Cyber Security & Ethical Hacking – From Zero to Job & Freelance Mastery

⏱ Duration:

3 Months | 28+ Classes | 30 Days Internship

Class	Lesson	Topics in Detail
Module 1	Foundation of Cyber Security and Networking	● Understanding Cyber Security: Importance and Principles ● Overview of Cyber Threats and Attack Vectors ● Introduction to Information Security Concepts ● Defining Ethical Hacking and Its Legal Implications ● Different Types of Hackers: White Hat, Black Hat, and Gray Hat ● Ethical Hacking Methodology and Phases ● Risk Management ● Computer Networking ● Network Diagram ● Networking types ● LAN, MAN, WAN ● Computer Network Architecture ● TCP & UDP protocol ● OSI & TCP/IP Model ● Network Topologies ● IP Address | IP Classes ● Networking devices | Switch, Router, Firewall, Bridge ● Private and Public IP address

Module 2	Kali Linux for Beginners	● Discussion on Virtualization ● VMware Workstation & Oracle VirtualBox ● Virtualization Network ● Clone and Snapshot ● Create a New Virtual Device ● Import and Export Virtual Machine ● Overview of Lab System ● Installation & Setup Kali Linux, Nessus, Acunetix, Metasploit Server & Application, Mobexler etc ● Discussion on Linux Operating System ● Overview of Kali System ● Linux Filesystem ● Difference between Linux and Windows ● Linux Commands | Linux User Management ● Group Management ● File & Directory & Permission Management ● Putty, SSH & Telnet ● File and Directory Creation ● GitHub | Package Installation ● Update & Upgrade Linux System ● System Info
Module 3	Human & System-Based Attacks(Denial of Service (DoS) Attack &	● What is Social Engineering ● Types: Phishing, Fake Websites, Impersonation

	Brute Force Attack)	● Lab: Detecting & Preventing Phishing Attacks ● Detail on DoS & DDoS Attack ● Detail on Password Attack ● Mitigation of the Attack & best practice for prevention ● Lab on DoS Attack ● Lab on Brute Force Attack ● Detail on Server System, OS & Application ● System Hacking Tools ● Detail on MITRE Attack ● Lab on System Hacking
Module 4	SOC (Security Operations Center) Essentials	● What is a SOC and How It Works ● Daily Workflow of SOC Analysts ● Introduction to SIEM, Firewall Logs, IDS/IPS ● Simple Log Analysis Activity ● Incident Response Steps ● SOC Career Path: Tier 1 to Analyst
Module 5	OSINT (Open-Source Intelligence)	● What is OSINT ● Why It's Important ● Legal and Ethical Boundaries of OSINT ● Google Dorking Basics ● Using Tools: Shodan, theHarvester, Whois, Maltego (Demo) ● Finding Digital Footprints & Email Leaks ● OSINT Case Study: Tracing a Threat

		Actor ● Freelance & Job Opportunities in OSINT
Module 6	System & Network Hacking	● Exploitation using vulnerability scan report ● Understanding CVE, CVSS ● Understanding and finding open exploits and exploit database ● Understanding Buffer overflow ● Understanding OS & Server Environments ● MITRE ATT&CK Framework Basics ● Tools: Metasploit, Nmap, Hydra Overview ● Lab: Controlled System Hacking Practice ● Ethical Disclosure & Legal Aspects
Module 7	Wi-Fi & Android Mobile Hacking	● Wi-Fi Network Basics & Security Protocols ● Common Wireless Attack Techniques ● Hack Any Wifi And Stealing Password, PIN Via WPS ● How to Perform Deauthentication Attack ● How to Perform Evil-Twin Attack ● Wifi Security ● Lab: Wi-Fi Password Cracking (Demo) ● How Do Hackers Hack Android Devices ● Hacking Android Via RAT/Backdoors

		● Access Any Files, SMS, Call Logs of Target Device ● Hack Front And Back Camera of Target Device ● Track Target Device Location ● Setup Listener & Established Connection of RAT ● Remove Android RAT/Backdoors ● Protect Yourself From RAT/Backdoors
Module 8	Packet Analysis with Wireshark	● Installing & Using Wireshark ● Capturing Live Network Traffic ● Identifying Suspicious Packets ● Lab: Analyze Traffic from a Simulated Attack
Module 9	Penetration Testing	● Introduction To Penetration Testing ● Phases Of Penetration Testing ● White Box Penetration Testing ● Black Box Penetration Testing ● Grey Box Penetration Testing
Module 10	Keyloggers & Spyware	● What is a keylogger? What is spyware? (definitions & real-world impact) ● Differences: keylogger vs spyware vs other endpoint threats ● How To Use Various Keyloggers ● How to Steal Login And Others Information via Spying ● How To Protect Against Keyloggers

