Certified Ethical Hacker (CEH)

EC-Council

CEH
Certified Ethical Hacker

Version 1.0

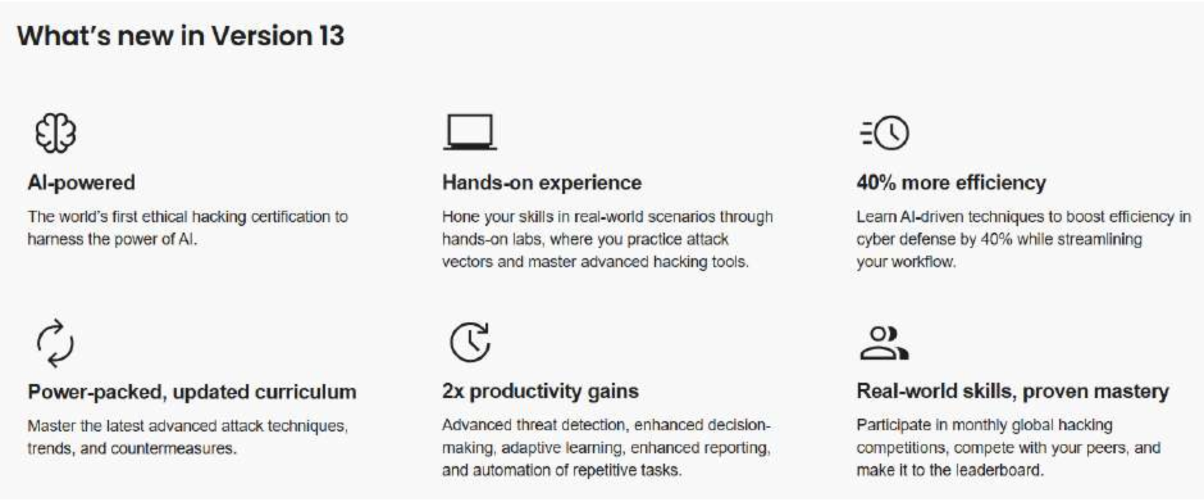
CEH v13 Overview

- Who Is Eligible for This Course?
  - Freshers looking for basic cybersecurity knowledge
  - Working IT professionals looking for basic cybersecurity certification

- Course Duration
  - 1.25 Months (48 Hours)

- Course Syllabus
  - Introduction to Ethical Hacking
  - Footprinting and Reconnaissance
  - Scanning Networks
  - Enumeration
  - Vulnerability Analysis
  - System Hacking
  - Malware Threats
  - Sniffing
  - Social Engineering
  - Denial-of-Service
  - Session Hijacking
  - Evading IDS, Firewalls, and Honeypots
  - Hacking Web Servers
  - Hacking Web Applications
  - SQL Injection
  - Hacking Wireless Networks
  - Hacking Mobile Platforms
  - IoT Hacking
  - Cloud Computing
  - Cryptography

- Why Training @CyberSPAIS?
  - Job Oriented Industry Relevant Curriculum
  - Based On Latest Cyber Security Topics & Trends
  - 100% Assistance for Placements & Internships
  - Industry Experienced & Certified Trainer
  - Concepts Explained with Industry Scenarios
  - Comprehensive Hands-on Sessions & Labs
  - Regular Module Wise Assessments & Evaluations
  - Cybersecurity Projects & Internships
  - Thorough Preparation – Job Interview & Soft Skills
  - Arrangement To Write Certification Exams
  - Among The Top Cybersecurity Institutes in Kerala



What's new in Version 13

AI-powered

The world's first ethical hacking certification to harness the power of AI.

Hands-on experience

Hone your skills in real-world scenarios through hands-on labs, where you practice attack vectors and master advanced hacking tools.

40% more efficiency

Learn AI-driven techniques to boost efficiency in cyber defense by 40% while streamlining your workflow.

Power-packed, updated curriculum

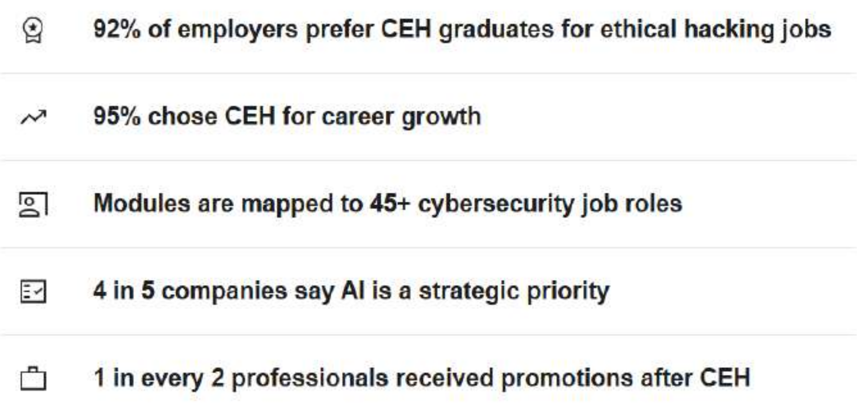
Master the latest advanced attack techniques, trends, and countermeasures.

