

(Time: 3hrs)

(Marks 80)

1. Question No 1 is compulsory.
2. Attempt any three out of the remaining five questions.

- Q1. (a) Explain with examples, Vulnerability, Threat and attacks. 08
- Q1. (b) Discuss with examples the following:
- | | | |
|-------------------|---------------------------|----|
| i) ARP spoofing | iii) TCP syn flood attack | 12 |
| ii) Port scanning | iv) IP spoofing | |
- Q2. (a) Discuss with an example how knapsack is used in cryptography. 10
- Q2. (b) Explain the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers? 10
- Q3. (a) Define access control list and capability list and compare them. Explain the Bell La Padula access control model. 10
- Q3. (b) Differentiate between the tunnel mode and transport mode of IPSec. Explain how integrity is achieved. 10
- Q4. (a) List the different protocols of SSL. Explain in detail Handshake protocol. How does server get authenticated to client? 10
- Q4. (b) List and explain the different TCP/IP vulnerabilities. 10
- Q5. (a) What are the different approaches to Software Reverse Engineering? 10
- Q5. (b) With the help of examples explain cross-site scripting and SQL injection attacks 10
- Q6. Write short notes on: 20
- | | |
|---------------------------------------|--|
| i) Linux File Security | |
| ii) Phishing and Pharming techniques | |
| iii) Federated Identity Management | |
| iv) Biometric authentication schemes. | |