

Ethical Hacker | factsheet

Course Description

This course will immerse the student into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The course gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defences 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 completes this intensive course, they will have hands-on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

Study Resources

- > Over 200 hours of interactive digital courseware
- > Preloaded onto 120Gb Apple iPod Classic
- > Courseware also supplied on CD-ROMs
- > Syllabus Certified textbooks
- > 12 months email tutor support

Who Should Enrol

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

This course follows the official EC-Council syllabus

EC-Council offers the Certified Ethical Hacker Certification Exam over these channels.

- > **Exam 312-50:** Web based 'Prometric Prime' at Accredited Training Centres (ATC).
- > **Exam EC0-350:** Proctored test at Authorized Prometric Testing Centres (APTC) globally.
- > **Exam 312-50:** VUE Testing centres

Please note that the difference in the exam is only in terms of exam delivery channel and are otherwise identical in source.

Statement of Compliance

Due to the sensitive nature of the course materials, students will be asked to sign and return a statement of compliance attesting that the course will be used for legal and ethical purposes only.



Learning on the move

Combining the finest learning methods with the latest technology, our new courses are delivered by innovative coaching techniques installed on your complementary iPod or Laptop



Ethical Hacker | topics

Your CEH course maps the EC-Council accredited Syllabus and covers the following topics:

- Module 1: Introduction to Ethical Hacking
- Module 2: Hacking Laws
- Module 3: Footprinting
- Module 4: Google Hacking
- Module 5: Scanning
- Module 6: Enumeration
- Module 7: System Hacking
- 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 16: Hacking Web Servers
- Module 17: Web Application Vulnerabilities
- Module 18: Web-Based Password Cracking Techniques
- Module 19: SQL Injection
- 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 38: VoIP 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
- 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 62: Case Studies
- Module 63: Botnets
- Module 64: Economic Espionage
- Module 65: Patch Management
- Module 66: Security Convergence
- Module 67: Identifying the Terrorist



Ethical Hacker | statement of compliance

The objective of the certification 'Certified Ethical Hacker' is to introduce, educate and demonstrate hacking techniques and tools for legal security testing purposes only. Those who are certified by EC-Council in this discipline acknowledge that such certification is a mark of distinction that must be both earned and respected.

In lieu of this, all Certified Ethical Hackers pledge to fully support the Code of Ethics. Certified professionals who deliberately or intentionally violate any provision of the Code will be subject to action by a review panel, which can result in the revocation of the certification.

To this end, you will not exploit the thus acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to illegally compromise any computer system. Additionally you agree to indemnify ICS and its partners with respect to the use or misuse of these tools, regardless of intent. You agree to comply with all applicable laws and regulations in this regard.

I understand that if I engage in any inappropriate, unethical, or illegal behaviour or activity, my ICS student status will be terminated immediately and a report made to the EC Council.

Signature

Date