2x productivity gains

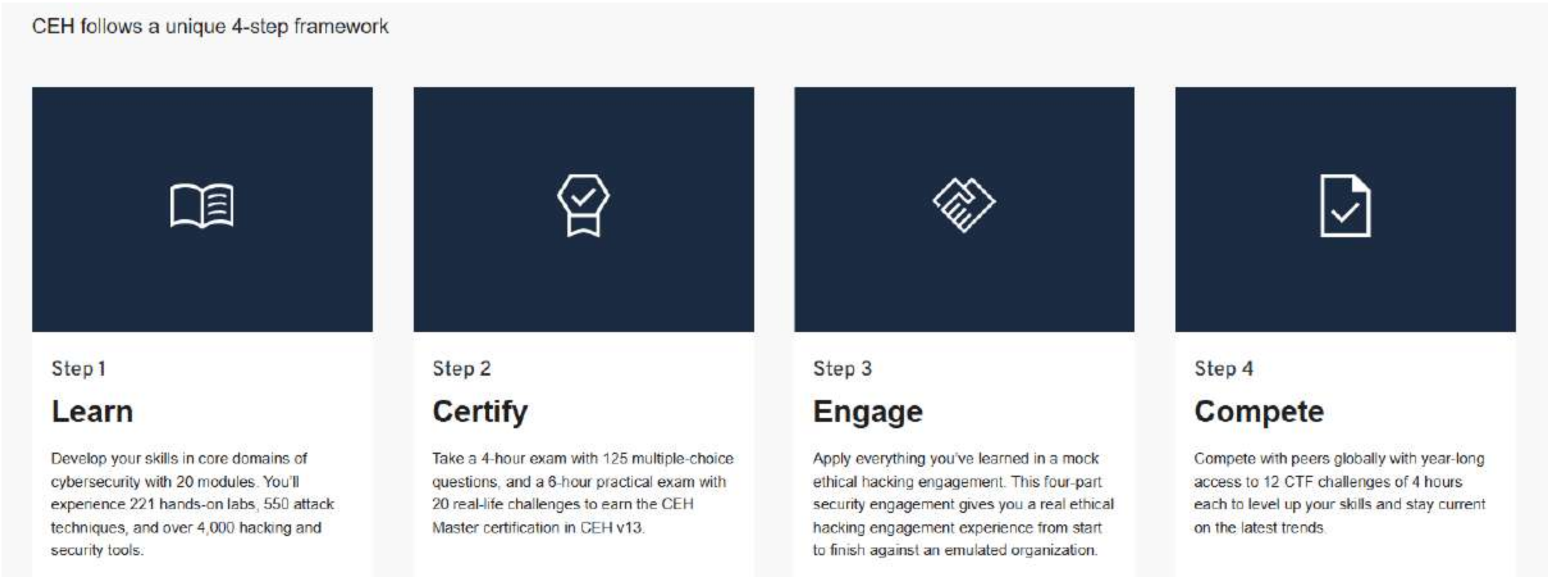
Advanced threat detection, enhanced decision-making, adaptive learning, enhanced reporting, and automation of repetitive tasks.

Real-world skills, proven mastery

Participate in monthly global hacking competitions, compete with your peers, and make it to the leaderboard.



- **92% of employers prefer CEH graduates for ethical hacking jobs**
- **95% chose CEH for career growth**
- **Modules are mapped to 45+ cybersecurity job roles**
- **4 in 5 companies say AI is a strategic priority**
- **1 in every 2 professionals received promotions after CEH**



CEH follows a unique 4-step framework

Step 1

Learn

Develop your skills in core domains of cybersecurity with 20 modules. You'll experience 221 hands-on labs, 550 attack techniques, and over 4,000 hacking and security tools.

Step 2

Certify

Take a 4-hour exam with 125 multiple-choice questions, and a 6-hour practical exam with 20 real-life challenges to earn the CEH Master certification in CEH v13.

Step 3

Engage

Apply everything you've learned in a mock ethical hacking engagement. This four-part security engagement gives you a real ethical hacking engagement experience from start to finish against an emulated organization.

Step 4

Compete

Compete with peers globally with year-long access to 12 CTF challenges of 4 hours each to level up your skills and stay current on the latest trends.

CEH v13 – Syllabus

Module 1: Introduction to Ethical Hacking

- Information Security
- Attack Classification
- Hacker Classes
- Ethical Hacking
- ChatGPT Powered Tools
- Ethical Hacking Framework
- Cyber Kill Chain
- MITRE ATT&CK Framework
- Information Assurance
- Risk Management
- Threat Intelligence
- Incident Management
- PCI DSS, HIPAA, SOX, GDPR, DPA

Module 2: Footprinting & Reconnaissance

- Reconnaissance
- Google Hacking
- People Search Services
- Dark Web Footprinting
- Intelligence Gathering
- Social Networking Sites
- Whois Lookup
- DNS Footprinting
- DNS Analysis
- Traceroute
- Email Footprinting
- Social Engineering
- OSINT
- AI Tools

Module 3: Scanning Networks

- Network Scanning
- Scanning Tools
- Host Discovery Techniques
- Port Scanning Techniques
- Service Version Discovery
- OS Discovery & Banner Grabbing
- Scanning Beyond IDS & Firewall
- AI Tools

Module 4: Enumeration

- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- NFS Enumeration
- SMTP Enumeration
- DNS Cache Snooping
- DNNSec Zone Walking
- IPsec Enumeration
- VoIP Enumeration
- RPC Enumeration
- SMB Enumeration

Module 5: Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Scoring Systems and Databases
- Vulnerability-Management Life Cycle
- Vulnerability Research
- Vulnerability Scanning and Analysis
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

Module 6: System Hacking

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

Module 7: Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Viruses and Worms
- Fileless Malware Concepts
- AI-based Malware Concepts
- Malware Countermeasures
- Anti-Malware Software

- Module 8: Sniffing
  - Sniffing Concepts
  - Sniffing Technique
  - Sniffing Tools
  - Sniffing Countermeasures
- Module 9: Social Engineering
  - Social Engineering Concepts
  - Human-based Social Engineering Techniques
  - Computer-based Social Engineering Techniques
  - Mobile-based Social Engineering Techniques
  - Social Engineering Countermeasures
- Module 10: Denial-of-Service
  - DoS/DDoS Concepts
  - Botnets
  - DDoS Case Study
  - DoS/DDoS Attack Techniques
  - DoS/DDoS Attack Countermeasures
- Module 11: Session Hijacking
  - Session Hijacking Concepts
  - Application-Level Session Hijacking
  - Network-Level Session Hijacking
  - Session Hijacking Tools
  - Session Hijacking Countermeasures
- Module 12: Evading IDS, Firewalls, and Honeypots
  - Intrusion Detection/Prevention System (IDS/IPS) Concepts
  - Firewall Concepts
  - IDS, IPS, and Firewall Solutions
  - Evading IDS/Firewalls
  - Evading NAC and Endpoint Security
  - IDS/Firewall Evading Tools
  - Honeypot Concepts
  - IDS/Firewall Evasion Countermeasures
- Module 13: Hacking Web Servers
  - Web Server Concepts

- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Countermeasures
- Patch Management

Module 14: Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API and Webhooks
- Web Application Security

Module 15: SQL Injections

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- Evasion Techniques
- SQL Injection Countermeasures

Module 16: Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Attack Countermeasures

Module 17: Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines
- Mobile Security Tools

Module 18: IoT Hacking & OT Hacking

- IoT Hacking
- IoT Concepts and Attacks
- IoT Hacking Methodology
- OT Hacking

- Module 19: Cloud Computing
  - Cloud Computing Concepts
  - Container Technology
  - Serverless Computing
  - Cloud Hacking
  - Cloud Hacking Methodology
  - AWS Hacking
  - Microsoft Azure Hacking
  - Google Cloud Hacking
  - Container Hacking
  - Cloud Security

