Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – I • EXAMINATION – WINTER 2012

Subject code: 715104N Date: 11-01-2013

Subject Name: Network Defense and Countermeasures

Time: 02.30 pm – 05.00 pm Total Marks: 70

Instructions:

1. **Attempt question 1, which is compulsory and answer any five from the rest questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right hand indicate the marks.**

Q. No. 1 [2 Marks X 10 = 20 Marks]

a. Define security policy?
b. What is an intrusion?
c. What is proxy server?
d. Define risk?
e. Define types of risk analysis?
f. Define Transport mode of IPSEC?
g. What is a VLAN in a switch?
h. Define Network Address Translation?
i. Define Disaster?
j. What are the functions of VPN?

Q. No. 2

a. Differentiate between intrusion detection system and intrusion prevention system. [6 Marks]

b. Explain the Application Gateways or Proxy Firewalls? [4 Marks]

Q. No. 3

a. Brief on the working of a signature based Intrusion Detection System? [5 Marks]

b. Brief on the working of anomaly based Intrusion Detection System? [5 Marks]

Q. No. 4

a. Brief on Authentication Header protocol of IPSEC? [5 Marks]

b. Brief on Encapsulating Security Payload protocol of IPSEC? [5 Marks]

Q. No. 5

a. How VLAN's in a switch provides security? [6 Marks]
b. Explain the working of TCP FIN and RST flags? [4 Marks]

Q. No. 6

Describe the working of a host based intrusion detection system? State its advantages and disadvantages? [10 Marks]

Q. No. 7

Describe PPTP, L2TP and SSTP VPN protocols and differentiate between them? [10 Marks]

Q. No. 8

Explain the best practices or procedures that can help an organization make its network more secure? [10 Marks]

****