



CertsMania

Free Questions for **SY0-701**

Shared by **Dominic** on **Dec 2, 2025**

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

Which of the following is the best way to improve the confidentiality of remote connections to an enterprise's infrastructure?

Options:

A.

Firewalls

B.

Virtual private networks

C.

Extensive logging

D.

Intrusion detection systems



CertsMania

Answer

B

Explanation

A Virtual Private Network (VPN) (B) encrypts all data transmitted between remote users and the enterprise infrastructure, ensuring confidentiality. VPNs are essential in protecting sensitive data from interception over untrusted networks.

This is covered under Domain 3.3: Secure network designs, where VPNs are listed as a key control for ensuring confidentiality of remote connections.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.3 - "Remote access security: VPN (ensures confidentiality).", , , ,]

Questions # 2:

A recent penetration test identified that an attacker could flood the MAC address table of network switches. Which of the following would best mitigate this type of attack?

Options:

A.

Load balancer

B.

Port security

C.

IPS

D.

NGFW



CertsMania

Answer

B

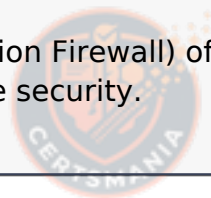
Explanation

Port security is the best mitigation technique for preventing an attacker from flooding the MAC address table of network switches. Port security can limit the number of MAC addresses learned on a port, preventing an attacker from overwhelming the switch's MAC table (a form of MAC flooding attack). When the allowed number of MAC addresses is exceeded, port security can block additional devices or trigger alerts.

Load balancer distributes network traffic but does not address MAC flooding attacks.

IPS (Intrusion Prevention System) detects and prevents attacks but isn't specifically designed for MAC flooding mitigation.

NGFW (Next-Generation Firewall) offers advanced traffic inspection but is not directly involved in MAC table security.



CertsMania

Questions # 3:

A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

- . Something you know
- . Something you have

. Something you are

Which of the following would accomplish the manager's goal?

Options:

A.

Domain name, PKI, GeolIP lookup

B.

VPN IP address, company ID, facial structure

C.

Password, authentication token, thumbprint

D.

Company URL, TLS certificate, home address

Answer

C

Explanation

The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactor authentication that uses something you know, something you have, and something you are.

Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12

Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12

Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN12

[References:, 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 177 2: CompTIA Security+ Certification Kit: Exam

Questions # 4:

A growing organization, which hosts an externally accessible application, adds multiple virtual servers to improve application performance and decrease the resource usage on individual servers Which of the following solutions is the organization most likely to employ to further increase performance and availability?

Options:

A.

Load balancer

B.

Jump server

C.

Proxy server

D.

SD-WAN

Answer

A

Questions # 5:

A security analyst is prioritizing vulnerability scan results using a risk-based approach. Which of the following is the most efficient resource for the analyst to use?

Options:

A.

Business impact analysis

B.

Common Vulnerability Scoring System

C.

Risk register

D.

Exposure factor



CertsMania

Answer

B

Explanation

The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of vulnerabilities. It provides a numerical score (0-10) based on factors such as exploitability, impact, and complexity, helping security analysts prioritize remediation efforts based on risk.

Business impact analysis (A) helps identify critical business functions but does not specifically prioritize vulnerabilities.

Risk register (C) tracks identified risks but does not classify vulnerabilities.

Exposure factor (D) is used in quantitative risk assessment but is not an industry standard for vulnerability prioritization.

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

Questions # 6:

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

Options:

A.

To gather IoCs for the investigation

B.

To discover which systems have been affected



CertsMania

C.

To eradicate any trace of malware on the network

D.

To prevent future incidents of the same nature

Answer

D

Explanation

Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization. Root cause analysis is not meant to gather IoCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment and eradication phases of incident response. References = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

Questions # 7:

Which of the following most securely protects data at rest?

Options:

A.

TLS 1.2

B.

AES-256

C.

Masking

D.

Salting

Answer

B

Explanation



CertsMania

AES-256 is a symmetric encryption algorithm widely used to protect data at rest by converting plaintext into ciphertext that is unreadable without the proper key. It provides strong confidentiality and is a standard for encrypting stored data.

TLS 1.2 (A) secures data in transit, not at rest. Masking (C) obscures data but typically for display or limited use and is reversible. Salting (D) is used alongside hashing to protect passwords and data integrity but does not encrypt data.

Encryption with AES-256 is recognized as a best practice for securing stored data in the Security+ Cryptography and General Security Concepts domains [6:Chapter 7] CompTIA Security+ Study Guide [1].

Questions # 8:

An employee in the accounting department receives an email containing a demand for payment for services performed by a vendor. However, the vendor is not in the vendor management database. Which of the following in this scenario is an example of?

Options:

A.

Pretexting

B.

Impersonation

C.

Ransomware

D.



CertsMania

Invoice scam

Answer

D

Explanation

The scenario describes an instance where an employee receives a fraudulent invoice from a vendor that is not recognized in the company's vendor management system. This is a classic example of an invoice scam, where attackers attempt to trick organizations into making payments for fake or non-existent services. These scams often rely on social engineering tactics to bypass financial controls.

References = CompTIA Security+ SY0-701 study materials, particularly in the context of social engineering attacks and common scams.

Questions # 9:

A company decides to purchase an insurance policy. Which of the following risk management strategies is this company implementing?

Options:

A.

Mitigate

B.

Accept

C.

Avoid

D.

Transfer

Answer

D

Explanation

Purchasing insurance is a classic example of **risk transfer**, where financial risk associated with potential losses is shifted to a third party (the insurer). This strategy does not eliminate the risk but moves the financial burden.

Mitigation (A) reduces risk impact or likelihood through controls, acceptance (B) involves acknowledging the risk without action, and avoidance (C) eliminates the risk by not engaging in the activity.

Risk transfer is a fundamental concept taught in the Risk Management domain of SY0-701 [6:Chapter 17†CompTIA Security+ Study Guide].

Questions # 10:

Which of the following is a prerequisite for a DLP solution?

Options:

- A.
Data destruction
- B.
Data sanitization
- C.
Data classification
- D.
Data masking

Answer

C

Explanation

Data classification is required before implementing a Data Loss Prevention (DLP) solution because DLP policies depend on identifying and categorizing sensitive data to monitor, block, or encrypt it accordingly.

Data destruction (A) and sanitization (B) remove data, and masking (D) obscures data but classification is foundational for DLP effectiveness.

Data classification is emphasized in Security Program Management and Data Protection topics [6:Chapter 16†CompTIA Security+ Study Guide].



CertsMania



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