Cyber Leelawat Ethical Hacking Certified Course (CLEHC)

Professional Ethical Hacking & AI-Based Cyber Security Program

Course Overview

CLEHC is a practical cyber security course designed for beginners to advanced learners. This program helps students become professional ethical hackers and penetration testers through real-world practical training, AI-integrated security concepts, and hands-on labs.

Key Highlights

- Beginner to Advanced Learning
- 100% Practical Training
- AI-Integrated Cyber Security
- Real-World Hacking Labs
- Offensive & Defensive Security
- Capture The Flag (CTF) Challenges
- Report Writing Training
- Bug Bounty Fundamentals
- Career Guidance
- Industry-Level Tools

Course Modules

Module 1: Cyber Awareness & Basics

- Ethical Hacking Phases
- Cyber Security Fundamentals
- Types of Hackers
- Cyber Threats & Cyber Hygiene
- Phishing & Social Engineering
- Password & Email Security

- AI in Cyber Security

Tools

- VirusTotal
- HaveIBeenPwned
- Google Password Manager

Module 2: Networking Fundamentals

- LAN, WAN, MAN
- IP Addressing & Subnetting
- OSI & TCP/IP Models
- DNS, HTTP, FTP, SSH
- Routing & Switching
- AI-based Network Monitoring

Tools

- Wireshark
- Cisco Packet Tracer
- Angry IP Scanner

Module 3: Hacking Lab Setup

- Virtual Machines
- Kali Linux Setup
- Windows & Ubuntu Lab Setup
- Virtual Networking
- Snapshots & Recovery
- AI-powered Lab Simulation

Tools

- VirtualBox
- VMware
- Kali Linux

Module 4: Linux for Offensive Security

- Linux Basics & Commands
- Networking Commands
- Bash Scripting
- Linux Hardening
- AI-assisted Automation

Mini Projects

- Bash Port Scanner
- Automated Recon Script

Module 5: Footprinting & Reconnaissance

- WHOIS & DNS Enumeration
- Google Dorking
- Metadata Extraction
- OSINT Techniques
- AI-assisted Reconnaissance

Tools

- theHarvester
- Amass
- Recon-ng
- Maltego
- Shodan

Module 6: Network Scanning & Enumeration

- TCP/UDP Scanning
- Service Enumeration
- Vulnerability Identification
- AI-assisted Network Analysis

Tools

- Nmap
- Enum4linux

- Netcat
- Nessus

Module 7: System Hacking & Exploitation

- Password Attacks
- Exploitation Basics
- Privilege Escalation
- AI-assisted Exploit Analysis

Tools

- Metasploit
- Hydra
- John the Ripper
- LinPEAS
- WinPEAS

Module 8: Advanced Intrusion Techniques

- Post Exploitation
- SQL Injection
- XSS & CSRF
- Persistence Techniques
- AI-driven Threat Simulation

Tools

- Burp Suite
- SQLMap
- Metasploit

Module 9: Malware Threats & Analysis

- Viruses, Worms & Trojans
- Ransomware & Spyware
- Malware Analysis Basics
- AI-based Malware Detection

Tools

- PEStudio
- Procmon
- Wireshark
- Any.Run

Module 10: Cryptography & Data Security

- Encryption & Hashing
- AES, RSA, SHA256
- SSL/TLS & Certificates
- Data Privacy & Integrity
- AI-enhanced Encryption Monitoring

Tools

- OpenSSL
- Hashcat
- VeraCrypt

Module 11: Wireless Network Hacking

- WiFi Security
- WPA/WPA2/WPA3
- Packet Sniffing
- Wireless Defense
- AI-based Wireless Monitoring

Tools

- Aircrack-ng
- Bettercap
- Wireshark

Final Capstone Project

Students will perform:

- Reconnaissance
- Enumeration
- Vulnerability Assessment
- Exploitation
- Professional Reporting

Practical Environment

- Kali Linux Labs
- Windows Labs
- Vulnerable Web Apps
- Internal Network Labs
- CTF Challenges

Course Duration

- Duration: 2.5 Months
- Live Classes: Monday to Friday
- Daily Timing: 1 to 1.5 Hours
- Weekend Practice & Assignments

Course Fees

₹5999 Only

Included:

- Complete Ethical Hacking Training
- AI Cyber Security Modules
- Practical Labs
- Study Material
- Notes & Resources
- Certificate of Completion

Certification

Students will receive the:

Cyber Leelawat Ethical Hacking Certification (CLEHC)

Certification Validates:

- Ethical Hacking Skills
- Penetration Testing Fundamentals
- Linux & Networking Knowledge
- Security Assessment Skills
- AI-assisted Cyber Security Understanding