- Module 20: Cryptography
  - Cryptography Concepts and Encryption Algorithms
  - Applications of Cryptography
  - Cryptanalysis
  - Cryptography Attack Countermeasures

C|EH v13

BECOME A CERTIFIED ETHICAL HACKER

Powered by AI Capabilities

LEARN | CERTIFY | ENGAGE | COMPETE

EC-Council C|EH v13

Certified Ethical Hacker

Build Your Career with the Most In-Demand Ethical Hacking Certification

Ranked 1st in Ethical Hacking Certifications by ZDNet

Ranked in the List of Top 10 Cybersecurity Certifications

Ranked 4th Among the Top 50 Leading Cybersecurity Certifications

01 The World's #1 Ethical Hacking Certification for 20+ years

01 EC-Council Introduces the Industry's First AI Cybersecurity Courses

12 CEH Ranks 12th among the Top 75 Highest-Paying IT Certifications in the US and Globally

97% Stated That the Skills They Acquired in CEH Helped Safeguard Their Organizations

95% Chose CEH for Career Growth

92% of Hiring Managers Prefer Candidates with the CEH for Jobs That Require Ethical Hacking Skills

45+ Cybersecurity Job Roles Are Mapped to the CEH Certification in 2024, Compared to 20+ Roles in 2022

1 in every 2 Professionals Received Promotions After Completing the CEH

CEH is the only Globally In-Demand Ethical Hacking Certification that covers Core Domains of Cybersecurity and has Global Recognition and Accreditations while offering a Higher Employability Rate

Future Proof Your Cybersecurity Career with AI

The Demand for Cybersecurity Professionals with AI Skills is on the Rise

AI Skills No Longer Optional; They Are Essential

42% of large enterprises actively use AI, and 59% of early adopters plan to increase investment and accelerate AI integration (IBM, 2024)

40% surge in demand for specialists in Artificial Intelligence and Machine Learning (World Economic Forum, 2023)

96% of security leaders deem AI solutions essential for countering AI-powered threats due to their speed and effectiveness (Darktrace, 2024)

87% of business leaders expect at least a quarter of their workforce will need to upskill in AI (IBM, 2024)

AI in Cybersecurity

Threats

83% note tangible alterations in attack methodologies amidst the AI revolution (EC-Council, 2024)

66% admit Being Unprepared for AI Cyber Onslaughts (EC-Council, 2024)

Countermeasures

Up to **90%** of fraud costs can be reduced by AI models in specific scenarios where behavioral data analysis is effectively applied (IBM, 2024)

AI and automation slashed breach impact by 30%, saving businesses USD 850,000 and reducing breach lifecycles by 108 days (IBM, 2023)

*McAfee Report. ˜Darktance. †Forbes. ±Projected by Future of Jobs Report 2023.
ˆ2023 Emerging Jobs Report, LinkedIn.

Gain Cybersecurity Mastery for Real-world Success with Certified Ethical Hacker v13

Why Should You Join the AI Revolution with the Certified Ethical Hacker Program?

By joining the AI Revolution as a Certified Ethical Hacker, you'll gain the expertise to navigate the cutting-edge world of cybersecurity.

Certified Ethical Hackers, trained in the latest version of CEH v13, are equipped with AI-powered tools and techniques to identify, exploit, and secure vulnerabilities in systems and networks. You'll learn to leverage AI for automating threat detection, predicting security breaches, and responding swiftly to cyber incidents. Moreover, you'll also gain the skills needed to secure AI-driven technologies against potential threats. This combination of ethical hacking and AI capabilities will place you at the forefront of cybersecurity, ready to defend organizations across industries from advanced threats and adapt to evolving challenges.

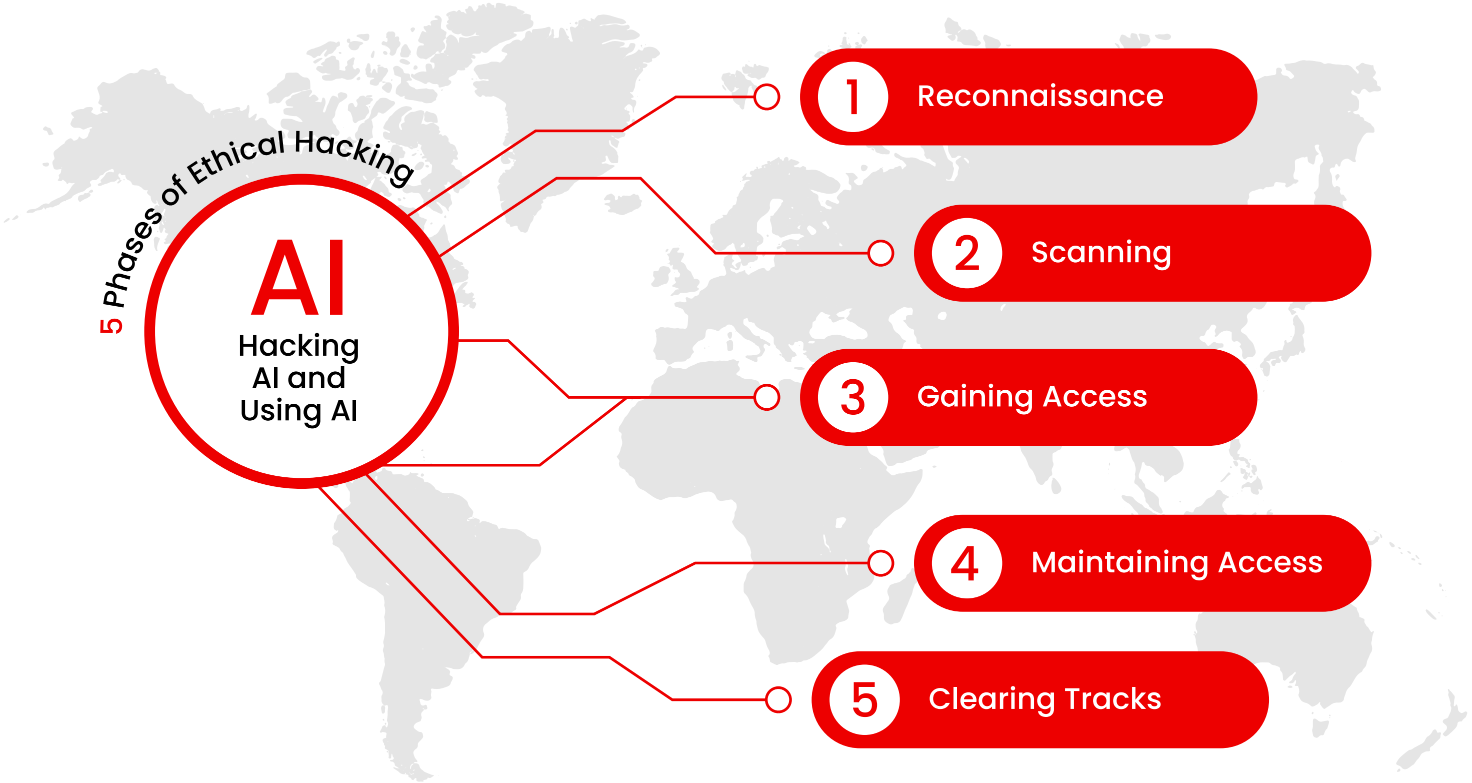
Amplify Your Edge as a Certified Ethical Hacker Powered by AI Capabilities:
Advanced Knowledge: As a Certified Ethical Hacker powered by AI, you'll possess in-depth knowledge of ethical hacking methodologies, enhanced with cutting-edge AI techniques.
AI Integration: You'll effectively integrate AI across every phase of ethical hacking, from reconnaissance and scanning to gaining access, maintaining access, and covering your tracks.
Automation and Efficiency: You'll leverage AI to automate tasks, boost efficiency, and detect sophisticated threats that traditional methods might overlook.
Proactive Defense: With AI at your disposal, you'll be equipped for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks before they happen.

