

CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: DE

Explanation:

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

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

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

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

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

- (Exam Topic 1)

A 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 4

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

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

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 7

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

➤ [CompTIA Security+ Study Guide Exam SY0-601, Chapter 8](#)

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 9

- (Exam Topic 1)

A security assessment found that several embedded systems are running unsecure protocols. These systems were purchased two years ago and the company that developed them is no longer in business. Which of the following constraints BEST describes the reason the findings cannot be remediated?

- A. inability to authenticate
- B. Implied trust
- C. Lack of computing power
- D. Unavailable patch

Answer: D

Explanation:

If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue. References:

➤ CompTIA Security+ Study Guide, Sixth Edition, pages 35-36

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (Exam Topic 1)

The following are the logs of a successful attack.

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

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

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

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 15

- (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 20

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 21

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 26

- (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 31

- (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 36

- (Exam Topic 1)

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

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

Answer: A

Explanation:

Hardware Security Module (HSM) is a network appliance designed to securely store cryptographic keys and perform cryptographic operations. HSMs provide a secure environment for key management and can be used to keep cryptographic keys safe from theft, loss, or unauthorized access. Therefore, an enterprise can achieve the goal of keeping cryptographic keys in a safe manner by using an HSM appliance. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 2.0: Technologies and Tools, 2.4 Given a scenario, use appropriate tools and techniques to troubleshoot security issues, p. 21

NEW QUESTION 38

- (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 42

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 46

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 48

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

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

The other options are not correct because:

- B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.
- C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.
- D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans. According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack: "A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers."
- References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/>

NEW QUESTION 52

- (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 56

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 60

- (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 64

- (Exam Topic 1)

An organization wants to enable built-in FDE on all laptops Which of the following should the organization ensure is Installed on all laptops?

- A. TPM
- B. CA
- C. SAML
- D. CRL

Answer: A

Explanation:

The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

NEW QUESTION 66

- (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 68

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 71

- (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 75

- (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 time 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 78

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Detailed

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

NEW QUESTION 82

- (Exam Topic 1)

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

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

Answer: A

Explanation:

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

NEW QUESTION 83

- (Exam Topic 1)

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

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

Which of the following is MOST likely the issue?

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

Answer: C

Explanation:

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

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

NEW QUESTION 86

- (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. SSL/TLS 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 88

- (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 89

- (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 93

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 94

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

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

- .pfx: This is a file format that stores a certificate and its private and public keys. It is also known as PKCS#12 or Personal Information Exchange. It is used by some applications such as Microsoft Internet Explorer and Outlook to import and export certificates and keys.1

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

NEW QUESTION 98

- (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 101

- (Exam Topic 1)

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

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

Answer: C

Explanation:

an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection¹². However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications³⁴. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspection³ⁿ⁴⁵, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly³⁴.

NEW QUESTION 103

- (Exam Topic 1)

As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

- A. Creating a playbook within the SOAR
- B. Implementing rules in the NGFW
- C. Updating the DLP hash database
- D. Publishing a new CRL with revoked certificates

Answer: A

Explanation:

Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 352-354

NEW QUESTION 104

- (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 105

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 110

- (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 115

- (Exam Topic 1)

A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

- A. Create a new network for the mobile devices and block the communication to the internal network and servers
- B. Use a captive portal for user authentication.
- C. Authenticate users using OAuth for more resiliency
- D. Implement SSO and allow communication to the internal network
- E. Use the existing network and allow communication to the internal network and servers.
- F. Use a new and updated RADIUS server to maintain the best solution

Answer: BC

Explanation:

When allowing mobile BYOD devices to access network resources, using a captive portal for user authentication and authenticating users using OAuth are both best practices for authentication and infrastructure security. A captive portal requires users to authenticate before accessing the network and can be used to enforce policies and restrictions. OAuth allows users to authenticate using third-party providers, reducing the risk of password reuse and credential theft. References: CompTIA Security+ Study Guide, pages 217-218, 225-226

NEW QUESTION 118

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 123

- (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 128

- (Exam Topic 1)

A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

- A. Implement input validations
- B. Deploy MFA
- C. Utilize a WAF
- D. Configure HIPS

Answer: A

Explanation:

Implementing input validations will prevent code injection attacks by verifying the type and format of user input. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

NEW QUESTION 131

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 134

- (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 137

- (Exam Topic 1)

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

- A. Shadow IT
- B. Credential stuffing

- C. SQL injection
- D. Man in the browser
- E. Bluejacking

Answer: A

Explanation:

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

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

NEW QUESTION 140

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 141

- (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 146

- (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 151

- (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 155

- (Exam Topic 1)

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

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

Which of the following should the analyst recommend to disable?

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

Answer: A

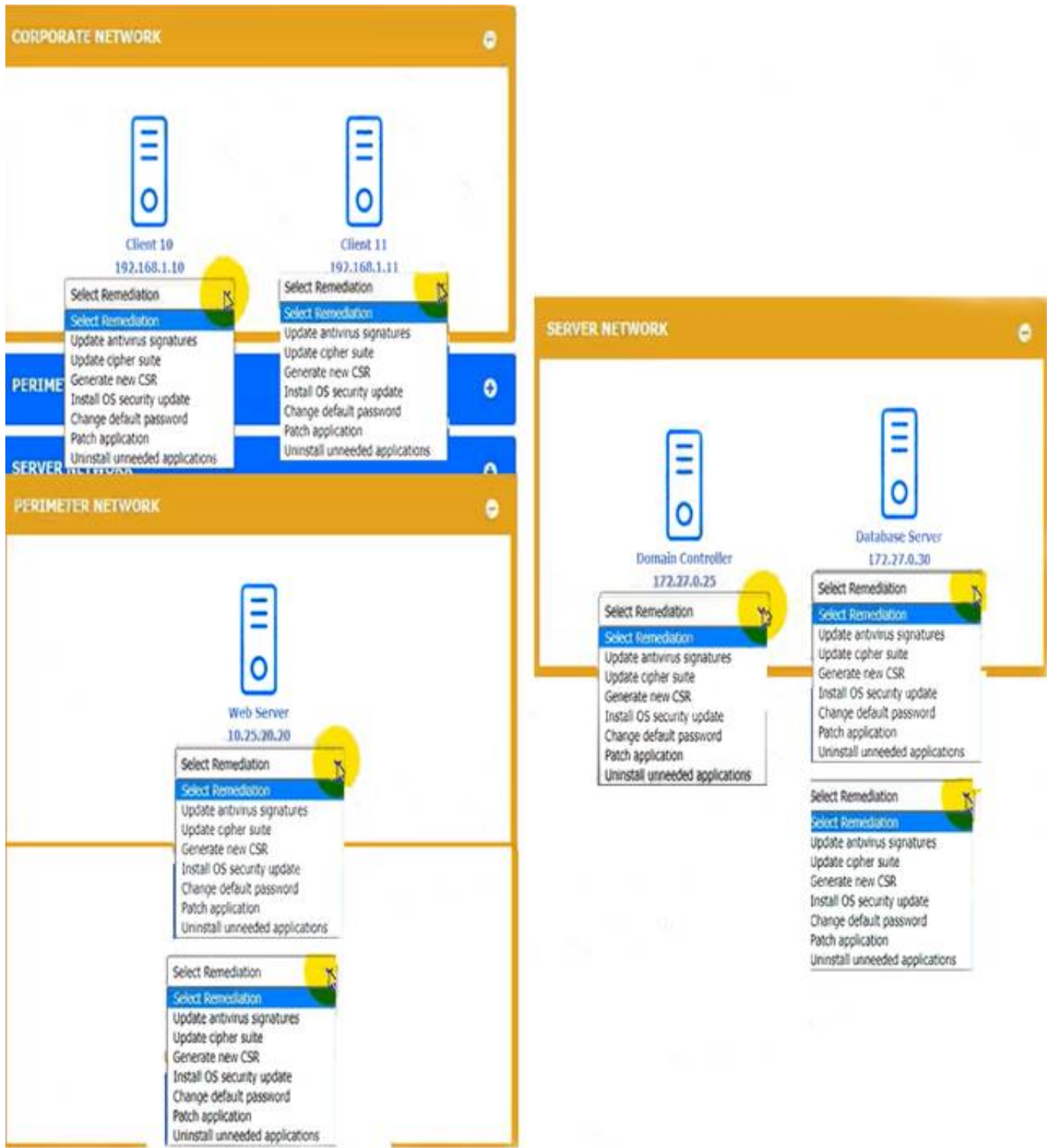
NEW QUESTION 159

