id Cyber Solutions
protecting your business from cyber crime

C|EH™
Certified Ethical Hacker

CEH: CERTIFIED ETHICAL HACKER v9

SUMMARY

The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the first part of a 3 part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one!

As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment,

This course was designed to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, *"To beat a hacker, you need to think like a hacker"*. This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver's seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be taught the Five Phases of Ethical Hacking, and thought how you can approach your test target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access and Covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopaedic approach to help you identify when an attack has been used against your own targets.

Why is this training called the Certified Ethical Hacker Course? We teach the same techniques as the bad guys, you can assess the security posture of an organization with the same approach these malicious hackers use, identify weaknesses and fix the problems before they are identified by the enemy, causing what could potentially be a catastrophic damage to your respective organization.

Throughout the CEH course, you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.

Who Should Attend?

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure.

What Will You Learn?

CEHv9 consists of 20 core modules designed to facilitate a comprehensive ethical hacking and penetration testing training.

1 Introduction to Ethical Hacking

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts, Types and Phases
- Ethical Hacking Concepts and Scope
- Information Security Controls
- Physical Security
- Incident Management
- What is Vulnerability assessment?
- Penetration Testing
- Information Security Laws and Standards

2 Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting Methodology
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Penetration Testing

3 Scanning Networks

- Overview of Network Scanning
- CEH Scanning Methodology

4 Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Penetration Testing

5 System Hacking

- Evaluating Information for System Hacking
- System Hacking Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps
- Hiding Files
- Covering Tracks
- Penetration Testing

6 Malware Threats

- Introduction to Malware
- Trojan Concepts
- Types of Trojans
- Virus and Worms Concepts
- Malware Reverse Engineering
- Countermeasures
- Anti-Malware Software
- Penetration Testing

7 Sniffing

- Sniffing Concepts
- MAC Attacks
- DHCP Attacks
- ARP Poisoning
- Spoofing Attack
- DNS Poisoning
- Sniffing Tools
- Sniffing Tool: Wireshark
- Packet Sniffing Tool: Capsa Network Analyser
- Network Packet Analyser
- Countermeasures Sniffing Detection and Penetration Testing

8 Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft

9 Denial of Service

- DoS/DDos Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- Dos/DDos Attack Tools
- Counter-Measures
- Dos/DDos Protection Tools
- DoS/DDos Attack Penetration Testing

10 Session Hijacking

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures and Penetration Testing

11 Hacking Webservers

- Webserver Concepts
- Webserver Attacks
- Attack Methodology
- Webserver Attack Tools
- Countermeasures, Security Tool and Penetration Testing
- Webserver Security Tools

12 Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web Application Hacking Tools
- Countermeasures, Security Tool and Penetration Testing
- Web Application Perpetration Testing Framework

13 SQL Injection

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

14 Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Counter Measures and Wi-Fi Penetration Testing
- Wireless Security Tools

15 Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Hacking Windows Phone
- Hacking Blackberry
- Mobile Device Management (MDM)
- Mobile Security Guidelines, Tools And Penetration Testing

16 Evading IDS, Firewalls and Honeypots

- IDS, Firewalls and honeypot Concepts
- IDS, Firewalls and honeypot Systems
- Evading IDS/Firewalls
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures and Penetration Testing

17 Cloud Computing

- Introduction to Cloud Computing
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security Tools and Penetration Testing

18 Cryptography

- Market Survey 2014: The Year of Encryption
- Case Study: Heartbleed
- Case Study: Poodlebleed
- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptography Attacks
- Cryptanalysis Tools

Legal Agreement

Ethical Hacking and Countermeasures course's mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent. Not anyone can be a student - the Accredited Training Centres (ATC) will make sure the applicants work for legitimate companies.

Educational Approach

- This training is based on both theory and practice:
  - Sessions of lectures illustrated with examples based on real cases
  - Practical exercises based on a full case study and lab environment to carry out test using real tools and techniques
  - Review exercises to assist the exam preparation
- To benefit from the practical exercises, the number of training participants is limited

Examination and Certification

- EXAM TITLE: CERTIFIED ETHICAL HACKER v9
- EXAM CODE: 312-50 (ECC EXAM)
- NUMBER OF QUSTIONS: 125
- DURATION 4 HOURS
- PASSING SCORE 70%
- TEST FORMAT: MULTIPLE CHOICE