



# 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

Which of the following can best protect against an employee inadvertently installing malware on a company system?

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list

**Answer: D**

#### Explanation:

An application allow list is a security technique that specifies which applications are authorized to run on a system and blocks all other applications. An application allow list can best protect against an employee inadvertently installing malware on a company system because it prevents the execution of any unauthorized or malicious software, such as viruses, worms, trojans, ransomware, or spyware. An application allow list can also reduce the attack surface and improve the performance of the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 551 1

### NEW QUESTION 2

An administrator is reviewing a single server's security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task Category
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:05 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:07 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:09 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:11 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:13 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:15 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:17 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:19 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:21 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:23 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:25 AM	Windows security		
Audit	09/16/2022	Microsoft	4625	Logon
Failure	11:13:27 AM	Windows security		

Which of the following best describes the action captured in this log file?

- A. Brute-force attack
- B. Privilege escalation
- C. Failed password audit
- D. Forgotten password by the user

**Answer: A**

#### Explanation:

A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

### NEW QUESTION 3

Which of the following allows for the attribution of messages to individuals?

- A. Adaptive identity
- B. Non-repudiation
- C. Authentication
- D. Access logs

**Answer: B**

**Explanation:**

Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it.

Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document. References = Non- repudiation – CompTIA Security+ SY0-701 – 1.2, CompTIA Security+ SY0-301: 6.1 – Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

**NEW QUESTION 4**

Which of the following enables the use of an input field to run commands that can view or manipulate data?

- A. Cross-site scripting
- B. Side loading
- C. Buffer overflow
- D. SQL injection

**Answer:** D

**Explanation:**

= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server.

SQL injection is one of the most common and dangerous web application

vulnerabilities. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

**NEW QUESTION 5**

A business received a small grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?

- A. Security of cloud providers
- B. Cost of implementation
- C. Ability of engineers
- D. Security of architecture

**Answer:** D

**Explanation:**

Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud

infrastructure. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 3491

**NEW QUESTION 6**

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

- A. Risk tolerance
- B. Risk transfer
- C. Risk register
- D. Risk analysis

**Answer:** C

**Explanation:**

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks. References = CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification

Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

**NEW QUESTION 7**

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

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

**Answer:** C

**Explanation:**

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the

attacker can bypass the normal execution flow of the application and execute arbitrary commands.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1;  
Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

#### NEW QUESTION 8

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role
- C. Adaptive identity
- D. Threat scope reduction

**Answer:** D

#### Explanation:

The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.

One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.

The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.

References = <https://bing.com/search?q=Zero+Trust+data+plane> <https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>

#### NEW QUESTION 9

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure

**Answer:** D

#### Explanation:

A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network. Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:

? A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.

? A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.

? A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.

? A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.

? A change documentation that records the details and status of the change, as well as the lessons learned and best practices.

? A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.

A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:

? Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.

? Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.

? Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.

? Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.

The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

#### NEW QUESTION 10

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing



D. Peer review and approval

**Answer:** D

**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

**NEW QUESTION 10**

A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network. Which of the following would have mitigated the spread?

- A. IPS
- B. IDS
- C. WAF
- D. UAT

**Answer:** A

**Explanation:**

IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

**NEW QUESTION 14**

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

- A. Clustering servers
- B. Geographic dispersion
- C. Load balancers
- D. Off-site backups

**Answer:** B

**Explanation:**

Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network. Geographic dispersion can also enhance the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption<sup>12</sup>.

The other options are not the best ways to address the company's concern:

? Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system. Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building<sup>3</sup>.

? Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources. Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building<sup>4</sup>.

? Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor

Messer<sup>3</sup>: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

**NEW QUESTION 18**

An organization disabled unneeded services and placed a firewall in front of a business- critical legacy system. Which of the following best describes the actions taken by the organization?

- A. Exception
- B. Segmentation
- C. Risk transfer
- D. Compensating controls

**Answer:** D

**Explanation:**

Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.

References:

? Official CompTIA Security+ Study Guide (SY0-701), page 29

? Security Controls - CompTIA Security+ SY0-701 - 1.1 1

**NEW QUESTION 23**

Which of the following exercises should an organization use to improve its incident response process?

