SILVER OAK UNIVERSITY

School of Technology, Design and Computer Application
Silver Oak College of Computer Application
Department of Computer Application
Master of Science Cyber Security & Digital Forensics

Course Name: IT Network Security
Course Code: 1040147107
Semester: 2nd

Prerequisite: Basics of network, working of VPN, Network sniffing and security, Wireless Protocols.

Course Objective: To develop a comprehensive understanding of IT networks and security, encompassing principles, protocols, technologies, and best practices, with the aim of enhancing professional expertise, bolstering organizational security measures, and contributing to the effective management and protection of digital assets and information infrastructure.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
3	1	0	4	4

Content:

Unit No.	Course Contents	Teaching Hours	% Weightage
1	**Introduction to Computer Network :** Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP, IP Model, Routers, Switches, Endpoint solutions, Access Directory, TOR Network.	13	30
2	**Types of Networks & policy :** Networking Devices (Layer1,2,3), Different types of network layer, Attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails), IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based).	13	30
3	**VPNS :** VPN and its types, Tunneling Protocols, Tunnel and Transport Mode, Authentication Header Encapsulation Security Payload (ESP)- IPSEC, Protocol Suite, IKE PHASE 1, II – Generic Routing Encapsulation(GRE), Implementation of VPNs.	8	20
4	**Industrial Network Security and Management:** Introduction to industrial network security and threat overview, Configuring industrial firewalls, Setting up and managing IDS/IPS systems, Implementing secure communication protocols (IPsec,	8	20

	SSL/TLS), Secure remote access solutions (VPNs), Network segmentation and access controls, Monitoring and logging practices, Compliance and regulatory requirements (NIST, ISO/IEC 27001), Emerging threats and future trends (IoT, cyber-physical attacks).		

Course Outcomes:

Sr. No.	CO-Statement	Unit No
CO-1	Analyze IP addressing, NAT, IP subnets, DHCP servers, and DNS servers within a network context.	1
CO-2	Implement and configure firewall solutions including ACLs, packet filtering, DMZ, and audit trails.	2
CO-3	Identify various types of VPNs and understand the principles of tunneling protocols.	3
CO-4	Evaluate compliance standards and their application to industrial networks.	4

Major Equipment:

1. Computer System
2. LAN cable

Teaching & Learning Methodology: -

1. The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
2. Projector and Computer
3. Experiments shall be performed in the laboratory related to course contents

List of Practicals: **Total Hours: 14**

Sr. No.	Practical Name
1.	Setting up Pfsense firewall
2.	DNS Poisoning attack
3.	Installing and configuring Nessus
4.	Installing and configuring OpenVAS
5.	Scanning network with nessus
6.	Scanning network with OpenVAS
7.	Injecting HTML Code to Packets
8.	Setting up proxy chains
9.	Surfing the web with full anonymity -proxychains
10.	Configuring and Testing Firewall Security in an Industrial Network

Books Recommended:

1. William Stallings "Network Security Essentials: Applications and Standards" Pearson
2. James F. Kurose and Keith W. Ross "Computer Networking: A Top-Down Approach" Pearson
3. Chris Sanders "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" No Starch Press

CO-PO-PSO MATRIX:

Co.No	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	2	2	1	1				2	2
CO-2	1	3	2	2	1			1	2
CO-3	3	1	1	3	2		2	2	1
CO-4	1	2	1	2				3	3