



[View Full Course Details including Latest Schedule Online](#)

EC-COUNCIL

CEH Certification Training

Award Winning CEH Training from Phoenix TS. This course fortifies the knowledge of IT security professionals to help them think as a hacker to detect weaknesses and vulnerabilities within network infrastructures.

Course Overview

Our 5-day, instructor-led CEH (Certified Ethical Hacker) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is geared toward IT security professionals concerned with their organization's network infrastructure. It covers:

- Policy creation
- Intrusion detection
- Virus creation
- DDoS attacks
- Buffer overflows
- Social engineering

This course will fully prepare you for the [CEH Certification exam](#).

Before taking this course, you should have at least two years of IT security work experience and a strong knowledge of TCP/IP and how to implement them. Though not required, it is also recommended that you have the [CompTIA Security+ Certification](#).

Course Outline

Introduction to Ethical Hacking

- Information security overview



- Information security threats and attack vectors
- Hacking concepts
- Ethical hacking concepts
- Information Security Controls
- Penetration testing concepts
- Information security laws and standards

Footprinting and Reconnaissance

- Footprinting concepts
- Footprinting through search engines
- Footprinting through web services
- Footprinting through social networking sites
- Website footprinting
- Email footprinting
- Competitive Intelligence
- WHOIS Footprinting
- DNS footprinting
- Network footprinting
- Footprinting through social engineering
- Footprinting tools
- Countermeasures
- Footprinting pen testing

Scanning Networks

- Network scanning concepts
- Scanning tools
- Scanning techniques
- Scanning beyond IDS and firewall
- Banner grabbing
- Draw network diagrams
- Scanning pen test

Enumeration

- Enumeration concepts
- NetBIOS enumeration
- SNMP enumeration
- LDAP enumeration
- NTP enumeration SMTP and DNS enumeration



- Other enumeration techniques
- Enumeration countermeasures
- Enumeration pen testing

Vulnerability Analysis

- Vulnerability assessment concepts
- Vulnerability assessment solutions
- Vulnerability scoring systems
- Vulnerability assessment tools
- Vulnerability assessment reports

System Hacking

- System hacking concepts
- Cracking passwords
- Escalating privileges
- Executing applications
- Hiding files
- Covering tracks
- Penetration testing

Malware Threats

- Malware concepts
- Trojan concepts
- Virus and worm concepts
- Malware analysis
- Countermeasures
- Anti-malware software
- Malware penetration testing

Sniffing

- Sniffing concepts
- Sniffing techniques: MAC attacks
- Sniffing techniques: DHCP attacks
- Sniffing techniques: ARP Poisoning
- Sniffing techniques: Spoofing attacks
- Sniffing techniques: DNS poisoning



- Sniffing tools
- Countermeasures
- Sniffing detection techniques
- Sniffing pen testing

Social Engineering

- Social engineering concepts
- Social engineering techniques
- Insider threats
- Impersonation on social networking sites
- Identity theft
- Countermeasures
- Social engineering pen testing

Denial of Service

- DoS/DDoS Concepts
- DoS/DDoS attack techniques
- Botnets
- DDoS case study
- DoS/DDoS attack tools
- Countermeasures
- DoS/DDoS protection tools
- DoS/DDoS penetration testing

Session Hijacking

- Session hijacking concepts
- Application level session hijacking
- Network level session hijacking
- Session hijacking tools
- Countermeasures
- Penetration testing

Evading IDS, Firewalls, and Honeypots

- IDS, firewall and honeypot concepts
- IDS, firewall and honeypot solutions
- Evading IDS



- Evading firewalls
- IDS/firewall evading tools
- Detecting honeypots
- IDS/Firewall evasion countermeasures
- Penetration testing

Hacking Webservers

- Web server operations
- Web server attacks
- Web server attack methodology
- Web server attack tools
- Countermeasures
- Patch management
- Web server security tools
- Web server pen testing

