



# CompTIA

## Exam Questions SY0-701

CompTIA Security+ Exam

#### NEW QUESTION 1

- (Exam Topic 1)

A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

- A. Use fuzzing testing
- B. Use a web vulnerability scanner
- C. Use static code analysis
- D. Use a penetration-testing OS

**Answer: C**

#### Explanation:

Using static code analysis would be the best approach to scan the source code looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. This method involves analyzing the source code without actually running the software, which can identify security vulnerabilities that may not be detected by other testing methods. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Risk Management, pp. 292-295

#### NEW QUESTION 2

- (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 3

- (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 4

- (Exam Topic 1)

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

- A. Perfect forward secrecy
- B. Elliptic-curve cryptography
- C. Key stretching
- D. Homomorphic encryption

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 5

- (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-logon.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 c1o2s.tA 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 domain1

**NEW QUESTION 6**

- (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 7**

- (Exam Topic 1)

Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?

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

**Answer:** A

**Explanation:**

The test environment is used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics. References: CompTIA Security+ Study Guide 601, Chapter 2

**NEW QUESTION 8**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 9**

- (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 10

- (Exam Topic 1)

A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

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

**Answer: C**

#### Explanation:

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

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

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

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

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

The other options are not correct because:

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

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

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

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

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

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

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

#### NEW QUESTION 10

- (Exam Topic 1)

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

- A. SSO
- B. MFA
- C. PKI
- D. OLP

**Answer: A**

#### Explanation:

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

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

#### NEW QUESTION 13

- (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 16

- (Exam Topic 1)

A help desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?

- A. Check the metadata in the email header of the received path in reverse order to follow the email's path.
- B. Hover the mouse over the CIO's email address to verify the email address.
- C. Look at the metadata in the email header and verify the "From." line matches the CIO's email address.
- D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.

**Answer:** B

#### Explanation:

The "From" line in the email header can be easily spoofed or manipulated by an attacker to make it look like the email is coming from the CIO's email address. However, this does not mean that the email address is actually valid or that the email is actually sent by the CIO. A better way to check the email address is to hover over it and see if it matches the CIO's email address exactly. This can help to spot any discrepancies or typos that might indicate a phishing attempt. For example, if the CIO's email address is cio@company.com, but when you hover over it, it shows cio@compnay.com, then you know that the email is not authentic and likely a phishing attempt.

#### NEW QUESTION 21

- (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 24

- (Exam Topic 1)

Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

- A. GDPR
- B. PCI DSS
- C. ISO 27000
- D. NIST 800-53

**Answer:** D

#### Explanation:

NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

#### NEW QUESTION 29

- (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 33



- (Exam Topic 1)

A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

- A. Content filter
- B. SIEM
- C. Firewall rules
- D. DLP

**Answer:** C

**Explanation:**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

**NEW QUESTION 38**

- (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 43**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 44**

- (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 48**

- (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 52**

- (Exam Topic 1)

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

- A. Geofencing
- B. Self-sovereign identification
- C. PKI certificates
- D. SSO

**Answer:** A

**Explanation:**

Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

**NEW QUESTION 54**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 57**

- (Exam Topic 1)

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

- A. Buffer overflow
- B. Pass the hash
- C. SQL injection
- D. Replay attack

**Answer:** B

**Explanation:**

Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user's password, rather than requiring the plaintext password

**NEW QUESTION 60**

- (Exam Topic 1)

A security engineer needs to build @ solution to satisfy regulatory requirements that stale certain critical servers must be accessed using MFA However, the critical servers are older and are unable to support the addition of MFA, Which of te following will the engineer MOST likely use to achieve this objective?

- A. A forward proxy
- B. A stateful firewall
- C. A jump server
- D. A port tap

**Answer:** C

**Explanation:**

A jump server is a secure host that allows users to access other servers within a network. The jump server acts as an intermediary, and users can access other servers via the jump server after authenticating with MFA.

## NEW QUESTION 62

- (Exam Topic 1)

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

- A. Security patches were uninstalled due to user impact.
- B. An adversary altered the vulnerability scan reports
- C. A zero-day vulnerability was used to exploit the web server
- D. The scan reported a false negative for the vulnerability

**Answer:** A

### Explanation:

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

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

The other options are not correct because:

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

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

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

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

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

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

## NEW QUESTION 63

- (Exam Topic 1)

After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

- A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
- B. Multiple alerts were generated due to an attack occurring at the same time.
- C. An error in the correlation rules triggered multiple alerts.
- D. The SIEM was unable to correlate the rules, triggering the alert

**Answer:** A

### Explanation:

Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.

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

## NEW QUESTION 68

- (Exam Topic 1)

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

- A. Establish chain of custody.
- B. Inspect the file metadata.
- C. Reference the data retention policy.
- D. Review the email event logs

**Answer:** D

### Explanation:

Reviewing the email event logs can support an investigation for fraudulent submission, as these logs can provide details about the history of emails, including the message content, timestamps, and sender/receiver information. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 3.2 Given a scenario, implement appropriate data security and privacy controls.

## NEW QUESTION 71

- (Exam Topic 1)

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

Which of the following documents did Ann receive?