- (Exam Topic 1)

You received the output of a recent vulnerability assessment.

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

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



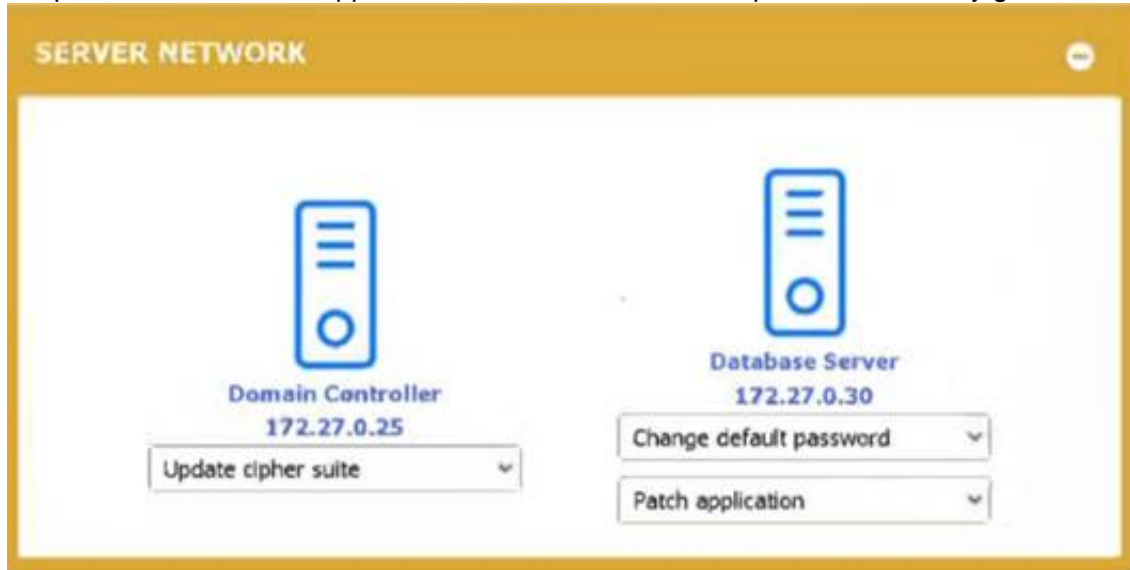
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



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



Graphical user interface, text, application Description automatically generated



NEW QUESTION 164

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

References:

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

NEW QUESTION 167

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 168

- (Exam Topic 1)

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

- A. TAXII
- B. TLP
- C. TTP
- D. STIX

Answer: A

Explanation:

Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations. It allows organizations to automate the exchange of information in a secure and timely manner. References: CompTIA Security+ Certification Exam Objectives 3.6 Given a scenario, implement secure network architecture concepts. Study Guide: Chapter 4, page 167.

NEW QUESTION 169

- (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 172

- (Exam Topic 1)

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

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

Answer: A

Explanation:

A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees. References: CompTIA Security+ SY0-601 Exam Objectives: 3.3 Given a scenario, implement secure mobile solutions.

