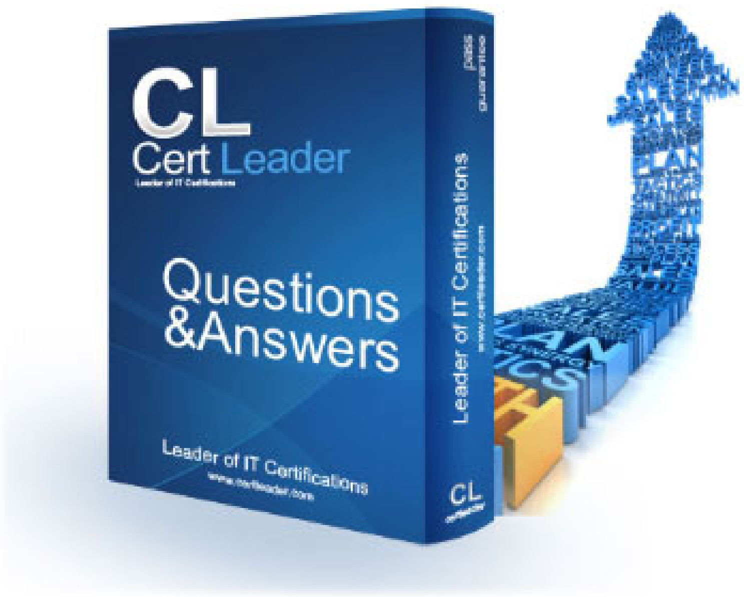
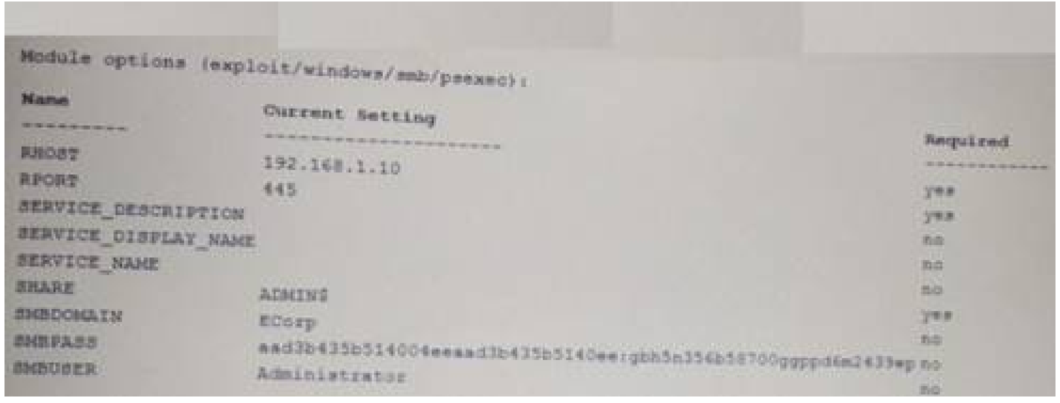
PT0-001 Dumps

