PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.pass4itsure.com/pt0-001.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 has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.

B. Identify the issues that can be remediated most quickly and address them first.

C. Implement the least impactful of the critical vulnerabilities\\' remediations first, and then address other critical vulnerabilities

D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long lime.

Correct Answer: D

QUESTION 2

A penetration tester runs the following on a machine:

```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $ (cat a.txt); do echo $i; done | wc -1
```

Which of the following will be returned?

B. 3

C. 5

D. 6

Correct Answer: B

QUESTION 3

In which of the following scenarios would a tester perform a Kerberoasting attack?

A. The tester has compromised a Windows device and dumps the LSA secrets.

B. The tester needs to retrieve the SAM database and crack the password hashes.

C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.

D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

Correct Answer: C

QUESTION 4

Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

A. Stack pointer register

B. Index pointer register

C. Stack base pointer

D. Destination index register

Correct Answer: A

Reference: http://www.informit.com/articles/article.aspx?p=704311andseqNum=3

QUESTION 5

When negotiating a penetration testing contract with a prospective client, which of the following disclaimers should be included in order to mitigate liability in case of a future breach of the client\\'s systems?

A. The proposed mitigations and remediations in the final report do not include a cost-benefit analysis.

B. The NDA protects the consulting firm from future liabilities in the event of a breach.

C. The assessment reviewed the cyber key terrain and most critical assets of the client\\'s network.

D. The penetration test is based on the state of the system and its configuration at the time of assessment.

Correct Answer: D