M.Sc. (I.T.) Sem. III

INFORMATION SECURITY MANAGEMENT

QUESTION BANK (2014 – 2015)

Unit 1:

1. Explain the process of risk management.
2. What are the steps for risk assessment?
3. What are steps to Prepare for a risk assessment?
4. What are the different risk assessment approaches?
5. What are the different risk analysis approaches?
6. Explain generic risk model in detail.
7. What are the key characteristics of OCTAVE approach?
8. Explain reactive approach to Risk management with proper diagram.
9. Explain proactive approach to risk management. What are the benefits over reactive approach?
10. Write a short note on OCTAVE.
11. What are the various domains & corresponding processes of COBIT?
12. Explain any 2 methods of quantitative risk assessment.
13. Explain with diagram OCTAVE method.
14. Explain with diagram OCTAVE allegro.
15. What are the various risk framing components & explain relationship among them?
16. How are the values of asset derived in quantitative risk assessment approach?
17. List various risk models. Explain.
18. Explain the following risk models i. Threats ii. Likelihood iii. Impact
19. With neat diagram explain the risk management hierarchy.
20. How risk assessment is carries out at the organization tier of risk management hierarchy.
21. How risk assessment is carries out at the information system of risk management hierarchy.
22. Explain the quantitative risk assessment.
23. Compare the quantitative and qualitative risk assessment approaches.
24. List and explain the steps in risk assessment process.

Unit 2:

25. What are the various uses of IDPS technologies?
26. What are the various functions of IDPS technologies?
27. What are the common detection methodologies of IDPS?
28. What are the various types of IDPS technologies?
29. What are the typical components of IDPS System?

30. What are the typical components of network based IDPS System?
31. List and explain various security capabilities of IDPS technologies.
32. What are the various types of sensors used in network based IDPS System?
33. Explain packet filtering firewall technology.
34. Explain the dedicated proxy server, application proxy server firewall technology.
35. Explain how firewall act as network address translators.
36. Explain stateful inspection.
37. Write short note on application firewalls.
38. Write short note on Application-Proxy Gateways & Dedicated Proxy Servers.
39. Write short note on Web Application Firewalls & Firewalls for Virtual Infrastructures.
40. State the Limitations of Firewall Inspection.
41. Write short note on VPN.
42. Explain various network layouts with firewall implementation.
43. What are the various policies based on ip addresses.
44. What are the various policies based on protocols.
45. What are the various policies based on applications, user identity & Network Activity.
46. Explain with diagram IT security requirements.
47. What should be considered in the planning stages of a Web server?
48. What are the steps for securely installing web server?
49. Sate and explain any 4 Wireless Standards.
50. State IEEE 802.11 Network Components and explain its Architectural Models.
51. What are the various types of authentic methods implemented in IEEE 802.11 security?
52. Write short note on IEEE 802.11i security.
53. Write short note on the following:

- Server Backup Procedures
- Recovering From a Security Compromise
- Security Testing Servers

54. What is penetration testing?
55. Write a note on Identification & Authentication Technologies.
56. List and explain the important implementation issues for I&A systems.
57. What are various criteria used by the system to determine if a request for access will be granted?

Unit 3:

58. What are the various components of PKI?
59. Explain mesh and hierarchical PKI structure.
60. Explain bridge PKI architecture.
61. Explain the two basic data structures used in PKIs.
62. Write a note on physical architecture of PKI.
63. List the most commonly logged types of information and their potential benefits.
64. State & explain the common log management infrastructure functions.

65. What are the various types of network & host based security software.
66. What are the challenges in log management?
67. Explain log management infrastructure.
68. What are the various functions of log management infrastructure?
69. Write short note on Syslog Security
70. 13. Explain the Need for Log Management
71. List& Explain the classic categories of malware.
72. List& Explain the popular attacker tools.
73. What are the recommended capabilities of an antivirus software?
74. Write a note on sandboxing.
75. Explain malware incident response life cycle in detail.
76. List and explain the major component of containment of malware.
77. Explain the three main categories of patch and vulnerability metrics.
78. What is The Patch and Vulnerability Group & what are their duties?
79. What are the primary methods of remediation that can be applied to an affected system?
80. Who are involved in log management planning? Explain their responsibilities.
81. What are the steps included in developing logging policies?
82. List and explain the components of key management infrastructure.
83. Write a short note on key management policy.
84. What are the security objectives of key management policy?
85. Explain the sample KMP format.
86. Write a short note on Kerberos.
87. List & explain the KMI components in detail.
88. Write a short note on Key Management Policy.
89. Explain any six server security principles.
90. How the server security is planned?
91. How the server security is maintained?
92. List various PKI data structures. Explain in short.
93. What is the need for log management?
94. What are the challenges in log management?
95. Explain the tiers used in a log management infrastructure.
96. Define roles and responsibilities of the persons involved in log management.
97. List and explain various forms of malware.
98. List and explain the popular types of attacker tools.

Unit 4:

99. State the benefits & objectives of information security audit.
100. List the principles of Auditing.
101. List and explain the phases of a disaster recovery plan.
102. State and explain any 4 interdependencies of audit trails.
103. Write a note on cost considerations in audit trails.
104. What are the various types of audit trails?

105. Explain Audit Trails. What are the two types of audit records explain in detail?
106. List the steps to perform information security audit.
107. What are the implementations issues regarding Audit Trail?
108. Write a note on interdependences in Audit Trial.
109. Explain the concept of Business Continuity Planning with its different phases.
110. Explain the concept of Business Continuity Planning and Recovery Plan in industry.
111. Explain the various backup & recovery techniques for applications.
112. Write a short note on logical security audit.
113. Explain the system-level, application level and user audit trails.

Unit 5:

114. What is forensic science? What is the need of it?
115. Who are the primary users of forensic tools and techniques? Also state the various factors to be considered when selecting an external or internal party?
116. What are the different groups in which primary users of forensic tools and techniques within an organization usually can be divided into?
117. What are the key recommendations of establishing and organizing a forensic capability?
118. Write a note on forensic process.
119. Write a note on forensic toolkit.
120. Write a note on Examining data files.
121. Explain the two different techniques used for copying files from media.
122. What is NESSUS? Why is it considered as the most popular vulnerability scanner?
123. What types of vulnerabilities are scanned by NESSUS?
124. What are the control objectives of ISO 17799 standard?
125. What is the functionality of NMAP tool?
126. State the features of NMAP.
127. What are the basic phases of forensic process? Give a brief overview of it.
128. Write a short note on File Systems.
129. How is the collection of files done in forensic science?
130. What is the need for forensics?
131. What are the key recommendations on establishing and organizing a forensic capability?
132. List various phases in forensics process. Explain in short.
133. Explain the two techniques used to copy files from media.