PROFESSIONAL CYBERSECURITY CERTIFICATION OUTLINE

CEH v13 AI Certification

Certified Ethical Hacker with AI • EC-Council 312-50 Examination Blueprint

The world's premier ethical hacking certification, now revolutionized with artificial intelligence. Master AI-augmented penetration testing, automated exploit development, OSINT intelligence, deepfake threat mitigation, and defensive cybersecurity operations.

WHY ALL SAFE • Industry Achievements & Institutional Credibility

VERIFIED TRACK RECORD

PILLAR 01 • MARKET LEADERSHIP

1. Pakistan's Leading Cyber Security Platform

Pioneering offensive and defensive cybersecurity training, trusted by leading universities, corporate enterprises, and defense professionals nationwide for elite technical capacity building.

PILLAR 02 • GLOBAL IMPACT

2. Trained 2,000+ Students Internationally

Empowered a diverse global alumni network spanning 15+ countries, equipping learners with practical command-line muscle memory, live cyber range experience, and enterprise deployment skills.

PILLAR 03 • CAREER OUTCOMES

3. Global Success Stories

Alumni actively employed across multinational technology firms, telecom providers, Fortune 500 infrastructure teams, and Security Operations Centers (SOC) across the globe.

PILLAR 04 • NEXT-GEN INNOVATION

4. Partner of First Security AI Platform

Official partner integrating **Securiti AI Pro**—the pioneering AI-powered platform for automated threat intelligence, vulnerability correlation, and AI-driven cyber defense simulation.

20	220+	24/7	FREE
OFFICIAL CORE MODULES	HANDS-ON CYBER LABS	LIVE RED TEAM MENTORSHIP	SECURITI AI PRO™ ACCESS

Enrollment: +92 321 2077222 • allsafeus@gmail.com
www.allsafeinnovate.com

OFFENSIVE SECURITY & AI DEFENSE

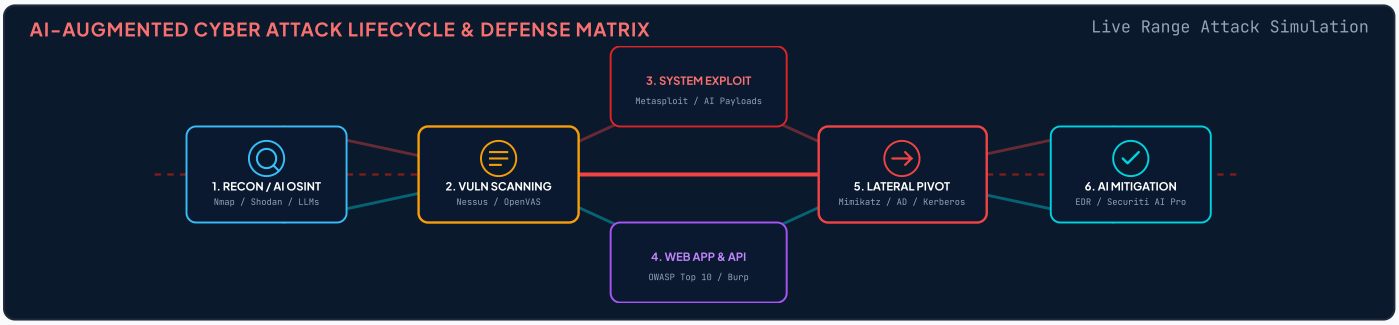
AI Cyber Attack Kill Chain & The ALL SAFE Advantage

Mastering modern penetration testing, automated offensive tradecraft, and proactive enterprise defense through hands-on cyber range labs.

What is CEH v13 AI & Why Does It Matter?

EC-Council Premier Benchmark

The **Certified Ethical Hacker v13 AI (CEH v13 AI)** represents the latest evolution of the world's most demanded cybersecurity credential. As threat actors weaponize Generative AI, automated exploit generators, and LLM-driven reconnaissance, security teams must master offensive AI capabilities to anticipate, detect, and neutralize complex cyber attacks. CEH v13 AI provides rigorous, hands-on validation across network scanning, vulnerability discovery, system exploitation, web application security, cloud environments, and AI-assisted defense.



