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 Metasploit modules is used to take advantage of a vulnerability on some target system?

a. Exploit
b. Payload
c. Auxiliary
d. Encoder
e. None of these

Correct Answer: a

Detail Solution: Encoder module is used to encode the payloads. Exploit module is used to take advantage of System/Application bugs (vulnerabilities). 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 describes meterpreter accurately?

a. It is a static payload generator.
b. It is an interactive payload that allows remote commands and file operations.
c. It is a Metasploits web Graphical User Interface.
d. It is a network scanner bundled with Metasploit.
e. It is a database for storing exploits.

Correct Answer: b

Detail Solution: Meterpreter is a powerful payload that provides remote interactive access, file transfers, VNC, and privilege escalation support.

The correct option is (b)

QUESTION 3:

Which Metasploit option is used to set the remote target port?

a. Set LHOST
b. Set LPORT
c. Set RHOST
d. Set RPORT
e. None of these

Correct Answer: d

Detail Solution: LHOST = attacker machine IP, LPORT = local port, RHOST = target IP, RPORT = target port.

The correct option is (d).

QUESTION 4:

What is the purpose of the Metasploit Encoder module?

a. Scan for vulnerabilities
b. Escalate privileges on the target
c. Encode payloads to evade antivirus detection
d. None of these

Correct Answer: c

Detail Solution: Encoder encodes payloads to bypass Antivirus detection. It does not exploit or scan vulnerabilities.

The correct option is (c).

QUESTION 5:

Which SQLMAP option lists all database names on the target?

a. --dbs
b. --tables
c. --databases
d. --dump
e. --current-db

Correct Answer: a

Detail Solution: The option --dbs lists all available databases. --tables lists tables, --dump dumps entries, --current-db shows current DB.

The correct option is (a).

QUESTION 6:

Which of the following is **not** a type of SQL injection technique?

a. Error-based
b. Union query-based
c. Opcode injection
d. Boolean-based blind

Correct Answer: c

Detail Solution: Error-based, Boolean-based, time-based blind, and union query are SQL injection techniques. Opcode injection is unrelated to SQL.

The correct option is (c).

QUESTION 7:

Which of the following are valid Metasploit payload types?

a. Command shell
b. Meterpreter
c. Dynamic payloads
d. Static payloads
e. SQL payload

Correct Answer: a, b, c, d

Detail Solution: Metasploit includes command shell, Meterpreter, dynamic and static payloads. There is no "SQL payload."

The correct options are (a), (b), (c), (d).

QUESTION 8:

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

The correct option is (b).

QUESTION 9:

Which of the following SQLMAP options can extract credential-related information?

a. - -users
b. - -passwords
c. - -current-user
d. - -hostname

Correct Answer: a, b, c

Detail Solution: SQLMAP can retrieve DB users, hashed passwords, privileges, and current-user. Hostname only returns DBMS host, not credentials.

The correct options are (a), (b), (c).

QUESTION 10:

Which of the following are recognized types of XSS attacks?

a. Stored (persistent) XSS
b. Reflected (non-persistent) XSS
c. DOM-based XSS
d. SQL-based XSS
e. Cookie Injection XSS

Correct Answer: a, b, c

Detail Solution: Stored, reflected, and DOM are the three classical XSS forms. SQL-based XSS, and Cookie based XSS are invalid.

The correct options are (a), (b), (c).

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