- A. An annual privacy notice
- B. A non-disclosure agreement
- C. A privileged-user agreement
- D. A memorandum of understanding

**Answer:** A



**Explanation:**

Ann received an annual privacy notice from her mortgage company. An annual privacy notice is a statement from a financial institution or creditor that outlines the institution's privacy policy and explains how the institution collects, uses, and shares customers' personal information. It informs the customer about their rights under the Gramm-Leach-Bliley Act (GLBA) and the institution's practices for protecting their personal information. References:

➤ CompTIA Security+ Certification Exam Objectives - Exam SY0-601

**NEW QUESTION 76**

- (Exam Topic 1)

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

- A. The Cyber Kill Chain
- B. The incident response process
- C. The Diamond Model of Intrusion Analysis
- D. MITRE ATT&CK

**Answer: D**

**Explanation:**

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

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

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

The other options are not correct because:

- A. The Cyber Kill Chain is a model that describes the stages of a cyberattack from reconnaissance to exfiltration. The Cyber Kill Chain does not provide a way to create named groups based on adversary TTPs.
- B. The incident response process is a set of procedures and guidelines that defines how an organization should respond to a security incident. The incident response process does not provide a way to create named groups based on adversary TTPs.
- C. The Diamond Model of Intrusion Analysis is a framework that describes the four core features of any intrusion: adversary, capability, infrastructure, and victim. The Diamond Model of Intrusion Analysis does not provide a way to create named groups based on adversary TTPs.

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

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

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

**NEW QUESTION 81**

- (Exam Topic 1)

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

- A. Unsecured root accounts
- B. Zero day
- C. Shared tenancy
- D. Insider threat

**Answer: C**

**Explanation:**

When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

**NEW QUESTION 85**

- (Exam Topic 1)

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

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer: A**

**Explanation:**

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

**NEW QUESTION 89**

- (Exam Topic 1)

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

- A. The Diamond Model of Intrusion Analysis
- B. CIS Critical Security Controls

- C. NIST Risk Management Framework
- D. ISO 27002

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 90**

- (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 92**

- (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 95**

- (Exam Topic 1)

Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time?

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

**Answer:** A

**Explanation:**

A proof of concept (PoC) environment can be stood up quickly and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time. This environment can utilize either dummy data or actual data. References: CompTIA Security+ Certification Guide, Exam SY0-501

**NEW QUESTION 97**

- (Exam Topic 1)

Which of the following incident response steps occurs before containment?

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

**Answer:** D

**Explanation:**

Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed

by eradication, recovery, and lessons learned.

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

#### NEW QUESTION 99

- (Exam Topic 1)

An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

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

**Answer: C**

#### Explanation:

Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.

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

<https://www.kaspersky.com/resource-center/definitions/what-is-phishing>

#### NEW QUESTION 103

- (Exam Topic 1)

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

To improve security? (Select TWO.)

- A. RADIUS
- B. PEAP
- C. WPS
- D. WEP-EKIP
- E. SSL
- F. WPA2-PSK

**Answer: AF**

#### Explanation:

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

#### NEW QUESTION 107

- (Exam Topic 1)

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

- All users share workstations throughout the day.
- Endpoint protection was disabled on several workstations throughout the network.
- Travel times on logins from the affected users are impossible.
- Sensitive data is being uploaded to external sites.
- All user account passwords were forced to be reset and the issue continued. Which of the following attacks is being used to compromise the user accounts?

- A. Brute-force
- B. Keylogger
- C. Dictionary
- D. Rainbow

**Answer: B**

#### Explanation:

The symptoms suggest a keylogger is being used to compromise the user accounts, allowing the attackers to obtain the users' passwords and other sensitive information. References:

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

#### NEW QUESTION 110

- (Exam Topic 1)

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

```
IPv4 Address ..... 10.0.0.87
Subnet Mask ..... 255.255.255.0
Default Gateway ..... 10.0.0.1
```

Internet Address	Physical Address
10.10.255.255	ff-ff-ff-ff-ff-ff
10.0.0.1	aa-aa-aa-aa-aa-aa
10.0.0.254	aa-aa-aa-aa-aa-aa
224.0.0.2	01-00-5e-00-00-02

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

- A. Denial of service
- B. ARP poisoning
- C. Command injection
- D. MAC flooding

**Answer: B**

**Explanation:**

ARP poisoning (also known as ARP spoofing) is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another host on the network. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 6, page 271.

**NEW QUESTION 115**

- (Exam Topic 1)

