NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# 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 is used to take advantage of system/application bugs?

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

**Correct Answer: a**

**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 (a).

---

**QUESTION 2:**

Which of the following statement is **true** for meterpreter payload?

a. Meterpreter payload is used to perform brute force attack.
b. Meterpreter payload provides an interactive shell to the attacker from which attacker can explore the target machine and can execute codes.
c. Meterpreter payload is used to launch Metasploit framework.
d. Meterpreter payload is used to bypass the anti-virus installed in target system.
e. None of these.

**Correct Answer: b**

**Detail Solution:** To perform brute force attack auxiliaries are used, to bypass antivirus encoders are used to encode payloads, to launch Metasploit framework msfconsole command is used. Meterpreter payload is used to create an interactive shell such that an attacker can explore target system and can run various other commands.

The correct answer is (b).

---

**QUESTION 3:**

Which of the following module is used to create new payloads.

a. Msfconsol
b. Encoders
c. Exploit
d. None of these

**Correct Answer: d**

**Detail Solution:** msfconsol provides an user interface for Metasploit framework, encoders are used to encode payloads to bypass anti-virus installed in target system, Exploit module consist of exploits which is basically a piece of code that is made to take advantage of system/application bugs.

Msfvenom is used to create new payloads.

The correct option is (d).

---

**QUESTION 4:**

In Metasploit, to check various parameters that need to be set for an exploit, which of the following commands is used?

a. Show parameters
b. Show options
c. Set parameters
d. Set options
e. None of these

**Correct Answer: b**

**Detail Solution:** To check all parameters that need to be set for any exploit we can use “show options” command.

The correct option is (b).

---

**QUESTION 5:**

To create a payload (backdoor), which of the following is required?

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:**

Which of the following tools/approach can be used to extract existing and hidden pages of a webserver?

a. Dirb
b. NMAP scan using “http-enum” script
c. Hydra
d. Crunch

**Correct Answer: a, b**

**Detail Solution:** To scan a webserver tools like dirb, dnsenum is used, we also use nmap script http-enum for the same purpose. Hydra and Crunch are used for password cracking.

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

---

**QUESTION 7:**

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 has the malicious condition 1=1.

The correct option is (d).

---

**QUESTION 8:**

Which of the following statement(s) is/are **true** for sql injection attack?

a. If a webpage is vulnerable to blind sql injection then it will print error message for an incorrect user input.
b. If a webpage is vulnerable to blind sql injection then it will not print anything for an incorrect user input.
c. If a webpage is vulnerable to error-based sql injection then it will print error message for an incorrect user input.
d. If a webpage is vulnerable to error-based sql injection then it will not print anything for an incorrect user input.

**Correct Answer: b, c**

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

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

---

**QUESTION 9:**

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

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

**Correct Answer: c**

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

The correct option is (c).

---

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

The correct option is (b).

---

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