

--	--	--	--	--	--	--	--	--	--

## Eighth Semester B.E. Degree Examination, December 2011

### Information and Network Security

Time: 3 hrs.

Max. Marks:100

**Note: Answer any FIVE full questions, selecting at least TWO questions from each part.**

#### PART – A

1. a. Define the terms : policy, standards and practices in the context of information security. Draw a schematic diagram depicting the inter-relationship between the above. (06 Marks)
- b. What are the policies that must be defined by the managements (of organizations) as per NIST SP 800 – 14? Describe briefly the specific areas covered by any two of these policies. (07 Marks)
- c. What are the components of contingency planning? Describe briefly the important steps involved in the recovery process after the extent of damage caused by an incident has been assessed. (07 Marks)
2. a. What is a firewall? List the type of firewalls categorized by processing mode. Draw a schematic diagram of a packet-filtering router used as a firewall and explain its function using a sample firewall rule. (10 Marks)
- b. Describe the steps involved in Kerberos login and Kerberos request for services, with suitable illustrations. (10 Marks)
3. a. Define the following terms related to IDS :
  - i) Alert
  - ii) False attack stimulus
  - iii) False negative
  - iv) False positive
  - v) True attack stimulus. (05 Marks)
- b. Discuss the reasons for acquisition and use of IDSs by organizations. (06 Marks)
- c. Discuss the differences between host IDS and network IDS, with the help of a schematic diagram. (06 Marks)
- d. Define the terms : honey pots, honey net and padded cells. (03 Marks)
4. a. Define the following terms related to cryptography :
  - i) Algorithm
  - ii) Cipher
  - iii) Key
  - iv) Link encryption
  - v) Work factor. (05 Marks)
- b. Distinguish between symmetric encryption and asymmetric encryption, with suitable examples. (06 Marks)
- c. Describe the terms : authentication, integrity, privacy, authorization and non-repudiation. (05 Marks)
- d. Discuss the “man-in-the-middle” attack. (04 Marks)

**PART – B**

- 5 a. Describe briefly the various security attacks and specific security mechanisms covered by X.800. (14 Marks)  
b. Describe briefly the authentication procedures covered by X.809. (06 Marks)
- 6 a. Describe the steps involved in providing authentication and confidentiality by PGP, with suitable illustrations. (10 Marks)  
b. Discuss the limitations of SMTP/RFC 822 and how MIME overcomes these limitations. (10 Marks)
- 7 a. Describe the benefits of IPSec. (05 Marks)  
b. What is security association? Discuss briefly the parameters that are used to define a security association. (05 Marks)  
c. Describe the transport and tunnel modes used for IPSec AH authentication bringing out their scope relevant to IPV4. (10 Marks)
- 8 a. Discuss the SSL protocol stack. (04 Marks)  
b. What are the services provided by SSL record protocol? Describe the operation of this protocol, with suitable illustration. (08 Marks)  
c. What is SET? Discuss its specifications. (08 Marks)

\*\*\*\*\*