DIPLOMA IN ETHICAL HACKING & CYBER SECURITY

Duration: 1 Year (2 Semester)
Eligibility: 12th Pass / Basic Computer Knowledge
Mode: Theory + Practical + Lab + Live Projects

Semester 1 – Cyber Security Foundations

Introduction to Cyber Security

- What is Cyber Security?
- Types of Hackers (White, Black, Grey)
- Cyber Crimes Overview
- Cyber Laws (Basic)
- Information Security Concepts
- CIA Triad (Confidentiality, Integrity, Availability)

Networking Fundamentals

- Basics of Networking
- OSI Model
- TCP/IP
- IP Addressing
- Subnetting
- DNS, DHCP
- Routers & Switches

Practical:

- IP Configuration
- Network Scanning Basics

Linux Fundamentals

- Introduction to Linux
- Kali Linux Overview
- Linux Commands
- File Permissions
- Package Installation

Practical:

- Kali Linux Setup
- Terminal Practice

Ethical Hacking Basics

- Footprinting
- Reconnaissance
- Scanning Networks
- Vulnerability Assessment
- Introduction to Penetration Testing

Tools Practice:

- Nmap
- Wireshark
- Netstat

Semester 2 – Advanced Ethical Hacking

Web Application Security

- Website Vulnerabilities
- SQL Injection
- XSS (Cross Site Scripting)
- CSRF
- Brute Force Attack
- Password Cracking Basics

Tools:

- Burp Suite
- SQLMap

System Hacking

- Malware Basics
- Trojans
- Keyloggers (Concept)
- Social Engineering
- Phishing Awareness

Wireless Network Security

- Wi-Fi Security
- WPA/WPA2 Concept
- Wireless Attacks (Concept Level)
- Network Hardening

Cyber Defense & Prevention

- Firewall Basics
- Antivirus & IDS/IPS
- Data Encryption
- Secure Coding Basics
- Incident Response

Final Projects

- Network Vulnerability Scan
- Website Security Testing
- Cyber Security Audit Report
- Final Viva & Practical Demonstration

Examination Pattern

- Theory – 100 Marks
- Practical – 100 Marks
- Project – 100 Marks
- Viva – 100 Marks

Career Opportunities

- Ethical Hacker (Junior)
- Cyber Security Analyst
- Network Security Executive
- Penetration Testing Intern
- Security Support Executive