PT0-001 Dumps

CompTIA PenTest+ Certification Exam

https://www.certleader.com/PT0-001-dumps.html
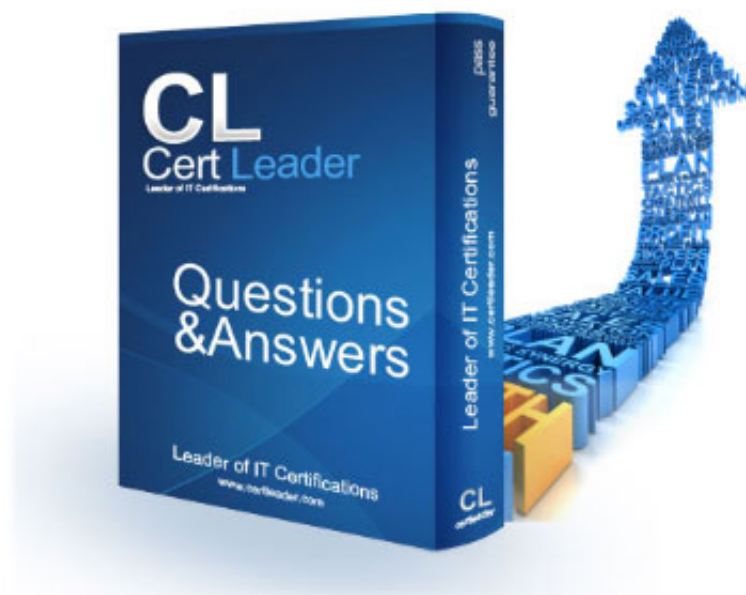
NEW QUESTION 1
DRAG DROP
Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented Each password may be used only once
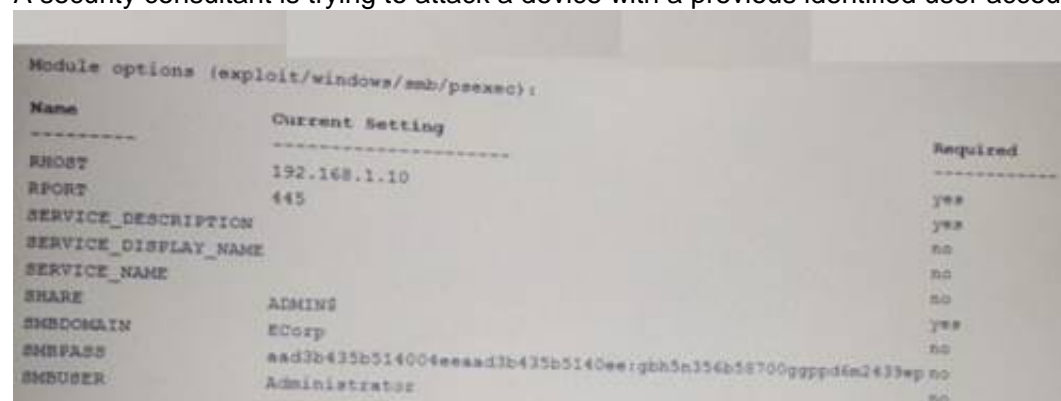

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Zverlory
Zverl0ry
zv3rlory
Zv3r!0ry

NEW QUESTION 2
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 3
The following command is run on a Linux file system: Chmod 4111 /usr/bin/sudo
Which of the following issues may be explogted now?

A. Kernel vulnerabilities
B. Sticky bits
C. Unquoted service path
D. Misconfigured sudo

Answer: D

NEW QUESTION 4
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 5
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
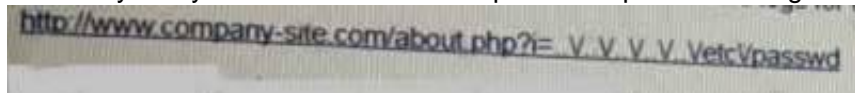
obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

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 6
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 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
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
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 notices that the X-Frame-Optjons header on a web application is not set. Which of the following would a malicious actor do to explogt 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 maliciou

Answer: B

NEW QUESTION 14
A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?

