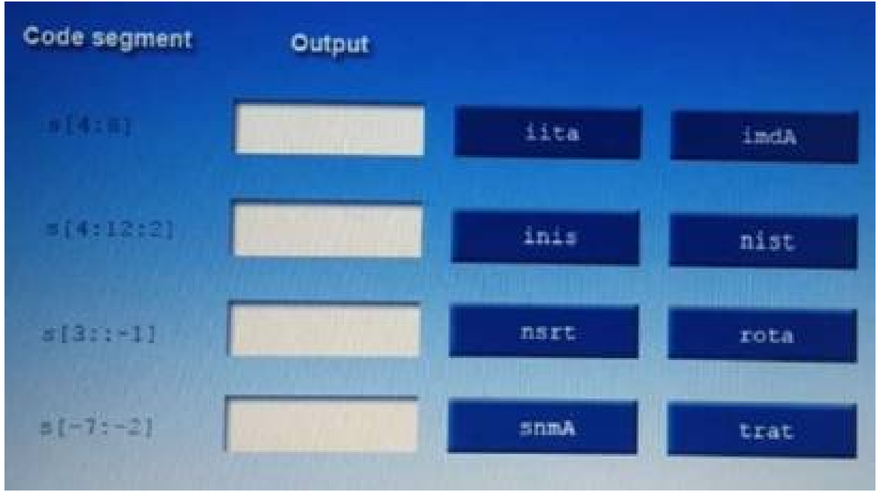
CompTIA

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

NEW QUESTION 1
DRAG DROP
A manager calls upon a tester to assist with diagnosing an issue within the following Python script:
#!/usr/bin/python
s = "Administrator"
The tester suspects it is an issue with string slicing and manipulation Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment Options may be used once or not at all



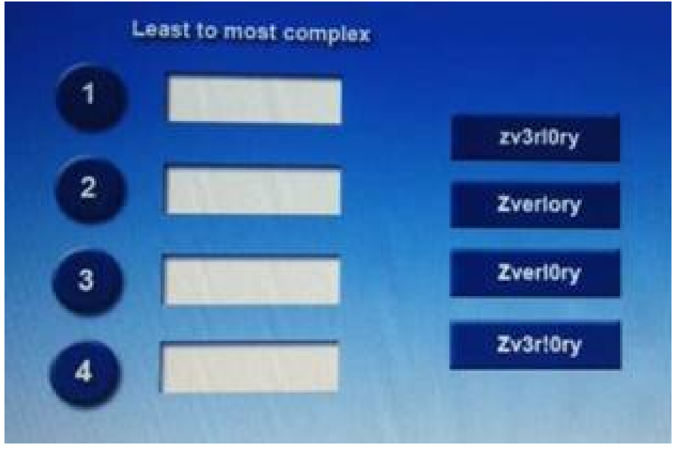
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Nsrt
Snma
Trat
Imda

NEW QUESTION 2
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:

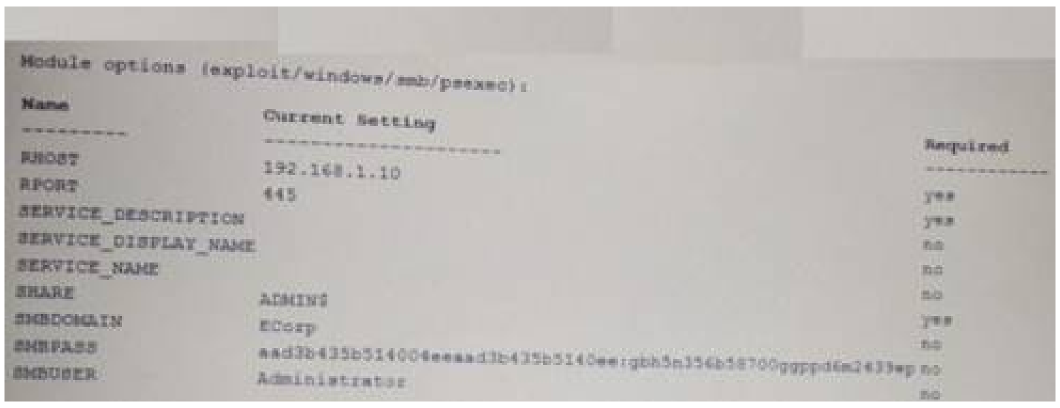
Zverlory
Zverl0ry
zv3rlory
Zv3r!0ry

NEW QUESTION 3
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 4
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                  aad3b435b51404eeaad3b435b51404ee:gbh5n356b58700gppd6m2433ep                    no
SMBUSER                  Administrator                                                                  no
                                                                                                        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 5
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

