

Sem VIII / Rev / IT  
(REVISED COURSE)

25/05/09  
VR-4326

Con. 2820-09.

(3 Hours)

[Total Marks : 100

Information Security

- 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**.

1. (a) Explain the requirement of selecting a good firewall and implementing the same. 10  
 What are the limitations of firewalls ?
- (b) What is targeted malicious code ? What is trap door and salami attack ? Write in brief. 10
2. (a) Distinguish between vulnerability, threat and control. 10  
 (b) Discuss the similarities between signature based IDS and heuristic based IDS. 10  
 What are the limitations of IDS ?
3. (a) Explain the role of Kerberos for supporting authentication in distributed systems. 10  
 (b) Compare the two encryption strategies—Link and end-to-end encryption—used as tools for network security, from all view points. 10
4. (a) What is the Denial of Service (DOS) attack ? What is the meaning of the term 'service' in DOS ? What can possibly prevent DOS attacks ? 10  
 (b) Explain why asynchronous I/O activity is a problem with many memory protection schemes, including base/bounds and paging. Suggest a solution to the problem. 10
5. (a) Explain in detail the steps in risk analysis. 10  
 (b) What are covert channels and how are they created ? In which cases, the closure of a covert channels can be bother some ? 10
6. (a) Explain what is spoofing ? Write about different types of spoofing techniques. 10  
 (b) Discuss the strategies for risk reductions, in database security. Write in brief about integrity lock and sensitivity lock. 10
7. Write short notes on (any two) :— 20
- (a) VPN  
 (b) Possible attacks on passwords  
 (c) Secure E-mail  
 (d) Kerberos  
 (e) PGP and MIME.