312-50V10$^{Q\&As}$

Certified Ethical Hacker Exam (C|EH v10)

Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee

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

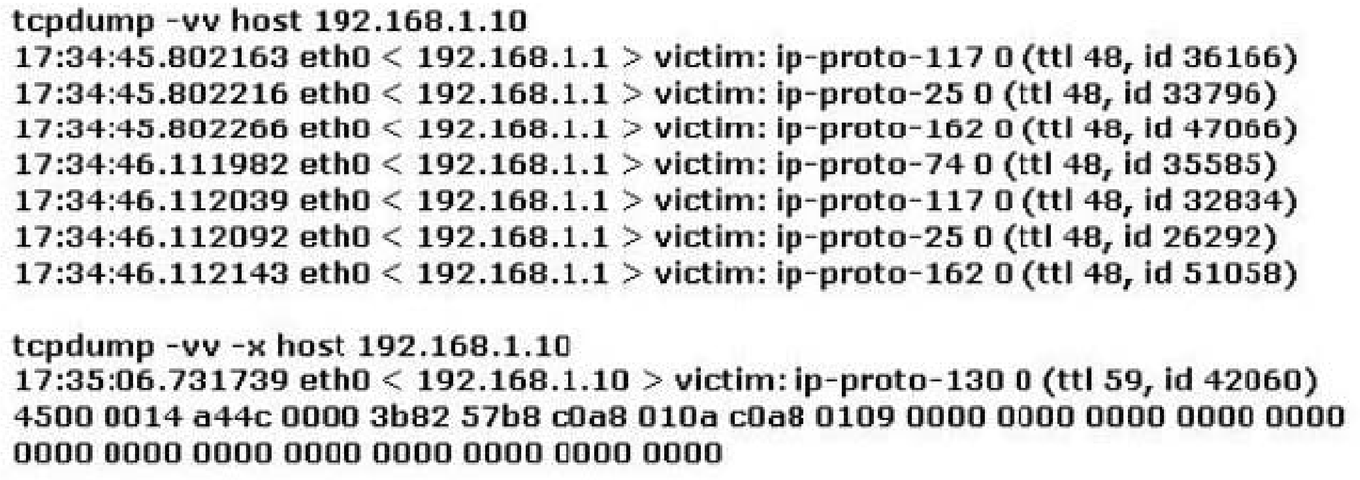
https://www.certbus.com/312-50v10.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Study the log below and identify the scan type.



```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)

tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060)
4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```

A. nmap -sR 192.168.1.10

B. nmap -sS 192.168.1.10

C. nmap -sV 192.168.1.10

D. nmap -sO -T 192.168.1.10

Correct Answer: D

QUESTION 2

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

A. Scripting languages are hard to learn.

B. Scripting languages are not object-oriented.

C. Scripting languages cannot be used to create graphical user interfaces.

D. Scripting languages are slower because they require an interpreter to run the code.

Correct Answer: D

QUESTION 3

The purpose of a __________ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Intrusion Prevention System

B. Wireless Access Point

C. Wireless Access Control List

D. Wireless Analyzer

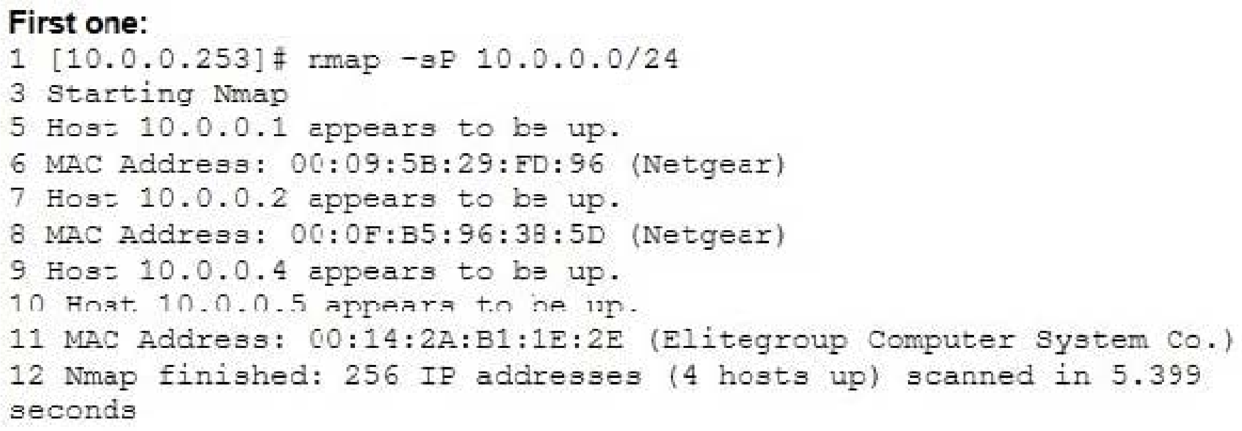
Correct Answer: A

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

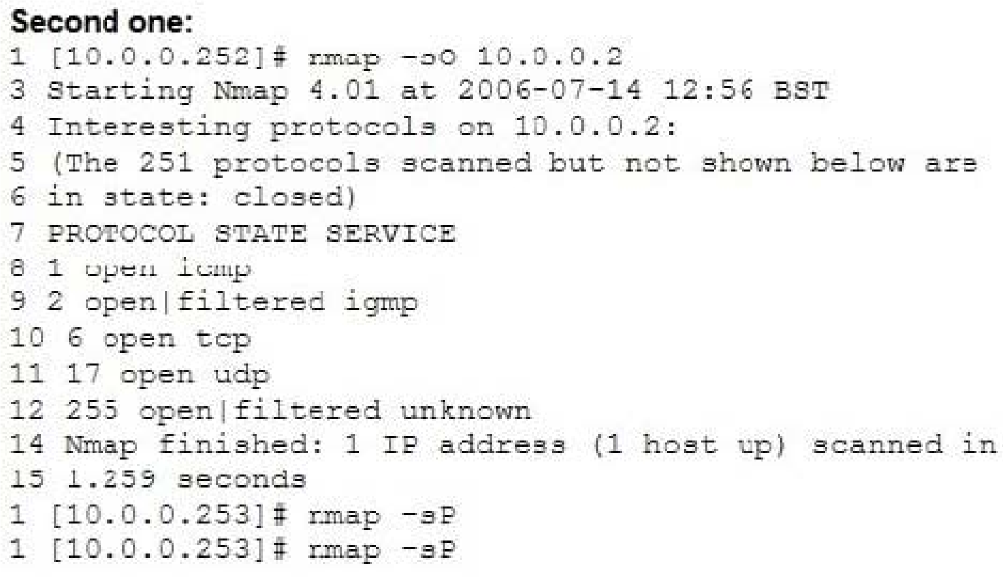
QUESTION 4

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



First one:

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



Second one:

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

QUESTION 5

Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 (content:"|00 01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111

B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet

C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the

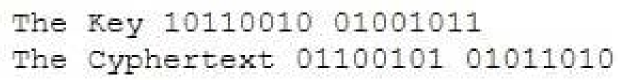
192.168.1.0 subnet

D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Correct Answer: D

QUESTION 6

A hacker was able to sniff packets on a company\\'s wireless network. The following information was discovered:



```
The Key 10110010 01001011
The Cyphertext 01100101 01011010
```

Using the Exlcusive OR, what was the original message?

A. 00101000 11101110

B. 11010111 00010001

C. 00001101 10100100

D. 11110010 01011011

Correct Answer: B

QUESTION 7

A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

A. Ignore it.

B. Try to sell the information to a well-paying party on the dark web.

C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.

D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

Correct Answer: C

QUESTION 8

Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth

B. Three-way handshake

C. Covert channels

D. Exponential backoff algorithm

Correct Answer: A

QUESTION 9

While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

A. Immediately stop work and contact the proper legal authorities

B. Ignore the data and continue the assessment until completed as agreed

C. Confront the client in a respectful manner and ask her about the data

D. Copy the data to removable media and keep it in case you need it

Correct Answer: A

QUESTION 10

Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True

B. False

Correct Answer: B

QUESTION 11

In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing

B. Key Stretching

C. Salting

D. Double Hashing

Correct Answer: C

QUESTION 12

Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code

B. Checking creation dates on all webpages on a server

C. Resetting the administrator password on multiple systems

D. Troubleshooting communication resets between two systems

Correct Answer: D

QUESTION 13

A penetration test was done at a company. After the test, a report was written and given to the company\\'s IT authorities. A section from the report is shown below:

According to the section from the report, which of the following choice is true?

A. MAC Spoof attacks cannot be performed.

B. Possibility of SQL Injection attack is eliminated.

C. A stateful firewall can be used between intranet (LAN) and DMZ.

D. There is access control policy between VLANs.

Correct Answer: C

QUESTION 14

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

A. Security through obscurity

B. Host-Based Intrusion Detection System

C. Defense in depth

D. Network-Based Intrusion Detection System

Correct Answer: C

QUESTION 15

What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

A. c:\compmgmt.msc

B. c:\gpedit

C. c:\ncpa.cpl

D. c:\services.msc

Correct Answer: A