Free Questions for SY0-701 by certscare

Shared by Simon on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening'?

Options:

A- Using least privilege

B- Changing the default password

C- Assigning individual user IDs

D- Reviewing logs more frequently

Answer:

B

Explanation:

Changing the default password for the local administrator account on a VPN appliance is a basic security measure that would have most likely prevented the unexpected login to the remote management interface. Default passwords are often easy to guess or publicly

available, and attackers can use them to gain unauthorized access to devices and systems. Changing the default password to a strong and unique one reduces the risk of brute-force attacks and credential theft. Using least privilege, assigning individual user IDs, and reviewing logs more frequently are also good security practices, but they are not as effective as changing the default password in preventing the unexpected login.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 116;Local Admin Accounts - Security Risks and Best Practices (Part 1)

Question 2

Question Type: **MultipleChoice**

A company is working with a vendor to perform a penetration test Which of the following includes an estimate about the number of hours required to complete the engagement?

Options:

A- SOW

B- BPA

C- SLA

D- NDA

Answer:

A

Explanation:

A statement of work (SOW) is a document that defines the scope, objectives, deliverables, timeline, and costs of a project or service. It typically includes an estimate of the number of hours required to complete the engagement, as well as the roles and responsibilities of the parties involved. A SOW is often used for penetration testing projects to ensure that both the client and the vendor have a clear and mutual understanding of what is expected and how the work will be performed. A business partnership agreement (BPA), a service level agreement (SLA), and a non-disclosure agreement (NDA) are different types of contracts that may be related to a penetration testing project, but they do not include an estimate of the number of hours required to complete the engagement.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 492;What to Look For in a Penetration Testing Statement of Work?

Question 3

Question Type: MultipleChoice

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.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

Question 4

Question Type: MultipleChoice

Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

Options:

A- Mitigate

B- Accept

C- Transfer

D- Avoid

Answer:

A

Explanation:

Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy

first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk management strategies, but they are not the best options for this scenario. Accept means acknowledging the risk and accepting the consequences without taking any action. Transfer means shifting the risk to a third party, such as an insurance company or a vendor. Avoid means eliminating the risk by removing the source or changing the process.These strategies may not be feasible or desirable for a legacy application that is critical to business operations and has no preventative controls in place.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; A Risk-Based Framework for Legacy System Migration and Deprecation2

Question 5

Question Type: MultipleChoice

Which of the following incident response activities ensures evidence is properly handied?

Options:

A- E-discovery

B- Chain of custody

C- Legal hold

D- Preservation

Answer:

B

Explanation:

Chain of custody is the process of documenting and preserving the integrity of evidence collected during an incident response. It involves recording the details of each person who handled the evidence, the time and date of each transfer, and the location where the evidence was stored. Chain of custody ensures that the evidence is admissible in legal proceedings and can be traced back to its source. E-discovery, legal hold, and preservation are related concepts, but they do not ensure evidence is properly handled.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487;NIST SP 800-61: 3.2. Evidence Gathering and Handling

Question 6

Question Type: MultipleChoice

Which of the following describes the maximum allowance of accepted risk?

Options:

A- Risk indicator

B- Risk level

C- Risk score

D- Risk threshold

Answer:

D

Explanation:

Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 34;Accepting Risk: Definition, How It Works, and Alternatives

Question 7

Question Type: **MultipleChoice**

A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

Options:

A- Hashing

B- Tokenization

C- Encryption

D- Segmentation

Answer:

C

Explanation:

Encryption is a method of transforming data in a way that makes it unreadable without a secret key necessary to decrypt the data back into plaintext. Encryption is one of the most common and effective ways to protect data at rest, as it prevents unauthorized access, modification, or theft of the data. Encryption can be applied to different types of data at rest, such as block storage, object storage, databases, archives, and so on. Hashing, tokenization, and segmentation are not methods of rendering data at rest unreadable, but rather of protecting data in other ways. Hashing is a one-way function that generates a fixed-length output, called a hash or digest, from an input, such that the input cannot be recovered from the output. Hashing is used to verify the integrity and authenticity of data, but not to encrypt it. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, called tokens, that have no meaning or

value on their own. Tokenization is used to reduce the exposure and compliance scope of sensitive data, but not to encrypt it. Segmentation is a technique that divides a network or a system into smaller, isolated units, called segments, that have different levels of access and security.Segmentation is used to limit the attack surface and contain the impact of a breach, but not to encrypt data at rest.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, pages 77-781; Protecting data at rest - Security Pillar3

Question 8

Question Type: MultipleChoice

Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule Which of the following but describes this form of security control?

Options:

A- Physical

B- Managerial

C- Technical

D- Operational

Answer:

A

Explanation:

A physical security control is a device or mechanism that prevents unauthorized access to a physical location or asset. An access control vestibule, also known as a mantrap, is a physical security control that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. This prevents unauthorized individuals from following authorized individuals into the facility, a practice known as piggybacking or tailgating. A photo ID check is another form of physical security control that verifies the identity of visitors.Managerial, technical, and operational security controls are not directly related to physical access, but rather to policies, procedures, systems, and processes that support security objectives.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

Question 9

Question Type: MultipleChoice

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis Which of the following types of controls is the company setting up?

Options:

A- Corrective

B- Preventive

C- Detective

D- Deterrent

Answer:

C

Explanation:

A detective control is a type of security control that monitors and analyzes events to detect and report on potential or actual security incidents. A SIEM system is an example of a detective control, as it collects, correlates, and analyzes security data from various sources and generates alerts for security teams. Corrective, preventive, and deterrent controls are different types of security controls that aim to restore, protect, or discourage security breaches, respectively.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 33;What is Security Information and Event Management (SIEM)?

Question 10

Question Type: MultipleChoice

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

Options:

A- Deploying PowerShell scripts

B- Pushing GPO update

C- Enabling PAP

D- Updating EDR profiles

Answer:

B

Explanation:

A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 115;Password Policy - Windows Security

Question 11

Question Type: MultipleChoice

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

Options:

A- A full inventory of all hardware and software

B- Documentation of system classifications

C- A list of system owners and their departments

D- Third-party risk assessment documentation

Answer:

A

Explanation:

A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones.Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

Question 12

Question Type: MultipleChoice

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

Options:

A- Vishing

B- Smishing

C- Pretexting

D- Phishing

Answer:

B

Explanation:

Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic.Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs.Phishing: Understanding the Differences2