Diplomado en Hacking Ético y Ciberseguridad

Objetivo: Aprenderás simulando, atacando y defendiendo una infraestructura corporativa real. Pasa del escaneo básico a convertirte en el Arquitecto de Seguridad que exigen las grandes empresas de hoy.

Plan de Evaluación: Curso presencial práctico mediante la realización de ejercicios en clase y evaluadas por Ingeniería Digital CA.

Duración del Curso: 176 Horas Académicas de 45 minutos cada hora. 44 Clases

Perfil del Estudiante: Estudiantes o profesionales de Informática, Programadores o afines a la Ciberseguridad

Contenido del Curso

Módulo 1: Infraestructura as a Code (IaC) y Reconocimiento Ofensivo Avanzado

Objetivo: Nivelación táctica, dominio de la terminal, despliegue de laboratorios e inteligencia de amenazas.

Nodos Core	Contenido y Laboratorios
1.1 a 1.2	Bootcamp Táctico en Linux y Despliegue de Infraestructura como Código (Vagrant).

Nodos Core	Contenido y Laboratorios
1.3 a 1.4	Inteligencia de Fuentes Abiertas (OSINT), Anatomía del Tráfico TCP/IP y Ceguera de Red (Wireshark).
1.5 a 1.6	Descubrimiento Activo, Evasión Perimetral (Nmap) y Enumeración de Servicios (DNS, SMB, RPC).
1.7 a 1.8	Gestión de Vulnerabilidades y Redacción del Informe Ejecutivo C-Level (Base normativa ISO 27001).

Módulo 2: Brecha de Perímetro y Explotación de Sistemas Base

Objetivo: Obtener el primer acceso, transicionar del reconocimiento a la explotación de servicios en red.

Nodos Core	Contenido y Laboratorios
2.1 a 2.2	Explotando Protocolos Core (FTP, SSH) e Introducción al Hacking Web v1 (OWASP Top 10 Básico).

Nodos Core	Contenido y Laboratorios
2.3 a 2.4	Armamento Táctico (Metasploit, Payloads) y Escalada de Privilegios Local (Linux/Windows v1).

Módulo 3: Infiltración Moderna (Aplicaciones Web, APIs y Contenedores)

Objetivo: Auditar el ecosistema actual empresarial basado en microservicios y despliegues en la nube.

Nodos Core	Contenido y Laboratorios
3.1 a 3.2	Hacking Web v2 (Lógica de Negocios, APIs, JWT) y el Ecosistema Docker (IaC v2).
3.3 a 3.4	Rompiendo Contenedores (Docker Escape), Auditoría Cloud (AWS) y Evasión de Defensas (WAF).

Módulo 4: Operaciones de Red Team y el Dominio Corporativo

Objetivo: Simulación de ataques avanzados persistentes dentro de la red corporativa interna.

Nodos Core	Contenido y Laboratorios
4.1 a 4.2	Introducción a Active Directory y Envenenamiento de Red Interna (Movimiento Lateral, Kerberoasting).
4.3 a 4.4	Escalada de Privilegios en Dominio (BloodHound) y Persistencia Silenciosa (Evasión de Antivirus).

Módulo 5: Ciberresiliencia, SOC y Gobierno Corporativo

Objetivo: Formación del Arquitecto Defensivo y Auditor. Triage, Respuesta a Incidentes y Auditoría Normativa.

Nodos Core	Contenido y Laboratorios
5.1 a 5.2	Operaciones Blue Team (Ingesta de Logs, Splunk/Wazuh) y Simulacro Vivo de Respuesta a Incidentes.

Nodos Core	Contenido y Laboratorios
5.3 a 5.4	Gobierno del SGSI (ISO 27001) y Sustentación del Entregable Maestro ante la "Junta Directiva".

Entregables y Criterios de Aprobación

Para obtener la titulación, el estudiante deberá entregar **Informes Ejecutivos** al finalizar cada módulo, culminando en el **Entregable Final** del Módulo 5, el cual consiste en la auditoría completa (Red Team) y propuesta de remediación (Blue Team) de la infraestructura corporativa simulada.