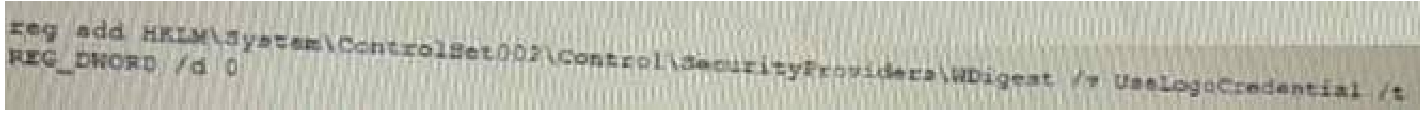
NEW QUESTION 6
A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood
B. SQL injection
C. xss
D. XMAS scan

Answer: A

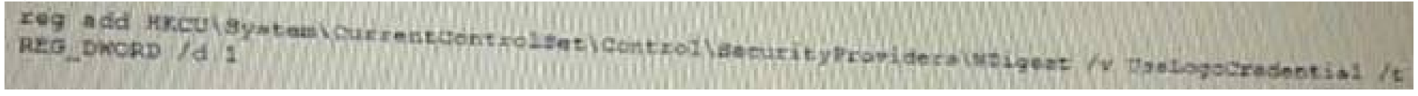
NEW QUESTION 7
During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikazt. Which of the following registry changes would allow for credential caching in memory?

A)



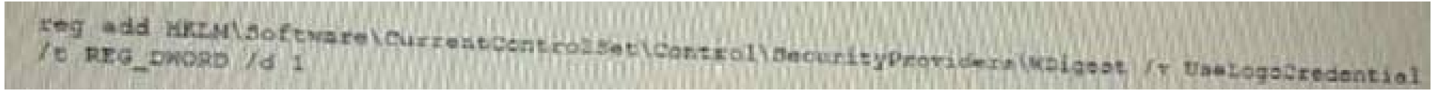
```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogonCredential /t
REG_DWORD /d 0
```

B)



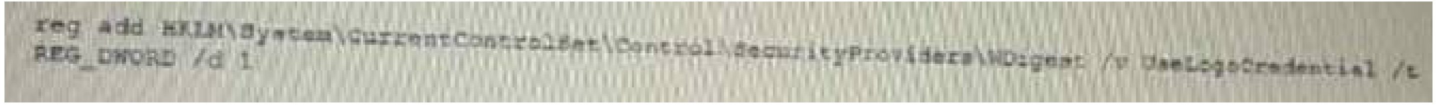
```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t
REG_DWORD /d 1
```

C)



```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential
/t REG_DWORD /d 1
```

D)



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

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

Answer: D

NEW QUESTION 8
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

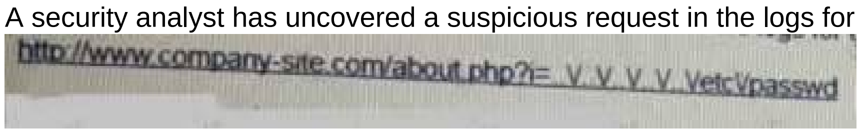
Answer: A

NEW QUESTION 9
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 10
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 10
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 12
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 17
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 cente

Answer: AB

NEW QUESTION 26
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

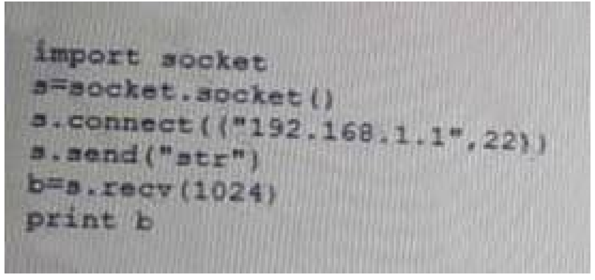
Answer: A

NEW QUESTION 31
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 36
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

