- **Vendor:** CompTIA
- **Exam Code:** PT0-001
- **Exam Name:** CompTIA PenTest+ Exam
- **New Updated Questions from Braindump2go (Updated in Nov./2020)**

QUESTION 183
After successfully exploiting a local file inclusion vulnerability within a web application a limited reverse shell is spawned back to the penetration tester's workstation Which of the following can be used to escape the limited shell and create a fully functioning TTY?

A. per1 -e ' : set shall=/bin/bash:shell'
B. php -r ,Sshell=f3hellopen("/bin/bash-);exec($9he:i)'
C. bash -i >fi /dev/localhosc Oil
D. python -c 'import pty;pcy.3pawn("/bin/bash")'

Answer: D

QUESTION 184
When performing active information reconnaissance, which of the following should be tested FIRST before starting the exploitation process?

A. SQLmap
B. TLS configuration
C. HTTP verbs
D. Input fields

Answer: A

QUESTION 185
During a penetration test a tester Identifies traditional antivirus running on the exploited server. Which of the following techniques would BEST ensure persistence in a post-exploitation phase?

A. Shell binary placed in C:\windowsttemp
B. Modified daemons
C. New user creation
D. Backdoored executaWes

Answer: B

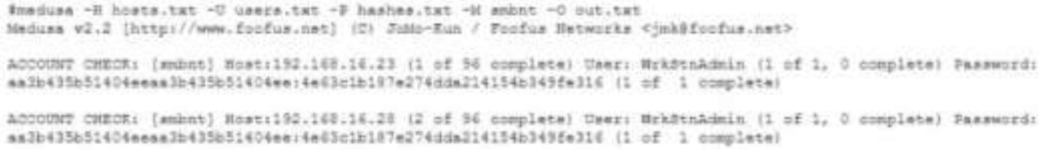
QUESTION 186
Which of the following attacks is commonly combined with cross-site scripting for session hijacking?

A. CSRF
B. Clickjacking
C. SQLI

D. RFI

Answer: A

QUESTION 187
During an internal network penetration test the tester is able to compromise a Windows system and recover the NTLM hash for a local wrltsrnAdrain account Attempting to recover the plaintext password by cracking the hash has proved to be unsuccessful, and the tester has decided to try a pass-the-hash attack to see if the credentials are reused on other in-scope systems Using the Medusa tool the tester attempts to authenticate to a list of systems, including the originally compromised host, with no success Given the output below:



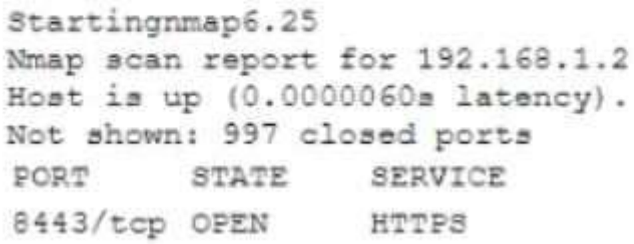
```
#medusa -H hosts.txt -U users.txt -P hashes.txt -M smbnt -O out.txt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [smbnt] Host:192.168.16.23 (1 of 96 complete) User: WrkStnAdmin (1 of 1, 0 complete) Password:
aa3b435b51404eeaa3b435b51404ee:4e63c1b187e274dda214154b349fe316 (1 of  1 complete)

ACCOUNT CHECK: [smbnt] Host:192.168.16.28 (2 of 96 complete) User: WrkStnAdmin (1 of 1, 0 complete) Password:
aa3b435b51404eeaa3b435b51404ee:4e63c1b187e274dda214154b349fe316 (1 of  1 complete)
```

Which of the following Medusa commands would potentially provide better results?

A. #medusa -h hosts.txt -U usera.txt -P hashes, txt -M smbnt. -m GROP:LOCAL -O out.txt -m PASS:HASH
B. #medusa -H hosts.txt -U users, txt -P hashes, txt -M smbnt -m PASS:HASH -o out. txt
C. #medusa -H hosts.txt -u WrkStnAdmin -p aa3b435b51404eeaa3b435b51404ee:4e63c1b137e274dda214154b349fe316 -M smbnt -m GROUP:DOMAIN -o out.txt
D. #medusa -H hosts.txt -C creds.txt -M mssq1 -m GROUP: DOMAIN -o out.txt

Answer: A

QUESTION 188
A penetration tester is performing a validation scan after an organization remediated a vulnerability on port 443 The penetration tester observes the following output:



```
Startingnmap6.25
Nmap scan report for 192.168.1.2
Host is up (0.0000060s latency).
Not shown: 997 closed ports
PORT       STATE      SERVICE
8443/tcp   OPEN       HTTPS
```

Which of the following has MOST likely occurred?

A. The scan results were a false positive.
B. The IPS is blocking traffic to port 443
C. A mismatched firewall rule is blocking 443.
D. The organization moved services to port 8443

Answer: D

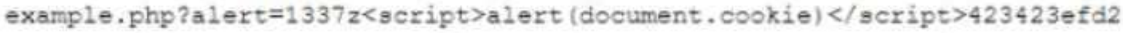
QUESTION 189
When communicating the findings of a network vulnerability scan to a client's IT department which of the following metrics BEST prioritize the severity of the findings? (Select TWO)

A. Threat map statistics
B. CVSS scores
C. Versions of affected software
D. Media coverage prevalence

E. Impact criticality
F. Ease of remediation

Answer: BE

QUESTION 190
While reviewing logs, a web developer notices the following user input string in a field:



```
example.php?alert=1337z<script>alert(document.cookie)</script>423423efd2
```

Which of the following types of attacks was done to the website?

A. XSS injection
B. Blind XSS
C. Reflected XSS
D. Persistent XSS

Answer: A

QUESTION 191
You can find XSS vulnerabilities in which of the following?

A. Search fields that echo a search string back to the user
B. HTTP headers
C. Input fields that echo user data
D. All of the above

Answer: D

QUESTION 192
A potential customer is looking to test the security of its network. One of the customer's primary concerns is the security awareness of its employees.
Which type of test would you recommend that the company perform as part of the penetration test?

A. Social engineering testing
B. Wireless testing
C. Network testing
D. Web application testing

Answer: A

QUESTION 193
Which tool included in Kali is most helpful in compiling a quality penetration testing report?

A. Nmap
B. Metasploit
C. Dradis
D. SET

Answer: C