escuela de postgrado UPC

PRESENTACIÓN DEL CERTIFICADO

DOCENTE

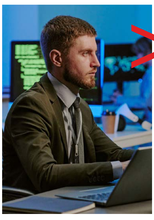
PROPUESTA ACADÉMICA

CONTÁCTANOS

Certificación

Ethical Hacking

¿Por qué estudiar la certificación en Ethical Hacking?



CERTIFICACIÓN

Al culminar satisfactoriamente y aprobar el programa, el alumno obtendrá:

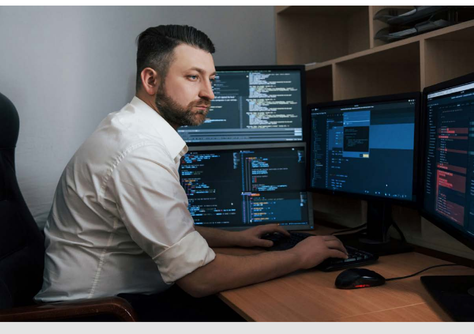
— **Certificado en Ethical Hacking,** otorgado por la Escuela de Postgrado de la UPC.

Aprendizaje práctico e intensivo

Adquiere conocimientos aplicados en evaluación de vulnerabilidades, pruebas de penetración y elaboración de reportes técnicos.

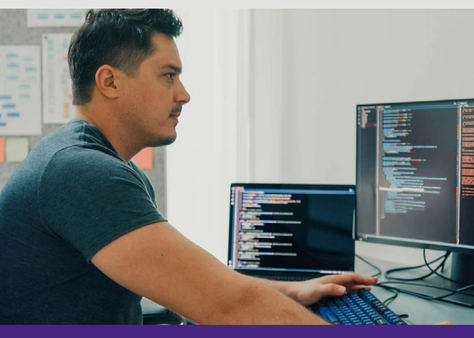
Docentes practitioners

Profesionales en ciberseguridad con experiencia en hacking ético y en proyectos reales de evaluación y protección de sistemas.



Herramientas clave

Domina las herramientas más usadas en hacking ético como Kali Linux, Metasploit, Nmap, Burp Suite y SET para realizar pruebas y proteger sistemas reales.



Certificación a distancia

Clases virtuales en vivo.

DOCENTE

Conoce más sobre nuestro docente

ROBERTO MUNAYCO

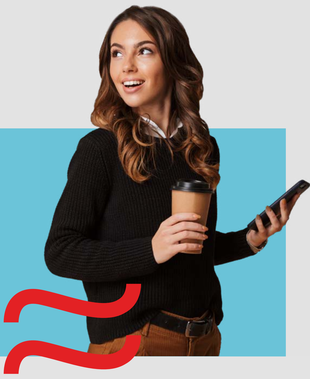
Docente de la certificación

Consultor en ciberseguridad con enfoque técnico y estratégico. Experto en la implementación en marcos de seguridad como ISO/IEC 27000 y NIST, aplicados en sectores como: banca, finanzas, industria y retail. Ha liderado CyberSOC y servicios de detección y respuesta ante incidentes. Domina hacking ético, auditorías técnicas, pentesting, evaluación de vulnerabilidades y diseño de arquitecturas seguras. Ha gestionado equipos que operan bajo marcos de seguridad ofensiva y defensiva.

*UPC se reserva el derecho de hacer cambios en el listado de especialistas.

> PROPUESTA ACADÉMICA

Malla curricular de la certificación en Ethical Hacking



1 INTRODUCCIÓN AL HACKING ÉTICO Y FUNDAMENTOS

- ¿Qué es el hacking ético?
- Tipos de hackers: White, Black, Grey hat.
- Aspectos legales y éticos.
- Fases del test de penetración.
- Fundamentos de redes: TCP/IP, puertos, protocolos.

2 RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN

- Concepto de Footprinting: pasivo vs. activo.
- Herramientas: Whois, NSlookup, Google Dorks, Shodan.
- Enumeración DNS y OSINT básico.

3 ESCANEO Y ANÁLISIS DE VULNERABILIDADES

- Escaneo de red y puertos con Nmap.
- Identificación de servicios y sistemas operativos.
- Escaneo web con Nikto.
- Introducción a vulnerabilidades comunes (OWASP Top 10).

4 EXPLOTACIÓN CON METASPLOIT

- Metasploit Framework: uso básico.
- Selección y ejecución de exploits.
- Shells y sesiones Meterpreter.
- Post-explotación básica.

5 SEGURIDAD EN APLICACIONES WEB

- Vulnerabilidades comunes: XSS, SQLi, CSRF.
- Herramientas de análisis: Burp Suite, OWASP ZAP.
- Práctica en entornos simulados (DVWA, Juice Shop).

6 SEGURIDAD EN SISTEMAS OPERATIVOS

- Enumeración en Windows y Linux.
- Análisis de usuarios, servicios y contraseñas.
- Herramientas: Netcat, John the Ripper, Hashcat.
- Conceptos de escalación de privilegios.

7 INGENIERÍA SOCIAL Y ATAQUES DE PHISHING

- Principios de ingeniería social.
- Métodos de ataque (pretexting, baiting, phishing).
- Herramientas como Social-Engineer Toolkit (SET).
- Medidas de concientización y defensa.

8 LABORATORIO FINAL Y REPORTE

- Simulación completa de pentesting en entorno controlado.
- Aplicación práctica de técnicas vistas.
- Elaboración de informe de vulnerabilidades.
- Recomendaciones y buenas prácticas.

EPG escuela de postgrado UPC

PRESENTACIÓN DEL CERTIFICADO

PROPUESTA ACADÉMICA

DOCENTE

CONTÁCTANOS

Contáctanos

giancarlo.bravo@upc.pe

postgrado.upc.edu.pe

917 326 616

Av. Cádiz 446 - 450, San Isidro