

Curso preparatorio para la obtención de la certificación Ethical Hacking (CEH)

Temario del curso

Curso independiente de fabricante que pretende introducir, demostrar y enseñar las herramientas utilizadas por los hackers. Estas herramientas se utilizarán solo para test quedando prohibido hacer un uso malicioso de ellas ateniéndose el alumno a las responsabilidades legales en las que pudiera incurrir. Alhambra-Eidos tiene el derecho y la obligación, de comprobar que el alumno cumple el requisito de pertenecer a compañías o entidades reconocidas legalmente.

Objetivos

Con una duración de cinco días intensivos los objetivos son:

- Aprender cómo escanear, testear y asegurar los sistemas propios
- Aprender cómo trabajan las defensas perimétricas ensayando ataques sobre maquetas de los esquemas de red más habituales.
- Aprender los métodos que utilizan los intrusos para adquirir progresivamente derechos y los pasos necesarios para evitar esto.
- Aprender sobre Detección de intrusos, creación de reglas, Inteligencia Open Source, manejo de incidentes y confección e interpretación de logs de seguridad.

Dirigido a

- Profesionales, Gestores, Decisores y Responsables de IT que necesiten conocer las soluciones de Seguridad existentes hoy día.
- Profesionales pertenecientes a Compañías, entidades y organismos que quieran de manera segura aprovechar sin riesgos todo el potencial tanto de Internet como de las Intranets propias.

Prerrequisitos

Experiencia en trabajos con redes Linux, Windows o TCP/IP en general.

Módulos que contiene el curso

- Módulo 1: Introduction to Ethical Hacking
- Módulo 2: Footprinting
- Módulo 3: Scanning
- Módulo 4: Enumeration
- Módulo 5: System Hacking
- Módulo 6: Trojans and Backdoors
- Módulo 7: Sniffers

- Módulo 8: Denial of Service
- Módulo 9: Social Engineering
- Módulo 10: Session Hijacking
- Módulo 11: Hacking Web Servers
- Módulo 12: Web Application Vulnerabilities
- Módulo 13: Web Based Password Cracking Techniques
- Módulo 14: SQL Injection
- Módulo 15: Hacking Wireless Networks
- Módulo 16: Virus
- Módulo 17: Physical Security
- Módulo 18: Linux Hacking
- Módulo 19: Evading Firewalls, IDS and Honeypots
- Módulo 20: Buffer Overflows
- Módulo 21: Cryptography
- Módulo 22: Penetration Testing

Duración y horario

El Curso se desarrollará en sesiones de jornada completa de lunes a jueves (9 a 13h y de 14:30 a 19h) y el último día (viernes) en horario de mañana (8:30 a 14h).

Próximas convocatorias

La próxima convocatoria de este curso tiene previsto su comienzo el día 16 de abril de 2012 . El plazo de inscripción finaliza cinco días antes del comienzo de la misma.

Precio

2.190 Euros + IVA - Incluye comida de los cuatro días y el coste del examen de certificación.

Estructura de distribución del temario del curso

LUNES

Mañana		Tarde	
Module 00: CEH Introduction	9:00 - 9:15	Module 02: Footprinting (cont.)	14:30 - 15:30
Module 01: Introduction to Ethical Hacking	9:15 - 10:45	Descanso	15:30 - 15:45
Descanso	10:45 - 11:00	Module 03: Scanning	15:45 - 17:15
Module 02: Footprinting	11:00 - 13:00	Descanso	17:15 - 17:45
Comida	13:00 - 14:30	Module 03: Scanning (cont.)	17:45 - 19:00

MARTES

Mañana		Tarde	
Module 04: Enumeration	9:00 - 10:30	Module 05: System Hacking	14:30 - 15:30
Descanso	10:30 - 10:45	Descanso	15:30 - 15:45
Module 05: System Hacking	10:45 - 13:00	Module 05: System Hacking	15:45 - 17:15
Comida	13:00 - 14:30	Descanso	17:15 - 17:45
		Module 05: System Hacking	17:45 - 19:00

MIÉRCOLES

Mañana		Tarde	
Module 06: Trojans and Backdoors	9:00 - 10:30	Module 07: Sniffers (cont.)	14:30 - 15:15
Descanso	10:30 - 10:45	Descanso	15:15 - 15:30
Module 06: Trojans and Backdoors (cont.)	10:45 - 12:00	Module 08: Denial of Service	15:30 - 16:30
Module 07: Sniffers	12:00 - 13:00	Module 09: Social Engineering	16:30 - 17:30
Comida	13:00 - 14:30	Descanso	17:30 - 18:00
		Module 09: Social Engineering (cont.)	18:00 - 19:00

JUEVES

Mañana		Tarde	
Module 10: Session Hijacking	9:00 - 10:30	Module 12: Web Application Vulnerabilities	14:30 - 15:30
Descanso	10:30 - 11:00	Descanso	15:30 - 15:45
Module 11: Hacking Web Servers	11:00 - 13:00	Module 13: Web-based Password Cracking Techniques	15:45 - 16:45
Comida	13:00 - 14:30	Module 14: SQL Injection	16:45 - 17:45
		Descanso	17:45 - 18:00
		Module 15: Hacking Wireless Networks	18:00 - 19:00

VIERNES

Mañana	
Module 16: Virus and Worms	08:30 - 09:00
Module 17: Physical Security	09:00 - 09:30
Descanso	9:30 - 9:45
Module 18: Linux Hacking	9:45 - 11:15
Descanso	10:15-11:30
Module 19: Evading, IDS, Firewalls, and Honeypots	11:30 - 12:15
Module 20: Buffer Overflows	12:15 - 12:45
Descanso	12:45 - 13:15
Module 21: Cryptography	13:15 - 13:45
Module 22: Penetration Testing	13:45 - 14:30