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 Metasploit module can be used for vulnerability scanning and brute force attack?

a. Encoder
b. Payload
c. Exploit
d. Auxiliary

Correct Answer: d

Detail Solution: Encoder module is used to encode the payloads. Exploit module is used to take advantage of System/Application bugs. Payload module is used to establish communication channel between Metasploit framework and target system. Auxiliary module is used to perform brute force attack, DoS attack, host and port scanning, vulnerability scanning, etc.

The correct option is (d).

QUESTION 2:

To set port number of the target system in Metasploit framework, which of the following commands is used?

a. Set LHOST
b. Set RHOST
c. Set RPORT
d. Set LPORT

Correct Answer: c

Detail Solution: LHOST and RHOST options are used to set IP of local and target (remote) system, whereas LPORT and RPORT are used to set port number for local and target system.

The correct option is (c).

QUESTION 3:

What of the following is/are true for meterpreter shell?

a. An interactive command shell (terminal) that helps to explore target system.
b. A standard command shell (terminal) that helps to explore target system.
c. We can use Metasploit modules and commands inside meterpreter shell.
d. We cannot use Metasploit modules and command inside meterpreter shell.

Correct Answer: a, c

Detail Solution: A Meterpreter shell gives access to Metasploit modules and other actions not available in the standard command shell.

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

QUESTION 4:

Which of the following commands can be used for privilege escalation in Metasploit framework?

a. getuid
b. getsystem
c. hashdump
d. ps

Correct Answer: b

Detail Solution: getuid is used to get user id. getsystem is used to escalate privilege and get administrative login. hashdump is used to get user account details, and ps is used to get details of all running process of the target system.

The correct option is (b).

QUESTION 5:

To create a payload (backdoor), which parameters needs to be set in msfvenom module?

a. Name of the payload
b. IP of the target system
c. IP of an attacker system
d. Port of target system

e. Port of an attacker system.

Correct Answer: a, c, e

Detail Solution: To create payload, name of payload, IP and port of the attacker system are required.

The correct options are (a), (c) and (e).

QUESTION 6:

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

u_id	u_name	pass
1	NPTEL	nptel1234
2	IIT_KGP	kgp1234
3	Eth_Hack	eth4321

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 = "5"
c. SELECT * from USERS where u_name = "any"
d. SELECT * from USERS where u_name = "any" or 1=1

Correct Answer: d

Detail Solution: The first three SQL queries are valid queries, however, we will not get any output for the queries (b) and (c). The last query is a malicious query, which have the malicious condition 1=1.

The correct option is (d).

QUESTION 7:

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

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

Correct Answer: b

Detail Solution: If the webpage is vulnerable to blind sql injection then it will not generate any output (no error message).

The correct option is (b).

QUESTION 8:

Which of the following tools is used to automate sql injection attacks?

a. Accunetix
b. Metasploit
c. SQL MAP
d. NMAP

Correct Answer: c

Detail Solution: To automate sql injection attack, SQL MAP tool can be used. NMAP and Accunetix are used for vulnerability scanning in a network or web application, whereas Metasploit framework is used to exploit various weakness of the system.

The correct option is (c).

QUESTION 9:

Which of the following options can be used to extract the current user name in SQL MAP?

a. - - users
b. - - current-user
c. - - current-db
d. - - dbs

Correct Answer: b

Detail Solution: --current-user option is used to get the current user name in SQL MAP.

The correct option is (b).

QUESTION 10:

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

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

Correct Answer: b

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

The correct option is (b).

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