-mdm

Question #:130 - (Exam Topic 1)

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

A. TFTP was disabled on the local hosts

B. SSH was turned off instead of modifying the configuration file

C. Remote login was disabled in the networkd.conf instead of using the sshd.conf

D. Network services are no longer running on the NAS

Answer: B

Explanation

Secure Copy Protocol (SCP) is a protocol for securely transferring files between a local and a remote host or between two remote hosts. The protocol has certain options that can be displayed on a Linux or UNIX system using the man scp command.

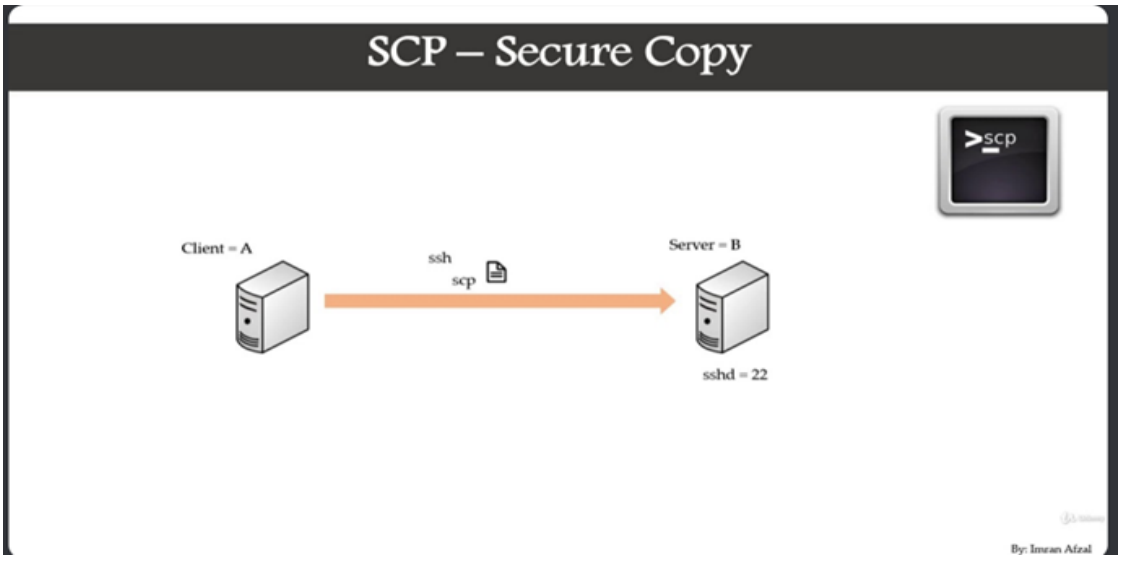
Disabling remote logins to the NAS may involve turning off certain protocols or services, such as SSH or Telnet. In this case, it is likely that the security engineer turned off SSH instead of modifying the SSH configuration file to restrict remote access. SCP uses SSH for file transfers, so disabling SSH would prevent SCP from working properly.

A. TFTP: Trivial File Transfer Protocol, is a simple high-level protocol for transferring data servers use to boot diskless workstations, X-terminals, and routers by using User Data Protocol (UDP). Its a different protocol from SSH and is not used for secure file transfers, so it is unlikely to be the cause of the issue.

C. "networkd.conf" is a configuration file that controls for global network parameters. While modifying the SSH configuration file (sshd.conf) is a common method of configuring SSH settings. If the security engineer disabled SSH instead of modifying the SSH configuration file, this would still be the most likely cause of the issue.

D. If network services were not running on the NAS, users would not be able to view the data from their PCs at all, so this is an unlikely cause of the issue.

Therefore, it is most likely that the security engineer disabled SSH instead of modifying the SSH configuration file, which has caused SCP to fail when attempting to transfer files to the NAS. The security engineer should modify the SSH configuration file to restrict remote access instead of disabling SSH entirely.



Petra Martina Vrancic
—
Today at 10:40 AM
SCP relies on SSH (Secure Shell) for secure file transfer. If SSH is disabled or turned off, SCP will not function. The scenario describes that users are unable to use SCP, which suggests a problem with the SSH service. Turning off SSH without modifying the configuration file can result in the service being completely disabled, affecting not only remote logins but also services like SCP that rely on SSH. Checking the SSH configuration file (typically sshd_config) and ensuring that it is properly configured for remote access is essential for allowing SCP transfers.

David Berrios
—
Today at 10:40 AM
b

Question #:131 - (Exam Topic 1)

A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating the incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services

B. SQLi on the field to bypass authentication

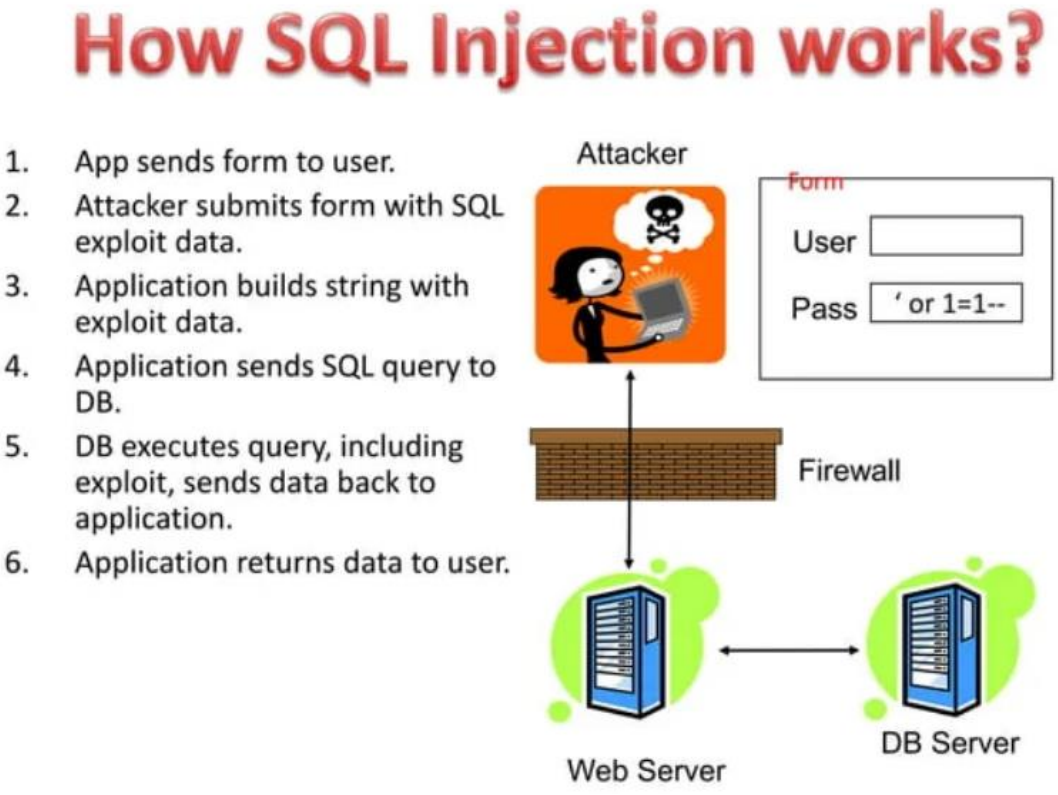
C. Execution of a stored XSS on the website

D. Code to execute a race condition on the server

Answer: B

Explanation

The input "admin' or 1=1--" in the username field is an example of SQL injection (SQLi) attack. In this case, the attacker is attempting to bypass authentication by injecting SQL code into the username field that will cause the authentication check to always return true. References: CompTIA Security+ SY0-601 Exam Objectives: 3.1 Given a scenario, use appropriate software tools to assess the security posture of an organization.



Question #:132 - (Exam Topic 1)

Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

A. ISO 27701

B. The Center for Internet Security

C. SSAE SOC 2

D. NIST Risk Management Framework

Answer: D

Explanation

The NIST Risk Management Framework is a six-step process that helps organizations manage and mitigate risks to their systems and data. The six steps include:

Categorize Information Systems

Select Security Controls

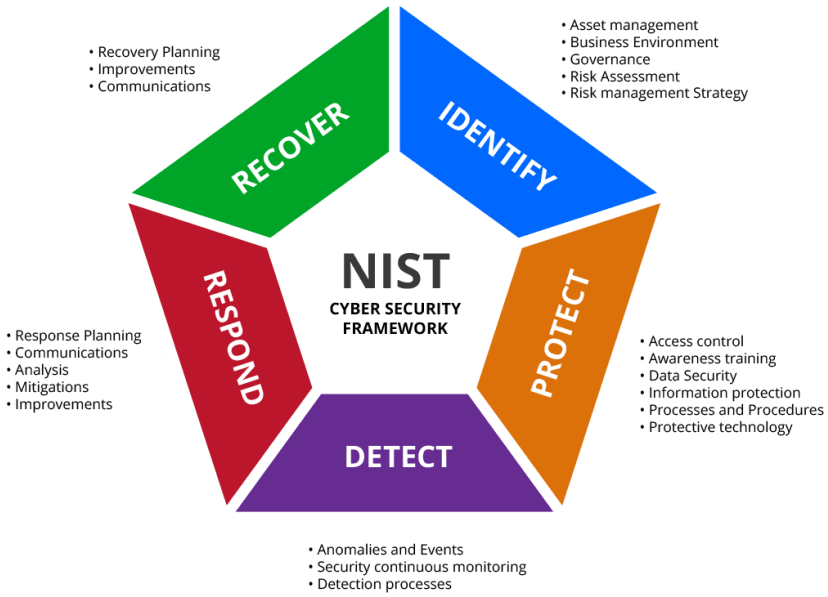
Implement Security Controls

Assess Security Controls

Authorize Information System

Monitor Security Controls

The framework includes continuous monitoring and emphasizes the importance of hardware and software inventory, vulnerability management, and risk management in all network environments.



A. ISO 27701: This is a privacy management standard that specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS) in the context of an organization's overall business risks. It focuses on protecting personal data and ensuring compliance with privacy regulations. While it may include security measures, it does not specifically focus on the six steps mentioned in the question.

B. The Center for Internet Security: This is a nonprofit organization that provides cybersecurity resources and tools, including benchmarks and controls for various systems and platforms. The Center for Internet Security has developed a

set of critical security controls that include continuous vulnerability management and monitoring, but it does not provide a comprehensive framework like the NIST Risk Management Framework.

C. SSAE SOC 2: This is a standard developed by the American Institute of Certified Public Accountants (AICPA) for auditing and reporting on the controls at a service organization related to security, availability, processing integrity, confidentiality, and privacy. It is used to assess and report on the effectiveness of controls related to these areas, but it does not provide a framework for managing risks in all network environments like the NIST Risk Management Framework does.

Question #:133 - (Exam Topic 1)

A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:

- Must be able to differentiate between users connected to WiFi
- The encryption keys need to change routinely without interrupting the users or forcing reauthentication
- Must be able to integrate with RADIUS
- Must not have any open SSIDs

Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise

B. WPA3-PSK

C. 802.11n

D. WPS

Answer: A

Explanation

Detailed Explanation: WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication. Additionally, WPA2-Enterprise does not allow for open SSIDs.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7: Securing Networks, p. 317

WPA2-Enterprise would be the best option to accommodate the given requirements. It supports RADIUS integration, provides individual user authentication through 802.1X, and allows for automatic key rotation. Additionally, it does not have an open SSID, as it requires a user to provide credentials for access.

WPA3-Personal allows for better password-based authentication even when using non-complex combinations. WPA3 uses Simultaneous Authentication of Equals (SAE) to provide stronger defenses against password guessing. SAE is a secure key establishment protocol.

802.11n is a wireless standard and does not address the security requirements specified.

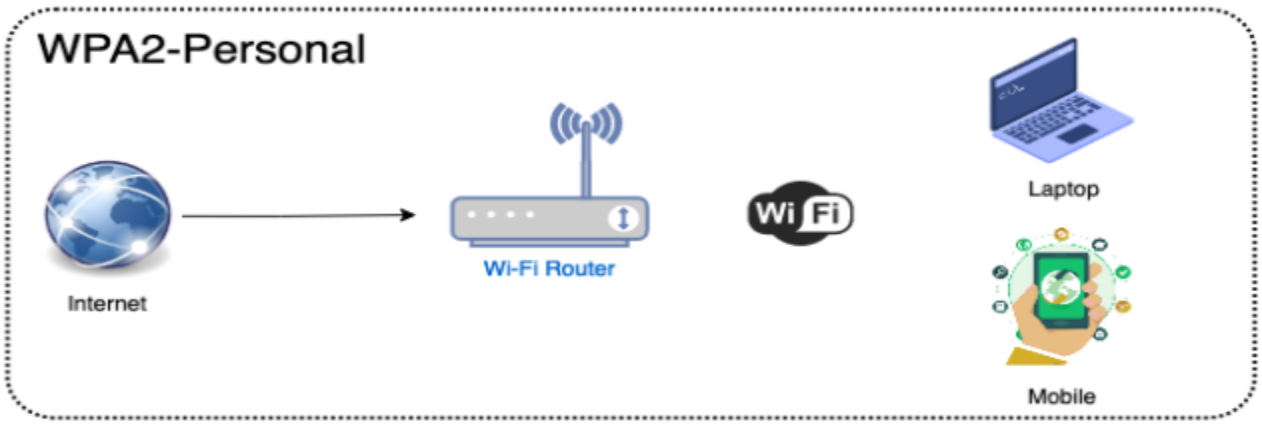
WPS is a configuration protocol and does not provide the necessary security features.

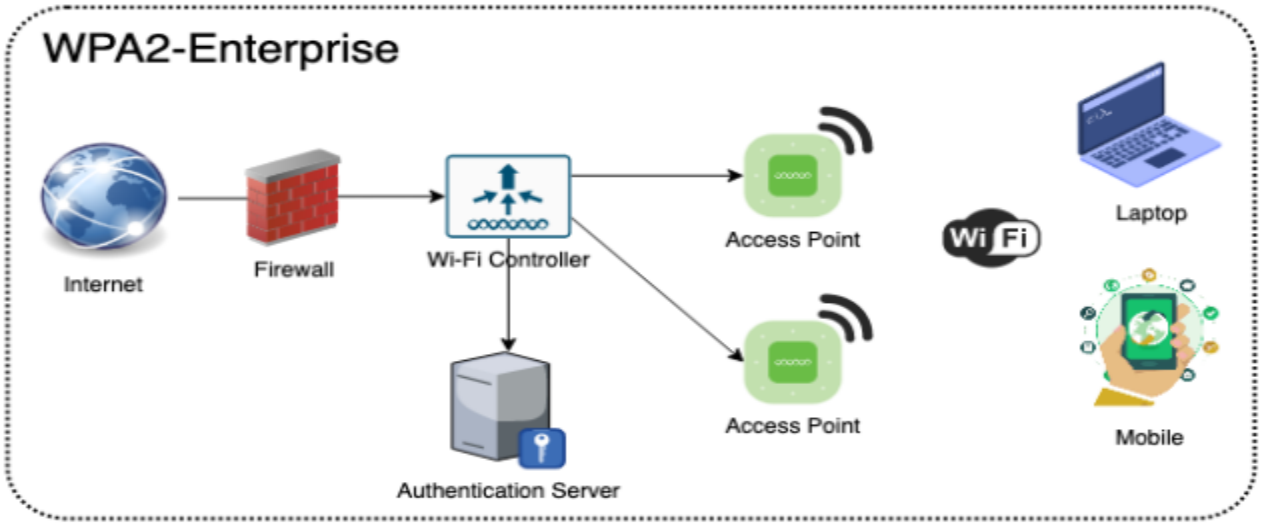
David Berrios

—

Today at 10:46 AM

WPA2-Enterprise supports user differentiation through individual user authentication via raidus 1





Question #:134 - (Exam Topic 1)

A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot

B. Differential

C. Full

D. Tape

Answer: B

Explanation:

Differential: In a differential backup, only the files that have changed since the last full backup was completed are backed up. This also implies that periodically a full backup needs to be accomplished. The frequency of the full backup versus the interim differential backups depends on your organization and needs to be part of your defined strategy. Restoration from a differential backup requires two steps: the last full backup first needs to be loaded and then the last differential backup performed can be applied to update the files that have been changed since the full backup was conducted. Again, this is not a difficult process, but it does take some time. The amount of time to accomplish the periodic differential backup, however, is much less than that for a full backup, and this is one of the advantages of this

method. Obviously, if a lot of time has passed between differential backups, or if most files in your environment change frequently, then the differential backup does not differ much from a full backup. It should also be obvious that to accomplish the differential backup, the system has to have a method to determine which files have been changed since some given point in time. The archive bit is not cleared in a differential backup since the key for a differential is to back up all files that have changed since the last full backup.

Differential backup is a type of backup that backs up all data that has changed since the last full backup. This backup method offers faster recovery than a full backup, as it only needs to restore the full backup and the differential backup, reducing the amount of data that needs to be restored. It also uses less storage than a full backup as it only stores the changes made from the last full backup.

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

Question #:135 - (Exam Topic 1)

A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis

B. The Cyber Kill Chain

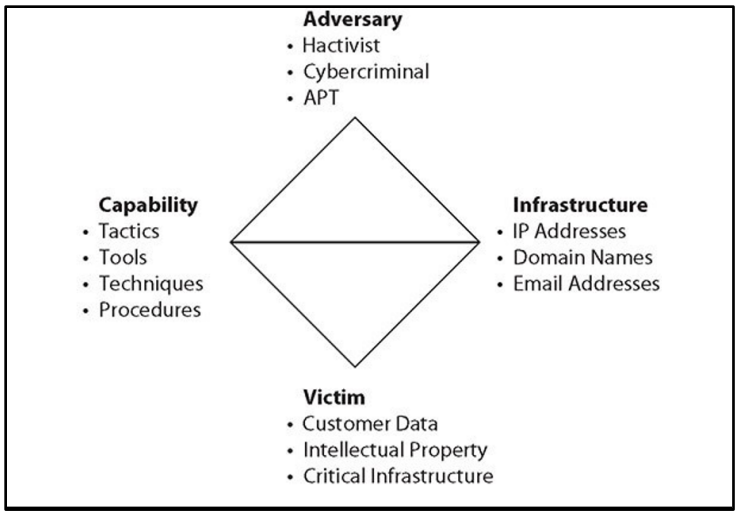
C. The MITRE CVE database

D. The incident response process

Answer: A

Explanation

The Diamond Model is a framework for analyzing cyber threats that focuses on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, security researchers can gain a better understanding of the threat landscape and develop more effective security strategies.



Question #:136 - (Exam Topic 1)

As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is recurring?

A. Creating a playbook within the SOAR

B. Implementing rules in the NGFW

C. Updating the DLP hash database

D. Publishing a new CRL with revoked certificates

Answer: A

Explanation

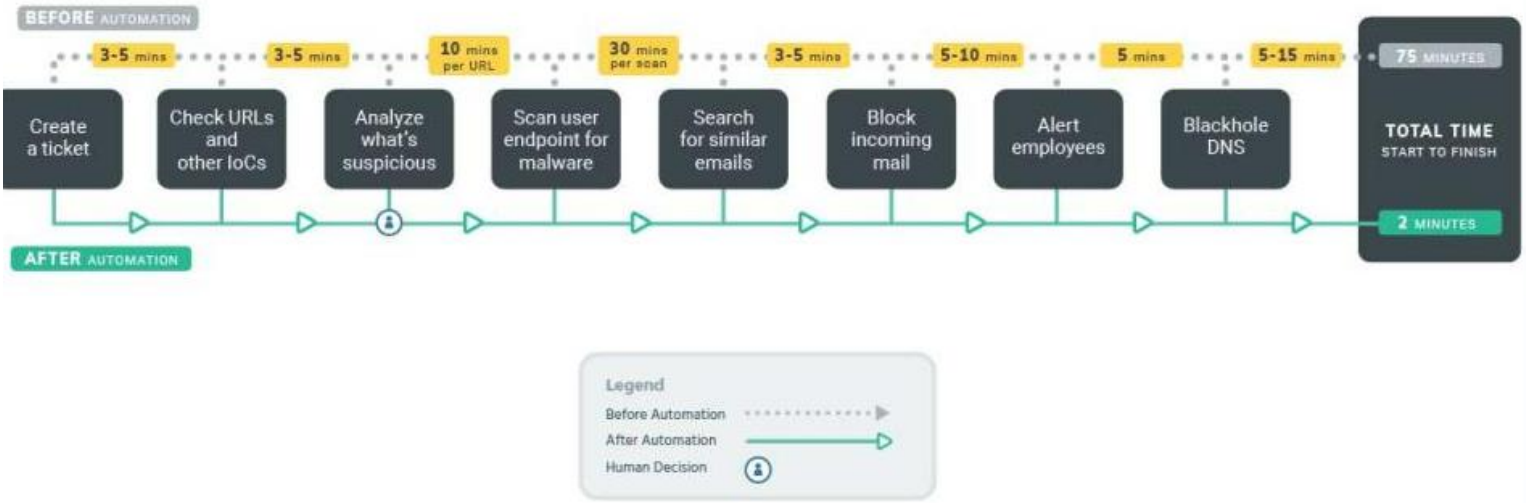
Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 352-354

Security Orchestration, Automation, and Response Automation is the action of scripting a single activity, while orchestration is the action of coordinating multiple automations (and possibly manual activity) to perform a complex, multistep task. In the case of security orchestration, automation, and response (SOAR), this task is principally incident response, though the technologies can also be used for tasks such as threat hunting too. SOAR is designed as a solution to the problem of the volume of alerts overwhelming analysts' ability to respond, measured as the mean time to respond (MTTR). A SOAR may be implemented as a standalone technology or integrated with a SIEM—often referred to as a next-gen SIEM. The basis of SOAR is to scan the organization's store of security and threat intelligence, analyze it using machine/deep learning techniques, and then use that data to automate and provide data enrichment for the workflows that drive incident response and threat hunting. It can also assist with provisioning tasks, such as creating and deleting user accounts, making shares available, or launching VMs from templates, to try to eliminate configuration errors. The SOAR will use technologies such as cloud and SDN/SDV APIs, orchestration tools, and cyberthreat intelligence (CTI) feeds to integrate the different systems that it is managing. It will also leverage technologies such as automated malware signature creation and user and entity behavior analytics (UEBA) to detect threats. An incident response workflow is usually defined as a playbook. A playbook is a checklist of actions to perform to detect and respond to a specific type of incident. A playbook should be made highly specific by including the query strings and signatures that will detect a particular type of incident. A playbook will also account for compliance factors, such as whether an incident must be reported as a breach plus when and to whom notification must be made. Where a playbook is implemented with a high degree of automation from a SOAR system, it can be referred to as a runbook, though the terms are also widely used

interchangeably. The aim of a runbook is to automate as many stages of the playbook as possible, leaving clearly defined interaction points for human analysis. These interaction points should try to present all the contextual information and guidance needed for the analyst to make a quick, informed decision about the best way to proceed with incident mitigation.

Official CompTIA Security+ Instructor Guide

Why might NGFW not be the best option? Well a NGFW may not be the only appliance residing at the network's security infrastructure but there might be several others like stateful and stateless firewalls, NIDS, NIPS, HIDS, routers/switches capable of catching and reporting incidents, etc. As the SOC, in order not to miss to detect any recurring malicious incident, instead of leaning on a single device, you need to create a robust SOAR playbook which is collecting the logs even from several different security devices, event from the SIEM, so that it is going to throw alert about a pre-occured malicious activity.



Question #:137 - (Exam Topic 1)

The Chief Information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

A. SAML

B. TACACS+

C. Password vaults

D. OAuth

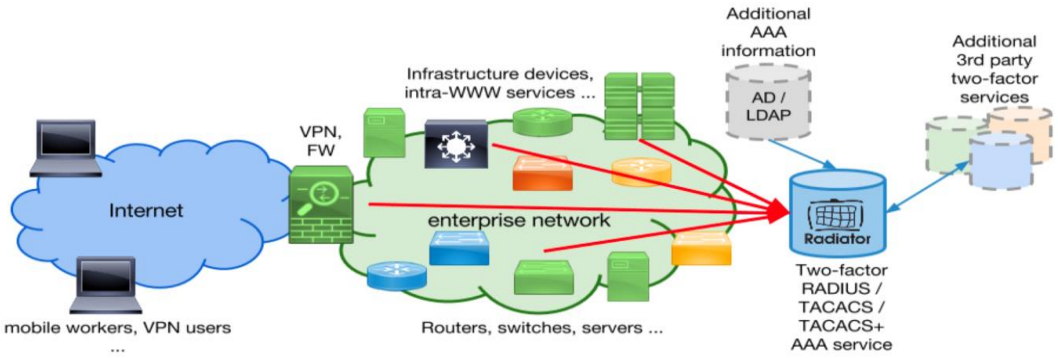
Answer: B

Explanation

B. TACACS+ is a protocol used for remote authentication, authorization, and accounting (AAA) that can be used to replace shared passwords on routers and switches. It provides a more secure method of authentication that allows for centralized management of access control policies. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

A. OAuth (Open Authorization) is a secure authentication and authorization protocol commonly used for enabling third-party applications or services to access a user's data without exposing their password. It allows users to grant limited access to their resources on one site (known as the "resource server") to another site or application (known as the "client") without sharing their credentials directly.