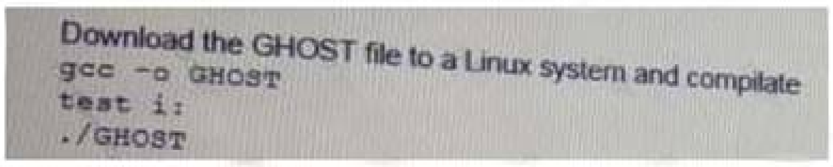
NEW QUESTION 41
During an internal network penetration test, a tester recovers the NTLM password hash tor a user known to have full administrator privileges on a number of target systems Efforts to crack the hash and recover the plaintext password have been unsuccessful Which of the following would be the BEST target for continued exploglation efforts?

A. Operating system Windows 7 Open ports: 23, 161
B. Operating system Windows Server 2016 Open ports: 53, 5900
C. Operating system Windows 8 1Open ports 445, 3389
D. Operating system Windows 8 Open ports 514, 3389

Answer: C

NEW QUESTION 46
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?

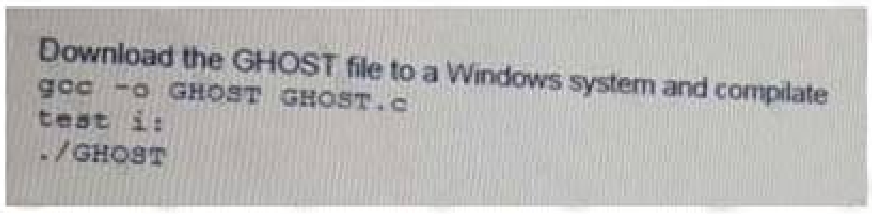
A)



Download the GHOST file to a Linux system and compilate

```
gcc -o GHOST
test i:
./GHOST
```

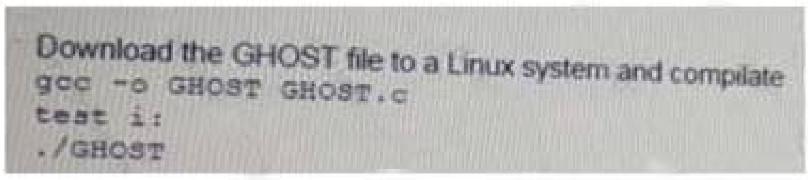
B)



Download the GHOST file to a Windows system and compilate

```
gcc -o GHOST GHOST.c
test i:
./GHOST
```

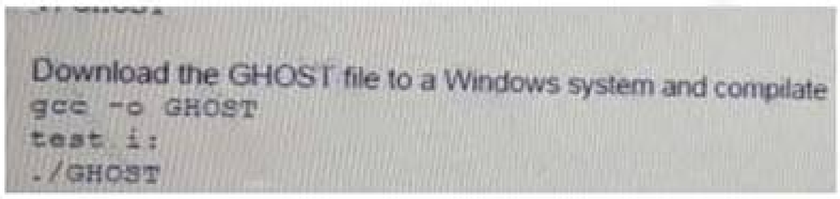
C)



Download the GHOST file to a Linux system and compilate

```
gcc -o GHOST GHOST.c
test i:
./GHOST
```

D)



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 47
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 48
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 49
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 51
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 53
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 58
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 62
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 65
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