A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account 'JHDoe' does not exist...
User account 'VMAdmin' does not exist...
User account 'tomcat' wrong password...
User account 'Admin' does not exist...
```

Which of the following MOST likely would have prevented the attacker from learning the service account name?

- A. Race condition testing
- B. Proper error handling
- C. Forward web server logs to a SIEM
- D. Input sanitization

**Answer: D**

**Explanation:**

Input sanitization can help prevent attackers from learning the service account name by removing potentially harmful characters from user input, reducing the likelihood of successful injection attacks. References:

- > CompTIA Security+ Certification Exam Objectives 2.2: Given a scenario, implement secure coding techniques.
- > CompTIA Security+ Study Guide, Sixth Edition, pages 72-73

**NEW QUESTION 118**

- (Exam Topic 1)

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

- A. Dictionary
- B. Rainbow table
- C. Spraying
- D. Brute-force

**Answer: C**

**Explanation:**

Detailed

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

**NEW QUESTION 121**

- (Exam Topic 1)

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

- A. Implementation of preventive controls
- B. Implementation of detective controls
- C. Implementation of deterrent controls
- D. Implementation of corrective controls



**Answer:** B

**Explanation:**

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

**NEW QUESTION 122**

- (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 126**

- (Exam Topic 1)

Which of the following identifies the point in time when an organization will recover data in the event of an outage?

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

**Answer:** B

**Explanation:**

Detailed  
Recovery Point Objective (RPO) is the maximum duration of time that an organization can tolerate data loss in the event of an outage. It identifies the point in time when data recovery must begin, and any data loss beyond that point is considered unacceptable.

Reference: CompTIA Security+ Certification Guide, Exam SY0-601 by Mike Chapple and David Seidl, Chapter-7: Incident Response and Recovery, Objective 7.2: Compare and contrast business continuity and disaster recovery concepts, pp. 349-350.

**NEW QUESTION 129**

- (Exam Topic 1)

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

- A. Barricades
- B. Thermal sensors
- C. Drones
- D. Signage
- E. Motion sensors
- F. Guards
- G. Bollards

**Answer:** AD

**Explanation:**

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

References:

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

**NEW QUESTION 132**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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



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

#### NEW QUESTION 134

- (Exam Topic 1)

A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted Which of the following resiliency techniques was applied to the network to prevent this attack?

- A. NIC Teaming
- B. Port mirroring
- C. Defense in depth
- D. High availability
- E. Geographic dispersal

**Answer: C**

#### Explanation:

Defense in depth is a resiliency technique that involves implementing multiple layers of security controls to protect against different types of threats. In this scenario, the NIPS likely provided protection at a different layer than the boundary firewall, demonstrating the effectiveness of defense in depth. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

#### NEW QUESTION 138

- (Exam Topic 1)

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices Which of the following is a cost-effective approach to address these concerns?

- A. Enhance resiliency by adding a hardware RAID.
- B. Move data to a tape library and store the tapes off-site
- C. Install a local network-attached storage.
- D. Migrate to a cloud backup solution

**Answer: D**

#### Explanation:

a backup strategy is a plan that defines how to protect data from loss or corruption by creating and storing copies of data on a different medium or location<sup>1</sup>. A backup strategy should consider the security and reliability of the backup data and the backup storage<sup>234</sup>.

Based on these definitions, the best option that is a cost-effective approach to address the security and reliability concerns regarding the on-site backup strategy would be D. Migrate to a cloud backup solution<sup>4</sup>. A cloud backup solution can provide several benefits, such as:

- Enhanced physical security of the backup data by storing it in a remote location that is protected by multiple layers of security measures.
- Enhanced durability of the backup data by storing it on highly reliable storage devices that are replicated across multiple availability zones or regions.
- Reduced costs of backup storage by paying only for the amount of data stored and transferred, and by using features such as compression, deduplication, encryption, and lifecycle management.
- Increased flexibility and scalability of backup storage by choosing from various storage classes and tiers that match the performance and availability requirements of the backup data.

#### NEW QUESTION 141

- (Exam Topic 1)

A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?

- A. TOP
- B. IMAP
- C. HTTPS
- D. S/MIME

**Answer: D**

#### Explanation:

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that enables secure email messages to be sent and received. It provides email encryption, as well as digital signatures, which can be used to verify the authenticity of the sender. S/MIME can be used with a variety of email protocols, including POP and IMAP.

References:

- <https://www.comptia.org/content/guides/what-is-smime>
- CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 139

#### NEW QUESTION 145

- (Exam Topic 1)

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

Which of the following types of attacks has occurred?

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 147**

- (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 152**

- (Exam Topic 1)

The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

- A. HIDS
- B. Allow list
- C. TPM
- D. NGFW

**Answer:** D

**Explanation:**

Next-Generation Firewalls (NGFWs) are designed to provide advanced threat protection by combining traditional firewall capabilities with intrusion prevention, application control, and other security features. NGFWs can detect and block unauthorized access attempts, malware infections, and other suspicious activity. They can also be used to monitor file access and detect unauthorized copying or distribution of copyrighted material.

A next-generation firewall (NGFW) can be used to detect and prevent copyright infringement by analyzing network traffic and blocking unauthorized transfers of copyrighted material. Additionally, NGFWs can be configured to enforce access control policies that prevent unauthorized access to sensitive resources.

References:

➤ CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

**NEW QUESTION 157**

- (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 161**

- (Exam Topic 1)

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

- A. Vulnerabilities with a CVSS score greater than 6.9.
- B. Critical infrastructure vulnerabilities on non-IP protocols.
- C. CVEs related to non-Microsoft systems such as printers and switches.
- D. Missing patches for third-party software on Windows workstations and servers.

**Answer:** D

**Explanation:**

An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

#### NEW QUESTION 166

- (Exam Topic 1)

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

- A. Physically move the PC to a separate Internet point of presence.
- B. Create and apply microsegmentation rules,
- C. Emulate the malware in a heavily monitored DMZ segment
- D. Apply network blacklisting rules for the adversary domain

**Answer: C**

#### Explanation:

Emulating the malware in a heavily monitored DMZ segment is the best option for observing network-based transactions between a callback domain and the malware running on an enterprise PC. This approach provides an isolated environment for the malware to run, reducing the risk of lateral spread and detection by the adversary. Additionally, the DMZ can be monitored closely to gather intelligence on the adversary's tactics and techniques. References: CompTIA Security+ Study Guide, page 129

#### NEW QUESTION 171

- (Exam Topic 1)

An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?

- A. Jamming
- B. Bluesnarfing
- C. Evil twin
- D. Rogue access point

**Answer: B**

#### Explanation:

Bluesnarfing is a hacking technique that exploits Bluetooth connections to snatch data from a wireless device. An attacker can perform bluesnarfing when the Bluetooth function is on and your device is discoverable by other devices within range. In some cases, attackers can even make calls from their victim's phone.

#### NEW QUESTION 176

- (Exam Topic 1)

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

- A. Default system configuration
- B. Unsecure protocols
- C. Lack of vendor support
- D. Weak encryption

**Answer: C**

#### Explanation:

Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 1: Attacks, Threats, and Vulnerabilities

#### NEW QUESTION 177

- (Exam Topic 1)

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

- A. Adding a new UPS dedicated to the rack
- B. Installing a managed PDU
- C. Using only a dual power supplies unit
- D. Increasing power generator capacity

**Answer: B**

#### Explanation:

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

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

#### NEW QUESTION 178

- (Exam Topic 1)

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

- A. Whaling
- B. Spam

- C. Invoice scam
- D. Pharming

**Answer:** A

**Explanation:**

A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

**NEW QUESTION 179**

- (Exam Topic 1)

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

- A. SOAP
- B. SAML
- C. SSO
- D. Kerberos

**Answer:** C

**Explanation:**

Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials. References: CompTIA Security+ Study Guide 601, Chapter 6

**NEW QUESTION 181**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

Infrastructure as a Service (IaaS) providers offer a la carte services, including cloud backups, VM elasticity, and secure networking. With IaaS, businesses can rent infrastructure components such as virtual machines, storage, and networking from a cloud service provider. References: CompTIA Security+ Study Guide, pages 233-234

**NEW QUESTION 185**

- (Exam Topic 1)

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

**Answer:** BF

**Explanation:**

To protect the servers in the company's DMZ from external attack due to the new vulnerability in the SMB protocol on the Windows systems, the security administrator should block TCP ports 139 and 445 for all external inbound connections to the DMZ. SMB uses TCP port 139 and 445. Blocking these ports will prevent external attackers from exploiting the vulnerability in SMB protocol on Windows systems. Blocking TCP ports 139 and 445 for all external inbound connections to the DMZ can help protect the servers, as these ports are used by SMB protocol. Port 135 is also associated with SMB, but it is not commonly used. Ports 143 and 161 are associated with other protocols and services. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.4 Compare and contrast network architecture and technologies.

**NEW QUESTION 188**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

Detailed

Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 10: Managing Identity and Access, p. 465

**NEW QUESTION 189**

- (Exam Topic 1)

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

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

Which of the following options BEST accommodates these requirements?

- A. WPA2-Enterprise
- B. WPA3-PSK
- C. 802.11n
- D. WPS

**Answer:** A

**Explanation:**

Detailed

WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication.

Additionally, WPA2-Enterprise does not allow for open SSIDs.

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

**NEW QUESTION 192**

- (Exam Topic 1)

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

- A. DoS attack
- B. ARP poisoning
- C. DNS spoofing
- D. NXDOMAIN attack

**Answer:** C

**Explanation:**

The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7

**NEW QUESTION 196**

- (Exam Topic 1)

After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

- A. A DMZ
- B. A VPN a
- C. A VLAN
- D. An ACL

**Answer:** D

**Explanation:**

After segmenting the network, a network manager can use an access control list (ACL) to control the traffic between the segments. An ACL is a set of rules that permit or deny traffic based on its characteristics, such as the source and destination IP addresses, protocol type, and port number. References: CompTIA Security+ Certification Guide, Exam SY0-501

**NEW QUESTION 199**

- (Exam Topic 1)

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

- A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
- B. Install a sandbox to run the malicious payload in a safe environment
- C. Perform a traceroute to identify the communication path
- D. Use netstat to check whether communication has been made with a remote host

**Answer:** B

**Explanation:**

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 203

- (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 208

- (Exam Topic 1)

A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
Server: rogue.comptia.com
Address: 172.16.1.250
Non-authoritative answer:
Name: software-solution.com
Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC

```
helpdesk> nslookup software-solution.com
Server: dns.comptia.com
Address: 172.16.1.1
Non-authoritative answer:
Name: software-solution.com
Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

- A. Domain hijacking
- B. DNS poisoning
- C. MAC flooding
- D. Evil twin

**Answer: B**

#### Explanation:

DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, such as an IP address. This results in traffic being diverted to the attacker's computer (or any other malicious destination).

DNS poisoning can be performed by various methods, such as:

- > Intercepting and forging DNS responses from legitimate servers
  - > Compromising DNS servers and altering their records
  - > Exploiting vulnerabilities in DNS protocols or implementations
  - > Sending malicious emails or links that trigger DNS queries with poisoned responses
- According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential

indicators to determine the type of attack:

"DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record."

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://www.cloudflare.com/learning/dns/dns-cache-poisoning/>

### NEW QUESTION 210

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

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

### NEW QUESTION 212

- (Exam Topic 1)

The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL

categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

- A. CASB
- B. Next-generation SWG
- C. NGFW
- D. Web-application firewall

**Answer:** B

**Explanation:**

The solution that the CISO should choose is Next-generation Secure Web Gateway (SWG), which provides URL filtering and categorization to prevent users from accessing malicious sites, even when they are away from the office. NGFWs are typically cloud-based and offer multiple security layers, including malware detection, intrusion prevention, and data loss prevention. References:

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

**NEW QUESTION 216**

- (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 220**

- (Exam Topic 1)

Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

- A. Privileged access management
- B. SSO
- C. RADIUS
- D. Attribute-based access control

**Answer:** A

**Explanation:**

The company is implementing privileged access management, which provides just-in-time permissions for administrative functions.