D. SAML (Security Assertion Markup Language) is an XML-based standard for exchanging authentication and authorization data between parties, typically between an identity provider (IdP) and a service provider (SP). It can be used for single sign-on (SSO) scenarios but still typically involves initial username and password authentication.



Mamurjon Ismatov

Today at 10:55 AM

Terminal Access Controller Access-Control System Plus is a network security protocol that provides centralized authentication, authorization, and accounting

David Berrios

Today at 10:56 AM

to meet the requirement of retiring the use of shared passwords on routers and switches, the best choice is TACACS+ (Terminal Access Controller Access-Control System Plus)

Question #:138 - (Exam Topic 1)

Which of the following would produce the closest experience of responding to an actual incident response scenario?

A. Lessons learned

B. Simulation

C. Walk-through

D. Tabletop

Answer: B

Explanation

closest experience = simulation

A simulation is a practice exercise that closely mimics a real incident response scenario. It involves simulating various aspects of an incident, such as the incident itself, the response team's actions, and the decision-making process. Simulations often involve using realistic scenarios, tools, and environments to test the effectiveness of the incident response plan, the skills of the team, and the coordination of actions. This provides a hands-on, immersive experience that closely resembles an actual incident response situation.
While "tabletop" and "walk-through" exercises are also used in incident response planning, they tend to be more focused on discussing and reviewing procedures rather than actively simulating the incident.

"Lessons learned" typically involves a retrospective analysis of past incidents and may not involve active participation in a simulated incident response scenario.

Petra Martina Vrancic

—

Today at 10:58 AM

simulation involves creating a realistic scenario that mimics an actual incident.

Question #:139 - (Exam Topic 1)

Which of the following roles would MOST likely have direct access to the senior management team?

A. Data custodian

B. Data owner // is an executive

C. Data protection officer

D. Data controller

Answer: C

Explanation

A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders.

A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.

The other options are not correct because:

A. Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.

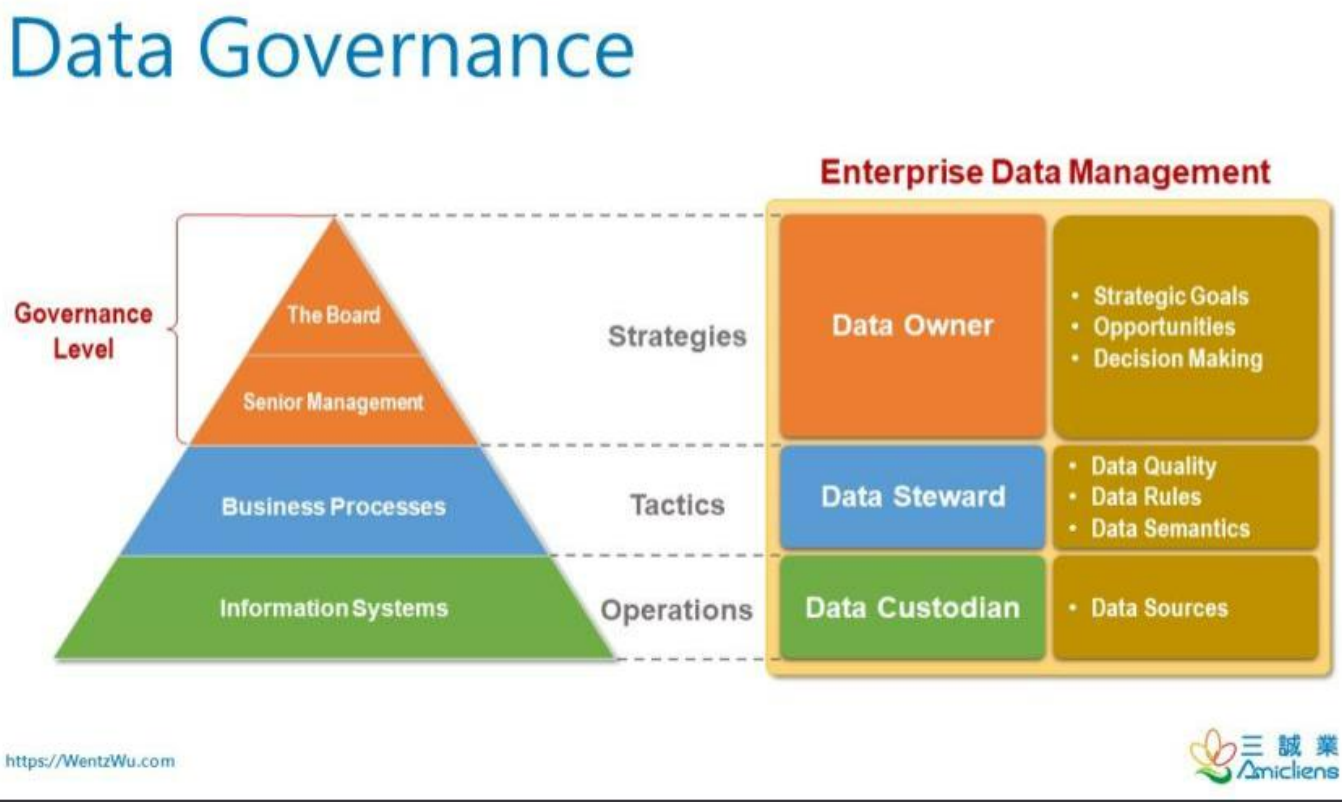
B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.

D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.

According to CompTIA Security+ SY0-601 Exam Objectives 2.3 Given a scenario, implement secure protocols:

"A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization."

References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://gdpr-info.eu/issues/data-protection-officer/



Question #:140 - (Exam Topic 1)

A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?

A. Implementation of preventive controls

B. Implementation of detective controls

C. Implementation of deterrent controls

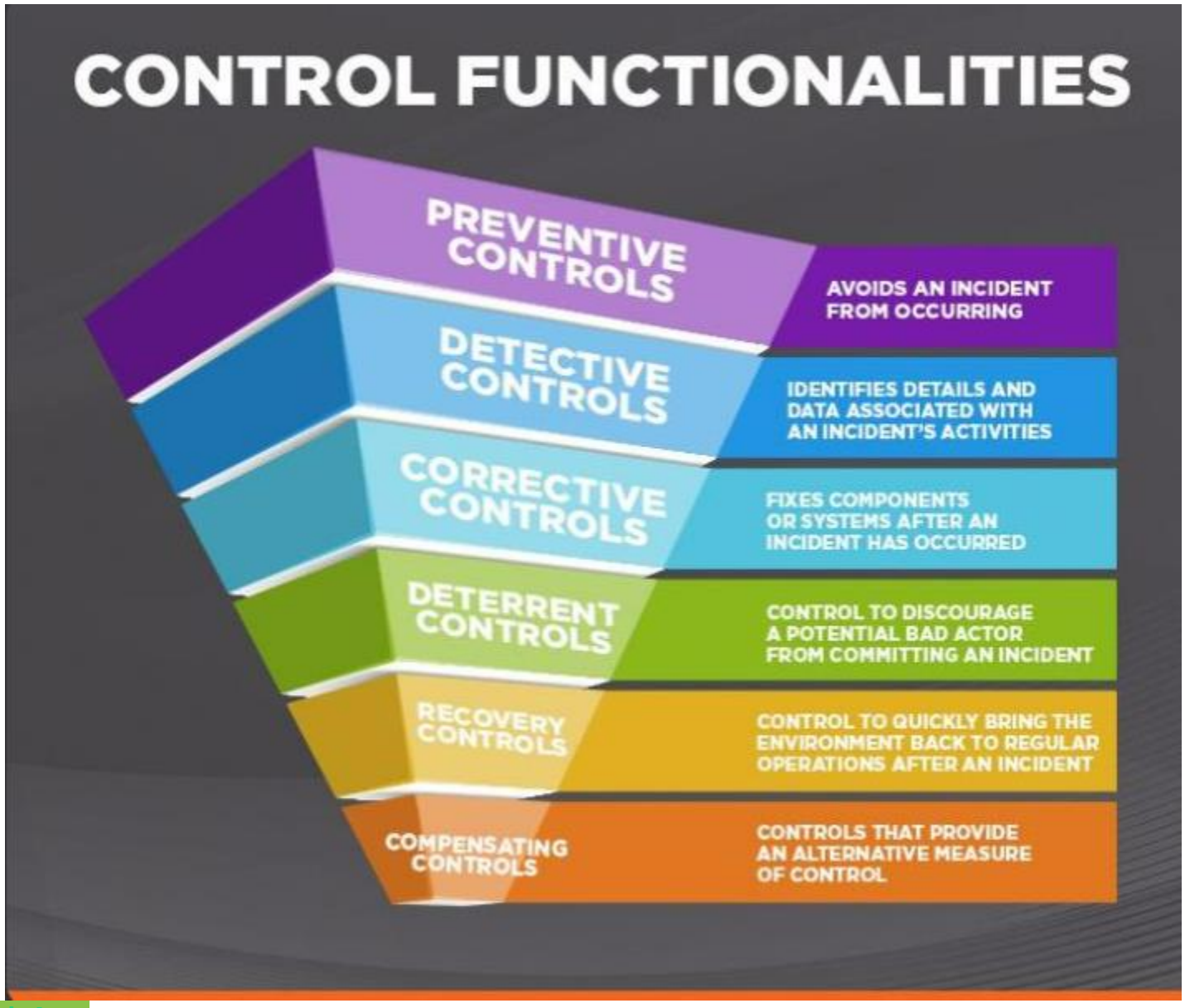
D. Implementation of corrective controls

Answer: B

Explanation

A Security Information and Event Management (SIEM) system is a tool that collects and analyzes security-related data from various sources to detect and respond to security incidents. References: CompTIA Security+ Study Guide 601, Chapter 5

The company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. In essence, Detective controls are security measures that are designed to identify and alert on security incidents and anomalies after they have occurred. In this case, the SIEM system is used to detect and alert on malicious activity that has been blocked by the antivirus and web content filters. It helps in monitoring the network for signs of security threats and provides real-time alerts to security teams, allowing them to investigate and respond to incidents promptly.



Burak Acar

—

Today at 11:07 AM

SIEM=Detective

Question #:141 - (Exam Topic 1)

A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor

B. Service requestor

C. Identity provider ////verifies the identity of a user and providing authentication and authorization

D. Service provider /// consumes the security tokens generated by the identity provider to allow access to protected resources or services.

E. Tokenized resource

F. Notarized referral

Answer: C D

Explanation

A single pane of glass is **a management console that presents data from multiple sources in a unified display**.

Single pane of glass monitoring **enables developers, operations, security, and business teams to collaborate on shared data using the same view**. Unified monitoring with Datadog allows you to easily correlate metrics, traces, logs, and more in real time using a shared pane of glass.

C. Identity provider - An identity provider (IdP) is responsible for verifying the identity of a user and providing authentication and authorization data in the form of security tokens that can be used to access various services and resources.

D. Service provider - A service provider (SP) consumes the security tokens generated by the identity provider to allow access to protected resources or services.

An identity processor is not a standard role in authentication and authorization protocols.

Service requestor is a term that is not commonly used in this context.

Tokenized resource and notarized referral are not standard terms used in authentication and authorization protocols.

A single pane of glass is **a management console that presents data from multiple sources in a unified display**.

Single pane of glass monitoring **enables developers, operations, security, and business teams to collaborate on shared data using the same view**. Unified monitoring with Datadog allows you to easily correlate metrics, traces, logs, and more in real time using a shared pane of glass.

The other options (A, B, E, F) are not directly related to the standard roles involved in implementing authentication and authorization with security tokens using assertions in the context of identity and access management.

Question #:142 - (Exam Topic 1)

Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

A. Penetration testing

B. Code review

C. Wardriving

D. Bug bounty

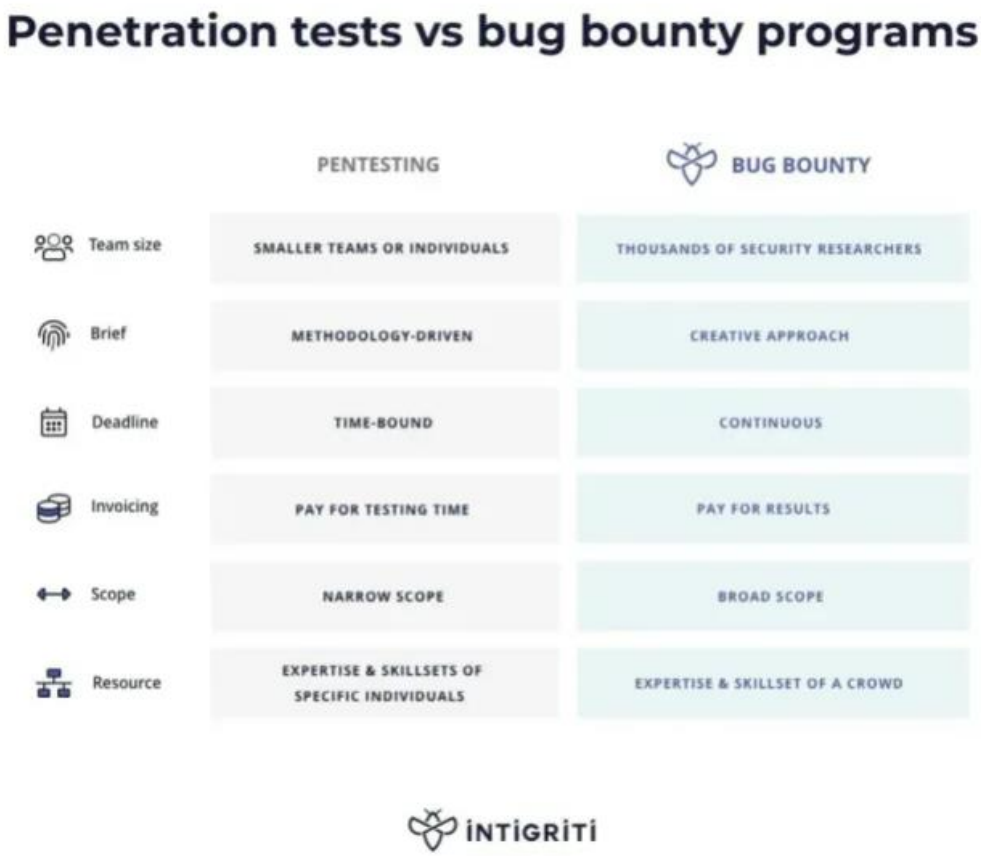
Answer: D

Explanation

A bug bounty is a technique that compensates researchers for finding vulnerabilities in software or systems. A bug bounty program is an initiative that offers rewards, usually monetary, to ethical hackers who report security flaws to the owners or developers of the software or system. Bug bounty programs are often used by companies such as Meta (formerly Facebook), Google, Microsoft, and others to improve the security of their products and services

Bug bounty programs compensate researchers, often financially, for finding vulnerabilities in software, websites, or other technology. These programs provide an additional layer of security testing and incentivize researchers to report vulnerabilities instead of exploiting them.

Penetration testing and code review are methods of testing the security of an organization's systems or applications, but they do not involve compensation for researchers who find vulnerabilities. Unlike a vulnerability assessment, which typically just catalogs vulnerabilities, a pen test attempts to exploit vulnerabilities to see how much access they allow.



Azamat Iskakov

—

Today at 11:15 AM

bug bounty researchers get paid for each vulnerability they find. Pentesters get paid monthly like a regular employee

Question #:143 - (Exam Topic 1)

Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area? (Select TWO).

A. Barricades

B. Thermal sensors

C. Drones

D. Signage

E. Motion sensors

F. Guards

G. Bollards

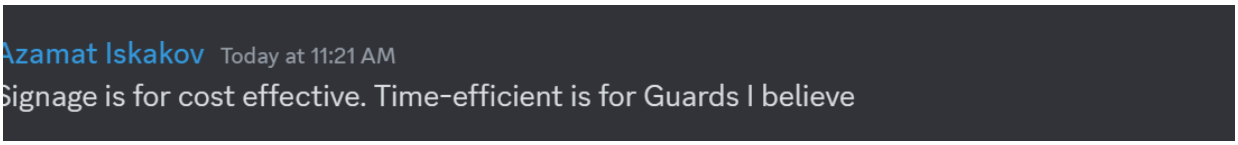
Answer: D F

Explanation

Signage is a cost-effective and visible way to deter intrusions by warning potential trespassers of the consequences of unauthorized entry. Signs can be easily deployed and are often enough to deter casual trespassers.

Guards are a cost-effective and efficient way to deter intrusions by providing a physical presence at the perimeter. Guards can monitor the area and respond quickly to any intrusions. They can also interact with potential trespassers, providing a human face and voice to the warning messages on the signage.

The other controls listed, such as barricades, thermal sensors, drones, motion sensors, and bollards, may also be useful in deterring intrusions, but they are likely to be more expensive and time-consuming to deploy and maintain than signage and guards. Additionally, some of these controls may require specialized training or equipment, which could add to the costs and time required for deployment.



From Eitan

The key word is "deter". When you want to deter intrusions in a cost effective and time-efficient way, Signage and Guards would be the best solutions. Preparing signages takes least amount of time and military do not spend so much money to guards as they're already on duty after all.

So, we should think the types of precautions based on the entity. While these solutions are suitable for military, it wouldn't be that suitable for civilian companies.

[3:11 PM]

Barricades wouldn't be that deterrent as intruders do not use normal ways.

If you put a signage like there is electricity with the fence or dogs are here or trespassing is so dangerous that you might be shot, that would deter anybody.

[3:15 PM]

And imagine that you have those kind of precautions but do not have proper signages indicating them, that would not be so effective to deter the intruders from trying to break into.

Question #:144 - (Exam Topic 1)

An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box

B. Red-leam

C. Bug bounty

D. Gray-box

E. Black-box

Answer: C

Explanation

Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

Bug bounty programs are a type of vulnerability assessment where organizations offer financial or other incentives to external security researchers or the public for finding and reporting security vulnerabilities in their software or systems. The security firm hired by the enterprise is offering to pay for each vulnerability discovered, which indicates that they are conducting a bug bounty program.

Note: **pay for each vulnerability = bug bounty**

Question #:145 - (Exam Topic 1)

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic.

Which of the following should the analyst use?

A. openssl

B. hping

C. netcat

D. tcpdump

Correct answer: D

Explanation

To verify that a client-server (non-web) application is sending encrypted traffic, the security analyst should use a packet capture tool such as tcpdump. Tcpdump is a command-line tool that allows the analyst to capture and analyze network traffic.

The analyst can use tcpdump to capture packets exchanged between the client and server, and then examine the packets to verify that they are encrypted. Tcpdump can capture traffic on a specific interface, port, or IP address, and can filter traffic based on various criteria.

What is tcpdump used for?

Tcpdump is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool. A powerful and versatile tool that includes many options and filters, tcpdump can be used in a variety of cases.

OpenSSL is a library that provides cryptographic functionality to **applications** such as secure **web** servers.

OpenSSL is a software library for applications that provide secure communications over computer networks against eavesdropping, and identify the party at the other end. It is widely used by Internet servers, including the majority of HTTPS websites.

Question #:146 - (Exam Topic 1)

An attacker replaces a digitally signed document with another version that goes unnoticed. Upon reviewing the document's contents, the author notices some additional verbiage that was not originally in the document but can't validate an integrity issue. Which of the following attacks was used?

A. Cryptomalware

B.Hash Subsition

C. Collision

D. Phishing

Answer: C

This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

A *collision* attack is where two different inputs yield the same output of a hash function. Through the manipulation of data, subtle changes are made that are not visible to the user yet create different versions of a digital file. With the creation of many different versions and the use of the birthday attack to find a collision between any two of the many versions, an attacker has a chance to create a file with changed visible content but identical hashes.

A collision attack was used, in which the attacker replaced a digitally signed document with a different version that was identical in every way except for the added verbiage.

A collision attack takes advantage of weaknesses in cryptographic hash functions, causing two different inputs to produce the same hash value. In this case, the attacker was able to produce a second version of the document that had the same digital signature as the original, allowing it to go unnoticed.

A hash algorithm can be compromised with what is called a collision attack, in which an attacker finds two different messages that hash to the same value

prepending refers to **when an attacker prepends, or attaches, a trustworthy value like "RE:" or "MAILSAFE: PASSED" to a message in order to make the message appear more trustworthy**. Values like that are usually automatically added by a user's email client.

Question #:147 - (Exam Topic 1)

A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.

B. Define the PC firewall rules to limit access.

C. Encrypt the disk on the storage device.

D. Plug the storage device in to the UPS

Answer: C

Explanation

Encrypting the disk on the storage device ensures that even if malicious files are present on the storage device, they cannot be easily accessed or executed without the proper decryption key. This protects the data on the storage device and mitigates the risk of malware spreading to the PC.

C is a form of FDE

Changing the default settings on the PC: This is a good practice for security but doesn't specifically address the threat from the storage device.

Defining PC firewall rules to limit access: Firewall rules control network traffic, so they are more relevant for network security. They may not prevent the introduction of malicious files from a storage device.

Plugging the storage device into the UPS (Uninterruptible Power Supply): This is related to power management and hardware reliability but does not provide protection against malicious files on the storage device.

Question #:148 - (Exam Topic 1)

An analyst is generating a security report for the management team. Security guidelines recommend disabling all listening to **unencrypted services**. Given this output from Nmap:

PORT	STATE
21/tcp	filtered
22/tcp	open
23/tcp	open
443/tcp	open

Which of the following should the analyst recommend to disable?

A. 21/tcp

B. 22/tcp

C. 23/tcp

D. 443/tcp

Answer: C

The analyst should recommend disabling Telnet (port 23/tcp) since it is an **unencrypted** service that is commonly used by attackers to perform credential harvesting attacks.

23/tcp: Port 23 is used for Telnet, which is not an encrypted protocol. Telnet transmits data in plain text, and as a result, it is considered insecure for most purposes. It is recommended to use secure alternatives like SSH instead of Telnet.

443/tcp: Port 443 is used for encrypted communication using the HTTPS (HTTP Secure) protocol. HTTPS encrypts the data transferred between a web browser and a web server, ensuring that it cannot be easily intercepted or tampered with during transit. It's commonly used for secure web browsing, online banking, and other sensitive transactions.

21/tcp: Port 21 is used for FTP (File Transfer Protocol), which does not inherently encrypt data. However, there are secure variants of FTP, like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol), which use different ports (990/tcp for FTPS and 22/tcp for SFTP) to provide encryption.

However, in the question it was labeled as “filtered” at the nmap query result. "filtered" does not definitively indicate whether a port is open or closed; it simply means that Nmap was unable to determine the status due to some external factors like firewall rules or network conditions. To further investigate the port's status, security analysts may need to perform additional testing or analyze firewall rules and network configurations. So that is not the correct answer.

22/tcp: Port 22 is used for SSH (Secure Shell) communication. SSH is a cryptographic network protocol that provides secure access to a remote device or server. It encrypts the data exchanged during remote shell access, file transfers, and other interactions.

Question #:149 - (Exam Topic 1)

Which of the following conditions impacts data sovereignty?

A. Rights management

B. Criminal investigations

C. Healthcare data

D. International operations

Answer: D

Explanation

Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations. References:

CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

Data sovereignty laws can inhibit that mobility. It can mean additional restrictions on how businesses can move data between two countries. It can also mean that specific cloud locations and services cannot be used. There might also be rules regarding the degree of encryption for data while it's in transit and at rest.

• Data sovereignty: Refers to a jurisdiction preventing or restricting processing and storage from taking place on systems do not physically reside within that jurisdiction.

