Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous Institute Affiliated to University of Mumbai)

Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	T	P	L	T	P	Total
CPL701	Network threats and attacks Laboratory	--	--	4	--	--	2	2
		Examination Scheme						
		ISE		ESE			Total	
				Practical		Oral		
		40		--		20	60	

Pre-requisite Course Codes		CPL601(Network Programming Lab)
At end of successful completion of this course, student will be able to		
Course Outcomes	CO1	Use network-based tools for network analysis
	CO2	Use techniques for Network scanning
	CO3	Identify network vulnerability
	CO4	Use tools to simulate intrusion detection system
	CO5	To understand and install a firewall

Exp. No.	Experiment Details	Ref.	Marks
1	**Title: Study the use of network reconnaissance** tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars. **Objective:** Objective of this module to how to gather information about the networks by using different n/w reconnaissance tools. **Scope**: Network analysis using network based tools **Technology:** Networking	1,3	5
2	**Title:Study of packet sniffer tools like wireshark, ethereal, tcpdump** etc. You should be able to use the tools to do the following 1. Observer performance in promiscuous as well as non-promiscuous mode. 2. Show that packets can be traced based on different filters. **Objective:** Objective of this module is to observer the performance in promiscuous & non-promiscuous mode & to find the packets based on different filters. **Scope:** Packet grapping, message and protocol analysis **Technology:** Networking	1,2	5
3	**Title: Download and install nmap**. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, etc. **Objective:** objective of this module to learn nmap installation & use this to scan different ports. **Scope:** used for ip spoofing and port scanning **Technology:** Networking	1,4	5
4	**Title:** Use the Nessus tool to scan the network for vulnerabilities.	1,3	5

	Objective:Objective of the module is scan system and network analysis. **Scope:** It used for system analysis, security and process analysis **Technology:** Networking		
5	**Title**: Install IDS (e.g. SNORT) and study the logs. **Objective**: Simulate intrusion detection system using tools such as snort **Scope:** It is used for intrusion detection system vulnerability scans **Technology:** Networking	1,2	**5**
6	**Title**: Use of iptables in linux to create firewalls. **Objective:** To study how to create and destroy firewall security parameters. **Scope**: system security and network security **Technology**: Networking	1,2	**5**
7	**Title:** Mini project **Objective:** To implement Networking concepts **Scope:** To understand Network & system tools **Technology:** Networking		**10**
		Total Marks	**40**

References:

[1]Chris McNab,"Network Security Assessment", O'Reilly

[2]Andrew Lockhart, "Network Security Hacks", O'Reilly

[3]DafyddStuttard& Marcus Pinto, "The Web Application Hacker's Handbook 2nd Edition", Wiley Publication(2014).

[4]DaviOttenheimer& Matthew Wallace, "Securing the Virtual Environment", Willey Publication(2012).