Course Name: ETHICAL HACKING

Assignment Solution- Week 11

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following command is used to launch Metasploit framework?

a. msfconsole
b. msfvenum
c. Metasploit
d. None of these.

Correct Answer: a

Detail Solution: The msfconsole command is used to launch Metasploit framework.

The correct option is (a).

QUESTION 2:

In Metasploit to check the compatible target (OS) for any exploit, which of the following command (option) is used?

a. Show targets
b. Set payloads
c. Set targets
d. Show payloads
e. None of these.

Correct Answer: a

Detail Solution: To check the compatible operating systems for any exploits we can use “Show targets” command, similarly to check compatible payload we can use “Show payloads” option.

The correct option is (a).

QUESTION 3:

We can execute basic commands and tools inside Metasploit console.

a. True
b. False

Correct Answer: a

Detail Solution: The very interesting feature of Metasploit framework is that we can use all commands and tools such as nmap, inside the Metasploit framework.

The correct option is (a).

QUESTION 4:

Which of the following commands can be used to get an administrative privilege in Metasploit framework?

a. getsystem
b. hashdump
c. getuser
d. msfvenum

Correct Answer: a

Detail Solution: getsystem is used to escalate privilege and get administrative login, hashdump is used to get user account details, msfvenum is used for creating payloads. There is no command called getuser.

The correct option is (a).

QUESTION 6:

Which of the following tools uses brute-force attack to extract existing and hidden pages of a webserver?

a. DIRB
b. SQL MAP
c. Hydra
d. Crunch
e. None of these

Correct Answer: a

Detail Solution: To scan a webserver we use tools like dirb, dnsenum; we also use nmap script http-enum for the same purpose. Dirb tool performs brute-force attack to find out existing and hidden webpages and directories. To automate sql injection attack, SQL MAP tool can be used. Hydra and Crunch are used for password cracking.

The correct option is (a).

QUESTION 7:

If a web page is vulnerable to blind sql injection attack, then which of the following is true?

a. It will print error message for an incorrect user input.
b. It will not print anything for an incorrect user input.

Correct Answer: b

Detail Solution: If the webpage is vulnerable to error-based sql injection, then it will generate an error message for incorrect user input. If the webpage is vulnerable to blind sql injection, then it will not generate any error message for incorrect user input.

The correct option is (b).

QUESTION 8:

Consider the table “USERS” consist of 3 column **u_id**, **u_name** and **pass** as given below:

u_id	u_name	pass
1	NPTEL	Nptel2024
2	IIT_KGP	Kgp2024
3	Eth_Hack	Eth2024

Which of the following SQL queries are malicious with respect to the above table?

a. SELECT * from USERS;
b. SELECT * from USERS where u_id = “3”
c. SELECT * from USERS where u_name = “NPTEL”
d. None of these

Correct Answer: d

Detail Solution: All the given SQL queries are valid queries.

The correct option is (d).

QUESTION 9:

Which of the following SQLMAP options is used to list all users along with hashed password?

a. - - users
b. - - passwords
c. - - user-pass
d. - - user-privileges

Correct Answer: b

Detail Solution: --passwords option is used to list all users with their hashed password.

The correct option is (b).

QUESTION 10:

Which of the following statement(s) is/are **true** for stored XXS?

a. It is stored in the database of web application.
b. It affects all users of that web application.
c. It affects only a single client of the web application.
d. None of these.

Correct Answer: a, b

Detail Solution: Stored XSS is stored in a database of web application and can affect all users; however, reflected XSS is limited to a single client.

The correct options are (a) and (b).

**********END*******