CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

  All examinations will be up to date.

* 24/7 Quality Support

  We will provide service round the clock.

* 100% Pass Rate

  Our guarantee that you will pass the exam.

* Unique Gurantee

  If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

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

Answer: C

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

NEW QUESTION 2
- (Exam Topic 1)
A 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 3
- (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 4
- (Exam Topic 1)
An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

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

Answer: B

Explanation:
EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. References:
➢ CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops The review yielded the following results.
• The exception process and policy have been correctly followed by the majority of users
• A small number of users did not create tickets for the requests but were granted access
• All access had been approved by supervisors.
• Valid requests for the access sporadically occurred across multiple departments.
• Access, in most cases, had not been removed when it was no longer needed
Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

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

Answer: A

Explanation:
According to the CompTIA Security+ SY0-601 documents, the correct answer option is A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval12.
This option ensures that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame by requiring supervisors to approve or deny the exceptions on a regular basis. It also reduces the manual workload of the security team and improves the compliance with the company policy.

NEW QUESTION 7
- (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 company site com
Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

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

Answer: D

Explanation:
The company can use a wildcard certificate to secure its website if it is concerned with convenience and cost. A wildcard certificate can secure multiple subdomains, which makes it cost-effective and convenient for securing the various registered domains.
The retail company should use a wildcard certificate if it is concerned with convenience and c1o2s.tA wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (*) in the domain name field, and can secure multiple subdomains of the primary domain1

NEW QUESTION 8
- (Exam Topic 1)
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:

A. privilege escalation
B. footprinting
C. persistence
D. pivoting.

Answer: D

Explanation:
The technique of gaining access to a dual-homed multifunction device and then gaining shell access on another networked asset is an example of pivoting.

References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Enumeration and Penetration Testing

NEW QUESTION 9
- (Exam Topic 1)
A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

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

Answer: B

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

NEW QUESTION 10
- (Exam Topic 1)
A Chief Information Officer is concerned about employees using company-issued laptops lo 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 10
- (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 12
- (Exam Topic 1)
A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system Which of the following would be BEST suited for this task?

A. Social media analysis
B. Annual information security training
C. Gamification
D. Phishing campaign

Answer: D

Explanation:
A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

NEW QUESTION 17
- (Exam Topic 1)
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO
B. MFA

C. PKI
D. OLP

Answer: A

Explanation:
Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one. References:
> CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls.
> CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

NEW QUESTION 22
- (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 24
- (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 28
- (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 32
- (Exam Topic 1)
A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

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

Answer: C

Explanation:
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

NEW QUESTION 33
- (Exam Topic 1)
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

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

Answer: A

Explanation:
PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data1. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet1.
One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for2. The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org2. A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org2.
Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used3. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years3. The validity period can be checked by looking at the valid from and valid to dates on the certificate3.
Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org2. It also has a validity period of one year, which means it needs to be rotated annually3.

NEW QUESTION 34
- (Exam Topic 1)
Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

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

Answer: B

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

NEW QUESTION 36
- (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 37
- (Exam Topic 1)
A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

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

Answer: A

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

NEW QUESTION 39
- (Exam Topic 1)
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

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

Answer: A

Explanation:
Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.
References:
> CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2

NEW QUESTION 42
- (Exam Topic 1)
An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

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

Answer: B

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

NEW QUESTION 46
- (Exam Topic 1)
The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

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

Answer: A

Explanation:
Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

NEW QUESTION 48
- (Exam Topic 1)
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

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

Answer: D

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

NEW QUESTION 52
- (Exam Topic 1)
A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

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

Answer: C

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

NEW QUESTION 54
- (Exam Topic 1)
A security 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 56
- (Exam Topic 1)
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

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

Answer: D

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

NEW QUESTION 60
- (Exam Topic 1)
Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

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

Answer: A

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

NEW QUESTION 64
- (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 65
- (Exam Topic 1)
Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

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

Answer: D

Explanation:
Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 99-102.

NEW QUESTION 66
- (Exam Topic 1)
A Chief Information Security Officer (CISO) is evaluating (he dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system, selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system Which of the following is the CISO using to evaluate Hie environment for this new ERP system?