How CEH v13 Powered by AI Redefines Your Cybersecurity Career

- Experience the world's first ethical hacking program powered by AI
- Master the five phases of ethical hacking integrated with AI
- Achieve 40% efficiency and double your productivity with AI-driven skills
- Learn how to hack AI systems
- Become an AI expert with hands-on labs for practicing AI skills
- Master the latest advanced attack techniques, trends, and countermeasures
- Gain practical experience with 221 labs, attack vectors, and hacking tools
- Experience with over 550 attack techniques
- Explore 4,000+ commercial-grade hacking and security tools
- Follow a unique four-phase learning framework: Learn, Certify, Engage, Compete
- Practice hacking a real organization in a live cyber range
- Validate your skills in a 6-hour practical exam or 4-hour knowledge-based exam
- Compete with hackers in global CTF competitions on the latest issues
- Earn the globally recognized No.1 Ethical Hacking Certification
- Gain a certification that is approved and accredited by U.S. DoD 8140, ANAB 17024, and NCSC
- Meet the rigorous standards of NICE 2.0 and the NIST Framework
- Get the opportunity to be employed by top organizations including Fortune 500 companies, government, and private sector firms

What's New in The CEH v13

The CEH v13 not only provides extensive hands-on coverage but also integrates AI into all five phases of ethical hacking:



Get CEH Trained from Anywhere with our World-Class Instructors

1. Live-Online
2. Self-Paced Video Lectures
3. In-Person training
4. Masterclass

Master AI to Automate Ethical Hacking Tasks, to hack and defend against AI systems,

and boost your task efficiency by 40% in your job role.

Develop a Hacker's Mindset: Master the 5 Phases of Ethical Hacking and Gain AI Skills to Automate Them

1. Reconnaissance

| Learn to gather essential information about your target

2. Vulnerability Scanning

| Gain the ability to identify weaknesses in the target system

3. Gaining Access

| Learn how to actively exploit identified vulnerabilities

4. Maintaining Access

| Develop skills to maintain continued access to the target systems

5. Clearing Tracks

| Master the art of erasing any trace of your activities

Learn AI Tools:

- ShellGPT
- ChatGPT
- FraudGPT
- WormGPT
- DeepExploit
- Nebula
- Veed.io

And many more!

Learn to Hack AI Systems Based on OWASP's Top 10 AI Attack Vulnerabilities and Threats

In CEH v13, you will not only master AI-driven cybersecurity but also learn to hack AI systems. This comprehensive training equips you with cutting-edge AI-driven skills, enhancing your ability to execute cybersecurity tasks with up to 40% greater efficiency, while significantly boosting your productivity.

- Prompt Injection
- Insecure Output Handling
- Training Data Poisoning
- Model Denial of Service
- Supply Chain Vulnerabilities
- Sensitive Information Disclosure
- Insecure Plugin Design
- Excessive Agency
- Overreliance
- Model Theft

CEH v13 Gain Skills to Battle AI Against AI Your Ultimate Training Ground for Mastering AI-driven Cybersecurity Skills

CEH v13 equips professionals with advanced skills to enhance their hacking techniques and leverage AI. Gain the expertise to:

- Drive 40% efficiency in cybersecurity tasks
- Double your productivity with AI-driven methods
- Master the application of AI in cybersecurity
- Learn to hack AI systems
- Explore multiple AI and GPT tools
- Automate repetitive tasks
- Detect advanced threats
- Make informed decisions using AI-enhanced analysis
- Adapt to evolving threats through AI-driven learning
- Improve reporting with AI-powered insights

CEH v13: The World's First Ethical Hacking Certification with a 4-Phase AI-Powered Learning Framework

The CEH v13 is a specialized, one-of-a-kind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry.

This learning framework offers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.

