PT0-002Q&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.pass2lead.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 penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig:

comptia.org. 3569 IN MX comptia.org-mail.protection.outlook.com. comptia.org. 3569 IN A 3.219.13.186. comptia.org.

3569 IN NS ns1.comptia.org. comptia.org. 3569 IN SOA haven. administrator.comptia.org. comptia.org. 3569 IN MX new.mx0.comptia.org. comptia.org. 3569 IN MX new.mx1.comptia.org.

Which of the following potential issues can the penetration tester identify based on this output?

A. At least one of the records is out of scope.

B. There is a duplicate MX record.

C. The NS record is not within the appropriate domain.

D. The SOA records outside the comptia.org domain.

Correct Answer: A

QUESTION 2

A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

A. Add a dependency checker into the tool chain.

B. Perform routine static and dynamic analysis of committed code.

C. Validate API security settings before deployment.

D. Perform fuzz testing of compiled binaries.

Correct Answer: A

QUESTION 3

During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign.

Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client\\'s cybersecurity tools? (Choose two.)

A. Scraping social media sites

B. Using the WHOIS lookup tool

C. Crawling the client\\'s website

D. Phishing company employees

E. Utilizing DNS lookup tools

F. Conducting wardriving near the client facility

Correct Answer: AC

Technical and billing addresses are usually posted on company websites and company social media sites for the their clients to access. The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.

QUESTION 4

A compliance-based penetration test is primarily concerned with: A. obtaining Pll from the protected network.

B. bypassing protection on edge devices.

C. determining the efficacy of a specific set of security standards.

D. obtaining specific information from the protected network.

Correct Answer: C

QUESTION 5

A penetration tester is explaining the MITRE ATTandCK framework to a company\\'s chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

A. Understanding the tactics of a security intrusion can help disrupt them.

B. Scripts that are part of the framework can be imported directly into SIEM tools.

C. The methodology can be used to estimate the cost of an incident better.

D. The framework is static and ensures stability of a security program overtime.

Correct Answer: A

Reference: https://attack.mitre.org/