Data sovereignty may demand certain concessions on your part, such as using location-specific storage facilities in a cloud service. ✔ Jurisdiction that enforces personal data processing and storage regulations

• Geographical considerations ✔ Select storage locations to mitigate sovereignty issues ✔ Define access controls on the basis of client location.

Rights management (A) refers to the process of controlling access to digital content and determining how it can be used and distributed.

Criminal investigations (B) are a law enforcement matter and may involve accessing data stored in a particular jurisdiction, but it does not directly impact data sovereignty.

Healthcare data (C) may be subject to specific privacy and security regulations, but this also does not directly impact data sovereignty.

Question #:150 - (Exam Topic 1)

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive

B. Compensating

C. Corrective

D. Detective

Answer: D

Explanation

A SIEM is a security solution that helps detect security incidents by monitoring for notable events across the enterprise. A detective control is a control that is designed to detect security incidents and respond to them. Therefore, a SIEM

represents a detective control.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

Farid Abbasov

—

Today at 11:35 AM

siem = dedective

Question #:151 - (Exam Topic 1)

Which of the following is a cryptographic concept that **operates** on a fixed length of bits?

A. Block cipher

B. Hashing

C. Key stretching

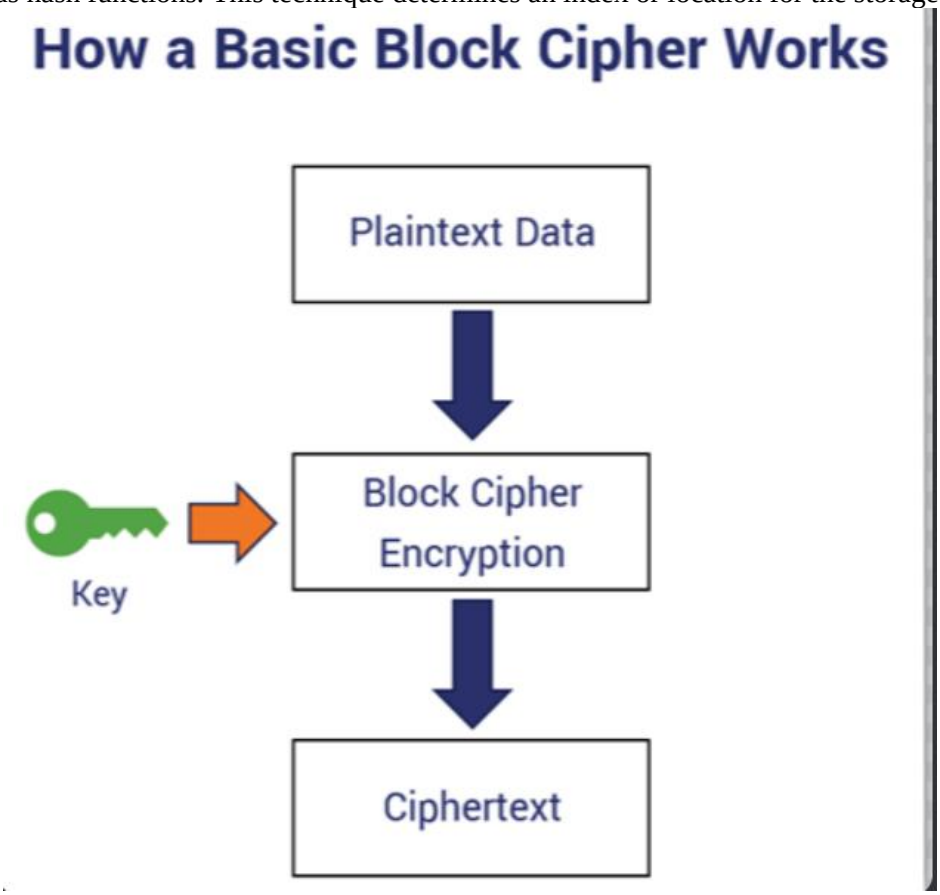
D. Salting

Answer: A

Explanation

block cipher: An algorithm that operates on fixed-length blocks of data, one block at a time, rather than encrypting one bit at a time as in stream ciphers.

Hashing refers to the process of generating a fixed-size output from an input of variable size using the mathematical formulas known as hash functions. This technique determines an index or location for the storage of an item in a data structure.



Question #:152 - (Exam Topic 1)

During an incident, a company's CSIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate internet point of presence

B. Create and apply micro segmentation rules.

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

D. Apply network blacklisting rules for the adversary domain

Correct Answer: B

Explanation

Microsegmentation is a security technique that involves dividing a network into smaller segments to reduce the risk of lateral spread. By creating and applying microsegmentation rules, the CIRT can restrict communication between the infected PC and other devices on the network, limiting the ability of the malware to propagate.

In addition, creating and applying microsegmentation rules can also limit the risk of the adversary detecting any changes. If the microsegmentation rules are applied in a way that is transparent to the malware and the adversary, there is less risk of detection.

Segmentation is also the network process of separating network elements into segments and regulating traffic between the segments. The presence of a segmented network creates security barriers for unauthorized accessors through the inspection of packets as they move from one segment to another. This can be done in a multitude of ways—via MAC tables, IP addresses, and even tunnels, with devices such as firewalls and secure web gateways inspecting at each connection. The ultimate in segmentation is the zero-trust environment, where microsegmentation is used to continually invoke the verification of permissions and controls. All of these can be performed in a cloud network. Also, as with the other controls already presented, the details are in the service level agreement (SLA) with the cloud service provider.

****

The ability to keep multiple instances of software separated so that each instance only sees and can affect itself.

Question #:153 - (Exam Topic 1)

Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyber activity?

A. Intelligence fusion

B. Review reports

C. Log reviews

D. Threat feeds

Answer: D

Explanation

Threat feeds are data streams that are compiled through artificial intelligence (AI) and provide insight on current cyberintrusions, phishing, and other malicious cyberactivity.

Threat feeds are a mechanism for users to receive current data on cyber intrusions, phishing and other types of fresh information on malicious activity. They are continuous data streams compiled via artificial intelligence to provide insights into risks and trends as they occur.

What is intelligence fusion in cyber security?

The cyber fusion approach focuses on integrating threat intelligence across all security aspects of an organization to tackle the targeted threats. This strategy allows security teams to contextualize insights into malicious activities and meaningfully orchestrate cybersecurity operations across the network.

A List of the Best Open Source Threat Intelligence Feeds

- Emerging Threats. ...
- FBI InfraGard. ...
- Dan.me.uk. ...
- CINS Score. ...
- Blocklist.de. ...
- hpHosts. ...
- AlienVault OTX. ...
- Abuse.ch Feodo Tracker.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Glossary, p. 767.

Question #:154 - (Exam Topic 1)

If a current private key is compromised, which of the following would ensure it cannot be used to decrypt any historical data?

A. Perfect forward secrecy

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption

Answer: A

Explanation

Perfect Forward Secrecy (PFS) is a property of secure communication protocols that ensures that even if a private key is compromised in the future, it will not compromise past encrypted sessions. This is achieved by using a different key

for each session, and discarding it after the session is over. This way, even if one session key is compromised, it will only affect the confidentiality of that particular session, and not any other sessions or future sessions. PFS is an important security feature that is often used in secure communication protocols such as TLS and VPNs.

Perfect forward secrecy would ensure that it cannot be used to decrypt all historical data. Perfect forward secrecy (PFS) is a security protocol that generates a unique session key for each session between two parties. This ensures that even if one session key is compromised, it cannot be used to decrypt other sessions.

Note: Perfect forward secrecy is used in top secret data

Question #:155 - (Exam Topic 1)

After a WiFi scan of a local office was conducted, an unknown wireless signal was identified upon investigation. An unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

A. loT sensor

B. Evil twin

C. Rogue access point

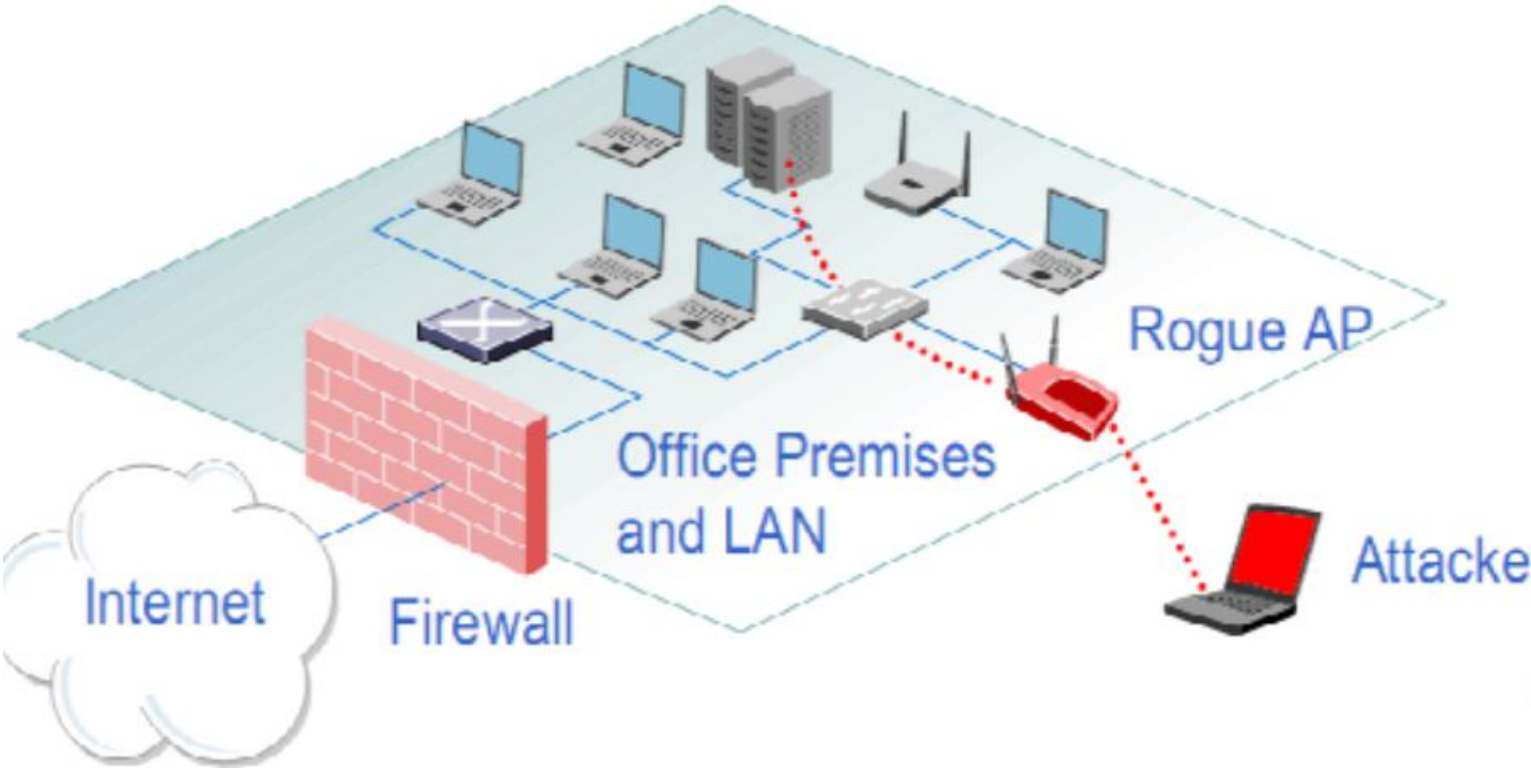
D. On-path attack

Answer: C

Explanation

A Raspberry Pi device connected to an Ethernet port could be configured as a rogue access point, allowing an attacker to intercept and analyze network traffic or perform other malicious activities. References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

Since it is mentioning a situation at a local office, it is a Rogue access point attached to the corporate network. A rogue access point is an unauthorized wireless access point that has been installed on a network without the consent or knowledge of the network's administrator. In this scenario, the Raspberry Pi device was found connected to an Ethernet port, which means it was not broadcasting a wireless signal. However, it could still be acting as a rogue access point by providing wireless access to the network via the Ethernet connection.



Question #:156 - (Exam Topic 1)

A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL

B. Implement a network-wide scan for other instances of the malware.

C. Quarantine the host from other parts of the network

D. Revoke the client's network access certificates

Answer: C

Explanation

When malware is discovered on a host, the best course of action is to quarantine the host from other parts of the network as the first and foremost step. This prevents the malware from spreading and potentially infecting other hosts. Adding a deny-all rule to the host in the network ACL may prevent legitimate traffic from being processed, implementing a network-wide scan is time-consuming and may not be necessary, and revoking the client's network access certificates is an extreme measure that may not be warranted. References: CompTIA Security+ Study Guide, pages 113-114

A and D: Adding a deny-all rule to the network ACL or revoking the client's network access certificates may be appropriate in certain circumstances but are not the best options in this scenario. These actions could be overly restrictive and may cause additional issues or disruptions to the network.

B: is also a good practice but may not be the best immediate action to take. Before conducting a network-wide scan, the analyst should first isolate the infected host to prevent further spread of the malware.

Question #:157 - (Exam Topic 1)

A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled in the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers

B. Use a captive portal for user authentication.

C. Authenticate users using OAuth for more resiliency

D. Implement SSO and allow communication to the internal network

E. Use the existing network and allow communication to the internal network and servers.

F. Use a new and updated RADIUS server to maintain the best solution

Correct Answer: B D

Explanation

Use a captive portal for user authentication: A captive portal is a web page that users are redirected to when they first connect to the network. They must authenticate themselves through this portal before gaining access to the internal network. This approach allows you to verify the identity of users and potentially apply policies or restrictions based on user credentials. It's a common method for guest or BYOD networks.

Implement SSO (Single Sign-On) and allow communication to the internal network: SSO enables users to log in once and gain access to multiple resources without needing to repeatedly enter their credentials. Implementing SSO for BYOD devices can improve user experience and security. However, ensure that proper security measures, like strong authentication and authorization controls, are in place to protect the internal network and data.

Creating a new network for mobile devices and blocking communication to the internal network and servers: While this approach can isolate mobile devices, it may not be practical in many scenarios, as it restricts the purpose of BYOD devices and limits their usefulness. It's better to control access through authentication and authorization mechanisms.

Authenticating users using OAuth for more resiliency: OAuth is typically used for granting access to third-party applications and services, not for device authentication on a corporate network. It's not a suitable option for BYOD device authentication in this context.

Using the existing network and allowing communication to the internal network and servers: Allowing BYOD devices unrestricted access to the internal network without proper authentication and authorization is a security risk. It's generally not recommended to open up the internal network to untrusted devices in this manner.

Using a new and updated RADIUS server to maintain the best solution: While updating RADIUS (Remote Authentication Dial-In User Service) servers is important for security, it's just one part of the solution. RADIUS alone won't address the need for user authentication and BYOD policy enforcement.

So, we created a network and used captive portal to authenticate.

Question #:158 - (Exam Topic 1)

Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?

A. Development

B. Staging

C. Production

D. Test

Answer: A

Explanation

Development Environment: The Development environment is where developers write and test their code changes. This environment is usually separate from other environments and may not be accessible to end-users. Developers typically use this environment to experiment with new features, write code, and test individual components of the application.

Test Environment: The Test environment is usually where automated and manual testing is done to verify that the code changes work as expected before moving them to the staging environment. This environment is where developers, testers, and quality assurance teams can test the functionality of the application before it is released to the end-users.

Staging Environment: The Staging environment is typically where the final version of the code is tested before deployment to the production environment. This environment is a replica of the production environment with the same hardware, software, and network settings. It allows developers to test new features, compare user-story responses and workflows, and verify that the application functions correctly. Staging environments typically use a modified version of actual data for testing to ensure that the application performs well with real-world data. This helps identify any issues before the code is deployed to the production environment.

Production Environment: The Production environment is where the live application is deployed for end-users to access. This environment is usually a more stable and secure environment than the previous environments.

Changes are made to this environment less frequently, and only after they have been thoroughly tested in the other environments.

Question #:159 - (Exam Topic 1)

An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer

B. Data owner

C. Backup administrator

D. Data custodian

E. Internal auditor

Answer: D

Explanation

Data custodian, role would be the best fit because it includes responsibilities for protecting data, including securing, monitoring, and controlling access to it, as well as ensuring data is accurate, complete, and accessible when needed. Ensuring that backups are

properly maintained would fall under the responsibilities of a data custodian, as they would be responsible for protecting data and ensuring its availability.

The responsibilities of ensuring backups are properly maintained and implementing technical controls to protect data are the responsibilities of the data custodian role. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 7: Securing Hosts and Data, Data Custodian

> A data custodian or data steward is the role responsible for the day-to-day caretaking of data. The data owner sets the relevant policies, and the steward or custodian ensures they are followed. It is responsible for the storage, protection, and maintenance of data. They are tasked with ensuring the data's security and integrity.
>
> The data owner has ultimate control and responsibility over the data. They decide who gets access and what happens with the data. In our scenario, it's more likely that the Data Custodian is in charge of the data protection, not the data owner.

Mamurjon Ismatov

—

Today at 12:03 PM

> The role of a data custodian typically involves the responsibility for implementing technical controls to protect data, including ensuring that backups are properly maintained.

Question #:160 - (Exam Topic 1)

A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?

A. IaaS

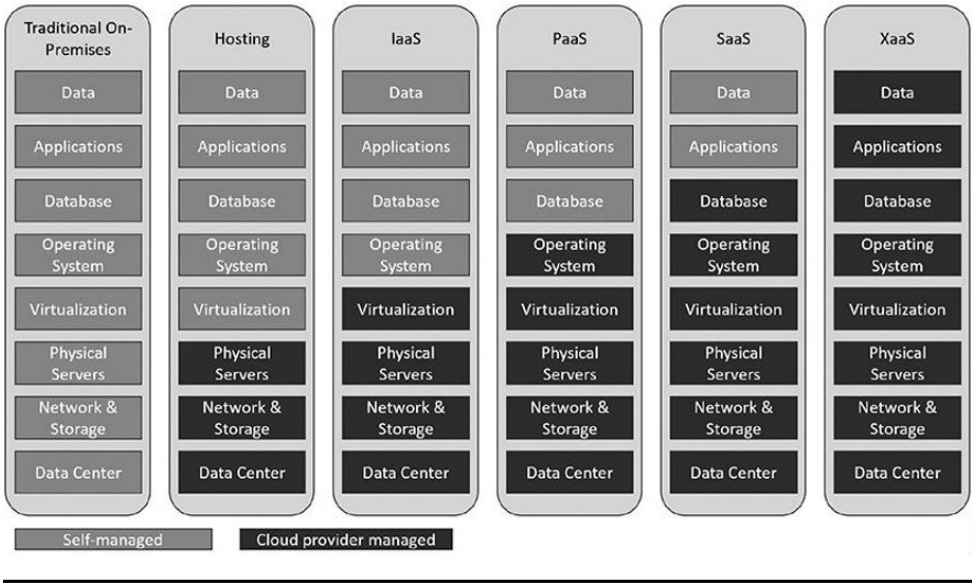
B. PaaS

C. XaaS

D. SaaS

Answer: C

Explanation



A la carte is a French term that loosely translates to “upon request.” So, a la carte self-service IT is a cloud computing model that allows users to customize their service and support needs related to their critical business services when they need it.

XaaS, or Anything as a Service, is a broad term that encompasses many different types of cloud services, including IaaS, PaaS, and SaaS, so it is not a specific type of provider.

10 Types of XaaS Businesses:
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)
AaaS (Analytics as a Service)
DaaS (Desktop as a Service)
FaaS (Functions as a Service)
STaaS (Storage as a Service)
CaaS (Containers as a Service)
DBaaS(Database as a Service)
AaaS (Authentication as a Service)

Question #:161 - (Exam Topic 1)

A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted. Which of the following is the researcher MOST likely using?

A. The Cyber Kill Chain

B. The incident response process

C. The Diamond Model of Intrusion Analysis

D. MITRE ATT&CK

Answer: D

Explanation

The researcher is most likely using the MITRE ATT&CK framework. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations. It helps security teams better understand and track adversaries by creating a named group, which aligns with the scenario described in the question. The framework is widely recognized and referenced in the cybersecurity industry, including in CompTIA Security+ study materials. References: 1. CompTIA Security+ Certification Exam Objectives (SY0-601):

https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf 2. MITRE ATT&CK: https://attack.mitre.org/

MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors. MITRE ATT&CK also allows security researchers to create named groups that track specific adversaries based on their TTPs.

The other options are not correct because:

A. The Cyber Kill Chain is a model that describes the stages of a cyberattack from reconnaissance to exfiltration. The Cyber Kill Chain does not provide a way to create named groups based on adversary TTPs.

B. The incident response process is a set of procedures and guidelines that defines how an organization should respond to a security incident. The incident response process does not provide a way to create named groups based on adversary TTPs.

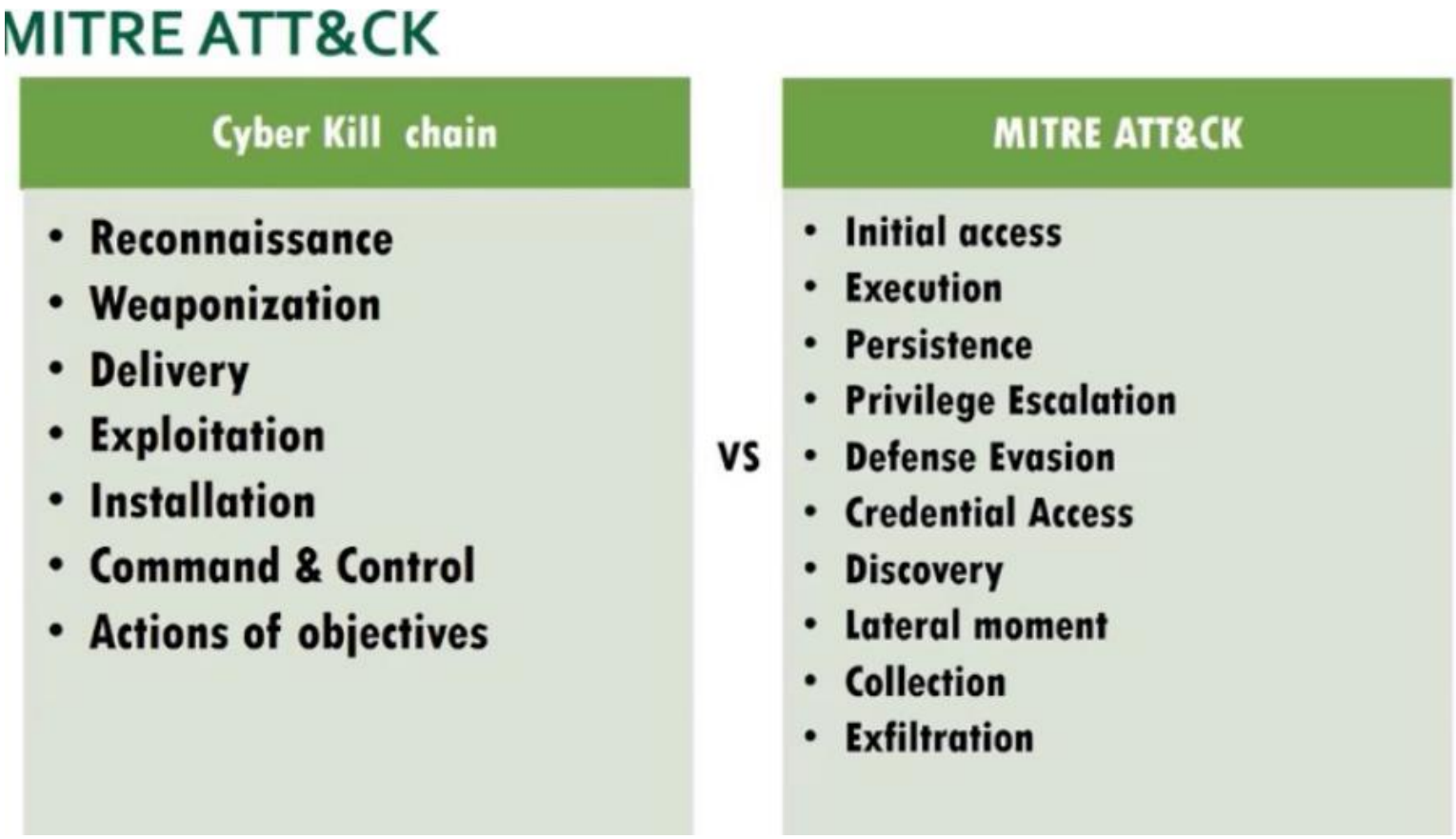
C. The Diamond Model of Intrusion Analysis is a framework that describes the four core features of any intrusion: adversary, capability, infrastructure, and victim. The Diamond Model of Intrusion Analysis does not provide a way to create named groups based on adversary TTPs.

