



ECSAV10^{Q&As}

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

<https://www.geekcert.com/ecsav10.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

Richard is working on a web app pen testing assignment for one of his clients. After preliminary information, gathering and vulnerability scanning Richard runs the SQLMAP tool to extract the database information.

Which of the following commands will give Richard an output as shown in the screenshot?

```
root@kali: ~  
File Edit View Search Terminal Help  
L,NULL,NULL --  
Type: stacked queries  
Title: Microsoft SQL Server/Sybase stacked queries  
Payload: name=1'; WAITFOR DELAY '0:0:5' ..  
  
Type: AND/OR time-based blind  
Title: Microsoft SQL Server/Sybase time-based blind  
Payload: name=1' WAITFOR DELAY '0:0:5'..  
...  
[12:57:46] [INFO] the back-end DBMS is Microsoft SQL Server  
web server operating system: Windows 2008  
web application technology: Microsoft IIS 7.5, ASP.NET, ASP.NET 2.0.50727  
back-end DBMS: Microsoft SQL Server 2008  
[12:57:46] [INFO] fetching tables for database: queenhotel  
Database: queenhotel  
[1 table]  
+-----+  
| Orders |  
+-----+  
[12:57:46] [INFO] fetched data logged to text files under 'Yusr/share/sqlmap/out/out/10.10.30.3'
```

- A. `sqlmap -url http://quennhotel.com/about.aspx?name=1 -D queenhotel --tables`
- B. `sqlmap -url http://quennhotel.com/about.aspx?name=1 -dbs`
- C. `sqlmap -url http://quennhotel.com/about.aspx?name=1 -D queenhotel -T --columns`
- D. `sqlmap -url http://quennhotel.com/about.aspx?name=1 -database queenhotel -tables`

Correct Answer: A

QUESTION 2



ABC bank, a UK-based bank hired Anthony, to perform a penetration test for the bank. Anthony began performing lookups on the bank's DNS servers, reading news articles online about the bank, performing competitive intelligence gathering, watching what times the bank employees come and go, and searching the bank's job postings. What phase of the penetration testing is Anthony currently in?

- A. Attack phase
- B. Post-attack phase
- C. Pre-attack phase
- D. Remediation phase

Correct Answer: C

QUESTION 3

Which of the following statements highlights the difference between a vulnerability assessment and a penetration test?

- A. A vulnerability assessment identifies and ranks the vulnerabilities, and a penetration test exploits the identified vulnerabilities for validation and to determine impact.
- B. A vulnerability assessment focuses on low severity vulnerabilities and pen testing focuses on high severity vulnerabilities.
- C. A vulnerability assessment requires only automated tools to discover the vulnerabilities whereas pen testing also involves manual discovery of vulnerabilities.
- D. A vulnerability assessment is performed only on software components of an information system, whereas pen testing is performed on all hardware and software components of the system.

Correct Answer: A

QUESTION 4

Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

- A. Special-Access Policy
- B. User Identification and Password Policy
- C. Personal Computer Acceptable Use Policy
- D. User-Account Policy

Correct Answer: B

QUESTION 5

Which one of the following log analysis tools is used for analyzing the server's log files?



- A. Performance Analysis of Logs tool
- B. Network Sniffer Interface Test tool
- C. Ka Log Analyzer tool
- D. Event Log Tracker tool

Correct Answer: C

[Latest ECSAV10 Dumps](#)

[ECSAV10 Study Guide](#)

[ECSAV10 Braindumps](#)