

EC Council – CEH

Certified Ethical Hacker v10



Days: 5

Prerequisites: In order to have a successful learning experience, students should have existing knowledge of, and support experience with, networked desktop and notebook computers, as well as advanced user-level skills in Windows Vista, Windows XP, or Windows 7.

EC-Council | Accredited Training Center

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.

Description: This class (version 10) will immerse the students into an interactive environment where they will be shown 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. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. 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. 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.

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

OUTLINE:

MODULE 1 - INTRODUCTION TO ETHICAL HACKING

MODULE 2 - FOOTPRINTING AND RECONNAISSANCE

MODULE 3 - SCANNING NETWORKS

MODULE 4 - ENUMERATION

MODULE 5 - VULNERABILITY ANALYSIS

MODULE 6 - SYSTEM HACKING

MODULE 7 - MALWARE THREATS

MODULE 8 - SNIFFING

MODULE 9 - SOCIAL ENGINEERING

MODULE 10 - DENIAL-OF-SERVICE

MODULE 11 - SESSION HIJACKING

MODULE 12 - EVADING IDS, FIREWALLS, AND HONEYPOTS

MODULE 13 - HACKING WEB SERVERS

MODULE 14 - HACKING WEB APPLICATIONS

MODULE 15 - SQL INJECTION

MODULE 16 - HACKING WIRELESS NETWORKS

MODULE 17 - HACKING MOBILE PLATFORMS

MODULE 18 - IOT HACKING

MODULE 19 - CLOUD COMPUTING

MODULE 20 - CRYPTOGRAPHY

Baton Rouge | Lafayette | New Orleans

www.lantecctc.com