/ /42

0706E454

Candidate's Seat No :_____

M.Sc Sem.-2 Examination

P - 407

Cyber Security & Forensics

June 2022

Time : 2-00 Hours] **[Max. Marks : 50**

Q.1 **Answer the following questions (Any 6)** **(7 Marks each)** **42 Marks**

1 What isthe Importance of Penetration Testing?

2 Describe the phases of the VA&PT Methodology.

3 What arethe payloads in the metasploit-framework?Outline payload types.

4 Illustrate the architecture of the metasploit-framework and explain three libraries of MSF.

5 What is Information Gathering?
1. What is Information Gathering and why it is so important?
2. What are the methods of Information Gathering?
3. Name module of MSF that is useful to Gather Information?

6 Provide service name running on below port numbers and possible attacks associated with service/port in metasploitable2. ***Port number: 21, 22, 23, 25, 137&139, 8080***

7 Describe privilege escalation in Metasploit. Write down relevant commands for the same.

8 During your nmap scan, you find the VSFTPD version 2.3.4 is running on linux system with the IP Address 192.168.2.11. Considering the above scenario provide an answer to the following.
1. Vulnerability name associated with service VSFTPD version 2.3.4
2. Steps to exploit the vulnerability with Metasploit-framework.

9 What do you include in the VAPT report?

10 Differentiate between Manual and Automated Testing

Q.2 **Answer the following short questions (Any 8)** **(1 Marks each)** **8 Marks**

1 Give a list of penetration testing types;based on approach of testing.

2 What is SMB?

3 What do you mean by vulnerability disclosure?

4 How would you set the global value for RHOSTS to 192.168.2.33 ?

5 Define the metasploit module command: ***sessions***

6 List down variables of Metasploit with it's types.

7 Provide path of the metasploit-framework installed in KALI Linux.

8 What is SMTP?

9 Provide Command Syntax to connect with SSH Server.

10 You are asked to test an application but are not given access to its source code - what testing process is this?