NEW QUESTION 175

- (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 176

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

NEW QUESTION 180

- (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 184

- (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 188

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 192

- (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 194

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 199

- (Exam Topic 2)

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

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

Answer: A

Explanation:

OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for improving the security of web applications. It publishes a list of the most common web application vulnerabilities, such as injection, broken authentication, cross-site scripting, etc., and provides recommendations and best practices for preventing and mitigating them

NEW QUESTION 200

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Isolating the device is the first thing that a security analyst should do if they suspect that a user's device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://resources.infosecinstitute.com/topic/incident-response-process/>

NEW QUESTION 201

- (Exam Topic 2)

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

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

Answer: AC

Explanation:

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

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

NEW QUESTION 206

- (Exam Topic 2)

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

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

Answer: C

Explanation:

IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a

VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association. References:
<https://www.comptia.org/content/guides/what-is-vpn>

NEW QUESTION 208

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

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

NEW QUESTION 210

- (Exam Topic 2)

A security analyst is hardening a network infrastructure. The analyst is given the following requirements:

- Preserve the use of public IP addresses assigned to equipment on the core router
- Enable "in transport" encryption protection to the web server with the strongest ciphers. Which of the following should the analyst implement to meet these requirements? (Select two).

- A. Configure VLANs on the core router
- B. Configure NAT on the core router.
- C. Configure BGP on the core router
- D. Enable AES encryption on the web server
- E. Enable 3DES encryption on the web server
- F. Enable TLSv2 encryption on the web server

Answer: BF

Explanation:

NAT (Network Address Translation) is a technique that allows a router to translate private IP addresses into public IP addresses and vice versa. It can preserve the use of public IP addresses assigned to equipment on the core router by allowing multiple devices to share a single public IP address. TLSv2 (Transport Layer Security version 2) is a cryptographic protocol that provides secure communication over the internet. It can enable "in transport" encryption protection to the web server with the strongest ciphers by encrypting the data transmitted between the web server and the clients using advanced algorithms and key exchange methods.

NEW QUESTION 212

- (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 215

- (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 219

- (Exam Topic 2)

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

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

Answer: AF

Explanation:

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

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

NEW QUESTION 222

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 223

- (Exam Topic 2)

A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

- A. Install DLP software to prevent data loss.
- B. Use the latest version of software.
- C. Install a SIEM device.
- D. Implement MDM.
- E. Implement a screened subnet for the web server.
- F. Install an endpoint security solution.
- G. Update the website certificate and revoke the existing ones.
- H. Deploy additional network sensors.

Answer: BEF

NEW QUESTION 228

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 231

- (Exam Topic 2)

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

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

Answer: C

Explanation:

A buffer overflow is a type of vulnerability that occurs when an attacker sends more data than a buffer can hold, causing the excess data to overwrite adjacent memory locations such as registers. It can allow an attacker to overwrite a register with a malicious address that changes the execution path and executes arbitrary code on the target system

NEW QUESTION 234

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 236

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

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

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

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

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

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

NEW QUESTION 241

- (Exam Topic 2)

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

- A. User

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

Answer: B

Explanation:

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

NEW QUESTION 243

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

NEW QUESTION 245

- (Exam Topic 2)

An analyst is concerned about data leaks and wants to restrict access to internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service. Which of the following would be the best technology for the analyst to consider implementing?

- A. DLP
- B. VPC
- C. CASB
- D. Content filtering

Answer: C

Explanation:

A cloud access security broker (CASB) is a technology that can restrict access to internet services to authorized users only and control the actions each user can perform on each service. A CASB is a type of software or service that acts as an intermediary between users and cloud service providers. A CASB can enforce security policies, monitor user activity, detect and prevent data leaks, encrypt data, and provide visibility and auditability of cloud usage. References:

<https://www.comptia.org/blog/what-is-a-cloud-access-security-broker>

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

NEW QUESTION 249

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

References: <https://www.comptia.org/blog/what-is-a-data-controller>

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

NEW QUESTION 253

- (Exam Topic 2)

A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

- A. Application management
- B. Content management
- C. Containerization
- D. Full disk encryption

Answer: B

Explanation:

Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.

