MCA473B – CYBER SECURITY

Total Teaching Hours for Semester: 75
Max Marks: 150 Credits: 5

Course Objectives

This course is designed to understand various types of cyber-attacks and cyber-crimes. It describes the threats and risks within context of the cyber security. An overview of the cyber laws & concepts of cyber forensics and the defensive techniques against these attacks are discussed.

Course Outcomes

The students will be able to
CO1: Demonstrate an understanding of Cyber-Attacks, Types of Cyber Crimes, Cyber Laws and also how to protect them self and ultimately the entire Internet community from such attacks.
CO2: Describe the Cyber Security Laws and Computer Forensics
CO3: Apply policies and procedures to manage Privacy issues
CO4: Analyze and interpret forensically investigated security incidents

Unit-1 Teaching Hours: 15

INTRODUCTION TO CYBER SECURITY

Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage - Comprehensive Cyber Security Policy.

Lab Exercises:

1. Use Nmap to discover devices on a given network, identify open ports, and determine operating systems using scanning techniques like TCP SYN, UDP, and OS detection
2. Set up OpenVAS (Open Vulnerability Assessment System) in Kali Linux and scan a target machine for vulnerabilities.

Unit-2 Teaching Hours: 15

CYBERSPACE AND THE LAW & CYBER FORENSICS

Introduction, Cyber Security Regulations, Roles of International Law. The Indian Cyberspace, National Cyber Security Policy. Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics. **Lab Exercises:**

1. Capture network traffic using Wireshark and analyze packets exchanged between two machines.

1. Use OSINT techniques to gather information about a specific target (e.g., a company or individual).

Unit-3 Teaching Hours: 15
CYBERCRIME: MOBILE AND WIRELESS DEVICES
Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops. **Lab Exercises:**

1. Exploit a known vulnerability on a vulnerable machine using Metasploit modules.
2. Install and configure OWASP ZAP (Zed Attack Proxy) in Kali Linux to perform a web application vulnerability scan. Detect common web vulnerabilities like XSS (Cross-Site Scripting), SQL injection, and CSRF (Cross-Site Request Forgery).

Unit-4 Teaching Hours: 15
CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS
Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for organizations.
Lab Exercises:

1. Use tools like Aircrack-ng or Wifite to perform a wireless security assessment by cracking WEP/WPA keys or identifying insecure access points.
2. Simulate a social engineering attack by crafting a phishing email or executing a pretexting scenario.

Unit-5 Teaching Hours: 15
PRIVACY ISSUES: BASIC DATA PRIVACY CONCEPTS
Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial domains.
Cybercrime: Examples and Mini-Cases
Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.
Lab Exercises:

1. Analyze a system or network, identify potential threats.
2. Perform a risk assessment of a system or network.

Text Books and Reference Books

1 Anand Shinde, Introduction to Cyber Security, Notion Press, 2021.

2 Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley, 2011.

1 B.B.Gupta, D.P.Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018.Digital Computer Fundamentals, Floyd, Thomas L, Pearson International, 11th Edition, 2015.

Essential Reading / Recommended Reading

1 Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.

2 Introduction to Cyber Security, Chwan-Hwa(john) Wu, J. David Irwin, CRC Press T&F Group.

Web Resources:

1. https://www.meity.gov.in/content/cyber-laws
2. https://www.niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
3. https://www.coursera.org/learn/foundations-of-cybersecurity