



# 312-50V7<sup>Q&As</sup>

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

How can telnet be used to fingerprint a web server?

- A. telnet webserverAddress 80 HEAD / HTTP/1.0
- B. telnet webserverAddress 80 PUT / HTTP/1.0
- C. telnet webserverAddress 80 HEAD / HTTP/2.0
- D. telnet webserverAddress 80 PUT / HTTP/2.0

Correct Answer: A

### QUESTION 2

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 18:14:27 GMT
Content-Length: 30344
Content-Type: text/html
Expires: Wed, 01 Nov 2006 18:19:27 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

---

### QUESTION 3

Which of the following is considered an acceptable option when managing a risk?

- A. Reject the risk.
- B. Deny the risk.
- C. Mitigate the risk.
- D. Initiate the risk.

Correct Answer: C

---

### QUESTION 4

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

- A. NMAP -PN -A -O -sS 192.168.2.0/24
- B. NMAP -P0 -A -O -p1-65535 192.168.0/24
- C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
- D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Correct Answer: B

---

### QUESTION 5

What is a sniffing performed on a switched network called?

- A. Spoofed sniffing
- B. Passive sniffing
- C. Direct sniffing
- D. Active sniffing

Correct Answer: D

---