

Exam Questions SY0-701

CompTIA Security+ Exam

<https://www.2passeasy.com/dumps/SY0-701/>



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

> [CompTIA Security+ Study Guide Exam SY0-601, Chapter 4](#)

NEW QUESTION 2

- (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 3

- (Exam Topic 1)

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

- * www.companysite.com
- * shop.companysite.com
- * about-us.companysite.com
- * contact-us.companysite.com
- * secure-logon.companysite.com

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 4

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?

- A. Functional testing
- B. Stored procedures
- C. Elasticity
- D. Continuous integration

Answer: D

Explanation:

Continuous integration is a software development practice where developers merge their code into a shared repository several times a day, and the code is tested automatically. This ensures that code changes are tested and integrated continuously, reducing the risk of errors and conflicts.

NEW QUESTION 7

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: DF

Explanation:

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

NEW QUESTION 9

- (Exam Topic 1)

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

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

Which of the following BEST explains this type of attack?

- A. DLL injection to hijack administrator services
- B. SQLi on the field to bypass authentication

- C. Execution of a stored XSS on the website
- D. Code to execute a race condition on the server

Answer: B

Explanation:

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

NEW QUESTION 10

- (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 10

- (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 12

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 14

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid-state drives and have reached their end-of-life¹. Shredding reduces electronic devices to pieces no larger than 2 millimeters². Therefore, shredding is the most secure but least expensive data destruction method for data that is stored on hard drives.

NEW QUESTION 15

- (Exam Topic 1)

Which of the following 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 20

- (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 24

- (Exam Topic 1)

Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?

- A. Intelligence fusion
- B. Review reports
- C. Log reviews
- D. Threat feeds

Answer: A

Explanation:

Intelligence fusion is a process that involves aggregating and analyzing data from multiple sources, including artificial intelligence, to provide insight on current cyberintrusions, phishing, and other malicious cyberactivity.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Glossary, p. 767.

NEW QUESTION 29

- (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 33

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

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

The other options are not correct because:

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

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

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

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

NEW QUESTION 36

- (Exam Topic 1)

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

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

Answer: AF

Explanation:

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

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

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

NEW QUESTION 40

- (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 42

- (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 46

- (Exam Topic 1)

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security control standards. Which of the following is the MOST likely source of the breach?

- A. Side channel
- B. Supply chain
- C. Cryptographic downgrade
- D. Malware

Answer: B

Explanation:

A supply chain attack occurs when a third-party supplier or business partner is compromised, leading to an attacker gaining unauthorized access to the targeted organization's network. In this scenario, the dedicated business partner connection to a vendor was used to exfiltrate customer credit card data, indicating that the vendor's network was breached and used as a supply chain attack vector.

NEW QUESTION 50

- (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 55

- (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 59

- (Exam Topic 1)

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

Answer: BC

Explanation:

Non-repudiation is the ability to ensure that a party cannot deny a previous action or event. Cryptographic concepts that can be used to implement non-repudiation include hashing and digital signatures, which use a private key to sign a message and ensure that the signature is unique to the signer. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 63

- (Exam Topic 1)

A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

- A. BYOD
- B. VDI
- C. COPE
- D. CYOD

Answer: D

Explanation:

Choose Your Own Device (CYOD) is a deployment model that allows employees to select from a predefined list of devices. It provides employees with flexibility in device preference while allowing the company to maintain control and security over company data and infrastructure. CYOD deployment model provides a compromise between the strict control provided by Corporate-Owned, Personally Enabled (COPE) deployment model and the flexibility provided by Bring Your Own Device (BYOD) deployment model. References: CompTIA Security+ Study Guide, Chapter 6: Securing Application, Data, and Host Security, 6.5 Implement Mobile Device Management, pp. 334-335

NEW QUESTION 66

- (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 location¹. A backup strategy should consider the security and reliability of the backup data and the backup storage²³⁴.

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 solution²ⁿ⁴. 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 69

- (Exam Topic 1)

While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches. Which of the following is the security analyst MOST likely observing?

- A. SNMP traps
- B. A Telnet session
- C. An SSH connection
- D. SFTP traffic

Answer: B

Explanation:

The security analyst is likely observing a Telnet session, as Telnet transmits data in plain text format, including usernames and passwords. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware.

