Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject code: 715104 **Date: 01-01-2014**

Subject Name: Network Defense and Countermeasures

Time: 10.30 am – 01.00 pm **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q. No. 1 [2 Marks X 07= 14 Marks]

a. Define War Driving?
b. Differentiate between Phishing & Vishing?
c. What are the drawbacks of a packet filtering firewalls?
d. What is bastion Host?
e. Name any two layer3 protocol?
f. Name any two version control systems?
g. Differentiate between threat and risk?

Q. No. 2

a. Explain SNAT [6 Marks]
b. Explain DNAT [8 Marks]

Or

b. Explain [8 Marks]

1. Two differences between IPV4 & IPV6?
2. What are the drawbacks of a packet filtering firewalls?
3. What is an Access Control List?
4. Difference between IDS & IPS

Q. No. 3

a. Discuss the purpose of raw Table in iptables. [7 Marks]
b. Explain rule based and anomaly detection in IDS. [7 Marks]

Or

Q. No. 3

a. Explain the two main protocols used by IPSec. [7 Marks]

b. Explain the post-routing chain in detail. [7 Marks]

Q. No. 4

a. Explain the three types of security mechanisms in detail. [8 Marks]

b. Explain the four critical functions of VPN. [6 Marks]

Or

Q. No. 4

Discuss the role of Spanning Port, Hubs and TAPs in IDS / IPS architecture. [14 Marks]

Q. No. 5

What is snort signature? Explain the structure of a signature with some examples. [14 Marks]

Or

Q. No. 5

What is tcpdump? Explain it's features and uses from a network security perspective. [14 Marks]