

Programa de Certificación en Hacking Ético v.6 (CEH) (Certified Ethical Hacker), desarrollado por la Internacional E-Commerce Consultants (EC-Council) para proveer a la industria de personal cualificado en materia de seguridad.

Director del curso	Walter Llop Masía		
Profesor/es	Walter Llop Masía		
Duración	1 Año de acceso a plataforma E-learning EC-Council 50 Horas presenciales:	Fecha de Inicio: <i>por confirmar</i> Fecha de Fin: <i>por confirmar</i>	
Precio	2.150 €	Precio especial : 1.850 € *	Alumnos que hayan superado el curso de Introducción al Hacking ético: 1.250 €

\* Descuento aplicable según criterio.

## Descripción general del curso



El programa Ethical Hacking and Countermeasures, está orientado al profesional de la seguridad que, con experiencia en la materia, desea actualizar o mejorar sus conocimientos en seguridad informática. También, sirve como continuación del curso de **Introducción Hacking Ético CEH (Fundamentals in Information Security)** regulado por el EC-Council.

Este curso pretende "envolver" al asistente a un entorno interactivo, donde se le mostrará cómo explorar, probar, "hackear" y asegurar sus propios sistemas. El entorno intensivo del laboratorio da a cada estudiante un profundo conocimiento y experiencia práctica con los actuales sistemas de seguridad. Los estudiantes empezarán por entender cómo funcionan las defensas periféricas y posteriormente serán llevados a explorar y atacar sus propias redes; ninguna red real es dañada. Luego los estudiantes aprenden cómo los intrusos escalan privilegios y qué pasos se pueden tomar para asegurar un sistema. Los asistentes también aprenderán sobre sistemas IDS, Creación de Políticas, Ingeniería Social, Ataques DDoS, Buffers overflows, etc.

Tras la finalización del curso, el alumno que supere el 80% de la asistencia obtendrá un diploma acreditativo. Aquellos alumnos que deseen obtener la certificación CEH deberán superar el examen 312-50 en las instalaciones del centro, gracias al certificado Prometric - VUE Testing Center que posee la escuela. El pago del examen se realizará 15 días antes del mismo.

La misión del curso es educar, presentar y demostrar las herramientas de "hackeo", únicamente para propósitos de pruebas de penetración. Antes de asistir a este curso, se le pedirá que firme un acuerdo donde declara que no utilizará las habilidades recién adquiridas, para ataques ilegales o maliciosos. Y que no usará dichas herramientas en un intento de comprometer algún sistema computacional.

## Objetivos del curso

Al terminar el curso, dispondrá de los conocimientos necesarios para poder obtener la certificación CEH, si bien, la realización del curso no garantiza la superación de dicho examen.

## Material proporcionado al alumno

Documentación de apoyo.  
Acceso a la plataforma de formación online del ec-council, mediante modalidad iLearn.

## Temario del curso

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 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 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