

# CompTIA

## Exam Questions SY0-701

CompTIA Security+ Exam



**NEW QUESTION 1**

- (Exam Topic 1)

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

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

**Answer:** DE

**Explanation:**

MDM solutions emerged to solve problems created by BYOD. With MDM, IT teams can remotely wipe devices clean if they are lost or stolen. MDM also makes the life of an IT administrator a lot easier as it allows them to enforce corporate policies, apply software updates, and even ensure that password protection is used on each device. Containerization and application whitelisting are two features of MDM that can help retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.

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

Application whitelisting is a technique that allows only authorized applications to run on the device. This way, IT admins can prevent users from installing or using malicious or unapproved applications that might compromise the security of corporate data. Application whitelisting also allows IT admins to control which applications can access corporate resources, such as email servers or cloud storage.

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

**NEW QUESTION 2**

- (Exam Topic 1)

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

- A. Block cipher
- B. Hashing
- C. Key stretching
- D. Salting

**Answer:** A

**Explanation:**

Single-key or symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.

**NEW QUESTION 3**

- (Exam Topic 1)

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

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 4**

- (Exam Topic 1)

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

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

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 5**

- (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 6**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 7**

- (Exam Topic 1)

A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

- A. Disable Telnet and force SSH.
- B. Establish a continuous ping.
- C. Utilize an agentless monitor
- D. Enable SNMPv3 With passwords.

**Answer:** C

**Explanation:**

An agentless monitor is the best method to monitor network operations because it does not require any software or agents to be installed on the devices being monitored, making it less intrusive and less likely to disrupt network operations. This method can monitor various aspects of network operations, such as traffic, performance, and security.

CompTIA Security+ Study Guide, Sixth Edition (SY0-601), Chapter 4: Attacks, Threats, and Vulnerabilities, Monitoring and Detection Techniques, pg. 167-170.

**NEW QUESTION 8**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data when accessing network shares. References:

➤ CompTIA Security+ Study Guide Exam SY0-601, Chapter 8

**NEW QUESTION 9**

- (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 10**

- (Exam Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 14**

- (Exam Topic 1)

The following are the logs of a successful attack.

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

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

- A. Password history
- B. Account expiration
- C. Password complexity
- D. Account lockout

**Answer: C**

**Explanation:**

To prevent such a breach in the future, the BEST control to use would be Password complexity.

Password complexity is a security measure that requires users to create strong passwords that are difficult to guess or crack. It can help prevent unauthorized access to systems and data by making it more difficult for attackers to guess or crack passwords.

The best control to use to prevent a breach like the one shown in the logs is password complexity. Password complexity requires users to create passwords that are harder to guess, by including a mix of upper and lowercase letters, numbers, and special characters. In the logs, the attacker was able to guess the user's password using a dictionary attack, which means that the password was not complex enough. References:

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

**NEW QUESTION 18**

- (Exam Topic 1)

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

- A. Apply a DLP solution.
- B. Implement network segmentation
- C. Utilize email content filtering,
- D. isolate the infected attachment.

**Answer: B**

**Explanation:**

Network segmentation is the BEST course of action for the analyst to take to prevent further spread of the worm. Network segmentation helps to divide a network into smaller segments, isolating the infected attachment from the rest of the network. This helps to prevent the worm from spreading to other devices within the network. Implementing email content filtering or DLP solution might help in preventing the email from reaching the target or identifying the worm, respectively, but will not stop the spread of the worm. References: CompTIA Security+ Study Guide, Chapter 5: Securing Network Infrastructure, 5.2 Implement Network Segmentation, pp. 286-289

**NEW QUESTION 23**

- (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 27**

- (Exam Topic 1)

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

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

**Answer: A**

**Explanation:**

PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data<sup>1</sup>. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet<sup>1</sup>.

One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for<sup>2</sup>. The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as \*.comptia.org<sup>2</sup>. A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org<sup>2</sup>.



Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used<sup>3</sup>. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years<sup>3</sup>. The validity period can be checked by looking at the valid from and valid to dates on the certificate<sup>3</sup>.

Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. [HTTPS://\\*.comptia.org](https://*.comptia.org), Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (\*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org<sup>2</sup>. It also has a validity period of one year, which means it needs to be rotated annually<sup>3</sup>.

