

QP CODE: 24001350



Reg No :

Name :

B.Sc DEGREE (CBCS) REGULAR / REAPPEARANCE EXAMINATIONS, MARCH 2024

Sixth Semester

B.Sc Cyber Forensic Model III

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

2019 Admission Onwards

DFF3A6B3

Time: 3 Hours

Max. Marks : 80

Part A

*Answer any **ten** questions.*

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

1. Which are the factors and causes affecting internal security threats?
2. Fundamental threats in sustaining information about physical security threats.
3. What you mean by hacker?
4. Define integrity attack?
5. Explain power analysis attacks.
6. What is the definition of network authentication?
7. What is antivirus?
8. What are various tangible costs associated with downtime?
9. What is CSIRT?
10. Explain dedicated servers and shared servers in web hosting.
11. Explain various multi user operating modes.
12. Explain Lipner's Model.

(10×2=20)

Part B

*Answer any **six** questions.*

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

13. Explain the concept and definition of nonrepudiation.
14. Explain CIA.





15. Write a short note on distinguishing DOS attacks.
16. Explain Hardware security module with suitable diagram.
17. Write a notes on server side security.
18. What are the disadvantages of a network intrusion detection system?
19. What is risk management and steps involved in it?
20. Explain Rights Management and Rights Enforcement in DRM.
21. Describe the processs involved in identification of basic security threats.

(6×5=30)

Part C

*Answer any **two** questions.*

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

22. Explain the hacking techniques in wired networks.
23. Briefly explain network sniffer, network scanning.
24. Explain in detail suggested rules for secure use of biometrics.
25. Explain various types of network intrusion detection systems along with its strengths and weaknesses.

(2×15=30)

