



CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

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

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

- A. Incremental backups followed by differential backups
- B. Full backups followed by incremental backups
- C. Delta backups followed by differential backups
- D. Incremental backups followed by delta backups
- E. Full backup followed by different backups

Answer: B

Explanation:

The best backup strategy for minimizing the number of backups that need to be restored in case of data loss is full backups followed by incremental backups. This strategy allows for a complete restoration of data by restoring the most recent full backup followed by the most recent incremental backup. Reference: CompTIA Security+ Certification Guide, Third Edition (Exam SY0-601) page 126

NEW QUESTION 7

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 9

- (Exam Topic 1)

A 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 10

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

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

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

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

➤ A. Enable the remote-wiping option in the MDM software in case the phone is stolen. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. Remote wiping can erase both work and personal data on the device, which may not be desirable for employees.

➤ B. Configure the MDM software to enforce the use of PINs to access the phone. This option may enhance the security of the device, but it may not address the company's concern about data loss. PINs can be guessed or bypassed by attackers, and they do not protect data if the device is physically accessed.

➤ D. Perform a factory reset on the phone before installing the company's applications. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. A factory reset will erase all data on the device, including personal data, which may not be acceptable to employees.

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

"MDM software is a type of remote asset-management software that runs from a central server¹. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets²."

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

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

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

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

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 11

- (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 15

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 19

- (Exam Topic 1)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 24

- (Exam Topic 1)

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

- A. Privacy
- B. Cloud storage of telemetry data
- C. GPS spoofing
- D. Weather events

Answer: A

Explanation:

The use of a drone for perimeter and boundary monitoring can raise privacy concerns, as it may capture video and images of individuals on or near the monitored premises. The company should take measures to ensure that privacy rights are not violated. References:

> CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 8

NEW QUESTION 26

- (Exam Topic 1)

Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

- A. Penetration testing
- B. Code review
- C. Wardriving
- D. Bug bounty

Answer: D

Explanation:

A bug bounty is a technique that compensates researchers for finding vulnerabilities in software or systems. A bug bounty program is an initiative that offers rewards, usually monetary, to ethical hackers who report security flaws to the owners or developers of the software or system. Bug bounty programs are often used by companies such as Meta (formerly Facebook), Google, Microsoft, and others to improve the security of their products and services

Bug bounty programs compensate researchers, often financially, for finding vulnerabilities in software, websites, or other technology. These programs provide an additional layer of security testing and incentivize researchers to report vulnerabilities instead of exploiting them.

NEW QUESTION 30

- (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 32

- (Exam Topic 1)

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

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

Answer: A

Explanation:

PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data¹. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet¹.

One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for². The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org². A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org².

Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used³. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years³. The validity period can be checked by looking at the valid from and valid to dates on the certificate³.

Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org². It also has a validity period of one year, which means it needs to be rotated annually³.

NEW QUESTION 35

- (Exam Topic 1)

A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

- A. Change the default settings on the PC.
- B. Define the PC firewall rules to limit access.
- C. Encrypt the disk on the storage device.
- D. Plug the storage device in to the UPS

Answer: A

Explanation:

The best option that will help to protect the PC from malicious files on the storage device would be A. Change the default settings on the PC. Changing the default settings on the PC can include disabling the autorun or autoplay feature, which can prevent malicious files from executing automatically when the storage device is plugged in. Changing the default settings can also include enabling antivirus software, updating the operating system and applications, and configuring user account control and permissions.

NEW QUESTION 38

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 39

- (Exam Topic 1)

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

does this scenario describe?