According to CompTIA Security+ SY0-601 Exam Objectives 1.1 Compare and contrast different types of social engineering techniques:

“MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors.”

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

https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://attack.mitre.org/



Question #:162 - (Exam Topic 1)

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

A. Vulnerabilities with a CVSS score greater than 6.9.

B. Critical infrastructure vulnerabilities on non-IP protocols.

C. CVEs related to non-Microsoft systems such as printers and switches.

D. Missing patches for third-party software on Windows workstations and servers.

Answer: D

Explanation

Credentialed scans are more thorough and accurate than uncredentialed scans because they can access more information on the target system. For example, credentialed scans can identify missing patches for third-party software on Windows workstations and servers, while uncredentialed scans may not be able to detect these vulnerabilities.

Credentialed Scan:

- In a credentialed scan, the scanning tool or system has access credentials (username and password or other authentication mechanisms) to the target systems.
- This level of access allows the scanning tool to log in to the target systems with appropriate privileges, which can include administrative or root access.
- With such privileges, the scanning tool can gather detailed information about the target systems, including the

installed software, configurations, and patch levels.
- The scanning tool can then cross-reference this information with known vulnerabilities and patches, including those for third-party software.

Uncredentialed Scan:

- In an uncredentialed scan, the scanning tool does not have access credentials to log in to the target systems.
- Therefore, it relies on network-level scans and service enumeration to identify open ports, services, and potential vulnerabilities.
- While uncredentialed scans can identify some vulnerabilities related to the operating system and open ports, they often lack the depth of information needed to identify specific third-party software vulnerabilities and missing patches.

Now, considering the options provided:

Vulnerabilities with a CVSS score greater than 6.9: Both credentialed and uncredentialed scans can potentially identify vulnerabilities based on their Common Vulnerability Scoring System (CVSS) scores, although uncredentialed scans may miss some context.

Critical infrastructure vulnerabilities on non-IP protocols: This would likely depend on the specific scanning tool and the capabilities of both credentialed and uncredentialed scans. Some specialized scans may be required to detect vulnerabilities on non-IP protocols, and the credentialing status may not be the primary factor.

CVEs related to non-Microsoft systems such as printers and switches: These vulnerabilities are often associated with specific devices and software, and a credentialed scan with access to the device's configuration and software details is more likely to identify them accurately.

Missing patches for third-party software on Windows workstations and servers: This scenario involves specific software applications running on Windows systems. Credentialed scans, with access to detailed system information, are better equipped to identify missing patches for third-party software because they can examine the installed software inventory and compare it to known vulnerabilities and patches. Uncredentialed scans typically lack this level of detail and are more focused on open ports and services.

Question #:163 - (Exam Topic 1)

Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

A. A biometric scanner

B. A smart card reader

C. API Token

D. A PIN pad

Answer: A

Explanation

A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

Question #:164 - (Exam Topic 1)

Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

A. Tabletop

B. Parallel

C. Full interruption

D. Simulation

Answer: A

Explanation

A tabletop exercise is a type of disaster recovery test that simulates a disaster scenario in a discussion-based format, without actually disrupting operations or requiring physical testing of recovery procedures. It is the least time-consuming type of test for the disaster recovery team.

Question #:165 - (Exam Topic 1)

A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks Which of the following should the administrator consider?

A. Hashing

B. Salting

C. Lightweight cryptography

D. Steganography

Answer: B

Explanation

Salting is a technique that adds random data to a password before hashing it. This makes the hash output more unique and unpredictable, and prevents attackers from using precomputed tables (such as rainbow tables) to crack the password hash. Salting also reduces the risk of collisions, which occur when different passwords produce the same hash.

References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Note :salting = stop rainbow attack

Question #:166 - (Exam Topic 1)

After gaining access to a dual-homed (i.e. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access to another networked asset. This technique is an example

of:

A. privilege escalation

B. footprinting

C. persistence

D. pivoting

Answer: D

Explanation

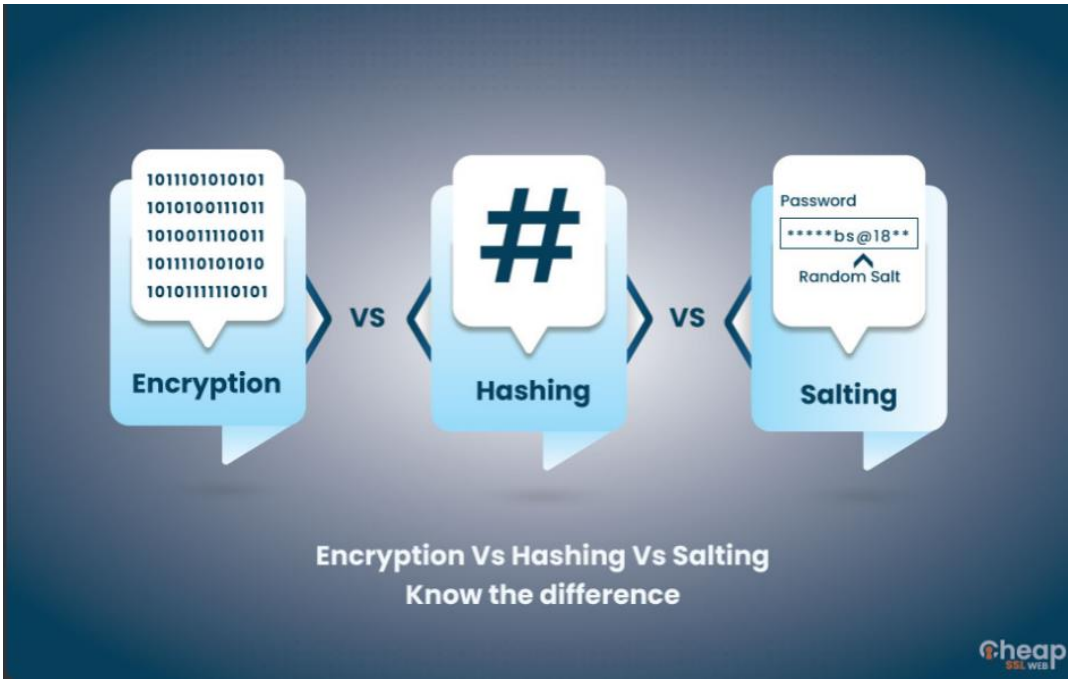
Pivoting refers to the technique used by a penetration tester or attacker to move from one compromised network or system to another, leveraging the initial access as a jumping-off point. This can be achieved through various methods, such as exploiting vulnerabilities, reusing credentials, or utilizing network trust relationships. The goal of pivoting is to expand the scope of the attack and gain access to more valuable systems and data within the network.

Pivoting -> The act of an attacker moving from one compromised system to one or more other systems on the network

Pivoting in cybersecurity refers to the practice of using a compromised system or network as a launching point to further exploit or attack other systems or networks within a target environment. It involves moving laterally through the network from one compromised host to another to gain deeper access and control. Pivoting allows attackers to escalate their attacks and maintain persistence within a targeted network, making it a significant concern in cybersecurity threat detection and response.

The technique of gaining access to a dual-homed multifunction device and then gaining shell access on another networked asset is an example of pivoting.

References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Enumeration and Penetration Testing



Question #:167 - (Exam Topic 1)

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering

B. Zero trust segmentation

C. Network access control

D. Access control vestibules

E. Guards

F. Bollards

Answer: C D

Explanation

Access control vestibules work:

Initial Entry: An individual enters the first door or access point, often through the use of access control measures like key cards, biometrics, or PIN codes.

In-Between Space: Once inside the vestibule, they are in an enclosed space with limited access to the outside and inside. This space is often referred to as an "airlock" or "mantrap."

Secondary Access: To proceed further into the facility, the individual must pass through a second door or access point, which is controlled in a similar manner to the first.

Access control vestibules help in several ways:

- They provide a controlled space where security personnel can verify the identity and intentions of individuals before allowing them deeper into the facility.
- They reduce the risk of unauthorized access, tailgating (one person following closely behind another), or piggybacking (one person using their access to let others in) since each person must be individually authenticated.
- They can also help with physical security by providing an additional layer of separation between the outside environment and the internal secure areas.

Network Access Control (NAC): Network Access Control is a technology that helps organizations enforce security policies and control access to the network. NAC solutions can authenticate and authorize devices before granting them access to the network. If an unauthorized device like a Kali Linux box is plugged in, NAC can detect it and prevent it from gaining network access.

So, combining Access Control Vestibules and Network Access Control (NAC) is a strong security approach. Access control vestibules address the physical entry and initial authentication, while NAC further controls and monitors the network access of devices connected within the facility.

Question #:168 - (Exam Topic 1)

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

A. Security patches were uninstalled due to user impact.

B. An adversary altered the vulnerability scan reports.

C. A zero-day vulnerability was used to exploit the web server.

D. The scan reported a false negative for the vulnerability.

Answer: A

Explanation

A patch was available for the vulnerability that was used to exploit the web server, but the patch was not applied, which allowed the attacker to exploit the server. This could have happened if the patch was uninstalled due to compatibility issues or user complaints. It is important to keep systems updated and patched to prevent vulnerabilities from being exploited.

A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers. Security patches are essential for maintaining the security and functionality of systems and applications.

If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.

The other options are not correct because:

B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.

C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.

D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans.

According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:

"A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers."

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/

Question #:169 - (Exam Topic 1)

A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPN, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate. Which of the following statements BEST explains the issue?

A. OpenID is mandatory to make the MFA requirements work

B. An incorrect browser has been detected by the SAML application

C. The access device has a trusted certificate installed that is overwriting the session token

D. The user's IP address is changing between logins, but the application is not invalidating the token

Answer: D

Explanation

This is because the policy of requiring re-authentication when changing locations is not being enforced by the application. This allows users to log in without going through MFA, even when they are in a different location.

The user's IP address is changing between logins, but the application is not invalidating the token.

Here's why this statement best explains the problem:

- ***SAML application with MFA:*** The SAML application is configured to use Multi-Factor Authentication (MFA), which is designed to enhance security by requiring additional authentication steps beyond just a username and password.
- ***High volume of successful logins without MFA:*** Despite being configured for MFA, the logs show a high volume of successful logins that did not require MFA. This is a security concern because MFA should be enforced for enhanced protection.
- ***Users traveling internationally:*** The fact that this issue is occurring for users who are traveling internationally suggests that it may be related to their location changes.
- ***Time-based tokens:*** The application allows time-based tokens to be generated, which implies that sessions have a limited duration for security purposes.
- ***Users changing locations should require reauthentication:*** The security policy is clear that when users change locations, they should be required to reauthenticate. This is a common security practice to prevent unauthorized access.
- ***Changing IP addresses:*** Users traveling internationally may have changing IP addresses as they move from one country to another or switch between mobile networks. If the application does not properly account for these IP address changes and invalidate the session or require reauthentication when an IP change is detected, it could explain why MFA is not being enforced for international users.

The other statements do not directly address the issue:

OpenID is mandatory to make the MFA requirements work: OpenID is typically used for identity and authentication purposes, but doesn't directly address the issue of MFA not being enforced.

An incorrect browser has been detected by the SAML application: Browser detection is more related to user agent strings and may affect the user experience, but is unlikely to explain the lack of MFA enforcement.

The access device has a trusted certificate installed that is overwriting the session token: While certificates can be used for authentication, this statement doesn't address the specific issue of MFA not being enforced for international users based on location changes.

In summary, the issue appears to be related to the application's failure to invalidate the session or require reauthentication when a user's IP address changes, especially when users are traveling internationally, as per the security policy.

"users who changed locations..." is the key point

Question #:170 - (Exam Topic 1)

A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour, the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows https://www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

A. DoS attack

B. ARP poisoning

C. DNS spoofing

D. NXDOMAIN attack

Answer: C

Explanation

The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address. DNS spoofing, also known as DNS cache poisoning or DNS poisoning, is a cyber attack in which a malicious actor manipulates the Domain Name System (DNS) to redirect users to fraudulent or malicious websites by altering DNS records. This can result in users unknowingly visiting fake websites that mimic legitimate ones, potentially leading to various types of cyberattacks such as phishing or data theft. DNS spoofing typically involves injecting false DNS information into a DNS cache or DNS server, causing it to resolve domain names to incorrect IP addresses.

Additional information: An NXDOMAIN (Non-Existent Domain) attack is a type of cyber attack that manipulates the Domain Name System (DNS) to return a response indicating that a domain name does not exist when, in fact, it does exist. This attack is also known as DNS NXDOMAIN manipulation or DNS forgery.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7

Note: Same DNS name, pointing to different IP. So is spoofing

Question #:171 - (Exam Topic 1)

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel.

Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. Bluesnarfing

E. DDoS

Answer: A

Explanation

The attack being conducted is an Evil twin attack. An Evil twin attack involves creating a rogue wireless access point (WAP) with the same Service Set Identifier (SSID) as a legitimate WAP to trick users into connecting to it. Once connected, the attacker can intercept traffic or steal login credentials. The successful login attempts with impossible travel times suggest that an attacker is using a stolen or compromised credential to access the external site to which the sensitive data is being downloaded. The non-standard DHCP configurations and overlapping channels of the WAPs suggest that the attacker is using a rogue WAP to intercept traffic.

References: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.4 Compare and contrast types of attacks, p. 8

Note: Impossible Travel is a calculation made by comparing a user's last known location to their current location, then assessing whether the trip is likely or even possible in the time that elapsed between the two measurements.

Question #:172 - (Exam Topic 1)

A security administrator has discovered that workstations on the LAN are becoming infected with malware.The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

A. Forward proxy

B. HIDS

C. Awareness training

D. A jump server

E. IPS

Answer: A

Explanation

A **forward proxy** is a server that sits between a client and a destination server and acts as an intermediary for requests from the client. The client sends a request to the forward proxy, which then makes the request on behalf of the client and returns the response back to the client.

Forward proxies are used to enhance privacy and security, control access to websites and web resources, and cache frequently requested content. They can also be used to enforce organizational policies, such as filtering access to certain websites or monitoring employee internet usage.

In terms of security, forward proxies can help to hide the client's IP address and provide an additional layer of **protection against cyber threats such as malware, phishing, and other types of attacks.**

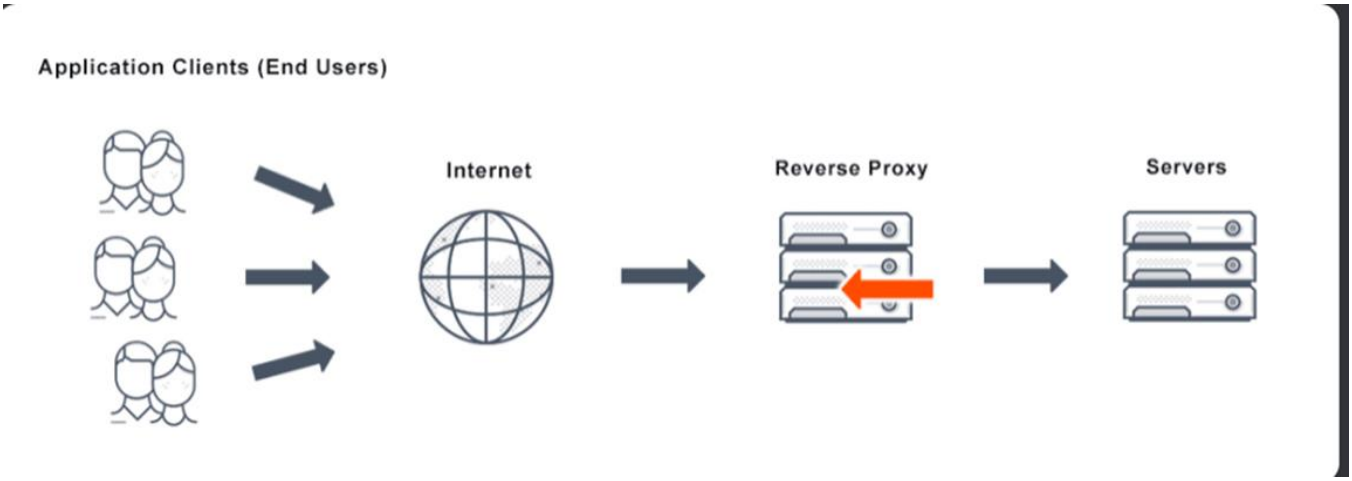
Awareness training should be implemented also to educate users on the risks of clicking on malicious URLs.

Phishing is a social engineering attack: Phishing emails exploit human behavior and psychology, making users the first line of defense. While technical solutions like email filtering and security devices are important, they may not

catch all phishing attempts. Raising user awareness about phishing attacks and how to recognize them is critical.

Users as the target: Phishing attacks often target users and rely on them to take action, such as clicking on malicious links. Training users to recognize phishing attempts can significantly reduce the success rate of such attacks.

Cost-effective: Awareness training is a cost-effective solution compared to implementing new technical controls like a forward proxy or an Intrusion Prevention System (IPS). It empowers users to become more vigilant and better equipped to protect themselves and the organization.



References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 9

Question #:173 - (Exam Topic 1)

The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history

B. Account expiration

C. Password complexity

D. Account lockout

Answer: D

Explanation

To prevent such a breach in the future, the BEST control to use would be Account lockout:

Account lockout policies are designed to prevent attackers from repeatedly attempting to gain unauthorized access to an account by locking the account after a certain number of failed login attempts. In the logs, you can see that the attacker made multiple login attempts with different passwords in quick succession. An account lockout policy would have locked the account after a certain number of failed attempts, making it much more difficult for the attacker to guess the correct password.

While the other controls mentioned are important for overall password security, they would not have prevented the specific attack described in the logs:

Password History: Password history policies typically prevent users from reusing recent passwords, but they wouldn't have prevented the attack, since the attacker was trying different passwords.

Account Expiration: Account expiration policies set a time limit for how long an account can be active, but they wouldn't have prevented the attack if the attacker was attempting to gain access within the valid timeframe.

Password Complexity: Password complexity policies require users to create strong passwords with a mix of characters, but they wouldn't have prevented the attack because the attacker was using various complex passwords as well.

In this scenario, the attacker's repeated login attempts could have been effectively mitigated with an account lockout policy that temporarily locks the account after a certain number of failed login attempts, making it more difficult for an attacker to guess the correct password.

Question #:174 - (Exam Topic 1)

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going to the polls. This is an example of:

A. prepending.

B. an influence campaign.

C. a watering-hole attack.

D. intimidation.

E. information elicitation.

Answer: B

Explanation

Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people's minds on a topic. One can engage in an influence campaign against a single person, but the effect is limited. Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation. Influencers are people who have large followings of people who read what they post, and in many cases act in accordance or agreement. This results in an amplifying mechanism, where single pieces of disinformation can be rapidly spread and build a following across the Internet.

A: Prepending: Prepending is not a term commonly used in the context of misinformation or election interference. In general computing terminology, it refers to adding a piece of data at the beginning of a file or message.

C: A watering-hole attack: A watering-hole attack is a type of cyber attack where the attacker targets a specific group of people by infecting websites that the group frequently visits with malware. This is not directly related to the scenario you presented.

D: Intimidation: Intimidation involves using threats or coercion to influence someone's behavior. While intimidation could potentially be used to discourage people from voting, the scenario you presented involves the spread of misinformation rather than direct threats.

E: Information elicitation: Information elicitation refers to the practice of extracting information from people through various means, such as social engineering or phishing. This does not directly relate to the scenario you presented.

Question #:175 - (Exam Topic 1)

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

A. HSM

B. CASB

C. TPM

D. DLP

Answer: A

Explanation

The network appliance that is specifically designed for securely storing cryptographic keys is HSM (Hardware Security Module).

Here's a brief explanation of each option:

HSM (Hardware Security Module): HSMs are dedicated hardware devices or appliances designed to manage and safeguard cryptographic keys, perform cryptographic operations, and protect sensitive data. They provide a secure and tamper-resistant environment for storing and managing keys used in various security applications, such as encryption, digital signatures, and secure communication.

CASB (Cloud Access Security Broker): CASBs are used for enforcing security policies and controls in cloud environments. While they offer valuable security features for cloud-based applications and data, they do not typically serve the primary purpose of securely storing cryptographic keys.

TPM (Trusted Platform Module): TPM is a hardware-based security feature that is often integrated into computer systems (e.g., laptops, desktops, servers). It provides a secure environment for storing keys and performing cryptographic operations at the device level. While TPMs are essential for device-level security, they may not be as versatile as HSMs for enterprise-wide key management.

DLP (Data Loss Prevention): DLP solutions focus on preventing the unauthorized sharing or leakage of sensitive data. While DLP systems play a crucial role in data protection, they are not specifically designed for cryptographic key management.

In the context of securely storing cryptographic keys, HSMs are the preferred choice due to their dedicated design for this purpose and their ability to meet stringent security and compliance requirements.

References: CompTIA Security+ Certification Exam Objectives, Exam Domain 2.0: Technologies and Tools, 2.4 Given a scenario, use appropriate tools and techniques to troubleshoot security issues, p. 21

David Berrios

—

Today at 12:32 PM

A. HSM (Hardware Security Module) A Hardware Security Module (HSM) is a network appliance that can securely store and manage cryptographic keys. HSMs are specialized hardware devices designed to provide a high level of security for key management and cryptographic operations. They are often used in enterprise environments to protect sensitive keys used for encryption, digital signatures, and other cryptographic function

Characteristics	TPM	HSM
Hardware	Chip in motherboard (included with many laptops)	Removable or external hardware device, (purchased separately)
Uses	Full disk encryption (for laptops and some servers)	High-end mission-critical servers (SSL accelerators, high availability clusters, certificate authorities)
Authentication	Performs platform authentication (verifies drive not moved)	Performs application authentication (only used by authorized applications)
Encryption Keys	RSA key burned into chip when created and can generate other keys	Stores RSA keys used in asymmetric encryption and can generate keys

Question #:176 - (Exam Topic 1)

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing

B. Salting

C. Integrity

D. Digital signature

Answer: A

Explanation

Hashing is a process that takes an input (in this case, the downloaded file) and generates a fixed-length string of

characters, which is known as a hash value or checksum. The hash value is unique to the content of the file. If the file is altered in any way, even a minor change, the resulting hash value will be significantly different from the original. By comparing the downloaded file's hash value with the verified checksum provided by the trusted source, a security analyst can confirm that the file has not been altered during transit or corrupted.

Common uses of hashing algorithms are to store computer passwords and to ensure message integrity. The idea is that hashing can produce a unique value that corresponds to the data entered. It is simple to check the validity or integrity of something by matching the given hash to one that is locally generated.

Question #:177 - (Exam Topic 1)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis

B. CIS Critical Security Controls

C. NIST Risk Management Framework

D. ISO 27002

Answer: C

Explanation

"ERP" stands for Enterprise Resource Planning.
The CISO is using the NIST Risk Management Framework (RMF) to evaluate the environment for the new ERP system. The RMF is a structured process for managing risks that involves categorizing the system, selecting controls, implementing controls, assessing controls, and authorizing the system.

The NIST RMF is a widely used framework for managing information security risk in organizations. It involves the following steps, which are similar to the approach described:

Categorization: Identifying and categorizing the system, including understanding its importance and impact on the organization's mission and assets.

