

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.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

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



QUESTION 1

Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

- A. Use of non-optimized sort functions
- B. Poor input sanitization
- C. Null pointer dereferences
- D. Non-compliance with code style guide
- E. Use of deprecated Javadoc tags
- F. A cyclomatic complexity score of 3

Correct Answer: BC

QUESTION 2

A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

- A. `nmap192.168.1.1-5-PU22-25,80`
- B. `nmap192.168.1.1-5-PA22-25,80`
- C. `nmap192.168.1.1-5-PS22-25,80`
- D. `nmap192.168.1.1-5-Ss22-25,80`

Correct Answer: C

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

QUESTION 3

Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

- A. A quick description of the vulnerability and a high-level control to fix it
- B. Information regarding the business impact if compromised
- C. The executive summary and information regarding the testing company
- D. The rules of engagement from the assessment

Correct Answer: A

The systems administrator and the technical staff would be more interested in the technical aspect of the findings

QUESTION 4

A penetration tester is conducting an engagement against an internet-facing web application and planning a phishing campaign. Which of the following is the BEST passive method of obtaining the technical contacts for the website?

- A. WHOIS domain lookup
- B. Job listing and recruitment ads
- C. SSL certificate information
- D. Public data breach dumps

Correct Answer: A

The BEST passive method of obtaining the technical contacts for the website would be a WHOIS domain lookup. WHOIS is a protocol that provides information about registered domain names, such as the registration date, registrant's name and contact information, and the name servers assigned to the domain. By performing a WHOIS lookup, the penetration tester can obtain the contact information of the website's technical staff, which can be used to craft a convincing phishing email.

QUESTION 5

A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

- A. Cost of the assessment
- B. Report distribution
- C. Testing restrictions
- D. Liability

Correct Answer: B

[PT0-002 PDF Dumps](#)

[PT0-002 Practice Test](#)

[PT0-002 Exam Questions](#)