**NEW QUESTION 224**

- (Exam Topic 1)

During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

- A. User behavior analytics
- B. Dump files
- C. Bandwidth monitors
- D. Protocol analyzer output

**Answer:** A

**Explanation:**

User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 338-341

**NEW QUESTION 225**

- (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 230

- (Exam Topic 1)

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

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

Which of the following should the analyst recommend to disable?

- A. 21/tcp
- B. 22/tcp
- C. 23/tcp
- D. 443/tcp

**Answer: A**

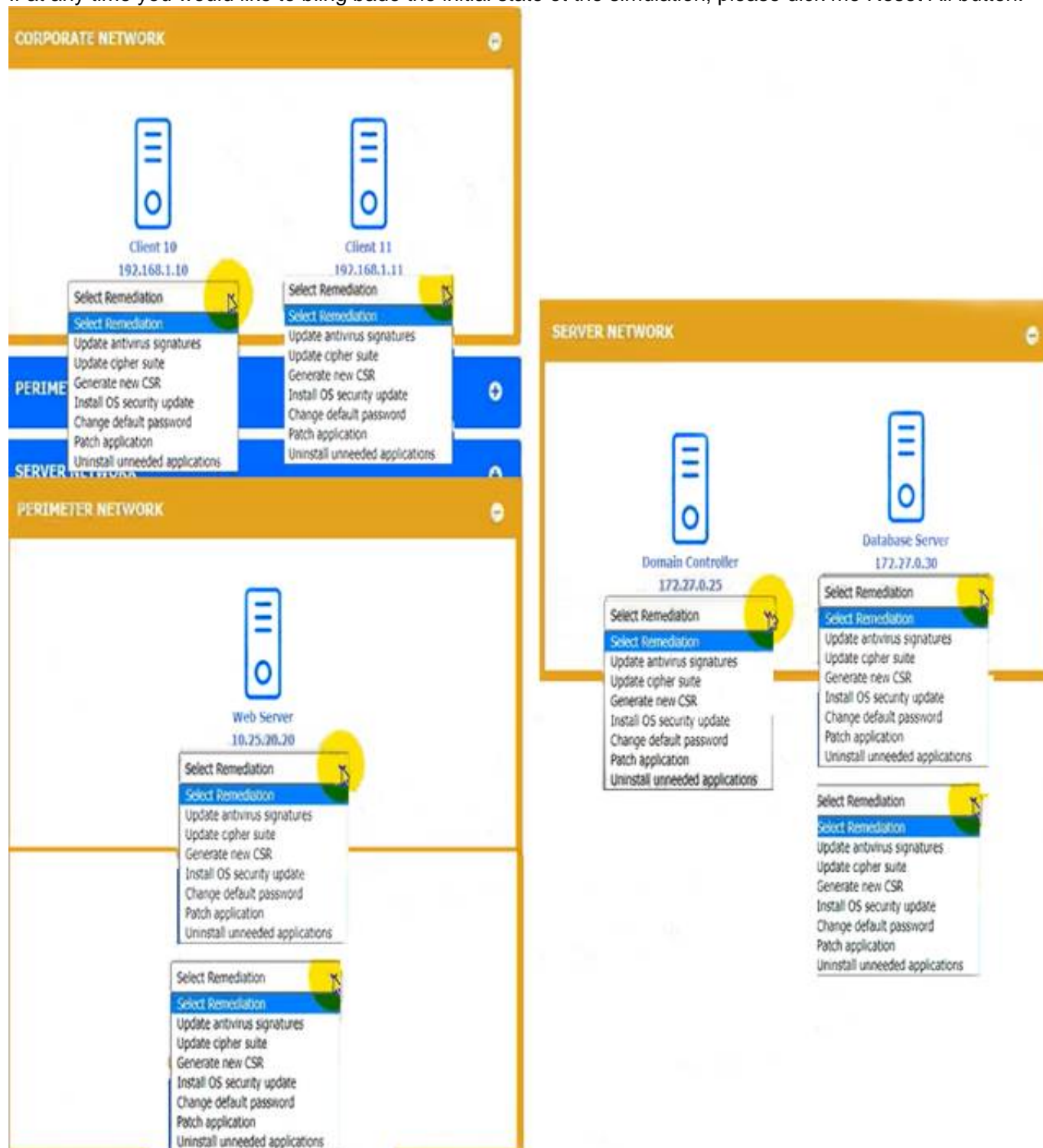
#### NEW QUESTION 231

- (Exam Topic 1)

You received the output of a recent vulnerability assessment.

Review the assessment and scan output and determine the appropriate remediation(s) for each device. Remediation options may be selected multiple times, and some devices may require more than one remediation.

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



The screenshot displays a network simulation interface with three main network segments: Corporate Network, Perimeter Network, and Server Network. Each segment contains several devices with 'Select Remediation' menus open, displaying a list of remediation options.

- Corporate Network:** Contains Client 10 (192.168.1.10) and Client 11 (192.168.1.11). Both have 'Select Remediation' menus open.
- Perimeter Network:** Contains a Web Server (10.25.20.20). It has 'Select Remediation' menus open.
- Server Network:** Contains a Domain Controller (172.27.0.25) and a Database Server (172.27.0.30). Both have 'Select Remediation' menus open.

