

Con. 5454-09.

B.E. (IT) Sem VIII
Information Security

(3 Hours)

SP-6947

[Total Marks : 100

17/12/09

Lib
N.B.: (1) Question No. 1 is **compulsory**.

(2) Attempt any **four** questions out of remaining **six** questions.(3) **All** questions carry **equal** marks.(4) Draw **neat** diagrams wherever **necessary**.

10:30 to 1:30

1. (a) Distinguish between vulnerability, threat and control. 10
(b) Explain in detail the steps in risk analysis. 10
2. (a) What are covert channels and how are they created ? In which cases problems are created in covert channels ? 10
(b) Explain what is spoofing ? Write about different types of spoofing techniques. 10
3. (a) Discuss the similarities and differences between signature based IDS and heuristic based IDS. What are the limitations of IDS ? 10
(b) Compare different separation methods used as a basis for protection in OS. State their uses and advantages. 10
4. (a) Compare the two encryption strategies—Link and end-to-end encryption used as tools for network security, from all view points. 10
(b) Explain the role of Kerberos for supporting authentication in distributed systems. 10
5. (a) Discuss the design of multilevel secure databases. 10
(b) What is the Denial of service (attack) ? What is the meaning of the term 'service' in DOS ? What can possibly prevent DOS attacks ? 10
6. (a) List majority security threats dealt with each level of OSI protocol stack. 10
(b) What is targeted malicious code ? Write in brief about trap door and Salami attack. 10
7. Write short notes on any **two** of the following :— 20
 - (a) PGP and MIME
 - (b) SSH
 - (c) Virtual private networks
 - (d) D-DOS (Denial of service)