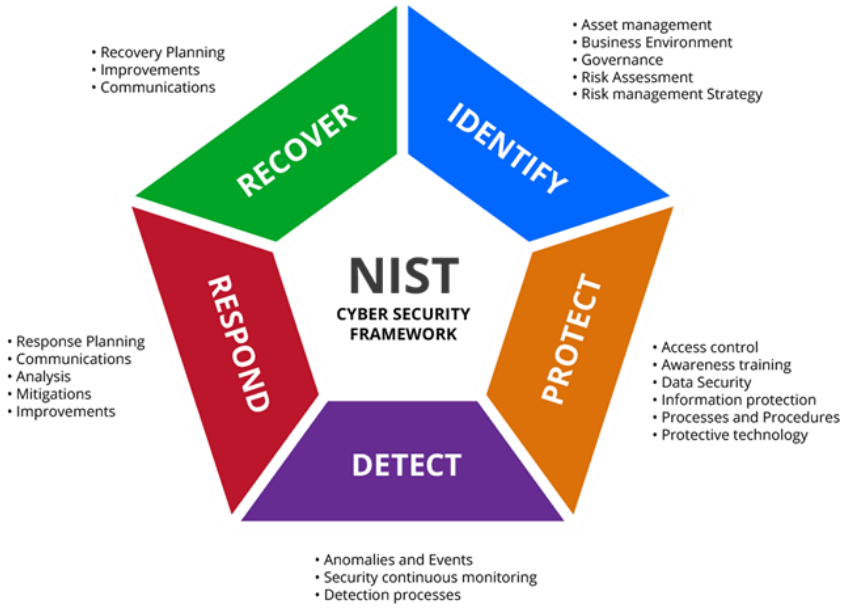
Selection of Controls: Selecting appropriate security controls based on the system's categorization and specific security requirements. The controls can be selected from various sources, including NIST Special Publication 800-53, which outlines a catalog of security controls.

Implementation: Implementing the selected security controls to protect the system and its associated data.

Assessment: Assessing the effectiveness of the implemented controls through testing, evaluation, and monitoring to ensure they are working as intended.

Authorization: Based on the assessment of controls and overall risk management, the system is authorized for operation if it meets the organization's security requirements and risk tolerance.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 4: Risk Management, pp. 188-191.



Question #:178 - (Exam Topic 1)

A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets available?

A. Adding a new UPS dedicated to the rack

B. Installing a managed PDU

C. Using only a dual power supplies unit

D. Increasing power generator capacity

Answer: B

Explanation

A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.

A managed PDU provides control and monitoring capabilities over individual power outlets. Here's how it helps:

Control: A managed PDU allows you to remotely turn on or off individual power outlets. This means you can deactivate unused outlets and prevent unauthorized devices from being plugged in. It offers control without reducing the number of physical outlets available.

Monitoring: Managed PDUs typically provide power usage monitoring and reporting. This can help identify power consumption patterns and detect any unauthorized or abnormal power usage, which may indicate the presence of unauthorized devices.

The other options mentioned are less suitable for addressing this specific issue:

Adding a new UPS dedicated to the rack: While this might provide additional power backup, it doesn't directly

address the problem of unauthorized devices being connected to power outlets.

Using only a dual power supplies unit: This might ensure redundancy for devices with dual power supplies, but it doesn't prevent unauthorized devices from being connected to power outlets.

Increasing power generator capacity: Increasing generator capacity may address power overload issues but doesn't directly address the issue of unauthorized use of power outlets.

Installing a managed Power Distribution Unit (PDU) is the most appropriate option to mitigate the issue of unauthorized use of empty power outlets in the network rack without compromising the number of outlets available. A managed PDU provides control and monitoring capabilities over individual power outlets, allowing administrators to remotely turn outlets on or off as needed. This means that unused outlets can be powered off to prevent unauthorized devices from being connected while maintaining the overall number of outlets available for authorized devices.

Question #:179 - (Exam Topic 1)

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

A. Privacy

B. Cloud storage of telemetry data

C. GPS spoofing

D. Weather events

Answer: C

Explanation

The vulnerability of GPS to spoofing has serious implications for UAVs, as victim drones using civil GPS can be misdirected or even completely hijacked for malicious intents, as already demonstrated in several academic research efforts using commercially available GPS spoofing hardware.

A: The company needs to ensure that it has appropriate policies, procedures, and safeguards in place to protect the privacy of individuals and organizations within the drone's operational range.

B: Cloud storage of telemetry data is a common practice for storing and analyzing drone data, but the company should ensure that the data is stored securely and is accessible only to authorized personnel.

D: Weather events can impact the drone's flight performance, but it is not a significant concern if the drone is designed to withstand adverse weather conditions and if the company has a contingency plan in place to handle such situations.

Perimeter and boundary = geo location

The choice between privacy and GPS spoofing as the MOST concerning issue depends on the specific context and priorities of the company using the drone for monitoring. Both are valid concerns, but the level of concern may vary based on the company's objectives and compliance requirements.

Privacy Concerns: If the company's monitoring activities involve capturing sensitive or private data about individuals or properties, then privacy concerns would indeed be the MOST concerning issue. Ensuring compliance with privacy

laws and regulations, obtaining necessary permissions, and safeguarding the collected data are critical in such cases.

GPS Spoofing: GPS spoofing can be a significant concern, especially if the monitoring system relies heavily on GPS for accurate location data. Spoofing attacks can disrupt the drone's operations, potentially leading to security breaches or inaccurate monitoring results. Mitigating GPS spoofing may require additional security measures.

GPS spoofing is a cyberattack technique that involves generating fake Global Positioning System (GPS) signals to deceive GPS receivers or navigation systems. The goal of GPS spoofing is to manipulate the location information received by GPS devices, leading them to provide incorrect or misleading location data to users.

Question #:180 - (Exam Topic 1)

A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m – 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT

B. Ransomware

C. Polymophic

D. A worm

Answer: C

Explanation

A polymorphic virus, sometimes referred to as a metamorphic virus, is **a type of malware that is programmed to repeatedly mutate its appearance or signature files through new decryption routines**.
Polymorphism is used to evade pattern-matching detection relied on by security solutions like antivirus software.

How does polymorphic virus avoid detection?

Polymorphic viruses are complex file infectors that can **create modified versions of itself** to avoid detection yet retain the same basic routines after every infection. To vary their physical file makeup during each infection, polymorphic viruses encrypt their codes and use different encryption keys every time.

Not worm, because there is no indication that the malware is spreading out
Not ransomware, because there is no indication for it

Topic 2, Exam Set 2

Question #:1 - (Exam Topic 2)

A systems engineer thinks a business system has been compromised and is being used to exfiltrated data to a competitor. The engineer contacts the CSIRT. The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else. Which of the following is the most likely reason for this request?

A. The CSIRT thinks an insider threat is attacking the network.

B. Outages of business-critical systems cost too much money.

C. The CSIRT does not consider the systems engineer to be trustworthy.

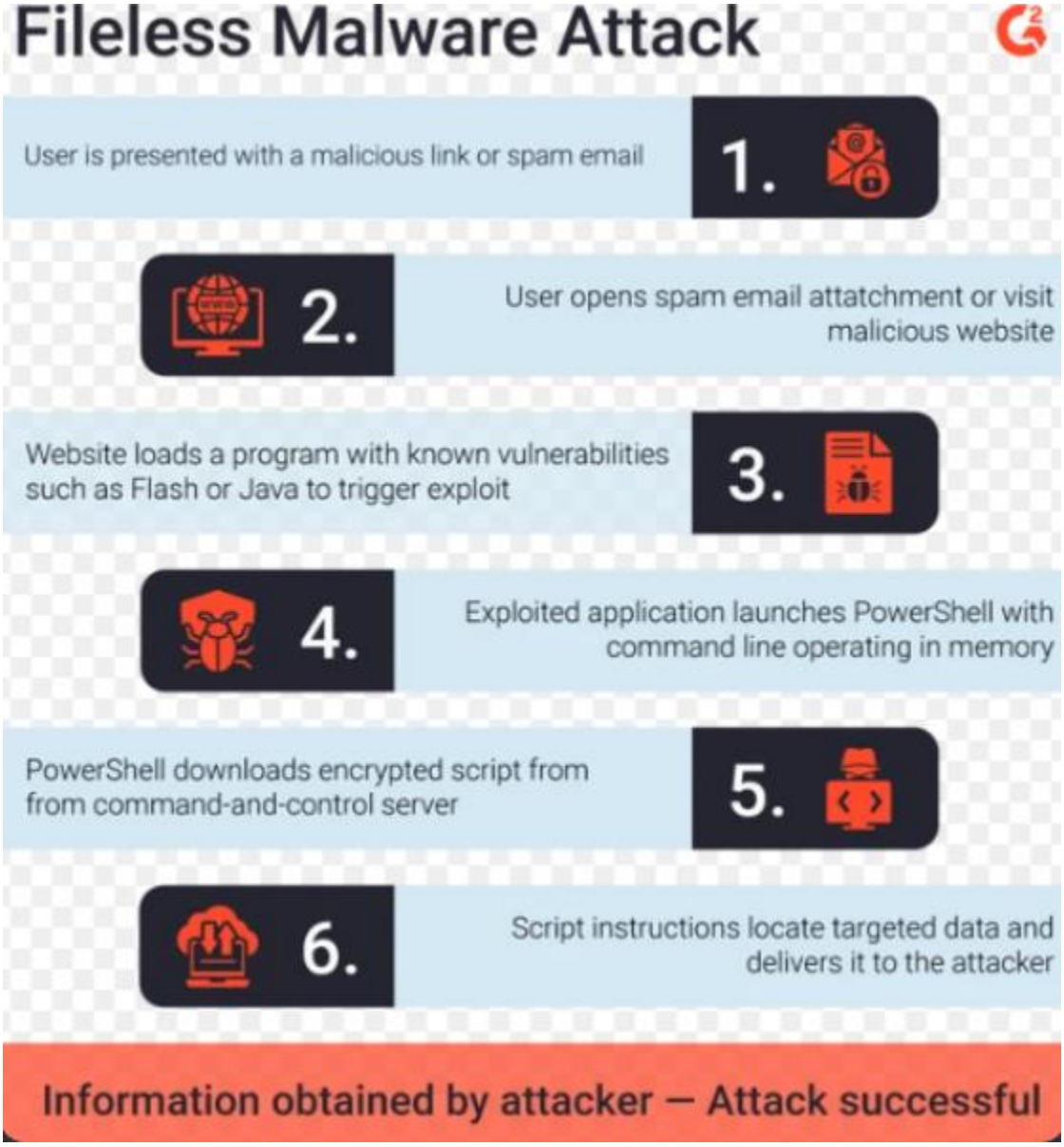
D. Memory contents including fileless malware are lost when the power is turned off.

Answer: D

Explanation

Memory contents including files and malware are lost when the power is turned off. This is a standard precautionary measure when dealing with suspected cybersecurity incidents. By disconnecting the network cable and powering off the compromised system, the organization aims to preserve the state of the system for forensic analysis while preventing further data exfiltration or potential harm. In cases of sophisticated attacks, fileless malware, volatile memory, or active network connections may be present, and shutting down the system can help prevent further damage or data loss. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.

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/memory-acquisition-and-analysis/



You are correct that the contents of a computer's volatile memory (RAM) are typically lost when the power is turned off. RAM is a type of volatile memory, meaning that it stores data temporarily and requires a constant supply of electrical power to maintain that data

Question #:2 - (Exam Topic 2)

A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?

A. Compensating controls

B. Directive control

C. Mitigating controls

D. Physical security controls

Answer: C

Explanation

Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.

In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure. Removable media threats can be used to bypass network defenses and target industrial/OT environments. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.

Some examples of mitigating controls for removable media threats are:

- Encrypting data on removable media
- Scanning removable media for malware before use
- Restricting access to removable media ports
- Implementing policies and procedures for removable media usage and disposal
- Educating users on the risks and best practices of removable media

Directive Controls are the mandatory controls that are implemented to monitor the regulations. It provides guidance primarily aligned with the organizations required to follow, like policies, regulations, etc.

Question #:3 - (Exam Topic 2)

A company has a "right to forgotten" request. To legally comply, the company must remove data related to the requester from its systems. Which of the following company most likely complying with?

A. NIST CSF

B. GDPR

C. PCI OSS

D. ISO 27001

Answer: B

Explanation

GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas.

GDPR grants individuals the right to request the deletion or removal of their personal data from an organization's systems under certain circumstances. This right is also known as the "right to be forgotten" or the "right to erasure". An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.

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

https://gdpr-info.eu/issues/right-to-be-forgotten/

Question #:4 - (Exam Topic 2)

Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

A. Edge computing

B. Microservices

C. Containers

D. Thin client

Answer: C

Explanation

Containers are a method of virtualization that allow you to run multiple isolated applications on a single server. Containers are lightweight, portable, and scalable, which means they can save resources, improve performance, and simplify deployment. Containers also enable centralized monitoring and management of the applications running on them, using tools such as Docker or Kubernetes. Containers are different from edge computing, which is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed. Microservices are a software architecture style that breaks down complex applications into smaller, independent services that communicate with each other. Thin clients are devices that rely on a server to perform most of the processing tasks and only provide a user interface.

Edge computing: Edge computing is a distributed computing paradigm where processing is done closer to the data source, typically at the edge of the network. While it can be useful for certain use cases, it doesn't necessarily align with the goal of centrally storing and monitoring data on a server.

Microservices: Microservices is an architectural approach for building applications as a collection of loosely coupled services. While it can provide scalability and flexibility, it doesn't inherently address the goal of central data storage or monitoring.

Thin client: Thin client refers to a lightweight computing device that relies on a central server for processing and storage. While it can centralize data and applications, it doesn't provide the same level of scalability and flexibility as containers.

Question #:5 - (Exam Topic 2)

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.

Perform the following steps:

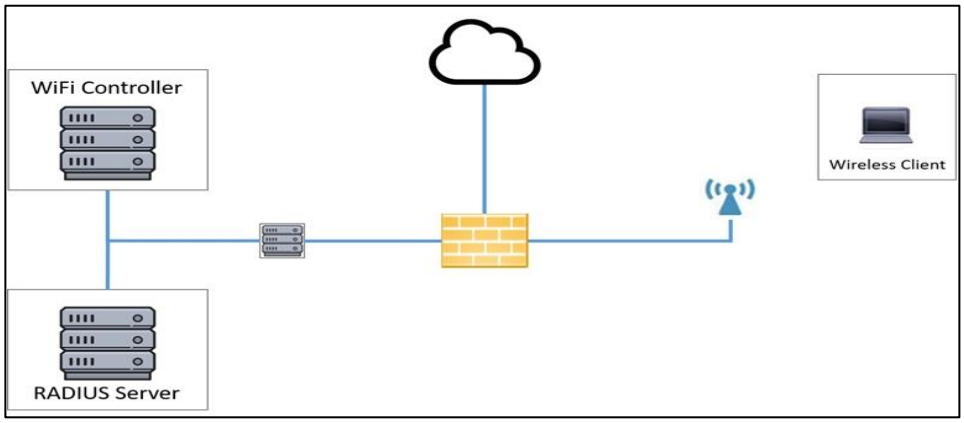
1. Configure the RADIUS server.

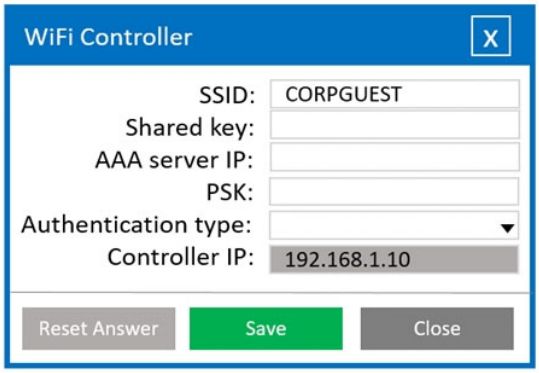
2. Configure the WiFi controller.

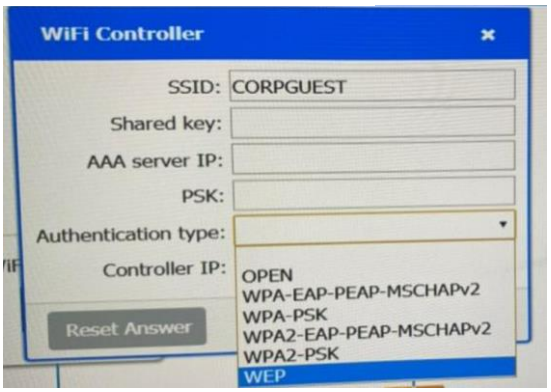
3. Preconfigure the client for an incoming guest. The guest AD credentials are:

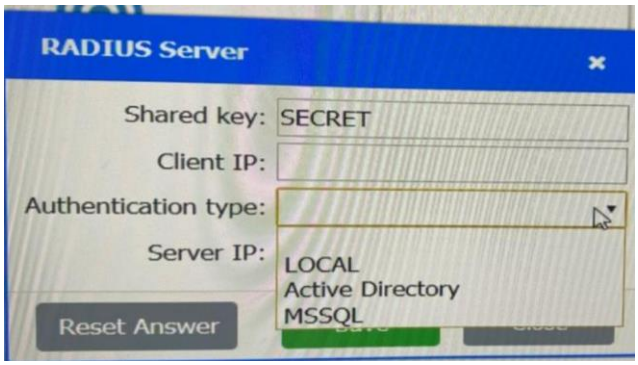
User: guest01

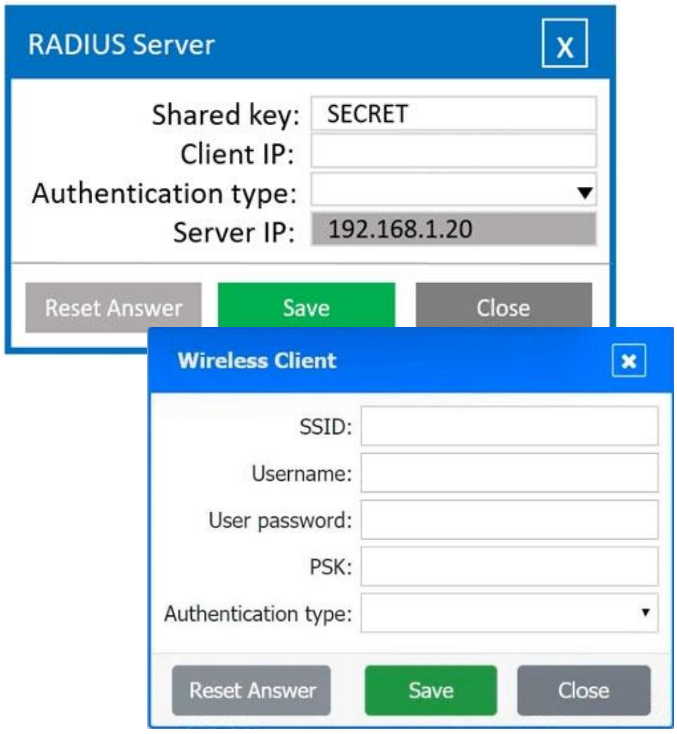
Password: guestpass

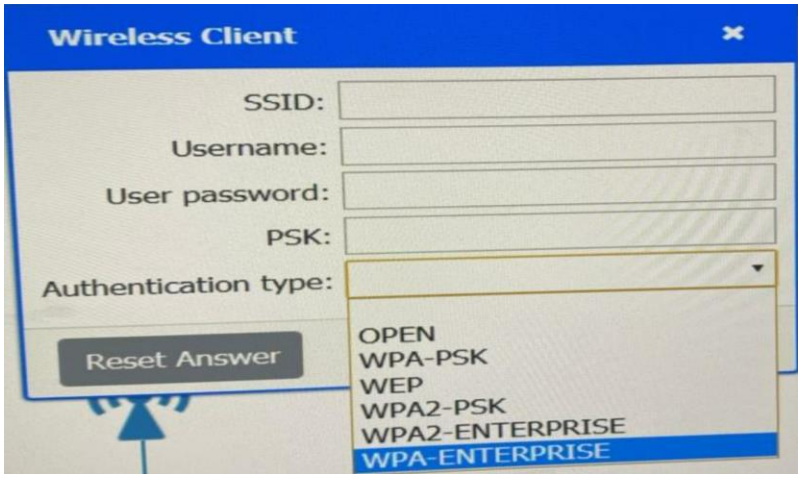

WiFi Controller
Wireless Client
RADIUS Server


WiFi Controller
X
SSID:
CORPGUEST
Shared key:
AAA server IP:
PSK:
Authentication type:
Controller IP:
192.168.1.10
Reset Answer
Save
Close


WiFi Controller
SSID:
CORPGUEST
Shared key:
AAA server IP:
PSK:
Authentication type:
Controller IP:
Reset Answer
OPEN
WPA-EAP-PEAP-MSCHAPv2
WPA-PSK
WPA2-EAP-PEAP-MSCHAPv2
WPA2-PSK
WEP


RADIUS Server
Shared key:
SECRET
Client IP:
Authentication type:
Server IP:
LOCAL
Active Directory
MSSQL
Reset Answer





See the explanation below for the solution.

Explanation

Explanation:

Wifi Controller
SSID: CORPGUEST
SHARED KEY: Secret
AAA server IP: 192.168.1.20
PSK: Blank
Authentication type: WPA2-EAP-PEAP-MSCHAPv2
Controller IP: 192.168.1.10

Radius Server
Shared Key: Secret
Client IP: 192.168.1.10
Authentication Type: Active Directory

Server IP: 192.168.1.20

Wireless Client
SSID: CORPGUEST
Username: guest01
Userpassword: guestpass
PSK: Blank
Authentication type: WPA2-Enterprise

Question #:6 - (Exam Topic 2)

A security engineer is concerned the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer wants a tool that can monitor for changes to key files and network traffic for the device. Which of the following tools should the engineer select?

A. HIDS

B. AV

C. NGF-W

D. DLP

Answer: A

Explanation

The security engineer should select a Host Intrusion Detection System (HIDS) to address the concern. HIDS monitors and analyzes the internals of a computing system, such as key files and network traffic, for any suspicious activity. Unlike antivirus software (AV), which relies on known signatures of malware, HIDS can detect anomalies, policy violations, and previously undefined attacks by monitoring system behavior and the network traffic of the device.

AV (Antivirus): Antivirus software is primarily designed to detect and remove malware (viruses, trojans, etc.) but may not provide the detailed file and network monitoring capabilities required in this scenario.

NGF-W (Next-Generation Firewall): Next-generation firewalls focus on network traffic filtering and threat prevention at the network level but may not provide the detailed endpoint file monitoring capabilities required here.

DLP (Data Loss Prevention): DLP solutions are designed to prevent unauthorized data transfer or leakage. While they can monitor network traffic for sensitive data, their primary focus is data protection, and they may not offer the same level of host-based file monitoring as HIDS.

References:

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

2. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

3. he tool the security engineer should select to monitor for changes to key files and network traffic on endpoints is: HIDS (Host-based Intrusion Detection System). HIDS (Host-based Intrusion Detection System) monitors and analyzes the internals of a computing system, including files, configurations, and network traffic on a specific host. It is designed to detect suspicious activities and changes on individual devices or hosts. In this scenario, HIDS would be the appropriate choice to monitor key files and network traffic for the device, providing a more holistic approach to endpoint security beyond predefined

attack patterns.

Another similar question

A security engineer is concerned that the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key files and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?

A. NIDS
B. HIPS
C. AV
D. NGFW

Answer: B

HIPS monitors changes to key files and network traffic on a single device, and can detect and prevent malicious activities by comparing the current state of the system to a known good state.

system (NIDS) only monitors network traffic for signs of malicious activity and does not provide prevention capabilities.

An antivirus (AV) program only detects and removes malware from a device, and does not monitor changes to key files or network traffic.

A next-generation firewall (NGFW) monitors and controls network traffic, but does not provide the detailed monitoring and prevention capabilities of a HIPS.

Question #:7 - (Exam Topic 2)

A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: “SELECT * FROM customername”. Which of the following is most likely being attempted?

A. Directory traversal

B. SQL injection

C. Privilege escalation

D. Cross-site scripting

Answer: B

Explanation

SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the database behind the application. SQL injection can be used to perform various

actions, such as reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement “SELECT * FROM customername” to retrieve all data from the customername table in the database.

Question #:8 - (Exam Topic 2)

A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).

A. DLP

B. MAC filtering

C. NAT

D. VPN

E. Content filter

F. WAF

Answer: C E

Explanation

NAT (Network Address Translation): NAT should be used to allow all 50 users to share the same single Internet connection. NAT translates internal private IP addresses to a single public IP address, enabling multiple devices to access the Internet using the same external IP address. This allows for efficient use of the Internet connection.

Content Filter (or Web Content Filtering): To block access to social media sites and external email services, a content filtering solution should be implemented. This can be achieved through a content filtering proxy server, a dedicated web content filtering appliance, or cloud-based content filtering services. Content filtering allows you to define and enforce policies that restrict access to specific categories of websites, including social media and external email services.

The other options mentioned have different purposes and are not directly related to achieving the specified requirements:

DLP (Data Loss Prevention): DLP is used to prevent the unauthorized transmission of sensitive data from within the organization. While it's important for data security, it doesn't directly address the stated requirements.