The 6 ALL SAFE Institutional Advantages

WHY CHOOSE ALL SAFE?

1. Live Practical Sessions

Live instructor-led offensive exercises in isolated cyber ranges. Attack real vulnerable machines, analyze payloads, and practice realistic enterprise red team scenarios.

2. 24/7 Mentorship Support

Around-the-clock technical guidance to help you debug exploits, understand complex vulnerabilities, and master advanced hands-on lab environments.

3. Free International Certs

Free international certification opportunities through eligible ALL SAFE programs. **Eligibility and applicable program criteria must be confirmed.*

4. International Experts Community

Connect with a worldwide network of ethical hackers, red teamers, penetration testers, and cyber defenders across multinational corporations.

5. Securiti AI Pro — Free

Complimentary access to Securiti AI Pro, ALL SAFE's flagship AI security platform. Practice AI-driven attack mapping, threat detection, and automated audit flows.

6. Career-Oriented Learning

Equip yourself with practical offensive skills directly mapped to high-demand roles: Penetration Tester, Security Analyst, SOC Tier 2/3, and Red Team Operator.

EC-COUNCIL OFFICIAL BLUEPRINT

EC-Council CEH v13 AI Official 20-Module Outline

Comprehensive coverage across all 20 official domains infused with cutting-edge AI offensive tradecraft and enterprise cyber range labs.

01. Intro to Ethical Hacking & AI
Core Foundation

Cyber threat landscapes, hacker classes, CIA triad, ethical hacking legalities, and AI-assisted offensive/defensive operations.

02. Footprinting & Reconnaissance
AI-OSINT

Search engine OSINT, DNS footprinting, automated WHOIS, social networking recon, and AI intelligence synthesis.

03. Scanning Networks
Discovery

TCP/UDP port scanning, Nmap scripting (NSE), AI banner grabbing, IDS evasion during scans, and vulnerability detection.

04. Enumeration
Deep Audit

Active Directory, NetBIOS, SNMP, LDAP, SMB, and RPC enumeration; automated extraction of user accounts and shares.

05. Vulnerability Analysis
Assessment

Nessus/OpenVAS vulnerability scanning, CVSS scoring, false-positive elimination, and AI-driven patch correlation.

06. System Hacking
Privilege Esc

Password cracking (Hashcat/John), privilege escalation (Windows/Linux), Metasploit, keyloggers, and hiding files (steganography).

07. Malware Threats & AI Synthesis
Malware

Trojans, worms, ransomware, polymorphic malware, AI-synthesized payloads, reverse engineering, and dynamic sandbox analysis.

08. Sniffing & MITM Attacks
Packet Capture

MAC flooding, ARP poisoning, DHCP starvation, DNS spoofing, Wireshark deep packet analysis, and SSL stripping.

09. Social Engineering & Deepfakes
Human Vector

AI-generated spear phishing, voice cloning, video deepfakes, credential harvesting, and enterprise security awareness defense.

10. Denial-of-Service (DoS/DDoS)
Availability

SYN floods, UDP amplification, botnet architectures, Layer 7 HTTP floods, and AI-powered volumetric traffic mitigation.

11. Session Hijacking
Traffic Hijack

TCP/UDP session hijacking, cookie tampering, cross-site scripting session fixation, and encrypted session protection.

12. Evading IDS, Firewalls & Honeypots
Evasion

Packet fragmentation, HTTP/TLS tunneling, proxy chains, AI-driven shellcode obfuscation, and honeypot detection.

13. Hacking Web Servers
Web Infra

Apache, Nginx, and IIS architecture attacks; web server misconfigurations, directory traversal, and patch management auditing.

14. Hacking Web Applications
OWASP Top 10

OWASP Top 10 vulnerabilities, XSS, CSRF, IDOR, SSRF, API endpoint security testing, and Burp Suite Pro workflows.

