Detailed Syllabus for B. Tech. Degree Programme in Computer Science & Engineering

Semester – VI

(Departmental Core Subject)

CS-3212 L-T-P-S-C
System Security Lab 0-0-1-0-1

Laboratory Outcome: *Learner will able to apply the knowledge of symmetric cryptography to implement simple ciphers, analyze and implement public key algorithms like RSA and El Gamal, analyze and evaluate performance of hashing algorithms, explore the different network reconnaissance tools to gather information about networks, explore and use tools like sniffers, port scanners and other related tools for analysing packets in a network, set up firewalls and intrusion detection systems using open source technologies and to explore email security, explore various attacks like buffer-overflow, and web-application attacks.*

PO1	PO2	PO3	PO4	PO5	PO6	PO8	PO10	PO12	PSO1
1	1	1	1	1	1	1	1	1	1

List of Experiments

S. No.	Title of the Experiment	Module
1.	Design and Implementation of a product cipher using Substitution and	01

	Transposition ciphers.	
2.	Implementation and analysis of RSA cryptosystem and RSA/El Gamal.	02
3.	Implementation of Diffie Hellman Key exchange algorithm	02
4.	For varying message sizes, test integrity of message using MD-5, SHA-1, and analyse the performance of the two protocols. Use crypt APIs	03
5.	Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.	05
6.	Study of packet sniffer tools : wireshark: 1. Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode. 2. Explore how the packets can be traced based on different filters.	5
7.	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, xmas scan etc.	05
8.	Detect ARP spoofing using nmap and/or open source tool ARPWATCH and wireshark. Use arping tool to generate gratuitous arps and monitor using wireshark	05
9.	Simulate DOS attack using Hping, hping3 and other tools.	05
10.	Simulate buffer overflow attack using Ollydbg,	05

	Splint, Cppcheck etc	
11.	Set up IPSEC under LINUX. Set up Snort and study the logs.	05
12.	Setting up personal Firewall using iptables	05
13.	Explore the GPG tool of linux to implement email security	05
14.	SQL injection attack, Cross-Cite Scripting attack simulation	06

Text/Reference Books

1. Build your own Security Lab. Gregg M., Wiley India.
2. CCNA Security, Study Guide. Boyles T., Sybex.
3. Network Security Bible. Cole E., Wiley India.
4. Web Application Hacker's Handbook. Stuttard D. & Pinto M., Wiley India.