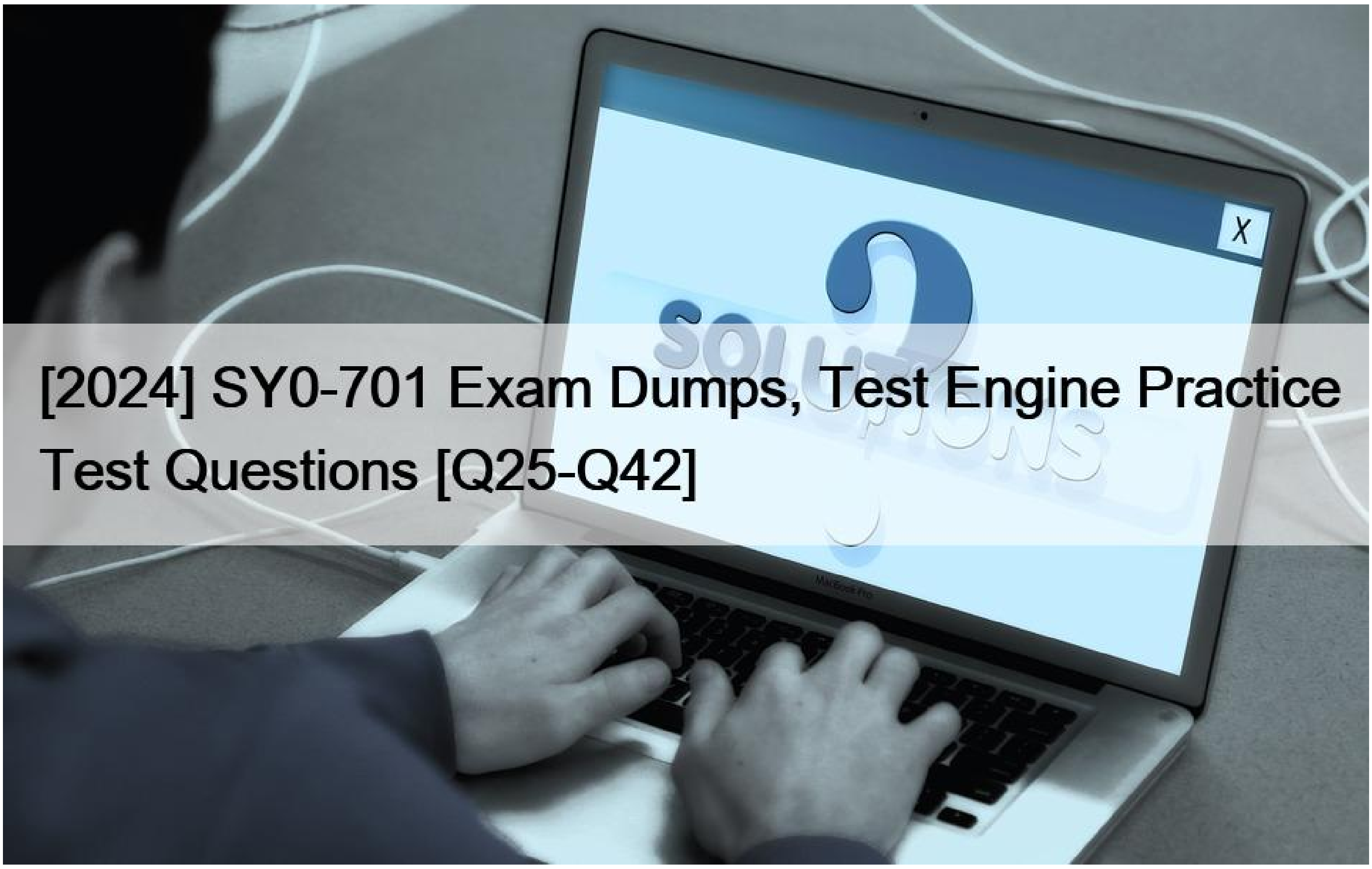
[2024 SY0-701 Exam Dumps, Test Engine Practice Test Questions [Q25-Q42


[2024] SY0-701 Exam Dumps, Test Engine Practice Test Questions [Q25-Q42]
SOLUTIONS

[2024] SY0-701 Exam Dumps, Test Engine Practice Test Questions
Pass SY0-701 exam [Mar 26, 2024] Updated 158 Questions

QUESTION 25

An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?
* Partially known environment
* Unknown environment
* Integrated
* Known environment
A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the devicetype. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test1.

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

QUESTION 26

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&#8217;s intranet account? (Select two).
* Federation
* Identity proofing
* Password complexity
* Default password changes
* Password manager
* Open authentication
Explanation

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user&#8217;s credentials and provides them to the requested resources or services without exposing them.

Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and

312-313 1

QUESTION 27

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?
* Secure cookies
* Version control
* Input validation
* Code signing
Explanation

Input validation is a technique that checks the user input for any malicious or unexpected data before processing it by the web application. Input validation can prevent cross-site scripting (XSS) attacks, which exploit the vulnerability of a web application to execute malicious scripts in the browser of a victim. XSS attacks can compromise the confidentiality, integrity, and availability of the web application and its users.