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

Answer: A

Explanation:

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

NEW QUESTION 42

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

References:

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

NEW QUESTION 45

- (Exam Topic 1)

An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

- A. SIEM
- B. SOAR
- C. EDR
- D. CASB

Answer: B

Explanation:

Security Orchestration, Automation, and Response (SOAR) should be implemented to integrate incident response processes into a workflow with automated decision points and actions based on predefined playbooks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

NEW QUESTION 46

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 51

- (Exam Topic 1)

Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

- A. Hashing
- B. Salting
- C. Integrity
- D. Digital signature

Answer: A

Explanation:

Hashing is a cryptographic function that produces a unique fixed-size output (i.e., hash value) from an input (i.e., data). The hash value is a digital fingerprint of the data, which means that if the data changes, so too does the hash value. By comparing the hash value of the downloaded file with the hash value provided by the security website, the security analyst can verify that the file has not been altered in transit or corrupted.

NEW QUESTION 55

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 58

- (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 61

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 63

- (Exam Topic 1)

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

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

Which of the following attacks occurred?

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

Answer: B

Explanation:

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

NEW QUESTION 65

- (Exam Topic 1)

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

- A. A forward proxy
- B. A stateful firewall

- C. A jump server
- D. A port tap

Answer: C

Explanation:

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

NEW QUESTION 69

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 70

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 75

- (Exam Topic 1)

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

Which of the following documents did Ann receive?

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

Answer: A

Explanation:

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

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

NEW QUESTION 79

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

materials. References: 1. CompTIA Security+ Certification Exam Objectives (SY0-601):

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

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

The other options are not correct because:

➤ A. The Cyber Kill Chain is a model that describes the stages of a cyberattack from reconnaissance to exfiltration. The Cyber Kill Chain does not provide a way to create named groups based on adversary TTPs.

➤ B. The incident response process is a set of procedures and guidelines that defines how an organization should respond to a security incident. The incident response process does not provide a way to create named groups based on adversary TTPs.

➤ C. The Diamond Model of Intrusion Analysis is a framework that describes the four core features of any intrusion: adversary, capability, infrastructure, and victim. The Diamond Model of Intrusion Analysis does not provide a way to create named groups based on adversary TTPs.

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

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

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

NEW QUESTION 81

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 85

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 89

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 94

- (Exam Topic 1)

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

- A. The Diamond Model of Intrusion Analysis
- B. CIS Critical Security Controls
- C. NIST Risk Management Framework
- D. ISO 27002

Answer: C

Explanation:

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

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

NEW QUESTION 96

- (Exam Topic 1)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 97

- (Exam Topic 1)

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

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 100

- (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 104

- (Exam Topic 1)

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

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

Answer: C

Explanation:

The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it

may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run.
References: <https://www.techopedia.com/definition/31541/application-whitelisting>

NEW QUESTION 106

- (Exam Topic 1)

Which of the following biometric authentication methods is the MOST accurate?

- A. Gait
- B. Retina
- C. Signature
- D. Voice

Answer: B

Explanation:

Retina authentication is the most accurate biometric authentication method. Retina authentication is based on recognizing the unique pattern of blood vessels and other features in the retina. This makes it virtually impossible to duplicate or bypass, making it the most secure form of biometric authentication currently available.

NEW QUESTION 111

- (Exam Topic 1)

A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

- A. A RAT
- B. Ransomware
- C. Polymorphic
- D. A worm

Answer: A

Explanation:

Based on the given information, the most likely type of malware infecting the hosts is a RAT (Remote Access Trojan). RATs are often used for stealthy unauthorized access to a victim's computer, and they can evade traditional antivirus software through various sophisticated techniques. In particular, the fact that the malware is communicating with external IP addresses during specific hours suggests that it may be under the control of an attacker who is issuing commands from a remote location. Ransomware, polymorphic malware, and worms are also possible culprits, but the context of the question suggests that a RAT is the most likely answer.

NEW QUESTION 114

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 119

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 120

- (Exam Topic 1)

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


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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 123

- (Exam Topic 1)

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

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

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 124

- (Exam Topic 1)

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

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

Which of the following is MOST likely occurring?

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

Answer: C

Explanation:

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

NEW QUESTION 129

- (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 130

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 132

- (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 134

- (Exam Topic 1)

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

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

Answer: E

Explanation:

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

NEW QUESTION 135

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 136

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 137

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

References:

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

NEW QUESTION 142

- (Exam Topic 1)

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

Which of the following types of attacks has occurred?