- A. Tabletop

- B. Replication
- C. Failover
- D. Recovery

**Answer:** A

**Explanation:**

A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures. It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

**NEW QUESTION 27**

Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

- A. Hacktivist
- B. Whistleblower
- C. Organized crime
- D. Unskilled attacker

**Answer:** C

**Explanation:**

Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption<sup>12</sup>. References = 1: Threat Actors - CompTIA Security+ SY0-701 - 2.1 2: CompTIA Security+ SY0-701 Certification Study Guide

**NEW QUESTION 30**

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

- A. SIEM
- B. DLP
- C. IDS
- D. SNMP

**Answer:** A

**Explanation:**

SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page 393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

**NEW QUESTION 35**

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

- A. EAP
- B. DHCP
- C. IPSec
- D. NAT

**Answer:** C

**Explanation:**

IPSec is a protocol suite that provides secure communication over IP networks. IPSec can be used to create virtual private networks (VPNs) that encrypt and authenticate the data exchanged between two or more parties. IPSec can also provide data integrity, confidentiality, replay protection, and access control. A security consultant can use IPSec to gain secure, remote access to a client environment by establishing a VPN tunnel with the client's network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 385 1

**NEW QUESTION 39**

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

- A. Private
- B. Critical
- C. Sensitive
- D. Public

**Answer:** C

**Explanation:**

Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical. Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include

marketing materials, press releases, and public web pages.

Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.

Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.

Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.

Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

#### NEW QUESTION 42

A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).

- A. Key escrow
- B. TPM presence
- C. Digital signatures
- D. Data tokenization
- E. Public key management
- F. Certificate authority linking

**Answer:** AB

#### Explanation:

? Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.

? TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication.

#### NEW QUESTION 44

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on jsmith's workstation
- C. An attacker is attempting to brute force jsmith's account.
- D. Ransomware has been deployed in the domain.

**Answer:** C

#### Explanation:

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user jsmith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of jsmith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset jsmith's password, and notify jsmith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+ : 1.1

#### NEW QUESTION 46

Which of the following must be considered when designing a high-availability network? (Select two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

**Answer:** AE

#### Explanation:

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.

Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation. Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to



protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0- 701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652.

#### NEW QUESTION 49

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off\
- B. http://
- C. www.\*.com
- D. :443

**Answer: B**

#### Explanation:

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words “gambling”, “porn”, or “malware” in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.

To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.

The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.\*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol.

:443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page 69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

#### NEW QUESTION 52

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A. Console access
- B. Routing protocols
- C. VLANs
- D. Web-based administration

**Answer: D**

#### Explanation:

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANS). References: CCNA SEC: Router Hardening Your Router's Security Stinks: Here's How to Fix It

#### NEW QUESTION 54

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:

Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are:

? Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.

? Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.

? Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.

? Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.

By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B. Transfer. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

#### NEW QUESTION 55

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A. A thorough analysis of the supply chain
- B. A legally enforceable corporate acquisition policy
- C. A right to audit clause in vendor contracts and SOWs
- D. An in-depth penetration test of all suppliers and vendors

**Answer:** A

#### Explanation:

Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability<sup>12</sup>. Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it<sup>3</sup>. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:

- ? Establishing a trusted relationship with the OEM and authorized resellers
  - ? Requesting documentation and certification of the hardware from the OEM or authorized resellers
  - ? Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components
  - ? Testing the hardware for functionality, performance, and security
  - ? Implementing a tracking system to monitor the hardware throughout its lifecycle
  - ? Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies
- References = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security? Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, : Counterfeit Hardware: The Threat and How to Avoid It

#### NEW QUESTION 57

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

**Answer:** C

#### Explanation:

Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

#### NEW QUESTION 61

A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies. Which of the following is the most important consideration during development?

- A. Scalability
- B. Availability
- C. Cost
- D. Ease of deployment

**Answer:** B

#### Explanation:

Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of-service attacks, and have backup and recovery plans in case of failures<sup>2</sup>.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

#### NEW QUESTION 64

A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

- A. Zero Trust
- B. AAA
- C. Non-repudiation
- D. CIA

**Answer:** A

**Explanation:**

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

References:

? 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.

? 8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

**NEW QUESTION 65**

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

- A. The device has been moved from a production environment to a test environment.
- B. The device is configured to use cleartext passwords.
- C. The device is moved to an isolated segment on the enterprise network.
- D. The device is moved to a different location in the enterprise.
- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

**Answer:** E

**Explanation:**

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

**NEW QUESTION 66**

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 following best describes this step?