Master Ethical Hacking and AI Skills That Go Beyond Certification

Learn

Courseware
Cyber Range
Gain Skills

1

Certify

Knowledge-Based
Practical Exam
Gain Recognition

2

Engage

Live Cyber Range
Gain Experience

3

Compete

Global Ethical
Hacking Competition
Gain Respect

4

Beat Hackers in their Own Game with CEH v13! A Revolutionary Way to Learn Ethical Hacking

1. Learn

20 modules

2500+ pages of student manual

2000 pages of lab manual

Over 221 hands-on labs to practice attack vectors and hacking tools

AI integrated skills in the 5 phases of the ethical hacking framework

Hacking AI system, based on the Top 10 OWASP vulnerabilities

Over 4000 hacking and security tools

Learn how to hack multiple operating systems (Windows 11, Windows servers, Linux, Ubuntu, Android)

More than 50% of training time is dedicated to labs

2. Certify

Knowledge-Based Exam
(ANAB ISO 17024 and US DoD 8140)

4 hours

125 multiple-choice questions

Practical Exam
(ANAB ISO 17024 and US DoD 8140)

6 hours

20 real scenario based questions

3. Engage

4000 hacking tools

550 attack techniques

Conduct a real-world ethical hacking assignment

Apply the 5 phases

1. Reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access
5. Covering your tracks

4. Compete

New challenges every month

4-hour CTF competition

Compete with your peers worldwide

Hack your way to the top of the leaderboard

Focus on new attack vectors

Exploit emerging vulnerabilities

Challenges include:

- Ransomware
- Web app hardening
- Unpatched software
- System hacking
- Service exploitation
- Incident response
- Forensic analysis
- Web app hacking and pen testing
- Reverse engineering
- Cryptography
- Encryption
- Hacking cloud networks
- ICS/SCADA

Learn

Learn ethical hacking with the revolutionary CEH v13—a game-changer for aspiring ethical hackers.

With 20 cutting-edge modules, you'll gain the core skills needed to dominate the cybersecurity landscape. CEH isn't just keeping pace—it's leading the charge, evolving with the latest operating systems, exploits, tools, and hacking techniques to ensure you're always ahead of the curve.

Dive deep into the future of cybersecurity with training that integrates AI into all five phases of ethical hacking, reconnaissance and scanning to gaining access, maintaining access, and covering tracks. You'll harness the power of AI to supercharge your hacking techniques and disrupt AI systems—giving you 10x efficiency in your cybersecurity role.

CEH v13 isn't just a certification; it's a fully immersive experience. CEH combines comprehensive knowledge-based training with immersive hands-on labs to ensure a well-rounded learning experience. You'll engage with live targets, tools, and vulnerable systems in a controlled environment, building real-world skills that empower you to confidently apply your expertise in any scenario. Get ready to transform the way you hack and protect the digital world!

Course Outline

Get the AI edge with 20 Power-packed Modules of the CEH v13

Learn	Course Outline
Module 01 Introduction to Ethical Hacking	Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
Module 02 Footprinting and Reconnaissance	Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking
Module 03 Scanning Networks	Learn different network scanning techniques and countermeasures.
Module 04 Enumeration	Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.
Module 05 Vulnerability Analysis	Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.
Module 06 System Hacking	Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.
Module 07 Malware Threats	Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.
Module 08 Sniffing	Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.
Module 09 Social Engineering	Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
Module 10 Denial-of-Service	Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Learn	Course Outline
Module 11 Session Hijacking	Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
Module 12 Evading IDS, Firewalls, and Honeypots	Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
Module 13 Hacking Web Servers	Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.
Module 14 Hacking Web Applications	Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.
Module 15 SQL Injection	Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.
Module 16 Hacking Wireless Networks	Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.
Module 17 Hacking Mobile Platforms	Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
Module 18 IoT Hacking	Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
Module 19 Cloud Computing	Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.
Module 20 Cryptography	Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

Hands-On Learning Labs

With 221 hands-on labs in our cutting-edge cyber range, you'll practice every skill on live machines and real-world vulnerabilities. Armed with over 4,000 powerful hacking tools and a range of operating systems, you'll gain unrivaled, practical expertise with the most widely used security tools, current vulnerabilities, and industry-standard operating systems.

This revolutionary environment brings the industry's top security tools and the latest vulnerabilities to your fingertips, all in a web-accessible platform. No matter where you are, you can dive into the real-world experience and emerge as a force to be reckoned with in cybersecurity.

Open AI API credits are not included as part of the program.

Lab Environment

Cloud-Based Cyber Range

What's Covered

100% virtualization for a complete learning experience

Full access to pre-configured targets, networks, and the attack tools necessary to exploit them:

Pre-configured vulnerable websites

Vulnerable, unpatched operating systems

Fully networked environments

4000+ hacking tools and so much more!

Wide range of target platforms to hone your skills

550 attack techniques covered

Objective-oriented flags for critical thinking and applied knowledge assessment

Cloud-based cyber range

Certify

Prove Your Skills and Abilities with Online, Practical Examinations

CEH Exams: 4-hour Knowledge-Based Exam and 6-hour Practical Exam.

The Certified Ethical Hacker (CEH) is globally recognized as the gold standard for assessing ethical hacking skills. With CEH v13, you have the option to take two exams: a knowledge-based exam and a practical exam to earn the CEH Master certification. Both exams are approved by the U.S. DoD 8140 and accredited by ANAB ISO/IEC 17024.

Industry practitioners meticulously vet certification domains to align with current industry demands. Each exam undergoes rigorous psychometric evaluation, ensuring a fair and accurate assessment of your ethical hacking expertise.

Achieving the CEH certification and passing both the knowledge-based and practical exams earns you the prestigious CEH Master certification. This advanced recognition demonstrates not only your theoretical understanding but also your mastery of real-world ethical hacking skills, proving you're ready to excel in any cybersecurity role.

Certification Outline

Knowledge Exam
4 Hours
Multiple-Choice Exam

Skills Exam
6 Hours
20 Practical Challenges

CEH Knowledge-Based Exam

The CEH knowledge-based exam is a four-hour exam with 125 multiple-choice questions. It will test your skills in information security threats, attack vectors, attack detection, attack prevention, procedures, methodologies, and more! This exam is recognized worldwide as the original and most trusted tactical cybersecurity certification exam.

Access our Exam Blueprint for CEH (Download Now)

CEH Practical Exam

The CEH Practical exam is the world's first ethical hacking practical exam to have ANAB and US DoD approval. The CEH Practical is a 6-hour, 100% hands-on exam delivered in our Cyber Range that requires you to demonstrate the skills and abilities of ethical hacking techniques such as:

- Port scanning tools (e.g., Nmap, Hping)
- Vulnerability detection
- Attacks on a system (e.g., DoS, DDoS, session hijacking, web server and web application attacks, SQL injection, and wireless threats)
- SQL injection methodology and evasion techniques
- Web application security tools (e.g., Acunetix WVS)
- SQL injection detection tools (e.g., IBM Security AppScan)
- Communication protocols

In the CEH Practical, you have a limited time to complete 20 challenges that test your proficiency in a performance-based cyber range.
This exam is NOT a simulation and incorporates a live corporate network of VMs and applications with solutions to uncover vulnerabilities.