NEW QUESTION 74

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

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

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

NEW QUESTION 79

- (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 80

- (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 83

- (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 88

- (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 92

- (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 VPB, 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 93

- (Exam Topic 1)

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

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

Answer: BF

Explanation:

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

NEW QUESTION 94

- (Exam Topic 1)

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

- A. Shadow IT
- B. Credential stuffing
- C. SQL injection
- D. Man in the browser
- E. Bluejacking

Answer: A

Explanation:

The most likely cause of the enterprise data being compromised from a local database is Shadow IT. Shadow IT is the use of unauthorized applications or devices by employees to access company resources. In this case, the sales director's laptop was stolen, and the attacker was able to use it to access the local database, which was not secured properly, allowing unauthorized access to sensitive data. References:

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

NEW QUESTION 99

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 103

- (Exam Topic 1)

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

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

Which of the following options BEST accommodates these requirements?

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

Answer: A

Explanation:

Detailed

WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication. Additionally, WPA2-Enterprise does not allow for open SSIDs.

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

NEW QUESTION 107

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 108

- (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 110

- (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 113

- (Exam Topic 1)

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

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

Answer: A

Explanation:

A bollard would work best to prevent individuals from driving a car into the building. A bollard is a short, vertical post that can be used to block vehicles from entering a designated area. It is specifically designed to stop cars from crashing into buildings or other structures.

NEW QUESTION 115

- (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 117

- (Exam Topic 1)

A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

Internet address	Physical address	Type
192.168.1.1	ff-ec-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0c-29-1a-e7-fa	dynamic
192.168.1.10	fc-41-5e-48-00-ff	dynamic
224.215.54.47	fc-00-5e-48-00-fb	static

Which of the following BEST describes the attack the company is experiencing?

- A. MAC flooding
- B. URL redirection
- C. ARP poisoning
- D. DNS hijacking

Answer: C

Explanation:

The output of the "netstat -ano" command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.

The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client's browser.

Based on the output of the "netstat -ano" command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.

ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

NEW QUESTION 121

- (Exam Topic 1)

one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

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

Answer: D

Explanation:

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

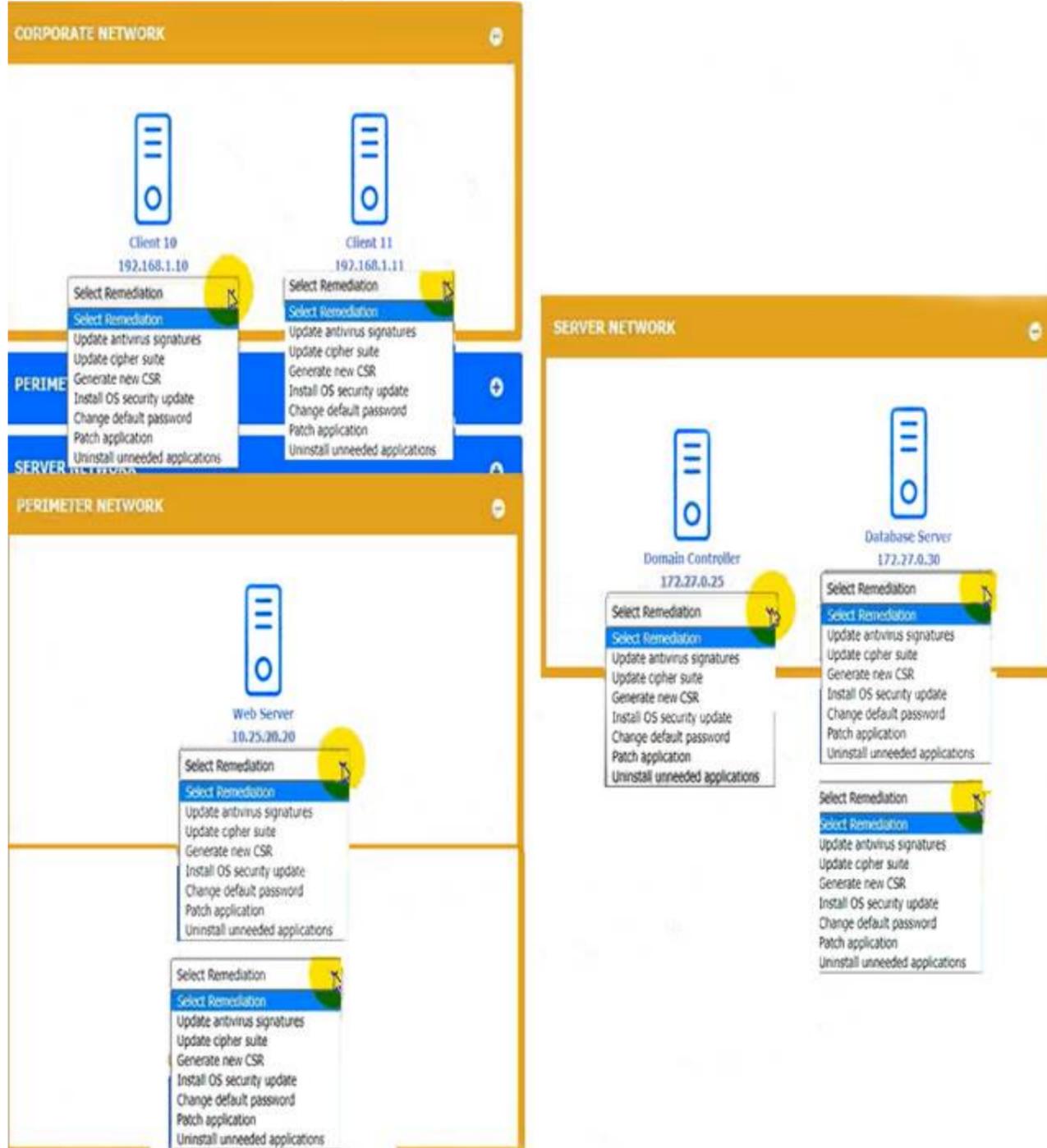
NEW QUESTION 126

- (Exam Topic 1)

You received the output of a recent vulnerability assessment.

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

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



- A. Mastered
- B. Not Mastered

Answer: A

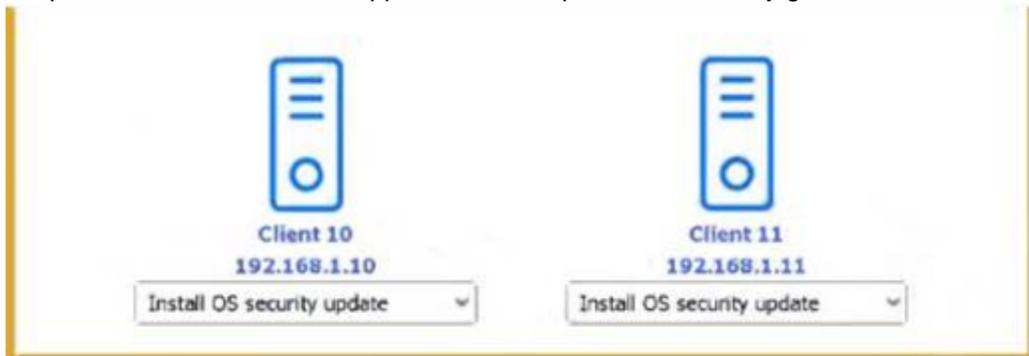
Explanation:



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



Graphical user interface, text, application Description automatically generated



NEW QUESTION 130

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 131

- (Exam Topic 1)

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

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

Answer: D

Explanation:

A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 136

- (Exam Topic 1)

An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

- A. White-box
- B. Red-learn
- C. Bug bounty
- D. Gray-box
- E. Black-box

Answer: C

Explanation:

Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network

or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

NEW QUESTION 141

- (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 145

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 150

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

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

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

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

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

NEW QUESTION 155

- (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

NEW QUESTION 160

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 164

- (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 168

- (Exam Topic 2)

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following best describes these systems?

- A. DNS sinkholes
- B. Honey pots
- C. Virtual machines
- D. Neural networks

Answer: B

Explanation:

Honey pots are decoy systems or resources that are designed to attract and deceive threat actors and to learn more about their motives, techniques, etc. They can be deployed alongside production systems to create an illusion of a vulnerable target and divert attacks away from the real systems. They can also collect valuable information and evidence about the attackers and their activities for further analysis or prosecution.