- A. Capacity planning
- B. Redundancy
- C. Geographic dispersion
- D. Tablet exercise

**Answer:** A

**Explanation:**

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. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity – SY0-601 CompTIA Security+ : 4.1

**NEW QUESTION 67**

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

**Answer:** A

**Explanation:**

A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls – SY0-601 CompTIA Security+ : 5.1, Security Controls – CompTIA Security+ SY0-501 – 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

**NEW QUESTION 72**

Which of the following involves an attempt to take advantage of database misconfigurations?

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

**Answer:** B

**Explanation:**

SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

**NEW QUESTION 75**

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring trainin
- D. D Implement a phishing campaign

**Answer:** C

**Explanation:**

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

**NEW QUESTION 76**

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?

- A. Packet captures
- B. Vulnerability scans
- C. Metadata
- D. Dashboard

**Answer:** D

**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 criteria<sup>12</sup>.

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 directors<sup>13</sup>.

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 quarter<sup>14</sup>.

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 – 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.

**NEW QUESTION 80**

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?

- A. Impact analysis
- B. Scheduled downtime
- C. Backout plan
- D. Change management boards

**Answer:** B

**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



### NEW QUESTION 81

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

- A. Data masking
- B. Encryption
- C. Geolocation policy
- D. Data sovereignty regulation

**Answer: C**

#### Explanation:

A geolocation policy is a policy that restricts or allows access to data or resources based on the geographic location of the user or device. A geolocation policy can be implemented using various methods, such as IP address filtering, GPS tracking, or geofencing. A geolocation policy can help the company's legal department to prevent unauthorized access to sensitive documents from individuals in high-risk countries<sup>12</sup>.

The other options are not effective ways to limit access based on location:

? Data masking: This is a technique of obscuring or replacing sensitive data with fictitious or anonymized data. Data masking can protect the privacy and confidentiality of data, but it does not prevent access to data based on location<sup>3</sup>.

? Encryption: This is a process of transforming data into an unreadable format using a secret key or algorithm. Encryption can protect the integrity and confidentiality of data, but it does not prevent access to data based on location. Encryption can also be bypassed by attackers who have the decryption key or method<sup>4</sup>.

? Data sovereignty regulation: This is a set of laws or rules that govern the storage, processing, and transfer of data within a specific jurisdiction or country. Data sovereignty regulation can affect the availability and compliance of data, but it does not prevent access to data based on location. Data sovereignty regulation can also vary depending on the country or region.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Account Policies – SY0-601 CompTIA Security+ : 3.7, video by Professor Messer<sup>3</sup>: CompTIA Security+ SY0-701 Certification Study Guide, page 1004: CompTIA Security+ SY0-701 Certification Study Guide, page 101. : CompTIA Security+ SY0-701 Certification Study Guide, page 102.

### NEW QUESTION 82

Which of the following would be the best way to block unknown programs from executing?

- A. Access control list
- B. Application allow list.
- C. Host-based firewall
- D. DLP solution

**Answer: B**

#### Explanation:

An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network<sup>12</sup>.

The other options are not the best ways to block unknown programs from executing:

? Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object. An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing<sup>13</sup>.

? Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing<sup>1</sup>.

? DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing<sup>1</sup>.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting – CompTIA Security+ SY0-701 – 3.5, video by Professor Messer<sup>3</sup>: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

### NEW QUESTION 84

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- A. IDS
- B. ACL
- C. EDR
- D. NAC

**Answer: C**

#### Explanation:

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 256<sup>1</sup>

### NEW QUESTION 86

A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

- A. Logging all NetFlow traffic into a SIEM
- B. Deploying network traffic sensors on the same subnet as the servers
- C. Logging endpoint and OS-specific security logs
- D. Enabling full packet capture for traffic entering and exiting the servers

**Answer:** D

**Explanation:**

Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 372-373

**NEW QUESTION 88**

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. MOA
- B. SOW
- C. MOU
- D. SLA

**Answer:** D

**Explanation:**

A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

**NEW QUESTION 92**

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

- A. Fines
- B. Audit findings
- C. Sanctions
- D. Reputation damage

**Answer:** A

**Explanation:**

PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.

