312-50V9^{Q&As}

312-50V9^{Q&As}

Certified Ethical Hacker Exam V9

Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/312-50v9.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-
16])
Press 'q' or Ctrl-C to abort. almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

A. She is encrypting the file.

B. She is using John the Ripper to view the contents of the file.

C. She is using ftp to transfer the file to another hacker named John.

D. She is using John the Ripper to crack the passwords in the secret.txt file.

Correct Answer: D Section: (none)

QUESTION 2

Which tool would be used to collect wireless packet data?

A. NetStumbler

B. John the Ripper

C. Nessus

D. Netcat

Correct Answer: A Section: (none)

QUESTION 3

Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A. A race condition is being exploited, and the operating system is containing the malicious process.

B. A page fault is occurring, which forces the operating system to write data from the hard drive.

C. Malware is executing in either ROM or a cache memory area.

D. Malicious code is attempting to execute instruction in a non-executable memory region.

Correct Answer: D Section: (none)

QUESTION 4

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.

B. They send alerts to security monitors.

C. They use the same packet analysis engine.

D. They use the same packet capture utility.

Correct Answer: D Section: (none)

QUESTION 5

Emil uses nmap to scan two hosts using this command.

nmap -sS -T4 -O 192.168.99.1 192.168.99.7

He receives this output: What is his conclusion?

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT    STATE  SERVICE
21/tcp  open   ftp
23/tcp  open   telnet
53/tcp  open   domain
80/tcp  open   http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)


Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

A. Host 192.168.99.7 is an iPad.

B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.

C. Host 192.168.99.1 is the host that he launched the scan from.

D. Host 192.168.99.7 is down.

Correct Answer: B Section: (none)