

QP CODE: 25021108



Reg No :

Name :

**B.Sc DEGREE (CBCS) REGULAR / REAPPEARANCE / MERCY CHANCE
EXAMINATIONS, FEBRUARY 2025**

Sixth Semester

B.Sc Cyber Forensic Model III

**CHOICE BASED CORE COURSE - CF6CBT01 - SECURITY THREATS AND
VULNERABILITIES**

2019 Admission Onwards

70EDB53B

Time: 3 Hours

Max. Marks : 80

Part A

*Answer any **ten** questions.*

*Each question carries **2** marks.*

1. How to mitigate internal security threats?
2. Briefly explain physical means of misappropriating resources in the case of physical security threats.
3. Explain wireless network sniffing.
4. Name any 3 alternatives to WEP.
5. What are DOS attacks?
6. What are the uses of hardware security module?
7. Write a notes on client side security.
8. Explain disaster recovery.
9. Explain the importance of CSIRT.
10. What is Rights management?
11. Explain Lipner's Model.
12. Explain the formation of the security task force.

(10×2=20)

Part B

*Answer any **six** questions.*

*Each question carries **5** marks.*





13. Explain mail bombing.
14. Briefly explain any four hacking tools used in wireless devices.
15. Explain power analysis attacks.
16. Access control in data base, Explain.
17. Explain in detail signature scanning.
18. What is a network intrusion detection system?
19. What are the disadvantages of a network intrusion detection system?
20. Describe dedicated servers and shared servers used in web hosting.
21. Describe various levels in multilevel security.

(6×5=30)

Part C

*Answer any **two** questions.*

*Each question carries **15** marks.*

22. Briefly explain the concept of hacking and which are the seven steps involved in hacking.
23. The main counter measure in the identification of the fault & which are they? Explain.
24. Explain in detail system description of biometric devices with example diagram.
25. Describe risk management and various steps involved in risk management.

(2×15=30)

