

Learn.
Hack.
Belong.



Propuesta académica

Nuestra filosofía de aprendizaje

En The Hacking Circle formamos **hackers éticos reales** para problemas reales. Nuestra metodología se basa en **cuatro pilares**:

- Aprendizaje por Experiencia (Learning by Hacking)
- Pensamiento Crítico y Mentalidad Ofensiva/Defensiva
- Laboratorios Reales y Entornos Simulados
- Comunidad, Feedback y Mentoría Constante

En The Hacking Circle **nadie aprende solo**.

- Recibirás **feedback** técnico detallado.
- Tendrás **acompañamiento de mentores** activos en la industria.
- Trabajarás en equipo y en **proyectos reales**.
- Construirás **red profesional** desde el día uno.

No vas a ser sólo alumno, vas a formar parte de un **círculo de profesionales** que te estará acompañando a lo largo de toda tu carrera.



Al finalizar tus estudios

Tendrás la posibilidad de efectuar tus prácticas en una **empresa real**, acompañado por uno de nuestros mentores.

Te enseñaremos cómo buscar **trabajo en el sector** y como atravesar **entrevistas técnicas** con éxito.

También formarás parte de nuestra **bolsa de trabajo**, así como acceso a eventos exclusivos de Ciberseguridad.



Plan de estudio

DIPLOMADO EN HACKING ÉTICO, CIBERINTELIGENCIA Y CIBERSEGURIDAD

Duración: 6 meses

Modalidad: Clases en vivo + prácticas guiadas

Fase 1: Fundamentos de Ciberseguridad y Redes

En esta fase el estudiante construye la base técnica del programa. Aprende cómo funcionan las redes, los principales protocolos (HTTP, DNS, SSH), el modelo OSI y TCP/IP, y cómo analizar tráfico básico.

Se introduce en Linux como entorno esencial para seguridad, comprendiendo estructura de archivos, permisos y comandos fundamentales. Además, comienza a utilizar Python aplicado a automatización básica.

Al finalizar esta etapa, el estudiante comprende cómo se comunican los sistemas, puede analizar tráfico simple y se desenvuelve en un entorno Linux con seguridad.

Fase 2: Reconocimiento y Análisis de Superficie de Ataque

En esta fase el estudiante aprende a pensar como un profesional de seguridad ofensiva. Se trabaja OSINT, escaneo y enumeración de servicios, identificación de versiones vulnerables y análisis de superficie de ataque. Comprende qué es un CVE, cómo se mide el riesgo y cómo interpretar hallazgos técnicos. También adquiere fundamentos sólidos sobre el funcionamiento de aplicaciones web.

Al finalizar, puede realizar un reconocimiento estructurado, identificar vulnerabilidades y documentar hallazgos con criterio técnico.

Fase 3: Seguridad en Aplicaciones Web

Esta etapa se enfoca en el análisis y explotación de vulnerabilidades web. El estudiante estudia el OWASP Top 10, incluyendo inyección SQL, XSS, fallos de autenticación y control de acceso.

Aprende a utilizar herramientas profesionales para interceptar y analizar tráfico, comprender sesiones y explotar entornos vulnerables controlados. Además, se introduce en la redacción de informes técnicos de pentesting.

Al finalizar, puede identificar y explotar vulnerabilidades web en laboratorio y redactar un informe profesional básico.



Plan de estudio

Fase 4: Seguridad en Infraestructura y Entornos Corporativos

En esta fase se aborda la seguridad en redes empresariales. El estudiante aprende cómo funciona Active Directory, la gestión de identidades y los errores de configuración más comunes.

Se trabajan técnicas de escalada de privilegios, movimiento lateral y análisis de entornos comprometidos, tanto en Linux como en Windows.

Al finalizar, comprende cómo se estructuran los ataques internos y cómo evaluar riesgos en infraestructuras corporativas.

Fase 5: Defensa, SOC y Respuesta ante Incidentes

Esta etapa desarrolla la visión defensiva del profesional. El estudiante aprende cómo funciona un SOC, qué es un SIEM y cómo se gestionan alertas.

Se introducen conceptos de MITRE ATT&CK, respuesta a incidentes, análisis básico de logs y fundamentos de threat hunting. También se abordan principios esenciales de seguridad en entornos cloud.

Al finalizar, el estudiante comprende cómo detectar actividad maliciosa y cómo se gestiona un incidente en un entorno real.

Fase 6: Proyecto Profesional y Estrategia de Inserción Laboral

En la fase final el estudiante ejecuta un proyecto integral de seguridad, aplicando metodología profesional desde la definición de alcance hasta la entrega del informe.

Paralelamente, trabaja en su posicionamiento laboral: construcción de CV técnico, optimización de LinkedIn, desarrollo de portfolio, simulaciones de entrevistas y estrategia de búsqueda de empleo.

Al finalizar el programa, el estudiante cuenta con un proyecto documentado, un perfil profesional optimizado y una estrategia concreta para ingresar al mercado laboral en ciberseguridad.



Aprende acompañado

En The Hacking Circle nadie estudia solo. Nuestras clases son **en vivo** con profesores con trayectoria en la industria. Sin embargo, todo quedará grabado para poder combinar el aprendizaje con tu vida laboral.



Certificación

Al finalizar y aprobar el trabajo de fin de curso, se emitirá el certificado:

Diplomado en Ciberseguridad, Ciberinteligencia y Hacking ético.

Para todos nuestros cursos se emite certificación oficial, con firma digital del director académico, cantidad de horas de cursada y QR para su comprobación.

Adicionalmente, se les solicitará a las empresas partner que escriban una recomendación para cada uno de los alumnos que estuvieron involucrados en las prácticas profesionales.



listo para Unirte al Círculo?

More info:
www.hackingcircle.com



Contact:
hello@hackingcircle.com