CyberHunt

CERTIFIED ETHICAL HACKER (CEH v13)

CEH v13 Certification Program

Master ethical hacking methodologies, vulnerability assessment, system exploitation, web attacks, and wireless security.
Built by practitioners. Proven by results.

- 100% Practical Training
- CEH-Aligned Curriculum
- Ethical Hacking Methodology
- Real-World Attack Simulation

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

— ABOUT COURSE

Certified Ethical Hacker (CEH v13)

The **CEH v13** Certification Program is a comprehensive, hands-on ethical hacking and vulnerability assessment training designed to build strong foundational and intermediate-level offensive security skills. Every module focuses on practical application of ethical hacking methodologies aligned with CEH standards.

This program prepares candidates for the **CEH v13** certification while building practical penetration testing expertise required in enterprise environments. You will work through real machines, perform vulnerability assessments, exploit systems, and document your findings in a professional security report — all before certification day.

With a curriculum spanning reconnaissance, vulnerability assessment, web exploitation, wireless security, and cloud/IoT threats, this is the most comprehensive **CEH** prep available — covering all domains that EC-Council tests.

CyberHunt

COURSE OBJECTIVES

Course Objectives

- Ethical hacking fundamentals, cyber kill chain concepts, and an overview of information security and security measures with AI-enhanced threat detection and response.
- Concepts, methodologies, and tools of footprinting using AI for automated information gathering and reconnaissance.
- Concepts of vulnerability assessment, its categories and strategies, and AI-driven exposure to technologies used in the industry.
- Social engineering concepts and terminologies, including identity theft, impersonation, insider threats, social engineering techniques, and AI-based countermeasures.
- Operational Technology (OT) essentials, threats, attack methodologies, and AI-powered attack prevention.
- Recognizing vulnerabilities in IoT and ensuring the safety of IoT devices using AI-based security solutions.
- Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, cryptanalysis, and enhanced cryptographic defense.
- Cloud computing, threats and security, AI-driven container technology, and serverless computing security measures.

CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.

CyberHunt

01 Ethical Hacking Foundations

- Information Security Concepts
- CIA Triad
- Cyber Kill Chain
- Attack Models & Threat Landscape
- Ethical Hacking Methodology
- Penetration Testing Phases
- Vulnerability Assessment Basics
- Footprinting & Reconnaissance
- Scanning & Enumeration
- Social Engineering Awareness
- Legal & Compliance Framework
- Security Policies & Governance
- Ethics in Penetration Testing
- Professional Responsibilities
- Risk Management Fundamentals
- Introduction to AI in Cybersecurity

Practical: Understanding ethical boundaries, reconnaissance basics & security assessment workflow.

CyberHunt

02 Reconnaissance & Scanning

Overview

This module covers the essential techniques used to gather information about target systems and networks. You will learn how to collect, analyze, and identify crucial details that help in mapping the attack surface and planning further assessment activities.

Key Topics

OSINT & Footprinting Techniques	Learn to collect publicly available information about to organizations, domains, IPs, employees, and technologies using OSINT resources and footprinting methodologies.
Passive Information Gathering	Understand how to gather information without directly interacting with the target, using search engines, DNS records, WHOIS, social media, and other public sources.
Network Scanning with Nmap	Explore Nmap for discovering live hosts, open ports, running services, OS detection, and network mapping.
Enumeration Techniques	Learn various enumeration methods to extract detailed information about users, shares, services, and system resources.
Service Version Detection	Identify service versions and banners to understand software in use and potential associated vulnerabilities.
Vulnerability Scanning Fundamentals	Understand the basics of vulnerability scanning, its importance, and how scanners identify security weaknesses.

Practical:

Complete reconnaissance and enumeration of target networks using OSINT tools, Nmap, and basic scanning techniques to identify live hosts, open ports, and running services.

CyberHunt

03 Vulnerability Assessment

Overview

This module focuses on identifying, analyzing, and evaluating security weaknesses in systems and applications. You will learn how to assess vulnerabilities, determine their impact, and provide actionable recommendations to improve overall security posture.

Key Topics

Vulnerability Scanners (Nessus, OpenVAS)	Use industry-leading scanners to identify vulnerabilities in systems, networks, and applications.
CVE Analysis & Severity Rating	Analyze CVEs and understand CVSS scoring to evaluate the severity and potential impact of vulnerabilities.
Risk Assessment & Prioritization	Assess risks based on likelihood and impact to prioritize vulnerabilities for effective remediation.
False Positive Management	Identify and validate false positives to reduce noise and focus on real security issues.
Reporting Vulnerabilities	Document findings clearly with evidence, impact analysis, and risk ratings for stakeholders.
Remediation Recommendations	Provide practical and effective solutions to fix identified vulnerabilities and strengthen security.

Practical:

Perform complete vulnerability assessment on lab systems using industry tools, analyze results, and generate a professional vulnerability report with remediation recommendations.

CyberHunt

04 System Exploitation

Overview

This module focuses on exploiting vulnerabilities to gain unauthorized access to systems and escalate privileges. You will learn techniques used by attackers to take control of systems, maintain persistence, and cover tracks.

Key Topics

• **Password Attacks & Cracking**	Explore various password attack methods and cracking techniques to compromise user credentials.
• **Privilege Escalation Techniques**	Learn methods to gain higher privileges on a system and bypass security restrictions.
• **Maintaining Access & Persistence**	Understand techniques to maintain long-term access and ensure persistence on compromised systems.
• **Covering Tracks & Log Manipulation**	Learn how attackers hide their activities by clearing logs and manipulating system records.
• **Creating Backdoors & Remote Access**	Explore backdoor creation and remote access techniques to control systems covertly.

