EC-Council

Certified Ethical Hacker

Program Brochure

Course Description

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!

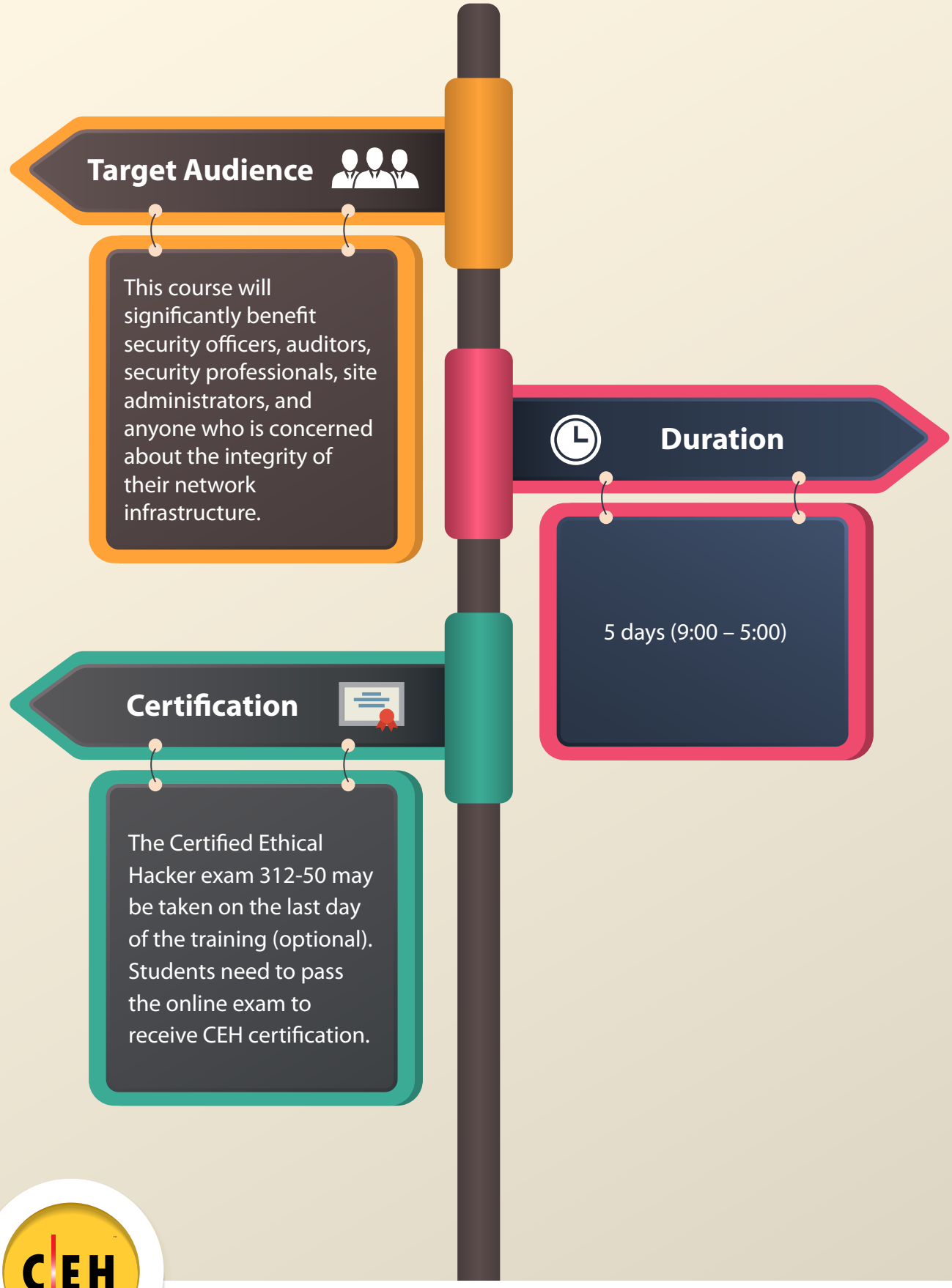
As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment,

This course was desgined 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 thought the Five Phases of Ethical Hacking and thought 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 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.


Target Audience
This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure.
Duration
5 days (9:00 – 5:00)
Certification
The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online exam to receive CEH certification.

Exam Details

Exam Title: Certified Ethical Hacker (ANSI)

Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)

Number of Questions: 125

Duration: 4 hours

Availability: Prometric Prime / VUE / ECCEXAM

Test Format: Multiple Choice

Passing Score: 70%

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.

CEHv9 Recognition / Endorsement / Mapping

The National Initiative for Cybersecurity Education (NICE)

American National Standards Institute (ANSI)

Committee on National Security Systems (CNSS)

United States Department of Defense (DoD)

National Infocomm Competency Framework (NICF)

Department of Veterans Affairs

KOMLEK

MSC

What is New in the CEHV9 Course

This is the worlds most advanced ethical hacking course with 18 of the most current security domains any ethical hacker will ever want to know when they are planning to beef up the information security posture of their organization. In 18 comprehensive modules, the course covers over 270 attack technologies, commonly used by hackers.

Our security experts have designed over 140 labs which mimic real time scenarios in the course to help you "live" through an attack as if it were real and provide you with access to over 2200 commonly used hacking tools to immerse you into the hacker world.

As "a picture tells a thousand words", our developers have all this and more for you in over 2200 graphically rich, specially designed slides to help you grasp complex security concepts in depth which will be presented to you in 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 EC-Council Certified Ethical Hacker exam 312-50.

In short, you walk out the door with hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification!

Course Outline Version 9

CEHv9 consists of 18 core modules designed to facilitate a comprehensive ethical hacking and penetration testing training.

Certified Ethical Hacker

What will you learn?

Students going through CEH training will learn:

01 Key issues plaguing the information security world, incident management process, and penetration testing

02 Various types of footprinting, footprinting tools, and countermeasures

03 Network scanning techniques and scanning countermeasures

04 Enumeration techniques and enumeration countermeasures

05 System hacking methodology, steganography, steganalysis attacks, and covering tracks

06 Different types of Trojans, Trojan analysis, and Trojan countermeasures

07 Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures

08 Packet sniffing techniques and how to defend against sniffing

09 Social Engineering techniques, identify theft, and social engineering countermeasures

10 DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures

C|EH Certified Ethical Hacker

Certified Ethical Hacker

11	Session hijacking techniques and countermeasures
12	Different types of webserver attacks, attack methodology, and countermeasures
13	Different types of web application attacks, web application hacking methodology, and countermeasures
14	SQL injection attacks and injection detection tools
15	Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-fi security tools
16	Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
17	Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
18	Various cloud computing concepts, threats, attacks, and security techniques and tools
19	Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
20	Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap

EC-Council