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.pass2lead.com/pt0-001.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

A penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A. Download the GHOST file to a Linux system and compile

gcc -o GHOST

test i:

 ./GHOST

B. Download the GHOST file to a Windows system and compile

gcc -o GHOST GHOST.c

test i:

 ./GHOST

C. Download the GHOST file to a Linux system and compile

gcc -o GHOST GHOST.c

test i:

./GHOST

D. Download the GHOST file to a Windows system and compile

gcc -o GHOST

test i:

 ./GHOST

Correct Answer: C

QUESTION 2

A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to exploit the NETBIOS name service?

A. arPspoof

B. nmap

C. responder

D. burpsuite

Correct Answer: B

Reference: http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/

QUESTION 3

Which of the following actions BEST matches a script kiddie\\'s threat actor?

A. Exfiltrate network diagrams to perform lateral movement.

B. Steal credit cards from the database and sell them in the deep web.

C. Install a rootkit to maintain access to the corporate network.

D. Deface the website of a company in search of retribution.

Correct Answer: B

Reference: https://www.skyetechnologies.com/2020/08/20/meet-the-threat-actors-part-1-script-kiddies/

QUESTION 4

A penetration tester is performing a code review against a web application Given the following URL and source code:

```
URL: http://example.com/dnslookup?domain=example1.com&server=192.168.1.1

if (is_admin(COOKIES['sessioncookie'])){
        $a="dig a"+GETREQUESTPARAM["domain"]+"@"+GETREQUESTPARAM["server"]
        print systemfunction($a)
```

Which of the following vulnerabilities is present in the code above?

A. SQL injection

B. Cross-site scripting

C. Command injection

D. LDAP injection

Correct Answer: C

QUESTION 5

Which of the following are MOST important when planning for an engagement? (Select TWO).

A. Goals/objectives

B. Architectural diagrams

C. Tolerance to impact

D. Storage time for a report

E. Company policies

Correct Answer: AC

[Latest PT0-001 Dumps](#)   [PT0-001 PDF Dumps](#)   [PT0-001 Practice Test](#)