ECSAV10$^{\text{Q\&As}}$

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.leads4pass.com/ecsav10.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Robert is a network admin in XYZ Inc. He deployed a Linux server in his enterprise network and wanted to share some critical and sensitive files that are present in the Linux server with his subordinates. He wants to set the file access permissions using chmod command in such a way that his subordinates can only read/view the files but cannot edit or delete the files. Which of the following chmod commands can Robert use in order to achieve his objective?

A. chmod 666

B. chmod 644

C. chmod 755

D. chmod 777

Correct Answer: B

QUESTION 2

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS

B. Active IDS

C. Progressive IDS

D. NIPS

Correct Answer: B

QUESTION 3

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack

into his former company\\'s network. Since Simon remembers some of the server names, he attempts to run

the AXFR and IXFR commands using DIG.

What is Simon trying to accomplish here?

A. Enumerate all the users in the domain

B. Perform DNS poisoning

C. Send DOS commands to crash the DNS servers

D. Perform a zone transfer

Correct Answer: D

QUESTION 4

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted. Which one of the following scanned timing options in NMAP\\'s scan is useful across slow WAN links or to hide the scan?

A. Paranoid

B. Sneaky

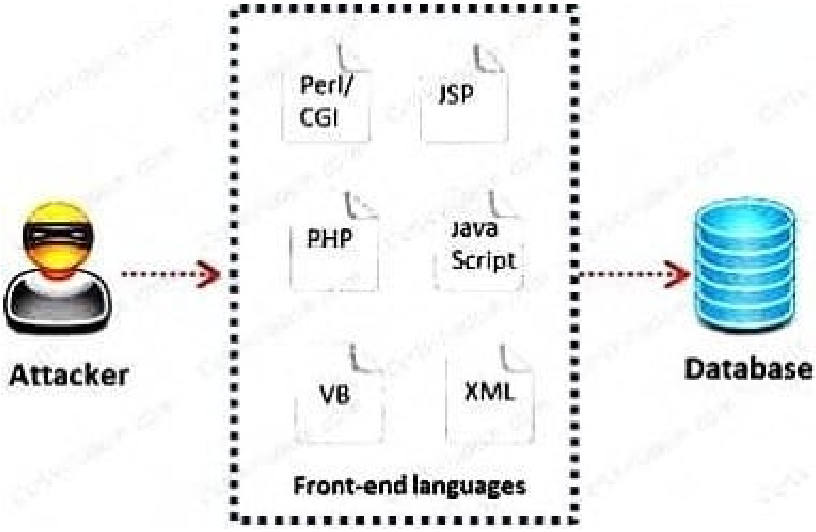
C. Polite

D. Normal

Correct Answer: C

QUESTION 5

A WHERE clause in SQL specifies that a SQL Data Manipulation Language (DML) statement should only affect rows that meet specified criteria; The criteria are expressed in the form of predicates. WHERE clauses are not mandatory clauses of SQL DML statements, but can be used to limit the number of rows affected by a SQL DML statement or returned by a query.



A pen tester is trying to gain access to a database by inserting exploited query statements with a WHERE

clause. The pen tester wants to retrieve all the entries from the database using the WHERE clause from a

particular table (e.g.

StudentTable).

What query does he need to write to retrieve the information?

A. EXTRACT* FROM StudentTable WHERE roll_number = 1 order by 1000

B. DUMP * FROM StudentTable WHERE roll_number = 1 AND 1=1-

C. SELECT * FROM StudentTable WHERE roll_number = \\'\\' or \\'1\\' = \\'1`

D. RETRIVE * FROM StudentTable WHERE roll_number = 1\\'#

Correct Answer: C

QUESTION 6

Richard, a penetration tester was asked to assess a web application. During the assessment, he discovered a file upload field where users can upload their profile pictures. While scanning the page for vulnerabilities, Richard found a file upload exploit on the website. Richard wants to test the web application by uploading a malicious PHP shell, but the web page denied the file upload. Trying to get around the security, Richard added the `jpg\\' extension to the end of the file. The new file name ended with `.php.jpg\\'. He then used the Burp suite tool and removed the `jpg\\'\\' extension from the request while uploading the file. This enabled him to successfully upload the PHP shell.

Which of the following techniques has Richard implemented to upload the PHP shell?

A. Session stealing

B. Cookie tampering

C. Cross site scripting

D. Parameter tampering

Correct Answer: D

QUESTION 7

Veronica, a penetration tester at a top MNC company, is trying to breach the company\\'s database as a part of SQLi penetration testing. She began to use the SQLi techniques to test the database security level.

She inserted new database commands into the SQL statement and appended a SQL Server EXECUTE

command to the vulnerable SQL statements.

Which of the following SQLi techniques was used to attack the database?

A. Function call injection

B. File inclusion

C. Buffer Overflow

D. Code injection

Correct Answer: A

QUESTION 8

What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of `in-depth ethical hacking\\'

B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities

C. Vulnerability testing is more expensive than penetration testing

D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Correct Answer: A

QUESTION 9

You are carrying out the last round of testing for your new website before it goes live. The website has

many dynamic pages and connects to a SQL backend that accesses your product inventory in a database.

You come across a web security site that recommends inputting the following code into a search field on

web pages to check for vulnerabilities:

alert("This is a test.")

When you type this and click on search, you receive a pop-up window that says:

"This is a test."

What is the result of this test?