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

Answer: C

Explanation:
The CISO is using the NIST Risk Management Framework (RMF) to evaluate the environment for the new ERP system. The RMF is a structured process for managing risks that involves categorizing the system, selecting controls, implementing controls, assessing controls, and authorizing the system.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 4: Risk Management, pp. 188-191.

NEW QUESTION 68
- (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 69
- (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 72
- (Exam Topic 1)
Which of the following biometric authentication methods is the MOST accurate?

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

Answer: B

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

NEW QUESTION 75
- (Exam Topic 1)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

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

Answer: C

Explanation:
Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/what-is-phishing

NEW QUESTION 77
- (Exam Topic 1)
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:
• All users share workstations throughout the day.
• Endpoint protection was disabled on several workstations throughout the network.
• Travel times on logins from the affected users are impossible.
• Sensitive data is being uploaded to external sites.
• All user account passwords were forced to be reset and the issue continued. Which of the following attacks is being used to compromise the user accounts?

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

Answer: B

Explanation:
The symptoms suggest a keylogger is being used to compromise the user accounts, allowing the attackers to obtain the users' passwords and other sensitive information. References:
➤ CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION 82
- (Exam Topic 1)
A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

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

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

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

Answer: D

Explanation:
Input sanitization can help prevent attackers from learning the service account name by removing potentially harmful characters from user input, reducing the likelihood of successful injection attacks. References:
➢ CompTIA Security+ Certification Exam Objectives 2.2: Given a scenario, implement secure coding techniques.
➢ CompTIA Security+ Study Guide, Sixth Edition, pages 72-73

NEW QUESTION 86
- (Exam Topic 1)
A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?

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

Answer: B

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

NEW QUESTION 90
- (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 92
- (Exam Topic 1)
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

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

Answer: D

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

NEW QUESTION 96
- (Exam Topic 1)
Which of the following identifies the point in time when an organization will recover data in the event of an outage?

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

Answer: B

Explanation:

Detailed
Recovery Point Objective (RPO) is the maximum duration of time that an organization can tolerate data loss in the event of an outage. It identifies the point in time when data recovery must begin, and any data loss beyond that point is considered unacceptable.
Reference: CompTIA Security+ Certification Guide, Exam SY0-601 by Mike Chapple and David Seidl, Chapter-7: Incident Response and Recovery, Objective 7.2: Compare and contrast business continuity and disaster recovery concepts, pp. 349-350.

NEW QUESTION 100
- (Exam Topic 1)
A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

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

Answer: D

Explanation:
A SIEM is a security solution that helps detect security incidents by monitoring for notable events across the enterprise. A detective control is a control that is designed to detect security incidents and respond to them. Therefore, a SIEM represents a detective control.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 102
- (Exam Topic 1)
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

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

Answer: E

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

NEW QUESTION 103
- (Exam Topic 1)
Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area? (Select TWO).

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

Answer: AD

Explanation:
Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area.
References:
➤ CompTIA Security+ Study Guide Exam SY0-601, Chapter 7

NEW QUESTION 105
- (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 HIIPS 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. ASSLILS 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 106
- (Exam Topic 1)
A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices Which of the following is a cost-effective approach to address these concerns?

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

Answer: D

Explanation:
a backup strategy is a plan that defines how to protect data from loss or corruption by creating and storing copies of data on a different medium or location1. A backup strategy should consider the security and reliability of the backup data and the backup storage234.
Based on these definitions, the best option that is a cost-effective approach to address the security and reliability concerns regarding the on-site backup strategy would be D. Migrate to a cloud backup solutio2n4. A cloud backup solution can provide several benefits, such as:
> Enhanced physical security of the backup data by storing it in a remote location that is protected by multiple layers of security measures.
> Enhanced durability of the backup data by storing it on highly reliable storage devices that are replicated across multiple availability zones or regions.
> Reduced costs of backup storage by paying only for the amount of data stored and transferred, and by using features such as compression, deduplication, encryption, and lifecycle management.
> Increased flexibility and scalability of backup storage by choosing from various storage classes and tiers that match the performance and availability requirements of the backup data.

NEW QUESTION 107
- (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 108
- (Exam Topic 1)
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

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

Answer: CE

Explanation:
Network access control (NAC) is a technique that restricts access to a network based on the identity, role, device, location, or other criteria of the users or devices. NAC can prevent unauthorized or malicious devices from connecting to a network and accessing sensitive data or resources.
Guards are physical security personnel who monitor and control access to a facility. Guards can prevent unauthorized or malicious individuals from entering a facility and plugging in a remotely accessible device.