MAC Filtering: MAC filtering involves allowing or denying network access based on the Media Access Control (MAC) addresses of devices. It is not typically used for blocking access to specific websites or services.

VPN (Virtual Private Network): VPNs are used for secure communication over the Internet. While they have their own security benefits, they are not used to block social media or email services.

WAF (Web Application Firewall): WAFs are designed to protect web applications from various forms of cyberattacks. They are not used to restrict access to specific websites or services.

Question #:9 - (Exam Topic 2)

A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

A. RAID

B. UPS

C. NIC teaming

D. Load balancing

Answer: C

Explanation

NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches.

To configure NIC Teaming in Windows Server, see Microsoft's documentation: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming.
For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

Mamurjon Ismatov
—
Today at 1:40 PM
network interface card teaming or bonding, involves combining multiple network interfaces on a server to operate as a single logical interface.

Danut Halau
—
Today at 1:40 PM
NIC teaming, also known as network interface card (NIC) bonding, is a networking technology that combines multiple physical network interfaces (NICs) into a single logical network interface

Question #:10 - (Exam Topic 2)

A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, "Your connection is not private." Which of the following is the best way to fix this issue?

A. Ignore the warning and continue to use the application normally.

B. Install the certificate on each endpoint that needs to use the application.

C. Send the new certificate to the users to install on their browsers.

D. Send a CSR to a known CA and install the signed certificate on the application's server.

Answer: D

Explanation
Send a CSR (Certificate Signing Request) to a known public CA (Certificate Authority) and install the signed certificate on the application's server.

Here's why:

Public Application: Since the application is public and accessible to users outside your organization, it's essential to

use a certificate that is trusted by commonly used web browsers. Public CAs are widely recognized and trusted, ensuring that users won't receive security warnings when accessing the site.

Internal CA: Certificates issued by internal CAs are typically trusted only within the organization and are not automatically trusted by external users' browsers. This is why users are seeing the "Your connection is not private" warning message.

CSR to a Public CA: By sending a CSR to a known public CA and obtaining a certificate from them, you ensure that the certificate is signed by a trusted third-party authority. Users will not receive security warnings when accessing the application, as the certificate will be recognized by their browsers.

Installing the internal CA certificate on each endpoint is not a practical solution for a public application, as it requires manual configuration on each user's device, which is neither efficient nor user-friendly. Sending the new certificate to users to install on their browsers is also not a scalable or practical solution for a public application.

To ensure a smooth and secure user experience, obtaining a certificate from a trusted public CA is the recommended approach for public-facing applications.

Question #:11 - (Exam Topic 2)

An organization wants to quickly assess how effectively the IT team hardened new laptops. Which of the following would be the best solution to perform this assessment?

A. Install a SIEM tool and properly configure it to read the OS configuration files."

B. Load current baselines into the existing vulnerability scanner.

C. Maintain a risk register with each security control marked as compliant or non-compliant.

D. Manually review the secure configuration guide checklists.

Answer: B

Explanation

A vulnerability scanner is a tool that can scan devices and systems for known vulnerabilities, misconfigurations, and compliance issues. By loading the current baselines into the scanner, the organization can compare the actual state of the new laptops with the desired state and identify any deviations or weaknesses quickly. This is a quick and automated way to assess the hardening of the new laptops.

Question #:12 - (Exam Topic 2)

A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company implementing?

A. CYOD

B. MDM

C. COPE

D. VDI

Answer: D

Explanation

The deployment model the company is implementing is VDI (Virtual Desktop Infrastructure).

Remote Work Model: In a remote work model where employees access resources in the cloud from their personal computers, VDI allows for the creation of virtual desktops that are hosted in the cloud. Users can remotely connect to these virtual desktops from their personal devices.

Company-Managed Operating System: With VDI, the company manages and controls the operating system and applications within the virtual desktop environment. This ensures that the corporate environment remains secure and compliant, even when accessed from employees' personal devices.

The other deployment models mentioned are as follows:

CYOD (Choose Your Own Device): CYOD allows employees to choose from a list of approved devices provided by the company, but in the scenario described, employees are using their personal computers, so CYOD doesn't apply.

MDM (Mobile Device Management): MDM typically applies to managing mobile devices (smartphones and tablets). While it's important for device security, it doesn't address the scenario where employees are using their personal computers.

COPE (Corporate-Owned, Personally Enabled): COPE refers to a scenario where the company provides employees with a corporate-owned device that they can also use for personal purposes. This model doesn't apply when employees are using their own personal computers.

In the described scenario, VDI allows the company to maintain control over the virtual desktop environment while enabling employees to access corporate resources from their personal computers.

Petra Martina Vrancic

—

Today at 1:46 PM

VDI allows users to access a virtualized desktop environment hosted on a remote server. In this case, the company is managing the operating system in the cloud, and employees use their personal computers as thin clients to connect to their virtual desktops.

Question #:13 - (Exam Topic 2)

An upcoming project focuses on secure communications and trust between external parties. Which of the following security components will need to be considered to ensure a chosen trust provider is used, and the selected option is highly scalable?

A. Self-signed Certificate

B. Certificate Attributes

C. Public Key Infrastructure

D. Domain Validation

Answer: C

Explanation

To ensure secure communications and trust between external parties in a highly scalable manner, the security component that needs to be considered is Public Key Infrastructure (PKI).

Trust Provider: PKI provides a framework for managing digital certificates, including the issuance, distribution, and revocation of certificates. When implementing secure communications with external parties, using a trusted PKI ensures that the certificates issued are recognized and trusted by all parties involved. This helps establish trust in the communication channel.

Scalability: PKI is designed to scale efficiently, making it suitable for securing communications with external parties on a large scale. It can accommodate a growing number of certificates and users as the project expands.

The other options mentioned have specific purposes, but may not address the requirements for trust and scalability in the context of secure communications with external parties:

Self-signed certificate: Self-signed certificates are not typically used for establishing trust in external communications because they are not issued by a trusted third party. They also do not inherently provide scalability.

Certificate attributes: Certificate attributes are used to convey additional information about the certificate holder but do not address the broader requirements of trust and scalability in the same way that PKI does.

Domain validation: Domain validation is a process used to verify the ownership of a domain, but it is only one aspect of PKI. PKI encompasses a broader set of mechanisms and standards for managing digital certificates and establishing trust in communications.

In summary, PKI is the comprehensive solution for managing digital certificates and ensuring trust in secure communications with external parties, while providing scalability as the project grows.

Danut Halau
—
Today at 1:46 PM
yes

[
1:46 PM
]

Public Key Infrastructure (PKI) is a comprehensive framework of policies, processes, technologies, and standards used to manage digital keys (public and private keys) and digital certificates

David Berrios
—
Today at 1:46 PM
PKI with out eventhink about it

Question #:14 - (Exam Topic 2)

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system // PAM
D. An OpenID Connect authentication system

Answer: C

Explanation

Check-in/Checkout of Credentials: PAM systems typically include features for securely checking out and checking in credentials. This ensures that privileged credentials are only accessible to authorized individuals for a limited time.

Ability to Use but Not Know the Password: PAM systems often provide a feature called "credential injection" or "session recording" that allows users to use privileged accounts without actually knowing the underlying passwords. The PAM system handles the password injection securely.

Automated Password Changes: PAM systems can automate password changes for privileged accounts at regular intervals or in response to specific events. This helps ensure that passwords are regularly rotated for security purposes.

Logging of Access to Credentials: PAM solutions typically provide extensive auditing and logging capabilities, recording all access to privileged accounts, including who accessed them, when, and what actions were performed.

OAuth 2.0 and OpenID Connect are authentication and authorization protocols often used for single sign-on (SSO) and user authentication but are not designed for the specific requirements mentioned.

Secure Enclave is a hardware-based security feature used in some mobile devices, but it does not provide the comprehensive set of features needed for managing privileged credentials and service accounts in an enterprise context.

Therefore, a privileged access management (PAM) system is the most suitable solution for meeting the specified requirements.

A: OAuth 2.0 (A) is an open standard for authorization and is typically used for granting access to web and mobile applications. It is not specifically designed to meet the requirements for managing administrator/root credentials and service accounts.

B: A secure enclave (Apple) provides CPU hardware-level isolation and memory encryption on every server, by isolating application code and data from anyone with privileges, and encrypting its memory. With additional software, secure enclaves enable the encryption of both storage and network data for simple full stack security.

D: OpenID Connect (D) is an authentication protocol that provides identity federation and single sign-on (SSO) capabilities. While it can be used to authenticate users, it does not provide the specific capabilities required to manage administrator/root credentials and service accounts.

Examples of privileged access used by humans:

- **Super user account:** A powerful account used by IT system administrators that can be used to make configurations to a system or application, add or remove users or delete data.
- **Domain administrative account:** An account providing privileged administrative access across all workstations and servers within a network domain. These accounts are typically few in number, but they provide the most extensive and robust access across the network. The phrase "Keys to the IT Kingdom" is often used when referring to the privileged nature of some administrator accounts and systems.
- **Local administrative account:** This account is located on an endpoint or workstation and uses a combination of a username and password. It helps people access and make changes to their local machines or devices.
- **Secure socket shell (SSH) key:** SSH keys are heavily used access control protocols that provide direct root access to critical systems. Root is the username or account that, by default, has access to all commands and files on a Linux or other Unix-like operating system.
- **Emergency account:** This account provides users with administrative access to secure systems in the case of an emergency. It is sometimes referred to as firecall or break glass account.
- **Privileged business user:** Is someone who works outside of IT, but has access to sensitive systems. This could include someone who needs access to finance, human resources (HR) or marketing systems.

Examples of non-human privileged access:

- **Application account:** A privileged account that's specific to the application software and is typically used to administer, configure or manage access to the application software.
- **Service account:** An account that an application or service uses to interact with the operating system. Services use these accounts to access and make changes to the operating system or the configuration
- **SSH key:** (As outlined above). SSH keys are also used by automated processes.
- **Secret:** Used by development and operations (DevOps) team often as a catch-all term that refers to SSH keys, application program interface (API) keys and other credentials used by DevOps teams to provide privileged access.

Question #:15 - (Exam Topic 2)

A security analyst is reviewing packet capture data from a compromised host in the packet capture. The analyst locates packets that contain a large amount of text. Which of the following is most likely installed on the compromised host?

A. Keylogger

B. Spyware

C. Trojan

D. Ransomware

Answer: A

Explanation

A keylogger is a type of malicious software or hardware that records the keystrokes made by a user on a compromised system. This includes capturing the text that the user types, such as login credentials, messages, and other typed information. Keyloggers often send this captured data to a remote server or store it locally for later retrieval.

Question #:16 - (Exam Topic 2)

A security administrator is seeking a solution to prevent unauthorized access to the internal network. Which of the following security solutions should the administrator choose?

A. MAC filtering

B. Anti-malware

C. Translation gateway

D. VPN

Answer: D

Explanation

VPN (Virtual Private Network): A VPN allows secure remote access to the internal network over the internet. It establishes an encrypted tunnel between remote devices (such as remote employees' computers or remote offices) and the internal network. Only authorized users with the proper credentials can access the network through the VPN. This provides a high level of security and ensures that unauthorized users cannot gain access to internal resources.

The other options mentioned are not primarily focused on preventing unauthorized access to the internal network:

MAC Filtering (Media Access Control Filtering): MAC filtering allows or denies network access based on the MAC addresses of devices. While it can be a supplementary security measure, it's not sufficient on its own to prevent unauthorized access.

Anti-Malware: Anti-malware solutions are primarily designed to detect and prevent malware infections on devices. While they are important for overall network security, they don't directly address unauthorized access to the network.

Translation Gateway: This term is not typically used in the context of preventing unauthorized access to the internal network. It's not a common security solution for this purpose.

Petra Martina Vrancic

—

Today at 1:52 PM

encrypts the communication between devices and ensures secure access to the internal network, making it harder for unauthorized users to gain access.

Question #:17 - (Exam Topic 2)

A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

A. pcap reassembly

B. SSD snapshot

C. Image volatile memory

D. Extract from checksums

Answer: C

Explanation

Image Volatile Memory: This technique involves creating a memory dump or memory image of the system's RAM (Random Access Memory). By capturing the contents of RAM, you can potentially extract the running malicious code from memory. Analyzing the memory dump allows you to retrieve the malware binary, including its code and data, which can be crucial for further analysis and investigation.

The other options mentioned do not directly address the capture of malware binaries from volatile memory:

pcap reassembly: pcap reassembly is used for reassembling network traffic captured in pcap files. While it may capture network communication related to the malware download, it does not capture the malware binary itself.

SSD snapshot: An SSD snapshot typically refers to capturing the state of a Solid-State Drive (SSD) at a specific point in time. It is not typically used for capturing malware binaries from memory.

Extract from checksums: Extracting malware from checksums is not a standard forensic technique. Checksums are used for data integrity verification and error detection, not for extracting malware binaries.

Danut Halau

—

Today at 1:54 PM

Volatile memory, or RAM (Random Access Memory), is a physical component inside a computer or other electronic devices

Question #:18 - (Exam Topic 2)

Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

A. Walk-throughs

B. Lessons learned

C. Attack framework alignment

D. Containment

Answer: B

Explanation

After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as “lessons learned” and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of any potential changes that can be made to prevent similar incidents from occurring in the future.

Question #:19 - (Exam Topic 2)

A system's analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select two).

A. The order of volatility

B. A forensics NDA

C. The provenance of the artifacts

D. The vendor's name

E. The date and time

F. A warning banner

Answer: C E

Explanation

The system's analyst should include the following in the digital forensics chain-of-custody form:

C. The provenance of the artifacts

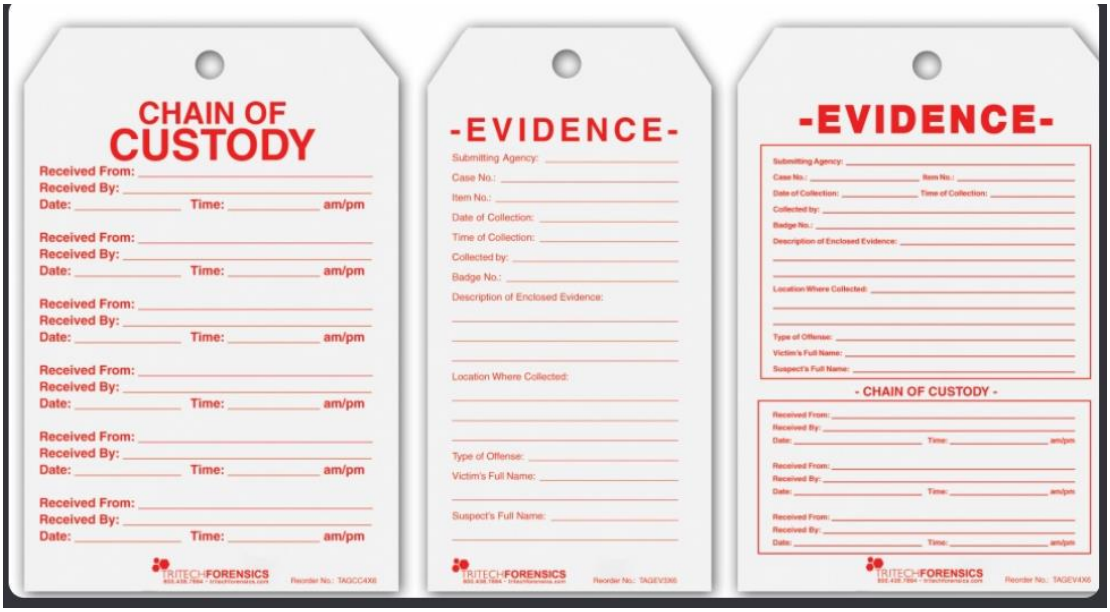
E. The date and time

The provenance of the artifacts is important because it helps establish the authenticity and integrity of the evidence collected. The chain-of-custody form serves as a record of who has had access to the evidence, and in what order, to prevent tampering or alteration.

The date and time are important because they provide a record of when the evidence was collected and by whom, which helps establish the relevance and reliability of the evidence. Having this information helps ensure that the evidence can be used in a court of law, if necessary

The order of volatility is an important concept in digital forensics, but it is not part of a chain-of-custody form. The chain-of-custody form is a record of the movement and handling of evidence in a manner that ensures its authenticity and integrity, and documents the steps taken to preserve and protect it. The order of volatility refers to the priority in which data should be collected from a system in order to ensure that volatile and rapidly changing data is collected before it is lost.

- ➔ Date and time of collection
- ➔ Location of collection
- ➔ Name of investigator(s)
- ➔ Name or owner of the media or computer
- ➔ Reason for collection
- ➔ Matter name or case number
- ➔ Type of media
- ➔ Serial number of media if available
- ➔ Make and model of hard drive or other media
- ➔ Storage capacity of device or hard drive
- ➔ Method of capture (tools used)
- ➔ Physical description of computer and whether it was on or off
- ➔ Name of the image file or resulting files that were collected
- ➔ Hash value(s) of source hard drive or files
- ➔ Hash value(s) of resulting image files for verification
- ➔ Any comments or issues encountered
- ➔ Signature(s) of persons giving and taking possession of evidence



Question #:20 - (Exam Topic 2)

Which of the following should a Chief Information Security Officer consider using to take advantage of industry standard guidelines?

A. SSAE SOC 2

B. GDPR

C. PCI DSS

D. NIST CSF

Answer: D

Explanation

NIST CSF: The NIST Cybersecurity Framework provides a comprehensive set of guidelines and best practices for improving cybersecurity posture. It is widely recognized and used by organizations to enhance their cybersecurity efforts. The framework offers a flexible and risk-based approach to managing cybersecurity and aligns with industry standards and regulations.

While the other options mentioned are important for specific purposes:

SSAE SOC 2 (Statement on Standards for Attestation Engagements Service Organization Control 2): This is a framework for assessing the controls related to security, availability, processing integrity, confidentiality, and privacy of customer data. It is particularly relevant for service organizations that handle customer data.

GDPR (General Data Protection Regulation): GDPR is a European regulation that governs data protection and privacy. It is essential for organizations that process personal data of European Union (EU) residents.

PCI DSS (Payment Card Industry Data Security Standard): PCI DSS is a set of security standards designed to ensure the secure handling of credit card information. It is mandatory for organizations that handle payment card data.

These standards and regulations address specific areas of cybersecurity and data protection, but are not as comprehensive or universally applicable as the NIST CSF. The NIST CSF can serve as a foundational framework that can be customized to align with other standards and regulations, making it a valuable choice for CISOs looking to improve their organization's cybersecurity posture while adhering to industry standards.

Question #:21 - (Exam Topic 2)

DRAG DROP

A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

INSTRUCTIONS

From the options below, drag each item to its appropriate classification as well as the MOST appropriate form of disposal.

Question #:22 - (Exam Topic 2)

The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

A. HIDS

B. FDE

C. NGFW

D. EDR

Answer: D

Explanation

EDR solutions are designed to detect and respond to malicious activity on workstations and servers, and they provide a detailed analysis of the incident, allowing organizations to quickly remediate the threat. According to the CompTIA Security+ SY0-601 Official Text Book, EDR solutions can be used to detect malicious activity on endpoints, investigate the incident, and contain the threat. EDR solutions can also provide real-time monitoring and alerting for potential security events, as well as detailed forensic analysis for security incidents. Additionally, the text book recommends that organizations also implement a host-based intrusion detection system (HIDS) to alert them to malicious activity on their workstations and servers.

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

Question #:23 - (Exam Topic 2)

A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release. Which of the following documents would the third-party vendor most likely be required to review and sign?

A. SLA

B. NDA

C. MOU

D. AUP

Answer: B

Explanation

NDA stands for Non-Disclosure Agreement, which is a legal contract that binds the parties to keep confidential information secret and not to disclose it to unauthorized parties. A third-party vendor who is doing a penetration test of a new proprietary application would most likely be required to review and sign an NDA to protect the intellectual property and trade secrets of the security team.

Question #:24 - (Exam Topic 2)

A data center has experienced an increase in under-voltage events following electrical grid maintenance outside the facility. These

events are leading to occasional losses of system availability. Which of the following would be the most cost-effective solution for the data center to implement?

A. Uninterruptible power supplies with battery backup

B. Managed power distribution units lo track these events

C. A generator to ensure consistent, normalized power delivery

D. Dual power supplies to distribute the load more evenly

Answer: A

Explanation

Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes.
Managed power distribution units (option B) would provide information about the under-voltage events but would not address the underlying issue. It may be helpful to track these events, but it will not prevent the occasional losses of system availability.
Dual power supplies (option D) can distribute the load more evenly, but they do not address the issue of under-voltage events caused by power grid maintenance. Additionally, adding dual power supplies may also require additional infrastructure and equipment, resulting in higher capital and operational costs.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.apc.com/us/en/faqs/FA158852/

Danut Halau

—

Today at 2:13 PM

an Uninterruptible Power Supply (UPS) with battery backup is a critical device used to provide a continuous supply of electrical power to connected equipment, such as computers, servers, networking gear, and other sensitive electronic devices, even in the event of a power outage or disruption

Question #:25 - (Exam Topic 2)

A major manufacturing company updated its internal infrastructure and just started to allow OAuth applications to access corporate data. Data leakage is being reported. Which of the following most likely caused the issue?

A. Privilege creep

B. Unmodified default settings

C. TLS protocol vulnerabilities

D. Improper patch management

Answer: B

Danut Halau

—

Today at 2:16 PM
Unmodified default typically refers to software or system settings and configurations that have not been altered or customized by the user or administrator. In many cases, software and operating systems come with default settings that are intended to work well for a wide range of users or devices

Nigina Novruzova

Today at 2:16 PM
Unmodified default settings in OAuth can also be a likely cause of data leakage. OAuth scopes define the level of access an application has to a particular resource. The default scope may be configured to provide access to resources that it shouldn't, resulting in unauthorized access to sensitive data. This can occur if the default scope was not modified to restrict access to only the necessary resources for the application. Therefore, B. Unmodified default settings can also be a likely cause of data leakage in this scenario.

David Berrios

Today at 2:16 PM
This issue might have occurred if the OAuth applications were allowed access with default or weak security configurations, which could lead to unauthorized access and data leakage. It's common for software and applications to come with default settings that might not be secure for a corporate environment. Proper configuration and security settings should be applied to ensure the safe use of OAuth applications in accessing corporate data

Danut Halau

Today at 2:15 PM

Privilege creep, also known as privilege escalation or entitlement creep, is a cybersecurity and access management challenge that occurs when individuals or entities within an organization gradually accumulate more privileges, permissions, or access rights than they need to perform their job responsibilities

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.techtarget.com/searchsecurity/definition/privilege-creep

Question #:26 - (Exam Topic 2)

A large bank with two geographically dispersed data centers is concerned about major power disruptions at Both locations. Every day each location experiences very brief outages that last for a few seconds. However, during the summer a high risk of intentional under-voltage events that could last up to an hour exists, particularly at one of the locations near an industrial shelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply

B. Generator

C. PDU

D. Daily backups

Answer: B

Explanation

A generator will provide uninterrupted power to the data centers, ensuring that they are not affected by any power disruptions, intentional or otherwise. This is more reliable than a dual supply or a PDU, and more effective than daily backups, which would not be able to protect against an outage lasting an hour.

