GUJARAT TECHNOLOGICAL UNIVERSITY

Subject Name: Network Defence and Countermeasures (NDC)

Subject Code: 3715104
Semester: I

Type of course: M.E. Computer Engineering (IT systems and Network Security)

Prerequisite:

- Understanding of Operating System Management
- Understanding of Network Communication
- Understanding of Security Basics

Rationale:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE (E)	PA (M)	PA (V) ESE	PA (I)	
3	2	0	4	70	30	30	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	Security Fundamentals	2	4
2	Firewalls, Application Layer Firewalls, Packet Filtering Firewalls, Hybrids	2	4
3	Intrusion Detection And Prevention	2	4
4	Intrusion risks, Security policy	2	4
5	Monitoring traffic and open ports	2	4
6	Detecting modified files	2	4
7	Investigating and verifying detected intrusions, Recovering from	2	4
8	reporting and documenting intrusions	2	4
9	Define the Types of intrusion Prevention Systems	2	4
10	Set Up an IPS,Manage an IPS	2	4
11	Understand Intrusion Prevention, Issues with Intrusion Prevention	2	4
12	Snort, IP Signature and Analysis, Risk Analysis, Virtual Private Networks	2	4
13	Define Virtual Private Networks, Deploy User VPNs	2	4
14	Benefits of user VPNs Managing User VPNs. Issues with User VPNs	2	6
15	Deploy Site VPNs, Benefits of Site VPNs	2	6
16	Managing Site VPNs, Issues with Site VPNs	3	6

Reference Books: - Fundamentals of network and Security, Eric Maiwald/TMH

- Network Security: The Complete Reference, Bragg

Course Outcome:

After learning the course the students should be able to:

- Safeguard the network infrastructure.
- Write policies for secure communication in network.
- Troubleshoot the Network Infrastructure Problems
- Counter the Intrusion attacks on Network
- Monitor the Networks.

List of Experiments: (with Open Ended Problems)

- Configure a windows FTP server for user based access. Capture packets while you connect to FTP server and Login. Find the packet that shows username and password. Now configure IPSec between FTP server and Client. Capture packets and observe the results?

- Install and configure squid on Linux to block following sites?
www.facebook.com, www.gmail.com, www.yahoo.com

- Configure 2 Windows 2008 R2 machines and 1 Windows XP machines. Now configure 1 Windows 2008 R2 as domain controller. Add 2nd Windows 2008 R2 machine into the domain as a member. Configure PPTP/L2TP VPN on this 2nd server to provide access to shared folders on domain controller. Create a VPN Dial-up client on XP and test?

- Configure IPSec on 2 Linux machines to secure communication between them. Capture packets and observe?

- Install and configure snort to work IDS to monitor a web server configured on a windows 2008 r2 machine. Try different attacks on the machine and show the snort logs displaying information about the attacks?

- Configure FTP service on 1 Linux machine. Configure web server on the 2nd machine. Configure iptables firewall to allow and block access to other machines in the same network?

- Configure FTP service and web service on a windows 2008 R2 machine. Configure windows firewall to allow and block access to other machines in the same network?

Major Equipments:

- Linux
- VMWare
- Router
- Switches
- IP camera
- Wi-Fi Adapters

List of Open Source Software/learning website:

- Nessus
- Metasploit
- Foca
- Untangle
- ClearOS
- Netfilter