Input validation can be implemented on both the client-side and the server-side, but server-side validation is more reliable and secure. Input validation can use various methods, such as whitelisting, blacklisting, filtering, escaping, encoding, and sanitizing the input data. References = CompTIA Security+ Study Guide with over

500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 70. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security &#8211; SY0-601 CompTIA Security+ :

3.2

QUESTION 28

Which of the following practices would be best to prevent an insider from introducing malicious code into a company&#8217;s development process?
* Code scanning for vulnerabilities
* Open-source component usage
* Quality assurance testing
* Peer review and approval
Explanation

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543
2

QUESTION 29

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users&#8217; passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?
* Multifactor authentication
* Permissions assignment
* Access management
* Password complexity
Explanation

The correct answer is A because multifactor authentication (MFA) is a method of verifying a user&#8217;s identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user&#8217;s password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication.

Permissions assignment (B) is the process of granting or denying access to resources based on the user&#8217;s role or identity. Access management is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References = You can learn more about multifactor authentication and other security concepts in the following resources:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1 Professor Messer&#8217;s CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2 Multi-factor Authentication &#8211; SY0-601 CompTIA Security+ : 2.43 TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication4 CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

QUESTION 30

Which of the following scenarios describes a possible business email compromise attack?
* An employee receives a gift card request in an email that has an executive&#8217;s name in the display field of the email.
* Employees who open an email attachment receive messages demanding payment in order to access files.

* A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
* An employee receives an email with a link to a phishing site that is designed to look like the company&#8217;s email portal.
Explanation

A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.

In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive&#8217;s name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.

Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority. Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company&#8217;s email portal and capture their credentials. These are all types of cyberattacks, but they are not examples of BEC attacks. References = 1: Business Email Compromise &#8211; CompTIA Security+ SY0-701 &#8211;

2.2 2: CompTIA Security+ SY0-701 Certification Study Guide 3: Business Email Compromise: The 12 Billion Dollar Scam 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

QUESTION 31

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?
* Insider threat
* Email phishing
* Social engineering
* Executive whaling
Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

QUESTION 32

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the followingbestdescribes the user&#8217;s activity?
* Penetration testing
* Phishing campaign
* External audit
* Insider threat
An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner,

who has authorized access to the organization&#8217;s data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization&#8217;s reputation, finances, operations, and legal compliance. The user&#8217;s activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization&#8217;s security policies and compromises the confidentiality and integrity of the data. References = Insider Threats &#8211; CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

QUESTION 33

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO&#8217;s report?
- Insider threat
- Hacktivist
- Nation-state
- Organized crime

Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

QUESTION 34

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?
- MSA
- SLA
- BPA
- ISOW

Explanation

An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objective and outcome.

For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training.

The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations of the partnership. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer&#8217;s CompTIA SY0-701 Security+ Training Course, Section 8.2:

Compliance and Controls, video: Contracts and Agreements (5:12).

QUESTION 35

Which of the following agreement types defines the time frame in which a vendor needs to respond?
* SOW
* SLA
* MOA
* MOU
A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.

References:

Security+ (Plus) Certification | CompTIA IT Certifications, under &#8220;About the exam&#8221;, bullet point 3:

&#8220;Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.&#8221; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: &#8220;Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider.&#8221;

QUESTION 36

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).
* The device has been moved from a production environment to a test environment.
* The device is configured to use cleartext passwords.
* The device is moved to an isolated segment on the enterprise network.
* The device is moved to a different location in the enterprise.
* The device&#8217;s encryption level cannot meet organizational standards.
* The device is unable to receive authorized updates.
An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.

References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671 CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512

QUESTION 37

Which of the following is thebestway to consistently determine on a daily basis whether security settings on servers have been modified?
* Automation
* Compliance checklist
* Attestation

* Manual audit
Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs.

Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise12.

The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:

Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3.

Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis4.

Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting &#8211; CompTIA Security+ SY0-701 &#8211; 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. :

CompTIA Security+ SY0-701 Certification Study Guide, page 99.

QUESTION 38

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?
* Impact analysis
* Scheduled downtime
* Backout plan
* Change management boards
Explanation

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

QUESTION 39

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the followingbestdescribes this step?
* Capacity planning
* Redundancy
* Geographic dispersion
* Tablet exercise
Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization.

Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic.

Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance.

QUESTION 40

A company&#8217;s marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?
* Processor
* Custodian
* Subject
* Owner
According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and responsibility to determine how data is classified, protected, and used.Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.

ReferencesCompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

QUESTION 41

A company&#8217;s end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?
* Concurrent session usage
* Secure DNS cryptographic downgrade
* On-path resource consumption
* Reflected denial of service
Explanation

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim&#8217;s IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

QUESTION 42

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?
* Packet captures
* Vulnerability scans
* Metadata
* Dashboard
Explanation

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria12.

A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors13.

A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14.

Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards &#8211; SY0-601 CompTIA Security+

4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464:

CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

CompTIA SY0-701 Real 2024 Braindumps Mock Exam Dumps: https://www.braindumpsit.com/SY0-701_real-exam.html]