Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – I • EXAMINATION – WINTER • 2014

Subject code: 3715104 **Date: 09-01-2015**

Subject Name: Network Defence and Countermeasures

Time: 02:30 pm - 05:00 pm **Total Marks: 70**

Instructions:

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

Q.1	**(a)**	Explain the OSI reference model in detail.	**07**
	(b)	Explain the TCP/IP Model in detail.	**07**
Q.2	**(a)**	Explain the three way handshake for connection establishment and connection termination in detail.	**07**
	(b)	Explain with examples the various types of attacks on communication systems	**07**
		OR	
	(b)	What is vulnerability and how they are classified?	**07**
Q.3	**(a)**	Explain the advantages and disadvantages of Hardware and Software Firewalls	**07**
	(b)	Explain the working of iptable architecture in detail	**07**
		OR	
Q.3	**(a)**	What is a screened host firewall and screened subnet firewall?	**07**
	(b)	Discuss the purpose of Filter Table in iptables	**07**
Q.4	**(a)**	Explain what is an IDS and the types of IDS. Explain rule based and anomaly detection in IDS	**07**
	(b)	Explain IDS Analysis scheme in details covering the various steps in IDS Analysis.	**07**
		OR	
Q.4	**(a)**	Discuss in detail the advantages and disadvantages of a site-to-site VPN.	**07**
	(b)	Discuss in detail the advantages and disadvantages of user VPN.	**07**
Q.5	**(a)**	Discuss the role of Spanning Port, Hubs and TAPs in IDS / IPS architecture	**07**
	(b)	Explain in detail IPSec Explain the four critical functions of VPN	**07**
		OR	
Q.5	**(a)**	What is tcpdump? Explain its features and uses from a network security perspective.	**07**
	(b)	What is snort signature? Explain the structure of a signature with some examples	**07**

****