A. Obtain staff information by calling the company and using social engineering techniques.
B. Visit the client and use impersonation to obtain information from staff.
C. Send spoofed emails to staff to see if staff will respond with sensitive information.
D. Search the Internet for information on staff such as social networking site

Answer: C

NEW QUESTION 15
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 19
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 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
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
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 37
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 42
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 45
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 50
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 54
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 56
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 61
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 63
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 65
A company planned for and secured the budget to hire a consultant to perform a web application penetration test. Upon discovered vulnerabilities, the company asked the consultant to perform the following tasks:
• Code review
• Updates to firewall setting

A. Scope creep
B. Post-mortem review
C. Risk acceptance
D. Threat prevention

Answer: C

NEW QUESTION 70
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 71
Click the exhibit button.
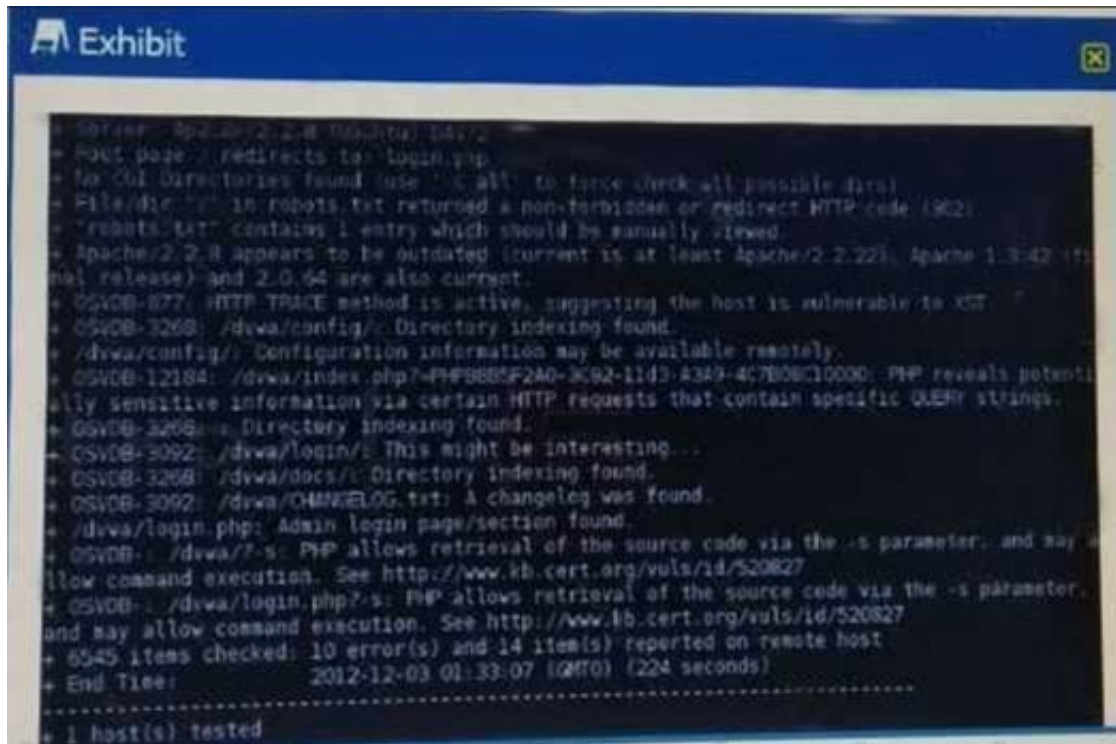
Given the Nikto vulnerability scan output shown in the exhibit, which of the following explogtation techniques might be used to explogt the target system? (Select TWO)

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

Answer: CE

NEW QUESTION 73
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 78
A penetration tester successfully explogts a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?

A)

    Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab

B)

    Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089e0:dfc312aeed12
    3

C)

    Administrator:$NTLM$11223344556677885B2B2220790F40C88BCFF347C652F67A7C4A70D3BEBD70233:::::::

D)

    Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788907659A550D5E9D02996DFD95C87EC1D5501010000
    000000000006CF6395B74CA01B3610B02D99732DD000000000200120

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

Answer: D

NEW QUESTION 80
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 83
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 88
A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < The tester runs the following command
nmap -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o —max rate 2 192. 168.130
Which ol the following BEST describes why multiple IP addresses are specified?

A. The network is submitted as a /25 or greater and the tester needed to access hosts on two different subnets
B. The tester is trying to perform a more stealthy scan by including several bogus addresses
C. The scanning machine has several interfaces to balance the scan request across at the specified rate
D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

Answer: C

NEW QUESTION 91
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
......

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