Free Questions for SY0-601

Shared by Walter on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker most likely attempting?

Options:

A- A spear-phishing attach

B- A watering-hole attack

C- Typo squatting

D- A phishing attack

Answer:

B

Explanation:

The attacker is most likely attempting a watering-hole attack. A watering-hole attack is a type of attack that targets a specific group of users by compromising a website that they frequently visit. The attacker then installs malware on the website that infects the visitors' devices or redirects them to malicious sites.The attacker hopes to gain access to the users' credentials, data, or networks by exploiting their trust in the legitimate website2.

Question 2

Question Type: MultipleChoice

A security analyst has been tasked with ensuring all programs that are deployed into the enterprise have been assessed in a runtime environment Any critical issues found in the program must be sent back to the developer for verification and remediation. Which of the following lost describes the type of assessment taking place?

Options:

A- Input validation

B- Dynamic code analysis

C- Fuzzing
D- Manual code review

Answer:

B

Explanation:

Dynamic code analysis is a technique that tests and analyzes an application during runtime to identify potential vulnerabilities, errors, or performance issues. Dynamic code analysis can detect problems that may not be visible in the source code or during static analysis, such as memory leaks, buffer overflows, or input validation errors. Dynamic code analysis can also simulate real-world scenarios and user inputs to evaluate the behavior and functionality of the application.Reference:CompTIA Security+ SY0-601 Certification Study Guide, Chapter 5: Implementing Host Security Solutions, page 246;What is Dynamic Code Analysis?

Question 3

Question Type: MultipleChoice

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 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 acmetimekeeping.com to a 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 malicious machine.

Answer:

D

Explanation:

ARP poisoning is a technique by which an attacker sends spoofed ARP messages to alter routing on a local area network.It can be used to intercept, modify, or stop data frames, or launch other attacks3In this scenario, the attacker likely used ARP poisoning to associate their MAC address with the IP address of the time-keeping website, causing the kiosks to send a copy of all the submitted credentials to the attacker's machine.This explains why only the credentials of the employees who clocked in and out while inside the building were stolen, and why the compromise was not detected by the DNS servers or the website itself4

Question 4

Question Type: MultipleChoice

Which of the following test helps to demonstrate integrity during a forensics investigation?

Options:

A- Event logs
B- Encryption
C- Hashing
D- Snapshots

Answer:

C

Explanation:

Hashing is a process that applies a mathematical algorithm to a data set, such as a file or a message, and produces a fixed-length string of characters called a hash or a digest. Hashing helps to demonstrate integrity during a forensics investigation because it can verify that the data has not been altered, corrupted, or tampered with. By comparing the hash values of the original and the copied data, investigators can ensure that they are identical and authentic.If the hash values are different, it means that the data has been modified in some way

Question 5

Question Type: MultipleChoice

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

Options:

A- Open-source intelligence

B- Bug bounty

C- Red team

D- Penetration testing

Answer:

B

Explanation:

A program that allows individuals to security test the company's internet-facing application and compensates researchers based on the vulnerabilities discovered is best described as a bug bounty program.A bug bounty program is an incentive-based program that rewards ethical hackers for finding and reporting security flaws in software or systems6.

Question 6

Question Type: MultipleChoice

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

Options:

A- A non-disclosure agreement
B- Least privilege
C- An acceptable use policy
D- Off boarding

Answer:

D

Explanation:

Off boarding is a security practice that involves revoking access rights and privileges from employees who leave an organization or change their roles. Off boarding can help address the issue of successful logon attempts to access the departed executive's accounts by disabling or deleting their accounts, changing passwords, collecting devices, etc., as soon as they leave the organization.

Question 7

Question Type: MultipleChoice

Which of the following scenarios best describes a risk reduction technique?

Options:

A- A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches
B- A security control objective cannot be met through a technical change, so the company implements a pokey to train users on a more secure method of operation
C- A security control objective cannot be met through a technical change, so the company performs regular audits to determine it violations have occurred
D- A security control objective cannot be met through a technical change, so the Chief Information Officer decides to sign off on the risk.

Answer:

B

Explanation:

A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation best describes a risk reduction technique. Risk reduction is a strategy that aims to lower the likelihood or impact of a risk by implementing controls or mitigations. For example, if a technical control is not feasible or cost-effective, a company can reduce the risk by educating users on how to avoid or handle the threat, such as using strong passwords, avoiding phishing emails, or reporting incidents.