# EC-Council Ethical Hacking Essentials (EHE)

**Category:** Networking & Security | **Vendor:** EC-Council

**Duration:** 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

## Course Information

**Delivery Format:** Instructor Led - Online

## Course Overview

Ethical Hacking Essentials is an introductory cybersecurity course that covers ethical hacking and penetration testing fundamentals and prepares learners for a career in cybersecurity. This ethical hacking course will introduce learners to computer and network security concepts such as threats and vulnerabilities, password cracking, web application attacks, IoT and OT attacks, cloud computing, pentesting fundamentals, and more. EC-Council’s ethical hacking essentials course provides hands-on practical experience to learners, thus giving them the skills necessary for a future in cybersecurity. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

## About This Course

Ethical Hacking Essentials is an introductory cybersecurity course that covers ethical hacking and penetration testing fundamentals and prepares learners for a career in cybersecurity. This ethical hacking course will introduce learners to computer and network security concepts such as threats and vulnerabilities, password cracking, web application attacks, IoT and OT attacks, cloud computing, pentesting fundamentals, and more. EC-Council's ethical hacking essentials course provides hands-on practical experience to learners, thus giving them the skills necessary for a future in cybersecurity. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

## Who Should Attend

- School students, fresh graduates, Professionals, Career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.
- Anyone who wants to start their cybersecurity career and master the fundamentals of security online.
- Anyone who wants to prepare for a cybersecurity career and aid their IT education.
- Professionals who want to get into the cybersecurity field but are unsure where to start their education journey

## Learning Outcomes

**Upon successful completion of this course, participants will be able to:**

Key issues plaguing the information security world and information security laws and standards. Fundamentals of ethical hacking Information security threats and vulnerabilities Different types of malware Different types of password-cracking techniques and countermeasures Social engineering techniques, insider threats, identity theft, and countermeasures Network level attacks (sniffing, denial-of-service, and session hijacking) and countermeasures. Application-level attacks (web-server attacks, web application attacks, and SQL injection) and countermeasures Wireless encryption, wireless threats, and countermeasures Mobile platform attack vector, mobile device management, mobile security guidelines, and security tools IoT and OT concepts, attacks, and countermeasures Cloud computing technologies, cloud computing threats, attacks, and security techniques Fundamentals of pen testing

## Detailed Course Outline

### Module 01: Information Security Fundamentals

- Information Security Fundamentals
- Information Security Laws and Regulations

### Module 02: Ethical Hacking Fundamentals

- Cyber Kill Chain Methodology
- Hacking Concepts and Hacker Classes
- Different Phases of Hacking Cycle
- Ethical Hacking Concepts, Scope, and Limitations
- Ethical Hacking Tools

### Module 03: Information Security Threats and Vulnerability Assessment

- Threat and Threat Sources
- Malware and its Types
- Malware Countermeasures
- Vulnerabilities
- Vulnerability Assessment

## Module 04: Password Cracking Techniques and Countermeasures

- Password Cracking Techniques
- Password Cracking Tools
- Password Cracking Countermeasures

## Module 05: Social Engineering Techniques and Countermeasures

- Social Engineering Concepts and its Phases
- Social Engineering Techniques
- Insider Threats and Identity Theft
- Social Engineering Countermeasures

## Module 06: Network Level Attacks and Countermeasures

- Packet Sniffing Concepts
- Sniffing Techniques
- Sniffing Countermeasures
- DoS and DDoS Attacks
- DoS and DDoS Attack Countermeasures
- Session Hijacking Attacks
- Session Hijacking Attack Countermeasures

## Module 07: Web Application Attacks and Countermeasures

- Web Server Attacks
- Web Server Attack Countermeasures
- Web Application Architecture and Vulnerability Stack
- Web Application Threats and Attacks
- Web Application Attack Countermeasures
- SQL Injection Attacks
- SQL Injection Attack Countermeasures

## Module 08: Wireless Attacks and Countermeasures

- Wireless Terminology
- Wireless Encryption
- Wireless Network-Specific Attack Techniques
- Bluetooth Attacks
- Wireless Attack Countermeasures

## Module 09: Mobile Attacks and Countermeasures

- Mobile Attack Anatomy
- Mobile Platform Attack Vectors and Vulnerabilities
- Mobile Device Management (MDM) Concept
- Mobile Attack Countermeasures

## Module 10: IoT and OT Attacks and Countermeasures

- IoT Concepts
- IoT Threats and Attacks
- IoT Attack Countermeasures
- OT Concepts
- OT Threats and Attacks
- OT Attack Countermeasures

## Module 11: Cloud Computing Threats and Countermeasures

- Cloud Computing Concepts
- Container Technology
- Cloud Computing Threats
- Cloud Attack Countermeasures

## Module 12: Penetration Testing Fundamentals

- Fundamentals of Penetration Testing and its Benefits
- Strategies and Phases of Penetration Testing
- Guidelines and Recommendations for Penetration Testing

# Frequently Asked Questions

### Q: What delivery options are available for EC-Council Ethical Hacking Essentials (EHE)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

---

### Q: How many CPD hours does this course provide?

The 2-day EC-Council Ethical Hacking Essentials (EHE) course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

---

### Q: What is the duration of the EC-Council Ethical Hacking Essentials (EHE) training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

---

### Q: Do you provide corporate training for EC-Council Ethical Hacking Essentials (EHE)?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council Ethical Hacking Essentials (EHE). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

---

### Q: Why choose Nexus Human for EC-Council Ethical Hacking Essentials (EHE)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

---

### Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council Ethical Hacking Essentials (EHE) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.


## Nexus Human

**Professional Training & Development**

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)


© 2026 Nexus Human. All rights reserved. This brochure was generated on 13/11/2026.