

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

Ethical Hacker Certified

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

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

<https://www.leads4pass.com/312-50.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

Bill is attempting a series of SQL queries in order to map out the tables within the database that he is trying to exploit.

Choose the attack type from the choices given below.

- A. Database Fingerprinting
- B. Database Enumeration
- C. SQL Fingerprinting
- D. SQL Enumeration

Correct Answer: A

He is trying to create a view of the characteristics of the target database, he is taking it's fingerprints.

---

## QUESTION 2

You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

- A. Visit google search engine and view the cached copy.
- B. Visit Archive.org site to retrieve the Internet archive of the acme website.
- C. Crawl the entire website and store them into your computer.
- D. Visit the company's partners and customers website for this information.

Correct Answer: B

The Internet Archive (IA) is a non-profit organization dedicated to maintaining an archive of Web and multimedia resources. Located at the Presidio in San Francisco, California, this archive includes "snapshots of the World Wide Web" (archived copies of pages, taken at various points in time), software, movies, books, and audio recordings (including recordings of live concerts from bands that allow it). This site is found at [www.archive.org](http://www.archive.org).

---

## QUESTION 3

When discussing passwords, what is considered a brute force attack?

- A. You attempt every single possibility until you exhaust all possible combinations or discover the password
- B. You threaten to use the rubber hose on someone unless they reveal their password
- C. You load a dictionary of words into your cracking program
- D. You create hashes of a large number of words and compare it with the encrypted passwords

E. You wait until the password expires

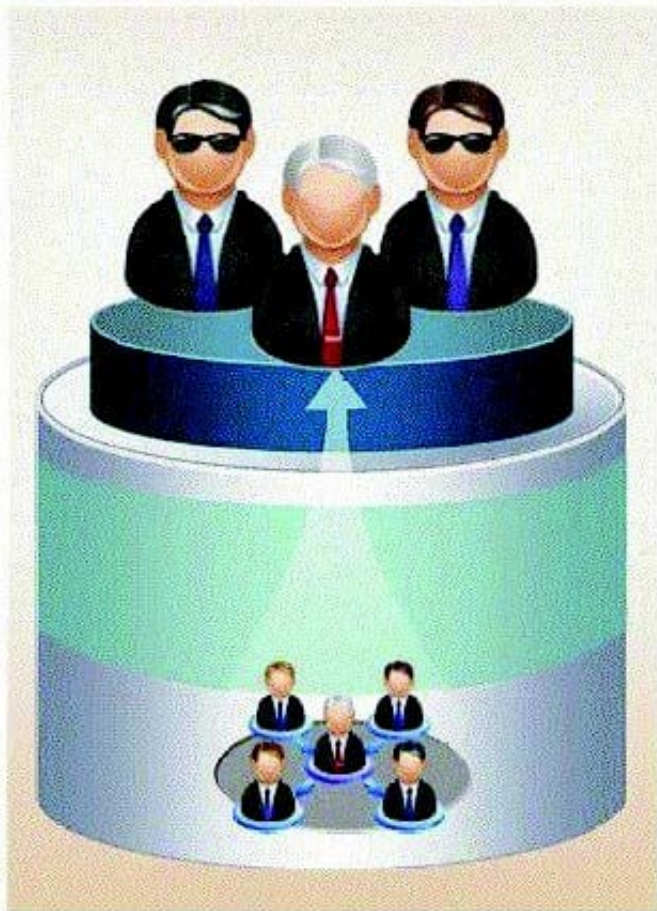
Correct Answer: A

Brute force cracking is a time consuming process where you try every possible combination of letters, numbers, and characters until you discover a match.

---

#### QUESTION 4

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.



How would you prevent such type of attacks?

- A. It is impossible to block these attacks
- B. Hire the people through third-party job agencies who will vet them for you
- C. Conduct thorough background checks before you engage them
- D. Investigate their social networking profiles

Correct Answer: C

## QUESTION 5

While performing a ping sweep of a subnet you receive an ICMP reply of Code 3/Type 13 for all the pings sent out. What is the most likely cause behind this response?

- A. The firewall is dropping the packets.
- B. An in-line IDS is dropping the packets.
- C. A router is blocking ICMP.
- D. The host does not respond to ICMP packets.

Correct Answer: C

Type 3 message = Destination Unreachable [RFC792], Code 13 (cause) = Communication Administratively Prohibited [RFC1812]

[Latest 312-50 Dumps](#)

[312-50 Practice Test](#)

[312-50 Exam Questions](#)