References: 1

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2
CompTIA

Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3 <https://www.comptia.org/blog/what-is-data-loss-prevention>

NEW QUESTION 257

- (Exam Topic 2)

To reduce and limit software and infrastructure costs the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data Which of the following cloud services would best accommodate the request?

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

Answer: D

Explanation:

SaaS (Software as a Service) is a cloud model that provides clients with applications and software that are hosted and managed by a cloud provider over the internet. It can move email services to the cloud by allowing clients to access and use email applications without installing or maintaining them on their own devices or servers

NEW QUESTION 260

- (Exam Topic 2)

A company's help desk has received calls about the wireless network being down and users being unable to connect to it The network administrator says all access points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

- A. Someone near the building is jamming the signal
- B. A user has set up a rogue access point near the building
- C. Someone set up an evil twin access point in the affected area.
- D. The APs in the affected area have been unplugged from the network

Answer: A

Explanation:

Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

NEW QUESTION 262

- (Exam Topic 2)

A company is moving to new location. The systems administrator has provided the following server room requirements to the facilities staff:

- Consistent power levels in case of brownouts or voltage spikes
- A minimum of 30 minutes runtime following a power outage
- Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

- A. Maintaining a standby, gas-powered generator
- B. Using large surge suppressors on computer equipment
- C. Configuring managed PDUs to monitor power levels
- D. Deploying an appropriately sized, network-connected UPS device

Answer: D

Explanation:

A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

NEW QUESTION 263

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 265

- (Exam Topic 2)

A security operations technician is searching the log named /var/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

- A. cat /var/messages | grep 10.1.1.1
- B. grep 10.1.1.1 | cat /var/messages
- C. grep /var/messages | cat 10.1.1.1
- D. cat 10.1.1.1 | grep /var/messages

Answer: A

Explanation:

the cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex. The cut command splits each line into fields based on a delimiter and extracts a specific field.

NEW QUESTION 270

- (Exam Topic 2)

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

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

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

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

Answer: B

Explanation:

User-agent spoofing is a technique that allows an attacker to modify the user-agent header of an HTTP request to impersonate another browser or device¹². User-agent spoofing can be used to bypass security controls that rely on user-agent filtering or validation¹². In this case, the attacker spoofed the user-agent header to match the company's mobile application, which was allowed to access the back-end server's API².

NEW QUESTION 273

- (Exam Topic 2)

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

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

Answer: D

Explanation:

Continuous Integration is the concept that best represents developers writing code and merging it into shared repositories several times a day, where it is tested automatically. Continuous Integration is a software development practice that involves integrating code changes from multiple developers into a shared repository frequently and running automated tests to ensure quality and functionality. Continuous Integration can help to detect and fix errors early, improve collaboration, reduce rework, and accelerate delivery. References: <https://www.comptia.org/blog/what-is-devops>
<https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pdf>

NEW QUESTION 275

- (Exam Topic 2)

Which of the following control types is patch management classified under?

- A. Deterrent
- B. Physical
- C. Corrective
- D. Detective

Answer: C

Explanation:

Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

NEW QUESTION 280

- (Exam Topic 2)

A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

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

Answer: D

Explanation:

An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

NEW QUESTION 282

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

NEW QUESTION 285

- (Exam Topic 2)

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- * Check-in/checkout of credentials
- * The ability to use but not know the password
- * Automated password changes
- * Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

Answer: C

Explanation:

A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources¹². A PAM system can meet the requirements of the project by providing features such as:

- Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin²g³.
- The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on²³. This prevents users from copying, changing, or sharing password²s.
- Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness²³. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise².
- Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them²³. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents².

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner⁴. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.

A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification⁵. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.

A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login⁶. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 287

- (Exam Topic 2)

Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

- A. An RTO report
- B. A risk register
- C. A business impact analysis
- D. An asset value register
- E. A disaster recovery plan

Answer: B

Explanation:

A risk register is a document or a tool that records and tracks information about the identified risks and their analysis, such as likelihood, impact, priority, mitigation strategies, residual risks, etc. It can contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented.