If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.

The other options are not correct because they are not the most likely outcomes if a large bank fails an internal PCI DSS compliance assessment. B. Audit findings. Audit findings are the results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls and recommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself. C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non-compliance. D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: PCI DSS (5:12). PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4. PCI Security Standards Council, PCI DSS FAQs, question 8. PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council], PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question 12. [PCI Security Standards Council], PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council], PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council], PCI DSS FAQs, question 17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council], PCI DSS FAQs, question 19. [PCI Security Standards Council], PCI DSS FAQs, question 20. [PCI Security Standards Council], PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question 22. [PCI Security Standards Council], PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council], PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council], PCI DSS FAQs, question 27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council], PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

**NEW QUESTION 93**

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?

- A. Partially known environment
- B. Unknown environment

- C. Integrated
- D. Known environment

**Answer:** A

**Explanation:**

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 device type. 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 test<sup>1</sup>. References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

**NEW QUESTION 95**

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- B. Orchestration
- C. Baseline
- D. Policy enforcement

**Answer:** B

**Explanation:**

Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457 1

**NEW QUESTION 100**

Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

- A. Provisioning resources
- B. Disabling access
- C. Reviewing change approvals
- D. Escalating permission requests

**Answer:** B

**Explanation:**

Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132.

**NEW QUESTION 104**

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

- A. Preparation
- B. Recovery
- C. Lessons learned
- D. Analysis

**Answer:** A

**Explanation:**

Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.

Some of the activities that a security analyst performs during the preparation phase are:

? Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.

? Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.

? Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.

? Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.

? Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.

? Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.

? Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.

References:

? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4: Secure Systems Design, p. 279-280

? CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16



#### NEW QUESTION 109

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

- A. Partition
- B. Asymmetric
- C. Full disk
- D. Database

**Answer: C**

#### Explanation:

Full disk encryption (FDE) is a technique that encrypts all the data on a hard drive, including the operating system, applications, and files. FDE protects the data from unauthorized access in case the laptop is lost, stolen, or disposed of without proper sanitization. FDE requires the user to enter a password, a PIN, a smart card, or a biometric factor to unlock the drive and boot the system. FDE can be implemented by using software solutions, such as BitLocker, FileVault, or VeraCrypt, or by using hardware solutions, such as self-encrypting drives (SEDs) or Trusted Platform Modules (TPMs). FDE is a recommended encryption technique for laptops and other mobile devices that store sensitive data.

Partition encryption is a technique that encrypts only a specific partition or volume on a hard drive, leaving the rest of the drive unencrypted. Partition encryption is less secure than FDE, as it does not protect the entire drive and may leave traces of data on unencrypted areas. Partition encryption is also less convenient than FDE, as it requires the user to mount and unmount the encrypted partition manually.

Asymmetric encryption is a technique that uses a pair of keys, one public and one private, to encrypt and decrypt data. Asymmetric encryption is mainly used for securing communication, such as email, web, or VPN, rather than for encrypting data at rest. Asymmetric encryption is also slower and more computationally intensive than symmetric encryption, which is the type of encryption used by FDE and partition encryption.

Database encryption is a technique that encrypts data stored in a database, such as tables, columns, rows, or cells. Database encryption can be done at the application level, the database level, or the file system level. Database encryption is useful for protecting data from unauthorized access by database administrators, hackers, or malware, but it does not protect the data from physical theft or loss of the device that hosts the database. References = Data Encryption – CompTIA Security+ SY0-401: 4.4, CompTIA Security+Cheat Sheet and PDF | Zero To Mastery, CompTIA Security+ SY0-601 Certification Course – Cybr, Application Hardening – SY0-601 CompTIA Security+ : 3.2.

#### NEW QUESTION 110

##### HOTSPOT

You are security administrator investigating a potential infection on a network.

Click on each host and firewall. Review all logs to determine which host originated the Infecton and then deny each remaining hosts clean or infected.