Hacking Web Applications

- Web app concepts
- Web app threats
- Hacking methodology
- Web app hacking tools
- Countermeasures
- Web app security testing tools
- Web app pen testing

SQL Injection

- SQL injection concepts
- Types of SQL injection
- SQL injection methodology
- SQL injection tools
- Evasion techniques
- Countermeasures

Hacking Wireless Networks

- Wireless concepts
- Wireless encryption



PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

- Wireless threats
- Wireless hacking methodology
- Wireless hacking tools
- Bluetooth hacking
- Countermeasures
- Wireless security tools
- Wireless pen testing

Hacking Mobile Platforms

- Mobile platform attack vectors
- Hacking Android OS
- Hacking iOS
- Mobile spyware
- Mobile device management
- Mobile security guidelines and tools
- Mobile pen testing

IoT and OT Hacking

- IoT and OT concepts
- IoT and OT attacks
- IoT and OT hacking methodology
- IoT and OT hacking tools
- Countermeasures
- IoT and OT pen testing

Cloud Computing

- Cloud computing concepts
- Cloud computing threats
- Cloud computing attacks
- Cloud security
- Cloud security tools
- Cloud penetration testing

Cryptography

- Cryptography concepts
- Encryption algorithms



- Cryptography tools
- Public key infrastructure (PKI)
- Email encryption
- Disk encryption
- Cryptanalysis Countermeasures

Exam Information

CEH Certification Exam Details:

- 125 Questions
- Passing Score: 60% to 85%
- Test Duration: 4 hours
- Test Format: Multiple choice
- Test Delivery: ECC EXAM, VUE
- Exam Prefix: 312-50 ECC EXAM, 312-50 VUE

CEH Certification Exam Objectives:

Exam 312-50 tests CEH candidates on each of the 20 domains covered in-depth through the training course, including:

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Evading IDS, Firewalls, and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT and OT Hacking
19. Cloud Computing



PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

20. Cryptography

Phoenix TS is an authorized testing center for Pearson Vue.

CEH Certification Training FAQs

[expandable_content]

What are the requirements for CEH?

Candidates need to attend official CEH Certification Training to be eligible to sit for the exam. Otherwise, candidates must be able to prove a minimum of 2 years' work experience in Information Security.

How long does the CEH certification last?

The CEH certification has a three year renewal period, during which time certificate holders must submit 40 ECEs each year for a total of 120 ECEs at the end of the renewal period.

What jobs can I get after CEH?

The CEH certification will benefit Site Administrators, Auditors, Security Officers and other Security Professionals.

What is the average salary of someone with the CEH certification?

According to payscale.com, professionals with their CEH certification earn an average of \$95,000 annually.

Starting at **\$2,695**

ATTENTION

For GSA pricing or Contractor quotes call

[240.667.7757](tel:240.667.7757)

GSA



Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

This **CEH Certification Training** course includes:

- 5 days instructor-led training with a CEH Certified Instructor
- CEH iLabs access (optional add-on)
- Official EC-Council CEH courseware
- 350+ attack technologies, 2200+ commonly used hacking tools and 140+ simulation labs covered
- CEH study videos (60 days access)
- CEH study guides (60 days access)
- CEH practice exams (60 days access)
- CEH mock exams (60 days access)
- CEH exam readiness assessment (60 days access)
- Pre and post assessments
- CEH exam voucher
- CEH testing on the last day of class
- Onsite exam scheduling and testing center
- Certificate of completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications
- EC-Council Training Center of the Year



- EC-Council Authorized Training Course
- CEH course retake guarantee
- Meets 8570.01-M training requirements for CSSP Analyst, CSSP Infrastructure Support, CSSP Incident Responder, CSSP Auditor
- Eligible for MyCAA scholarship
- This CEH v11 certification maps 100% to the NICE framework Protect and Defend specialty area.
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

**denotes this benefit is only available at participating locations.*