NEW QUESTION 169

- (Exam Topic 2)

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

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

Answer: E

Explanation:

Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks¹. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices¹, or you can use a network monitoring software to keep track of the firmware status of your devices². You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

NEW QUESTION 170

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

NEW QUESTION 175

- (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 177

- (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 180

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Invest in secure coding training and application security guidelines is the most effective approach for the manager to use to address the issue of common vulnerabilities in the applications developed by the team. Secure coding training can help the developers learn how to write code that follows security best practices and avoids common mistakes or flaws that can introduce vulnerabilities. Application security guidelines can provide a set of standards and rules for developing secure applications that meet the company's security requirements and policies. By investing in secure coding training and application security guidelines, the manager can improve the security awareness and skills of the development team and reduce the number of vulnerabilities in their applications. References: 1

CompTIA Security+ Certification Exam Objectives, page 9,

Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0:

Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3 <https://www.comptia.org/blog/what-is-secure-coding>

NEW QUESTION 182

- (Exam Topic 2)

Which of the following would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations?

- A. Machine learning
- B. DNS sinkhole
- C. Blocklist
- D. Honey pot

Answer: B

Explanation:

A DNS sinkhole would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations. A DNS sinkhole is a technique that involves redirecting malicious or unwanted domain names to an alternative IP address, such as a black hole, a honeypot, or a warning page. A DNS sinkhole can help to prevent or disrupt the communication between infected systems and command-and-control servers, malware distribution sites, phishing sites, or botnets. A DNS sinkhole can also help to identify and isolate infected systems by monitoring the traffic to the sinkhole IP address. References:

<https://www.comptia.org/blog/what-is-a-dns-sinkhole>

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

NEW QUESTION 184

- (Exam Topic 2)

A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

- A. pcap reassembly
- B. SSD snapshot
- C. Image volatile memory
- D. Extract from checksums

Answer: C

Explanation:

The best technique for the digital forensics team to use to obtain a sample of the malware binary is to image volatile memory. Volatile memory imaging is a process of collecting a snapshot of the contents of a computer's RAM, which can include active malware programs. According to the CompTIA Security+ SY0-601 Official Text Book, volatile memory imaging can be used to capture active malware programs that are running in memory, but have not yet been committed to disk. This technique is especially useful in cases where the malware is designed to self-destruct or erase itself from the disk after execution.

NEW QUESTION 188

- (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 191

- (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 194

- (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 195

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

References: 1

CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation, Objective 3.2: Implement secure protocols 2

CompTIA Security+ Certification Exam Objectives, page 15,

Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms 3

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731>

NEW QUESTION 196

- (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 199

- (Exam Topic 2)

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

- A. MFA
- B. Lockout
- C. Time-based logins
- D. Password history

Answer: A

Explanation:

MFA stands for multi-factor authentication, which is a method of verifying a user's identity using two or more factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident. References:

- > <https://www.comptia.org/certifications/security>
- > <https://www.youtube.com/watch?v=yCJyPPvM-xg>
- > <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/>

NEW QUESTION 202

- (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 205

- (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 210

- (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 213

- (Exam Topic 2)

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

Which of the following occurred?

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

Answer: C

Explanation:

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

NEW QUESTION 218

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 220

- (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 225

- (Exam Topic 2)

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

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

Answer: B

Explanation:

SSH is used to securely transfer files to the remote server and is required for SCP to work. Disabling SSH will prevent users from being able to use SCP to transfer files to the server. To enable SSH, the security engineer should modify the SSH configuration file (sshd.conf) and make sure that SSH is enabled. For more information on hardening systems and the security techniques that can be used, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 229

- (Exam Topic 2)

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

- Minimal interruption to the end user
- Mutual certificate validation

Which of the following authentication protocols would meet these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 233

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 235

- (Exam Topic 2)

A security administrator examines the ARP table of an access switch and sees the following output:

VLAN	MAC Address	Type	Ports
All	012b1283f77b	STATIC	CPU
All	c656da1009f1	STATIC	CPU
1	f9de6ed7d38f	DYNAMIC	Fa0/1
2	fb8d0ae3850b	DYNAMIC	Fa0/2
2	7f403b7cf59a	DYNAMIC	Fa0/2
2	f4182c262c61	DYNAMIC	Fa0/2

Which of the following is a potential threat that is occurring on this access switch?

