

Acronym/Nickname CEH		Certification Body EC-Council	
Description <p>The definition of an Ethical Hacker is very similar to a Penetration Tester. The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in the United States and most other countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target.</p> <p>The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.</p>		Certification Level Professional Covered competencies 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	
Target security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure		Requirements To achieve the Certified Ethical Hacker Certification, you must pass the CEH exam 312-50	
Authorized Testing Center: PEARSON VUE / PROMETRIC		Indicative Fee* 250 USD	Certification Schedule*
* Fees and schedules are subject to change without prior notice, please get in touch with certification body through contact details below			
Recommended/Preparatory Training Module 1: Introduction to Ethical Hacking Module 2: Footprinting Module 3: Scanning Module 4: Enumeration Module 5: System Hacking Module 6: Trojans and Backdoors Module 7: Sniffers Module 8: Denial of Service Module 9: Social Engineering Module 10: Session Hijacking Module 11: Hacking Web Servers Module 12: Web Application Vulnerabilities Module 13: Web-based Password Cracking Techniques Module 14: SQL Injection Module 15: Hacking Wireless Networks Module 16: Virus and Worms Module 17: Physical Security Module 18: Linux Hacking Module 19: Evading IDS, Firewalls, and Honeypots Module 20: Buffer Overflows Module 21: Cryptography Module 22: Penetration Testing			
Where to get more information: http://www.eccouncil.org/ceh.htm			