Q. P. Code: 27224

Duration: 03hrs Marks:80

Note: 1) Question 1 is compulsory.
2) Solve any 3 questions from remaining questions.

1. a) Explain with example Vulnerability, Threat and Attack. (5)
   b) What are different ways of authenticating a user? (5)
   c) Explain ARP Spoofing. (5)
   d) What is IP Spoofing & IP Sniffing? (5)

2. a) Explain RSA algorithm steps with an example and list real time applications where RSA can be used. (10)
   b) Explain different types of Firewalls that can be used to secure a network with advantages and disadvantages. (10)

3. a) What is the need of SSL? Explain all phases of SSL Handshake Protocol in detail. (10)
   b) Briefly explain types of Malicious Codes with example. Explain methods of malware detection. (10)

4. a) What is the need of Intrusion Detection System (IDS)? Explain different types of IDS with advantages and disadvantages. (10)
   b) Explain Secure Email protocols and S/MIME. (10)

5. a) What is SSO? Explain the working of Kerberos Authentication Protocol (KAP). (10)
   b) What is Digital Certificate? Explain the process of the generation & verification of digital certificate. (10)

6. Write short notes on: **(Any Four)** (20)
   a) ACM,ACL & C-List
   b) Federated Identity Management
   c) Distributed Denial of Service (DDoS) Attack
   d) Honey pots
   e) Windows Security Model

****