



**CertsMania**

# Free Questions for **SY0-701**

Shared by **Marisol** on **Apr 13, 2025**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**



**CertsMania**

## Questions # 1:

An administrator is reviewing a single server's security logs and discovers the following;  
Which of the following best describes the action captured in this log file?

### Options:

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



CertsMania

### 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

## Questions # 2:

A security analyst is creating the first draft of a network diagram for the company's new customer-facing payment application that will be hosted by a third-party cloud service

provider.

>

>

**Options:**

**Answer**

Answer:

See the Explanation for complete solution for this task.

**Explanation**

>A diagram of a computer AI-generated content may be incorrect.

Step 1: Understand Requirements & Security Principles

Requirements:

Customer-facing payment application (PCI DSS compliance applies)

Hosted on third-party cloud (e.g., AWS)

Must segment public-facing and internal resources

Needs to be scalable and resilient

Must have strong security controls

Step 2: Design the High-Level Network Layout

Core Components:

VPC (Virtual Private Cloud): Isolates your environment from other tenants in the cloud.

Subnets:

Public subnet: For resources that must communicate with the internet.

Private subnet: For internal resources, NOT directly exposed to the internet.

Step 3: Place Resources in Appropriate Subnets

Public Subnet:

Internet-facing Load Balancer (LB): Distributes traffic to application servers.

Web Application Firewall (WAF): Protects against web exploits.

Autoscaling Instances: EC2 (or VM) servers running your web front-end, automatically scaling as traffic grows.

Private Subnet:

Application servers: Back-end logic, not exposed to internet directly.

Database: Sensitive data storage, only accessible by application servers.

Internal Load Balancer: Manages traffic among app servers.

WAF: Can be used internally as well for defense-in-depth.

Step 4: Add Connectivity and Security Controls

Internet Gateway: Allows resources in public subnet to communicate with the internet.

NAT Gateway: Allows outbound internet traffic from private subnet without exposing private IPs.

Security Groups: Firewalls at the instance level; allow only necessary traffic (e.g., LB to web server, web server to DB).

Network ACLs: Subnet-level firewalls for additional control.

Step 5: Network Diagram Explanation (Based on Your Images)

Public Subnet (Top Layer)

Load Balancer

Accepts HTTPS traffic from customers.

Sends only necessary HTTP/HTTPS to web servers in public subnet.

WAF (Web Application Firewall)

Sits in front of Load Balancer.

Filters malicious requests (SQLi, XSS, etc.).

Autoscaling Group

Multiple web servers for redundancy and scalability.

Placed in public subnet to respond to traffic spikes.

Private Subnet (Bottom Layer)

Application Servers

Receive requests from public subnet's load balancer.

Not directly exposed to the internet.

Database

Only accessible from application servers, never public.

Security groups restrict all inbound traffic except from app servers.

Internal Load Balancer

Balances requests to application servers.

Step 6: Flow of Data (Step-by-Step)

Client -> Internet Gateway -> WAF -> Load Balancer (Public Subnet): Customers initiate connections to your app over the internet.

Load Balancer -> Autoscaling Web Servers (Public Subnet): Load balancer routes requests to available web servers.

Web Servers -> Application Logic (Private Subnet): Web servers pass necessary requests to the internal application servers.

App Servers -> Database (Private Subnet): Application servers query/update customer payment data in the database.

Outbound (NAT Gateway): App servers may need to access updates or external APIs—use NAT Gateway for secure outbound connections.

Step 7: Security Best Practices

Security Groups: Only allow necessary ports (e.g., 443 for HTTPS to LB, 3306 for MySQL between app server and DB).

Network ACLs: Add another layer of subnet-level restrictions.

Encryption: Use HTTPS for all external connections, encrypt data at rest and in transit (TLS, disk encryption).

IAM Roles/Policies: Principle of least privilege for accessing resources.

Monitoring/Logging: Enable VPC flow logs, cloud service logs, and application logging.

Patch Management: Automate patching for OS and applications.

Backups: Regular, secure backups of critical data.

Step 8: Compliance Considerations

For payment applications (PCI DSS):

Isolate cardholder data environment (CDE).

Strong access controls (multi-factor authentication, role separation).

Regular vulnerability assessments and penetration testing.

Retain logs for auditing.

Step 9: Draw the Architecture (Summary)

Internet Gateway: Allows inbound/outbound internet access.

Public Subnet: WAF, Load Balancer, Autoscaling group.

Private Subnet: App servers, DB, internal LB.

NAT Gateway: Outbound access for private resources.

Security Groups/ACLs: Control all traffic flows.

Monitoring/Logging: Enabled at all levels.

Bonus: Sample Security Group Rules

Web Server (Public Subnet):

Inbound: 443 (HTTPS) from Internet

Outbound: 80/443 to App Servers

App Server (Private Subnet):

Inbound: 80/443 from Web Servers

Outbound: 3306 (MySQL) to Database

Database (Private Subnet):

Inbound: 3306 from App Servers

Outbound: None (unless replication required)

References to Security+ Domains

1.0 General Security Concepts: Principle of least privilege, defense in depth.

2.0 Threats, Vulnerabilities, Mitigations: WAF, segmentation, patching.

3.0 Security Architecture: Network segmentation, secure design.

4.0 Security Operations: Monitoring, logging, response.

5.0 Security Program Management: Compliance, policy.

### Questions # 3:

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

#### Options:

- A.  
Configure all systems to log scheduled tasks.
- B.  
Collect and monitor all traffic exiting the network.
- C.  
Block traffic based on known malicious signatures.
- D.  
Install endpoint management software on all systems.

