



Curso

SKILL 54. HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Del 22 de septiembre al 2 de noviembre



En línea



32 horas



horas

Fecha Inicio: 22/09/2025 - Fecha Fin: 02/11/2025

Raúl Fuentes Ferrer

\$~: whoami



RAÚL FUENTES FERRER

- Security Pentester / Analista forense
- Profesor Formación Profesional Generalitat Valenciana
- Profesor Universidad Internacional de Valencia
- Profesor Universidad Castilla-La Mancha
- CHFI (Computer Hacking Forensic Investigator) / CEH (Certified Ethical Hacker) – EC-Council
- E-katec – Soluciones Informáticas
- H&B Valencia / TomatinaCON / SegurXest
- 2 vulnerabilidades CVE

<https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-hyperion-web-server>

SEGUR
XEST



HACK
& BEERS

Aprendiendo algo NUEVO todos los días!!

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Este curso tiene como finalidad proporcionar conocimientos teóricos y prácticos sobre la vulnerabilidades más comunes, las técnicas de explotación utilizadas por atacantes y las estrategias de defensa para mitigar estos riesgos.

Al finalizar el curso, los participantes serán capaces de auditar, proteger y mejorar la seguridad en entornos reales.

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Objetivos

- Capacitar a profesionales en técnicas avanzadas de hacking ético
- Simular escenarios de ataque en entornos reales controlados
- Implementar contramedidas y buenas prácticas de seguridad
- Evaluar la ciberseguridad de sistemas mediante pentesting avanzado

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Contenidos:

- ❑ **Módulo 1. Introducción y Legalidad:** Principios del hacking ético: ética y legalidad (ISO/IEC 27001, RGPD), Marco legal en España y Europa, Tipos de hackers y metodologías (OWASP, PTES)
- ❑ **Módulo 2. Reconocimiento y Fingerprinting:** OSINT avanzado (Shodan, theHarvester, Maltego), Enumeración de servicios y puertos: Nmap avanzado, Masscan, Fingerprinting de tecnologías web y servidores
- ❑ **Módulo 3. Explotación de Vulnerabilidades:** Explotación manual y automatizada (Metasploit, ExploitDB), Buffer overflows básicos y explotación en Linux, Vulnerabilidades web: SQLi, XSS, CSRF, RCE
- ❑ **Módulo 4. Evasión y Post-explotación:** Técnicas de evasión de antivirus y EDR (obfuscación, encoding, msfvenom), Persistencia y movimiento lateral, Escalada de privilegios en Windows y Linux
- ❑ **Módulo 5. Análisis de Infraestructuras Empresariales:** Análisis de seguridad en Active Directory, Enumeración LDAP, Kerberos (Pass-the-Hash, Golden Ticket)
- ❑ **Módulo 6. Hardening y Mitigación:** Hardening de sistemas y redes: benchmark CIS, firewalls, segmentación, Monitorización y respuesta: SIEM básico (Splunk, Wazuh)
- ❑ **Módulo 7. Informe de Pentesting Profesional:** Cómo elaborar informes técnicos y ejecutivos, Herramientas para documentación (Dradis, CherryTree)

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Recursos materiales:

- Plataforma de e-learning AULES del CEFIRE:
<https://aules.edu.gva.es/formaciodelprofessorat/login/index.php>
- Material del curso publicado en plataforma de e-learning.
- Software libre que se irá indicando en las sesiones.
- Es necesario que el/la participante disponga de ordenador personal con VirtualBox/VMWare y al menos 4 gigas libres de RAM para realizar con éxito las tareas del curso.

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Metodología:

- Sesiones síncronas voluntarias para resolución de dudas que quedarán grabadas.
- Realización de laboratorios y talleres para aplicación práctica al aula.
- Retos para fomentar la creatividad y participación activa de los asistentes.
- Fomento de debates en foros para participación de los asistentes y resolución de dudas.

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Criterios de evaluación:

Consulta del material del curso y realización de las actividades entregables y cuestionarios en la plataforma online.

- Realización de **una actividad obligatoria** de las propuestas (1 por módulo)
- Participación en el **Foro** del módulo con **una** entrada

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Videoconferencias

- **23/09/2025** – *Sesión síncrona Teams* - Presentación Curso – 16:00
- **07/10/2025** – *Sesión síncrona Teams* - Resolución de dudas y realización de demostraciones – 16:00

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Temporalización Contenidos

- **22/09/2025 - Módulo 1.** Introducción y Legalidad
- **28/09/2025 - Módulo 2.** Reconocimiento y Fingerprinting
- **04/10/2025 - Módulo 3.** Explotación de Vulnerabilidades
- **10/10/2025 - Módulo 4.** Evasión y Post-explotación
- **16/10/2025 - Módulo 5.** Análisis de Infraestructuras Empresariales
- **22/10/2025 - Módulo 6.** Hardening y Mitigación
- **28/10/2025 - Módulo 7.** Informe de Pentesting Profesional

HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Dudas y consultas

Curso

Raúl Fuentes – *r.fuentesferrer@edu.gva.es*



Curso

SKILL 54. HACKING ÉTICO Y CIBERSEGURIDAD PARA ENTORNOS PROFESIONALES

Del 22 de septiembre al 2 de noviembre



En línea



32 horas



horas