PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company\\'s network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.

Which of the following actions should the tester take?

A. Perform forensic analysis to isolate the means of compromise and determine attribution.

B. Incorporate the newly identified method of compromise into the red team\\'s approach.

C. Create a detailed document of findings before continuing with the assessment.

D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Correct Answer: D

Halting the assessment and following the reporting procedures as outlined in the contract is the best action to take after identifying that an application being tested has already been compromised with malware. This is because continuing the assessment might interfere with an ongoing investigation or compromise evidence collection. The reporting procedures are part of the contract that specifies how to handle any critical issues or incidents during the penetration testing engagement. They should include details such as who to contact, what information to provide, and what steps to follow.

QUESTION 2

A potential reason for communicating with the client point of contact during a penetration test is to provide resolution if a testing component crashes a system or service and leaves them unavailable for both legitimate users and further testing. Which of the following best describes this concept?

A. Retesting

B. De-escalation

C. Remediation

D. Collision detection

Correct Answer: C

Communicating with the client point of contact during a penetration test, especially when a testing component crashes a system or service, is crucial for remediation. Remediation involves the process of correcting or mitigating vulnerabilities that have been identified during the test. In the context of a system or service becoming unavailable, it\\'s essential to promptly address and resolve the issue to restore availability and ensure the continuity of legitimate business operations. This communication ensures that the client is aware of the incident and can work together with the penetration tester to implement corrective actions, thereby minimizing the impact on the business and further testing activities.

QUESTION 3

A penetration tester successfully infiltrated the targeted web server and created credentials with administrative privileges. After conducting data exfiltration, which of the following should be the tester\\'s NEXT step?

A. Determine what data is available on the web server.

B. Change or delete the logs.

C. Log out and migrate to a new session.

D. Log in as the new user.

Correct Answer: D

QUESTION 4

A penetration tester discovers passwords in a publicly available data breach during the reconnaissance phase of the penetration test. Which of the following is the best action for the tester to take?

A. Add the passwords to an appendix in the penetration test report.

B. Do nothing. Using passwords from breached data is unethical.

C. Contact the client and inform them of the breach.

D. Use the passwords in a credential stuffing attack when the external penetration test begins.

Correct Answer: C

QUESTION 5

During the assessment of a client\\'s cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the provided on-premises credentials. Which of the following best describes why the tester was able to gain access?

A. Federation misconfiguration of the container

B. Key mismanagement between the environments

C. IaaS failure at the provider

D. Container listed in the public domain

Correct Answer: A

The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container. Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users. Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials.

Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.