P23CSG22 - CYBER SECURITY

(Generic Elective - Common Paper for all PG Programmes in the II Semester)

Course Outcomes:

- **a.** Analyze and evaluate the cyber security needs of an organization.
- **b.** b) Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
- **c.** c) Measure the performance and troubleshoot cyber security systems.

Unit-1: Introduction to Cyber Security

Introduction, Computer Security, Threats, Harm, Vulnerabilities, Controls, Authentication, Access Control and Cryptography. Web attack: Browser Attacks, Web Attacks Targeting Users, Obtaining User or Website Data, Email Attacks. Network Vulnerabilities: Overview of vulnerability scanning, Open Port / Service Identification, Banner /Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit.Networks Vulnerability Scanning (Netcat, Socat), Network Sniffers and Injection tools.

Unit-2: Network Defense tools

Firewalls and Packet Filters: Firewall Basics, Packet Filter Vs Firewall, How a Firewall Protects a Network, Packet Characteristic to Filter, Stateless Vs Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding. VPN: the basic of Virtual Private Networks. Firewall: Introduction, Linux Firewall, Windows Firewall. Snort: Introduction Detection System.

Unit-3: Web Application Tools

Scanning for web vulnerabilities tools: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel.

Application Inspection tools – Zed Attack Proxy, Sqlmap, DVWA, Webgoat. Password Cracking and Brute-Force Tools: John the Ripper, L0htcrack, Pwdump, HTC-Hydra.

Unit-4: Introduction to Cyber Crime, law and Investigation

Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Computer Language, Network Language, Realms of the Cyber world. Internet crime and Act: A Brief History of the Internet, Recognizing and Defining Computer Crime, Contemporary Crimes, Computers as Targets, Contaminants and Destruction of Data, Indian IT ACT

Unit-5: Firewalls and Spyware

Firewalls and Packet Filters, password Cracking, Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless Networks.

Text Book:

1. Nina Godbole, Sunit Belapure, “Cyber Security: Understanding Cyber crimes, Computer Forensics and Legal Perspectives”, First Edition, Wiley India, 2011.

REFERENCES:

1. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing", Fifth Edition, Prentice Hall, New Delhi, 2015.

COURSE OUTCOMES: CO1:

Understand the fundamentals of networks security, security architecture, threats and vulnerabilities

CO2: Apply the different cryptographic operations of symmetric cryptographic algorithms

CO3: Apply the different cryptographic operations of public key cryptography

CO4: Apply the various Authentication schemes to simulate different applications.

CO5: Understand various cyber crimes and cyber security.