DIPLOMATURA EN

CIBERSEGURIDAD

RED TEAM



INSTITUTO
LEONARDO DA VINCI

100% ONLINE

CLASES EN VIVO

DURACIÓN: 6 MESES

Hacking ético y evaluación
de vulnerabilidades.

Fundamentación

Hacking ético, pentesting y evaluación de vulnerabilidades.

¿POR QUÉ ESTA FORMACIÓN?

En un mundo cada vez más digitalizado, gobiernos, empresas y usuarios están expuestos a amenazas cibernéticas que evolucionan constantemente. Esta diplomatura brinda herramientas para anticipar y detectar riesgos, evaluar vulnerabilidades y documentar hallazgos que contribuyan a mejorar la seguridad.

AL FINALIZAR, VAS A PODER:

- Comprender los fundamentos de la ciberseguridad y del hacking ético.
- Aplicar técnicas de reconocimiento, exploración y análisis de vulnerabilidades.
- Utilizar herramientas de pentesting en entornos de práctica y pruebas autorizadas.
- Documentar resultados y elaborar informes con recomendaciones de seguridad.

Salida Laboral

Red Team Jr.
Participación en equipos que simulan ataques para detectar fallos de seguridad.

Pentester Jr.
Pruebas controladas sobre sistemas, redes y aplicaciones; detección y reporte de vulnerabilidades.

Application Security Analyst Jr.
Evaluación de aplicaciones, integraciones y arquitecturas desde la seguridad.

Hacking ético: detección y documentación profesional de vulnerabilidades, con recomendaciones de mejora. Ámbitos: empresas privadas, organismos públicos, consultoras y ejercicio independiente en banca, salud, energía, tecnología, retail y startups.

CERTIFICACIÓN

Avales y certificaciones

Certificación final: Diplomatura en Ciberseguridad Red Team.

CERTIFICACIÓN NACIONAL

Cámara Argentina de Formación Profesional y Capacitación Laboral.
Resolución N° 2517/17.
Certificación arancelada.

CERTIFICACIÓN INTERNACIONAL

OIEP - Organización Internacional para la Educación Permanente.
Resolución IP3 N° 427 C/22.
Certificación arancelada.

AVAL Y CERTIFICACIÓN AAPGRA

Asociación Argentina de Peritos Grafólogos y Ciencias Forenses.
Resolución N° 252/C25.
Certificación arancelada.

Código QR para verificar la autenticidad de la certificación y el cumplimiento de los requerimientos académicos.

PLAN DE ESTUDIO

Contenido

8 módulos para recorrer las etapas de una evaluación de seguridad.

MÓDULO 1

Introducción

Qué es la ciberseguridad y sus ramas. Clasificación de perfiles (sombreros). Hacking ético y tipos de hacking. Instalación de VirtualBox y Kali Linux. Primeros comandos. Concientización. Pentest o pentesting y sus modalidades.

MÓDULO 2

Reconocimiento

Fases, alcance, reglas y objetivo a escanear. Importancia de la documentación y herramientas. Reconocimiento de tecnologías. Google dorking y Shodan. Búsqueda de subdominios. Códigos de respuesta y comprobación de URLs activas con HTTPX y Aquatone. Escaneo de puertos y servicios activos; documentación de servicios, tecnologías y puertos. Búsqueda de directorios activos. Extracción de URLs. Fuzzing y extensiones.

PLAN DE ESTUDIO

Contenido

8 módulos para recorrer las etapas de una evaluación de seguridad.

MÓDULO 3

Exploración y escaneo

Herramientas de desarrollador. Métodos HTTP y headers. Instalación de Nessus. Escaneo de infraestructura y web. Nmap, WPScan, Nikto, Nuclei y ZAP: instalación y escaneo.

MÓDULO 4

Enumeración y análisis de vulnerabilidades

Explicación de la fase. OWASP Top 10 para aplicaciones web.

MÓDULO 5

Configuraciones

Configuración de ZAP y Burp Suite. Certificados y uso de proxy. Recorrido por Burp Suite y ZAP. Intruder, Repeater, Decoder, Collaborator y extensiones.

PLAN DE ESTUDIO

Contenido

8 módulos para recorrer las etapas de una evaluación de seguridad.

MÓDULO 6

Explotación

Resultados de escaneos. SearchSploit, Rapid7 y ExploitDB. Toma de subdominios. TL, SSL y HSTS. MITM con Wireshark. Clickjacking. Fuerza bruta. Enumeración de usuarios. DoS y DDoS. Rate limit. Mail spamming. IDORs y errores de lógica. Criptografía y Hashcat. JWT y parámetros.

Inyección HTML. XSS reflejado, DOM, Self XSS, almacenado y blind. Herramientas KXSS y Dalfox. Contaminación de parámetros HTTP. CORS. Inyección SQL y SQLMap. CSRF. LFI. Directory traversal. Metasploit. RCE. SSRF. Open redirect. Race conditions. CRLF y POST.

PLAN DE ESTUDIO

Contenido

8 módulos para recorrer las etapas de una evaluación de seguridad.

MÓDULO 7

Post explotación

Aumento de privilegios y de criticidad. Toma de control de cuenta. Bug bounty, laboratorios y criticidades.

MÓDULO 8

Informe

Generación del informe de resultados.

EQUIPO DOCENTE

Docente

Experiencia en hacking ético, pentesting y Red Team.



MARCOS SUÁREZ

Experto universitario
en Hacking Ético.

ESPECIALIDAD

Ciberseguridad,
pentesting y Red Team.

PERFIL PROFESIONAL

- Analista en ciberseguridad, pentesting y Red Team.

- Bug bounty: búsqueda y reporte de vulnerabilidades.

INFORMACIÓN DE CURSADO

PREPARATE PARA EVALUAR LA SEGURIDAD CON HACKING ÉTICO

MODALIDAD

100% online

DURACIÓN

6 meses

CURSADO

Clases semanales en vivo por Google Meet

RECURSOS DE APRENDIZAJE

Campus virtual y grupos de apoyo

Pruebas de seguridad, laboratorios e informes.

Diplomatura en Ciberseguridad

Red Team