CompTIA PenTest+ Certification Exam

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



NEW QUESTION 1
A security consultant is trying to attack a device with a previous identified user account.



```
Module options (exploit/windows/smb/psexec):

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                                                                  no
SMBUSER                  aad3b435b514004eeaad3b435b5140ee:gbh5n356b58700gppd6m2433ep no
                         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 2
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 3
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 4
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 5
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 6
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 7
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 explogted
C. To report critical findings
D. To report the latest published explogts
E. To update payment information
F. To report a server that becomes unresponsive
G. To update the statement o(work
H. To report a cracked password

Answer: DEF

NEW QUESTION 8
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 9
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 10
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 10
A penetration test was performed by an on-staff technicians 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 Ihe findtngs with an executive summary, recommendations, and screenshots of the web apphcation 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 implementedon 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.

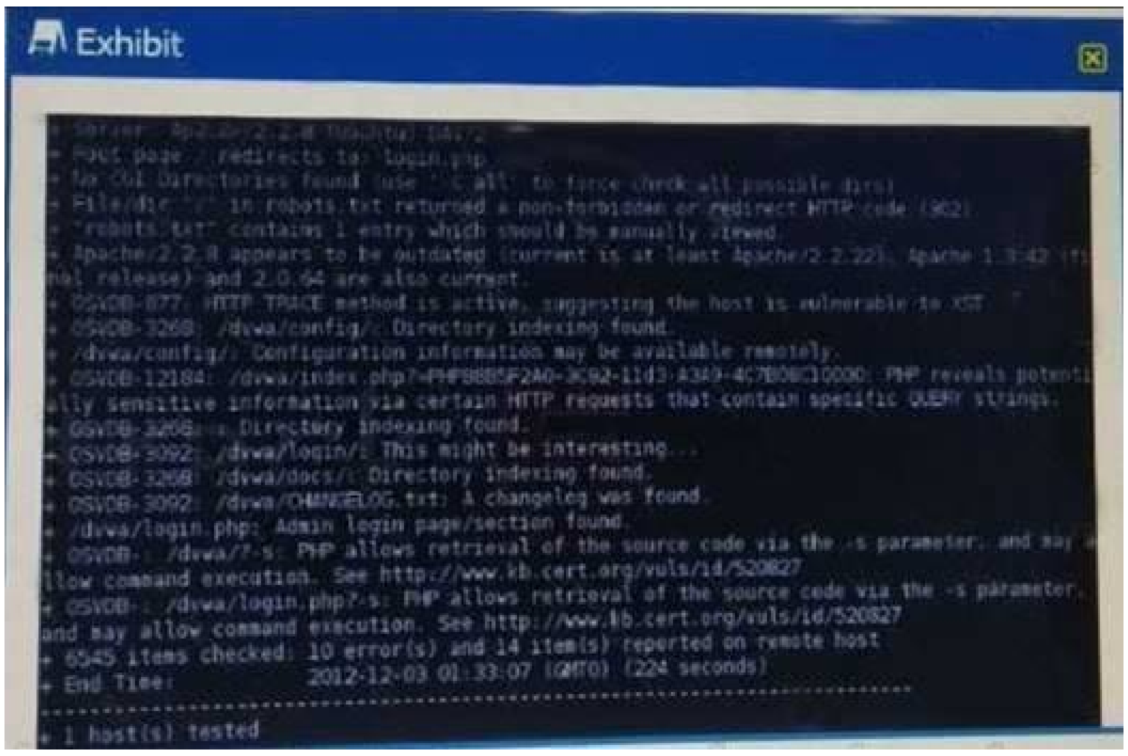
Answer: B

NEW QUESTION 11
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 13
Click the exhibit button.



```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (fi
nal release) and 2.0.64 are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ OSVDB-12184: /dvwa/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potenti
ally sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /dvwa/login/: This might be interesting...
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3092: /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+ OSVDB- : /dvwa/?-s: PHP allows retrieval of the source code via the -s parameter, and may a
llow command execution. See http://www.kb.cert.org/vuls/id/520827
+ OSVDB- : /dvwa/login.php?-s: PHP allows retrieval of the source code via the -s parameter,
and may allow command execution. See http://www.kb.cert.org/vuls/id/520827
+ 6545 items checked: 10 error(s) and 14 item(s) reported on remote host
+ End Time:           2012-12-03 01:33:07 (GMT0) (224 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

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

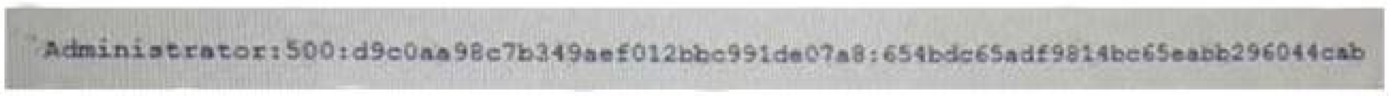
NEW QUESTION 15
Which of Ihe following commands would allow a penetration tester to access a private network from the Internet in Metasplogt?

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

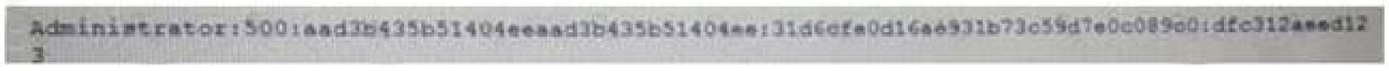
NEW QUESTION 16
A penetration tester successfully explogts a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?

A)



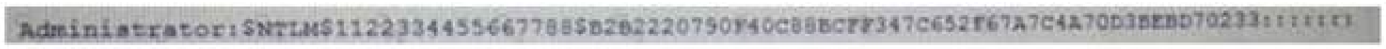
```
Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab
```

B)



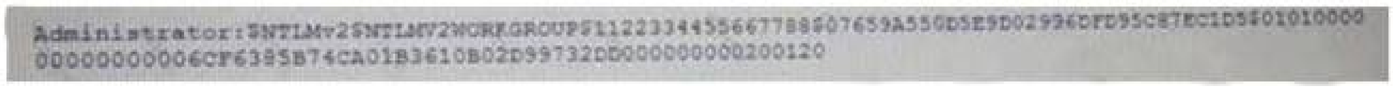
```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:dfc312aeed12
3
```

C)



```
Administrator:$NTLM$1122334455667788$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEBD70233::::::
```

D)



```
Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788$07659A550D5E9D02996DFD95C87EC1D5$01010000
000000000006CF6385B74CA01B3610B02D99732DD000000000200120
```

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

Answer: D

NEW QUESTION 20
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 24
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 26
......