2/96

0804N024

Candidate's Seat No :_____

IM.Sc. CSF Sem.-6 Examination

ICSF-307

V. A. P. T.

April-2025

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. What is Vulnerability Assessment, and how does it contribute to an organization's security? 7Marks

ii. Explain the life cycle of Vulnerability Assessment and Penetration Testing. 7Marks

OR

i. What are false positives in vulnerability scanning, and why is false positive analysis important? 7Marks

ii. Explain the differences between active and passive information gathering 7Marks

Question 2 Answer the following questions:

i. Explain the process of analysing scan results and why it is crucial for an effective vulnerability management program. 7Marks

ii. Discuss the importance of understanding an organization's environment during vulnerability assessment. 7Marks

OR

i. What is static code analysis, and how does it help in vulnerability assessment? 7Marks

ii. What is reverse engineering in the context of vulnerability exploitation? 7Marks

Question 3 Answer the following questions:

i. Explain the different phases of penetration testing and their significance. 7Marks

ii. Explain the penetration testing process for software, including operating systems, services, and applications. 7Marks

OR

i. What is the significance of test cases or test scenarios in penetration testing? 7Marks

ii. Describe the common challenges faced during penetration testing and how to mitigate them. 7Marks

Questions 4 Answer the following questions:

i. What are the different types of penetration testing, and why is it important for an organization to conduct them? 7Marks

ii. Describe the key features and role of Nmap in penetration testing. 7Marks

OR

i. What is the role of Wireshark in penetration testing? How does it assist in network traffic analysis? 7Marks

ii. How does Burp Suite assist in web application security testing? 7Marks

Questions 5: Attempt any Seven out of Twelve. **14Marks**

1. What are social engineering attacks?
2. What is the difference between active and passive reconnaissance?

(P.T.O.)

N024-2

3. What is the role of port scanning in vulnerability assessment?
4. What is the significance of patch management in vulnerability assessment?
5. What is the role of Nessus in vulnerability management?
6. What is Metasploit?
7. What is reverse engineering in vulnerability exploitation?
8. What is Black Box testing in penetration testing?
9. What is the purpose of VirtualBox in penetration testing?
10 What does a Man-in-the-Middle (MitM) attack entail?
11 What is a buffer overflow vulnerability, and how is it exploited?
12 What is a reverse shell, and how is it used in Metasploit?

.....X.....X.....