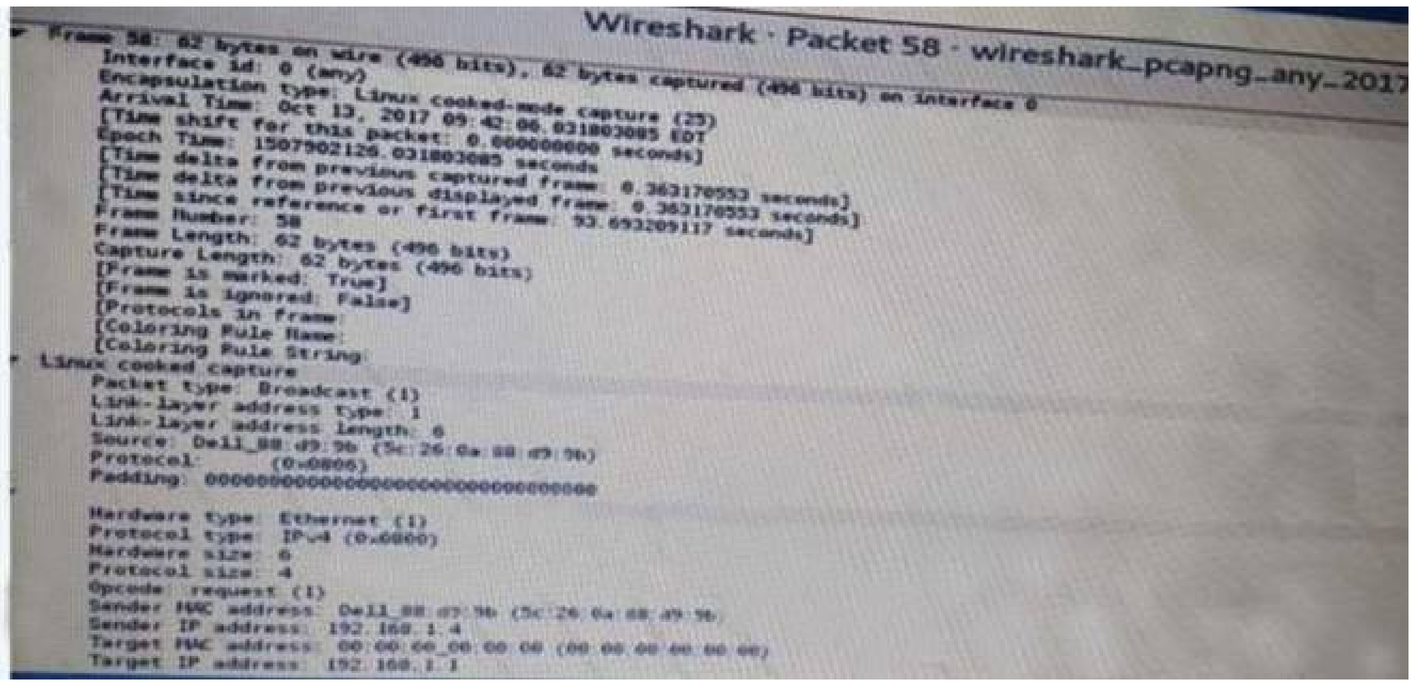
Answer: D

NEW QUESTION 68
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 73
Click the exhibit button.



```
Wireshark · Packet 58 · wireshark_pcapng_any_2017
▾ Frame 58: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
     Interface id: 0 (any)
     Encapsulation type: Linux cooked-mode capture (25)
     Arrival Time: Oct 13, 2017 09:42:06.031803085 EDT
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1507902126.031803085 seconds
     [Time delta from previous captured frame: 0.363170553 seconds]
     [Time delta from previous displayed frame: 0.363170553 seconds]
     [Time since reference or first frame: 93.693209117 seconds]
     Frame Number: 58
     Frame Length: 62 bytes (496 bits)
     Capture Length: 62 bytes (496 bits)
     [Frame is marked: True]
     [Frame is ignored: False]
     [Protocols in frame:
     [Coloring Rule Name:
     [Coloring Rule String:
▾ Linux cooked capture
     Packet type: Broadcast (1)
     Link-layer address type: 1
     Link-layer address length: 6
     Source: Dell_88:d9:9b (5c:26:0a:88:d9:9b)
     Protocol:        (0x0806)
     Padding: 00000000000000000000000000000000

     Hardware type: Ethernet (1)
     Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: request (1)
     Sender MAC address: Dell_88:d9:9b (5c:26:0a:88:d9:9b)
     Sender IP address: 192.168.1.4
     Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
     Target IP address: 192.168.1.1
```

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 74
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 75
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 78
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 81
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 84
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 89

......