#### Answer

D

#### Explanation

Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this purpose. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 137 1

### Questions # 4:

Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

**Options:**

A.

Client

B.

Third-party vendor

C.

Cloud provider

D.

DBA



CertsMania

**Answer**

A

**Explanation**

According to the shared responsibility model, the client and the cloud provider have different roles and responsibilities for securing the cloud environment, depending on the service model. In an IaaS (Infrastructure as a Service) model, the cloud provider is responsible for securing the physical infrastructure, such as the servers, storage, and network devices, while the client is responsible for securing the operating systems, applications, and data that run on the cloud infrastructure. Therefore, the client is responsible for securing the company's database in an IaaS model for a cloud environment, as the database is an application that stores data. The client can use various security controls, such as encryption, access control, backup, and auditing, to protect the database from unauthorized access, modification, or loss. The third-party vendor and the DBA (Database Administrator) are not roles defined by the shared responsibility model, but they may be involved in the implementation or management of the database security. References = CompTIA Security+ SY0-701 Certification Study Guide, page 263-264; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 5:00 - 7:40.

**Questions # 5:**

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?

**Options:**

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



CertsMania

**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

Questions # 6:

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

**Options:**

- A.  
Validate the code signature.
- B.  
Execute the code in a sandbox.

C.

Search the executable for ASCII strings.

D.

Generate a hash of the files.

## Answer

A

## Explanation

Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software's integrity and origin. References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

## Questions # 7:

Which of the following activities should be performed first to compile a list of vulnerabilities in an environment?

### Options:

A.

Automated scanning

B.

Penetration testing

C.

Threat hunting

D.

Log aggregation

E.

Adversarial emulation

## Answer

A

## Explanation

Automated vulnerability scanning is the first step in identifying system weaknesses. These scans systematically check for outdated software, misconfigurations, and known vulnerabilities in a network.

Penetration testing (B) is conducted after vulnerabilities are identified.

Threat hunting (C) focuses on detecting unknown threats, not listing vulnerabilities.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain., . . . ]

## Questions # 8:

A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?

### Options:

A.

Espionage

B.

Data exfiltration

C.

Nation-state attack

D.

Shadow IT

## Answer

D

## Questions # 9:

A security analyst identifies an incident in the network. Which of the following incident response activities would the security analyst perform next?

### Options:

A.

Containment

B.

Detection

C.

Eradication

D.

Recovery



CertsMania

### Answer

A

### Explanation

Once an incident is detected, the **next step is containment**, which involves limiting the scope and impact of the incident to prevent further damage. Containment can be temporary or long-term, isolating affected systems or networks.

Detection (B) is the initial identification phase before containment. Eradication (C) follows containment and involves removing the root cause. Recovery (D) is the final step to restore normal operations.

This workflow is fundamental in the Incident Response lifecycle detailed in Security Operations in SY0-701 [6:Chapter 14+CompTIA Security+ Study Guide].

## Questions # 10:

A software developer would like to ensure. The source code cannot be reverse engineered or debugged. Which of the following should the developer consider?

**Options:**

A.

Version control

B.

Obfuscation toolkit

C.

Code reuse

D.

Continuous integration

E.

Stored procedures



CertsMania

**Answer**

B

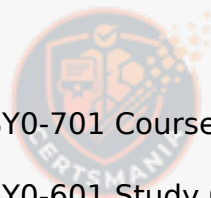
**Explanation**

An obfuscation toolkit is used by developers to make source code difficult to understand and reverse engineer. This technique involves altering the code's structure and naming conventions without changing its functionality, making it much harder for attackers to decipher the code or use debugging tools to analyze it. Obfuscation is an important practice in protecting proprietary software and intellectual property from reverse engineering.

References =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Coding Practices.



CertsMania

**Questions # 11:**

Employees sign an agreement that restricts specific activities when leaving the company. Violating the agreement can result in legal consequences. Which of the following agreements does this best describe?

**Options:**

A.

SLA

B.

BPA

C.

NDA

D.

MOA



CertsMania

**Answer**

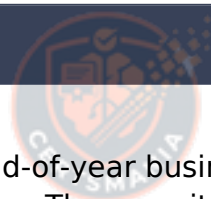
C

**Explanation**

A non-disclosure agreement (NDA) restricts employees from sharing proprietary or confidential information when they leave the company. Legal consequences may result from violating an NDA.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 5.2: "NDAs are legal agreements to prevent employees from disclosing sensitive information upon termination.", Exam Objectives 5.2: "Summarize business agreement and legal requirements.", , , ]

Questions # 12:



CertsMania

In a rush to meet an end-of-year business goal, the IT department was told to implement a new business application. The security engineer reviews the attributes of the application and decides the time needed to perform due diligence is insufficient from a cybersecurity perspective. Which of the following best describes the security engineer's response?

**Options:**

A.

Risk tolerance

B.

Risk acceptance

C.

Risk importance

D.

Risk appetite



CertsMania

### Answer

D

### Explanation

Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of risk management and understanding organizational risk appetite.

### Questions # 13:

A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

### Options:

A.

Serverless framework

B.

Type 1 hypervisor

C.

SD-WAN

D.



CertsMania

**Answer**

A

**Explanation**

A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.

A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.

SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

### Questions # 14:

An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?

#### Options:

A.

Side loading

B.

Target of evaluation

C.

Resource reuse

D.

SQL injection



CertsMania

#### Answer

D

### Questions # 15:

While a school district is performing state testing, a security analyst notices all internet services are unavailable. The analyst discovers that ARP poisoning is occurring on the network and then terminates access for the host. Which of the following is most likely responsible for this malicious activity?

