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.geekcert.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

A. To provide feedback on the report structure and recommend improvements

B. To discuss the findings and dispute any false positives

C. To determine any processes that failed to meet expectations during the assessment

D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Correct Answer: C

QUESTION 2

During passive reconnaissance of a target organization\\'s infrastructure, a penetration tester wants to identify key contacts and job responsibilities within the company. Which of the following techniques would be the most effective for this situation?

A. Social media scraping

B. Website archive and caching

C. DNS lookup

D. File metadata analysis

Correct Answer: A

Social media scraping involves collecting information from social media platforms where employees might share their roles, responsibilities, and professional affiliations. This method can reveal detailed insights into the organizational structure, key personnel, and specific job functions within the target organization, making it an invaluable tool for understanding the company\\'s internal landscape without alerting the target to the reconnaissance activities.

QUESTION 3

A penetration tester joins the assessment team in the middle of the assessment. The client has asked the team, both verbally and in the scoping document, not to test the production networks. However, the new tester is not aware of this request and proceeds to perform exploits in the production environment. Which of the following would have MOST effectively prevented this misunderstanding?

A. Prohibiting exploitation in the production environment

B. Requiring all testers to review the scoping document carefully

C. Never assessing the production networks

D. Prohibiting testers from joining the team during the assessment

Correct Answer: B

The scoping document is a document that defines the objectives, scope, limitations, deliverables, and expectations of a penetration testing engagement. It is an essential document that guides the penetration testing process and ensures that both the tester and the client agree on the terms and conditions of the test. Requiring all testers to review the scoping document carefully would have most effectively prevented this misunderstanding, as it would have informed the new tester about the client\\'s request not to test the production networks. The other options are not effective or realistic ways to prevent this misunderstanding.

QUESTION 4

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider\\'s metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery

B. Server-side request forgery

C. Remote file inclusion

D. Local file inclusion

Correct Answer: B

Server-side request forgery (SSRF) is the vulnerability that the tester exploited by querying the provider\\'s metadata and getting the credentials used by the instance to authenticate itself. SSRF is a type of attack that abuses a web application to make requests to other resources or services on behalf of the web server. This can allow an attacker to access internal or external resources that are otherwise inaccessible or protected. In this case, the tester was able to access the metadata service of the cloud provider, which contains sensitive information about the instance, such as credentials, IP addresses, roles, etc.

Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

QUESTION 5

A penetration tester is taking screen captures of hashes obtained from a domain controller. Which of the following best explains why the penetration tester should immediately obscure portions of the images before saving?

A. To maintain confidentiality of data/information

B. To avoid disclosure of how the hashes were obtained

C. To make the hashes appear shorter and easier to crack

D. To prevent analysis based on the type of hash

Correct Answer: A

When a penetration tester captures screen images that include hashes from a domain controller, obscuring parts of these images before saving is crucial to maintain the confidentiality of sensitive data. Hashes can be considered sensitive information as they represent a form of digital identity for users within an organization. Revealing these hashes in full could lead to unauthorized access if the hashes were to be cracked or otherwise misused by malicious actors. By

partially obscuring the images, the penetration tester ensures that the data remains confidential and reduces the risk of compromising user accounts and the integrity of the organization\\'s security posture.