



Course **Certified Ethical Hacking**

Overview This class will immerse the student 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 312-50.

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 Prometric exam to receive CEH certification.

Who should attend This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

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

Duration 6 Days (6 hours per day)
Dates March 8- 13, 2010
M-S: 09:15-16:45

Instructor i-learn Instructor

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.

Course outline CEHv6 Curriculum consists of instructor-led training and self-study. The Instructor will provide the details of self-study modules to the students beginning of the class.

- Module 1: Introduction to Ethical Hacking
- Module 2: Hacking Laws
- Module 5: Scanning
- Module 6: Enumeration
- Module 7: System Hacking





Professional Education Programs



- Module 8: Trojans and Backdoors
- Module 9: Viruses and Worms
- Module 10: Sniffers
- Module 11: Social Engineering
- Module 12: Phishing
- Module 13: Hacking Email Accounts
- Module 14: Denial-of-Service
- Module 15: Session Hijacking
- Module 16: Hacking Web Servers
- Module 17: Web Application Vulnerabilities
- Module 18: Web-Based Password Cracking Techniques
- Module 19: SQL Injection
- Module 20: Hacking Wireless Networks
- Module 21: Physical Security
- Module 22: Linux Hacking
- Module 23: Evading IDS, Firewalls and Detecting Honey Pots
- Module 24: Buffer Overflows
- Module 25: Cryptography
- Module 26: Penetration Testing
- Module 27: Covert Hacking
- Module 28: Writing Virus Codes
- Module 29: Assembly Language Tutorial
- Module 30: Exploit Writing
- Module 31: Smashing the Stack for Fun and Profit
- Module 32: Windows Based Buffer Overflow Exploit Writing
- Module 33: Reverse Engineering
- Module 34: MAC OS X Hacking
- Module 35: Hacking Routers, cable Modems and Firewalls
- Module 36: Hacking Mobile Phones, PDA and Handheld Devices
- Module 37: Bluetooth Hacking
- Module 39: RFID Hacking
- Module 40: Spamming
- Module 41: Hacking USB Devices
- Module 42: Hacking Database Servers
- Module 43: Cyber Warfare- Hacking, Al-Qaida and Terrorism
- Module 44: Internet Content Filtering Techniques
- Module 45: Privacy on the Internet
- Module 46: Securing Laptop Computers
- Module 47: Spying Technologies
- Module 48: Corporate Espionage- Hacking Using Insiders
- Module 49: Creating Security Policies





Professional Education Programs



- Module 50: Software Piracy and Warez
- Module 51: Hacking and Cheating Online Games
- Module 52: Hacking RSS and Atom
- Module 53: Hacking Web Browsers (Firefox, IE)
- Module 54: Proxy Server Technologies
- Module 55: Data Loss Prevention
- Module 56: Hacking Global Positioning System (GPS)
- Module 57: Computer Forensics and Incident Handling
- Module 58: Credit Card Frauds
- Module 59: How to Steal Passwords
- Module 60: Firewall Technologies
- Module 61: Threats and Countermeasures
- Module 63: Botnets
- Module 64: Economic Espionage
- Module 65: Patch Management
- Module 66: Security Convergence
- Module 67: Identifying the Terrorist

Tuition Fee Single Participation: 2.850€
Discount Policy
Cancellation Policy

Program Registration <http://hermes.ait.gr/registrations/multiple.php?prog=86>

Contact Catherine Cynthia Protonotarios
Executive Training Manager
Tel+30 2106682806, extn 5806
Fax+302106682844
execedu@ait.edu.gr