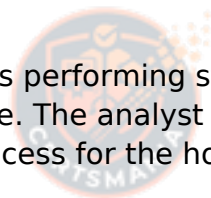
#### Options:

A.

Unskilled attacker

B.

Shadow IT



CertsMania

C.

Credential stuffing

D.

DMARC failure

## Answer

A

## Explanation

ARP poisoning (also known as ARP spoofing) is a basic man-in-the-middle (MITM) attack that involves sending fake ARP responses to redirect traffic. This technique is not sophisticated and can be easily executed using freely available tools like Cain & Abel, Ettercap, or Wireshark.

Such attacks are often attempted by unskilled attackers (script kiddies) testing their abilities, especially in environments like schools. The term "unskilled attacker" fits best here, as credential stuffing and DMARC are unrelated to ARP poisoning.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Attack techniques: MITM, ARP poisoning; attacker types: Unskilled/script kiddie.", , , ]

## Questions # 16:

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?

## Options:

A.

RBAC

B.

ACL

C.

SAML

- D.
- GPO

## Answer

A

## Explanation



# CertsMania

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

## Questions # 17:

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

### Options:

- A.

Retain the emails between the security team and affected customers for 30 days.

- B.

Retain any communications related to the security breach until further notice.

- C.

Retain any communications between security members during the breach response.

- D.

Retain all emails from the company to affected customers for an indefinite period of time.

## Answer

B

## Explanation

A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena<sup>12</sup>

In this scenario, the company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss<sup>34</sup>

[References:, 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 303 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3: Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6, , , , , , ]

## Questions # 18:

A systems administrator receives an alert that a company's internal file server is very slow and is only working intermittently. The systems administrator reviews the server management software and finds the following information about the server:

>

Which of the following indicators most likely triggered this alert?

## Options:

A.

Concurrent session usage

B.

Network saturation

C.

Account lockout

D.

Resource consumption



CertsMania

### Answer

D

### Questions # 19:

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.

Which of the following teams will conduct this assessment activity?

### Options:

A.

White

B.

Purple

C.

Blue

D.

Red



CertsMania

### Answer

D

### Explanation

A red team is a group of security professionals who perform offensive security

assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4. Security Teams - SY0-601 CompTIA Security+ : 1.8



CertsMania

#### Questions # 20:

A systems administrator receives a text message from an unknown number claiming to be the Chief Executive Officer of the company. The message states an emergency situation requires a password reset. Which of the following threat vectors is being used?

#### Options:

A.

Typosquatting

B.

Smishing

C.

Pretexting

D.

Impersonation



CertsMania

#### Answer

B

#### Explanation

Detailed Explanation:Smishing is a type of phishing attack that uses SMS text messages to deceive recipients into taking actions such as revealing sensitive information. The urgency in the text indicates this vector. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Social Engineering Techniques".

Questions # 21:

The security team at a large global company needs to reduce the cost of storing data used for performing investigations. Which of the following types of data should have its retention length reduced?

**Options:**

- A.  
Packet capture
- B.  
Endpoint logs
- C.  
OS security logs
- D.  
Vulnerability scan



CertsMania

**Answer**

A

**Explanation**

Packet capture data can be very large and may not need to be stored for extended periods compared to other logs essential for security audits.

=====



CertsMania

Questions # 22:

Which of the following is a preventive physical security control?

**Options:**

- A.  
Video surveillance system

B.

Bollards

C.

Alarm system

D.

Motion sensors



CertsMania

### Answer

B

### Questions # 23:

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).

### Options:

A.

Cancel current employee recognition gift cards.

B.

Add a smishing exercise to the annual company training.

C.

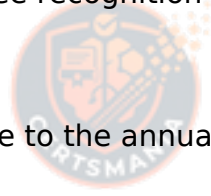
Issue a general email warning to the company.

D.

Have the CEO change phone numbers.

E.

Conduct a forensic investigation on the CEO's phone.



CertsMania

F.

Implement mobile device management.

## Answer

B, C

## Explanation



CertsMania

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

## Questions # 24:

An attorney prints confidential documents to a copier in an office space near multiple workstations and a reception desk. When the attorney goes to the copier to retrieve the documents, the documents are missing. Which of the following would best prevent this from reoccurring?

## Options:

A.

Place the copier in the legal department.

B.

Configure DLP on the attorney's workstation.

C.

Set up LDAP authentication on the printer.

D.

Conduct a physical penetration test.



CertsMania

## Answer

C

## Explanation

LDAP authentication on the printer (C) would require users to authenticate before printing, enabling secure print release. This ensures that documents are not printed until the authorized user is physically present, which directly addresses the issue of missing confidential documents.

As per CompTIA Security+ SY0-701, Domain 3.1 (Access management), integrating authentication mechanisms like LDAP improves physical and document security in shared environments.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.1 - "Access management: Authentication mechanisms (e.g., LDAP).", , , , ]

## Questions # 25:

An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?

### Options:

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., , , , , ]

## Questions # 26:

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message. Which of the following types of social engineering attacks occurred?

### Options:

A.

Brand impersonation

B.

Pretexting

C.

Typosquatting

D.

Phishing

## Answer

D

### Explanation

Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information.

The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one. The employee entered the log-in information, but received a "page not found" error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee's credentials for the payment website. References = Other Social Engineering Attacks - CompTIA Security+ SY0-701 - 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack ... - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

### Questions # 27:

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions over the phone to use a new account. Which of the following would most likely prevent this activity in the future?

#### Options:

A.

Standardizing security incident reporting

B.

Executing regular phishing campaigns

C.

Implementing insider threat detection measures

D.

