Course Title: - Cybersecurity Professional (120 hours)

This comprehensive course prepares students to become proficient ethical hackers by providing essential knowledge of cybersecurity fundamentals and hands-on hacking techniques. Covering topics from ethical hacking principles to network security and cryptography, the course equips students to understand, identify, and mitigate cyber threats effectively. Successful completion also prepares students for relevant certifications.

Key Learning Objectives	Course Content	Hours
Module 1: At the end of the module the students will be able to: ➢ Understand the concept of Ethical Hacking and its role in cybersecurity. ➢ Define the Cyber Kill Chain® and its stages. ➢ Differentiate between passive and active reconnaissance. ➢ Explore countermeasures against reconnaissance techniques.	**Module 1:** • **Introduction to Ethical Hacking** • Ethical Hacking • Differences & Limitations • Concepts & Outcome • **Footprinting & Reconnaissance** • Introduction to Reconnaissance • Passive Reconnaissance • Active Reconnaissance • Counter Measures • **Introduction To Cyber Kill Chain®** • **Summary and Review** • **Online quiz test**	**15**

Module 2: At the end of the module the students will be able to: ➢ Learn the fundamentals of network scanning and its importance. ➢ Explore various scanning tools and their applications. ➢ Understand port scanning techniques and methods to evade IDS/Firewall. ➢ Grasp the concept of enumeration and its role in vulnerability assessment. ➢ Identify different enumeration methods such as LDAP, NetBIOS, and DNS. ➢ Learn how to create network diagrams to visualize network architecture.	**Module 2:** • **Scanning Networks** • Network Scanning Concepts • Scanning Tools • Port Scanning Techniques • IDS/Firewall Evasion Techniques • Banner Grabbing • Draw Network Diagram • **Enumeration** • What is Enumeration • LDAP Enumeration • NetBIOS Enumeration • DNS Enumeration • Enumeration Defence • **Vulnerability Identification & Exploit Selection** • Vulnerability Assessment & Solutions • Vulnerability Scoring System • Exploit DB • **System Hacking** • System Hacking Introduction • Password Cracking, Privileged Escalation • Executing Applications • Data Hiding, Covering Tracks • **Summary and Review** • **Online quiz test**	**15**

Module 3: At the end of the module the students will be able to: ➢ Understand the concepts of malware and its different types. ➢ Learn about viruses, worms, trojans, and their characteristics. ➢ Explore malware analysis and anti-malware software. ➢ Gain insights into MAC attacks, ARP positioning, and DNS poisoning. ➢ Discover methods of defending against various attacks. ➢ Understand social engineering concepts and common attack techniques. ➢ Learn about insider threats, identity theft, and mitigation strategies.	**Module 3:** • **Malware** • Malware Concepts • Viruses and Worms • Trojans • Malware Analysis • Anti-Malware Software • **Sniffing** • Sniffing Concepts • Sniffing Techniques • MAC Attack, ARP Positioning • Spoofing Attack, DNS Poisoning • Sniffing Tools • Defending and Countermeasures Techniques Against Sniffing • **Social Engineering** • Social Engineering Concepts • Social Engineering Attacks • Insider Threats • Social Networking Sites • Identity Theft • Assisted Demo: • Getting Email IDs Available in the Public Domain using the Harvester • **Summary and Review** • **Online quiz test**	**15**

Module 4: At the end of the module the students will be able to: ➢ Learn about DoS and DDoS attack concepts and techniques. ➢ Understand session hijacking and its implications. ➢ Explore application-level and network-level session hijacking. ➢ Grasp the basics of IDS/IPS, firewalls, and honeypots. ➢ Discover strategies to detect the presence of honeypots.	**Module 4:** • **Denial of Service** • DoS/DDoS Concepts • DoS/DDoS Attack Techniques • **Session Hijacking** • Session Hijacking Concepts • Application-level Session Hijacking • Network-level Session Hijacking • Countermeasures • **Evading IDS, Firewalls, and Honeypots** • IDS/IPS - Basic Concepts • Firewalls - Basic Concepts • Honeypots • How to Detect a Honeypot • **Summary and Review** • **Online quiz test**	**12**
Module 5: At the end of the module the students will be able to: ➢ Understand web server concepts and attack methodologies. ➢ Explore various web server attacks and their implications. ➢ Learn about patch management and its importance. ➢ Understand web application concepts, threats, and hacking methodologies. ➢ Discover tools and countermeasures for securing web applications.	**Module 5:** • **Hacking Web Servers** • Webserver Concepts • Web Server Attack Methodologies • Web Server Attacks, Patch Management • Web Server Security • **Hacking Web Applications** • Web Application Concepts • Web App Threats • Hacking Methodologies	**14**

➢ Gain insights into SQL injection concepts, types, and prevention.	• Hacking Tools, Countermeasures • **SQL Injection** • SQL Injection Concepts • Types of SQL Injection • SQL Injection Tools • Countermeasures • **Summary and Review** • **Online quiz test**	
Module 6: At the end of the module the students will be able to: ➢ Explore wireless network concepts and terminology. ➢ Understand wireless encryption methods and vulnerabilities. ➢ Learn about wireless hacking techniques and attacks. ➢ Discover countermeasures to protect wireless networks.	**Module 6: Hacking Wireless Networks** • Concepts and Terminology • Wireless Encryption • Wireless Hacking • Wireless Attacks • Wireless Encryption Attacks • Protecting Wireless Networks • **Summary and Review** • **Online quiz test**	**12**
Module 7: At the end of the module the students will be able to: ➢ Learn about mobile platform hacking and countermeasures. ➢ Understand mobile attacks and ways to improve mobile security. ➢ Explore IoT concepts, technologies, and vulnerabilities.	**Module 7: Hacking Mobile Platforms & IoT** • Mobile Platform Hacking • Countermeasures • Mobile Attacks • Improving Mobile Security • IoT Concepts • IoT Technology Protocols • IoT Operating Systems	**15**

➢ Understand IoT hacking methodologies and countermeasures. ➢ Grasp cryptography concepts, encryption algorithms, and hash functions. ➢ Explore public key infrastructure, disk and email encryption, and cryptanalysis.	• IoT Communication Models • IoT Vulnerabilities and Attacks • IoT Hacking Methodology • Countermeasures • **Summary and Review** • **Online quiz test**	
Module 8: At the end of the module the students will be able to: ➢ Understand the fundamental concepts of cryptography. ➢ Explore various encryption algorithms and their applications. ➢ Learn about hash functions and their role in data integrity. ➢ Understand the basics of Public Key Infrastructure (PKI) and its applications. ➢ Discover methods of disk and email encryption. ➢ Gain insights into the process of cryptanalysis. ➢ Identify countermeasures to enhance cryptographic security.	**Module 8: Cryptography** • Cryptography Concepts • Encryption Algorithms • Hashes • Public Key Infrastructure • Disk Encryption • Email Encryption • Cryptanalysis • Countermeasures • **Summary and Review** • **Online quiz test**	**12**

Module 9: At the end of the module the students will be able to: ➢ Understand the concepts and benefits of cloud computing. ➢ Identify common cloud computing threats and attacks. ➢ Explore the layers of cloud security controls and their importance. ➢ Learn about cloud security tools and best practices for securing cloud environments.	**Module 9: Cloud Computing** • Cloud Computing Concepts • Cloud Computing Threats • Cloud Computing Attacks • Cloud Security Control Layers • Cloud Security Tools • **Summary and Review** • **Online quiz test**	**10**