HACKSTRIX

OFFENSIVE & DEFENSIVE CYBER SOLUTIONS

HACKSTRIX

CERTIFIED ETHICAL HACKER

HCEH Syllabus

Overview: Hackstrix Certified Ethical Hacking

01

Cybersecurity Foundations

Modules 1–5 cover ethical hacking basics, reconnaissance, scanning, enumeration, and vulnerability assessment.

02

Offensive Security

Modules 6–10 explore exploitation, malware analysis, packet sniffing, social engineering, and DoS attacks.

03

Web Security & Red Team

Modules 11–15 cover session attacks, evasion, web server testing, web app pentesting, and red team operations.

04

Certification Goal

Demonstrate real-world ethical hacking competency and earn the HCEH credential from Hackstrix.

Course At a Glance

15

Total Modules

Spanning three tracks: foundations, offensive security, and web & red team operations.

3

Difficulty Levels

Modules progress from Easy through Medium to Hard, building skills incrementally.

40+

Study Hours

Estimated hours across Modules 1–5 alone; full course demands deep practical engagement.

Modules 1–5: Cybersecurity Foundations

*The **foundational track** builds the core knowledge every ethical hacker needs — from understanding the threat landscape to hands-on reconnaissance, scanning, and vulnerability assessment techniques.*

Module 1

*Intro to **Ethical Hacking** — 6 hrs | Easy*

Module 2

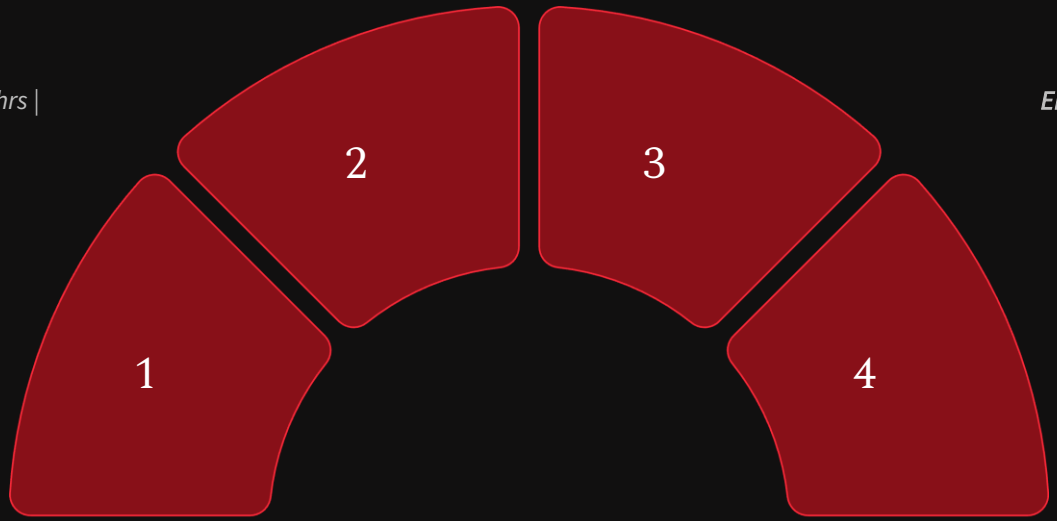
***Reconnaissance** & OSINT — 8 hrs | Medium*

Module 3

***Network Scanning** & Mapping — 8 hrs | Medium*

Modules 4–5

***Enumeration** & Vulnerability Assessment — 16 hrs*



Module 6: System Exploitation

The first offensive module dives into active attack techniques against live systems. Students learn how attackers gain and maintain unauthorized access — and how defenders detect and respond to each step.

Password Attacks

Brute force, dictionary attacks, and credential stuffing techniques against authentication systems

Privilege Escalation

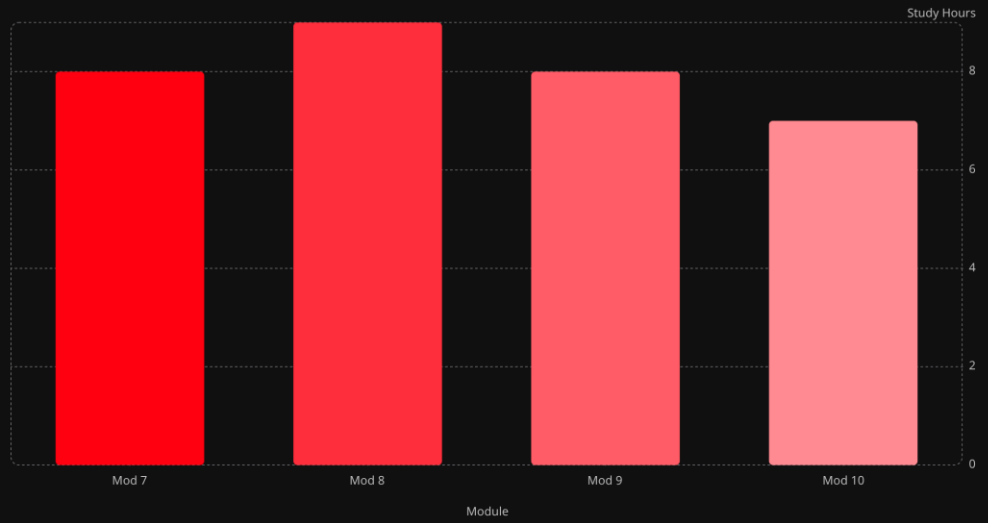
Authentication bypass and escalation methods to gain elevated access on compromised systems

Post-Exploitation

Persistence mechanisms, lateral movement, and responsible post-exploitation documentation

Modules 7–10: Attack Techniques

Estimated Study Time by Module



Offensive Security Deep Dives

Modules 7–10 build practical attack knowledge across malware analysis, network packet sniffing, social engineering manipulation, and denial-of-service methodologies.

Each module includes hands-on labs. Understanding attack techniques is essential for building effective defenses.

Web Security

Module 11: Session Attacks

Session hijacking, cookie manipulation, and authentication attack patterns against web applications.

Module 13–14: Web Testing

Web server security testing and full web application penetration testing methodologies and tools.

Red Team Operations

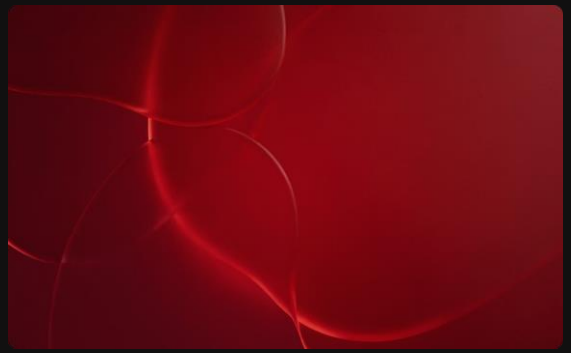
Module 12: Evasion

Techniques to bypass firewalls, IDS/IPS, antivirus, and other security device controls.

Module 15: Red Team Methods

Advanced adversary simulation, campaign planning, and coordinated red team operation strategies.

Detect • Defend • Dominate Cyber Threats

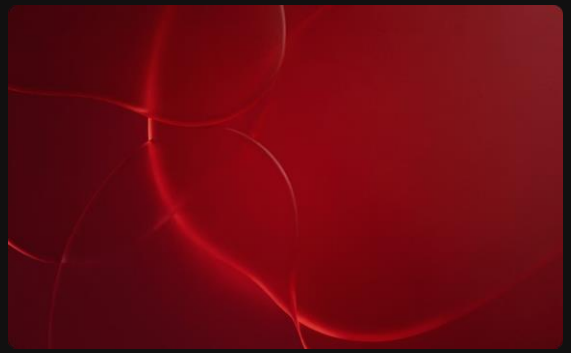


Foundations Track

Modules 1–5 build your base: ethical hacking principles, OSINT, scanning, enumeration, and vulnerability assessment.

Offensive Track

Modules 6–10 sharpen attack skills: exploitation, malware, sniffing, social engineering, and DoS techniques.



Red Team Track

Modules 11–15 complete the journey: web security, evasion, application pentesting, and red team operations.

The HCEH certification equips you with the skills to think like an attacker, defend like a professional, and operate with the ethics of a trusted security expert.
Hackstrix — Detect • Defend • Dominate.