CiotX

Ethical Hacking

Practical Offensive Security Bootcamp

CiotX

About Bootcamp

This is a fully practical training program designed to introduce you to ethical hacking and penetration testing.

You'll begin by learning the core principles of cybersecurity, then progress through hands-on labs and real-world attack simulations.

By the end of the bootcamp, you'll be equipped with skills that are directly applicable to roles Such as Penetration Tester, Offensive Security Engineer.

Whether you're a college student or someone already working in IT, this course will help you build a solid foundation in ethical hacking and to pursue a career in cybersecurity.

Requirements to Get Started

- No prior experience with cybersecurity required, Everything will be taught from the basics.
- Basic computer literacy is enough to begin
- A laptop with at least 256 GB storage
- Minimum 8 GB RAM
- Processor : Intel i3 or Ryzen 3 and above

Bootcamp Content

Phase 1 – Foundations of Ethical Hacking

- Introduction to Offensive Security and Ethical Hacking
- Understanding the CIA Triad and Security Models
- Phases of a Penetration Testing life cycle
- Introduction to Cybersecurity Frameworks
- Lab Setup: Virtual Machines on VMware
- Linux Fundamentals for Hackers (CLI, Bash, File System, Permissions)
- Windows Basics for Red Teamers (CMD, PowerShell, File System)
- Networking Essentials (IP, DNS, Subnetting, Ports, Protocols)

Phase 2 – Core Network Penetration Testing

- Information Gathering : Active and Passive
- Enumeration of services and ports
- Vulnerability Assessment using Nessus
- Exploitation with Metasploit, ExploitDB, and manual techniques
- Post-Exploitation: Privilege Escalation, Passwords and Hash Cracking

Bootcamp Content

Phase 3 – Web Application Security Testing

- OWASP Top 10 Deep Dive
- Lab Setup: Burp Suite
- Web Recon; crawling, fuzzing, enumeration
- File Upload Vulnerabilities and Bypasses
- SQL Injection (Manual and Automated with sqlmap)
- Command Injection and RCE
- Cross-Site Scripting (Stored, Reflected, DOM-based)
- Broken Authentication and Access Control Abuse
- OAUTH Vulenerabilities
- SSRF
- Business Logic Vulns - Race Conditions
- Local File Inclusion

Phase 4 – AI Penetration Testing

- Introduction to world Of Machine Learning, AI, RAG, MCP, Tokens
- Prompt Injections
- Jail Breaking LLMs
- RAG Exploitations
- MCP + SSRF
- AI Defenses

Bootcamp Content

Phase 5 – Misc

- Introduction to Reverse Engineering
- Git & Fundamentals of DevSecOps
- Basics Of Digital Forensics
- Developing our own VPN servers

Phase 6 – Professional Practice and Career Prep

- Bug Bounty Hunting Career Paths
- Writing Penetration Test Reports
- Red Team vs Blue Team Career Paths
- Resume Building for Cybersecurity Roles
- CTFs

Contact Information

+91 91769 99144
+91 88972 85938

MIG Flat No 36, Block 3, INSTACKS TECHNOLOGIES PVT LTD, 5, Kukatpally Housing Board Colony, Kukatpally, Hyderabad, Telangana 500072

www.ciotx.com