CIAAN

CYBER TECH

Cyber Security | Digital Forensics | AI

Ethical Hacking Training

# Prepare for a Career in Cyber Security

**“Now its time to start your career in Cyber Security”**

**Duration** - **6 Months**

Ethical Hacking is a comprehensive program designed to provide participants with a strong foundation in cyber security principles and practices. The course curriculum is structured to cover a range of topics in a hands-on, interactive format, and includes both lectures and lab exercises.

**Duration**

The Ethical Hacking program is typically delivered over a period of 30-45 days, with each day consisting of 1 hour of sessions. A total of 180 Hours. Including Live Sessions and Lab Access

Throughout the program, participants will have the opportunity to apply what they have learned in a variety of hands-on exercises and case studies, designed to give them practical experience in identifying and mitigating cyber security threats. Upon completion of the program, participants will have a strong understanding of the key concepts and practices needed to protect their organizations from cyber-attacks.

**Sessions**

The Sessions curriculum for the Ethical Hacking Training program includes the following topics:

**ETHICAL HACKING**

- What is Information Security?
- Problems faced by the Corporate World
- Why Corporate needs Information Security?
- Who is a Hacker?
- Type of Ethical Hackers
- Hackers vs. Crackers
- Classification of Hackers
- Phases of Hacking
- Basic Terminologies
- Skills of Ethical Hacker

**NETWORKING**

- IP Address
- Finding a Remote IP Address
- Hiding Your IP Address
- Tracing an IP Address
- MAC Address
- Internal VS External IP Addresses
- MAC Addresses
- MAC Addresses Spoofing
- MACCHANGER
- Unblocking Websites

**KALI LINUX**

- Introduction
- Installation
- Basic Linux Command
- Installing Linux Application
- Assigning IP Address in Kali
- Changing the default password
- Updating the applications and operating system
- VMware Workstation

**GOOGLE HACKING**

- GHDB
- Finding Login Page
- Directory Listing
- Use of Advance Search Operator

**WEBSITES TESTING & NETWORK SCANNING**

- Use of NMAP for Operating
- Port Scanning of Websites
- OS Fingerprinting

**SYSTEM HACKING**

- System Hacking Techniques
- Window Hacking
- Window Security
- Hiding Files
- Konboot

**WIRELESS HACKING**

- Introduction of Wireless Network
- Types of Wireless Network
- Wireless Technology
- Advantages and Disadvantages of Wireless Network Wireless Cracking WEP, WPA, WPA2
- Wireless Security
- Tips to Secure Wireless Network

**KEYLOGGER**

- What is Keylogger
- Categorization of Keystroke Loggers
- Advanced Keylogger
- Keylogger Installation
- Hardware Keylogger

**USB HACKING & BROWSER HACKING**

- USB
- Blocking USB Devices
- Browser Security
- Web Browser Hacking

**DDOS**

- Introduction to Distributed Denial of Service Attacks?
- Working of Distributed Denial of Service Attacks?
- Symptoms of a DOS Attack
- Impact DDOS/DOS Attack

**SOCIAL ENGINEERING**

- What is Social Engineering?
- Techniques of Social Engineering
- Attempt Using Phone, E-mail, Traditional Mail, In person.

**FIREWALLS**

- What Does a Firewall Do?
- What a Firewall cannot do
- How does a Firewall work?
- Types of Firewalls
- Working of Firewall
- Advantages and Disadvantages of Firewall

## Cyber Security Basics

| Day | Topics |
|---|---|
| 1 | Introduction to Cyber Security — CIA Triad, types of threats |
| 2 | Network Security — Basics of IP, ports, firewalls, IDS/IPS |
| 3 | System & Endpoint Security — Patch mgmt, antivirus, OS hardening |
| 4 | Web Security & Safe Browsing — HTTPS, cookies, OWASP intro |
| 5 | Cyber Hygiene & Career Paths — Passwords, MFA, cyber laws, careers |

## Offensive Hacking Fundamentals

| Day | Topics |
|---|---|
| 6 | Hacking Methodology — Phases: Recon to Reporting |
| 7 | Reconnaissance Techniques — Passive & Active (Nmap, Shodan) |
| 8 | Vulnerability Scanning — OpenVAS, Nikto, Metasploit |
| 9 | Web Hacking Basics — SQLi, XSS, Burp Suite hands-on |
| 10 | CTF & Red Team Basics — Reverse shell, privilege escalation, flag capture |