Question #:27 - (Exam Topic 2)

Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

A. Public cloud

B. Hybrid cloud

C. Community cloud

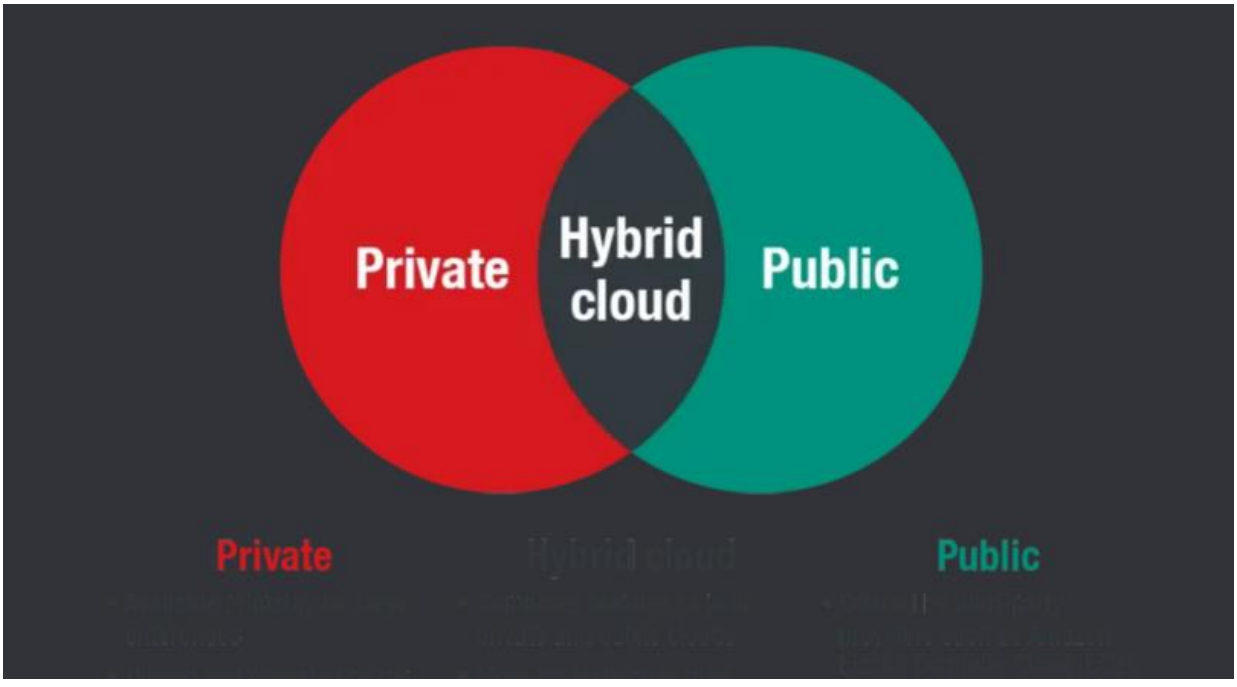
D. Private cloud

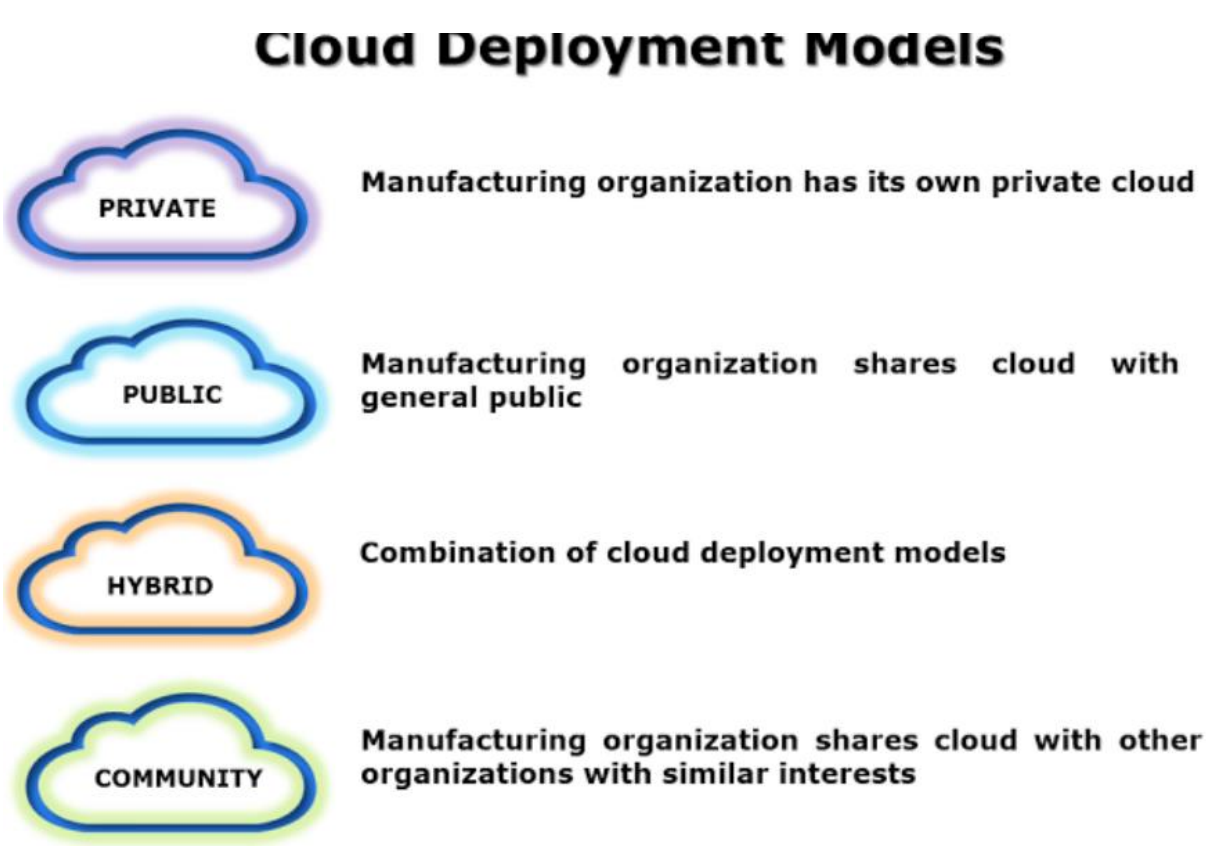
Answer: A

Explanation

There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.

According to one source, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.





Petra Martina Vrancic

—

Today at 2:21 PM

Community Cloud: Definition: A community cloud is a cloud infrastructure that is shared by several organizations with common concerns, such as security, compliance, or industry-specific requirements. Characteristics: Shared by a specific community or organizations with similar needs. The infrastructure can be managed by the organizations themselves or a third-party service provider. It provides a more controlled and secure environment compared to public cloud.

Question #:28 - (Exam Topic 2)

A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the following should the analyst recommend? (Select two).

A. TACACS+

B. RADIUS

C. OAuth

D. OpenlD

E. Kerberos

F. CHAP

Answer: B E

Explanation

RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with

network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

Question #:29 - (Exam Topic 2)

A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?

A. Weighted response

B. Round-robin

C. Least connection

D. Weighted least connection

Answer: B

Explanation

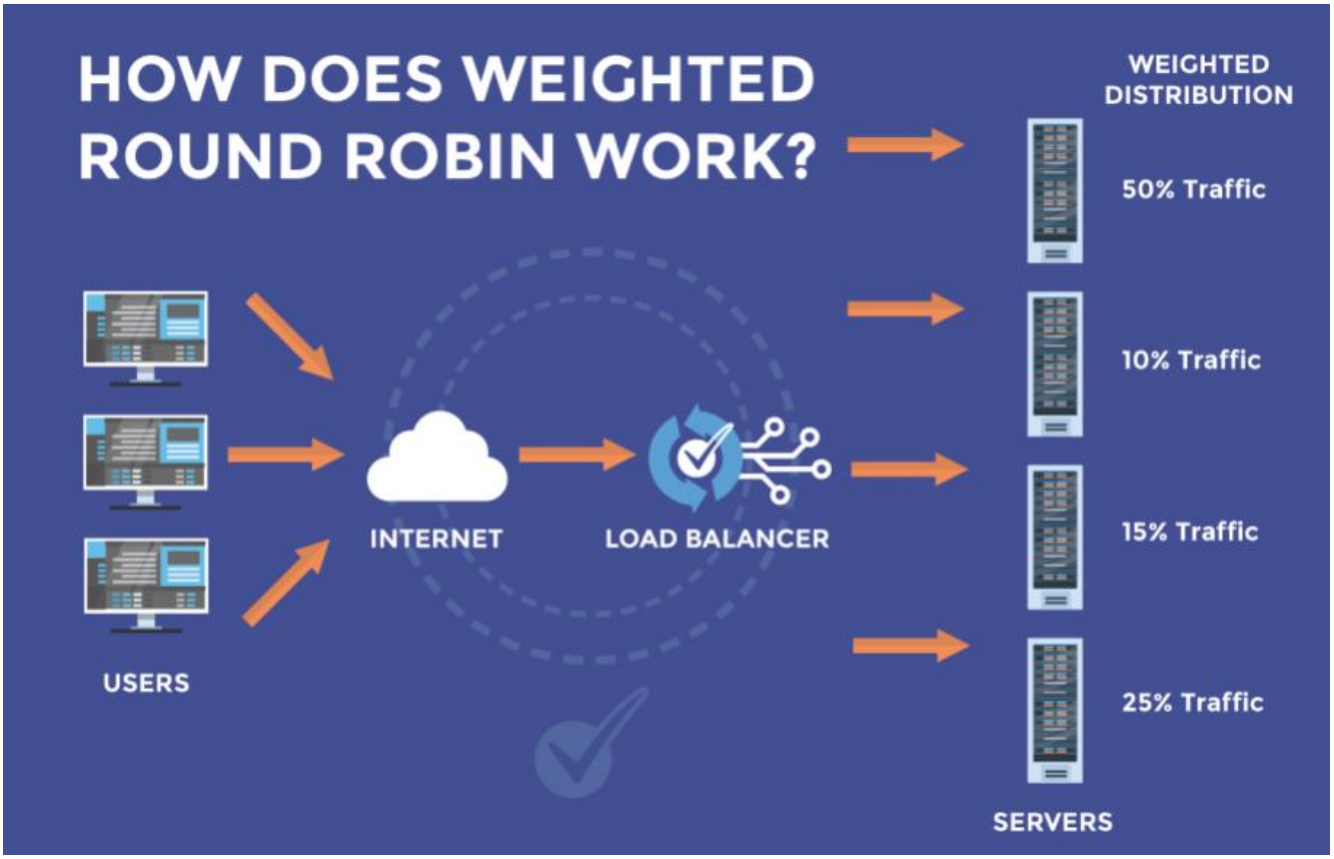
Round-robin is a type of load balancing algorithm that distributes traffic to a list of servers in rotation. It is a static algorithm that does not take into account the state of the system for the distribution of tasks. It assumes that all servers have equal capacity and can handle an equal amount of traffic.

The administrator should use a round-robin algorithm to split the number of connections on each server in half. Round-robin is a load-balancing algorithm that distributes incoming requests to the available servers one by one in a cyclical order. This helps to evenly distribute the load across all of the servers, ensuring that no single server is overloaded.

David Berrios
—
Today at 2:24 PM
round-robin

[
2:24 PM
]

n a round-robin load balancing algorithm, each server is selected in turn for new connections. When a new connection request comes in, it is forwarded to the next server in the list, ensuring an even distribution of connections among the servers. This method effectively balances the load across multiple servers without considering the server's current load or capacity.



Question #:30 - (Exam Topic 2)

A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?

A. SIEM

B. HIDS

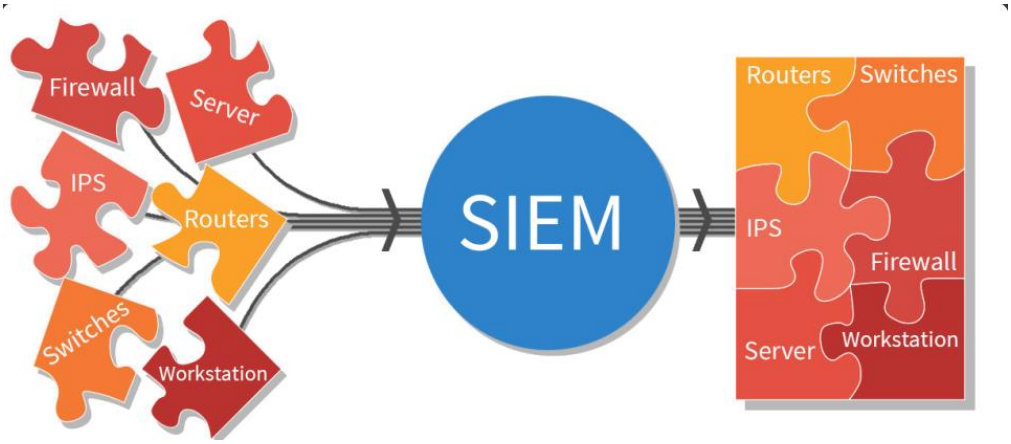
C. CASB

D. EDR

Answer: A

Explanation

SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.



Question #:31 - (Exam Topic 2)

Which of the following measures the average time that equipment will operate before it breaks?

A. SLE

B. MTBF

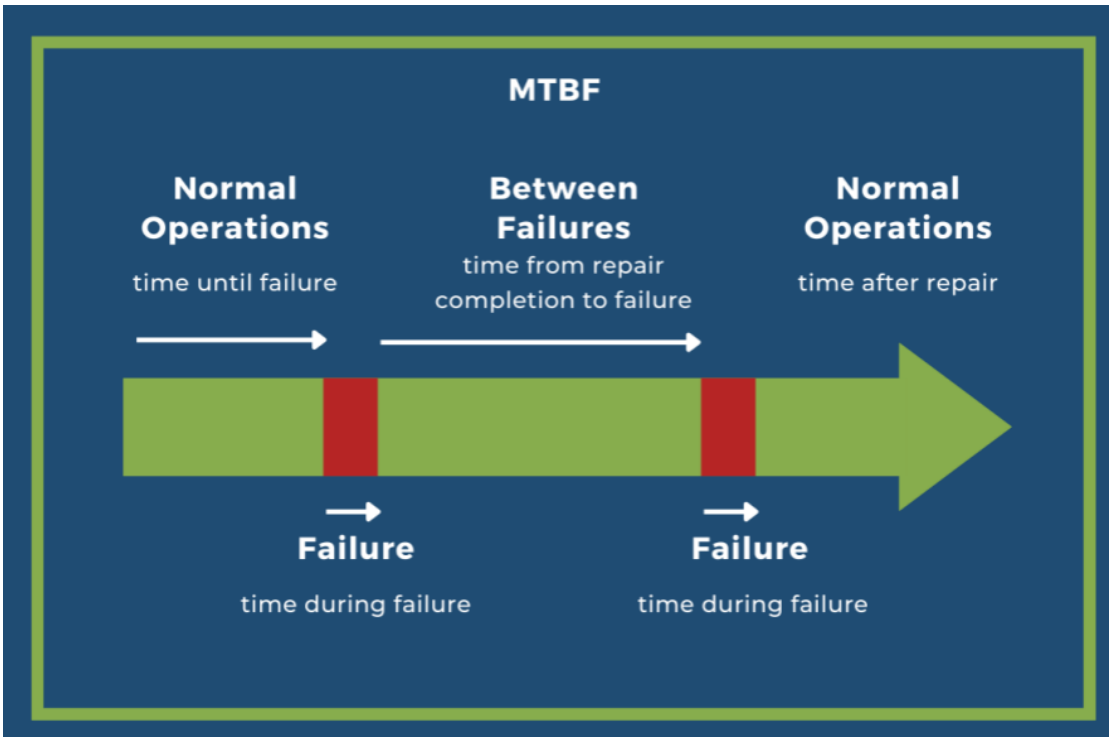
C. RTO

D. ARO

Answer: B

Explanation

The measure that calculates the average time that equipment will operate before it breaks is MTBF. MTBF stands for Mean Time Between Failures and it is a metric that represents the average time between two failures occurring in a given period. MTBF is used to measure the reliability and availability of a product or system. The higher the MTBF, the more reliable and available the product or system is.



Danut Halau

Today at 2:26 PM

MTBF stands for "Mean Time Between Failures." It is a reliability metric used in various industries, including technology, manufacturing, and engineering, to assess the expected average time between failures of a system, component, or product

Question #:32 - (Exam Topic 2)

Which of the following should be addressed first on security devices before connecting to the network?

A. Open permissions

B. Default settings

C. API integration configuration

D. Weak encryption

Answer: B

Explanation

Before connecting security devices to the network, it is crucial to address default settings first. Manufacturers often ship devices with default settings that include default usernames, passwords, and configurations. These settings are widely known and can be easily exploited by attackers. Changing default settings helps to secure the device and prevent unauthorized access. Reference: CompTIA Security+ SY0-501 Exam Objectives, Section 3.2: "Given a scenario, implement secure systems design." (https://www.comptia.jp/pdf/Security%2B%20SY0-501%20Exam%20Objectives.pdf)

Question #:33 - (Exam Topic 2)

A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment

B. Log queue

C. Log parser

D. Log collector

Answer: D

Explanation

A log collector can collect logs from various sources, such as servers, devices, applications, or network components, and forward them to a central source for analysis and storage.

A log collector is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance that collects logs from various sources, such as firewalls, routers, servers, applications, or endpoints. A log collector can also perform functions such as log filtering, parsing, aggregation, normalization, and enrichment. A log collector can help centralize logging by sending the collected logs to a central log server or a security information and event management (SIEM) system for further analysis and correlation.

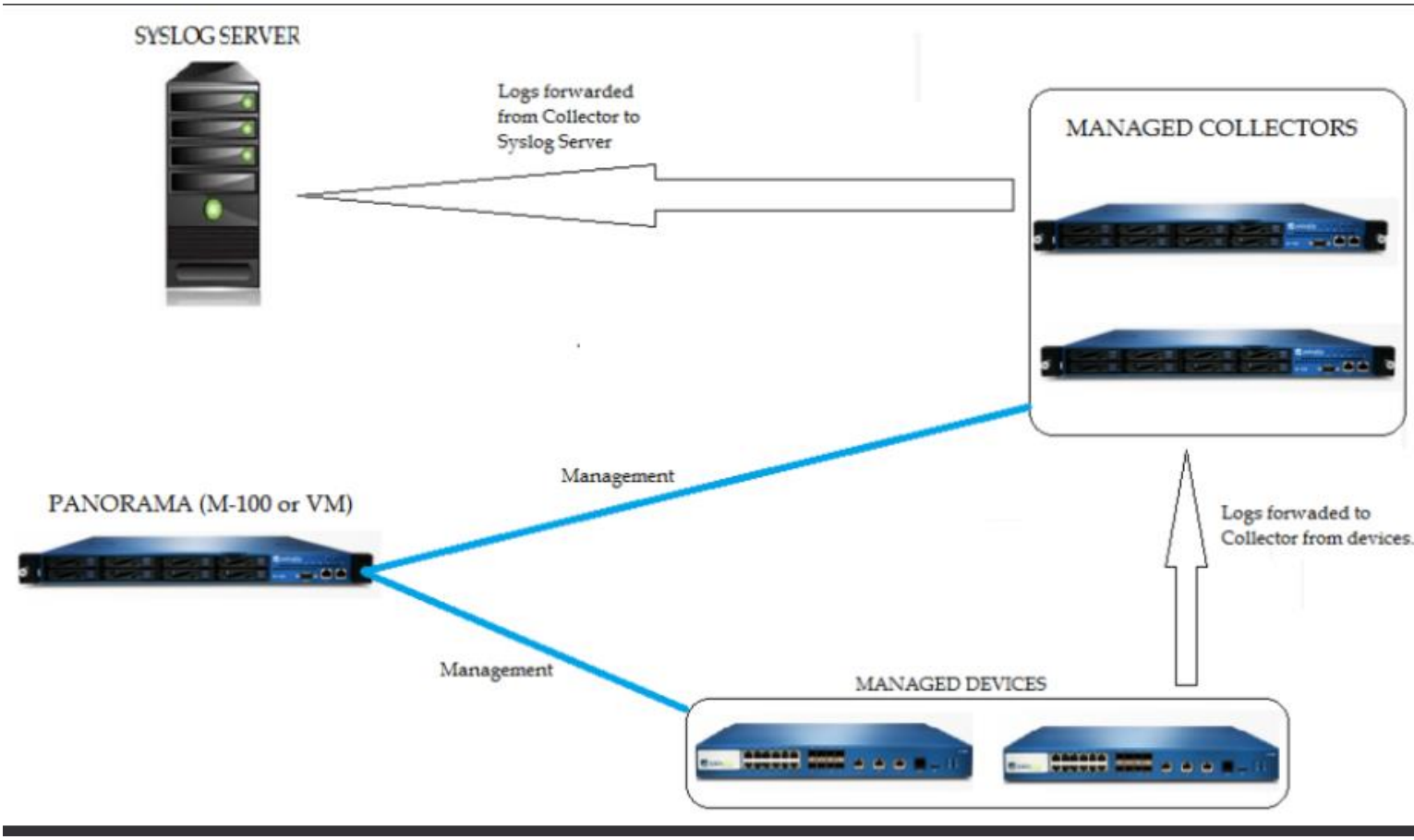
Log aggregation is the process of combining logs together. This is done to allow different formats from different systems to work together.

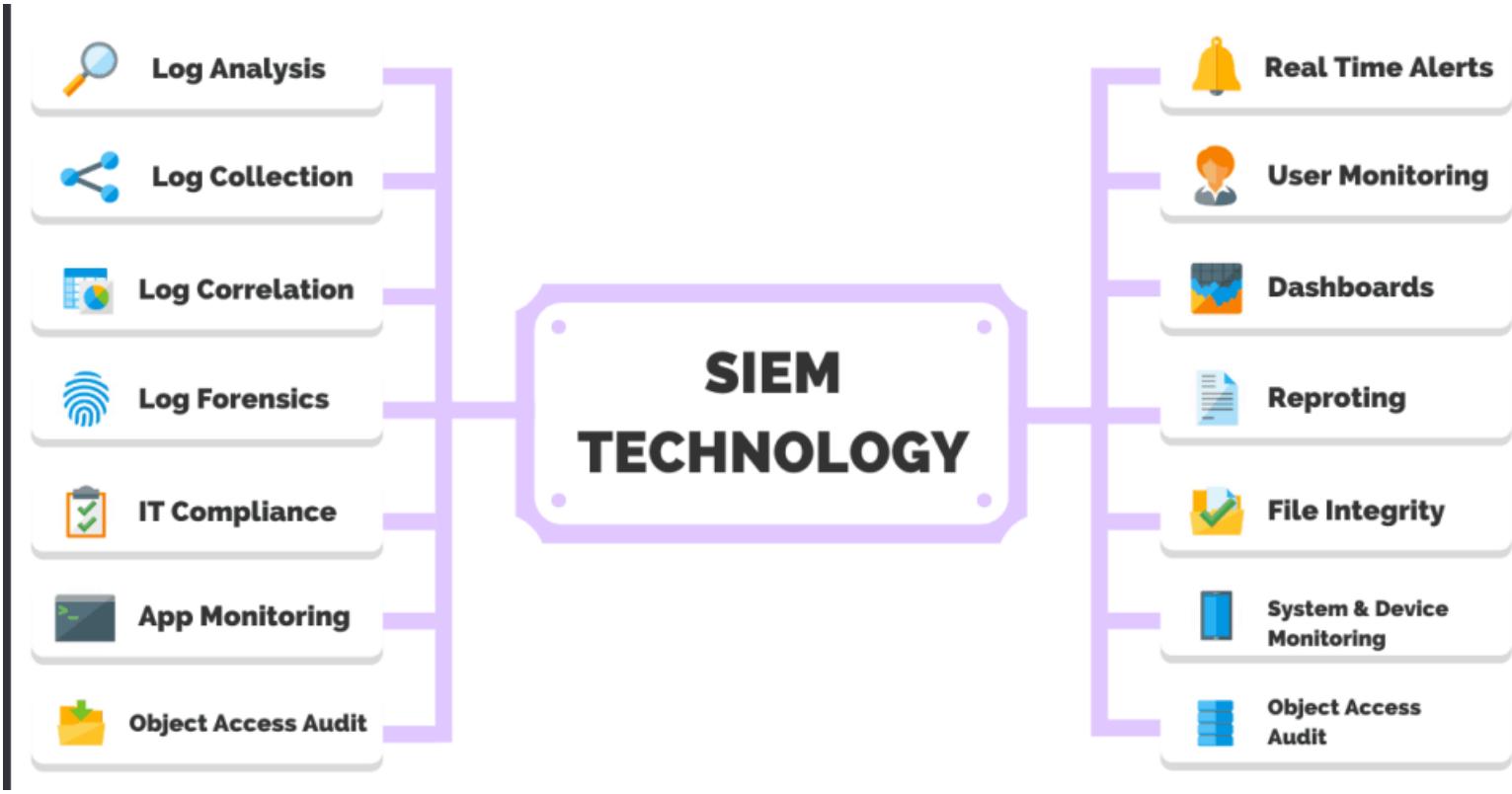
A: Log enrichment: Enhances log data with additional information or context to make it more valuable for analysis.

B:Log queue: Temporarily stores log entries before forwarding them to their destination. It helps manage the flow of logs in case the destination becomes temporarily unavailable.

