



# 312-50V11<sup>Q&As</sup>

Certified Ethical Hacker v11 Exam

**Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee**

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

<https://www.passapply.com/312-50v11.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

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Username: attack\` or 1=1

Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

- A. select \* from Users where UserName = `attack\` or 1=1 -- and UserPassword = `123456\`
- B. select \* from Users where UserName = `attack\` or 1=1 -- and UserPassword = `123456\`
- C. select \* from Users where UserName = `attack or 1=1 -- and UserPassword = `123456\`
- D. select \* from Users where UserName = `attack\` or 1=1 --\` and UserPassword = `123456\`

Correct Answer: A

---

### QUESTION 2

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. ESP confidential
- C. AH permissive
- D. AH Tunnel mode

Correct Answer: A

---

### QUESTION 3

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update



D. A zone estimate

Correct Answer: B

---

#### QUESTION 4

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence
- D. Human intelligence

Correct Answer: A

---

#### QUESTION 5

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

- A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
- B. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
- C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
- D. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Correct Answer: A

---

[Latest 312-50V11 Dumps](#)

[312-50V11 VCE Dumps](#)

[312-50V11 Practice Test](#)