A. Your website is vulnerable to web bugs

B. Your website is vulnerable to XSS

C. Your website is not vulnerable

D. Your website is vulnerable to SQL injection

Correct Answer: B

QUESTION 10

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100

B. 5000-5099

C. 6666-6674

D. 0 - 1023

Correct Answer: D

QUESTION 11

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

A. Type 8 ICMP codes

B. Type 12 ICMP codes

C. Type 3 ICMP codes

D. Type 7 ICMP codes

Correct Answer: C

QUESTION 12

Which of the following are the default ports used by NetBIOS service?

A. 135, 136, 139, 445

B. 134, 135, 136, 137

C. 137, 138, 139, 140

D. 133, 134, 139, 142

Correct Answer: A

QUESTION 13

GenSec Inc, a UK-based company, uses Oracle database to store all its data. The company also uses Oracle DataBase Vault to restrict users access to specific areas of their database. GenSec hired a senior penetration tester and security auditor named Victor to check the vulnerabilities of the company\\'s Oracle DataBase Vault. He was asked to find all the possible vulnerabilities that can bypass the company\\'s Oracle DB Vault. Victor tried different kinds of attacks to penetrate into the company\\'s Oracle DB Vault and succeeded. Which of the following attacks can help Victor to bypass GenSec\\'s Oracle DB Vault?

A. Man-in-the-Middle Attack

B. Denial-of-Service Attack

C. Replay Attack

D. SQL Injection

Correct Answer: D

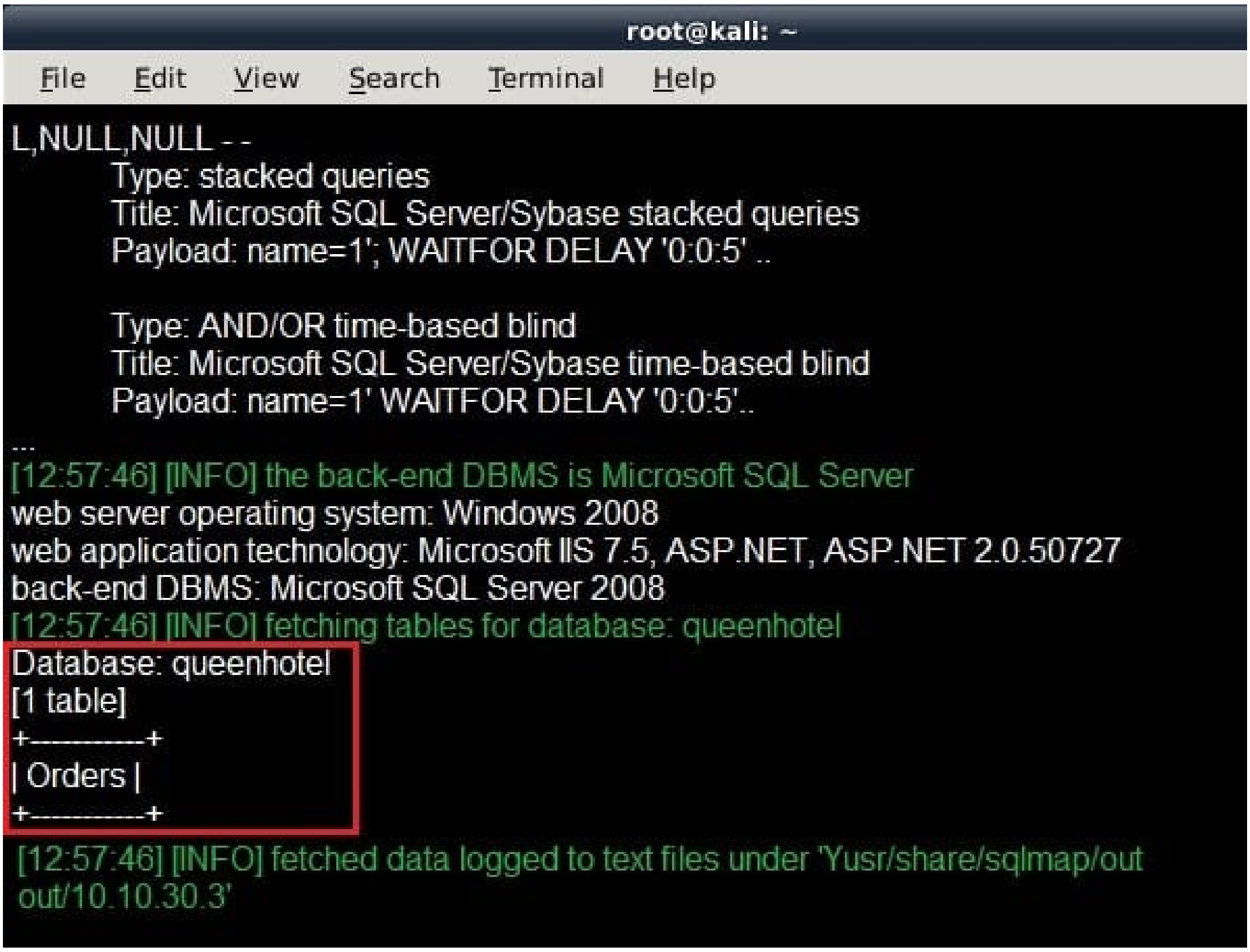
QUESTION 14

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?



```
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 15

Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areas that have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.

Functionality
(Features)
Security
Security
(Restrictions)
Usability
(GUI)

Which of the following flaws refers to an application using poorly written encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack

B. Insecure cryptographic storage attack

C. Hidden field manipulation attack

D. Man-in-the-Middle attack

Correct Answer: B