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

Answer: A

Explanation:

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

NEW QUESTION 144

- (Exam Topic 1)

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

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

Answer: DE

Explanation:

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

NEW QUESTION 149

- (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 150

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 155

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 158

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 160

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 164

- (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 167

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 170

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

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

> A. Disconnect all external network connections from the firewall. This could be another containment measure to prevent external attackers from accessing the network, but it would also disrupt legitimate network traffic and services. This action should be taken only if it is part of the incident response plan and after notifying the relevant parties.

> B. Send response teams to the network switch locations to perform updates. This could be a recovery measure to restore normal network operations and apply patches or updates to prevent future incidents, but it should be done only after the incident has been properly identified, contained, and eradicated.

> C. Turn on all the network switches by using the centralized management software. This could be a recovery measure to restore normal network operations, but it should be done only after the incident has been properly identified, contained, and eradicated.

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

"An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan

typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned.”

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

NEW QUESTION 174

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 175

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 179

- (Exam Topic 1)

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

- A. Whaling
- B. Spam
- C. Invoice scam
- D. Pharming

Answer: A

Explanation:

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

NEW QUESTION 180

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 184

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 186

- (Exam Topic 1)

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

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

Answer: BF

Explanation:

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

NEW QUESTION 188

- (Exam Topic 1)

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

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

Which of the following options BEST accommodates these requirements?

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

Answer: A

Explanation:

Detailed
WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication. Additionally, WPA2-Enterprise does not allow for open SSIDs.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7: Securing Networks, p. 317

NEW QUESTION 192

- (Exam Topic 1)

Which of the following must be in place before implementing a BCP?

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

Answer: D

Explanation:

A Business Impact Analysis (BIA) is a critical component of a Business Continuity Plan (BCP). It identifies and prioritizes critical business functions and determines the impact of their disruption. References: CompTIA Security+ Study Guide 601, Chapter 10

NEW QUESTION 197

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 198

- (Exam Topic 1)

Which of the following conditions impacts data sovereignty?

- A. Rights management
- B. Criminal investigations
- C. Healthcare data
- D. International operations

Answer: D

Explanation:

Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations. References:

➤ CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION 199

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

The other options are not correct because:

➤ A. Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.

➤ B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.

➤ D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.

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

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://gdpr-info.eu/issues/data-protection-officer/>

NEW QUESTION 203

- (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 206

- (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 210

- (Exam Topic 1)

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

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

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

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

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

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

Answer: B

Explanation:

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

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

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

indicators to determine the type of attack:

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

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

NEW QUESTION 214

- (Exam Topic 1)

The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

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

Answer: B

Explanation:

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

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

NEW QUESTION 216

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 218

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 221

- (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 225

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 230

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 234

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 239

- (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 242

- (Exam Topic 1)

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

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

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

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

Answer: CF

Explanation:

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

Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device. This can enhance security by

preventing unauthorized access from hostile or foreign region2s. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

NEW QUESTION 243

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 246

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 249

- (Exam Topic 1)

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

- A. Physical move the PC to a separate internet pint of presence
- B. Create and apply micro segmentation rules.
- C. Emulate the malware in a heavily monitored DM Z segment.
- D. Apply network blacklisting rules for the adversary domain

Answer: C

Explanation:

To observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC while reducing the risk of lateral spread and the risk that the adversary would notice any changes, the best technique to use is to emulate the malware in a heavily monitored DMZ segment. This is a secure environment that is isolated from the rest of the network and can be heavily monitored to detect any suspicious activity. By emulating the malware in this environment, the activity can be observed without the risk of lateral spread or detection by the adversary. References:

<https://www.sans.org/blog/incident-response-fundamentals-why-is-the-dmz-so-important/>

NEW QUESTION 254

- (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 256

- (Exam Topic 1)

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

the following:

- Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
- Internal users in question were changing their passwords frequently during that time period.
- A jump box that several domain administrator users use to connect to remote devices was recently compromised.
- The authentication method used in the environment is NTLM.