The 'Select Remediation' menu for each device lists the following options:

- Update antivirus signatures
- Update cipher suite
- Generate new CSR
- Install OS security update
- Change default password
- Patch application
- Uninstall unneeded applications

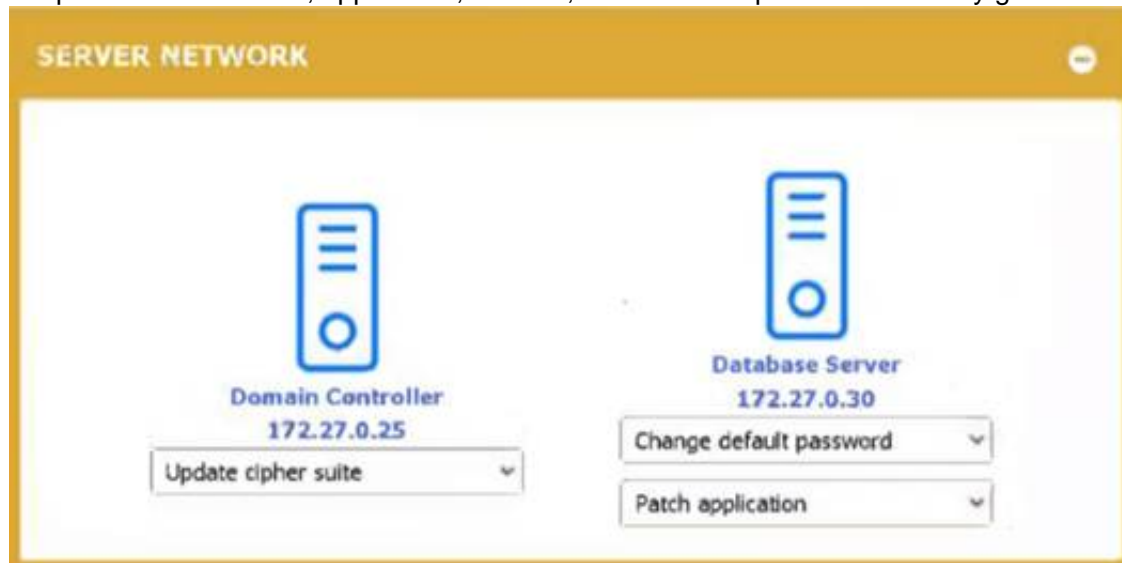
- A. Mastered
- B. Not Mastered

**Answer:** A

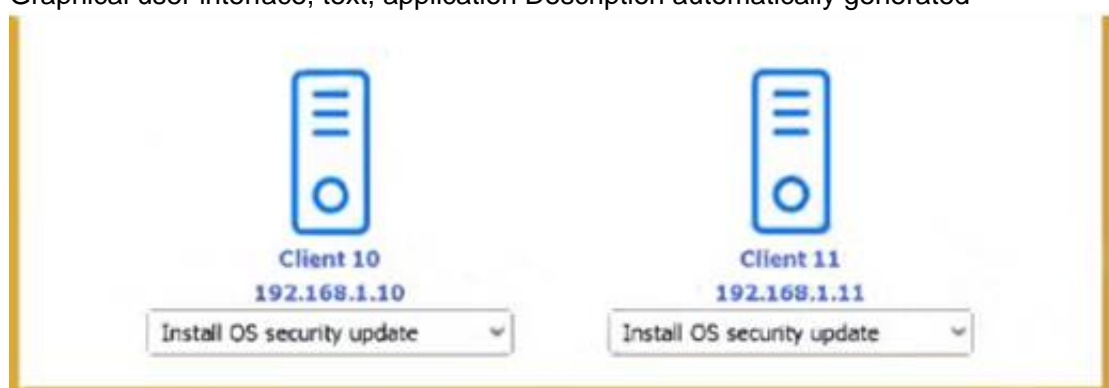
**Explanation:**



Graphical user interface, application, website, Teams Description automatically generated



Graphical user interface, text, application Description automatically generated



#### NEW QUESTION 234

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

References:

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

#### NEW QUESTION 235

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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



#### NEW QUESTION 238

- (Exam Topic 1)

The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

- A. Requiring all new, on-site visitors to configure their devices to use WPS
- B. Implementing a new SSID for every event hosted by the college that has visitors
- C. Creating a unique PSK for every visitor when they arrive at the reception area
- D. Deploying a captive portal to capture visitors' MAC addresses and names

**Answer: D**

#### Explanation:

A captive portal is a web page that requires visitors to authenticate or agree to an acceptable use policy before allowing access to the network. By capturing visitors' MAC addresses and names, potential malicious activity can be traced back to a specific person.

#### NEW QUESTION 239

- (Exam Topic 1)

The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

- A. The NOC team
- B. The vulnerability management team
- C. The CIRT
- D. The read team

**Answer: C**

#### Explanation:

The Computer Incident Response Team (CIRT) is responsible for handling incidents and ensuring that the incident response plan is followed. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

#### NEW QUESTION 241

- (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 245

- (Exam Topic 1)

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

- A. Cryptomalware
- B. Hash substitution
- C. Collision
- D. Phishing

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 249

- (Exam Topic 1)

Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

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

**Answer: D**



**Explanation:**

A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality.

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

**NEW QUESTION 250**

- (Exam Topic 1)

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?

- A. CASB
- B. VPN concentrator
- C. MFA
- D. VPC endpoint

**Answer: A**

**Explanation:**

A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees. References:

CompTIA Security+ SY0-601 Exam Objectives: 3.3 Given a scenario, implement secure mobile solutions.