**NEW QUESTION 31**

- (Exam Topic 1)

Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

- A. The key length of the encryption algorithm
- B. The encryption algorithm's longevity
- C. A method of introducing entropy into key calculations
- D. The computational overhead of calculating the encryption key

**Answer:** B

**Explanation:**

When selecting an encryption method for data that needs to remain confidential for a specific length of time, the longevity of the encryption algorithm should be considered to ensure that the data remains secure for the required period. References: CompTIA Security+ Certification Exam Objectives - 3.2 Given a scenario, use appropriate cryptographic methods. Study Guide: Chapter 4, page 131.

**NEW QUESTION 35**

- (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 40**

- (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 42**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

References:

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

#### NEW QUESTION 43

- (Exam Topic 1)

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

- A. Data protection officer
- B. Data owner
- C. Backup administrator
- D. Data custodian
- E. Internal auditor

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 46

- (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 48

- (Exam Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 52

- (Exam Topic 1)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 54

- (Exam Topic 1)

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

- A. A reverse proxy
- B. A decryption certificate
- C. A split-tunnel VPN
- D. Load-balanced servers

**Answer: B**

#### Explanation:

A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting

(XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests. To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

**NEW QUESTION 56**

- (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 59**

- (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 64**

- (Exam Topic 1)

Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

- A. White team
- B. Purple team
- C. Green team
- D. Blue team
- E. Red team

**Answer:** A

**Explanation:**

During a penetration testing exercise, the white team is responsible for acting as a referee and providing oversight and support to ensure that the testing is conducted safely and effectively. They may also be responsible for determining the rules and guidelines of the exercise, monitoring the progress of the teams, and providing feedback and insights on the strengths and weaknesses of the organization's security measures.

**NEW QUESTION 69**

- (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 70**

- (Exam Topic 1)

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

- A. Asymmetric



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

**Answer:** B

**Explanation:**

Symmetric encryption allows data to be encrypted and decrypted using the same key. This is useful when the data needs to be accessed and manipulated while still encrypted. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 6

**NEW QUESTION 72**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 75**

- (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 80**

- (Exam Topic 1)

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

- A. ISO 27701
- B. The Center for Internet Security
- C. SSAE SOC 2
- D. NIST Risk Management Framework

**Answer:** B

**Explanation:**

The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. References:

- CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.
- CompTIA Security+ Study Guide, Sixth Edition, pages 15-16

**NEW QUESTION 82**

- (Exam Topic 1)

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

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

**Answer:** B

**Explanation:**

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

a full backup as it only stores the changes made from the last full backup.

**NEW QUESTION 85**

- (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 87**

- (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 89**

- (Exam Topic 1)

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

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

**Answer:** D

**Explanation:**

The environment that utilizes dummy data and is most likely to be installed locally on a system that allows it to be assessed directly and modified easily with each build is the development environment. The development environment is used for developing and testing software and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy data can be used in the development environment to simulate real-world scenarios and test the software's functionality. References: <https://www.techopedia.com/definition/27561/development-environment>

**NEW QUESTION 92**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 97**

- (Exam Topic 1)

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

- A. The Diamond Model of Intrusion Analysis
- B. The Cyber Kill Chain
- C. The MITRE CVE database
- D. The incident response process

**Answer:** A

**Explanation:**

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

**NEW QUESTION 98**

- (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 101**

- (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 106**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 111**

- (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)

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 119**

- (Exam Topic 1)

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

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

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

- A. XS
- B. Implement a SIEM

- C. CSR
- D. implement an IPS
- E. Directory traversal implement a WAF
- F. SQL infection, mplement an IDS

**Answer:** C

**Explanation:**

Detailed

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

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

**NEW QUESTION 122**

- (Exam Topic 1)

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

- A. Preventive
- B. Compensating
- C. Corrective
- D. Detective

**Answer:** D

**Explanation:**

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

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

**NEW QUESTION 123**

- (Exam Topic 1)

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

- A. It allows for the sharing of digital forensics data across organizations
- B. It provides insurance in case of a data breach
- C. It provides complimentary training and certification resources to IT security staff.
- D. It certifies the organization can work with foreign entities that require a security clearance
- E. It assures customers that the organization meets security standards

**Answer:** E

**Explanation:**

ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). It provides a framework for managing and protecting sensitive information using risk management processes. Acquiring an ISO 27001 certification assures customers that the organization meets security standards and follows best practices for information security management. It helps to build customer trust and confidence in the organization's ability to protect their sensitive information. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware, p. 7

**NEW QUESTION 125**

- (Exam Topic 1)

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

Name	CPU %	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?

