# G.N. Khalsa College,Matunga(E.)
# Department of IT
# Semester VI
# Paper II-Security in Computing

## Unit I

1. What are the importance of information protection? Explain with example.
2. Explain various components used to build a security program.
3. What are the three recognized variants of malicious mobile code? Explain.
4. Write a short note on Network-Layer Attack.
5. Explain the two most common approaches of security.
6. Explain the best practices for network defense.
7. Explain three D's of security.
8. Explain the statement that "Achieving 100 percent protection against all conceivable attacks is an impossible job"
9. Write a note on Threat Vector.
10. Explain onion model with help of neat labelled diagram.
11. Explain lollipop model.
12. Differentiate between onion model and lollipop model.
13. List and explain the steps to create a Security defense model.

14.What is the importance of information Protection? Explain the various steps involved to protect security breach with a case study.

15. Explain the evolution of information security.
16. Explain the different ways to justify security investment
17. What are various benefits of security programs?
18. What is security methodology? Explain in brief.
19. Explain the various components used to build security programs with the help of next diagram.
20. Explain the problem of 100% security to be an impossible job.
21. What is the weakest link of security? Explain how to reduce vulnerabilities.
22. Explain the term strategy and tactics and also explain the differences between them.
23. Explain business process versus technical control.
24. Define threat. Explain in brief the various aspects of threat.
25. Explain the term threat vector in brief.
26. What are the different sources and targets of threat?
27. What is malicious mobile code? Explain the variants of malicious mobile code.
28. What is advanced persistent threat? Explain how advanced persistent threat attack works?
29. Write a note on manual attacks.
30. Explain various types of attacks.
31. What is risk analysis and how do enterprises and other organization use risk analysis.
32. Explain the various benefits of risk analysis.
33. Explain various steps involved in risk analysis process.
34. Explain the two main approaches of risk analysis.
35. Explain the concept of CIA triad in brief.
36. Explain the defense model in brief.
37. What are the different zones of trust in security of computing?
38. Explain in brief the best practices for network defense.
39. Explain the various steps to secure the physical environment in computing.
40. Explain the various steps to secure applications in environment.
41. What is ARP poisoning? Explain the various ways of implementing ARP poisoning defense.
42. What are Application layer attacks? Explain following application layer attacks:
    a. Buffer overflows
    b. Password cracking

# Unit II

1. Define authentication. Explain two parts of authentication.
2. Explain the authorization systems.
3. Explain public key Cryptography.
4. What are the three primary categories of storage infrastructure in modern storage security? Discuss.
5. Write a short note on integrity risks.
6. Explain Database-Level Security.
7. Explain certificate-based authentication in detail.
8. Write a note on Role-based Authorization (RBAC).
9. Write a note on symmetric key cryptography.
10. Explain any two confidentiality risks.
11. Write a note on object-level security.
12. Explain different types of database backups.
13. What is authentication? Explain various types of authentication.
14. Explain the various types of authentication system available.
15. Explain the concept of Kerberos in brief.
16. Explain the certificate based authentication in brief.
17. What is authorization? Explain the various types of authorization.
18. Explain the Role-Based Authorization in brief.
19. Explain the concept of access control list in brief.
20. What is the compliance with standards for security?
21. Explain the history of encryption in brief.
22. What is symmetric-Key Cryptography? Explain its types in brief with the help of neat diagram.
23. What is public key Cryptography? Explain the working of public key cryptography.
24. Explain Public Key Infrastructure in brief.
25. Explain the CA hierarchy of Public key infrastructure in brief.
26. Explain the various benefits and risks of public key infrastructure.

# Unit III

1. Explain the Cisco Hierarchical Internetworking model.
2. Explain network availability and security.
3. Write a short note on hubs and switches.
4. Explain the features of firewall.
5. Explain the five different types of wireless attacks.
6. What are the countermeasures against the possible abuse of wireless LAN?
7. Write a note on outbound filtering.
8. Explain the role of hubs and switches in network.
9. Explain in detail Network Address Translation (NAT).
10. Explain strengths and weaknesses of a firewall.
11. Explain the importance of antenna choice and positioning.
12. Explain any two types of wireless attacks.
13. Write a note on DMZ networks.
14. Write a note on Centralizing Account Management (AAA).
15. List the various techniques for network hardening. Explain any two.
16. What is spectrum technique? List the two techniques to spread the bandwidth.

## Unit IV

1. Explain intrusion Defense System types and detection models.
2. Write a note on IDS management.
3. Write a short note on Security Information and Event Management.
4. What are components of Voice Over IP? Explain.
5. Write a short note on Private Bank Exchange.
6. Explain different classic security models.
7. Write a short note on trustworthy computing.
8. Explain network-based intrusion detection system in detail.
9. List and explain steps to a successful IPS Deployment plan.
10. Write a note on H.323 protocol that includes:
    a. Governing Standard
    b. Purpose
    c. Function
    d. Known Compromises and Vulnerabilities
    e. Recommendations
11. What is Private Branch Exchange (PBX)? How will you secure PBX?
12. Write a note on access Control List (ACL).
13. Explain the reference monitor concept and windows security reference monitor.
14. What is Telecom Expense Management? Explain.
15. Write a note on TCSEC.
16. Write a note on Reference monitor.
17. Write a note on Microsoft’s Trustworthy Computing initiative.

## Unit V

1. Define virtual machine. How is hypervisor responsible for managing all guest OS installations on a VM server?
2. Explain any two confidentiality risks associated with cloud computing and their remediation
3. Explain any two integrity risks associated with cloud computing and their remediation
4. Explain any two availability risks associated with cloud computing and their remediation
5. What is cloud computing? Explain the types of cloud services.
6. Explain the application security practices and decisions that appear in most secure development lifecycle.
7. Explain the reasons for remote administration security. What are advantages of web remote administration?
8. Explain the security considerations for choosing a secure site location.
9. Explain the different factors for securing the assets with physical security devices.
10. Explain how to protect the Guest OS, Virtual Storage and Virtual Networks in Virtual machines.
11. State and explain types of cloud services.
12. Explain various Application Security Practices.
13. Write a note Custom Remote Administration.
14. Explain the classification of corporate physical Assets.
15. Explain Locks and Entry Controls that should be considered while securing assets with physical security devices.