- A. DDoS on Fa02 port
- B. MAC flooding on Fa0/2 port
- C. ARP poisoning on Fa0/1 port
- D. DNS poisoning on port Fa0/1

Answer: C

Explanation:

ARP poisoning is a type of attack that exploits the ARP protocol to associate a malicious MAC address with a legitimate IP address on a network¹. This allows the attacker to intercept, modify or drop traffic between the victim and other hosts on the same network. In this case, the ARP table of the access switch shows that the same MAC address (00-0c-29-58-35-3b) is associated with two different IP addresses (192.168.1.100 and 192.168.1.101) on port Fa0/12. This indicates that an attacker has poisoned the ARP table to redirect traffic intended for 192.168.1.100 to their own device with MAC address 00-0c-29-58-35-3b. The other options are not related to this scenario. DDoS is a type of attack that overwhelms a target with excessive traffic from multiple sources³. MAC flooding is a type of attack that floods a switch with fake MAC addresses to exhaust its MAC table and force it to operate as a hub⁴. DNS poisoning is a type of attack that corrupts the DNS cache with fake entries to redirect users to malicious websites.

References: 1: <https://www.imperva.com/learn/application-security/arp-spoofing/> 2:

<https://community.cisco.com/t5/networking-knowledge-base/network-tables-mac-routing-arp/ta-p/4184148> 3:

<https://www.imperva.com/learn/application-security/ddos-attack/> 4: <https://www.imperva.com/learn/application-security/mac-flooding/> :

<https://www.imperva.com/learn/application-security/dns-spoofing-poisoning/>

NEW QUESTION 240

- (Exam Topic 2)

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 242

- (Exam Topic 2)

Which Of the following is the best method for ensuring non-repudiation?

- A. SSO
- B. Digital certificate
- C. Token
- D. SSH key

Answer: B

Explanation:

A digital certificate is an electronic document that contains the public key and identity information of an entity, such as a person, organization, website, etc. It is issued and signed by a trusted authority called a certificate authority (CA). It can provide non-repudiation by proving the identity and authenticity of the sender and verifying the integrity of the message or data.

NEW QUESTION 245

- (Exam Topic 2)

A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, "Your connection is not private." Which of the following is the best way to fix this issue?

- A. Ignore the warning and continue to use the application normally.
- B. Install the certificate on each endpoint that needs to use the application.
- C. Send the new certificate to the users to install on their browsers.
- D. Send a CSR to a known CA and install the signed certificate on the application's server.

Answer: D

Explanation:

A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private¹. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems¹. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application's server². The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks³. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved³. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices³.

References: 1:

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

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

NEW QUESTION 246

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 250

- (Exam Topic 2)

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

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 253

- (Exam Topic 2)

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

- A. Documenting the new policy in a change request and submitting the request to change management
- B. Testing the policy in a non-production environment before enabling the policy in the production network
- C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy
- D. Including an "allow any" policy above the "deny any" policy

Answer: B

Explanation:

Testing the policy in a non-production environment before enabling the policy in the production network would prevent the issue of making several company servers unreachable. A non-production environment is a replica of the production network that is used for testing, development, or training purposes. By testing the policy in a non-production environment, the technician can verify the functionality and impact of the policy without affecting the real network or users. This can help to identify and resolve any errors or conflicts before applying the policy to the production network. Testing the policy in a non-production environment can also help to ensure compliance with security standards and best practices.

NEW QUESTION 257

- (Exam Topic 2)

A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send the file to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

- A. SMIME
- B. LDAPS
- C. SSH
- D. SRTP

Answer: C

Explanation:

SSH stands for Secure Shell, which is a protocol that can be used to securely transfer files over the internet. SSH uses encryption and authentication to protect the data in transit and ensure the identity of the sender and receiver. SSH can also support compression, tunneling, and port forwarding. SSH can be used to send files to a business partner by using a command-line tool such as scp or sftp, or by using a graphical user interface (GUI) tool such as FileZilla or WinSCP. SSH can

also be used to remotely access and manage servers or devices over the internet. References:

- > <https://www.globalscape.com/solutions/secure-file-transfer>
- > <https://www.jscape.com/blog/how-to-securely-transfer-large-files-over-the-internet>

NEW QUESTION 262

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network¹². A zero trust policy is a set of “allow rules” that specify conditions for accessing certain resources³.

According to one source⁴, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.

Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.

Reference: Zero Trust implementation guidance | Microsoft Learn

NEW QUESTION 264

- (Exam Topic 2)

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

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

Answer: A

Explanation:

Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.