192.168.10.22

4/17/2019 14:30 Info Scheduled scan initiated

4/17/2019 14:31 Info Checking for update

4/17/2019 14:32 Info No update available

4/17/2019 14:33 Info Checking for definition update

4/17/2019 14:34 Info No definition update available

4/17/2019 14:35 Info Scan type = full

4/17/2019 14:36 Info Scan start

4/17/2019 14:37 Info Scanning system files

4/17/2019 14:38 Info Scanning temporary files

4/17/2019 14:39 Info Scanning services

4/17/2019 14:40 Info Scanning boot sector

4/17/2019 14:41 Info Scan complete

4/17/2019 14:42 Info Files removed: 0

4/17/2019 14:43 Info Files quarantined: 0

4/17/2019 14:44 Info Boot sector: clean

4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30

4/18/2019 2:31 Warn Scheduled scan disabled by process svch0st.exe

4/18/2019 2:32 Warn Scheduled update disabled by process scvh0st.exe



192.168.10.37



```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
```

192.168.10.41



```
4/17/2019 14:30 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

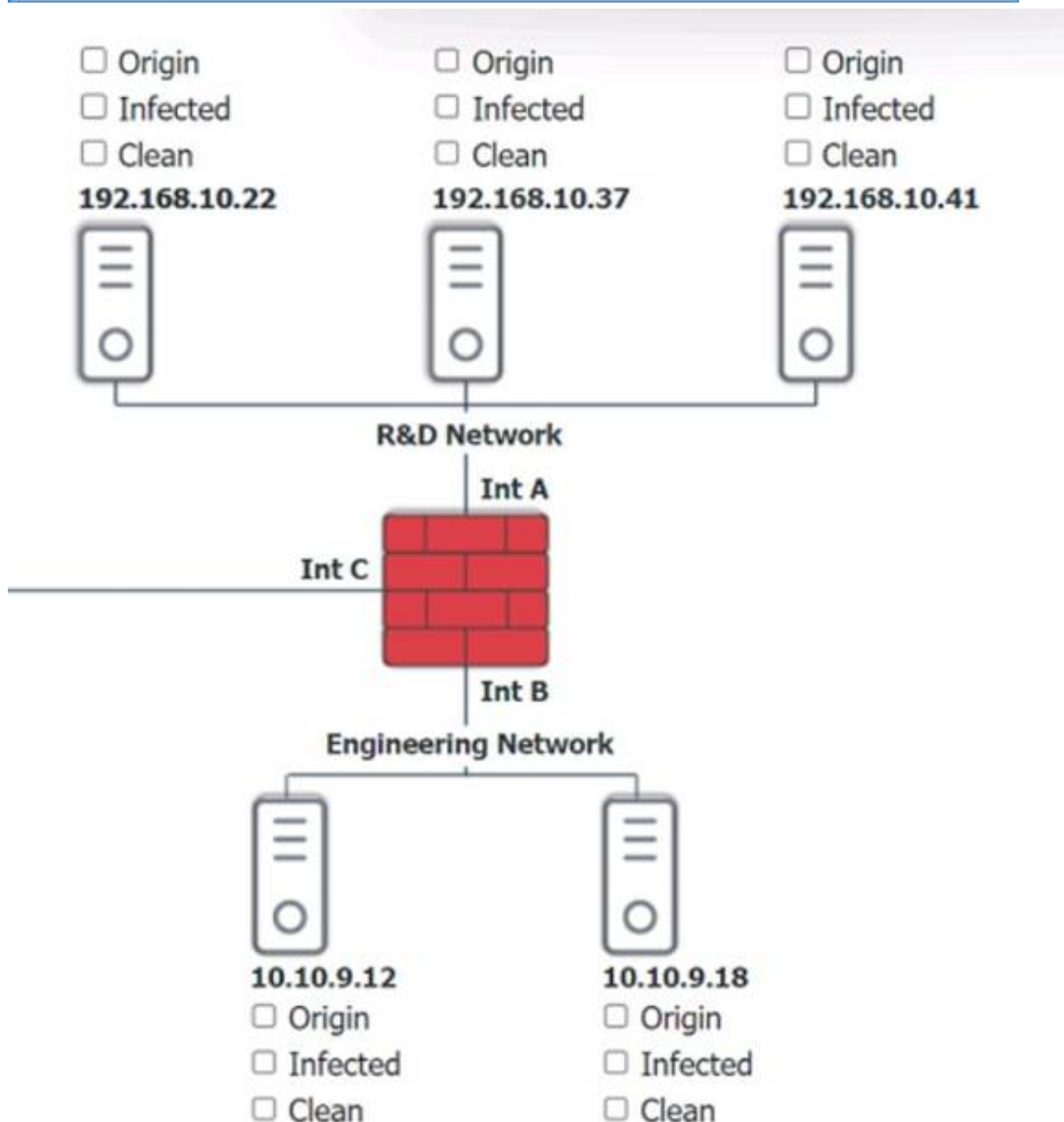
Firewall							
Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

10.10.9.12		
4/17/2019 14:30	Info	Scheduled scan initiated
4/17/2019 14:31	Info	Checking for update