## Deep Recon, Scanning & Exploitation

| Day | Topics |
|---|---|
| 11 | Footprinting: WHOIS, Dorking, OSINT |
| 12 | Network Scanning: Nmap, Netdiscover |
| 13 | Enumeration: SMB, FTP, SNMP |
| 14 | Vulnerability Scanning: Nessus/OpenVAS |
| 15 | Exploit Research: CVEs, ExploitDB, Searchsploit |
| 16 | Metasploit Usage + Manual Exploitation |
| 17 | Lab Practice – Recon to Exploit using Metasploitable2 |

## Web Application Hacking (OWASP)

| Day | Topics |
|---|---|
| 18 | OWASP Top 10 Overview |
| 19 | SQL Injection (manual & tool-based) |
| 20 | Cross-Site Scripting (Reflected, Stored, DOM) |
| 21 | File Upload & Directory Traversal |
| 22 | Command Injection & RCE |
| 23 | Broken Auth, Insecure Deserialization |
| 24 | Burp Suite Deep Dive (Intruder, Repeater, Scanner) |

**System Hacking, Passwords & Wireless**

| Day | Topics |
|---|---|
| 25 | Password Grabbing Tools |
| 26 | Windows Privilege Escalation Basics |
| 27 | Password Cracking (Hydra, John, Hashcat) |
| 28 | Wi-Fi Attacks: airodump-ng, aircrack-ng |
| 29 | Capturing Passwords of Saved WiFi |

## 🧰 Tools Used:

- **Operating Systems: Kali Linux, Windows 10, Ubuntu Server**
- **Platforms: TryHackMe, DVWA, Juice Shop, Metasploitable2, Hack The Box**
- **Tools: Nmap, Burp Suite, Nessus, Metasploit, Wireshark, Hydra, Aircrack-ng, SET Toolkit**

**There are 20+ more Ethical Hacking Modules mentioned below.**

**This Program is bundled course of Basic Networking, Linux Commands and Cyber Security as well.**

Our Ethical Hacking Course provides participants with the knowledge and skills to understand and counteract cybersecurity threats by ethically hacking systems. The course aims to train individuals on how to identify vulnerabilities in networks, systems, and applications in a lawful and legitimate way, simulating the techniques and tactics used by malicious hackers.

**Course Overview:**

**1. Introduction to Ethical Hacking**

- Definition and Role of Ethical Hackers: Understanding the legal and ethical aspects of hacking, and how ethical hackers differ from malicious hackers.
- Types of Hackers: White-hat (ethical), black-hat (malicious), and grey-hat hackers.
- Hacking Phases: Reconnaissance, scanning, gaining access, maintaining access, and covering tracks.
- Cybersecurity Landscape: Overview of the global cybersecurity landscape and the need for ethical hackers.

**2. Reconnaissance and Footprinting**

- Active and Passive Reconnaissance: Techniques for gathering information on a target system.
- Footprinting Tools: Use of tools like WHOIS, Nslookup, and social engineering tactics for gathering initial information.
- OSINT (Open Source Intelligence): Leveraging public data for footprinting.

**3. Scanning Networks**

- Network Scanning Techniques: Identifying live hosts, open ports, and services running on target machines.
- Vulnerability Scanning: Introduction to scanning tools such as Nmap, Nessus, and OpenVAS.
- Banner Grabbing: Identifying software and service versions to detect vulnerabilities.

**4. Enumeration and Exploitation**

- What is Enumeration?: Extracting information about users, groups, shares, and network resources.
- Tools for Enumeration: NetBIOS, SNMP enumeration, and LDAP enumeration.
- Exploitation: How to exploit known vulnerabilities in systems using ethical hacking tools like Metasploit.

**5. Gaining Access**

- System Hacking Techniques: Password cracking, privilege escalation, and exploiting vulnerabilities.
- Common Vulnerabilities: Misconfigurations, unpatched software, weak passwords, etc.
- Remote Exploits: Understanding tools like Metasploit and using exploits to gain access to target systems.

