Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CEH - Certified Ethical Hacker

Course Description

SecureNinja's CEH v12 (Certified Ethical Hacker) training and certification boot camp will immerse students into a hands-on environment where they will be shown how to conduct ethical hacking. They will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! They will 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. Students will begin by understanding how perimeter defenses work and then be led into scanning and attacking their own networks. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. All of this will be done without harming any real network.

Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virus Creation. When a student leaves this intensive 5-day class they will have hands-on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

What is New in the CEH v12?

The CEH v12 equips aspiring cybersecurity professionals with the tactics, techniques, and procedures (TTPs) to build ethical hackers who can uncover weaknesses in nearly any type of target system before cyber criminals do. In 20 comprehensive modules, the course covers over 270 attack technologies, commonly used by hackers. CEHv12 contains updates and new information that reflect the most recent developments and methods.

The World’s No. 1 Ethical Hacking Certification for 20 Years

The Certified Ethical Hacker has been battle-hardened over the last 20 years, creating hundreds of thousands of Certified Ethical Hackers employed by top companies, militaries, and governments worldwide.

As “a picture tells a thousand words”, the developers of the CEH v12 have all this and more for you in over 3000+ graphically rich, specially designed slides to help you grasp complex security concepts in depth which will be presented to you in the 5-day hands-on class by our Certified Instructor.

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the globally recognized Certified Ethical Hacker certification! This course prepares you for the EC-Council Certified Ethical Hacker exam 312-50.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

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 learn the Five Phases of Ethical Hacking and be instructed on how you can approach your 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 encyclopedic approach to help you identify when an attack has been used against your own targets. Why then is this training called the Certified Ethical Hacker Course? This is because by using 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 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.

Topics Covered

- 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

Who Would Benefit

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Security Officers
- Auditors
- Network Administrators
- Firewall Administrators
- Security Professionals
- Anyone concerned about the integrity of the network infrastructure

Prerequisites

- Strong knowledge of TCP/IP
- Information systems and security background
- Minimum of 12 months of experience in networking technologies

CEH Exam Info

- Number of Questions: 125
- Passing score: 70%
- Test Duration: 4 Hours
- Test Format: Multiple Choice
- Test Delivery: VUE / ECCEXAM

CEH training at SecureNinja will properly prepare you for the following exams:

- 312-50 – Certified Ethical Hacker (ANSI)
    - Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
- 312-99 – Certified Network Defense Architect (CNDA)

Courseware

- Official Certified Ethical Hacker v12 Courseware

Course Length

- 40 hours

Legal Agreement

Ethical Hacking and Countermeasures 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.

Not anyone can be a student - the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

CEH v12 Features

- 20 Modules

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- 270 Slides Attack Technologies
- 3500+ Hacking Tools
- 3000+ graphically rich slides

DoD Directive 8570.1-M and 8140

CEH v12 meets Government and DoD agencies' compliance with Federal Information Security Management Act (FISMA) and DoD Directive 8570.1-M and 8140

The CEH v12 (312-50) Certification can only be taken by students who have completed the EC-Council-authorized training. Note also that members of the U.S. Federal Government may also take the Certified Network Defense Architect (CNDA) certification. The CNDA program has been designed especially for the United States Government and military agencies. To achieve the Certified Network Defense Architect Certification, you must pass the CNDA exam 312-99.

US DOD Directive 8570/8140 & Certified Ethical Hacker (CEH) The United States of America Department of Defense issued Directive 8570 in 2004 and updated to 8140 in 2015 to mandate baseline certifications for all Information Assurance “IA” positions. In February of 2010, this directive was enhanced to include the Certified Ethical Hacker across its Computer Network Defense Categories “CND”.

DOD Directive 8570 / 8140 as stated by DIAP: DOD Directive 8570.01M Change 2 provides the basis for an enterprise-wide solution to train, certify, and manage the DoD Information Assurance (IA) workforce.

Career Track & Roles

- Network Administrator
- Systems Administrator
- Systems Engineer
- Systems Architect
- Network Security Specialist

Follow On Courses

- CHFI (Certified Hacking Forensics Investigator)
- CASP+ (CompTIA Advanced Security Practitioner)