cirvee

Ethical Hacking Program

Duration: 3½ Months (14 Weeks)

Mode: Physical & Virtual

Summary

Learn how to ethically hack, test, and secure systems through real-world labs and simulations — using the same tools trusted by global cybersecurity professionals.

Course Overview

The **Cirvee Ethical Hacking Program (Level 3)** is an advanced cybersecurity course that trains learners to ethically identify, exploit, and fix system vulnerabilities. Over 14 intensive weeks, you'll go beyond theory — performing live labs, penetration tests, and reporting exercises that mirror real company assessments.

You'll master tools like **Nmap, Burp Suite, Metasploit, Wireshark, and Nessus,** while learning how hackers think, operate, and are detected. The course includes vulnerability scanning, web app testing, privilege escalation, post-exploitation, and even phishing simulations — all carried out safely within isolated lab environments.

Every learner will complete a **capstone pentest simulation,** running a full engagement from reconnaissance to exploitation and report presentation. This course also prepares you for certifications like **CEH, OSCP, and CompTIA Pentest+**, equipping you for professional pentesting or red team roles anywhere in the world.

Modules Overview

01. **Introduction to Ethical Hacking & Lab Setup**

Understand ethics, rules of engagement, and set up your hacking lab safely using Kali or Parrot OS.

02. **Reconnaissance & OSINT**

Learn information gathering through WHOIS, Shodan, Google Dorking, and subdomain discovery.

03. **Scanning & Enumeration I**

Perform network discovery, port scanning, and service identification using Nmap and Masscan.

04. **Scanning & Enumeration II**

Deepen your scans using NSE scripts, banner grabbing, and web enumeration with Nikto.

05. **Vulnerability Discovery & Triage**

Use OpenVAS/Nessus for vulnerability scanning and learn CVE lookup and risk prioritization.

06. **Exploitation Fundamentals**

Understand exploit lifecycles, payloads, and use Metasploit to gain access ethically.

07. **Privilege Escalation (Linux & Windows)**

Practice local privilege escalation and misconfiguration exploitation in both environments.

08. **Post-Exploitation & Lateral Movement**

Learn persistence, pivoting, tunneling, and lateral network movement techniques.

09. **Web Application Hacking I (OWASP)**

Explore OWASP Top 10 vulnerabilities including XSS, injection, and file upload flaws.

10. **Web Application Hacking II (APIs & Authentication)**

Test APIs and session management using Burp, Postman, and JWT analysis.

11. **Wireless, IoT & Mobile Basics**

Capture WPA handshakes and analyze IoT and mobile application vulnerabilities.

12. **Social Engineering (Safe Simulation)**

Understand phishing techniques, email spoofing, and human-layer vulnerabilities.

13. **Reporting, AI Productivity & Detection**

Write professional pentest reports and use AI tools ethically for documentation.

14. **Capstone Pentest Simulation & Presentation**

Perform a full ethical hacking engagement and present your findings to a review panel.

Career Opportunities

After this program, you can work as a:

- Ethical Hacker / Penetration Tester
- Vulnerability Analyst
- Application Security Tester
- Red Team Operator (Junior)
- Cybersecurity Consultant
- Security Research Assistant

Stay Cirvee Tip

“You’re not just finding flaws — you’re building the skills to protect what matters most.”

Visit Us

☎ 07047007055

“Cirvee” on google map

www.cirvee.com

Stay Connected

@cirvee

@hellocirvee

Cirvee Academy

Cirvee