DUMPSARENA

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

ECCouncil ECSAv10

Version Demo

Total Demo Questions: 10

Total Premium Questions: 150

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A web application developer is writing code for validating the user input. His aim is to verify the user input against a list of predefined negative inputs to ensure that the received input is not one among the negative conditions. Identify the input filtering mechanism being implemented by the developer?

A. Black listing

B. White listing

C. Authentication

D. Authorization

ANSWER: A

QUESTION NO: 2

Cedric, who is a software support executive working for Panacx Tech. Inc., was asked to install Ubuntu operating system in the computers present in the organization. After installing the OS, he came to know that there are many unnecessary services and packages in the OS that were automatically installed without his knowledge. Since these services or packages can be potentially harmful and can create various security threats to the host machine, he was asked to disable all the unwanted services.

In order to stop or disable these unnecessary services or packages from the Ubuntu distributions, which of the following commands should Cedric employ?

A. # update-rc.d -f [service name] remove

B. # chkconfig [service name] –del

C. # chkconfig [service name] off

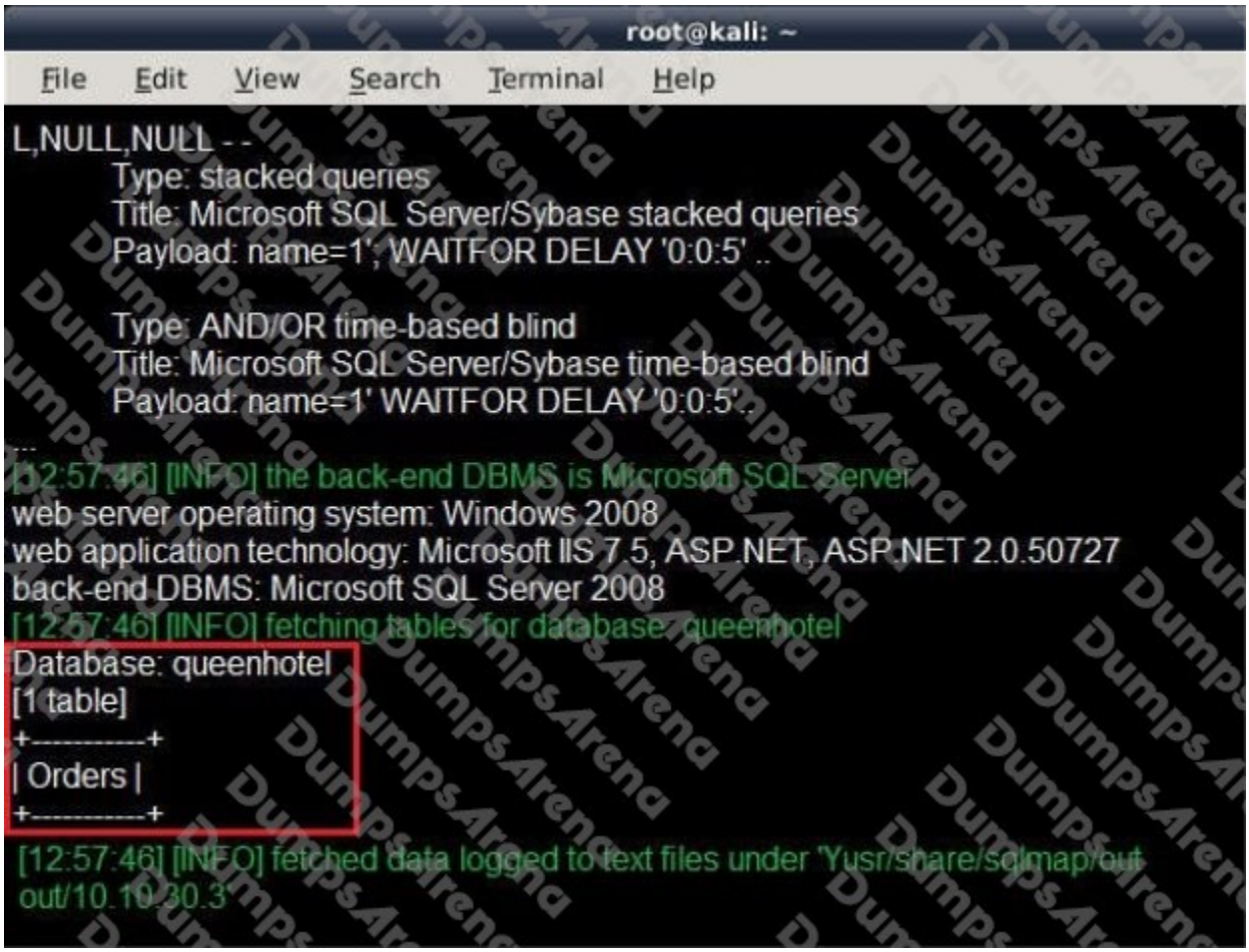
D. # service [service name] stop

ANSWER: C

QUESTION NO: 3

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?