NEW QUESTION 292

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

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

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

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

Reference: Zero Trust implementation guidance | Microsoft Learn

NEW QUESTION 293

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

NEW QUESTION 297

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 301

- (Exam Topic 2)

A company is auditing the manner in which its European customers' personal information is handled. Which of the following should the company consult?

- A. GDPR
- B. ISO
- C. NIST
- D. PCI DSS

Answer: A

Explanation:

GDPR stands for General Data Protection Regulation, which is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR also applies to organizations outside the EU that offer goods or services to, or monitor the behavior of, EU data subjects. GDPR aims to protect the privacy and rights of EU citizens and residents regarding their personal data. GDPR defines personal data as any information relating to an identified or identifiable natural person, such as name, identification number, location data, online identifiers, or any factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. A company that is auditing the manner in which its European customers' personal information is handled should consult GDPR to ensure compliance with its rules and obligations. References:

- > <https://www.gdpreu.org/the-regulation/key-concepts/personal-data/>
- > <https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regula>

NEW QUESTION 304

- (Exam Topic 2)

A company a "right to forgotten" request To legally comply, the company must remove data related to the requester from its systems. Which Of the following Company most likely complying with?

- A. NIST CSF
- B. GDPR
- C. PCI OSS
- D. ISO 27001

Answer: B

Explanation:

GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas. GDPR grants individuals the right to request the deletion or removal of their personal data from an organization's systems under certain circumstances. This right is also known as the "right to be forgotten" or the "right to erasure". An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.

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/right-to-be-forgotten/>

NEW QUESTION 306

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 307

- (Exam Topic 2)

A security analyst is reviewing computer logs because a host was compromised by malware After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

- A. Dump file
- B. System log
- C. Web application log
- D. Security too

Answer: A

Explanation:

A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files>

NEW QUESTION 312

- (Exam Topic 2)

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment Which of the following solutions should the engineer implement? (Select two).

- A. CASB
- B. WAF
- C. Load balancer
- D. VPN
- E. TLS
- F. DAST

Answer: BC

Explanation:

A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service¹. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability². A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization's users³. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.

References: 1: <https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/> 2:

<https://www.imperva.com/learn/application-security/load-balancing/> 3: <https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/> :

<https://www.imperva.com/learn/application-security/vpn-virtual-private-network/> : <https://www.imperva.com/learn/application-security/transport-layer-security-tls/> :

<https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/> : <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-ins>

: <https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall> :

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azur>

NEW QUESTION 315

- (Exam Topic 2)

Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's main gate?

- A. Crossover error rate
- B. False match raw
- C. False rejection
- D. False positive

Answer: C

Explanation:

False rejection Short

A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors. References: <https://www.comptia.org/blog/what-is-biometrics>

NEW QUESTION 320

- (Exam Topic 2)

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

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

Answer: C

Explanation:

Version control is a solution that can help a development team to analyze the deletion or editing of data sets without affecting the original copy. Version control is a system that records changes to a file or set of files over time so that specific versions can be recalled later. Version control can help developers track and manage changes to code, data, or documents, as well as collaborate with other developers and resolve conflicts.

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

<https://www.atlassian.com/git/tutorials/what-is-version-control>

NEW QUESTION 322

- (Exam Topic 2)

A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner. Which of the following concepts describes this scenario?

- A. Red-team exercise
- B. Business continuity plan testing
- C. Tabletop exercise
- D. Functional exercise

Answer: C

Explanation:

A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond

to it1. A tabletop exercise is a low-impact and cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and enhance communication and coordination among team members2. A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization3. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption4. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.

References: 1:

<https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-g>

2: <https://www.linuxjournal.com/content/security-exercises> 3:

<https://www.imperva.com/learn/application-security/red-team-blue-team/> 4: <https://www.ready.gov/business-continuity-plan> : <https://www.ready.gov/exercises>

NEW QUESTION 323

.....

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](#)