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

**Answer:** C

**Explanation:**

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

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

**NEW QUESTION 127**

- (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>2n4</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 132**

- (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 133**

- (Exam Topic 1)

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

- A. MAC filtering
- B. Zero trust segmentation
- C. Network access control
- D. Access control vestibules
- E. Guards
- F. Bollards

**Answer:** CE

**Explanation:**

Network access control (NAC) is a technique that restricts access to a network based on the identity, role, device, location, or other criteria of the users or devices. NAC can prevent unauthorized or malicious devices from connecting to a network and accessing sensitive data or resources.

Guards are physical security personnel who monitor and control access to a facility. Guards can prevent unauthorized or malicious individuals from entering a facility and plugging in a remotely accessible device.

**NEW QUESTION 137**

- (Exam Topic 1)

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

**Answer:** DE

**Explanation:**

The most likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases are included third-party libraries and vendors/supply chain. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Supply Chain and Software Development Life Cycle

#### NEW QUESTION 142

- (Exam Topic 1)

A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of the following should the manager request to complete the assessment?

- A. A service-level agreement
- B. A business partnership agreement
- C. A SOC 2 Type 2 report
- D. A memorandum of understanding

**Answer: C**

#### Explanation:

SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.

A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.

The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 5

#### NEW QUESTION 144

- (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 149

- (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 151

- (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 155

- (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 160

- (Exam Topic 1)

Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

- A. RTO
- B. MTBF
- C. MTTR
- D. RPO

**Answer: C**

#### Explanation:

Mean Time To Repair (MTTR) is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment. References: CompTIA Security+ Certification Exam Objectives 4.6 Explain the importance of secure coding practices. Study Guide: Chapter 7, page 323.

#### NEW QUESTION 161

- (Exam Topic 1)

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

- A. Disconnect all external network connections from the firewall
- B. Send response teams to the network switch locations to perform updates
- C. Turn on all the network switches by using the centralized management software
- D. Initiate the organization's incident response plan.

**Answer: D**

#### Explanation:

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

If the help desk has received calls from users in multiple locations who are unable to access core network services, it could indicate that a network outage or a denial-of-service attack has occurred. The network team has identified and turned off the network switches using remote commands, which could be a containment measure to isolate the affected devices and prevent further damage.

The next action that the network team should take is to initiate the organization's incident response plan, which would involve notifying the appropriate stakeholders, such as management, security team, legal team, etc., and following the predefined steps to investigate, analyze, document, and resolve the incident. The other options are not correct because:

- A. Disconnect all external network connections from the firewall. This could be another containment measure to prevent external attackers from accessing the network, but it would also disrupt legitimate network traffic and services. This action should be taken only if it is part of the incident response plan and after notifying the relevant parties.
- B. Send response teams to the network switch locations to perform updates. This could be a recovery measure to restore normal network operations and apply patches or updates to prevent future incidents, but it should be done only after the incident has been properly identified, contained, and eradicated.
- C. Turn on all the network switches by using the centralized management software. This could be a recovery measure to restore normal network operations, but it should be done only after the incident has been properly identified, contained, and eradicated.

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

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

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

#### NEW QUESTION 164

- (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:

One of the risks of using legacy software is the lack of vendor support. This means that the vendor may no longer provide security patches, software updates, or technical support for the software. This leaves the software vulnerable to new security threats and vulnerabilities that could be exploited by attackers.

**NEW QUESTION 168**

- (Exam Topic 1)

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

- A. Cellular
- B. NFC
- C. Wi-Fi
- D. Bluetooth

**Answer: B**

**Explanation:**

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

**NEW QUESTION 172**

- (Exam Topic 1)

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

- A. IoT sensor
- B. Evil twin
- C. Rogue access point
- D. On-path attack

**Answer: C**

**Explanation:**

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

**NEW QUESTION 176**

- (Exam Topic 1)

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

- A. OpenID is mandatory to make the MFA requirements work
- B. An incorrect browser has been detected by the SAML application
- C. The access device has a trusted certificate installed that is overwriting the session token
- D. The user's IP address is changing between logins, but the application is not invalidating the token

**Answer: D**

**NEW QUESTION 181**

- (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 the 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 the 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 184**

- (Exam Topic 1)

Which of the following involves the inclusion of code in the main codebase as soon as it is written?