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

ANSWER: A

QUESTION NO: 4

How does OS Fingerprinting help you as a pen tester?

A. It defines exactly what software the target has installed

B. It doesn't depend on the patches that have been applied to fix existing security holes

C. It opens a security-delayed window based on the port being scanned

D. It helps to research vulnerabilities that you can use to exploit on a target system

ANSWER: D

QUESTION NO: 5

An organization deployed Microsoft Azure cloud services for running their business activities. They appointed Jamie, a security analyst for performing cloud penetration testing. Microsoft prohibits certain tests to be carried out on their platform.

Which of the following penetration testing activities Jamie cannot perform on the Microsoft Azure cloud service?

A. Post scanning

B. Denial-of-Service

C. Log monitoring

D. Load testing

ANSWER: B

QUESTION NO: 6

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

ANSWER: B

QUESTION NO: 7

John is a network administrator and he is configuring the Active Directory roles in the primary domain controller (DC) server. Whilst configuring the Flexible Single Master Operation (FSMO) roles in the primary DC, he configured one of the roles to synchronize the time among all the DCs in an enterprise. The role that he configured also records the password changes

performed by other DCs in the domain, authentication failures due to entering an incorrect password, and processes account lockout activities. Which of the following FSMO roles has John configured?

A. RID master

B. PDC emulator

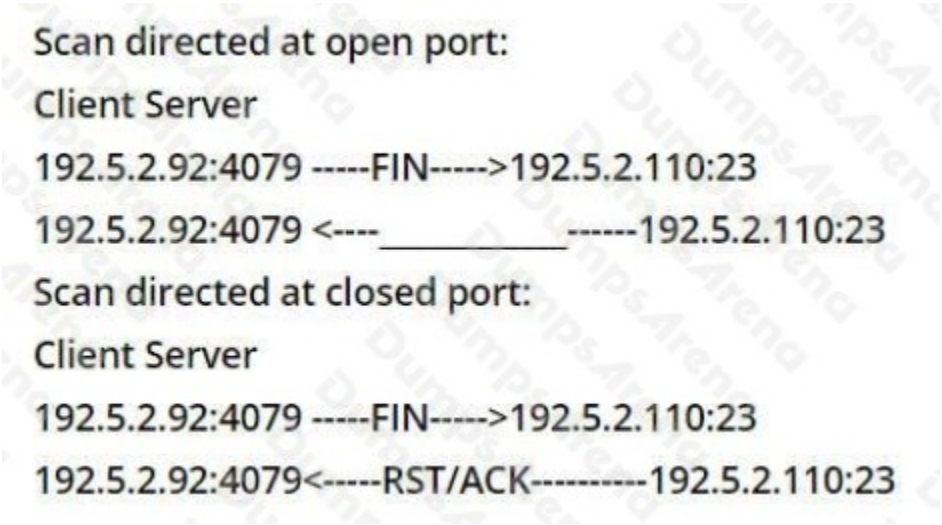
C. Domain naming master

D. Schema master

ANSWER: B

QUESTION NO: 8

As a part of the pen testing process, James performs a FIN scan as given below:



What will be the response if the port is open?

A. No response

B. FIN/RST

C. FIN/ACK

D. RST

ANSWER: A

QUESTION NO: 9

Harry, a penetration tester in SqSac Solutions Ltd., is trying to check if his company's SQL server database is vulnerable. He also wants to check if there are any loopholes present that can enable the perpetrators to exploit and gain access to the user account login details from the database. After performing various test attempts, finally Harry executes an SQL query that enabled him to extract all the available Windows Login Account details. Which of the following SQL queries did Harry execute to obtain the information?

A. SELECT name FROM sys.server_principals WHERE TYPE = 'R'

B. SELECT name FROM sys.server_principals WHERE TYPE = 'U'

C. SELECT name FROM sys.server_principals WHERE TYPE = 'G'

D. SELECT name FROM sys.server_principals WHERE TYPE = 'S'

ANSWER: B

QUESTION NO: 10

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

ANSWER: A