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

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

Answer: A

Explanation:

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

NEW QUESTION 257

- (Exam Topic 2)

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

- A. Insider threat
- B. Hacktivist
- C. Nation-state
- D. Organized crime

Answer: D

Explanation:

Organized crime is a term that describes groups of criminals who operate in a coordinated and systematic manner to pursue illicit activities for profit. Organized crime groups often use sophisticated tools and techniques to evade law enforcement and exploit vulnerabilities in various sectors, such as finance, transportation, or healthcare. Organized crime groups may also collaborate with other criminal groups or actors to share resources, information, or expertise. Ransomware as a service (RaaS) is an example of a business model used by organized crime groups to conduct ransomware and extortion attacks. RaaS is an arrangement between an operator, who develops and maintains the tools to power extortion operations, and an affiliate, who deploys the ransomware payload. When the affiliate conducts a successful ransomware and extortion attack, both parties profit. The RaaS model lowers the barrier to entry for attackers who may not have the skill or technical wherewithal to develop their own tools but can manage ready-made penetration testing and sysadmin tools to perform attacks¹². Insider threat is a term that describes individuals who have legitimate access to an organization's systems or data and use it for malicious purposes, such as theft, sabotage, or espionage. Insider threats may be motivated by various factors, such as greed, revenge, ideology, or coercion. Insider threats may also be unintentional, such as when an employee falls victim to phishing or social engineering. Hacktivist is a term that describes individuals or groups who use hacking or cyberattacks to promote a political or social cause. Hacktivists may target governments, corporations, or other entities that they perceive as oppressive, corrupt, or unethical. Hacktivists may also use cyberattacks to expose information, disrupt services, or deface websites. Nation-state is a term that describes a sovereign state that has a centralized government and a defined territory. Nation-state actors are individuals or groups who conduct cyberattacks on behalf of or with the support of a nation-state. Nation-state actors may target other states, organizations, or individuals for various reasons, such as espionage, sabotage, influence, or retaliation.

NEW QUESTION 260

- (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 263

- (Exam Topic 2)

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

- A. Blockchain
- B. Salting
- C. Quantum

D. Digital signature

Answer: B

Explanation:

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

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

NEW QUESTION 264

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 265

- (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 267

- (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 269

- (Exam Topic 2)

A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title

business phone number location first initial with last name and race Which of the following best describes this type of information?

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

Answer: B

Explanation:

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

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

NEW QUESTION 272

- (Exam Topic 2)

An attack has occurred against a company.

