CEH-001 Q&As

Certified Ethical Hacker (CEH)

Pass GAQM CEH-001 Exam with 100% Guarantee

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

https://www.passapply.com/ceh-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GAQM Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System

B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System

C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System

D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Correct Answer: A

QUESTION 2

An nmap command that includes the host specification of 202.176.56-57.* will scan _____ number of hosts.

A. 2

B. 256

C. 512

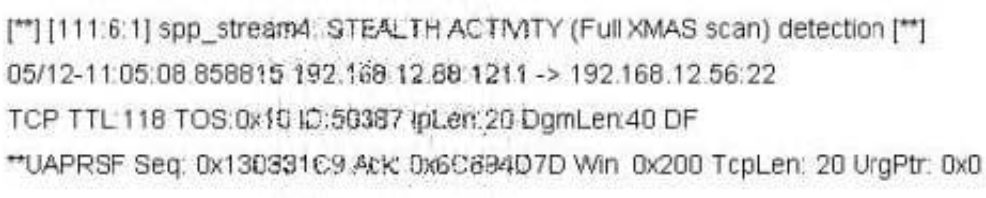
D. Over 10, 000

Correct Answer: C

QUESTION 3

Jason is the network administrator of Spears Technology. He has enabled SNORT IDS to detect attacks going through his network. He receives Snort SMS alerts on his iPhone whenever there is an attempted intrusion to his network.

He receives the following SMS message during the weekend.



An attacker Chew Siew sitting in Beijing, China had just launched a remote scan on Jason\\'s network with the hping command.

Which of the following hping2 command is responsible for the above snort alert?

A. chenrocks:/home/siew # hping -S -R -P -A -F -U 192.168.2.56 -p 22 -c 5 -t 118

B. chenrocks:/home/siew # hping -F -Q -J -A -C -W 192.168.2.56 -p 22 -c 5 -t 118

C. chenrocks:/home/siew # hping -D -V -R -S -Z -Y 192.168.2.56 -p 22 -c 5 -t 118

D. chenrocks:/home/siew # hping -G -T -H -S -L -W 192.168.2.56 -p 22 -c 5 -t 118

Correct Answer: A

QUESTION 4

What results will the following command yielD. \\'NMAP -sS -O -p 123-153 192.168.100.3\\'?

A. A stealth scan, opening port 123 and 153

B. A stealth scan, checking open ports 123 to 153

C. A stealth scan, checking all open ports excluding ports 123 to 153

D. A stealth scan, determine operating system, and scanning ports 123 to 153

Correct Answer: D

QUESTION 5

When analyzing the IDS logs, the system administrator notices connections from outside of the LAN have been sending packets where the Source IP address and Destination IP address are the same. There have been no alerts sent via

email or logged in the IDS.

Which type of an alert is this?

A. False positive

B. False negative

C. True positive

D. True negative

Correct Answer: B