Semester - 1
Paper 102: Network Basics and Network Security

Marks: 100 **Lectures 60**

Objective: This course aims at teaching students about the fundamentals and distinctions of network building along with setup of present day networks in complex environments. The networks today are vulnerable to various attacks and the course aims at acquainting students with the techniques used by hackers for network attacks and also the techniques adopted in order to guard the entire infrastructure against varied attacks.

Unit I: Introduction to Network Security

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. 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).

Unit II: Virtual Private Networks

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.

Unit III: Network Attacks Part 1

Network Sniffing, Wireshark, packet analysis, display and capture filters, ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta,Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP Pentesting,

Unit IV: Network Attacks Part 2

Network Exploitation OS Detection in network, nmap, open ports, filtered ports, service detection, metasploit framework, interface of metasploit framework, network vulnerability assessment, Evade anti viruses and firewalls, metasploit scripting, exploits, vulnerabilities,

payloads, custom payloads, nmap configuration, Social Engineering toolkit, Xero sploit Framework, exploits delivery. End Point Security.

Unit V: Wireless Attacks

Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentication, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP , WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework

Suggested Readings:

1. Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security, Private communication in public world* (2nd Ed.). PHI
2. Monte, M. (2015). *Network Attacks and Exploitation: A Framework*. Wiley.
3. Perez, Andre. (2014). *Network Security*. Wiley.
4. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice (5th Ed.). Prentice Hall

Latest research papers from refereed journals discussed by the faculty may also be referred.