

IM.B.A. (CSM) Sem.-6 Examination
CSM-BBA-CC-307

V. A. P. T.

April-2025

Time : 2-30 Hours]

[Max. Marks : 70

Question 1 Answer the following questions:

- i. What are the best practices for configuring a scan policy for a target system? 7Marks
- ii. Explain the life cycle of Vulnerability Assessment and Penetration Testing. 7Marks

OR

- i. Discuss the role of social engineering attacks in vulnerability assessments and penetration testing 7Marks
- ii. Explain the differences between active and passive information gathering 7Marks

Question 2 Answer the following questions:

- i. Describe the different stages of vulnerability management. 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. Describe the difference between Black Box, White Box, and Fuzz testing methodologies. 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 common types of vulnerabilities identified during penetration testing, and how can they be mitigated? 7Marks
- ii. Explain how penetration testers perform vulnerability exploitation and the role of tools like Metasploit in this phase. 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?

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.....