CEH Master

Upon successfully completing both the CEH Knowledge-based Exam and the CEH Practical Exam, the CEH (Master) designation is awarded. A CEH (Master) signifies a high level of proficiency in ethical hacking knowledge, skills, and abilities, with a total of 6 hours of testing to prove their competency. The top 10 performers in both the CEH Knowledge-based Exam and CEH Practical Exam are featured on the CEH Master Global Ethical Hacking Leader Board.

The CEH Exams at a Glance

Exam Details	CEH Knowledge Exam	CEH Practical Exam
Number of Questions/ Practical Challenges	125 Questions	20 Practical Challenges
Test Duration	4 Hours	6 Hours
Test Format	MCQ	iLabs Cyber Range
Test Availability	ECC Exam, Vue	ASPEN, iLabs
Exam Prefix	312-50 (ECC Exam), 312-50 (VUE)	-
Passing Score	60% - 85%	60% - 85%

Engage

The CEH v13 program immerses you in real-world ethical hacking through the dynamic CEH practice environment. With CEH Engage, you'll sharpen your skills and prove you have what it takes to thrive as an ethical hacker.

New to CEH v13, learners will embark on their first emulated ethical hacking engagement. This four-phase engagement requires students to think critically and test the knowledge and skills gained by capturing a series of flags in each phase. It demonstrates the live application of skills and abilities in a consequence-free environment through EC-Council's new "Cyber Range."

As you complete your training and labs, CEH Engage empowers you to put theory into practice through a mock hacking engagement. You'll navigate a real-world, four-part engagement, targeting an emulated organization. Using a capture-the-flag format, you'll progress by answering critical "flag" questions, gaining hands-on experience in a full-scale ethical hacking operation.

Your Mission:

Whether this is your first engagement or you're honing your skills, get ready to test your ethical hacking knowledge like never before! Once you've practiced through the hands-on guided labs, it's time to apply your knowledge, take on the hacker's persona, and find the vulnerabilities and weaknesses in the ABCD organization (fictitious organization, but with real live networks)—all built within our CEH Engage (practice range).

Target Organization Characteristics

- ABCDorg is a nationwide IT/ ITES organization
- Realistic segmented networks
- Demilitarized zones (DMZs) and private subnets stretch across the infrastructure to support various business units
- Various application servers and services support ABCDorg Operations
- Real networks, real operating systems, and real applications
- Private, dedicated access — no shared resources
- Fully automated network deployment with EC-Council's Cyber Range
- 24x7 browser-based access

Objectives

Armed with your attack platform (Parrot OS) and a plethora of tools used by ethical hackers, you will embark on a 4-part engagement to assess ABCDorg's security posture. Follow the process, practice your TTP, and experience the real thing in a controlled environment with no consequences. It's the ultimate learning experience to support your career as an ethical hacker! Each phase builds on the last as you progress through your ABCDorg engagement.

Phase 1

Vulnerability assessment:

Footpringing & Reconnaissance

Scanning

Enumeration

Vulnerability Analysis

Phase 2

Gaining access:

System Hacking

Malware Threats

Sniffing

Social Engineering

Denial-of-Service

Phase 3

Perimeter and Web App Exploitation:

Session Hijacking

Evading IDS

Firewalls

Honeypots

Hacking Web Servers

Hacking Web Applications

SQL Injection

Phase 4

Mobile, IoT, OT Exploitation:

Hacking Wireless Networks

Hacking Mobile Platforms

IoT Hacking

OT Hacking

Cloud Computing

Cryptography

Compete

True progress thrives on competition—it's what drives you to reach your full potential and become the best in the game!

The CEH global challenges takes place monthly, providing capture-the-flag style competitions that give learners exposure to various new technologies and platforms, from web applications, OT, IoT, SCADA, and ICS systems to cloud and hybrid environments.

You will compete against other ethical hackers in a fast-paced, four-hour event as you climb the leaderboard in curated CTFs designed around the ethical hacking process. Each objective-based flag sharpens your current skills, tests your critical thinking, and covers the latest vulnerabilities and exploits. Hosted entirely online in EC-Council's advanced Cyber Range, these scenario-based engagements are set in fully developed network and application environments with real operating systems, networks, tools, and vulnerabilities. You'll have the opportunity to practice, engage, compete, build and hone your hacking techniques as you engage with new target organizations, all while racing against the clock to prove your mastery.

CEH Global Challenges

Each month will present a different theme and challenge, with capture-the-flag-style competitions focusing on ethical hackers' core skills and abilities. Gain exposure to new tools, focus on new attack vectors, and try to exploit emerging vulnerabilities while

New Challenges Every Month

Month	Skill Challenge
September '24	Off-The ShelfOff-The-Shelf CMS Exploitation
October '24	Windows Wreckage: Unravelling Code & Hunting Threats
November '24	Web Warriors: Defend Against the OWASP Menace
December '24	Operation ATT&CK Unveil: Decoding Cyber Tactics
January '25	RansomWar: Battle for Decryption
February '25	Supply Chain Siege: Unravel the Hidden Links
March '25	Operation Nexus: Breach the Grid
April '25	Identity Infiltration: Breach the Directory
May '25	API Apocalypse: Breach the Gateways
June '25	Data Fortress Breach: Cracking the Core
July '25	Operation Deep Breach: Hack, Escalate, Pivot
August '25	eCommerce Rampage: Defend the Digital Marketplace
Sept '25	Cloud Clash: Battle for Infrastructure Security

Hack Your Way to the Top – Become the Name Everyone Knows!

As an ethical hacker, you will battle to the top of the monthly Ethical Hacking Leaderboards as you race against the clock in these four-hour CTF challenges. The challenge is open all month long, so compete when you're ready! Leaderboards" as you race against the clock in these 4-hour CTF challenges. The challenge is open all month long, so compete when you're ready!

Pre-Requisites

You need only an internet connection, and can compete through your browser.
We provide the attack platform, targets and all the required tools. You bring the skills to win!

Chance to Earn Prestigious CEH Compete Badges Each Month

Compete Examples (A Preview of Challenges)

Topic: Ransomware/Malware Analysis

Brief: You have been called in by a reputable MNC that was recently hit with malware. This malware locked up their services and infected a slew of customers who were using their software. The incident response team managed to extract some of the code. Now, your job is to reverse-engineer the malware and identify encryption algorithms used, plus identify any trace of command-and-control servers that may be helpful to law enforcement agencies.