Updating processes for sending wire transfers

#### Answer

D

#### Explanation

Comprehensive and Detailed In-Depth Explanation:

Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) can prevent fraudulent transactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.

Standardizing security incident reporting is useful for tracking security events but does not prevent fraud in real time.

Executing regular phishing campaigns improves awareness but does not enforce a verification process for financial transactions.

Implementing insider threat detection focuses on internal risks but does not specifically prevent external fraud.

A more secure wire transfer process with additional verification steps is the most effective measure against fraudulent transactions.



CertsMania

### Questions # 28:

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

#### Options:

A.

Compromise

B.

Retention

C.

Analysis

D.

Transfer

E.

Inventory



CertsMania

#### Answer

B

#### Explanation

A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.

#### References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211

CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

#### Questions # 29:

Which of the following best protects sensitive data in transit across a geographically dispersed Infrastructure?

#### Options:

A.

Encryption

B.

Masking

C.

Tokenization

D.

Obfuscation

#### Answer

A

#### Questions # 30:

Cadets speaking a foreign language are using company phone numbers to make unsolicited phone calls to a partner organization. A security analyst validates through phone system logs that the calls are occurring and the numbers are not being spoofed. Which of the following is the most likely explanation?

**Options:**

A.

The executive team is traveling internationally and trying to avoid roaming charges

B.

The company's SIP server security settings are weak.

C.

Disgruntled employees are making calls to the partner organization.

D.

The service provider has assigned multiple companies the same numbers

**Answer**

B

**Explanation**

If cadets are using company phone numbers to make unsolicited calls, and the logs confirm the numbers are not being spoofed, it suggests that the SIP (Session Initiation Protocol) server's security settings might be weak. This could allow unauthorized access or exploitation of the company's telephony services, potentially leading to misuse by unauthorized individuals.

References = CompTIA Security+ SY0-701 study materials, especially on SIP security and common vulnerabilities.

**Questions # 31:**

A company's website is www. Company. com Attackers purchased the domain wwww. company.com Which of the following types of attacks describes this example?

**Options:**

A.

Typosquatting

B.

Brand Impersonation

C.

On-path

D.

Watering-hole



CertsMania

**Answer**

A

**Explanation**

"Typosquatting, also known as URL hijacking, is a form of cybersquatting where attackers register domain names that are intentionally similar to legitimate ones, often differing by a single character or a common typographical error. For example, an attacker might register 'www.company.com ' to mimic 'www.company.com, ' tricking users who mistype the URL into visiting a malicious site. This attack exploits human error and can be used to steal credentials, distribute malware, or impersonate the legitimate entity."

[Reference:CompTIA Security+ SY0-701 Study Guide, Domain 1.0: General Security Concepts, Section: "Social Engineering Attacks and Threats" (Typosquatting is typically covered under threats related to domain misuse)., Explanation:In this scenario, the attackers registered "www.company.com," which is a subtle variation of "www.company.com," relying on users mistyping or not noticing the extra "w." This fits the definition of typosquatting perfectly. Brand impersonation (B) is related but broader and doesn't specifically tie to typographical errors. On-path (C) involves intercepting communication, and watering-hole (D) targets users via compromised legitimate sites—neither applies here., , , ]

**Questions # 32:**

Which of the following should be used to select a label for a file based on the file's value, sensitivity, or applicable regulations?

**Options:**

A.

Verification

B.

Certification

C.

Classification

D.

Inventory



CertsMania

**Answer**

C

**Explanation**

**Classification** is the process of assigning labels to files or data based on sensitivity, business value, or regulatory requirements. Proper classification guides handling, access controls, and protection measures.

Verification (A) and certification (B) are validation processes, and inventory (D) is a listing of assets.

Data classification is a foundational data governance control in SY0-701 [6:Chapter 16]†CompTIA Security+ Study Guide [6].

Questions # 33:



CertsMania

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

**Options:**

A.

Automation

B.

Compliance checklist

C.

Attestation

D.

Manual audit



CertsMania

## Answer

A

### Explanation

Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs. Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise<sup>12</sup>.

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

**Compliance checklist:** This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis<sup>3</sup>.

**Attestation:** This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis<sup>4</sup>.

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

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer<sup>3</sup>: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification

### Questions # 34:

A certificate authority needs to post information about expired certificates. Which of the following would accomplish this task?

#### Options:

A.

TPM

B.

CRL

C.

PKI

D.

CSR

#### Answer

B

#### Explanation

A Certificate Revocation List (CRL) is a digitally signed list maintained by a Certificate Authority (CA) that contains revoked or expired certificates. This prevents clients from trusting compromised or outdated certificates.

TPM (A) is a hardware security module, unrelated to certificate revocation.

PKI (C) is the overall system managing digital certificates, but it does not store revocation lists.

CSR (D) is a request to obtain a certificate, not to revoke one.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain., , , ]

## Questions # 35:

Which of the following should be deployed on an externally facing web server in order to establish an encrypted connection?

### Options:

A.

Public key

B.

Private Key

C.

Asymmetric key

D.

Symmetric key



CertsMania

### Answer

A

### Explanation

To establish an encrypted connection (such as HTTPS/TLS) with an externally facing web server, the server must deploy a public key as part of its digital certificate. Clients use the server's public key to initiate secure communication, which is validated by certificate authorities. The server holds the matching private key, but it is the public key that must be made available for encrypted connections to be established.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3: "A public key is made available to anyone and is used to establish secure connections with a web server.", , , ]

## Questions # 36:

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

**Options:**

A.

A worm is propagating across the network.

B.