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

NEW QUESTION 269

- (Exam Topic 2)

Which of the following allow access to remote computing resources, a operating system. and centrized configuration and data

- A. Containers
- B. Edge computing
- C. Thin client
- D. Infrastructure as a service

Answer: C

Explanation:

Thin clients are devices that have minimal hardware and software components and rely on a remote server to provide access to computing resources, an operating system, and centralized configuration and data. Thin clients can reduce the cost, complexity, and security risks of managing multiple devices.

NEW QUESTION 273

- (Exam Topic 2)

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

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

Answer: C

Explanation:

A reverse proxy backdoor is a malicious reverse proxy that can intercept and manipulate the traffic between the client and the web server³. This can allow an attacker to access sensitive data or execute commands on the web server.

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

NEW QUESTION 274

- (Exam Topic 2)

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

- > Limit the sites that can be accessed
- > Only allow access to internal resources while physically on campus.
- > Restrict employees from downloading images from company email

Which of the following controls would best address this situation? (Select two).

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

Answer: DE

Explanation:

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

References:

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

NEW QUESTION 278

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 281

- (Exam Topic 2)

An organization is repairing damage after an incident. Which of the following controls is being implemented?

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

Answer: C

Explanation:

Corrective controls are security measures that are implemented after an incident to repair the damage and restore normal operations. They can include actions such as patching systems, restoring backups, removing malware, etc. An organization that is repairing damage after an incident is implementing corrective controls.

NEW QUESTION 282

- (Exam Topic 2)

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

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

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

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

F. Geofencing

Answer: CD

Explanation:

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

NEW QUESTION 286

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 288

- (Exam Topic 2)

An audit report indicates multiple suspicious attempts to access company resources were made. These attempts were not detected by the company. Which of the following would be the best solution to implement on the company's network?

- A. Intrusion prevention system
- B. Proxy server
- C. Jump server
- D. Security zones

Answer: A

Explanation:

An intrusion prevention system (IPS) is the best solution to implement on the company's network to detect and prevent suspicious attempts to access company resources. An IPS is a network security technology that continuously monitors network traffic for malicious or anomalous activity and takes automated actions to block or mitigate it. An IPS can also alert the system administrators of any potential threats and provide detailed logs and reports of the incidents. An IPS can help the company to improve its security posture and prevent data breaches, unauthorized access, or denial-of-service attacks. References:

- > <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>
- > <https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips>

NEW QUESTION 291

- (Exam Topic 2)

A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the following should the analyst recommend? (Select two).

- A. TACACS+
- B. RADIUS
- C. OAuth
- D. OpenID
- E. Kerberos
- F. CHAP

Answer: BE

Explanation:

RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

NEW QUESTION 293

- (Exam Topic 2)

A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at [comptia.org](https://www.comptia.org))

- A. Identify rogue access points.
- B. Check for channel overlaps.
- C. Create heat maps.
- D. Implement domain hijacking.

Answer: A

Explanation:

Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points. To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.
<https://www.comptia.org/training/books/security-sy0-601-study-guide>

NEW QUESTION 298

- (Exam Topic 2)

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

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

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

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

Answer: B

Explanation:

User-agent spoofing is a technique that involves changing the user-agent string of a web browser or other client to impersonate another browser or device. The user-agent string is a piece of information that identifies the client to the web server and can contain details such as the browser name, version, operating system, and device type. User-agent spoofing can be used to bypass security controls that rely on the user-agent string to determine the legitimacy of a request. In this scenario, the consultants were able to spoof the user-agent string of the company's mobile application and access the API that should have been restricted to it.

NEW QUESTION 300

- (Exam Topic 2)

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the most acceptable?

- A. SED
- B. HSM
- C. DLP
- D. TPM

Answer: A

Explanation:

SED stands for Self-Encrypting Drive, which is a type of hard drive that automatically encrypts and decrypts data using a built-in hardware encryption engine1. SEDs do not require any additional software or configuration, and they do not affect the performance or usability of the laptop2. SEDs also have a feature called Instant Secure Erase, which allows the user to quickly and securely wipe the data on the drive by deleting the encryption key1.

NEW QUESTION 301

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 302

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 306

- (Exam Topic 2)

A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity incident response team. The caller asks the technician to verify the network's internal firewall IP address. Which of the following is the technician's best course of action?

