



# 312-50V10<sup>Q&As</sup>

Certified Ethical Hacker Exam (C|EH v10)

**Pass EC-COUNCIL 312-50V10 Exam with 100% Guarantee**

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

<https://www.passapply.com/312-50v10.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

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- A. nmap -A - Pn
- B. nmap -sP -p-65535-T5
- C. nmap -sT -O -T0
- D. nmap -A --host-timeout 99-T1

Correct Answer: C

---

### QUESTION 2

Which of the following is assured by the use of a hash?

- A. Integrity
- B. Confidentiality
- C. Authentication
- D. Availability

Correct Answer: A

An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

References:

[https://en.wikipedia.org/wiki/Cryptographic\\_hash\\_function#Verifying\\_the\\_integrity\\_of\\_files\\_or\\_messages](https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages)

---

### QUESTION 3

It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).

Which of the following vulnerabilities is being described?

- A. Shellshock



- B. Rootshock
- C. Rootshell
- D. Shellbash

Correct Answer: A

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.

References: [https://en.wikipedia.org/wiki/Shellshock\\_\(software\\_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

---

#### QUESTION 4

What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?

- A. Install Cryptcat and encrypt outgoing packets from this server.
- B. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
- C. Use Alternate Data Streams to hide the outgoing packets from this server.

Correct Answer: B

---

#### QUESTION 5

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *  
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as a user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

Correct Answer: C