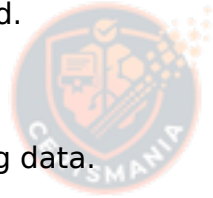
Data is being exfiltrated.

C.

A logic bomb is deleting data.

D.

Ransomware is encrypting files.



CertsMania

**Answer**

B

**Explanation**

Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; Introduction to DNS Data Exfiltration; Identifying a DNS Exfiltration Attack That Wasn't Real — This Time



CertsMania

**Questions # 37:**

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?

**Options:**

A.

Business email

B.

Social engineering

C.

Unsecured network

D.

Default credentials



CertsMania

## Answer

B

## Explanation

The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.

Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.

Unsecured network is unrelated to the email content.

Default credentials do not apply here, as the issue is with suspicious links, not login credentials.



CertsMania

Questions # 38:

A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?

## Options:

A.

Port security

B.

Web application firewall

C.

Transport layer security

D.

Virtual private network



CertsMania

### Answer

A

### Explanation

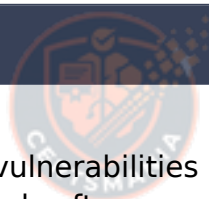
Port security is the best solution to prevent unauthorized devices, like a visitor's laptop, from connecting to the company's network. Port security can limit the number of devices that can connect to a network switch port and block unauthorized MAC addresses, effectively stopping unauthorized access attempts.

Web application firewall (WAF) protects against web-based attacks, not unauthorized network access.

Transport Layer Security (TLS) ensures encrypted communication but does not manage physical network access.

Virtual Private Network (VPN) secures remote connections but does not control access through physical network ports.

### Questions # 39:



CertsMania

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

### Options:

A.

Jailbreaking

B.

Memory injection

C.

Resource reuse

D.

Side loading

## Answer

D

## Explanation

Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideloaded - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers - CompTIA Security+ SY0-501 - 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

## Questions # 40:

An employee clicks a malicious link in an email that appears to be from the company's Chief Executive Officer. The employee's computer is infected with ransomware that encrypts the company's files. Which of the following is the most effective way for the company to prevent similar incidents in the future?

## Options:

A.

Security awareness training

B.

Database encryption

C.

Segmentation

D.

Reporting suspicious emails

## Answer

A

Questions # 41:

Which of the following actions must an organization take to comply with a person's request for the right to be forgotten?

### Options:

A.

Purge all personally identifiable attributes.

B.

Encrypt all of the data.

C.

Remove all of the person's data.

D.

Obfuscate all of the person's data.

## Answer

C

### Explanation

Comprehensive and Detailed In-Depth Explanation:

The right to be forgotten, as outlined in regulations such as the General Data Protection Regulation (GDPR), requires organizations to permanently delete an individual's personal data upon request, unless there is a legal or contractual obligation to retain it.

Purging personally identifiable attributes (A) removes some identifying data but does not fully satisfy the request.

Encrypting the data (B) does not remove it, and the data is still accessible with the

decryption key.

Obfuscating data (D)makes data unreadable but does not permanently remove it.

To comply withthe right to be forgotten, organizations mustremove all of the person's dataunless an exception applies.

Questions # 42:

Which of the following is the most important element when defining effective security governance?

**Options:**

A.

Discovering and documenting external considerations

B.

Developing procedures for employee onboarding and offboarding

C.

Assigning roles and responsibilities for owners, controllers, and custodians

D.

Defining and monitoring change management procedures

**Answer**

C

**Explanation**

Effective security governance requires clear assignment of roles and responsibilities, such as owners, controllers, and custodians, to ensure accountability for security-related tasks and data management within the organization. This establishes clear lines of responsibility and authority, which is fundamental to governance frameworks.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: "Assigning roles and responsibilities is fundamental to effective security governance.", Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks.", , , ]

## Questions # 43:

A security analyst is reviewing the following logs about a suspicious activity alert for a user's VPN log-ins. Which of the following malicious activity indicators triggered the alert?

□ Log Summary:

User logs in from Chicago, IL multiple times, then suddenly a successful login appears from Rome, Italy, followed again by Chicago logins — all within a short time span.

### Options:

A.

Impossible travel

B.

Account lockout

C.

Blocked content

D.

Concurrent session usage

### Answer

A

### Explanation

Impossible travel (A) refers to logins from geographically distant locations within a time period that makes travel between them physically impossible. In this case, a user logging in from Chicago and Rome within a short time frame triggers this anomaly.

This is a strong indicator of a compromised account or stolen credentials being used elsewhere.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: Impossible travel (geolocation anomalies).", , , ]

## Questions # 44:

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

**Options:**

A.

To track the status of patching installations

B.

To find shadow IT cloud deployments

C.

To continuously the monitor hardware inventory

D.

To hunt for active attackers in the network

**Answer**

A

**Explanation**

Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.

Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.

Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

**Questions # 45:**

Which of the following would a systems administrator follow when upgrading the firmware of an organization's router?

**Options:**

A.

Software development life cycle

B.

Risk tolerance

C.

Certificate signing request

D.

Maintenance window



CertsMania

**Answer**

D

Questions # 46:

Which of the following should be used to ensure a device is inaccessible to a network-connected resource?

**Options:**

A.

Disablement of unused services

B.

Web application firewall

C.

Host isolation

D.

Network-based IDS



CertsMania

## Answer

C

## Explanation

Detailed Explanation: Host isolation ensures that a device is separated from the network, preventing it from accessing or being accessed by other network resources. This is typically achieved by quarantining the device. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Isolation and Containment".

## Questions # 47:

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

### Options:

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

#### Questions # 48:

An employee who was working remotely lost a mobile device containing company data. Which of the following provides the best solution to prevent future data loss?