NEW QUESTION 111
- (Exam Topic 1)
After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session
Which of the following types of attacks has occurred?

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

Answer: A

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

NEW QUESTION 116
- (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 118
- (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 inspectio3n45, 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 120
- (Exam Topic 1)
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD

Answer: CD

Explanation:
In a forensic investigation, volatile data should be collected first, based on the order of volatility. RAM and Cache are examples of volatile data. References: CompTIA Security+ Study Guide 601, Chapter 11

NEW QUESTION 122
- (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 123
- (Exam Topic 1)
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the nsk of lateral spread and the risk that the adversary would notice any changes?

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

Answer: C

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

NEW QUESTION 126
- (Exam Topic 1)
Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

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

Answer: C

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

NEW QUESTION 128
- (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 133
- (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 phon1e.

NEW QUESTION 137
- (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 140
- (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 144
- (Exam Topic 1)
A company would like to set up a secure way to transfer data between users via their mobile phones The company's top pnonty is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?

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

Answer: B

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

NEW QUESTION 148
- (Exam Topic 1)
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

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

Answer: A

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

NEW QUESTION 152

- (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 154
- (Exam Topic 1)
A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPB, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate but have been Which of the following statements BEST explains the issue?

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

Answer: D

NEW QUESTION 156
- (Exam Topic 1)
A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?

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

Answer: A

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

NEW QUESTION 161
- (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 hitps://;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 164
- (Exam Topic 1)
Which of the following roles would MOST likely have direct access to the senior management team?

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

Answer: C

Explanation:
A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders.
A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.

The other options are not correct because:

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

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

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

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

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

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

NEW QUESTION 166
- (Exam Topic 1)
A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

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

Answer: B

Explanation:
To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

NEW QUESTION 169
- (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 173
- (Exam Topic 1)
The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

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

Answer: B

Explanation:
The solution that the CISO should choose is Next-generation Secure Web Gateway (SWG), which provides URL filtering and categorization to prevent users from accessing malicious sites, even when they are away from the office. NGFWs are typically cloud-based and offer multiple security layers, including malware detection, intrusion prevention, and data loss prevention. References:
> CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION 175
- (Exam Topic 1)
The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

A. Authentication protocol
B. Encryption type

C. WAP placement
D. VPN configuration

Answer: C

Explanation:
WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.
WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:

Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.

Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.

Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

NEW QUESTION 176
- (Exam Topic 1)
Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft
B. Data loss
C. Data exfiltration
D. Reputation

Answer: D

Explanation:
The best option that describes what is impacted the most by the hackers' attack and threat would be D. Reputation. Reputation is the perception or opinion that others have about a person or an organization. Reputation can affect the trust, credibility, and success of a person or an organization. In this scenario, if the hackers send the unfavorable pictures to the press, it can damage the reputation of the Chief Executive Officer and the company, and cause negative consequences such as loss of customers, partners, investors, or employees.

NEW QUESTION 179
- (Exam Topic 1)
A company recently experienced an attack during which 5 main website was directed to the atack-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 182
- (Exam Topic 1)
A security engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks. Which of the following should the engineer implement?

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

Answer: D

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

NEW QUESTION 185
- (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 189
- (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 191
- (Exam Topic 1)
Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?

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

Answer: A

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

NEW QUESTION 193
- (Exam Topic 1)
An employee's company account was used in a data breach Interviews with the employee revealed:
• The employee was able to avoid changing passwords by using a previous password again.
• The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.
Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)

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

Answer: CF

Explanation:
two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofenc1in2g. Password history is a feature that prevents users from reusing their previous passwords1. This can enhance password security by forcing users to create new and unique passwords periodically1. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords1.
Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device2. This can enhance security by preventing unauthorized access from hostile or foreign region2s. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

NEW QUESTION 196
- (Exam Topic 1)
The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific

person. Which of the following would BEST allow this objective to be met?

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

Answer: D

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

NEW QUESTION 198
- (Exam Topic 1)
A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?