- A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller.
- B. Ask for the caller's name, verify the person's identity in the email directory, and provide the requested information over the phone.
- C. Write down the phone number of the caller if possible, the name of the person requesting the information, hang up, and notify the organization's cybersecurity officer.
- D. Request the caller send an email for identity verification and provide the requested information via email to the caller.

Answer: C

Explanation:

This is the best course of action for the help desk technician because it can help prevent a potential social engineering attack. Social engineering is a technique that involves manipulating or deceiving people into revealing sensitive information or performing actions that compromise security. The caller may be impersonating a member of the organization's cybersecurity incident response team to obtain the network's internal firewall IP address, which could be used for further attacks. The help desk technician should not provide any information over the phone without verifying the caller's identity and authorization. The help desk technician should also report the incident to the organization's cybersecurity officer for investigation and response. References:

<https://www.comptia.org/blog/social-engineering-explained>

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

NEW QUESTION 309

- (Exam Topic 2)

Which of the following can be used to calculate the total loss expected per year due to a threat targeting an asset?

- A. $EF \times \text{asset value}$
- B. ALE / SLE
- C. $MTBF \times \text{impact}$
- D. $SLE \times ARO$

Answer: D

Explanation:

The total loss expected per year due to a threat targeting an asset can be calculated using the Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO). SLE is the monetary loss expected from a single event, while ARO is the estimated frequency of that event occurring in a year. Reference: CompTIA Security+ Study Guide: Exam SY0-501, 7th Edition, by Emmett Dulaney and Chuck Easttom, Chapter 9: Risk Management, page 414.

NEW QUESTION 312

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 315

- (Exam Topic 2)

Which of the following best reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

- A. Implement proper network access restrictions.
- B. Initiate a bug bounty program.
- C. Classify the system as shadow IT.
- D. Increase the frequency of vulnerability scans.

Answer: A

Explanation:

Network access restrictions can limit the exposure of systems that have expired vendor support and lack an immediate replacement, as they can prevent unauthorized or unnecessary access to those systems from other devices or networks. Network access restrictions can include firewalls, network segmentation, VPNs, access control lists, and other methods that can filter or block traffic based on predefined rules or policies. Network access restrictions can reduce the security risks introduced by running systems that have expired vendor support, as they can mitigate the impact of potential vulnerabilities or exploits that may affect those systems. Verified References:

➤ CompTIA Security+ Certification Exam Objectives Version 3.0 <https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf> (See Domain 2.1: Given a scenario, implement secure protocols.)

➤ CompTIA Security+ SY0-501 Study Guide

<https://www.certblaster.com/wp-content/uploads/2017/10/CompTIA-Security-SY0-501-Study-Guide.pdf> (See Chapter 2: Technologies and Tools, Section 2.5: Firewall and Network Security Appliances.)

NEW QUESTION 319

- (Exam Topic 2)

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sales systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the best options to accomplish this objective? (Select two.)

- A. Load balancing
- B. Incremental backups
- C. UPS
- D. RAID
- E. Dual power supply
- F. VLAN

Answer: AD

Explanation:

Load balancing and RAID are the best options to accomplish the objective of improving both server-data fault tolerance and site availability under high consumer load. Load balancing is a method of distributing network traffic across multiple servers to optimize performance, reliability, and scalability. Load balancing can help improve site availability by preventing server overload, ensuring high uptime, and providing redundancy and failover. RAID stands for redundant array of independent disks, which is a technology that combines multiple physical disks into a logical unit to improve data storage performance, reliability, and capacity. RAID can help improve server-data fault tolerance by providing data redundancy, backup, and recovery.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.nginx.com/resources/glossary/load-balancing/> <https://www.ibm.com/cloud/learn/raid>

NEW QUESTION 323

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 324

- (Exam Topic 2)

A user received an SMS on a mobile phone that asked for bank details. Which of the following social engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

Answer: D

Explanation:

Smishing is a type of social engineering technique that involves sending fraudulent or malicious text messages (SMS) to a user's mobile phone. It can trick the user into providing personal or financial information, clicking on malicious links, downloading malware, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity.

NEW QUESTION 325

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-701 Product From:

<https://www.2passeasy.com/dumps/SY0-701/>

Money Back Guarantee

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