Topic: Application Hardening

Brief: Your employer, a large financial institution, has suffered a breach where hackers were able to inject code into a web application, exposing sensitive customer data. Your company has faced tremendous scrutiny from the public and must pay fines to its regulators. You have to perform a series of manual and automated tests against the web application to identify weaknesses and provide recommended countermeasures to the app security team.

(Become an AI Powered Certified Ethical Hacker)

Stay Ahead of Emerging Threats:

New Focus Areas and Trends in CEH v13

Trained to think outside the box with a hacker's mindset, individuals who pursue the Certified Ethical Hacker (CEH) v13 thoroughly explore top OWASP attacks, active directory breaches, the vulnerability of traditional encryption to quantum computing, the growing ransomware threat, and other emerging risks, equipping learners with strategies to implement zero trust architecture and other cybersecurity measures. CEH v13 is comprehensive with the latest knowledge, providing cybersecurity professionals with the skills, tools, techniques, and strategies to defend against trending, modern, and complex cyber threats effectively and efficiently.

Active Directory Attacks

Ransomware Attacks and Mitigation

AI and Machine Learning in Cybersecurity

Critical Infrastructure Vulnerabilities

Extended Detection and Response (XDR)

Quantum Computing Risks and Attacks

Post-Quantum Cryptography

Deepfake Threats

Zero Trust Architecture

Cloud Security

IoT Security Challenges

Critical Infrastructure Vulnerabilities

Get 10 Ethical Hacking videos in CEH v13 Elite

1. Open Source Intelligence
2. Wireshark for Ethical Hackers
3. Ethical Hacking with Nmap
4. Windows Penetration Testing Essentials
5. Session Hijacking and Prevention Techniques
6. Power of Next Generation Firewalls
7. OWASP Top 10 Security Fundamentals
8. Burp Suite: Web Application Penetration Testing
9. Deep Dive into Network Assessments
10. Applied Secure Smart City

CEH Skills Mapped To 49 Cybersecurity Job Roles

1. Mid-Level Information Security Auditor
2. Cybersecurity Auditor
3. Security Administrator
4. IT Security Administrator
5. Information Security Analyst 1
6. Infosec Security Administrator
7. Cybersecurity Analyst (Level 1, Level 2, & Level 3)
8. Network Security Engineer
9. SOC Security Analyst
10. Network Engineer
11. Senior Security Consultant
12. Information Security Manager
13. Senior SOC Analyst
14. Solution Architect
15. Cybersecurity Consultant
16. Cyber Defense Analyst
17. Vulnerability Assessment Analyst
18. Warning Analyst
19. All-Source Analyst
20. Cyber Defense Incident Responder
21. Research & Development Specialist
22. Senior Cloud Security Analyst
23. Third Party Risk Management:
24. Threat Hunting Analyst
25. Penetration Tester
26. Cyber Delivery Manager
27. Application Security Risk
28. Threat Modelling Specialist
29. Web Application Penetration Testing
30. SAP Vulnerability Management - Solution Delivery Advisor
31. Ethical Hacker
32. SIEM Threat Responder
33. Product Security Engineer / Manager
34. Endpoint Security Engineer
35. Cybersecurity Instructor
36. Red Team Specialist
37. Data Protection & Privacy Officer
38. SOAR Engineer
39. AI Security Engineer
40. Sr. IAM Engineer
41. PCI Security Advisor
42. Exploitation Analyst (EA)
43. Zero Trust Solutions Engineer / Analyst
44. Cryptographic Engineer
45. AI/ML Security Engineer
46. Machine Learning Security Specialist
47. AI Penetration Tester
48. AI/ ML Security Consultant
49. Crypto Security Consultant

CEH v13 Training Information

Training: 5 days
Duration: 40 Hours

Training Options

iLearn (Self-Study)

This solution is an asynchronous, self-study environment in a video-streaming format.

iWeek (Live Online)

This solution is an online, live training course led by an instructor.

Master Class

This solution offers the opportunity to learn from world-class instructors and collaborate with top information security professionals.

Training Partner (In Person)

This solution offers in-person training so that you can benefit from collaborating with your peers.

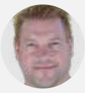
CEH Employed by Government and Top Fortune 500 Companies Across the Globe

Why Top Cybersecurity Professionals Love CEH?

"Skills from the CEH program have evolved and are valuable."

Mauricio Fernandes
Systems Architect,
Cisco, USA

"Knowledge I gained from CEH gave me the confidence I needed to step into a role as a security engineer and penetration tester."



Roy Davis
Security Engineer,
Zoom, USA

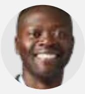
"Helping organization investigating SolarWinds hack, wouldn't have been possible without CEH."

Giulio Astori
Cyber Security Architect,
Microsoft, USA

"CEH was my first confidence booster and helped land me a job on a Red Team in the government sector."

Farzan Karimi
IT Security Manager,
Google, USA

"CEH made me an authoritive expert on security discussions with our clients."



Kojo Donkor
Security Architect,
Cisco, USA

"CEH helped me be able to understand exactly what I was doing once I finally landed a role in the cybersecurity field."

Lawan Cancer II
Security Analyst,
Morgan Stanley, USA

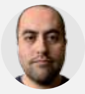
"CEH has helped me to work on mobile devices and AppSec - Pen testing and reverse engineering."

John Packiaraj
Security Architect,
Visa, USA

"While other certifications talk the talk, CEH walks the walk and is recognized by the department of defense."

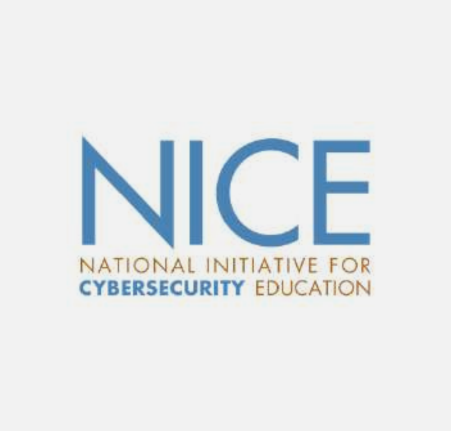
Michael Turner
Chief Security Engineer,
Lockheed Martin, USA

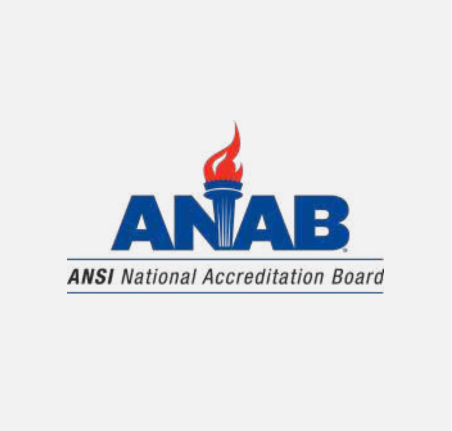
"CEH develops a "think outside the box" approach that you cannot get from other skills."