Practical:

Exploit vulnerabilities and escalate privileges on lab machines using industry-standard tools and techniques.

CyberHunt

05 Web Application Attacks

OWASP Top 10 Vulnerabilities	Understand the OWASP Top 10 risks and how they impact web applications.
SQL Injection & XSS Exploitation	Learn to identify and exploit SQL Injection and Cross-Site Scripting vulnerabilities.
File Upload Vulnerabilities	Discover file upload flaws and bypass restrictions to achieve arbitrary file execution.
Authentication Bypass Techniques	Explore methods to bypass authentication mechanisms and access restricted functionalities.
Session Hijacking & CSRF	Learn to hijack user sessions and exploit CSRF vulnerabilities.
Web Shell Deployment	Deploy web shells and understand post-exploitation techniques on web servers.

Practical: Exploit web applications & achieve full compromise.

CyberHunt

06 Wireless Network Security

Overview

This module focuses on securing wireless networks and exploiting common vulnerabilities in WiFi environments. You will learn wireless protocols, attacks, and defensive techniques to protect wireless infrastructure.

Key Topics

WiFi Protocols & Security (WEP, WPA, WPA2)	Understand WiFi standards and security protocols, their strengths, and vulnerabilities.
Wireless Reconnaissance	Discover wireless networks and gather information using active and passive reconnaissance techniques.
Password Cracking (Hashcat, Aircrack)	Learn to capture handshakes and crack WiFi passwords using tools like Hashcat and Aircrack-ng.
Rogue Access Points	Understand how rogue APs are created and used to steal credentials and intercept traffic.
Man-in-the-Middle Attacks	Perform traffic interception, ARP spoofing, and session hijacking in wireless networks.
Wireless Pentesting Lab	Hands-on lab exercises to perform real-world wireless penetration testing and network compromise.

Practical:

WiFi hacking & wireless network compromise in a controlled lab environment.

CyberHunt

07 Cloud & IoT Security

Overview

This module covers security challenges in cloud and IoT environments. You will learn to identify misconfigurations, assess risks, and secure cloud infrastructures, containers, APIs, and IoT devices.

Key Topics

Cloud Architecture Threats	Understand threats targeting cloud architectures, shared responsibility model, and attack surfaces.
AWS & Azure Misconfigurations	Identify and exploit common misconfigurations in AWS and Azure cloud services.
Container Security	Learn container technologies, image vulnerabilities, and container escape techniques.
IoT Device Vulnerabilities	Explore firmware analysis, insecure protocols, and hardware vulnerabilities in IoT devices.
Cloud Penetration Testing	Perform cloud penetration testing and privilege escalation in cloud environments.
API Security Testing	Test APIs for common vulnerabilities like broken auth, injection, and excessive data exposure.

Practical:

Cloud environment assessment & IoT device exploitation.

CyberHunt

08 Cryptography & Hashing

Overview

This module covers the fundamentals of cryptography and hashing. You will learn encryption algorithms, hashing techniques, and how they are used to protect data, ensure integrity, and secure communications.

Key Topics

Encryption Algorithms (AES, RSA)	Understand symmetric (AES) and asymmetric (RSA) encryption algorithms and their real-world applications.
Hash Functions & Salting	Learn how hash functions work and how salting improves security against rainbow table attacks.
Digital Signatures & Certificates	Explore digital signatures, certificate authorities (CA), and the role of certificates in securing communications.
PKI Infrastructure	Understand Public Key Infrastructure (PKI), its components, and how it enables secure environments.
Hash Cracking Techniques	Learn common hash cracking methods and tools used to recover plaintext from hashed data.
Man-in-the-Middle on Encrypted Traffic	Understand how MITM attacks work on encrypted traffic and techniques to detect and prevent them.

Practical:

Cryptographic attack & hash cracking labs.

CyberHunt

09 Social Engineering & Physical Security

Overview

This module focuses on human-centric attacks and physical security techniques. You will learn how attackers manipulate people and exploit physical weaknesses, and how to defend against these threats effectively.

Key Topics

Social Engineering Tactics	Explore common social engineering tactics used by attackers to manipulate and deceive individuals.
Phishing & Pretexting Techniques	Learn phishing and pretexting attack methods and how to identify and avoid falling victim to them.
Physical Security Bypass	Understand techniques attackers use to bypass physical security controls and gain unauthorized access.
Tailgating & Badge Cloning	Learn about tailgating, badge cloning, and other techniques used to exploit access control systems.
OSINT for Social Engineering	Use Open Source Intelligence (OSINT) to gather information and enhance social engineering attacks.

Practical:

Social engineering attack simulations & physical security assessment.

CyberHunt

10 Report Writing & Exam Strategy

Overview

This module covers the essential skills and strategies required to excel in CEH exams and professional reporting. You will learn how to structure reports, write executive summaries, assess risks, follow CEH exam formats, and manage your time effectively during the exam.

Key Topics

Professional Pentest Report Structure	Learn how to create well-structured penetration testing reports that are clear, concise, and impactful.
Executive Summary Writing	Write effective executive summaries that highlight key findings, risks, and recommendations.
Risk Rating & Remediation	Understand how to rate risks based on severity and provide actionable remediation recommendations.
CEH Exam Format & Strategy	Familiarize yourself with the CEH exam format and develop strategies to approach questions effectively.
Time Management During Exam	Learn time management techniques to maximize your performance and complete the exam successfully.

Practical:

Write professional CEH-style VAPT report.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!

For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on