Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – I • EXAMINATION – SUMMER • 2013

Subject code: 715104 Date: 11-06-2013

Subject Name: Network Defense and Counter Measures

Time: 10.30 am – 01.00 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. What is dumpster diving?
b. What do you mean by DMZ?
c. What is Denial of Service?
d. Differentiate between policy and a procedure.
e. What is access control list?
f. Name types of firewall.
g. Define integrity from an information security perspective.
h. What is risk?
i. What are modes of IPSEC?
j. Define Confidentiality.

Q. No. 2

a. Explain with examples the various types of attacks on communication systems. [5 Marks]
b. Explain the Stateful Packet Inspection Firewall? [5 Marks]

Q. No. 3

a. Discuss vulnerability in detail. [5 Marks]
b. Explain Filter Table. [5 Marks]

Q. No. 4

a. Define attack and discuss its components. [5 Marks]
b. What is signature based Intrusion Detection System? [5 Marks]

Q. No. 5

a. Discuss about protocols for IPSEC? [6 Marks]
b. Explain the four critical functions of VPN. [4 Marks

Q. No. 6

a. Explain IDS architecture. [6 Marks]
b. Discuss issues with Intrusion Prevention. [4 Marks]

Q. No. 7

Explain IDS peer-to-peer architecture and its advantages and disadvantages. [10 Marks]

Q. No. 8

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

****