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 module(s) can be used to establish communication channel between Metasploit framework and target system?

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

Correct Answer: b

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 (b).

QUESTION 2:

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 3:

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 4:

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 5:

Which of the following commands can be used to get user account details in Metasploit framework?

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

Correct Answer: b

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 (b).

QUESTION 6:

Which of the following types of attacks are possible on a webservers/web applications?

a. Denial-of-Services
b. Cross-Site-Scripting
c. SQL Injection
d. Session Hijacking
e. None of these.

Correct Answer: a, b, c, d

Detail Solution: In webserver various type of attacks are possible, the most common of which are: SQL Injection Attacks; Session Hijacking; Buffer Overflow Attacks; Cross-Site Scripting (XSS) Attacks; Denial-of-Service (DoS).

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

QUESTION 7:

Which of the following tools uses brute-force attack to extract existing and hidden page 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 tools like dirb, dnsenum is used, 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 8:

If any web page is vulnerable to error based 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: a

Detail Solution: If the webpage is vulnerable to error-based sql injection, then it will generate an error message for incorrect user input.

The correct option is (a).

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:

Consider the following statements related to stored Cross-Site-Scripting attack.
(i) It is stored in the database of web application.
(ii) It affects only a single client of the web application.

a. Only (i) is true
b. Only (ii) is true.

c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: a

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 (a).

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