A. MAC address filtering
B. 802.1X
C. Captive portal
D. WPS

Answer: D

Explanation:
The network analyst should enable Wi-Fi Protected Setup (WPS) to allow users to connect to the wireless access point securely without having to remember passwords. WPS allows users to connect to a wireless network by pressing a button or entering a PIN instead of entering a password.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4: Identity and Access Management

NEW QUESTION 202
- (Exam Topic 1)
The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

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

Answer: C

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

NEW QUESTION 205
- (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 FDE123. 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 data3. 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 208
- (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 211
- (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 212
- (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 213
- (Exam Topic 1)
An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box
B. Red-leam
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 218
- (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 219
- (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 221
- (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 225
- (Exam Topic 2)
The application development teams have been asked to answer the following questions:
- Does this application receive patches from an external source?
- Does this application contain open-source code?
- Is this application accessible by external users?
- Does this application meet the corporate password standard? Which of the following are these questions part of?

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

Answer: A

Explanation:
A risk control self-assessment (RCSA) is a process that allows an organization to identify, evaluate, and mitigate the risks associated with its activities, processes, systems, and products. A RCSA involves asking relevant questions to assess the effectiveness of existing controls and identify any gaps or weaknesses that need improvement. A RCSA also helps to align the risk appetite and tolerance of the organization with its strategic objectives and performance.
The application development teams have been asked to answer questions related to their applications' security posture, such as whether they receive patches from an external source, contain open-source code, are accessible by external users, or meet the corporate password standard. These questions are part of a RCSA process that aims to evaluate the potential risks and vulnerabilities associated with each application and determine how well they are managed and mitigated.

NEW QUESTION 227
- (Exam Topic 2)
An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding credit card statement with unusual purchases. Which of the following attacks took place?

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

Answer: A

Explanation:
An on-path attack is an attack that took place when an attacker was eavesdropping on a user who was shopping online and was able to spoof the IP address associated with the shopping site. An on-path attack is a type of network attack that involves intercepting or modifying traffic between two parties by placing

oneself in the communication path. An on-path attack can also be called a man-in-the-middle attack or a session hijacking attack. An on-path attacker can steal sensitive information, such as credit card details, or redirect the user to a malicious website. References: https://www.comptia.org/blog/what-is-a-man-in-the-middle-attack
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 230
- (Exam Topic 2)
A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?

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

Answer: C

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

NEW QUESTION 234
- (Exam Topic 2)
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?