15. SQL Injection (SQLi)
Database

In-band, blind, time-based, and out-of-band SQLi; automated database exfiltration with SQLmap, and parameterized defenses.

16. Hacking Wireless Networks
Wi-Fi & RF

WPA/WPA2/WPA3 4-way handshake capture, PMKID attacks, evil twin rogue APs, bluetooth exploitation, and RF spectrum defense.

17. Hacking Mobile Platforms
Android/iOS

Android APK decompilation, rooting/jailbreaking risks, reverse engineering, mobile malware analysis, and MDM auditing.

18. IoT & OT Hacking
Hardware/SCADA

IoT architecture vulnerabilities, firmware extraction, UART/JTAG hardware debuggers, SCADA/ICS protocols (Modbus), and mitigations.

19. Cloud Computing Security
Cloud Defense

AWS/Azure/GCP identity misconfigurations, S3 bucket enumeration, serverless exploitation, container escape, and cloud auditing.

20. Cryptography & AI Cyber Defense
Encryption

Symmetric/asymmetric ciphers, PKI, digital signatures, cryptanalysis attacks, and post-quantum cryptographic resilience.

CAREER TRANSFORMATION

CEH v13 AI Career Scope, Student Roadmap & Admissions

How certified ethical hacking and AI defense mastery unlock high-demand enterprise security careers, cohort logistics, and enrollment.

CEH v13 AI Career Scope & Target Enterprise Roles — Cybersecurity Industry Matrix

ENTERPRISE CYBER ROLE	CORE OPERATIONAL RESPONSIBILITIES	CAREER TRAJECTORY
Ethical Hacker / Pen Tester	Conduct authorized vulnerability assessments, execute controlled penetration tests on network/web apps, and deliver mitigation reports.	Lead Pen Tester / Consultant
Cybersecurity Analyst (SOC)	Investigate security alerts, detect intrusion attempts, analyze adversary behavior via MITRE ATT&CK, and coordinate incident response.	SOC Lead / Threat Hunter
Information Security Consultant	Audit enterprise security posture, review cloud/on-prem configurations, assess regulatory compliance (ISO 27001/NIST), and advise CISO.	Principal Security Architect
Red Team Operator	Simulate real-world advanced persistent threat (APT) attacks, test EDR/defense evasion, build C2 infrastructure, and train blue teams.	Red Team Director / Lead
Vulnerability Researcher	Identify zero-day vulnerabilities, audit application source code, write proof-of-concept exploits, and participate in enterprise bug bounties.	Exploit Dev / SecOps Lead
Cloud Security Specialist	Harden AWS/Azure environments, audit IAM permissions, secure CI/CD pipelines, and mitigate cloud misconfigurations and container escapes.	DevSecOps / Cloud Architect

The 7-Step Student Cyber Learning Journey

1	2	3	4	5	6	7
Enrollment	**AI Tools**	**Reconnaissance**	**Exploitation**	**Red Team**	**Exam Prep**	**EC-Council Exam**
Range Setup	Linux & AI Script	OSINT & Scanning	System & Web Labs	EDR Evasion & AD	Timed 312-50 Mocks	CEH v13 AI Cert

Course Duration:	12 Weeks (80+ Hours Live + Cyber Range)	**Training Mode:**	Live Interactive Online + 24/7 Range Access
Class Schedule:	Weekend & Weekday Evening Batches	**Trainer Credentials:**	Senior Red Team Leads (CEH Master / OSCP / CISSP)
Starting Date:	Upcoming Cohort (Contact Admissions)	**Course Fee:**	Inquire for Cohort Packages & Discounts

START BUILDING YOUR CYBERSECURITY CAREER WITH ALL SAFE

Take the next step toward developing professional ethical hacking and AI defense skills through practical training, expert mentorship, and a supportive technical learning community.

DIRECT EMAIL
allsafeus@gmail.com

ENROLLMENT CONTACT
+92 321 2077222

OFFICIAL WEBSITE
www.allsafeinnovate.com

Contact ALL SAFE Today to Enroll in the CEH v13 AI Training Program.