



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
 Zv3rl0ry

NEW QUESTION 2

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

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

Answer: A

NEW QUESTION 3

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 4

When performing compliance-based assessments, which of the following is the MOST important Key consideration?

- A. Additional rate
- B. Company policy
- C. Impact tolerance

D. Industry type

Answer: A

NEW QUESTION 5

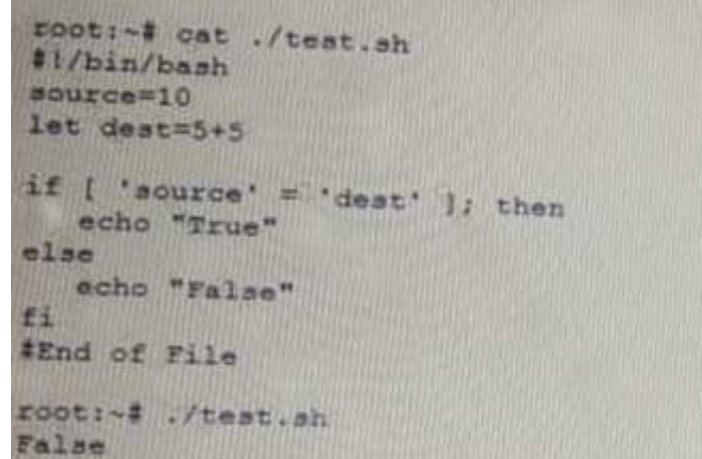
A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- 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 6

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
```

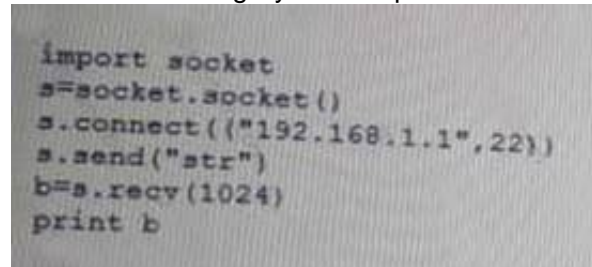
Given the output from the console above, which of the following explains how to correct the errors in the script? (Select TWO)

- 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 7

Given the following Python script:



```
import socket
s=socket.socket()
s.connect(("192.168.1.1",22))
s.send("str")
b=s.recv(1024)
print b
```

Which of the following actions will it perform?

- A. ARP spoofing
- B. Port scanner
- C. Reverse shell
- D. Banner grabbing

Answer: A

NEW QUESTION 8

A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer?

- A. Run the application through a dynamic code analyzer.
- B. Employ a fuzzing utility.
- C. Decompile the application.
- D. Check memory allocation

Answer: D

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

During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful. Which of the following would be the BEST target for continued exploitation efforts?

- A. Operating system Windows 7 Open ports: 23, 161
- B. Operating system Windows Server 2016 Open ports: 53, 5900
- C. Operating system Windows 8.1 Open ports: 445, 3389
- D. Operating system Windows 8 Open ports: 514, 3389

Answer: C

NEW QUESTION 10

A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

- A. Advanced persistent threat
- B. Script kiddie
- C. Hactivist
- D. Organized crime

Answer: A

NEW QUESTION 12

Which of the following types of physical security attacks does a mantrap mitigate?

- A. Lock picking
- B. Impersonation
- C. Shoulder surfing
- D. Tailgating

Answer: D

NEW QUESTION 17

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 21

Which of the following reasons does penetration tester needs to have a customer's point-of -contact information available at all time? (Select THREE).

- A. To report indicators of compromise
- B. To report findings that cannot be exploited
- C. To report critical findings
- D. To report the latest published exploits
- E. To update payment information
- F. To report a server that becomes unresponsive
- G. To update the statement of work
- H. To report a cracked password

Answer: DEF

NEW QUESTION 23

An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email to obtain the CEO's login credentials. Which of the following types of attacks is this an example of?

- A. Elicitation attack
- B. Impersonation attack
- C. Spear phishing attack
- D. Drive-by download attack

Answer: B

NEW QUESTION 24

During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests?

- A. Ettercap
- B. Tcpdump
- C. Responder
- D. Medusa

Answer: D

NEW QUESTION 28

A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline?

- A. Discovery scan
- B. Stealth scan
- C. Full scan
- D. Credentialed scan

Answer: A

NEW QUESTION 33

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 profiles. For which of the following types of attack would this information be used?

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

Answer: B

NEW QUESTION 35

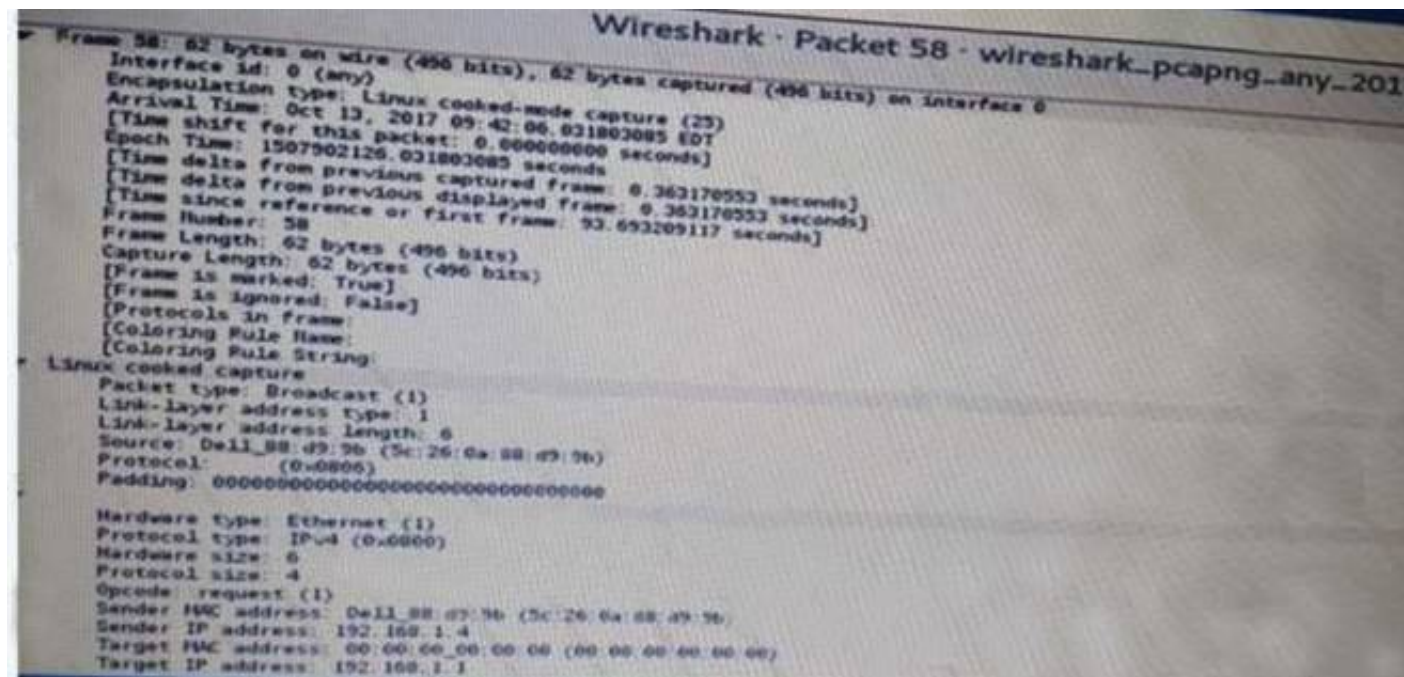
Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe is looking for a method that will enable him to enter the building during business hours or when there are no employees on-site. Which of the following would be MOST effective in accomplishing this?

- A. Badge cloning
- B. Lock picking
- C. Tailgating
- D. Piggybacking

Answer: A

NEW QUESTION 39

Click the exhibit button.



A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network Which of the following types of attacks should the tester stop?

- A. SNMP brute forcing
- B. ARP spoofing
- C. DNS cache poisoning
- D. SMTP relay

Answer: B

NEW QUESTION 44

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
- D. use auxiliary/servlet/aocka^a

Answer: D

NEW QUESTION 48

A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

- A. RID cycling to enumerate users and groups
- B. Pass the hash to relay credentials
- C. Password brute forcing to log into the host
- D. Session hijacking to impersonate a system account

Answer: C

NEW QUESTION 50

After successfully capturing administrator credentials to a remote Windows machine, a penetration tester attempts to access the system using PSEXec but is denied permission. Which of the following shares must be accessible for a successful PSEXec connection?

- A. IPCS and C\$
- B. C\$ and ADMIN\$
- C. SERVICES and ADMIN\$
- D. ADMIN\$ and IPCS

Answer: C

NEW QUESTION 52

In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

- A. Brute force the user's password.
- B. Perform an ARP spoofing attack.
- C. Leverage the BeEF framework to capture credentials.
- D. Conduct LLMNR/NETBIOS-ns poisonin

Answer: D

NEW QUESTION 53

A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < The tester runs the following command

nmap -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o —max rate 2 192. 168.130

Which of the following BEST describes why multiple IP addresses are specified?

- A. The network is submitted as a /25 or greater and the tester needed to access hosts on two different subnets

- B. The tester is trying to perform a more stealthy scan by including several bogus addresses
- C. The scanning machine has several interfaces to balance the scan request across at the specified rate
- D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Answer: C

NEW QUESTION 54

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry
- * PT0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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