4/17/2019 14:32	Info	No update available
4/17/2019 14:33	Info	Checking for definition update
4/17/2019 14:34	Info	No definition update available
4/17/2019 14:35	Info	Scan type = full
4/17/2019 14:36	Info	Scan start
4/17/2019 14:37	Info	Scanning system files
4/17/2019 14:38	Info	Scanning temporary files
4/17/2019 14:39	Info	Scanning services
4/17/2019 14:40	Info	Scanning boot sector
4/17/2019 14:41	Info	Scan complete
4/17/2019 14:42	Info	Files removed: 0
4/17/2019 14:43	Info	Files quarantined: 0
4/17/2019 14:44	Info	Boot sector: clean
4/17/2019 14:45	Info	Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30	Info	Scheduled scan initiated
4/18/2019 14:31	Info	Checking for update
4/18/2019 14:32	Info	No update available
4/18/2019 14:33	Info	Checking for definition update
4/18/2019 14:34	Info	Update available v10.2.3.4440
4/18/2019 14:33	Info	Downloading update
4/18/2019 14:35	Info	Definition update complete
4/18/2019 14:35	Info	Scan type = full
4/18/2019 14:36	Info	Scan start
4/18/2019 14:37	Info	Scanning system files
4/18/2019 14:37	Warn	File found svchost.exe match definition v10.2.3.4440
4/18/2019 14:37	Warn	File quarantined svchost.exe
4/18/2019 14:38	Info	Scanning temporary files
4/18/2019 14:39	Info	Scanning services