C:Log parser: Interprets and extracts information from log data, making it readable and structured for analysis. Log parsers are often used in log collectors as well as log management systems.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://geekflare.com/open-source-centralized-logging/





Question #:34 - (Exam Topic 2)

Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's main gate?

A. Crossover error rate

B. False match raw

C. False rejection

D. False positive

Answer: C

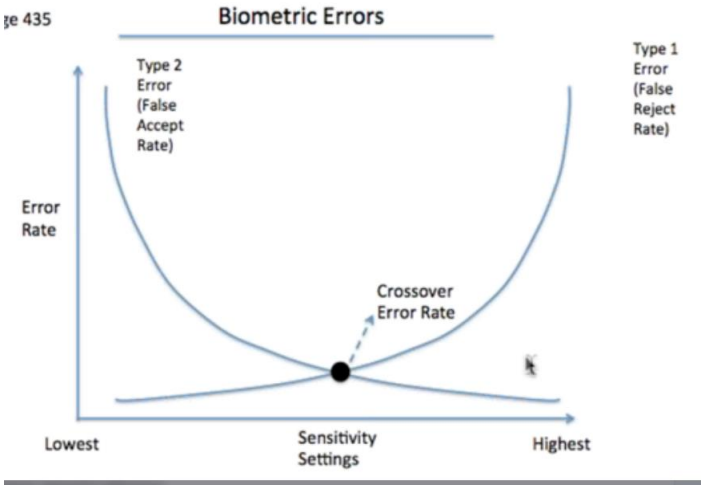
Explanation

False rejection Short Explanation: A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors.

A: Crossover Error Rate (CER): The crossover error rate is a metric used to evaluate the performance of biometric systems. It represents the point at which the false match rate (FMR) and false non-match rate (FNMR) are equal. It is used to measure the overall accuracy and reliability of a biometric system.

B: False Match Rate (FMR): The false match rate is a measure of the likelihood that the system incorrectly matches an input biometric sample (e.g., fingerprint) with a different user's stored biometric template. It represents a false positive error in biometric authentication.

D: False Positive: A false positive occurs when a system incorrectly identifies an unauthorized or incorrect user as a legitimate one. In biometric authentication, this would mean that the system incorrectly matches a person's biometric data (e.g., fingerprint) to a stored template, allowing access to an unauthorized user.



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

Question #:35 - (Exam Topic 2)

Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

A. IP schema

B. Application baseline configuration

C. Standard naming convention policy

D. Wireless LAN and network perimeter diagram

Answer: C

Explanation

A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.

A: IP Schema: An IP schema, often referred to as an IP addressing plan or subnetting plan, provides guidelines for allocating and managing IP addresses within a network. It focuses on how IP addresses are assigned to devices and subnets, rather than on device labeling.
B: Application Baseline Configuration: An application baseline configuration typically outlines the standard settings, configurations, and security measures that should be applied to software applications within the network. It doesn't directly relate to labeling network devices.
D: Wireless LAN and Network Perimeter Diagram: This represents a diagram or visual representation of the network layout, including wireless LAN components and network perimeters. While it can be a valuable reference for network design and security, it doesn't provide guidelines for labeling individual devices.

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/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P

Question #:36 - (Exam Topic 2)

A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase in the number of requests to delete user accounts. Which of the following best describes the consequence of this data disclosure?

A. Regulatory tines

B. Reputation damage

C. Increased insurance costs

D. Financial loss

Answer: B

Explanation

Reputation damage is the loss of trust or credibility that a company suffers when its customers' personal data is exposed or breached. This can lead to customer dissatisfaction, loss of loyalty, and requests to delete user accounts.
References: https://www.comptia.org/content/guides/what-is-cybersecurity

Nita Arapi
—
Today at 2:33 PM
question is about user accounts deleting

David Berrios
—

Today at 2:33 PM
first losss reputation

Danut Halau
—
Today at 2:33 PM
Reputation damage, in the context of organizations or individuals, refers to the harm or negative impact inflicted on their public image, credibility, and trustworthiness as a result of certain actions, events, or circumstancesì

Question #:37 - (Exam Topic 2)

A user is trying to upload a tax document, which the corporate finance department requested, but a security program is prohibiting the upload. A security analyst determines the file contains PII. Which of the following steps can the analyst take to correct this issue?

A. Create a URL filter with an exception for the destination website.

B. Add a firewall rule to the outbound proxy to allow file uploads

C. Issue a new device certificate to the user's workstation.

D. Modify the exception list on the DLP to allow the upload

Answer: D

Explanation

Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow the tax document to be uploaded without compromising the security of the system.

A: Creating a URL filter with an exception for the destination website: URL filtering is primarily used to control access to websites, but it doesn't address the issue of file uploads.
B: Adding a firewall rule to the outbound proxy to allow file uploads: While this can control network traffic, it does not address the content inspection and detection of PII within files.
C: Issuing a new device certificate to the user's workstation: This action is related to device authentication but doesn't address the issue of blocked uploads due to PII content in the file.

(Reference: CompTIA Security+ SY0-601 Official Textbook, page 479-480)

Question #:38 - (Exam Topic 2)

Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation for a few days. Which of the following attacks can the account lockout be attributed to?

A. Backdoor

B. Brute-force

C. Rootkit

D. Trojan

Answer: B

Explanation

The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

Question #:39 - (Exam Topic 2)

Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

A. User

B. Wildcard

C. Self-signed

D. Root

Answer: B

Explanation

A wildcard certificate is a type of digital certificate that can be used to secure multiple subdomains under a single domain name. For example, a wildcard certificate for *.example.com can be used to secure www.example.com, mail.example.com, blog.example.com, etc. A wildcard certificate can make administration easier by reducing the number of certificates that need to be issued, managed, and renewed. It can also save costs and simplify configuration.

Question #:40 - (Exam Topic 2)

An organization decided not to put controls in place because of the high cost of implementing the controls compared to the cost of a potential fine. Which of the following risk management strategies is the organization following?

A. Transference

B. Avoidance

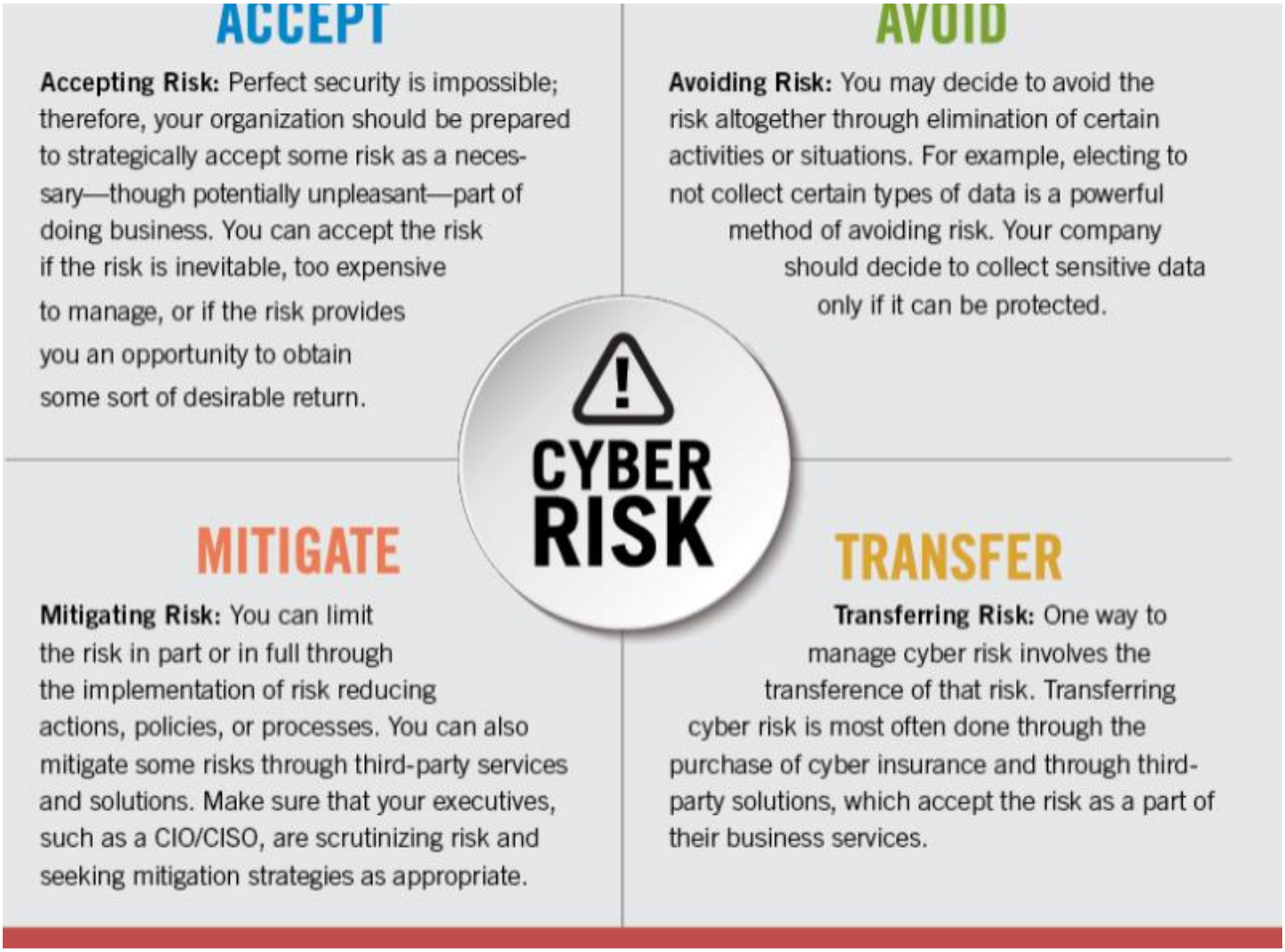
C. Mitigation

D. Acceptance

Answer: D

Explanation

Acceptance is a risk management strategy that involves acknowledging the existence and potential impact of a risk, but deciding not to take any action to reduce or eliminate it. This strategy is usually adopted when the cost of implementing controls outweighs the benefit of mitigating the risk, or when the risk is deemed acceptable or unavoidable. In this case, the organization decided not to put controls in place because of the high cost compared to the potential fine, which means they accepted the risk. References: https://www.comptia.org/blog/what-is-risk-acceptance



Question #:41 - (Exam Topic 2)

Which of the following control types is patch management classified under?

A. Deterrent

B. Physical

C. Corrective

D. Detective

Answer: C

Explanation

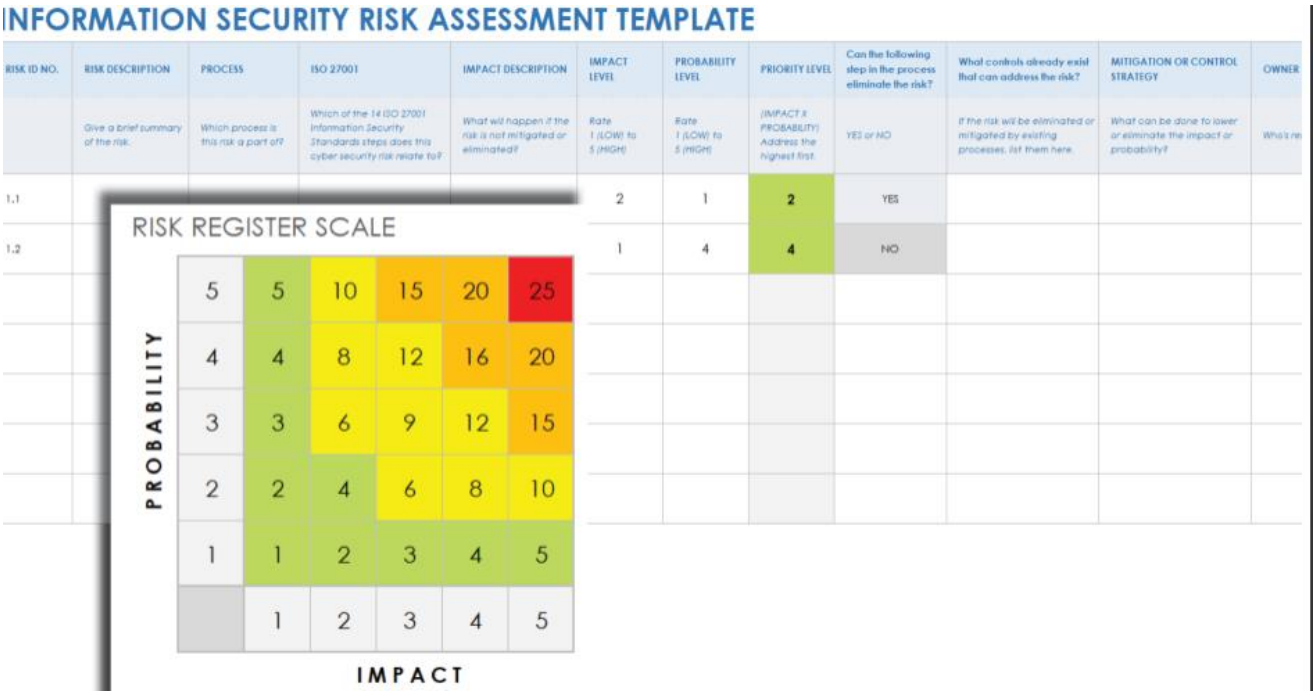
Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

Patch management is a process that involves applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patch management is classified under corrective control type, which is a type of control that aims to restore normal operations after an incident or event has occurred. Corrective controls can help mitigate the impact or damage caused by an incident or event and prevent it from happening again.

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 #:42 - (Exam Topic 2)

A desktop computer was recently stolen from a desk located in the lobby of an office building. Which of the following would be the best way to secure a replacement computer and deter future theft?

A. Installing proximity card readers on all entryway doors

B. Deploying motion sensor cameras in the lobby

C. Encrypting the hard drive on the new desktop

D. Using cable locks on the hardware

Answer: D

Explanation

Using cable locks on the hardware can be an effective way to secure a desktop computer and deter future theft. Cable locks are physical security devices that attach to the computer case and to a nearby stationary object, such as a desk or wall. This makes it more difficult for a thief to remove the computer without damaging it or attracting attention.

A: Installing proximity card readers on all entryway doors can enhance physical security by limiting access to authorized individuals.

B: Deploying motion sensor cameras in the lobby can also help deter theft by capturing images of any unauthorized individuals entering the premises or attempting to steal the computer.

C: Encrypting the hard drive on the replacement desktop can also help protect sensitive data in the event of theft, but it does not provide physical security for the device itself.

Question #:43 - (Exam Topic 2)

Which of the following can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan

B. Threat intelligence

C. Log aggregation

D. Packet capture

Answer: D

Packet capture, often referred to as network packet analysis or packet sniffing, involves capturing and inspecting the data packets that traverse a network. By analyzing the network traffic over port 80, you can potentially detect unauthorized or suspicious activities, such as data exfiltration or unauthorized access to web resources. Packet capture provides insights into the actual data being transmitted and can help identify anomalies or malicious activities.

A: Web application scan: This is typically used to assess the security of web applications and websites but may not directly capture ongoing data theft over port 80.

B:Threat intelligence: Threat intelligence involves collecting and analyzing data to identify potential threats and vulnerabilities. While it's valuable for proactive security measures, it may not provide real-time detection of a specific incident.

C: Log aggregation: Log aggregation involves collecting and centralizing logs from various sources, including network devices and servers. While it can help in incident response and investigation, it relies on the availability of relevant logs, and detection may occur after the fact. Packet capture is more immediate for detecting ongoing activity

Danut Halau

—

Today at 2:43 PM

Packet capture, also known as packet sniffing or network packet analysis, is the process of capturing and analyzing data packets as they traverse a network or communication medium

Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities

Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses

Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling

Using a CASB tool to control access to cloud resources and prevent data leaks or downloads Encrypting

data at rest and in transit and enforcing strong authentication and authorization policies

Nigina Novruzova

—

Today at 2:44 PM

Packet capturing: -helps to analyze networks -identify network performance issues -manage

network traffic.

Question #:44 - (Exam Topic 2)

A cybersecurity analyst at Company A is working to establish a secure communication channel with a counterpart at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal in a secure manner?

A. Digital signatures

B. Key exchange

C. Salting

D. PPTP

Answer: B

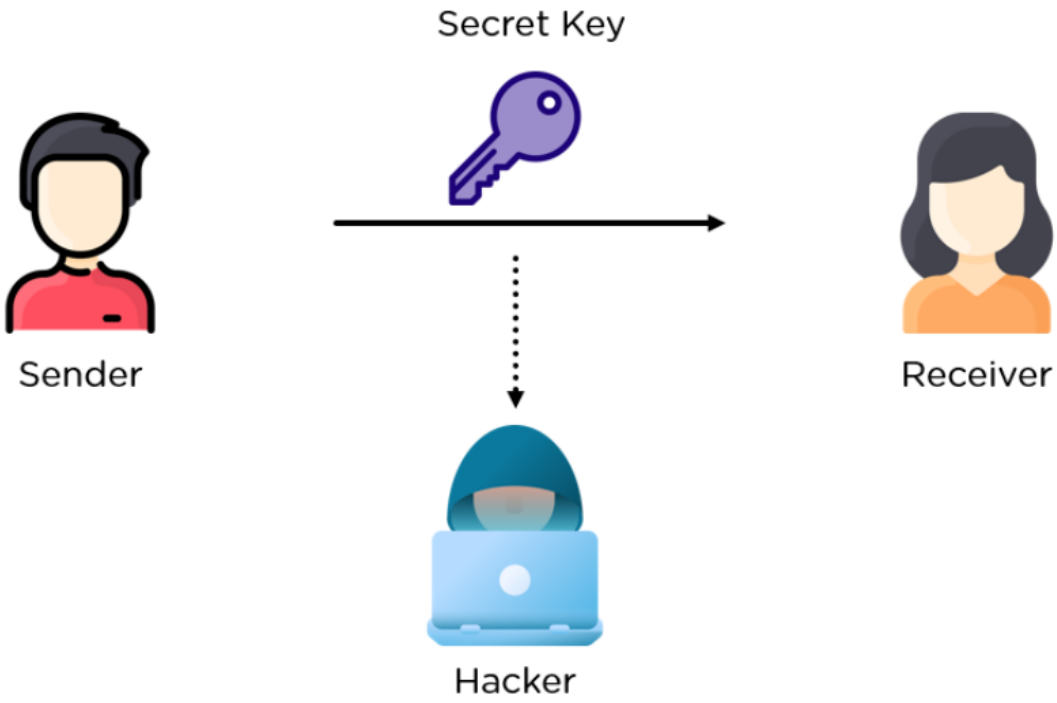
Explanation

Key exchange Short Explanation: Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA.

Key exchange protocols are designed to securely exchange cryptographic keys between two parties, enabling them to establish a secure communication channel over an insecure network, such as the internet. In this scenario, the analyst and counterpart can use a key exchange protocol to securely generate and share encryption keys, which can then be used to encrypt and decrypt their communication. This ensures the confidentiality and integrity of the data transmitted over the long-distance communication channel.

A: Digital signatures are used to verify the authenticity and integrity of digital messages or documents. While important for ensuring the source of a message, they are not directly related to establishing a secure communication channel.
C: Salting is a technique used to enhance the security of password storage by adding random data to each password before hashing it. It is not used to establish secure communication channels.
D: PPTP (Point-to-Point Tunneling Protocol) is a VPN protocol that can be used to create secure communication channels over networks, but it is considered outdated and not recommended for secure long-distance communications due to known vulnerabilities. Modern VPN protocols like IPsec or TLS are typically preferred.

References: https://www.comptia.org/content/guides/what-is-encryption



Question #:45 - (Exam Topic 2)

A security analyst received the following requirements for the deployment of a security camera solution:
* The cameras must be viewable by the on-site security guards.

* The cameras must be able to communicate with the video storage server.

* The cameras must have the time synchronized automatically.

* The cameras must not be reachable directly via the internet.

* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.

Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?

A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on

B. Deploying a jump server that is accessible via the internal network that can communicate with the servers

C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering

D. Implementing a WAF to allow traffic from the local NTP server to the camera server

Answer: B

Explanation
Not: Camera is an IOT device and we need to secure it

A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them.

A jump server can also be used for auditing traffic and user activity for real-time surveillance

By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet. The other options are not suitable because:

A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.

C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.

D. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.

References:

1: https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/

2 :https://www.ssh.com/academy/iam/jump-server

3: https://en.wikipedia.org/wiki/Jump_server

David Berrios — Today at 2:47 PM

Jump server

Danut Halau — Today at 2:47 PM

Deploying a jump server also known as a jump host or bastion host is a common practice in network security to provide controlled access to internal servers

NEW

Petra Martina Vrancic — Today at 2:47 PM

It acts as an intermediary, providing controlled access to the servers

Question #:46 - (Exam Topic 2)

A security analyst reviews web server logs and notices the following line:

104.35.45.53 - [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT user login, user _ pass, user email from wp users—— HTTP/I.I" 200 1072 http://www.example.com/wordpress/wp—admin/

Which of the following vulnerabilities is the attacker trying to exploit?

A. SSRF

B. CSRF

C. xss

D. SQLi

Answer: D

Explanation

SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution.

The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users' accounts.

What is union all in SQL query?

UNION ALL Operator is used to combine result set of two or more SELECT queries. The UNION ALL operator does not remove duplicate rows from SELECT statement result set. UNION and UNION ALL operators works same. Only difference is UNION operator exclude duplicate rows from result set.

Question #:47 - (Exam Topic 2)

Given the following snippet of Python code:

Which of the following types of malware MOST likely contains this snippet?

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename=("output.txt"), level=logging.DEBUG, format=" %(asctime) s - %(message) s")
def on_press(key) :
        logging.info(str(key))
with Listener(on_press=on_press) as listener :
        listener.join()
```

A. Logic bomb

B. Keylogger

C. Backdoor

D. Ransomware

Answer: B

Explanation

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename=("output.txt"), level=logging.DEBUG, format=" %(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener :
    listener.join()
```

https://nitratine.net/blog/post/python-keylogger/

This code is a simple example of a keylogger script written in Python. Keyloggers are a type of malware that records and logs keystrokes on a compromised system, often without the user's knowledge or consent. The code uses the pynput library to capture keyboard events and log them to an "output.txt" file. Keyloggers can be used for malicious purposes, such as capturing sensitive information like passwords or credit card numbers, making it a type of malware commonly associated with espionage and data theft.

Danut Halau

—

Today at 2:50 PM

also heare u find the anser heare from pynput.keyboard import Key, Listener logging.basicConfig(filename=("output.txt"), level=legging.DEBUG, format=" %(asctime) s - %(message) s")

Question #:48 - (Exam Topic 2)

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems

B. To keep all software and hardware fully patched for known vulnerabilities

C. To only allow approved, organization-owned devices onto the business network

D. To standardize by selecting one laptop model for all users in the organization

Answer: A

Explanation

An effective asset management policy helps an organization understand and manage the systems, hardware, and software it uses, and how they are used, including their vulnerabilities and risks. This information is crucial for accurately identifying and assessing risks to the organization, and making informed decisions about how to mitigate those risks. This is the best reason to maintain an effective asset management policy.

While keeping software and hardware fully patched for known vulnerabilities, only allowing approved, organization-owned devices onto the business network, and standardizing laptop models can also contribute to an organization's security posture, these measures alone are not sufficient to ensure effective asset management and security.

A comprehensive asset management policy should address all aspects of asset management, including procurement, deployment, maintenance, and retirement of assets, to provide a complete and effective security solution.

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

A - effective asset management help you identify critical systems etc. and the appropriate security controls

B - refers to patch management not asset management

C - refers to corporate owned model for devices not asset management

D – not practical

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

Danut Halau

—

Today at 2:53 PM

This process helps organizations understand and prioritize risks, make informed decisions, and allocate resources effectively.

Question #:49 - (Exam Topic 2)

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be best to help the organization's executives determine their next course of action?

A. An incident response plan

B. A communication plan

C. A disaster recovery plan

D. A business continuity plan

Answer: D

Explanation

A business continuity plan (BCP) is a document that outlines how an organization will continue its critical functions during and after a disruptive event, such as a natural disaster, pandemic, cyberattack, or power outage. A BCP typically covers topics such as business impact analysis, risk assessment, recovery strategies, roles and responsibilities, communication plan, testing and training, and maintenance and review. A BCP can help the organization's executives determine their next course of action by providing them with a clear framework and guidance for managing the crisis and resuming normal operations.

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 #: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 heare is BIOMETRICS so is going to screen