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

Which of the following is true of the wireless Service Set ID (SSID)? (Select all that apply.)

A. Identifies the wireless network

B. Acts as a password for network access

C. Should be left at the factory default setting

D. Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools

Correct Answer: AB

QUESTION 2

Botnets are networks of compromised computers that are controlled remotely and surreptitiously by one or more cyber criminals. How do cyber criminals infect a victim\\'s computer with bots? (Select 4 answers)

A. Attackers physically visit every victim\\'s computer to infect them with malicious software

B. Home computers that have security vulnerabilities are prime targets for botnets

C. Spammers scan the Internet looking for computers that are unprotected and use these "open-doors" to install malicious software

D. Attackers use phishing or spam emails that contain links or attachments

E. Attackers use websites to host the bots utilizing Web Browser vulnerabilities

Correct Answer: BCDE

QUESTION 3

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns

B. Request type=ns

C. Set type=ns

D. Transfer type=ns

Correct Answer: C

QUESTION 4

A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

A. Perform a dictionary attack.

B. Perform a brute force attack.

C. Perform an attack with a rainbow table.

D. Perform a hybrid attack.

Correct Answer: C

QUESTION 5

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