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

Answer: B

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

NEW QUESTION 238
- (Exam Topic 2)
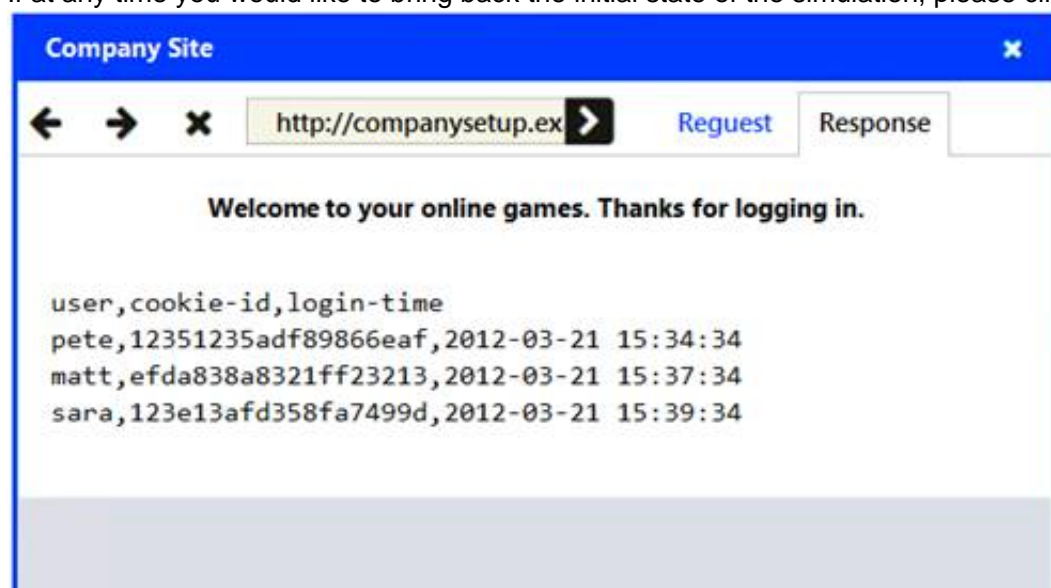An attack has occurred against a company.
INSTRUCTIONS
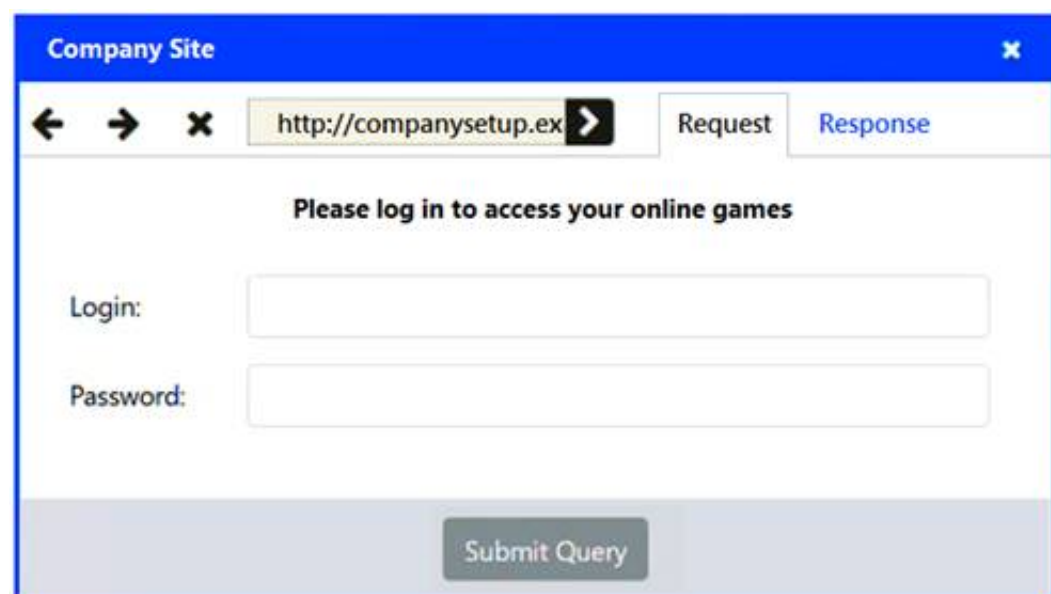You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).
Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.
(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Company Site ✖

← → ✖ | http://companysetup.ex ▶ | Request Response

Please log in to access your online games

Login: [_____]

Password: [_____]

[Submit Query]

Select and Place:

Answer Area 1

SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking

Type of attack
(?)

Answer Area 2
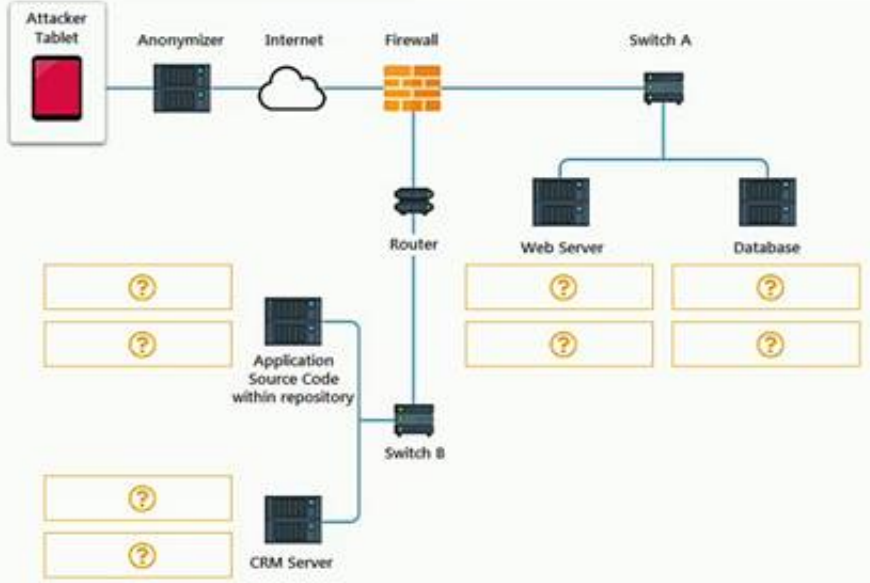
Input Validation
Code Review
WAF
URL Filtering
Record level access control

Attacker Tablet — Anonymizer — Internet — Firewall — Switch A

Router — Web Server — Database

Application Source Code within repository

Switch B

CRM Server

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 241
- (Exam Topic 2)
A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.
B. remove the single point of failure.
C. cut down the mean time to repair
D. reduce the recovery time objective

Answer: B

Explanation:
A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

NEW QUESTION 246
- (Exam Topic 2)
Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

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

Answer: C

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

NEW QUESTION 249
- (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 254
- (Exam Topic 2)
Which Of the following is a primary security concern for a setting up a BYOD program?