Module 11	Malware Threats & Malware Removal From Hacked Website	● What is malware? ● What is a virus and how does it spread? ● Difference between virus, worm, and trojan ● How hackers use malware to damage systems ● Common signs of a malware-infected computer ● What is backdoors ● What is Redirect Malware ● How to Create Malware ● Different Types of Malware Codes ● What is Redirect Malware ● Redirect Malware Injecting And Removal Process ● Remove Malicious Codes / Malware From Website ● Remove Malware Scripts / Malicious Links From Database
Module-12	Website Hacking & Brute Force Attack	● What is website hacking? ● Why hackers attack websites ● Common website attacks (SQL Injection, XSS – basic concept only) ● How hackers steal information from websites ● How to identify if a website is unsafe ● Importance of strong passwords and secure login pages ● How to protect your own website or online accounts ● Real-life examples of hacked website

		● Introduction To HTTP Request (GET, POST) ● Intercepting Request, Repeater, Intruder And Features Of BurpSuite ● Bruteforce & Dictionary Attack ● Sniper & Cluster Bomb Attack ● What is phishing? (simple: tricking people to give passwords or click bad links) ● Common phishing types: email phishing, SMS (smishing), voice (vishing) — very short examples ● What is social media hacking? (fake accounts, scams, account takeover) ● Why attackers target people on social media (easy info + trust) ● Signs of a phishing message or fake social account (bad links, urgent language, unknown sender) ● How attackers gather info from profiles (what to avoid sharing) ● Simple ways phishing is delivered (links, attachments, fake login pages) ● How to protect yourself: check sender, hover links, enable 2FA, strong passwords, privacy settings ● What to do if you or a friend is scammed (report, change passwords, enable recovery options) ● Real-life easy-to-understand examples

		and short stories (teach with cases students can relate to) ● Responsible behavior: never click unknown links or share OTPs/passwords
Module 13	Phishing & Social Media Hacking	● Definition of Cryptography ● Encryption And Decryption ● Kind of Hashes, Generation And Identify Hashes ● Disk Encryption ● Definition of Steganography ● Hiding Secret Messages in A Image ● How to Make Hidden Audio Message ● Hiding Secret File In A Audio ● How to Make Hidden Text File Message ● Hiding File Inside of a Text File
Module 14	Cryptography And Steganography	● Understanding AI and Its Role in Cybersecurity ● How AI Can Automate Scanning & Threat Detection ● AI for Phishing Detection & Malware Analysis ● Using ChatGPT/Gemini for Security Research & Report Writing ● Demo: Using AI to Create and Detect Social Engineering Scenarios ● Future of AI in Ethical Hacking & SOC
Module 15	AI in Cybersecurity &	● Introduction To Vulnerability

	Ethical Hacking	Assessment ● Scanning Vulnerability With Nessus ● Scanning Vulnerability With Acunetix ● Tools: Nessus, OpenVAS Overview ● Writing a Professional Security Report ● Freelancing & Job Roadmap ● Certifications: CEH, CompTIA Security+, OSCP, etc.
Module 16	Vulnerability Assessment & Career Path	● Introduction To Vulnerability Assessment ● Scanning Vulnerability With Nessus ● Scanning Vulnerability With Acunetix ● Tools: Nessus, OpenVAS Overview ● Writing a Professional Security Report ● Freelancing & Job Roadmap ● Certifications: CEH, CompTIA Security+, OSCP, etc.

Key Outcomes:

- 3 International Projects + 30-Day Internship (Assignment-Based)
- Job Placement with International Exam Guidance
- Live Classes + Lifetime Access to Recorded Videos
- Paid Tools Access (for Learning & Practice)
- Free Re-Admission Opportunity Once Within 1 Year After Course Completion
- Lifetime 24/7 Support — Post-Course Assistance for Questions, Career Guidance, and Technical Help
- Want to Study Abroad? — Special Support for International Students: Guidance and Opportunities for Jobs/Freelancing Abroad

- Until You Get Hired or Start Earning from Networking — Continuous Career/Freelancing Support (Job/Income Support Until You Get Hired or Start Earning)

👉 If anyone cannot complete the course or fails to understand properly — they can retake the entire course **completely free!**