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



**Answer:** D

**Explanation:**

Detailed

Continuous Integration (CI) is a practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration is verified by an automated build and automated tests. CI allows for the detection of errors early in the development cycle, thereby reducing overall development costs.

**NEW QUESTION 185**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

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

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

The other options are not correct because:

- A. Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.
- B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.
- D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.

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

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

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

<https://gdpr-info.eu/issues/data-protection-officer/>

**NEW QUESTION 189**

- (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 194**

- (Exam Topic 1)

Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?

- A. Phishing
- B. Vishing
- C. Smishing
- D. Spam

**Answer:** C

**Explanation:**

Smishing is a type of phishing attack which begins with an attacker sending a text message to an individual. The message contains social engineering tactics to convince the person to click on a malicious link or send sensitive information to the attacker. Criminals use smishing attacks for purposes like:

Learn login credentials to accounts via credential phishing Discover private data like social security numbers

Send money to the attacker Install malware on a phone

Establish trust before using other forms of contact like phone calls or emails

Attackers may pose as trusted sources like a government organization, a person you know, or your bank. And messages often come with manufactured urgency and time-sensitive threats. This can make it more difficult for a victim to notice a scam.

Phone numbers are easy to spoof with VoIP texting, where users can create a virtual number to send and receive texts. If a certain phone number is flagged for spam, criminals can simply recycle it and use a new one.

**NEW QUESTION 198**



- (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 201**

- (Exam Topic 1)

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

- A. Identity processor
- B. Service requestor
- C. Identity provider
- D. Service provider
- E. Tokenized resource
- F. Notarized referral

**Answer: CD**

**Explanation:**

An identity provider (IdP) is responsible for authenticating users and generating security tokens containing user information. A service provider (SP) is responsible for accepting security tokens and granting access to resources based on the user's identity.

**NEW QUESTION 206**

- (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 207**

- (Exam Topic 1)

The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

- A. Authentication protocol
- B. Encryption type
- C. WAP placement
- D. VPN configuration

**Answer: C**

**Explanation:**

WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.

WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:

- Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
- Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
- Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

#### NEW QUESTION 211

- (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 216

- (Exam Topic 1)

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

**Answer:** A

#### Explanation:

The Service Level Agreement (SLA) is a contract between the cloud service provider and the organization that stipulates the exact requirements for the cloud provider. It outlines the level of service that the provider must deliver, including the minimum uptime percentage, support response times, and the remedies and penalties for failing to meet the agreed-upon service levels.

#### NEW QUESTION 220

- (Exam Topic 1)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 222

- (Exam Topic 1)

An employee's company account was used in a data breach Interviews with the employee revealed:

- The employee was able to avoid changing passwords by using a previous password again.
- The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccurring? (Select TWO)

- A. Geographic dispersal
- B. Password complexity
- C. Password history
- D. Geotagging
- E. Password lockout
- F. Geofencing

**Answer:** CF

#### Explanation:

two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofencing. Password history is a feature that prevents users from reusing their previous passwords. This can enhance password security by forcing users to create new and unique passwords periodically. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords.

Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device. This can enhance security by preventing unauthorized access from hostile or foreign regions. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries.

#### NEW QUESTION 224

- (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 225**

- (Exam Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 229**

- (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 231**

- (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 236**

- (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 239**

- (Exam Topic 2)

Which of the following can reduce vulnerabilities by avoiding code reuse?

- A. Memory management
- B. Stored procedures
- C. Normalization
- D. Code obfuscation

**Answer:** A

**Explanation:**

Memory management is a technique that can allocate and deallocate memory for applications and processes. Memory management can reduce vulnerabilities by avoiding code reuse, which is a technique that exploits a memory corruption vulnerability to execute malicious code that already exists in memory. Memory management can prevent code reuse by implementing features such as address space layout randomization (ASLR), data execution prevention (DEP), or stack canaries.

