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.geekcert.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 tramitted, 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

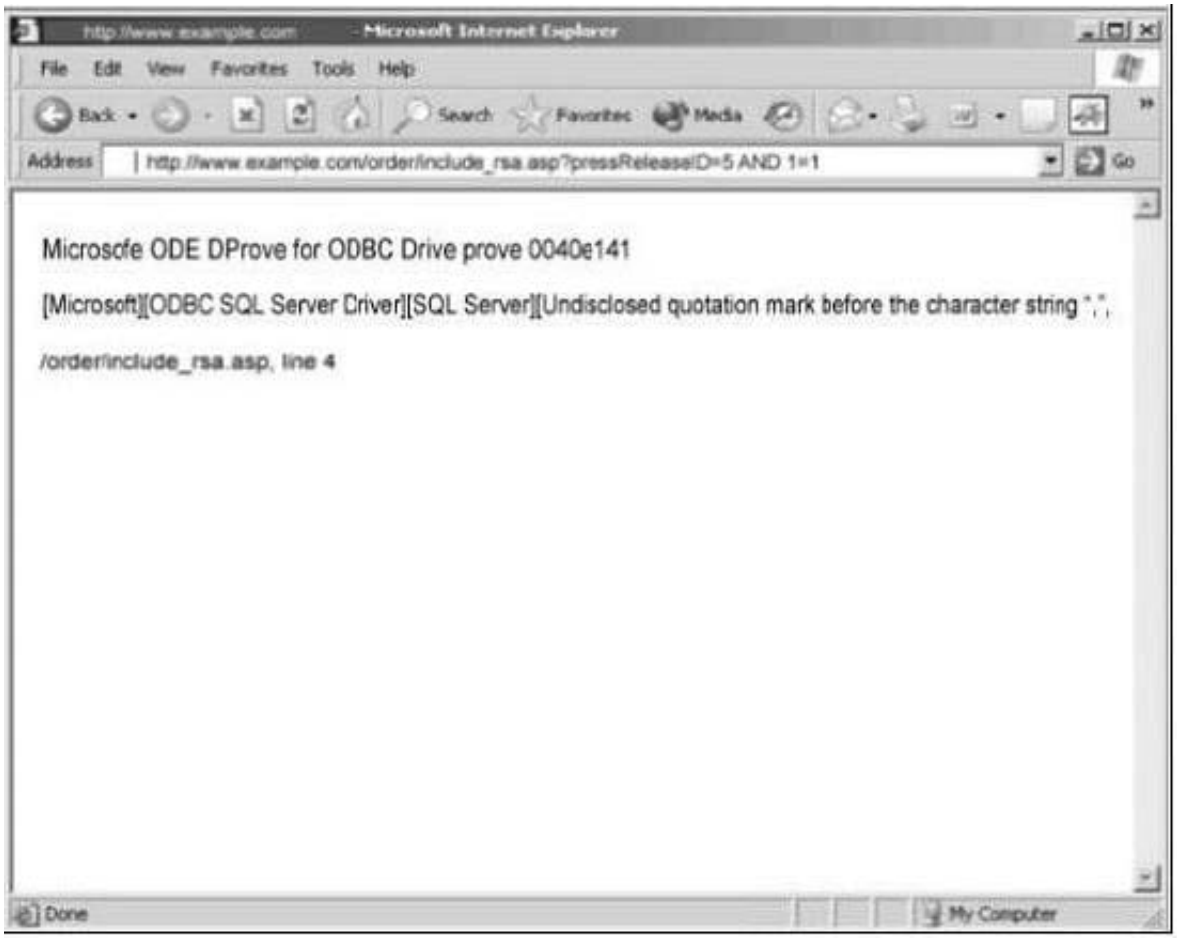
C. Hping2 uses stealth TCP packets to connect

D. Hping2 uses TCP instead of ICMP by default

Correct Answer: D

QUESTION 2

Exhibit:



You are conducting pen-test against a company\\'s website using SQL Injection techniques. You enter "anuthing or 1=1-" in the username filed of an authentication form. This is the output returned from the server.

What is the next step you should do?

A. Identify the user context of the web application by running_ http://www.example.com/order/include_rsa_asp?pressReleaseID=5 AND USER_NAME() = `dbo\\'

B. Identify the database and table name by running: http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype=\\'U\\'), 1))) > 109

C. Format the C: drive and delete the database by running: http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell `format c: /q /yes `; drop database myDB; -

D. Reboot the web server by running: http://www.example.com/order/include_rsa.asp?pressReleaseID=5 AND xp_cmdshell `iisreset eboot\\'; -

Correct Answer: A

QUESTION 3

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

Correct Answer: A

QUESTION 4

An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.

B. The wrong network card drivers were in use by Wireshark.

C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.

D. Certain operating systems and adapters do not collect the management or control packets.

Correct Answer: D

QUESTION 5

Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.

B. Firewall proxy servers decentralize all activity for an application.

C. Proxy firewalls block network packets from passing to and from a protected network.

D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Correct Answer: D