

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.leads4pass.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

You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not ping packet?

```
[ceh]# ping 10.2.3.4
PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.
--- 10.2.3.4 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4
HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers +
0 data bytes
len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms
len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms
len=46 ip=10.2.3.4 flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms
--- 10.2.3.4 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

- A. Ping packets cannot bypass firewalls
- B. You must use ping 10.2.3.4 switch
- C. Hping2 uses stealth TCP packets to connect
- D. Hping2 uses TCP instead of ICMP by default

Correct Answer: D

QUESTION 2

You are scanning into the target network for the first time. You find very few conventional ports open. When you attempt to perform traditional service identification by connecting to the open ports, it yields either unreliable or no results. You are unsure of which protocols are being used. You need to discover as many different protocols as possible.

Which kind of scan would you use to achieve this? (Choose the best answer)

- A. Nessus scan with TCP based pings.
- B. Nmap scan with the P (Ping scan) switch.
- C. Netcat scan with the switches.
- D. Nmap with the O (Raw IP packets) switch.

Correct Answer: D

QUESTION 3

Why attackers use proxy servers?

- A. To ensure the exploits used in the attacks always flip reverse vectors
- B. Faster bandwidth performance and increase in attack speed
- C. Interrupt the remote victim's network traffic and reroute the packets to attackers machine
- D. To hide the source IP address so that an attacker can hack without any legal corollary

Correct Answer: D

QUESTION 4

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP
- C. Samba
- D. SMB

Correct Answer: D

QUESTION 5

When Jason moves a file via NFS over the company's network, you want to grab a copy of it by sniffing. Which of the following tool accomplishes this?

- A. macof
- B. webspay
- C. filesnarf
- D. nfscopy

Correct Answer: C

[Latest CEH-001 Dumps](#)

[CEH-001 PDF Dumps](#)

[CEH-001 Study Guide](#)