**NEW QUESTION 242**

- (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 244**

- (Exam Topic 2)

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

- A. Walk-throughs
- B. Lessons learned
- C. Attack framework alignment
- D. Containment

**Answer:** B

**Explanation:**

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

**NEW QUESTION 247**

- (Exam Topic 2)

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

- A. Apply a DLP solution.
- B. Implement network segmentation.
- C. Utilize email content filtering.
- D. Isolate the infected attachment.

**Answer:** D

**Explanation:**

Isolating the infected attachment is the best course of action for the analyst to take to prevent further spread of the worm. A worm is a type of malware that can self-replicate and infect other devices without human interaction. By isolating the infected attachment, the analyst can prevent the worm from spreading to other

devices or networks via email, file-sharing, or other means. Isolating the infected attachment can also help the analyst to analyze the worm and determine its source, behavior, and impact. References:

- > <https://www.security.org/antivirus/computer-worm/>
- > [https://sec.cloudapps.cisco.com/security/center/resources/worm\\_mitigation\\_whitepaper.html](https://sec.cloudapps.cisco.com/security/center/resources/worm_mitigation_whitepaper.html)

**NEW QUESTION 249**

- (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 252**

- (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 253**

- (Exam Topic 2)

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

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

**Answer: B**

**Explanation:**

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

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

**NEW QUESTION 258**

- (Exam Topic 2)

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

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

**Answer: D**

**Explanation:**

Isolating the device is the first thing that a security analyst should do if they suspect that a user's device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating



the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.  
References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>  
<https://resources.infosecinstitute.com/topic/incident-response-process/>

#### NEW QUESTION 262

- (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 266

- (Exam Topic 2)

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

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

**Answer:** C

#### Explanation:

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

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

#### NEW QUESTION 270

- (Exam Topic 2)

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

- A. MAC filtering
- B. Zero trust segmentation
- C. Network access control
- D. Access control vestibules
- E. Guards
- F. Bollards.

**Answer:** AC

#### Explanation:

MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.

Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

#### NEW QUESTION 273

- (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 276**

- (Exam Topic 2)

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 277**

- (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 280**

- (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 285**

- (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 290**

- (Exam Topic 2)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 292**

- (Exam Topic 2)

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

- A. Directory traversal
- B. SQL injection
- C. Privilege escalation
- D. Cross-site scripting

**Answer:** B

**Explanation:**

SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the database behind the application. SQL injection can be used to perform various actions, such as reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement "SELECT \* FROM customername" to retrieve all data from the customername table in the database.

**NEW QUESTION 297**

- (Exam Topic 2)

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the 'company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

- A. Federation
- B. Identity proofing
- C. Password complexity
- D. Default password changes
- E. Password manager
- F. Open authentication

**Answer:** AF

**Explanation:**

Federation is an access management concept that allows users to authenticate once and access multiple applications or services that trust the same identity provider. Open authentication is a standard protocol that enables federation by allowing users to use their existing credentials from one service to access another service. The company is most likely using federation and open authentication to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account. For example, the company could use an identity provider such as Azure AD or Keycloak to manage the user identities and credentials for the intranet account, and then use open authentication to allow the users to access other company-owned websites without having to log in again. References:

- > <https://www.keycloak.org/>
- > <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-fed>

**NEW QUESTION 299**

- (Exam Topic 2)

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

- A. The business continuity plan
- B. The risk management plan
- C. The communication plan
- D. The incident response plan

**Answer:** A

**Explanation:**

A business continuity plan is a document or a process that outlines how an organization can continue its critical operations and functions in the event of a disruption or disaster. It can include strategies and procedures for recovering or relocating resources, personnel, data, etc., to ensure minimal downtime and impact. The organization will most likely consult the business continuity plan when setting up offices in a temporary work space after its corporate offices were destroyed due to a natural disaster.

**NEW QUESTION 303**

- (Exam Topic 2)

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

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

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

**Answer:** A

**Explanation:**

SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider<sup>1</sup>

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

**NEW QUESTION 305**

- (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 309**

- (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 312**

- (Exam Topic 2)

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate data center that houses confidential information. There is a firewall at the internet border, followed by a DLP appliance, the VPN server and the data center itself. Which of the following is the weakest design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance.
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
- D. Adding two hops in the VPN tunnel may slow down remote connections

**Answer:** C



**Explanation:**

VPN (Virtual Private Network) traffic is encrypted to protect its confidentiality and integrity over the internet. However, this also means that it cannot be inspected by security devices or tools when entering or leaving the network, unless it is decrypted first. This can create a blind spot or a vulnerability for the network security posture, as malicious traffic or data could bypass detection or prevention mechanisms by using VPN encryption

**NEW QUESTION 316**

- (Exam Topic 2)

A security team is providing input on the design of a secondary data center that has Which of the following should the security team recommend? (Select two).

- A. Configuring replication of the web servers at the primary site to offline storage
- B. Constructing the secondary site in a geographically disperse location
- C. Deploying load balancers at the primary site
- D. Installing generators
- E. Using differential backups at the secondary site
- F. Implementing hot and cold aisles at the secondary site

**Answer:** BD

**Explanation:**

\* B. Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience. References: 1

CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1 : Explain the importance of secure staging deployment concepts 2

CompTIA Security+ Certification Exam

Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 3

CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

**NEW QUESTION 320**

- (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 322**

- (Exam Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 324**

- (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 327**

- (Exam Topic 2)

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

- A. Accept
- B. Transfer
- C. Mitigate
- D. Avoid

**Answer: B**

**Explanation:**

A company purchased cyber insurance to address items listed on the risk register. This represents a transfer strategy. A transfer strategy involves transferring or sharing some or all of the responsibility or impact of a risk to another party, such as an insurer, a supplier, or a partner. A transfer strategy can help to reduce the financial liability or exposure of the company in case of a security incident or breach. References: <https://www.comptia.org/blog/what-is-cyber-insurance>  
<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

**NEW QUESTION 330**

- (Exam Topic 2)

A security analyst is creating baselines for the server team to follow when hardening new devices for deployment. Which of the following best describes what the analyst is creating?

- A. Change management procedure
- B. Information security policy
- C. Cybersecurity framework
- D. Secure configuration guide

**Answer: D**

**Explanation:**

A secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies. A security analyst can create baselines for the server team to follow when hardening new devices for deployment based on a secure configuration guide.

\* A. Change management procedure. This is not the correct answer, because a change management procedure is a document that describes the steps and processes for implementing, reviewing, and approving changes to an IT system or environment. A change management procedure helps to minimize the risks and impacts of changes on the system performance, availability, and security.

\* B. Information security policy. This is not the correct answer, because an information security policy is a document that defines the rules and principles for protecting the confidentiality, integrity, and availability of information assets within an organization. An information security policy helps to establish the roles and responsibilities of employees, managers, and stakeholders regarding information security.

\* C. Cybersecurity framework. This is not the correct answer, because a cybersecurity framework is a document that provides a set of standards, guidelines, and best practices for managing cybersecurity risks and improving resilience. A cybersecurity framework helps to align the business objectives and priorities with the security requirements and capabilities.

\* D. Secure configuration guide. This is the correct answer, because a secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies.

Reference: Secure Configuration Guide, Security Technical Implementation Guide - Wikipedia.

**NEW QUESTION 331**

- (Exam Topic 2)

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

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

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

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

**Answer: B**

**Explanation:**

A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (\*) as a placeholder for any subdomain name. For example, \*.company.com can secure www.company.com, contact.us.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

**NEW QUESTION 332**

- (Exam Topic 2)

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

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

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

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

**Answer: C**

**Explanation:**

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

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

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

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

**NEW QUESTION 337**

- (Exam Topic 2)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 338**

- (Exam Topic 2)

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
```

Which of the following password attacks is taking place?

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

**Answer: D**

**Explanation:**

Spraying is a password attack that involves trying a few common passwords against a large number of usernames. Spraying is different from brute-force attacks, which try many possible passwords against one username, or dictionary attacks, which try a list of words from a dictionary file against one username. Spraying is often used when the web application has a lockout policy that prevents multiple failed login attempts for the same username. Spraying can be detected by looking for patterns of failed login attempts from the same source IP address with different usernames and the same or similar passwords.

**NEW QUESTION 342**

.....

## 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](#)**