#### Options:

A.

MDM

B.

DLP

C.

FDE

D.

EDR

#### Answer

A

#### Questions # 49:

To which of the following security categories does an EDR solution belong?

**Options:**

A.

Physical

B.

Operational

C.

Managerial

D.

Technical



CertsMania

**Answer**

D

Questions # 50:

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?

**Options:**

A.

Exception

B.

Segmentation

C.

Risk transfer

D.

Compensating controls



CertsMania

## 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, , , ]

## Questions # 51:

Which of the following phases of the incident response process attempts to minimize disruption?

### Options:

A.

Recovery

B.

Containment

C.

Preparation

D.

Analysis



CertsMania

## Answer

B

## Explanation

Containment is the phase where an organization attempts to minimize the damage caused by a security incident. This may involve isolating affected systems, blocking malicious traffic, or temporarily shutting down compromised services to prevent further impact.

Recovery (A) focuses on restoring normal operations after an incident.

Preparation (C) involves planning and readiness before an incident occurs.

Analysis (D) involves investigating the root cause and assessing the damage.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain., , , , , , ]

## Questions # 52:

An engineer needs to ensure that a script has not been modified before it is launched. Which of the following best provides this functionality?

### Options:

A.

Masking

B.

Obfuscation

C.

Hashing

D.

Encryption

### Answer

C

### Explanation

**Hashing** produces a fixed-length fingerprint of the script's contents. By comparing the current hash with a known good hash, the engineer can verify if the script has been altered. Hashing is a one-way function used to validate integrity.

Masking (A) hides data, obfuscation (B) hides code logic, and encryption (D) protects confidentiality but does not verify integrity as simply.

Integrity checking through hashing is fundamental in General Security Concepts  
[6:Chapter 7+CompTIA Security+ Study Guide].

### Questions # 53:

Which of the following data recovery strategies will result in a quick recovery at low cost?

#### Options:

A.

Hot

B.

Cold

C.

Manual

D.

Warm



CertsMania

#### Answer

D

#### Explanation

A **warm site** offers a compromise between cost and recovery speed. It includes hardware and network infrastructure partially configured, allowing quicker recovery than a cold site but at lower cost than a hot site.

Hot sites (A) enable rapid recovery but at high cost. Cold sites (B) are low cost but slow to recover. Manual (C) refers to manual processes, typically slower.

Warm sites balance recovery time and cost in disaster recovery planning [6:Chapter 9] CompTIA Security+ Study Guide [6].

### Questions # 54:

An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

**Options:**

A.

Virus

B.

Trojan

C.

Spyware

D.

Ransomware



CertsMania

**Answer**

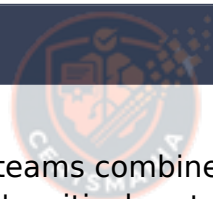
D

**Explanation**

Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.

[References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17., , , , , ]

Questions # 55:



CertsMania

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

**Options:**

A.

Red

B.

Blue

C.

Purple

D.

Yellow

## Answer

C

## Explanation

Purple is the team that combines both offensive and defensive testing techniques to protect an organization's critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization's systems. The blue team is the defensive team that monitors and protects the organization's systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization. Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques. The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

## Questions # 56:

Which of the following should a company use to provide proof of external network security testing?

### Options:

A.

Business impact analysis

B.

Supply chain analysis

C.

Vulnerability assessment

D.

Third-party attestation

### Answer

D

### Explanation



CertsMania

Detailed Explanation: Third-party attestation involves an external, independent party performing a network security assessment and providing documented proof, ensuring objectivity and compliance with regulatory or client requirements. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Compliance and Security Audits".

### Questions # 57:

Which of the following would best ensure a controlled version release of a new software application?

### Options:

A.

Business continuity planning

B.

Quantified risk analysis



CertsMania

C.

Static code analysis

D.

Change management procedures

### Answer

D

## Explanation

**Change management procedures** provide structured steps to approve, test, document, and deploy software changes, ensuring controlled and auditable version releases that minimize risks and disruptions.

Business continuity planning (A) relates to operational continuity, quantified risk analysis (B) assesses risks quantitatively, and static code analysis (C) finds coding defects but does not control release processes.

Change management is fundamental to software lifecycle governance in SY0-701  
[6:Chapter 16†CompTIA Security+ Study Guide].

## Questions # 58:

A systems administrator discovers a system that is no longer receiving support from the vendor. However, this system and its environment are critical to running the business, cannot be modified, and must stay online. Which of the following risk treatments is the most appropriate in this situation?

### Options:

A.

Refect

B.

Accept

C.

Transfer

D.

Avoid

## Answer

C

## Questions # 59:

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?

**Options:**

A.

Scalability

B.

Availability

C.

Cost

D.

Ease of deployment



CertsMania

**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., , , , , ]

**Questions # 60:**

A security engineer is installing an IPS to block signature-based attacks in the environment. Which of the following modes will best accomplish this task?

**Options:**

A.

Monitor

B.

Sensor

C.

Audit

D.

Active



CertsMania

**Answer**

D

**Explanation**

To block signature-based attacks, the Intrusion Prevention System (IPS) must be in active mode. In this mode, the IPS can actively monitor and block malicious traffic in real time based on predefined signatures. This is the best mode to prevent known attack types from reaching the internal network.

Monitor mode and sensor mode are typically passive, meaning they only observe and log traffic without actively blocking it.

Audit mode is used for review purposes and does not actively block traffic.

Questions # 61:



CertsMania

Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach that would affect offshore offices. Which of the following is this an example of?