**NEW QUESTION 253**

- (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 258**

- (Exam Topic 2)

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 259**

- (Exam Topic 2)

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

- A. Firewall
- B. SIEM
- C. IPS
- D. Protocol analyzer

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 260**

- (Exam Topic 2)

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

- A. Blockchain
- B. Salting
- C. Quantum
- D. Digital signature

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 264**

- (Exam Topic 2)

A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

- A. Trusted Platform Module
- B. IaaS
- C. HSMaaS
- D. PaaS

**Answer: C**

**Explanation:**

HSMaaS stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption. HSMaaS allows the organization to use its own keys or generate new ones, and to control and manage them centrally regardless of where the data is stored or processed. HSMaaS also reduces the latency and complexity of managing multiple encryption keys across different cloud providers, as well as the cost and maintenance of deploying physical HSM devices.

\* A. Trusted Platform Module. This is not the correct answer, because a Trusted Platform Module (TPM) is a hardware chip that provides secure storage and generation of cryptographic keys on a device, such as a laptop or a server. A TPM does not offer a cloud-based solution for key management and encryption across multiple cloud providers.

\* B. IaaS. This is not the correct answer, because IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources, such as servers, storage, and networks, over the internet. IaaS does not provide a specific solution for key management and encryption across multiple cloud providers.

\* C. HSMaaS. This is the correct answer, because HSMaaS stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption across multiple cloud providers.

\* D. PaaS. This is not the correct answer, because PaaS stands for Platform as a Service, which is a cloud computing model that provides a platform for developing and deploying applications over the internet. PaaS does not provide a specific solution for key management and encryption across multiple cloud providers.

Reference: HSM as a Service (HSMaaS) | Encryption Consulting, What Is Hardware Security Module (HSM) | Thales.

**NEW QUESTION 266**

- (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 271**

- (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 272**

- (Exam Topic 2)

A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

- A. User training
- B. CAsB
- C. MDM
- D. EDR

**Answer:** C

**Explanation:**

MDM stands for mobile device management, which is a solution that allows organizations to manage and secure mobile devices used by employees. MDM can help prevent data loss and leakage by enforcing policies and restrictions on the devices, such as encryption, password, app installation, remote wipe, and so on. MDM can also monitor and audit the device activity and compliance status. MDM can be the best mitigation strategy to prevent data leakage from an employee's COPE tablet via cloud storage, as it can block or limit the access to cloud services, or apply data protection measures such as containerization or encryption.

References:

- > <https://www.blackberry.com/us/en/solutions/corporate-owned-personally-enabled>
- > <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mobile-device-management/>

**NEW QUESTION 276**

- (Exam Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 279**

- (Exam Topic 2)

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

- A. Sensitive
- B. Non-PII
- C. Private
- D. Confidential

**Answer:** B

**Explanation:**

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

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

**NEW QUESTION 282**

- (Exam Topic 2)

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

- A. Vendor management
- B. Application programming interface
- C. Vanishing
- D. Encryption strength
- E. Firmware

**Answer:** E

**Explanation:**

Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks<sup>1</sup>. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices<sup>1</sup>, or you can use a network monitoring software to keep track of the firmware status of your devices<sup>2</sup>. You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

**NEW QUESTION 283**

- (Exam Topic 2)

Which of the following would be used to find the most common web-application vulnerabilities?

- A. OWASP
- B. MITRE ATT&CK
- C. Cyber Kill Chain
- D. SDLC

**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 publishes a list of the most common web application vulnerabilities, such as injection, broken authentication, cross-site scripting, etc., and provides recommendations and best practices for preventing and mitigating them

**NEW QUESTION 286**

- (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 to 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 290**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 292**

- (Exam Topic 2)

Which Of the following is a primary security concern for a setting up a BYOD program?

- A. End of life
- B. Buffer overflow
- C. VM escape
- D. Jailbreaking

**Answer:** D



**Explanation:**

Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device's operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc

**NEW QUESTION 294**

- (Exam Topic 2)

Recent changes to a company's BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

- A. Facial recognition
- B. Six-digit PIN
- C. PKI certificate
- D. Smart card

**Answer:** A

**Explanation:**

Facial recognition is a type of biometric authentication that uses the unique features of a person's face to verify their identity. Facial recognition is not something you know or have, but something you are, which is one of the three factors of authentication. Facial recognition can use various methods and technologies, such as 2D or 3D images, infrared sensors, machine learning and more, to capture, analyze and compare facial data. Facial recognition can provide a convenient and secure way to authenticate users on personal mobile devices, as it does not require any additional hardware or input from the user. Facial recognition can also be used in conjunction with other factors, such as passwords or tokens, to provide multi-factor authentication. Verified References:

➤ Biometrics - SY0-601 CompTIA Security+ : 2.4 - Professor Messer IT Certification Training Courses <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/biometrics/> (See Facial Recognition)

➤ Security+ (Plus) Certification | CompTIA IT Certifications <https://www.comptia.org/certifications/security> (See Domain 2: Architecture and Design, Objective 2.4: Given a scenario, implement identity and access management controls.)

➤ Biometric and Facial Recognition - CompTIA Security+ Certification (SY0-501) [https://www.oreilly.com/library/view/comptia-security-certification/9781789953091/video9\\_6.html](https://www.oreilly.com/library/view/comptia-security-certification/9781789953091/video9_6.html) (See Biometric and Facial Recognition)

**NEW QUESTION 296**

- (Exam Topic 2)

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

- A. Kerberos
- B. SSL/TLS
- C. IPSec
- D. SSH

**Answer:** C

**Explanation:**

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

**NEW QUESTION 299**

- (Exam Topic 2)

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

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

**Answer:** C

**Explanation:**

IaaS (Infrastructure as a Service) is a cloud model that provides clients with servers, storage, and networks but nothing else. It allows clients to have more control and flexibility over the configuration and management of their infrastructure resources, but also requires them to install and maintain their own operating systems, applications, etc.