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

Answer: D

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

NEW QUESTION 258
- (Exam Topic 2)
Recent changes to a company's BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

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

Answer: A

Explanation:
Facial recognition is a type of biometric authentication that uses the unique features of a person's face to verify their identity. Facial recognition is not something you know or have, but something you are, which is one of the three factors of authentication. Facial recognition can use various methods and technologies, such as 2D or 3D images, infrared sensors, machine learning and more, to capture, analyze and compare facial data. Facial recognition can provide a convenient and secure way to authenticate users on personal mobile devices, as it does not require any additional hardware or input from the user. Facial recognition can also be used in conjunction with other factors, such as passwords or tokens, to provide multi-factor authentication. Verified References:
➢ Biometrics - SY0-601 CompTIA Security+ : 2.4 - Professor Messer IT Certification Training Courses https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/biometrics/ (See Facial Recognition)
➢ Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 2: Architecture and Design, Objective 2.4: Given a scenario, implement identity and access management controls.)
➢ Biometric and Facial Recognition - CompTIA Security+ Certification (SY0-501) https://www.oreilly.com/library/view/comptia-security-certification/9781789953091/video9_6.html (See Biometric and Facial Recognition)

NEW QUESTION 261
- (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 263
- (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.pd

NEW QUESTION 266
- (Exam Topic 2)
A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

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

Answer: C

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

NEW QUESTION 267
- (Exam Topic 2)
A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?

A. Compensating controls
B. Directive control
C. Mitigating controls
D. Physical security controls

Answer: C

Explanation:
Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.
In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure123. Removable media threats can be used to bypass network defenses and target industrial/OT environments2. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.
Some examples of mitigating controls for removable media threats are:
> Encrypting data on removable media
> Scanning removable media for malware before use
> Restricting access to removable media ports
> Implementing policies and procedures for removable media usage and disposal
> Educating users on the risks and best practices of removable media

NEW QUESTION 272
- (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 277
- (Exam Topic 2)
A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.
Which of the following would provide the best proof that customer data is being protected?

A. SOC2
B. CSA
C. CSF
D. 1SO 31000

Answer: A

Explanation:
SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider1
https://www.csagroup.org/store/product/50072454/ 3: https://www.csagroup.org/store/product/50072454os/ 1: https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

NEW QUESTION 278
- (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 281
- (Exam Topic 2)
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

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

Answer: A

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

NEW QUESTION 283
- (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 288
- (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 292
- (Exam Topic 2)
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

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

Answer: AB

Explanation:
Geolocation and time-of-day restrictions would be best to mitigate the CEO's concerns about staff members working from high-risk countries while on holiday or outsourcing work to a third-party organization in another country. Geolocation is a technique that involves determining the physical location of a device or user based on its IP address, GPS coordinates, Wi-Fi signals, or other indicators. Time-of-day restrictions are policies that limit the access or usage of resources based on the time of day or week. Geolocation and time-of-day restrictions can help to enforce access control rules, prevent unauthorized access, detect anomalous behavior, and comply with regulations. References: https://www.comptia.org/blog/what-is-geolocation
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 295
- (Exam Topic 2)
A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

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

Answer: B

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

NEW QUESTION 299
- (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 303
- (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 308
- (Exam Topic 2)
A security team will be outsourcing several key functions to a third party and will require that:
• Several of the functions will carry an audit burden.
• Attestations will be performed several times a year.
• Reports will be generated on a monthly basis.
Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

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

Answer: C

Explanation:
A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.
Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968
CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558
Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

NEW QUESTION 313
......

Relate Links

100% Pass Your SY0-701 Exam with Exambible Prep Materials

https://www.exambible.com/SY0-701-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/