CEHv9: Certified Ethical Hacker v9

This class immerses students in an interactive environment where they learn how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. The majority of the class is hands-on labs with instruction to explain, reinforce, and show how these hacking tools and techniques can be used to secure and defend real world networks. Students begin by seeing how perimeter defenses work. They next learn how to reconnoiter, scan and attack their own networks and how intruders escalate privileges. Students also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When students leave this intensive 5 day class they have hands on understanding and experience in Ethical Hacking and what they can do to analyze and secure their own network without harming their own assets. CEHv9 is ANSI accredited and focuses on the latest hacking attacks targeted to mobile platform and tablet computers and covers countermeasures to secure mobile infrastructure. The latest development in mobile and web technologies including Google Android OS, Apple iOS, Windows Phone, and HTML 5 as well as mobile applications and mobile app stores.

AUDIENCE

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

*CEHv9 Certification exam not included with course, must be purchased by the student directly from EC-Council.

PREREQUISITES

» Students must have at least one year of hands-on experience in computer security. Students that are new to computer security should begin with the SEC155 – Security+ course or the SEC275 – Information Security for the IT Professional course.

» Students must have a strong understanding of computer networking including the TCP/IP Protocol Suite, IP Routing and LAN Switching Concepts, and a strong understanding of the Internet. A minimum of 12 months experience in networking or Cisco CCNA Certification is recommended.

WHAT YOU WILL LEARN

You will learn how to scan, test, hack and secure systems. Through the use of hand-on labs, students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.

Questions?
Call 602-266-8585

$3495.00

• 5-day course
• Includes Authorized CEHv9 Courseware
• Promo and package discounts may apply
• Prepares for CEHv9 Certification exam.

Can’t make it to class in person?
Attend many classes online with RemoteLive.™

Call 602-266-8585 today for a live demo.

©2016 Interface Technical Training  All rights reserved
<table>
<thead>
<tr>
<th>COURSE OUTLINE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CEHv9: Certified Ethical Hacker v9</strong></td>
</tr>
</tbody>
</table>

1. Introduction to Ethical Hacking
   - Internet is Integral Part of Business and Personal Life
   - What Happens Online in 60 Seconds
   - Information Security Overview
   - Information Security Threats and Attack Vectors
   - Hacking Concepts, Types and Phases
   - Ethical Hacking Concepts and Scope
   - Information Security Controls
   - 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
   - Scanning Beyond IDS
   - Banner Grabbing
   - Scan for Vulnerability
   - Draw Network Diagrams
   - Prepare Proxies
   - Scanning Pen Testing

4. Enumeration
   - Enumeration Concepts
   - NetBIOS Enumeration
   - SNMP Enumeration
   - LDAP Enumeration
   - NTP Enumeration
   - SMTP Enumeration
   - Enumeration Countermeasures
   - SMB Enumeration Countermeasures
   - Enumeration Pen Testing

5. System Hacking
   - Information at Hand Before System Hacking Stage
   - System Hacking: Goals
   - CEH Hacking Methodology (CHM)

6. Malware Threats
   - Introduction to Malware
   - Trojan Concepts
   - Types of Trojans
   - Virus and Worms Concepts
   - Malware Reverse Engineering
   - Malware Detection
   - 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
   - Follow TCP Stream in Wireshark
   - Display Filters in Wireshark
   - Additional Wireshark Filters
   - Packet Sniffing Tool: Capsa Network Analyzer
   - Network Packet Analyzer
   - Counter measures
   - Sniffing Detection Techniques
   - Sniffing Pen Testing

8. Social Engineering
   - Social Engineering Concepts
   - Social Engineering Techniques
   - Impersonation on Social Networking Sites
   - Identity Theft
   - Social Engineering Countermeasures
   - Penetration Testing

9. Denial of Service
   - DoS/DDoS Concepts
   - DoS/DDoS Attack Techniques
   - Botnets

10. Session Hijacking
    - Session Hijacking Concepts
    - Application Level Session Hijacking
    - Network-level Session Hijacking
    - Session Hijacking Tools
    - Countermeasures
    - Session Hijacking Pen Testing

11. Hacking Web Servers
    - Webserver Concepts
    - Webserver Attacks
    - Attack Methodology
    - Webserver Attack Tools
    - Countermeasures
    - Patch Management
    - Webserver Security Tools
    - Webserver Pen Testing

12. Hacking Web Applications
    - Web App Concepts
    - Web App Threats
    - Web App Hacking Methodology
    - Web Application Hacking Tools
    - Countermeasures
    - Security Tools
    - Web App Pen Testing

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
    - Countermeasures

15. Hacking Mobile Platforms
    - Mobile Platform Attack Vectors
    - Hacking Android OS
    - Hacking iOS
    - Hacking Windows Phone OS
    - Hacking BlackBerry
    - Mobile Device Management (MDM)
    - Mobile Security Guidelines and Tools
    - Mobile Pen Testing

16. Evading IDS, Firewalls and Honeypots
    - IDS, Firewall and Honeypot Concepts
    - IDS, Firewall and Honeypot System
    - Evading IDS
    - Evading Firewalls
    - IDS/Firewall Evading Tools
    - Detecting Honeypots
    - IDS/Firewall Evasion Countermeasures
    - Penetration Testing

17. Cloud Computing
    - Introduction to Cloud Computing
    - Cloud Computing Threats
    - Cloud Computing Attacks
    - Cloud Security
    - Cloud Security Tools
    - Cloud 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

Register by phone at 602-266-8585, or online at www.InterfaceTT.com.
©2016 Interface Technical Training  All rights reserved. v042516