INSTRUCTIONS

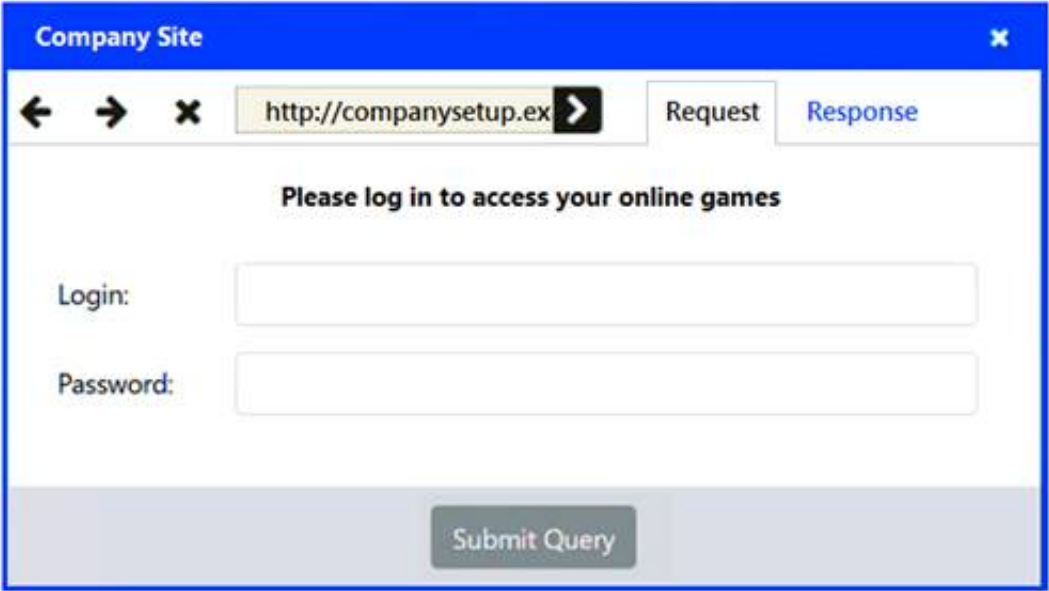
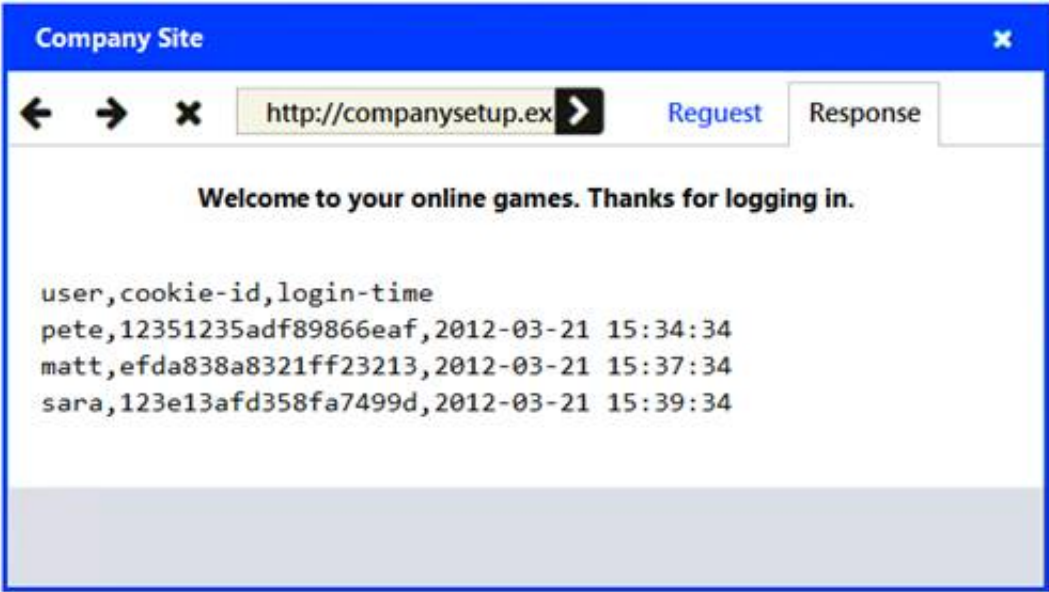
You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.

(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

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



Select and Place:

Answer Area 1

SQL Injection

Cross Site Scripting

XML Injection

Session Hijacking

Type of attack

?