**6. Maintaining Access**

- Backdoors and Rootkits: Techniques to maintain persistent access to a compromised system.
- Remote Administration Tools (RATs): How attackers use RATs to control systems.
- Covering Tracks: How hackers erase evidence of an attack and how ethical hackers can prevent this.

**7. Web Application Hacking**

- Web Application Security: Overview of common web vulnerabilities, such as SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).
- Web Application Exploitation Tools: Tools like Burp Suite, OWASP ZAP for testing web applications.
- Session Hijacking and Cookie Exploitation: Techniques used by hackers to

impersonate legitimate users.

**8. Wireless Network Hacking**

- Wi-Fi Security: Understanding WEP, WPA, and WPA2 encryption and how they can be compromised.
- Wireless Hacking Tools: Tools like Aircrack-ng for cracking wireless networks.
- Wireless Exploitation: How to exploit weak wireless configurations.

**9. Social Engineering**

- What is Social Engineering?: Techniques that manipulate human psychology to gain unauthorized access to systems.
- Common Attacks: Phishing, spear-phishing, and pretexting.
- Defensive Measures: How to educate users to prevent social engineering attacks.

**10. Malware Threats**

- Understanding Malware: Types of malware, such as viruses, worms, Trojans, ransomware, and spyware.
- Malware Detection and Prevention: How to detect and remove malware, and secure systems against infection.
- Analyzing Malware Behavior: Introduction to sandboxing and reverse engineering of malware.

**11. Sniffing and Evasion**

- What is Sniffing?: Techniques for intercepting network traffic using tools like Wireshark and tcpdump.
- Session Hijacking and Man-in-the-Middle (MitM) Attacks: How attackers intercept and manipulate communications.
- Defensive Measures: How to protect networks from sniffing and MitM attacks.

**12. Denial of Service (DoS) and DDoS Attacks**

- DoS and DDoS Attacks: Techniques that overload systems and networks to deny service to legitimate users.
- Common Tools: Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC).
- Mitigation Techniques: How to protect against DoS and DDoS attacks using firewalls, load balancers, and other techniques.

**13. Mobile Platform Hacking**

- Mobile OS Vulnerabilities: Exploiting vulnerabilities in Android and iOS devices.
- Mobile Hacking Tools: Tools and techniques for compromising mobile devices.
- Mobile Application Security: Testing the security of mobile apps.

**14. Cloud Security and Hacking**

- Cloud Infrastructure: Understanding cloud services (IaaS, PaaS, SaaS) and their vulnerabilities.
- Cloud Security Threats: Cloud misconfigurations, data breaches, and compromised credentials.
- Ethical Hacking in the Cloud: Testing cloud environments for vulnerabilities.

**15. Penetration Testing Methodology**

- Planning and Scoping: Understanding the objectives and scope of a penetration test.
- Testing Phases: Information gathering, vulnerability analysis, exploitation, post-exploitation, and reporting.
- Tools: Practical use of tools like Metasploit, Burp Suite, and Nmap in penetration testing.

**16. Real-World Case Studies**

- Live Hacking Demonstrations: Step-by-step walkthroughs of real-world hacking incidents.
- Case Studies: Analysis of major cyberattacks and how they were executed.
- Defensive Strategies: What organizations could have done to prevent these attacks.

**17. Reporting and Documentation**

- Ethical Hacker’s Reports: How to prepare comprehensive vulnerability reports.

- Remediation Plans: Providing clients with actionable steps to fix vulnerabilities.

**Learning Outcomes:**

By the end of the course, participants should be able to:

- Conduct ethical hacking and penetration testing in a lawful manner.

- Identify vulnerabilities and assess the security of systems and networks.

- Use common hacking tools and techniques to simulate real-world attacks.

- Create detailed security reports and offer remediation advice.

- Understand the legal, ethical, and practical implications of hacking.

**Attending Benefits**

▪ Software’s Toolkit  PPTs, PDFs, etc.

▪ Certificate of Completion

▪ Internship Opportunity for Freshers

**Learning Platform :**

Google Meet.

**Meeting link will be shared 2 days before the commencement of Sessions.*

**Pre-requisites**

Basic Knowledge of Computer

**Registration**

Fill out the registration form mentioned below.

---

**Contact**

Incase of queries, please feel free to write to us at **info@ciaancyber.com** or **WhatsApp** us at **+91 7670835742**