



CompTIA

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

In which of the following components is an exploited vulnerability MOST likely to affect multiple running application containers at once?

- A. Common libraries
- B. Configuration files
- C. Sandbox escape
- D. ASLR bypass

Answer: D

NEW QUESTION 4

A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack. Which of the following remediation steps should be recommended? (Select THREE)

- A. Mandate all employees take security awareness training
- B. Implement two-factor authentication for remote access
- C. Install an intrusion prevention system
- D. Increase password complexity requirements
- E. Install a security information event monitoring solution.
- F. Prevent members of the IT department from interactively logging in as administrators
- G. Upgrade the cipher suite used for the VPN solution

Answer: BDG

NEW QUESTION 5

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 6

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 7

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 8

Which of the following BEST explains why it is important to maintain confidentiality of any identified findings when performing a penetration test?

- A. Penetration test findings often contain company intellectual property
- B. Penetration test findings could lead to consumer dissatisfaction if made public
- C. Penetration test findings are legal documents containing privileged information
- D. Penetration test findings can assist an attacker in compromising a system

Answer: C

NEW QUESTION 9

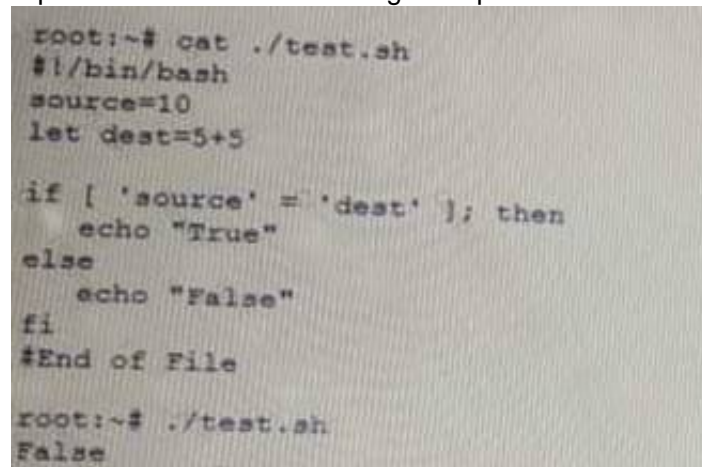
A recently concluded penetration test revealed that a legacy web application is vulnerable to SQL injection. Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not in a position to risk the availability of the application. Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Select TWO).

- A. Identify and eliminate inline SQL statements from the code.
- B. Identify and eliminate dynamic SQL from stored procedures.
- C. Identify and sanitize all user inputs.
- D. Use a whitelist approach for SQL statements.
- E. Use a blacklist approach for SQL statements.
- F. Identify the source of malicious input and block the IP address

Answer: DE

NEW QUESTION 10

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 10

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 13

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 16

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 19

While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

- A. Letter of engagement and attestation of findings
- B. NDA and MSA
- C. SOW and final report
- D. Risk summary and executive summary

Answer: D

NEW QUESTION 20

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 23

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 25

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 29

A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of the following BEST describes the types of adversaries this would identify?

- A. Script kiddies
- B. APT actors
- C. Insider threats
- D. Hacktrivist groups

Answer: B

NEW QUESTION 31

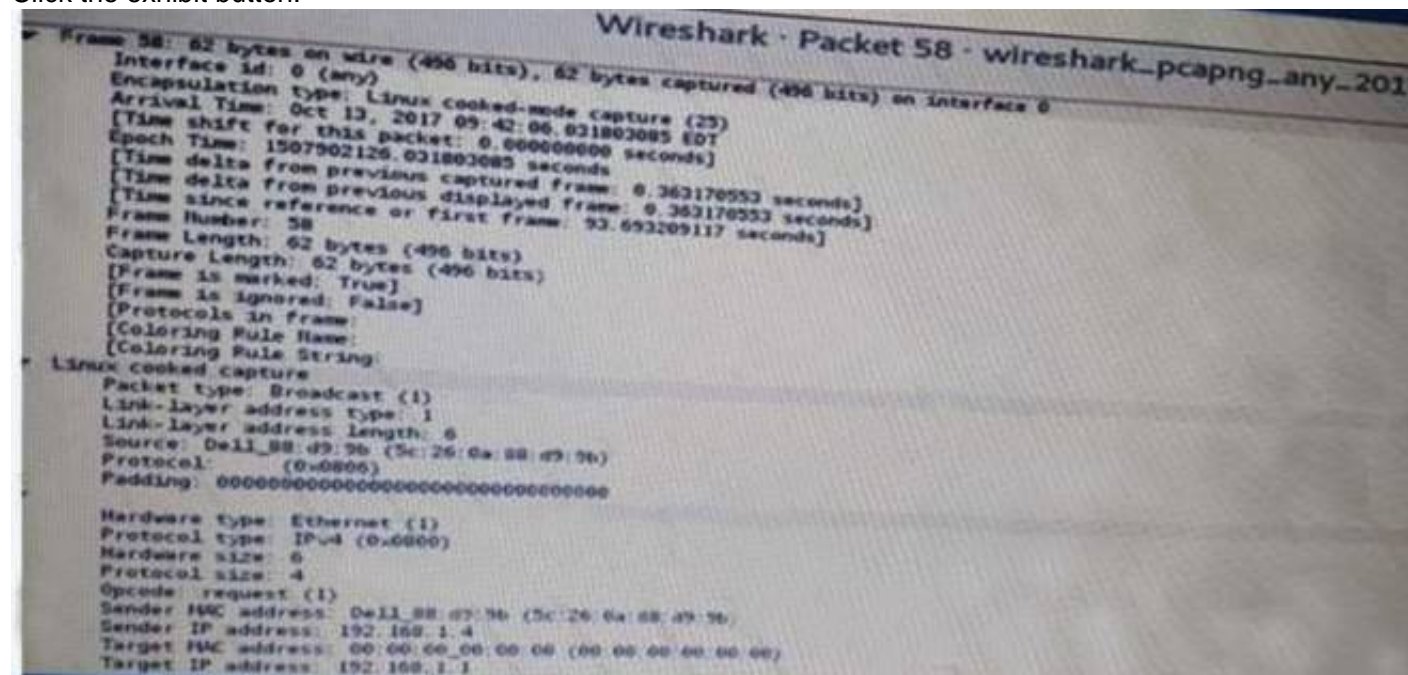
Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

- A. Stack pointer register
- B. Index pointer register
- C. Stack base pointer
- D. Destination index register

Answer: D

NEW QUESTION 33

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 35

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 37

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 38

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 42

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 por

Answer: A

NEW QUESTION 45

.....

Relate Links

100% Pass Your PT0-001 Exam with ExamBible Prep Materials

<https://www.exambible.com/PT0-001-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>