Answer Area 2

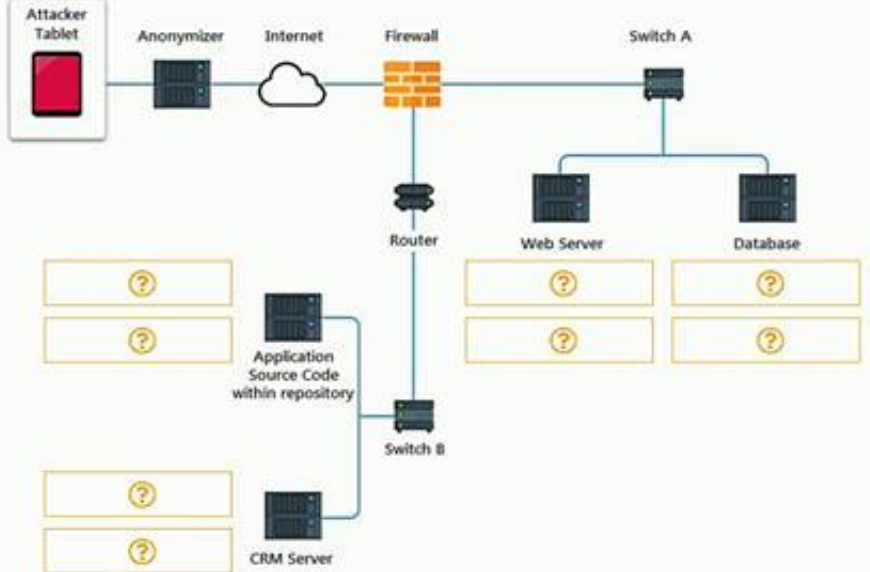
Input Validation

Code Review

WAF

URL Filtering

Record level access control



- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

A computer screen shot of a computer Description automatically generated with low confidence

NEW QUESTION 275

- (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 276

- (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 281

- (Exam Topic 2)

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

- A. Password, PIN, and physical token
 B. PIN, fingerprint scan, and iris scan

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

Answer: C

Explanation:

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

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

NEW QUESTION 286

- (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 289

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 292

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

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

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

NEW QUESTION 293

- (Exam Topic 2)

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.


Perform the following steps:

* 1. Configure the RADIUS server.

* 2. Configure the WiFi controller.

* 3. Preconfigure the client for an incoming guest. The guest AD credentials are:

User: guest01 Password: guestpass



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Wifi Controller SSID: CORPGUEST

SHARED KEY: Secret

AAA server IP: 192.168.1.20

PSK: Blank

Authentication type: WPA2-EAP-PEAP-MSCHAPv2 Controller IP: 192.168.1.10

Radius Server Shared Key: Secret

Client IP: 192.168.1.10

Authentication Type: Active Directory Server IP: 192.168.1.20

Wireless Client SSID: CORPGUEST

Username: guest01 Userpassword: guestpass PSK: Blank

Authentication type: WPA2-Enterprise

NEW QUESTION 297

- (Exam Topic 2)

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

GET

[http://yourbank.com/transfer.do?acctnum=087646959](http://yourbank.com/transfer.do?acctnum=087646959&amount=500000)

&amount=500000 HTTP/1.1

GET

[http://yourbank.com/transfer.do?acctnum=087646958](http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000)

&amount=5000000 HTTP/1.1

GET

[http://yourbank.com/transfer.do?acctnum=-087646958](http://yourbank.com/transfer.do?acctnum=-087646958&amount=1000000)

&amount=1000000 HTTP/1.1

GET

[http://yourbank.com/transfer.do?acctnum=087646953](http://yourbank.com/transfer.do?acctnum=087646953&amount=500)

&amount=500 HTTP/1.1

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

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

Answer: B

Explanation:

CSRF stands for Cross-Site Request Forgery, which is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated¹. In this case, the attacker may have tricked the user into clicking a malicious link or visiting a malicious website that sends forged requests to the web server of the bank, using the user's session cookie or other credentials. The web server then performs the money transfer requests as if they were initiated by the user, without verifying the origin or validity of the requests.

* A. SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application's database layer, where malicious SQL statements are inserted into an entry field for execution². The output of the web server log does not show any SQL statements or commands.

* B. CSRF. This is the correct answer, because CSRF is an attack that exploits the trust a web server has in a user's browser, where malicious requests are sent to the web server using the user's credentials¹. The output of the web server log shows multiple GET requests with different account numbers and amounts, which may indicate a CSRF attack.

* C. Spear phishing. This is not the correct answer, because spear phishing is an attack that targets a specific individual or organization with a personalized email or message that contains a malicious link or attachment³. The output of the web server log does not show any email or message content or headers.

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

NEW QUESTION 301

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 302

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 307

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SY0-701 Practice Exam Features:

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

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