312-50V9$^{Q\&As}$

Certified Ethical Hacker Exam V9

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

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

QUESTION 1

You\\'ve just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

A. TCP/IP doesn\\'t support ICMP

B. ARP is disabled on the target server

C. ICMP could be disabled on the target server D. You need to run the ping command with root privileges

Correct Answer: C Section: (none)

QUESTION 2

Perspective clients want to see sample reports from previous penetration tests.

What should you do next?

A. Decline but, provide references.

B. Share full reports, not redacted.

C. Share full reports with redactions.

D. Share reports, after NDA is signed.

Correct Answer: A Section: (none)

Penetration tests data should not be disclosed to third parties.

QUESTION 3

What kind of risk will remain even if all theoretically possible safety measures would be applied?

A. Residual risk

B. Inherent risk

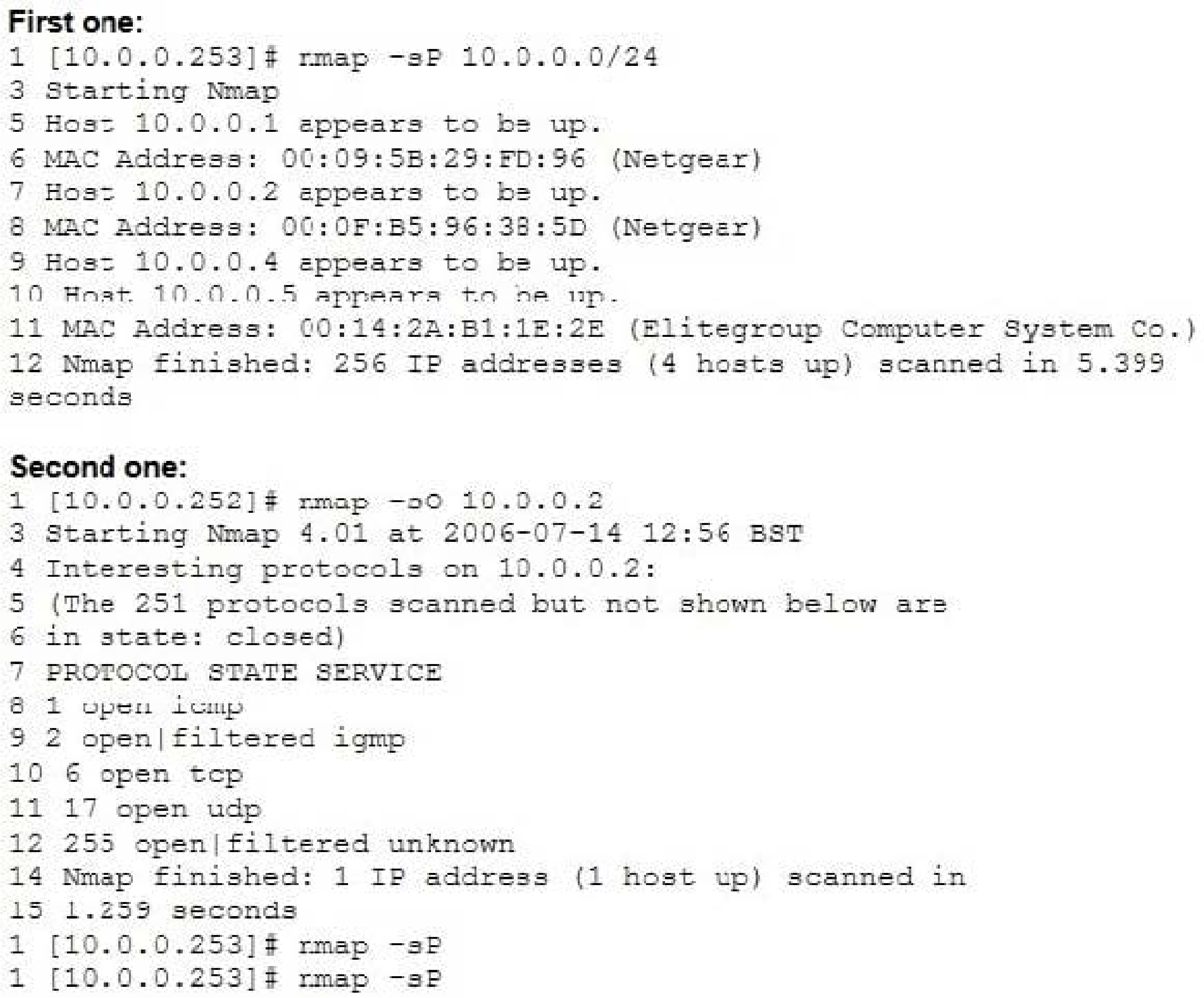
C. Impact risk

D. Deferred risk

Correct Answer: A Section: (none)

QUESTION 4

From the two screenshots below, which of the following is occurring?



First one:

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

Second one:

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against

10.0.0.2.

B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against

10.0.0.2.

C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against

10.0.0.2.

D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against

10.0.0.2.

Correct Answer: A Section: (none)

QUESTION 5

Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications

B. Register all machines MAC Address in a Centralized Database

C. Restrict Physical Access to Server Rooms hosting Critical Servers

D. Use Static IP Address

Correct Answer: A Section: (none)

A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn\\'t prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet\\'s payload so that all the sniffer sees is encrypted gibberish.

References: http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm