empowers Academy

CYBERSECURITY SPECIALISATION · 12 WEEKS · ONLINE

Cybersecurity (CEH v13) Programme

Become a proactive security defender. Master AI-driven ethical hacking, penetration testing and threat defense across a structured, institution-grade 12-week curriculum — built around the Certified Ethical Hacker v13 standard.

12	4	15+	1
WEEK FRAMEWORK	LEARNING PHASES	INDUSTRY TOOLS	CAPSTONE PEN-TEST

Document Type
Course Curriculum Brochure

Standard
Certified Ethical Hacker v13

Prepared For
Prospective Learners

ABOUT EMPOWERS ACADEMY

Built by Engineers. Designed for Outcomes.

Empowers Academy is a mentor-led online academy focused on one thing: turning motivated learners into industry-ready professionals. Our cohorts are intentionally small, our instructors are practising security and infrastructure professionals, and our curriculum is rebuilt continuously around how modern security teams actually work — with AI-driven tooling at the core, not as an afterthought.

12
WEEK INTENSIVE

4
LEARNING PHASES

0
INFRA COST TO LEARNERS

1:1
LAB & REPORT REVIEWS

Zero Cramming Model

We replace exam-dump memorisation with a paced, system-habit-first curriculum so graduates succeed in real deployments — not just on paper.

AI-Native Hacking

Specialised security models generate and explain commands dynamically, keeping learners focused on strategy and analysis over syntax memorisation.

Structured Lab Environments

A closed, institutional virtual lab network with vulnerable-by-design targets (DVWA, OWASP Juice Shop) guarantees legal, zero-cost hands-on practice.

Report-Ready Graduates

Every phase ends with a professional deliverable — from OSINT findings to a full penetration test report — building a real portfolio, not just a certificate.

PROGRAMME AT A GLANCE

From First Scan to Professional Ethical Hacker

The Certified Ethical Hacker (CEH) v13 is the latest, globally recognised standard for defensive security — notable for integrating AI into ethical hacking. This standalone module trains students to become Ethical Hackers or Cybersecurity Professionals, transitioning them from passive tech users into proactive security defenders who identify, assess and patch vulnerabilities before malicious actors can exploit them.

- 12 Weeks · 4 Phases
- Live + Recorded Delivery
- Weekend & Weekday Batches
- AI-Driven Threat Intelligence
- No Prior Security Experience Needed

Format

Live online, offline classroom, or hybrid delivery with recorded sessions — weekend and weekday batch options available.

Who It's For

B.Tech & MCA students, fresh graduates, working professionals and career switchers. A foundation module covers networking and Linux basics from zero.

How You'll Learn

30% theory, 70% hands-on labs — weekly quizzes, monthly assessments, a capstone project and mock interviews built around real attack-and-defend scenarios.

Where It Leads

SOC Analyst, Penetration Tester and Security Engineer roles — with a documented vulnerability assessment portfolio to prove it.

CYBERSECURITY SPECIALISATION

Four Phases, 12-Week Framework

Each phase builds directly on the last — from network fundamentals to a full-scale, professionally reported penetration test.

WEEKS 1-3

Phase 1
The Recon Baseline

Networking, Linux & AI-assisted scanning

WEEKS 4-6

Phase 2
System Hacking & Exploitation

Vulnerability analysis, Metasploit & cracking

WEEKS 7-9

Phase 3
Advanced Threats

Malware, sniffing & web app hacking

WEEKS 10-12

Phase 4
Modern Environments & Capstone

Wireless, IoT, cloud & final pen-test

CURRICULUM COVERAGE

- Cybersecurity fundamentals, networking basics, TCP/IP protocols, OSI model, and Linux/Windows security
- AI in Cybersecurity (new to v13): using AI tools to automate script creation, threat modelling and vulnerability scanning
- Footprinting, reconnaissance, network scanning, enumeration, system hacking and vulnerability assessment
- Malware analysis, sniffing, social engineering, IoT/Cloud hacking, and web application security (SQLi, XSS)
- Wireless security and mobile security
- Evading Intrusion Detection Systems (IDS), firewalls and applied cryptography

LEARNING OUTCOMES

Skills You'll Actually Use

This course transitions students from passive tech users to proactive security defenders — teaching them to identify, assess and patch vulnerabilities before malicious actors can exploit them, using the latest AI-driven threat intelligence.

- ✓ **Vulnerability Assessment** — Perform vulnerability assessments and conduct penetration testing on live lab targets.
- ✓ **Network & System Security** — Secure networks and systems while identifying and prioritising security risks.
- ✓ **Attack Analysis** — Analyse cyber attacks and write clear, professional security reports.
- ✓ **Tooling Fluency** — Use industry-standard security tools confidently across recon, exploitation and defence.
- ✓ **AI-Assisted Operations** — Use AI models to generate, explain and verify security commands and scripts.

Roles This Prepares You For

Jr. SOC Analyst | Penetration Tester | Security Engineer | Vulnerability Analyst | Ethical Hacker | Threat Intelligence Analyst

1 The Recon Baseline

Weeks 1–3
Deliverable: OSINT & Recon Report

Phase goal: build the networking, Linux and reconnaissance foundation every ethical hacker needs, and get comfortable generating AI-assisted scans with judgement.

WEEK-BY-WEEK

- **Week 1:** Networking & Linux Fundamentals — IP addressing, TCP/UDP, OSI model, Linux CLI
- **Week 2:** Footprinting & OSINT — passive information gathering using Whois, theHarvester, Shodan
- **Week 3:** AI-Assisted Scanning — active scanning using Nmap generated via AI tools like DorkGPT

YOU'LL BE ABLE TO

- Read and reason about IP addressing, TCP/UDP and the OSI model
- Passively gather intelligence on a target without alerting it
- Generate and verify AI-assisted Nmap scans with real understanding

ENGINEERING LABS

Set up your Kali Linux environment · run a full passive OSINT sweep on a lab target · complete an AI-generated active scan and document findings by week 3.

Tools

Kali Linux · Whois · theHarvester · Shodan · Nmap · DorkGPT

Deliverable

A documented OSINT & reconnaissance report on an assigned lab target.

2 System Hacking & Exploitation

Weeks 4–6
Deliverable: Exploitation & Cracking Report

Phase goal: move from scanning to exploitation — assess vulnerabilities, exploit them safely in the lab, and recover credentials the way real attackers and defenders do.

WEEK-BY-WEEK

- **Week 4:** Vulnerability Analysis — Nessus, OpenVAS scanning and triage
- **Week 5:** The Metasploit Framework — exploiting known vulnerabilities in a controlled lab
- **Week 6:** Password Cracking & Privilege Escalation — Hashcat, John the Ripper

YOU'LL BE ABLE TO

- Run and interpret vulnerability scans against lab infrastructure
- Exploit known CVEs using the Metasploit Framework responsibly
- Crack recovered password hashes and escalate privileges on a target host

ENGINEERING LABS

Scan a vulnerable lab host with Nessus/OpenVAS · exploit an identified vulnerability with Metasploit · crack recovered hashes with Hashcat and John the Ripper.

Tools

Nessus · OpenVAS · Metasploit · Hashcat · John the Ripper

Deliverable

An exploitation and privilege-escalation writeup with remediation notes.

3 Advanced Threats

Weeks 7–9
Deliverable: Web App & Traffic Assessment

Phase goal: understand how modern attacks unfold — from social engineering and malware to man-in-the-middle traffic manipulation and web application exploitation.

WEEK-BY-WEEK

- **Week 7:** Malware & Social Engineering — trojans, ransomware, deepfakes, AI-generated phishing
- **Week 8:** Network Sniffing & MITM — Wireshark, man-in-the-middle attacks
- **Week 9:** Web Application Hacking — OWASP Top 10, SQLi, XSS on local web apps like DVWA

YOU'LL BE ABLE TO

- Recognise malware families and social-engineering / AI-phishing tactics
- Capture and analyse live traffic to spot man-in-the-middle attacks
- Identify and responsibly exploit OWASP Top 10 vulnerabilities in a sandboxed web app

ENGINEERING LABS

Analyse a captured malware sample · run a MITM exercise with Wireshark on the campus lab network · complete SQLi and XSS exploitation drills on DVWA and OWASP Juice Shop.

Tools

Wireshark · Burp Suite · DVWA · OWASP Juice Shop

Deliverable

A web application security assessment covering at least two OWASP Top 10 categories.

4 Modern Environments & Capstone

Weeks 10–12
Deliverable: Full Penetration Test Report

Phase goal: extend offensive skills into wireless, IoT and cloud environments, then bring every phase together in a full-scale, professionally reported penetration test.

WEEK-BY-WEEK

- **Week 10:** Wireless & IoT Hacking — Aircrack-ng, smart device vulnerabilities
- **Week 11:** Cloud Security Evasion — misconfigurations in AWS S3 and Azure
- **Week 12:** Capstone Project — full-scale penetration test and professional vulnerability report submission

YOU'LL BE ABLE TO

- Assess wireless network and IoT device security
- Identify common cloud storage and access-control misconfigurations
- Plan, execute and document a full penetration test end-to-end

ENGINEERING LABS

Audit a wireless lab network with Aircrack-ng · identify misconfigured cloud storage on a sandbox AWS/Azure account · execute and document the capstone penetration test across a multi-host lab environment.

Tools

Aircrack-ng · AWS & Azure sandbox accounts · Maltego

Deliverable

A complete, professional-grade penetration test and vulnerability report.

THE PRACTICAL TOOLSET

The Complete Security Testing Toolkit

Everything below is used hands-on in labs and projects — not just mentioned on a slide. Every tool maps to a phase of the 12-week framework.

Reconnaissance & OSINT

Whois | theHarvester | Shodan | Maltego

Scanning & Vulnerability Analysis

Nmap | Nessus | OpenVAS

Exploitation & Access

Metasploit | Hydra | Hashcat | John the Ripper

Traffic & Web Application

Wireshark | Burp Suite | DVWA | OWASP Juice Shop

Wireless & Cloud

Aircrack-ng | AWS Educate | Azure Sandbox

AI-Assisted Operations

ShellGPT | DorkGPT | Kali Linux

WHAT SETS THIS COURSE APART

Our Strategic Edge

To outpace standard 8-week boot-camp offerings, the curriculum is anchored on two differentiators: AI-native tooling and a fully institutional lab environment.

1

The "AI-Native Hacking" Framework

We use specialised security models — like ShellGPT and DorkGPT — to dynamically generate and explain commands, bypassing steep syntax learning curves and keeping students focused on strategy and analysis rather than memorising 19+ separate tool syntaxes.

2

Structured Laboratory Environments

We replace unverified external downloads with a formal, closed institutional virtual lab network deploying open-source, vulnerable-by-design instances (DVWA, OWASP Juice Shop) on a centralised campus server — guaranteeing zero infrastructure cost and full legal compliance.

3

Verified, Zero-Cost Academic Partnerships

Authorised use of academic partnerships and verified free tiers (such as TryHackMe) keeps operational overhead at zero while still exposing learners to realistic, guided challenges.

WHY THIS CURRICULUM EXISTS

Identified Gaps In The Cybersecurity Training Market

Research into current cybersecurity market models surfaced three significant gaps that this curriculum is designed to close.

⚠

The Cramming Vulnerability

Standard 8-week boot camps force students to memorise command syntax and exam dumps without understanding underlying system and network habits — producing graduates who fail in real-world deployments.

🖨

The Pacing Overwhelm

Official platforms mandate over 19 separate tool categories, requiring students to learn dozens of distinct applications — overwhelming for institutional learners on a fixed timeline.

⚖

The Ethical & Legal Gray Area

Relying on unverified external channels for resources compromises institutional integrity and exposes academic networks to malware risk.

✔

Our Response

An AI-native, phased curriculum on a closed institutional lab network — paced for understanding, legally compliant, and free of unverified external dependencies.

HOW YOU'LL LEARN

A Standardised Lab Structure, Every Week

Every lab topic across the course follows the same eight-part structure — ensuring consistent learning outcomes and building the habit of professional security documentation from week one.

1. **Objective**
   What this lab is training you to be able to do.
2. **Requirements**
   Environment, access and tooling needed before you start.
3. **Commands**
   The exact, verified commands used in the exercise.
4. **Expected Output**
   What a correct run should return, so learners can self-check.
5. **Troubleshooting**
   Common failure points and how to resolve them.
6. **Assignment · Mini Project · Reflection**
   Applied practice, a small build, and questions that consolidate the concept.

BUILD AS YOU LEARN

Projects For Your Security Portfolio

Every project below is built, reviewed and documented during the programme — a public, verifiable record of what you can assess and defend.

Network Vulnerability Assessment

A full scan-to-report cycle on a lab network, identifying and prioritising discovered vulnerabilities.

Web Application Security Testing

OWASP Top 10 testing against DVWA / OWASP Juice Shop, including SQLi and XSS exploitation.

Wireless Security Assessment

An Aircrack-ng driven audit of a lab wireless network's configuration and defences.

Security Audit Report

A professional-grade written report summarising findings, risk ratings and remediation steps.

Capstone: Full Penetration Test

The week-12 finale — a full-scale, end-to-end penetration test across a multi-host lab environment, submitted as a professional vulnerability report.

BEYOND THE CORE COURSE

The DevSecOps Integration Track

While the Cybersecurity course stands independently, it converges powerfully with Empowers Academy's Cloud Computing & DevOps programme for a specialised, high-demand outcome: DevSecOps.

The Relationship

Cloud & DevOps teaches students how to build and run infrastructure (the "Dev" and the "Ops"). Cybersecurity teaches students how attackers try to break into that infrastructure (the "Sec").

The Bridge

An institutional track bridging both courses introduces "Shift-Left" security methodologies directly into the CI/CD pipeline — security embedded from day one, not bolted on after launch.

Institutional differentiation: learners can integrate both skill sets — building an automated cloud pipeline and then subjecting it to a successful, documented penetration test — tapping directly into the deeply underserved and high-paying DevSecOps hiring market.

CAREER LANDSCAPE & PROJECTIONS

Where This Course Leads

Based on current 2026 market standards in India, the Cybersecurity (CEH v13) track prepares graduates for a distinct, lucrative career pathway.

DISCIPLINE	DAILY RESPONSIBILITIES	2026 SALARY RANGE (INDIA)
Cybersecurity (CEH v13)	Monitoring live network traffic, running vulnerability scans, simulating cyberattacks, drafting reports.	Entry: ₹4.5L–₹8L Mid: ₹12L–₹22L Lead: ₹25L–₹50L+

GROWTH PATH

Jr SOC Analyst → **Penetration Tester** → **Sr Security Engineer** → **CISO**

FACULTY & IMPLEMENTATION

Ready To Teach.
Ready To Deploy.

The programme is designed to launch with zero infrastructure overhead, backed by focused instructor preparation.

Faculty Preparation

Instructors undergo guided preparation focused on deep expertise in TCP/IP networking, Linux CLI operations, and basic Python/Bash scripting before delivering the course.

Institutional Lab Network

A centralised campus server hosts open-source, vulnerable-by-design instances — no per-student licensing and no exposure to unverified external tools.

Academic Partnerships

Verified free tiers such as TryHackMe are authorised for use, extending guided challenge practice at zero operational cost.

Zero Overhead Target

The full implementation plan is built around keeping operational overhead at zero — no paid lab licensing, no unverified downloads.

ASSESSMENT

How You're Evaluated

Assessment mirrors real security engineering work: continuous, practical, and reviewed against professional reporting standards.

Module Quizzes & Weekly Assessments

20%

Practical Lab Evaluations & Mini-Projects

40%

Final Capstone Penetration Test & Viva

40%

Eligibility

- ✓ Open to B.Tech, MCA students & graduates
- ✓ Working professionals & career switchers welcome
- ✓ Basic computer & networking knowledge (foundation module included)
- ✓ No prior cybersecurity experience required

Certification

- ✓ Empowers Academy Professional Certificate
- ✓ Documented vulnerability assessment portfolio
- ✓ Capstone penetration test report
- ✓ Mock interview & viva completion record

COURSE LAUNCH STRATEGY

Your Path Into The Cybersecurity Track

Delivery is built around flexibility — live online, offline classroom or hybrid, with weekend and weekday batch options for working learners.

Target Audience

B.Tech students, MCA students, fresh graduates, working professionals, and career switchers.

Prerequisites

Basic computer knowledge and basic networking concepts — no prior cybersecurity experience required (foundation module included).

Delivery Model

Live online, offline classroom, hybrid, and recorded sessions with weekend and weekday batch options.

Resources

Virtual lab environments, practice machines, cloud sandbox accounts, GitHub repository, and an LMS with recorded sessions and notes.

FREQUENTLY ASKED QUESTIONS

- **I've never worked in security. Can I really do this?** Yes — the foundation module covers networking and Linux fundamentals from zero before any offensive content begins.
- **Can I do this alongside a job or college?** Yes. Weekend and weekday batches are available, with recorded sessions for every live class.
- **Are the labs legal to practise on?** Yes — every exercise runs on a closed institutional lab network with vulnerable-by-design, open-source targets.

empowers Academy

Your Security Career Starts This Cohort.

Seats are limited per cohort. Apply now and start building a documented, professional-grade vulnerability assessment portfolio that proves what you can do.

Apply at empowersacademy.com →

WEBSITE	EMAIL	FORMAT
empowersacademy.com	admissions@empowersacademy.com	Online · Offline · Hybrid