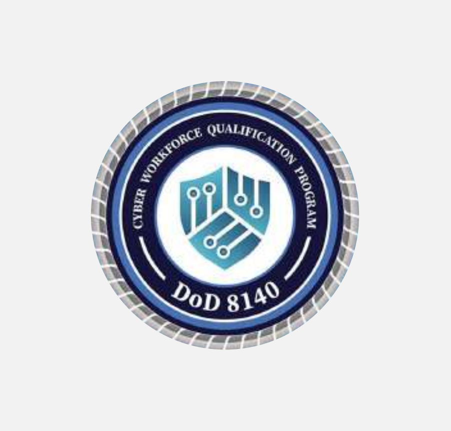


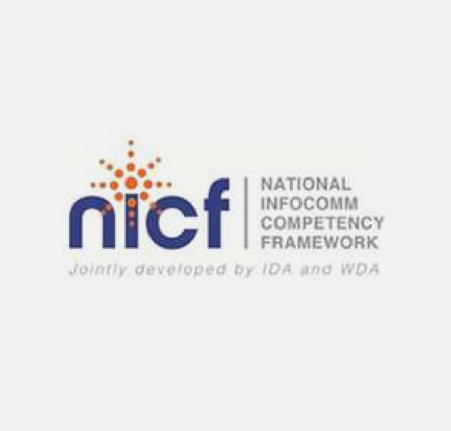
Felipe Munoz
IT Security Director,
Oracle, USA

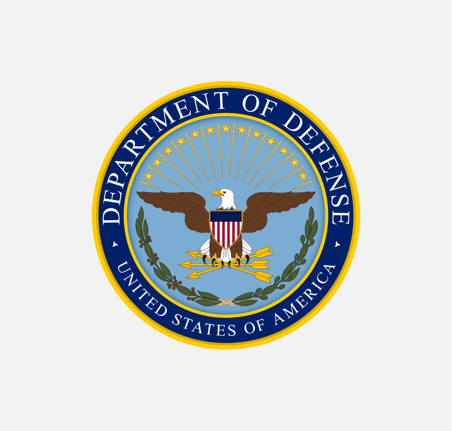
CEH v13 Recognition/ Endorsement/Mapping

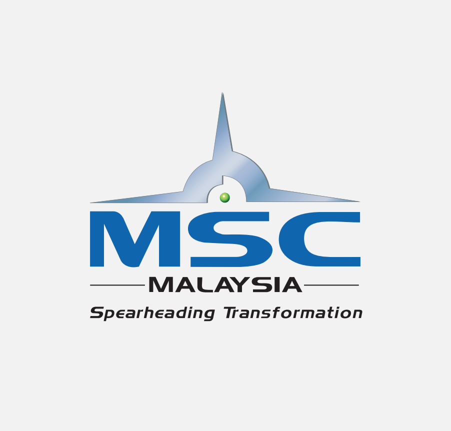


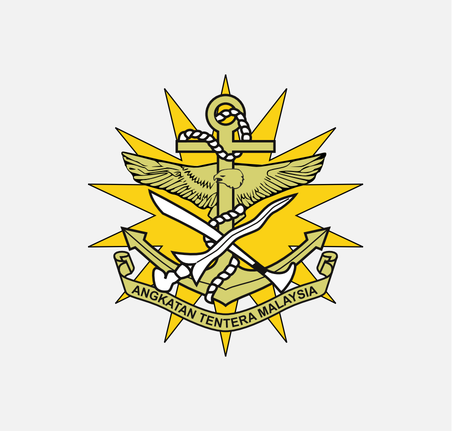





nicf
NATIONAL INFOCOMM COMPETENCY FRAMEWORK
Jointly developed by IDA and WDA







Discover Why Organizations Worldwide Trust the CEH Certification

For 20 years, EC-Council's cybersecurity programs have empowered cybersecurity professionals around the world to exercise their training and expertise to combat cyberattacks. The CEH Hall of Fame celebrates those individuals who have excelled, achieved, and fostered a spirit of leadership among their colleagues and peers within the cyber community.

Key Findings Reported by Thousands of Cybersecurity Professionals from the CEH Hall of Fame Report:

Download CEH Hall of Fame Report

Over 1 In Every 2 Professionals Received Promotions After CEH

97% Stated That the Skills They Acquired In CEH Helped Safeguard Their Organizations

97% Found That CEH Labs Accurately Mimic Real-World Cyber Threats

95% Chose CEH For Career Growth

93% Said That CEH Skills Improved Their Organizational Security

92% Of Hiring Managers Prefer Candidates With CEH For Jobs That Require Ethical Hacking Skills

92% Reported That CEH Boosted Their Self-Confidence

88% Considered CEH Is the Most Comprehensive Ethical Hacking Program in the Industry

85% Credited CEH With Helping Them Give Back to The Cybersecurity Community

80% Started Their Cybersecurity Careers with CEH

About EC-Council

EC-Council's sole purpose is to build and redefine the cybersecurity profession globally.

We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the intelligence community, NATO, and over 2,000 of the best universities, colleges, and training companies, our programs have certified people in over 140 countries, and set the bar in the field of cybersecurity education. Best known for the Certified Ethical Hacker (CEH) program, we are dedicated to equipping over 380,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against cyber adversaries. EC-Council builds individual and organization-wide cyber capabilities through our other programs as well, including Certified Secure Computer User (CSCU), Computer Hacking Forensic Investigator (CHFI), Certified Security Analyst, Certified Network Defender (CND), Certified SOC Analyst (CSA), Certified Threat Intelligence Analyst (CTIA), Certified Incident Handler (ECIH), and the Certified Chief Information Security Officer (CCISO). We are an ANAB ISO/IEC 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies. Founded in 2001, EC-Council employs over 400 individuals worldwide, with ten global offices in the U.S., UK, Malaysia, Singapore, India, and Indonesia. Our U.S. offices are in Albuquerque, NM, and Tampa, FL. Learn more at **eccouncil.org**.