```

10.10.9.18
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svchost.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svchost.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
    
```



- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Based on the logs, it seems that the host that originated the infection is 192.168.10.22. This host has a suspicious process named svchost.exe running on port 443, which is unusual for a Windows service. It also has a large number of outbound connections to different IP addresses on port 443, indicating that it is part of a

botnet.

The firewall log shows that this host has been communicating with 10.10.9.18, which is another infected host on the engineering network. This host also has a suspicious process named svchost.exe running on port 443, and a large number of outbound connections to different IP addresses on port 443. The other hosts on the R&D network (192.168.10.37 and 192.168.10.41) are clean, as they do not have any suspicious processes or connections.

#### NEW QUESTION 113

A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

- A. Set the maximum data retention policy.
- B. Securely store the documents on an air-gapped network.
- C. Review the documents' data classification policy.
- D. Conduct a tabletop exercise with the team.

**Answer: D**

#### Explanation:

A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

#### NEW QUESTION 116

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, ;, &, ` , and ? from variables set by forms in a web application. Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- A. Identify embedded keys
- B. Code debugging
- C. Input validation
- D. Static code analysis

**Answer: C**

#### Explanation:

Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as \$, |, ;, &, ` , and ? , can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.

Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security – SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

#### NEW QUESTION 117

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Segmentation
- B. Isolation
- C. Hardening
- D. Decommissioning

**Answer: C**

#### Explanation:

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats. One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:

? Applying patches and updates to the operating system and the application, if available

? Removing or disabling unnecessary services, features, or accounts

? Configuring firewall rules and network access control lists to restrict inbound and outbound traffic

? Enabling encryption and authentication for data transmission and storage

? Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity

? Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible. References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems



#### NEW QUESTION 122

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request.
- D. Apply the patch to the system.

**Answer: C**

#### Explanation:

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

#### NEW QUESTION 125

A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

- A. Certification
- B. Inventory list
- C. Classification
- D. Proof of ownership

**Answer: A**

#### Explanation:

The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel

involved. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

#### NEW QUESTION 127

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

- A. RBAC
- B. ACL
- C. SAML
- D. GPO

**Answer: A**

#### Explanation:

RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

#### NEW QUESTION 130

Which of the following is the most likely to be included as an element of communication in a security awareness program?

- A. Reporting phishing attempts or other suspicious activities
- B. Detecting insider threats using anomalous behavior recognition
- C. Verifying information when modifying wire transfer data
- D. Performing social engineering as part of third-party penetration testing

**Answer: A**

#### Explanation:

A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.

The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that

involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external security professionals or consultants, and it does not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question. References = Security Awareness and Training –

CompTIA Security+ SY0-701: 5.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 263.

#### NEW QUESTION 135

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.

SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

- A. [Digital forensics
- B. E-discovery
- C. Incident response
- D. Threat hunting

**Answer: D**

#### Explanation:

Threat hunting is the process of proactively searching for signs of malicious activity or compromise in a network, rather than waiting for alerts or indicators of compromise (IOCs) to appear. Threat hunting can help identify new tactics, techniques, and procedures (TTPs) used by malicious actors, as well as uncover hidden or stealthy threats that may have evaded detection by security tools. Threat hunting requires a combination of skills, tools, and methodologies, such as hypothesis generation, data

collection and analysis, threat intelligence, and incident response. Threat hunting can also help improve the security posture of an organization by providing feedback and recommendations for security improvements. References = CompTIA Security+ Certification Exam Objectives, Domain 4.1: Given a scenario, analyze potential indicators of malicious activity. CompTIA Security+ Study Guide (SY0-701), Chapter 4: Threat Detection and Response, page 153. Threat Hunting – SY0-701 CompTIA Security+ : 4.1, Video 3:18. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 3.

#### NEW QUESTION 140

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Non-repudiation

**Answer: C**

#### Explanation:

Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non-repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

#### NEW QUESTION 145

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, 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?

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption
- D. Reflected denial of service

**Answer: D**

#### 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'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

#### NEW QUESTION 147

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:

"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

- A. Cancel current employee recognition gift cards.
- B. Add a smishing exercise to the annual company training.
- C. Issue a general email warning to the company.
- D. Have the CEO change phone numbers.

- E. Conduct a forensic investigation on the CEO's phone.
- F. Implement mobile device management.

**Answer:** BC

**Explanation:**

This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money. References = What Is Phishing | Cybersecurity | CompTIA, Phishing – SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

**NEW QUESTION 149**

An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

- A. Deploying a SASE solution to remote employees
- B. Building a load-balanced VPN solution with redundant internet
- C. Purchasing a low-cost SD-WAN solution for VPN traffic
- D. Using a cloud provider to create additional VPN concentrators

**Answer:** A

**Explanation:**

SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457-458 1

**NEW QUESTION 150**

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

- A. Segmentation
- B. Isolation
- C. Patching
- D. Encryption

**Answer:** A

**Explanation:**

Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

**NEW QUESTION 153**

After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test: `nmap -p 23 192.168.14.6 --script telnet-encryption` PORT STATE SERVICE REASON

23/tcp open telnet syn-ack I telnet encryption:

| \_ Telnet server supports encryption

Which of the following would the security analyst conclude for this reported vulnerability?

- A. It is a false positive.
- B. A rescan is required.
- C. It is considered noise.
- D. Compensating controls exist.

**Answer:** A

**Explanation:**

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly. References: 3: Telnet Protocol - Can You Encrypt Telnet?

**NEW QUESTION 154**

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

- A. Active
- B. Passive
- C. Defensive
- D. Offensive

**Answer:** A

**Explanation:**

Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information. References = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

**NEW QUESTION 157**

A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

- A. Attribute-based
- B. Time of day
- C. Role-based
- D. Least privilege

**Answer:** D

**Explanation:**

The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

**NEW QUESTION 162**

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A. IRP
- B. DRP
- C. RPO
- D. SDLC

**Answer:** B

**Explanation:**

A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:

? A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.

? A business impact analysis that prioritizes the recovery of the most essential functions and data.

? A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.

? A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss.

References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

**NEW QUESTION 167**

A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).

- A. Private
- B. Confidential
- C. Public
- D. Operational
- E. Urgent
- F. Restricted

**Answer:** BF

**Explanation:**

Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following1:

? Public: Data that can be freely disclosed to anyone without any harm or risk.

? Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

? Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.

? Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.

In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2. References: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

**NEW QUESTION 172**



.....

## Relate Links

**100% Pass Your SY0-701 Exam with Examible 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/>