**Options:**

A.

Tabletop exercise

B.

Penetration test

C.

Geographic dispersion

D.

Incident response



CertsMania

## Answer

A

## Explanation

A tabletop exercise is a discussion-based simulation in which stakeholders review and talk through their roles, responsibilities, and actions in response to a hypothetical incident. This allows participants to evaluate and improve response plans without actual disruption.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 5.6: "Tabletop exercises involve key stakeholders discussing roles, responsibilities, and actions in response to simulated incidents.", Exam Objectives 5.6: "Given a scenario, implement security incident management processes.", , , , ]

## Questions # 62:

Prior to implementing a design change, the change must go through multiple steps to ensure that it does not cause any security issues. Which of the following is most likely to be one of those steps?

## Options:

A.

Management review

B.

Load testing

C.

Maintenance notifications

D.



CertsMania

Procedure updates

## Answer

A

## Explanation

Management review is a critical step in the change management process. Before implementing any design change, management reviews help evaluate the potential impact, security implications, and alignment with organizational goals and policies. This review ensures that the change is justified, risks are understood, and proper approvals are obtained.

Load testing is a performance test, maintenance notifications are communication steps, and procedure updates are documentation activities — all important but generally occur after management has approved the change.

The significance of management involvement in change governance is a foundational concept in the Security Program Management and Oversight domain of the SY0-701 exam [6:Chapter 16†CompTIA Security+ Study Guide].

## Questions # 63:

A company's online shopping website became unusable shortly after midnight on January 30, 2023. When a security analyst reviewed the database server, the analyst noticed the following code used for backing up data:

Which of the following should the analyst do next?

### Options:

A.

Check for recently terminated DBAs.

B.

Review WAF logs for evidence of command injection.

C.

Scan the database server for malware.

D.

Search the web server for ransomware notes.

## Answer

B

Questions # 64:

A human resources (HR) employee working from home leaves their company laptop open on the kitchen table. A family member walking through the kitchen reads an email from the Chief Financial Officer addressed to the HR department. The email contains information referencing company layoffs. The family member posts the content of the email to social media. Which of the following policies will the HR employee most likely need to review after this incident?

### Options:

A.

Hybrid work environment

B.

Operations security

C.

Data loss prevention

D.

Social engineering

## Answer

B

### Explanation

Comprehensive and Detailed In-Depth Explanation:

Operations security (OPSEC) focuses on identifying and protecting sensitive information to prevent unauthorized disclosure. In this scenario, the HR employee failed to safeguard confidential company information, leading to its exposure on social media.

Training in OPSEC would reinforce the need to maintain security best practices, such as

locking screens when away from a device and ensuring that sensitive data is not exposed in unsecured locations.

Hybrid work environment policies relate to managing remote and in-office work but do not specifically cover security risks like unauthorized data exposure.

Data loss prevention (DLP) deals with technology-based solutions to prevent unauthorized data transfers but does not address physical security practices.

Social engineering refers to deceptive tactics used by attackers to manipulate individuals, which is not applicable to this situation.

The HR employee should review operations security policies to prevent similar incidents in the future.

#### Questions # 65:

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?

#### Options:

A.

Active

B.

Passive

C.

Defensive

D.

Offensive

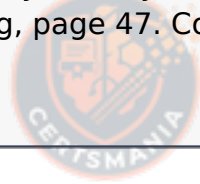
#### Answer

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.



CertsMania

#### Questions # 66:

A site reliability engineer is designing a recovery strategy that requires quick failover to an identical site if the primary facility goes down. Which of the following types of sites should the engineer consider?

#### Options:

A.

Recovery site

B.

Hot site

C.

Cold site

D.

Warm site



CertsMania

#### Answer

B

#### Explanation

A hot site is a fully operational offsite facility that is equipped with hardware, software, and up-to-date data, and is ready to take over operations immediately if the primary site fails. This allows for minimal downtime and quick failover, meeting the requirement for rapid recovery.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 4.4: "Hot sites are ready to take over operations instantly with minimal downtime.", Exam Objectives 4.4: "Summarize business continuity and disaster recovery concepts.", , , ]

## Questions # 67:

Which of the following best describe a penetration test that resembles an actual external attach?

### Options:

A.

Known environment

B.

Partially known environment

C.

Bug bounty

D.

Unknown environment

### Answer

D

### Explanation

An unknown environment in penetration testing, also known as a black-box test, simulates an actual external attack where the tester has no prior knowledge of the system. This type of penetration test is designed to mimic real-world attack scenarios, where an attacker has little to no information about the target environment. The tester must rely on various reconnaissance and attack techniques to uncover vulnerabilities, much like a real-world attacker would. This approach helps organizations understand their security posture from an external perspective, providing insights into how their defenses would hold up against a true outsider threat.

References =

CompTIA Security+ SY0-701 Course Content: The course highlights the importance of understanding different penetration testing environments, including black-box testing, which aligns with the "unknown environment" in the provided answer.

CompTIA Security+ SY0-601 Study Guide: The guide details penetration testing methodologies, including black-box testing, which is crucial for simulating real external attacks.

#### Questions # 68:

A company is considering an expansion of access controls for an application that contractors and internal employees use to reduce costs. Which of the following risk elements should the implementation team understand before granting access to the application?

#### Options:

A.

Threshold

B.

Appetite

C.

Tolerance

D.

Register

#### Answer

C

#### Questions # 69:

A university uses two different cloud solutions for storing student data. Which of the following does this scenario represent?

#### Options:

A.

Load balancing

B.

Parallel processing

C.

Platform diversity

D.