**NEW QUESTION 303**

- (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 305

- (Exam Topic 2)

A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to

reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.

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

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

Which of the following is most likely occurring?

- A. Evil twin attack
- B. Domain hijacking attack
- C. On-path attack
- D. MAC flooding attack

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 306

- (Exam Topic 2)

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET
http://yourbank.com/transfer.do?acctnum=08764 6959
&amount=500000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=087646958
&amount=5000000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=-087646958
&amount=1000000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=087646953
&amount=500 HTTP/1.1
```

Which of the following types of attacks is most likely being conducted?

- A. SQLi
- B. CSRF
- C. Spear phishing
- D. API

**Answer: B**

#### Explanation:

CSRF stands for Cross-Site Request Forgery, which is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated<sup>1</sup>. In this case, the attacker may have tricked the user into clicking a malicious link or visiting a malicious website that sends forged requests to the web server of the bank, using the user's session cookie or other credentials. The web server then performs the money transfer requests as if they were initiated by the user, without verifying the origin or validity of the requests.

\* A. SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application's database layer, where malicious SQL statements are inserted into an entry field for execution<sup>2</sup>. The output of the web server log does not show any SQL statements or commands.

\* B. CSRF. This is the correct answer, because CSRF is an attack that exploits the trust a web server has in a user's browser, where malicious requests are sent to the web server using the user's credentials<sup>1</sup>. The output of the web server log shows multiple GET requests with different account numbers and amounts, which may indicate a CSRF attack.

\* C. Spear phishing. This is not the correct answer, because spear phishing is an attack that targets a specific individual or organization with a personalized email

or message that contains a malicious link or attachment<sup>3</sup>. The output of the web server log does not show any email or message content or headers.

\* D. API. This is not the correct answer, because API stands for Application Programming Interface, which is a set of rules and specifications that allow software components to communicate and exchange data. API is not an attack method, but rather a way of designing and developing software applications.

#### NEW QUESTION 310

- (Exam Topic 2)

A web server has been compromised due to a ransomware attack. Further Investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

- A. The last incremental backup that was conducted 72 hours ago
- B. The last known-good configuration stored by the operating system
- C. The last full backup that was conducted seven days ago
- D. The baseline OS configuration

**Answer:** A

#### Explanation:

The last incremental backup that was conducted 72 hours ago would be the best option to restore the services to a secure state, as it would contain the most recent data before the ransomware infection. Incremental backups only store the changes made since the last backup, so they are faster and use less storage space than full backups. Restoring from an incremental backup would also minimize the data loss and downtime caused by the ransomware attack. References:

- <https://www.comptia.org/blog/mature-cybersecurity-response-to-ransomware>
- <https://www.youtube.com/watch?v=HszU4nEAlFc>

#### NEW QUESTION 314

- (Exam Topic 2)

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

- A. Tokenization
- B. Input validation
- C. Code signing
- D. Secure cookies

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 316

- (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 318

- (Exam Topic 2)

A data center has experienced an increase in under-voltage events following electrical grid maintenance outside the facility. These events are leading to occasional losses of system availability. Which of the following would be the most cost-effective solution for the data center to implement?

- A. Uninterruptible power supplies with battery backup
- B. Managed power distribution units to track these events
- C. A generator to ensure consistent, normalized power delivery
- D. Dual power supplies to distribute the load more evenly

**Answer:** A

#### Explanation:

Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes. References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.apc.com/us/en/faqs/FA158852/>

#### NEW QUESTION 322

- (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 326

- (Exam Topic 2)

Which Of the following vulnerabilities is exploited an attacker Overwrite a register with a malicious address that changes the execution path?

- A. VM escape
- B. SQL injection
- C. Buffer overflow
- D. Race condition

**Answer: C**

#### Explanation:

A buffer overflow is a type of vulnerability that occurs when an attacker sends more data than a buffer can

hold, causing the excess data to overwrite adjacent memory locations such as registers. It can allow an attacker to overwrite a register with a malicious address that changes the execution path and executes arbitrary code on the target system

#### NEW QUESTION 329

- (Exam Topic 2)

Which Of the following best ensures minimal downtime for organizations vÃh critical 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 334

- (Exam Topic 2)

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

**Answer: AB**

#### Explanation:

Geolocation and time-of-day restrictions would be best to mitigate the CEO's concerns about staff members working from high-risk countries while on holiday or outsourcing work to a third-party organization in another country. Geolocation is a technique that involves determining the physical location of a device or user based on its IP address, GPS coordinates, Wi-Fi signals, or other indicators. Time-of-day restrictions are policies that limit the access or usage of resources based on the time of day or week. Geolocation and time-of-day restrictions can help to enforce access control rules, prevent unauthorized access, detect anomalous behavior, and comply with regulations. References: <https://www.comptia.org/blog/what-is-geolocation>

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

#### NEW QUESTION 335

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### SY0-701 Practice Exam Features:

- \* SY0-701 Questions and Answers Updated Frequently
- \* SY0-701 Practice Questions Verified by Expert Senior Certified Staff
- \* SY0-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SY0-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SY0-701 Practice Test Here](#)**