Free Questions for SY0-701 by ebraindumps

Shared by Baird on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

Options:

A- Key stretching

B- Tokenization

C- Data masking

D- Salting

Answer:

D

Explanation:

Adding a random string of characters, known as a 'salt,' to a password before hashing it is known as salting. This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it

much harder for attackers to crack passwords using precomputed tables. Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Question 2

Question Type: MultipleChoice

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. Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Question 3

Question Type: MultipleChoice

A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

Options:

A- Memory injection

B- Race condition

C- Side loading

D- SQL injection

Answer:

A

Explanation:

Memory injection vulnerabilities allow unauthorized code or commands to be executed within a software program, leading to abnormal behavior such as generating outbound traffic over random high ports. This issue often arises from software not properly validating or encoding input, which can be exploited by attackers to inject malicious code. Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Question 4

Question Type: MultipleChoice

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

Options:

A- ARO

B- RTO

C- RPO

D- ALE

E- SLE

Answer:

D

Explanation:

The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions. Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Question 5

Question Type: MultipleChoice

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.

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.Reference: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

Question 6

Question Type: MultipleChoice

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup dat

a. Which of the following should the company consider?

Options:

A- Geographic dispersion

B- Platform diversity

C- Hot site

D- Load balancing

Answer:

A

Explanation:

Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449;Disaster Recovery Planning: Geographic Diversity