Clustering



CertsMania

### Answer

C

### Explanation

Using two different cloud solutions to store data is an example of **platform diversity**, which helps reduce dependency on a single cloud provider and enhances resilience against vendor-specific failures or outages.

Load balancing (A) distributes workloads across resources; parallel processing (B) refers to simultaneous processing of tasks; clustering (D) involves grouping servers to act as a single system.

Platform diversity is a recognized architectural strategy to improve availability and fault tolerance, covered in Security Architecture concepts for SY0-701 [6:Chapter 10] CompTIA Security+ Study Guide [

### Questions # 70:

An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?

### Options:

A.

To defend against insider threats altering banking details

B.

To ensure that errors are not passed to other systems

C.

To allow for business insurance to be purchased

D.

To prevent unauthorized changes to financial data

### Answer

D

### Explanation



CertsMania

Detailed Explanation:

Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Controls for Financial Systems".

### Questions # 71:

A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.

Most employees clocked in and out while they were inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.

Hourly employees are required to use a website called [acmetimekeeping.com](http://acmetimekeeping.com) to clock in and out. This website is accessible from the internet. Which of the following is the most likely reason for this compromise?

### Options:

A.

A brute-force attack was used against the time-keeping website to scan for common passwords.

B.

A malicious actor compromised the time-keeping website with malicious code using an

unpatched vulnerability on the site, stealing the credentials.

C.

The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site

D.

ARP poisoning affected the machines in the building and caused the kiosks to send a copy of all the submitted credentials to a machine.machine.

## Answer

B

## Explanation

The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.

References =

CompTIA Security+ SY0-701 Course Content: The course discusses web application vulnerabilities and how attackers can exploit them to steal credentials.

## Questions # 72:

Several customers want an organization to verify its security controls are operating effectively and have requested an independent opinion. Which of the following is the most efficient way to address these requests?

## Options:

A.

Hire a vendor to perform a penetration test.

B.

Perform an annual self-assessment.

C.

Allow each client the right to audit.

D.

Provide a third-party attestation report.

**Answer**

D



CertsMania

Questions # 73:

An attacker used XSS to compromise a web server. Which of the following solutions could have been used to prevent this attack?

**Options:**

A.

NGFW

B.

UTM

C.

WAF

D.

NAC



CertsMania

**Answer**

C

**Explanation**

Comprehensive and Detailed In-Depth Explanation:

A Web Application Firewall (WAF) is designed to protect web applications from attacks such as Cross-Site Scripting (XSS) by filtering and monitoring HTTP traffic between the internet and a web application.

Next-Generation Firewalls (NGFW) (A) provide advanced network security but are not specifically designed to protect web applications from XSS attacks.

Unified Threat Management (UTM) (B) provides multiple security functions but lacks the specialized application-layer protection needed to mitigate XSS.

Network Access Control (NAC) (D) controls device access to the network but does not prevent web-based attacks.

AWAF is the best solution for protecting web servers from XSS, SQL injection, and other web-based threats.

#### Questions # 74:

Which of the following definitions best describes the concept of log co-relation?

#### Options:

A.

Combining relevant logs from multiple sources into one location

B.

Searching end processing, data to identify patterns of malicious activity

C.

Making a record of the events that occur in the system

D.

Analyzing the log files of the system components

#### Answer

D

#### Questions # 75:

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the

first step the security team should take?

**Options:**

A.

Enable SAML

B.

Create OAuth tokens.

C.

Use password vaulting.

D.

Select an IdP



CertsMania

**Answer**

D

**Explanation**

The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.

Enabling SAML would be part of the technical implementation but comes after selecting an IdP.

OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.

Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

**Questions # 76:**

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?

**Options:**

A.

Console access

B.

Routing protocols

C.

VLANs

D.

Web-based administration



# CertsMania

**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

**Questions # 77:**

Which of the following is the most likely motivation for a hacktivist?

**Options:**

A.

Financial gain

B.

Service disruption

C.

Philosophical beliefs

D.

Corporate espionage



CertsMania

**Answer**

C

**Explanation**

Hacktivists are individuals or groups who use hacking to promote a political agenda, social cause, or philosophical beliefs. Their primary motivation is not personal gain but rather to draw attention to, or protest against, perceived injustices or causes.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1: "Hacktivists are motivated by ideology or political/social causes.", Exam Objectives 2.1: "Compare and contrast different types of threat actors.", , , ]

Questions # 78:

A security manager is implementing MFA and patch management. Which of the following would best describe the control type and category? (Select two).

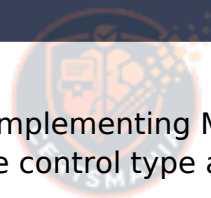
**Options:**

A.

Physical

B.

Managerial



CertsMania

C.

Detective

D.

Administrator

E.

Preventative

F.

Technical



CertsMania

### **Answer**

E, F

### **Explanation**

Multi-Factor Authentication (MFA) and patch management are both examples of preventative and technical controls. MFA prevents unauthorized access by requiring multiple forms of verification, and patch management ensures that systems are protected against vulnerabilities by applying updates. Both of these controls are implemented using technical methods, and they work to prevent security incidents before they occur.

[References:, CompTIA Security+ SY0-701 Course Content: Domain 1: General Security Concepts, and Domain 4: Identity and Access Management, which cover the implementation of preventative and technical controls., , , ]



CertsMania

**To Get Premium Files for SY0-701 Visit**

**<https://www.certsmania.com/comptia/sy0-701-practice>**

**For More Free Questions Visit**

**<https://www.certsmania.com/comptia/pdf/sy0-701>**



**CertsMania**