



CompTIA

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

NEW QUESTION 1

DRAG DROP

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Zverlory
 Zverl0ry
 zv3rlory
 Zv3r!0ry

NEW QUESTION 2

The following command is run on a Linux file system: `Chmod 4111 /usr/bin/sudo`
 Which of the following issues may be exploited now?

- A. Kernel vulnerabilities
- B. Sticky bits
- C. Unquoted service path
- D. Misconfigured sudo

Answer: D

NEW QUESTION 3

Which of the following would be BEST for performing passive reconnaissance on a target's external domain?

- A. Peach
- B. CeWL
- C. OpenVAS
- D. Shodan

Answer: A

NEW QUESTION 4

A software development team recently migrated to new application software on the on-premises environment. Penetration test findings show that multiple vulnerabilities exist. If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment on the VM. Which of the following is MOST important for confirmation?

- A. Unsecure service and protocol configuration
- B. Running SMB and SMTP service
- C. Weak password complexity and user account
- D. Misconfiguration

Answer: A

NEW QUESTION 5

A penetration tester has successfully exploited an application vulnerability and wants to remove the command history from the Linux session. Which of the following will accomplish this successfully?

- A. `history --remove`
- B. `cat history | clear`
- C. `rm -f ./history`
- D. `history -c`

Answer: D

NEW QUESTION 6

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- A. Use path modification to escape the application's framework.
- B. Create a frame that overlays the application.
- C. Inject a malicious iframe containing JavaScript.
- D. Pass an iframe attribute that is malicious

Answer: B

NEW QUESTION 7

A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?

- A. Obtain staff information by calling the company and using social engineering techniques.
- B. Visit the client and use impersonation to obtain information from staff.
- C. Send spoofed emails to staff to see if staff will respond with sensitive information.
- D. Search the Internet for information on staff such as social networking site

Answer: C

NEW QUESTION 8

A penetration tester is checking a script to determine why some basic persisting. The expected result was the program outputting "True."

```

root:~$ cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File

root:~$ ./test.sh
False
    
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Select TWO)

- A. Change 'fi' to 'Endlf'
- B. Remove the 'let' in front of 'dest=5+5'.
- C. Change the '=' to '-eq'.
- D. Change 'source' and 'dest' to 'Ssource' and 'Sdest'
- E. Change 'else' to 'eli'

Answer: BC

NEW QUESTION 9

A penetration tester runs the following from a compromised box 'python -c -import pty;Pty.sPawn("/bin/bash").' Which of the following actions is the tester taking?

- A. Removing the Bash history
- B. Upgrading the shell
- C. Creating a sandbox
- D. Capturing credentials

Answer: A

NEW QUESTION 10

After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

- A. SOW
- B. NDA
- C. EULA
- D. BRA

Answer: D

NEW QUESTION 10

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
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 11

A penetration tester is utilizing social media to gather information about employees at a company. The tester has created a list of popular words used in employee profile s. For which of the following types of attack would this information be used?

- A. Explogt chaining
- B. Session hijacking
- C. Dictionary
- D. Karma

Answer: B

NEW QUESTION 12

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

Answer: C

NEW QUESTION 16

A company planned for and secured the budget to hire a consultant to perform a web application penetration test. Upon discovered vulnerabilities, the company asked the consultant to perform the following tasks:

- Code review
- Updates to firewall setting

- A. Scope creep
- B. Post-mortem review
- C. Risk acceptance
- D. Threat prevention

Answer: C

NEW QUESTION 18

Which of the following commands would allow a penetration tester to access a private network from the Internet in Metasploit?

- A. set rhost 192.168.1.10
- B. run autoroute -a 192.168.1.0/24
- C. db_nm«p -iL /tmp/privatehoots . txt

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PT0-001 Practice Exam Features:

- * PT0-001 Questions and Answers Updated Frequently
- * PT0-001 Practice Questions Verified by Expert Senior Certified Staff
- * PT0-001 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * PT0-001 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PT0-001 Practice Test Here](#)