312-50V7^{Q&As}

312-50V7^{Q&As}

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.geekcert.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update
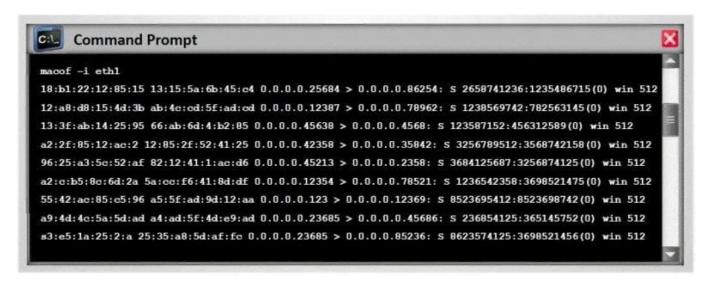
800,000+ Satisfied Customers

QUESTION 1

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop

B. SYN flood

C. Smurf attack

D. Ping of death

Correct Answer: A

QUESTION 2

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

A. Switch then acts as hub by broadcasting packets to all machines on the network

B. The CAM overflow table will cause the switch to crash causing Denial of Service

C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF

D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

Correct Answer: A

QUESTION 3

What type of port scan is shown below?

```
Scan directed at open port:
Client Server
192.5.2.32:4079 ---------FIN--------->192.5.2.110:23
192.5.2.32:4079 <----NO RESPONSE------192.5.2.110:23

Scan directed at closed port:
Client Server
192.5.2.32:4079 ---------FIN--------->192.5.2.110:23
192.5.2.32:4079<-----RST/ACK----------192.5.2.110:23
```

A. Idle Scan

B. FIN Scan

C. XMAS Scan

D. Windows Scan

Correct Answer: B

QUESTION 4

A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy.

B. transfers information over, within a computer system, or network that is within the security policy.

C. transfers information via a communication path within a computer system, or network for transfer of data.

D. transfers information over, within a computer system, or network that is encrypted.

Correct Answer: A

QUESTION 5

Blake is in charge of securing all 20 of his company\\\'s servers. He has enabled hardware and software firewalls, hardened the operating systems, and disabled all unnecessary services on all the servers. Unfortunately, there is proprietary AS400 emulation software that must run on one of the servers that requires the telnet service to function properly. Blake is especially concerned about this since telnet can be a very large security risk in an organization. Blake is concerned about how this particular server might look to an outside attacker so he decides to perform some footprinting, scanning, and penetration tests on the server. Blake telnets into the server using Port 80 and types in the following command:

HEAD / HTTP/1.0

After pressing enter twice, Blake gets the following results: What has Blake just accomplished?

```
HTTP/1.0 200 OK
Date: Wed, 01 Nov 2006 10:14:27 GMT
Content-Length: 30344
Content-Type: text/html
Expires: Wed, 01 Nov 2006 10:19:27 GMT
Cache-Control: max-age=300
Server: Apache/1.3.33 (Darwin) PHP/4.3.10
Age: 120


Connection to host lost.

C:\>
```

A. Downloaded a file to his local computer

B. Submitted a remote command to crash the server

C. Poisoned the local DNS cache of the server

D. Grabbed the Operating System banner

Correct Answer: D

Latest 312-50V7 Dumps   312-50V7 PDF Dumps   312-50V7 Practice Test