HTTPS://ESCUELADELHACKER.COM/

Profesional experto en Ciberseguridad y Hacking Ético Empresarial

8 ESPECIALIZACIONES POR UN SOLO PRECIO

$7,990 MXN / $460 USD

4 Mensualidades de $1,997.50 MXN / 115 USD

ACCESO 24/7 POR 90 DÍAS

Disfruta de **acceso ilimitado las 24 horas, los 7 días de la semana durante 90 días** a contenido, videos, materiales, recursos y entorno de práctica.

CONTENIDO COMPLETO INCLUIDO

Acceso total a **manuales, videos, descargables, material técnico y rutas de aprendizaje** para avanzar a tu ritmo con una experiencia integral.

MÁQUINA KALI DE ALTO PERFORMANCE

Obtén acceso a una **máquina Kali Linux lista para trabajar, optimizada y de alto rendimiento**, preparada para prácticas ofensivas reales desde el primer momento.

ENTORNO LISTO PARA PRACTICAR

Entra a un ecosistema diseñado para aprender de verdad con **laboratorios, escenarios ofensivos y acceso inmediato sin configuraciones complejas**.

Para más información e inscripciones escribe a **ventas@escueladelhacker.com**

PROFESIONAL EXPERTO EN CIBERSEGURIDAD Y HACKING ÉTICO EMPRESARIAL

Plan de estudios completo en ciberseguridad, pentesting, explotación, post-explotación, pivoting, Active Directory y ATM

Un recorrido técnico, progresivo y estructurado que integra fundamentos profesionales, análisis de servicios, explotación de infraestructura, escalada de privilegios, pivoting, seguridad web, compromiso de entornos Windows, seguridad en ATM.

Enfoque progresivo

Desde fundamentos y metodología hasta explotación avanzada, movimiento lateral y dominio de entornos empresariales.

Orientación práctica

Incluye laboratorios, técnicas reales, escenarios ofensivos y ejercicios alineados con situaciones profesionales.

Desarrollo profesional

Diseñado para construir criterio técnico, visión ofensiva y capacidad de documentar hallazgos con enfoque ejecutivo y técnico.

ESPECIALIZACIÓN 1

Fundamentos Profesionales en Ciberseguridad y Pentesting Realista

Base conceptual, ética, metodológica y profesional para construir una carrera sólida en seguridad ofensiva.

- **Formación Realista y Progresiva: te Prepara para el Mundo Real**
  Evolución estructurada de competencias, madurez técnica por fases y desarrollo de criterio para entornos ofensivos reales.
- **Programa de Impulso Profesional – Promovemos tu CV**
  Construcción de perfil técnico, portafolio profesional, narrativa de experiencia y posicionamiento frente al mercado laboral.
- **Preparación Intensiva para certificaciones internacionales**
  Hábitos de estudio, organización de objetivos, resolución de retos complejos y fortalecimiento de pensamiento técnico orientado a certificación.
- **Método de aprendizaje de la Certificación**
  Modelo basado en práctica guiada, repetición técnica, consolidación progresiva y aprendizaje centrado en escenarios.
- **"Menos libros, más práctica" Aprende seguridad ofensiva ejecutando ataques**
  Desarrollo de mentalidad ofensiva, comprensión de vectores de ataque y análisis del impacto operativo de cada técnica.
- **La Mejor Formación Técnica de Ciberseguridad en Habla Hispana**
  Accesibilidad, profundidad académica, claridad pedagógica y alineación con necesidades reales del mercado hispanohablante.
- **Fundamentos Teóricos en Ciberseguridad**
  Principios esenciales de confidencialidad, integridad y disponibilidad, modelos de seguridad y nociones de arquitectura defensiva.
- **Fundamentos Técnicos Iniciales**
  Conceptos base de redes, sistemas, servicios, autenticación, permisos, exposición de activos y superficie de ataque.
- **Pentesting y Hacking Ético**
  Definición, objetivos, fases de una prueba profesional, delimitación de alcance y diferencias frente a otras actividades ofensivas.
- **Conceptos Legales y Éticos del Hacking**
  Autorización, responsabilidad profesional, límites operativos y principios éticos aplicados a ejercicios de seguridad ofensiva.
- **Comprendiendo los CVEs y Estándares de Vulnerabilidades**
  Identificación pública de fallas, taxonomías de referencia, trazabilidad de debilidades y lectura contextual de exposiciones conocidas.
- **Clasificación de Criticidad de Vulnerabilidades**
  Valoración de impacto, probabilidad de explotación, contexto del negocio y priorización basada en riesgo real.
- **Reporte y Normativas en Pentesting**
  Estructura de informe, redacción de hallazgos, evidencia técnica, lenguaje ejecutivo y coherencia entre hallazgo, riesgo y recomendación.
- **Guías y Estándares Profesionales en Ciberseguridad para Pentesters**
  Marcos de referencia, buenas prácticas, disciplina metodológica y alineación con expectativas de clientes y organizaciones.

Algunas herramientas, sin limitarse a:

Kali Linux, Nmap, Wireshark, Burp Suite, Nessus, OpenVAS, Netcat, tcpdump, Nikto, WhatWeb, documentación técnica, metodologías de reporte, matrices de criticidad, CVSS, checklists de evaluación y estándares de pentesting.

ESPECIALIZACIÓN 2

Técnicas de Exploración y Análisis de Servicios en Pentesting

Dominio operativo del entorno de trabajo y de las técnicas esenciales para reconocimiento, descubrimiento y evaluación inicial.

- **Uso de Kali Linux para Exploración y Análisis de Servicios en Entornos Vulnerables**
  Comprensión del entorno operativo, organización del sistema, flujo de trabajo ofensivo y preparación técnica del laboratorio.
- **Visualización de Archivos en Kali Linux**
  Lectura de información local, interpretación de contenidos, revisión rápida de evidencias y análisis básico de archivos.
- **Moviéndose a Través del Sistema de Archivos**
  Navegación eficiente, estructura jerárquica, ubicación de recursos relevantes y comprensión del contexto del sistema.
- **Creación de Directorios**
  Organización de evidencias, segmentación del trabajo por objetivo y construcción de una metodología ordenada.
- **Manejo de Directorios con Espacios en el Nombre**
  Buenas prácticas de manipulación de rutas, sintaxis correcta y prevención de errores operativos durante la ejecución.
- **Eliminación de Directorios**
  Gestión ordenada del entorno de trabajo, control de residuos técnicos y cuidado en operaciones de modificación local.
- **Búsqueda de Archivos en Kali Linux**
  Localización eficiente de información, rastreo de rutas relevantes y clasificación de artefactos de interés.
- **Localización de Comandos en el Sistema**
  Comprensión del entorno de ejecución, resolución de rutas y validación de componentes disponibles en el sistema.
- **Búsqueda Rápida de Archivos en el Sistema**
  Recuperación ágil de información, mejora de tiempos operativos y análisis preliminar de contenidos locales.
- **Búsqueda Avanzada de Archivos en el Sistema**
  Filtrado por contexto, patrones de búsqueda, reconocimiento de configuraciones y localización de artefactos estratégicos.
- **Descubriendo la Superficie de Ataque: Escaneo Directo de Puertos**
  Identificación de exposición, validación de disponibilidad de servicios y análisis inicial del mapa técnico del objetivo.
- **Verificación de Puerto en un Host Remoto**
  Comprobación puntual de accesibilidad, análisis de respuesta y evaluación inicial de conectividad remota.
- **Modo Escucha en Puertos TCP/UDP**
  Comprensión de sesiones, recepción de conexiones, observación de tráfico básico y validación de comunicaciones.
- **Consulta Local de Exposiciones y Vulnerabilidades**
  Correlación de versiones, análisis de fallas conocidas, interpretación contextual y priorización de vectores potenciales.
- **Detección de Puertos y Servicios Activos**
  Enumeración de servicios, reconocimiento de roles funcionales y construcción del perfil técnico del objetivo.
- **Transferencia de Archivos entre el atacante y el objetivo**
  Intercambio de evidencias, movimiento controlado de archivos y comprensión de vectores de transferencia en laboratorio.
- **Evaluación Avanzada de Vulnerabilidades Mediante Scripts**
  Análisis automatizado, validación de exposición y uso de lógica de evaluación para identificar debilidades iniciales.
- **Escaneo Automatizado para Identificación de Exposiciones**
  Detección acelerada de debilidades, cobertura amplia y priorización temprana del esfuerzo ofensivo.
- **Exploración de Directorios y Archivos en un Servidor Web**
  Descubrimiento de rutas sensibles, análisis de recursos públicos y evaluación de configuraciones expuestas.
- **Fuerza Bruta y Ataques de Credenciales – Explotando Autenticaciones Mal Implementadas**
  Patrones de autenticación débil, reutilización de credenciales, validación de acceso y entendimiento del riesgo asociado.
- **Uso de Nano en Pentesting**
  Edición rápida de contenido, ajuste de configuraciones, creación de notas y apoyo a actividades del flujo ofensivo.
- **Escaneo de Vulnerabilidades en entorno local y nube**
  Visibilidad técnica, detección preliminar de riesgos y comparación entre contextos de análisis internos y remotos.
- **Notas del Pentester: El Arte de Documentar Bitácoras**
  Registro ordenado, trazabilidad de evidencias, cronología de acciones y generación de material útil para reporte técnico.
- **Laboratorios Prácticos**
  Aplicación progresiva de conceptos, repetición técnica y consolidación de habilidades mediante entornos controlados.
- **Introducción a los Labs**
  Objetivos, dinámica de resolución, interpretación de escenarios y metodología para abordar ejercicios ofensivos.

Algunas herramientas, sin limitarse a:

Kali Linux, Nmap, Netcat, Socat, Wireshark, tcpdump, telnet, curl, wget, ss, netstat, find, locate, grep, awk, sed, nano, scripts de enumeración, analizadores de banners, escáneres de puertos y herramientas de transferencia de archivos.

ESPECIALIZACIÓN 3

Descubrimiento, Análisis de Vulnerabilidades y Explotación de Servicios de Red

Explotación ofensiva de protocolos y servicios expuestos en infraestructura, con enfoque práctico en red team y pentesting realista.

- **Laboratorio Práctico: Infiltración Estratégica en Infraestructura FTP**
  Análisis de configuraciones expuestas, acceso indebido, validación de permisos inseguros y exposición de información sensible.
- **Laboratorio Práctico: Explotación de Servicios SSH para Control Remoto no Autorizado**
  Evaluación de autenticación, debilidades de acceso remoto y consecuencias operativas de una administración insegura.
- **Laboratorio Práctico: Manipulación del Correo Corporativo: Ataque a Infraestructura SMTP**
  Exposición del servicio de correo, abuso de funciones abiertas y entendimiento del impacto sobre comunicaciones institucionales.
- **Laboratorio Práctico: SNMP como Vector de Información Estratégica**
  Extracción de información de inventario, reconocimiento de topología y filtrado de datos sensibles de administración.
- **Laboratorio Práctico: Bases de Datos al Descubierto: Acceso No Autorizado a Información Crítica**
  Debilidades en exposición de datos, privilegios inseguros y riesgos de acceso a información estructurada de negocio.
- **Laboratorio Práctico: Mapeo y Exfiltración en Redes de Almacenamiento Desprotegidas**
  Reconocimiento de recursos compartidos, acceso indebido a almacenamiento y análisis del riesgo de fuga de información.
- **Laboratorio Práctico: Hackeando la Memoria del Backend: Intrusión Avanzada en Tiempo Real**
  Comprensión de exposición de datos en memoria, recuperación de información sensible y análisis contextual del hallazgo.
- **Laboratorio Práctico: Arquitectura Expuesta – Análisis Estratégico de Servicios SMB**
  Identificación de recursos compartidos, revisión de niveles de exposición y entendimiento de vectores de acceso lateral.
- **Laboratorio Práctico: Acceso Invisible – Comprometiendo Infraestructuras vía SMB**
  Validación de acceso no autorizado, exploración de rutas internas y aprovechamiento de configuraciones débiles.
- **Laboratorio Práctico: Explotación FTP**
  Cadena de ataque sobre servicios de transferencia, abuso de permisos y manipulación de información accesible.
- **Laboratorio Práctico: Fuerza Bruta SSH**
  Evaluación de robustez en credenciales, patrones de autenticación pobre y consecuencias de acceso repetitivo exitoso.
- **Laboratorio Práctico: Enumeración SNMP**
  Obtención de metadatos, visibilidad de configuración y relación entre monitoreo inseguro y exposición operativa.
- **Laboratorio Práctico: Ataque a MySQL**
  Acceso a estructuras de datos, revisión de privilegios inseguros y explotación de configuraciones débiles en bases de datos.
- **Conclusión Técnica: Descubrimiento, Análisis y Explotación de Servicios de Red**
  Síntesis del compromiso de servicios de red, correlación entre exposición, abuso funcional y riesgo operacional en infraestructura.

Algunas herramientas, sin limitarse a:

Nmap, Netcat, Hydra, Medusa, smbclient, enum4linux, CrackMapExec, snmpwalk, snmp-check, ftp, lftp, ssh, mysql client, rpcclient, showmount, tcpdump, Wireshark, scripts de enumeración, analizadores de servicios y herramientas de validación de credenciales.

ESPECIALIZACIÓN 4

Post-Explotación: Dominando la Escalada de Privilegios

Técnicas para elevar privilegios, recuperar credenciales y transformar accesos limitados en control total del objetivo.

- **Escalada de Privilegios**
  Fundamentos, objetivos, diferencia entre acceso inicial y control elevado, y comprensión del impacto de una mala gestión de privilegios.
- **Laboratorio Práctico: Escalada de Privilegios por Descifrado de Hashes**
  Análisis de credenciales protegidas, debilidades en almacenamiento y conversión de material sensible en acceso operativo.
- **Laboratorio Práctico: Escalada de Privilegios por Exposición de Claves SSH**
  Revisión de llaves expuestas, herencia de confianza indebida y abuso de mecanismos de autenticación persistente.
- **Laboratorio Práctico: Escalada de Privilegios Aprovechando Binarios Débiles**
  Identificación de ejecuciones inseguras, abuso de permisos heredados y ampliación del nivel de control local.
- **Laboratorio Práctico: Escalada de Privilegios por Abuso de Cron Jobs**
  Persistencia programada, ejecución privilegiada insegura y relación entre automatización débil y elevación de privilegios.
- **Laboratorio Práctico: Explotación Web para Escalación de Privilegios**
  Puente entre vulnerabilidades web y control del sistema, ampliación de acceso y abuso de confianza entre capas.
- **Conclusión Técnica: Escalada de Privilegios y Gestión de Credenciales**
  Visión integral sobre cómo credenciales, configuraciones débiles y automatismos inseguros permiten tomar control total del objetivo.

Algunas herramientas, sin limitarse a:

LinPEAS, Linux Exploit Suggester, GTFOBins, John the Ripper, Hashcat, ssh2john, cron, sudo, find, getcap, pspy, herramientas de enumeración local, análisis de permisos y revisión de credenciales expuestas.

ESPECIALIZACIÓN 5

Técnicas de Pivoting y Movimiento Lateral

Acceso a redes internas, tránsito entre segmentos y expansión del compromiso mediante túneles, reenvíos y técnicas de salto.

- **Introducción al Pivoting y Movimiento Lateral**
  Conceptos clave, objetivos estratégicos, importancia del acceso intermedio y expansión progresiva dentro de una infraestructura.
- **Laboratorio Práctico: Pivoting con Túnel Dinámico SSH para Acceso a Redes Internas**
  Canalización de tráfico, acceso a segmentos no visibles inicialmente y ampliación del reconocimiento desde un punto comprometido.
- **Laboratorio Práctico: Pivoting con Reenvío de Puertos SSH hacia Servicios Internos**
  Exposición controlada de servicios internos, encapsulamiento de acceso y alcance técnico sobre recursos restringidos.
- **Laboratorio Práctico: Pivoting tipo VPN para Movimiento Lateral Total**
  Consolidación de presencia interna, alcance completo a subredes y acceso ofensivo extendido en entornos segmentados.
- **Conclusión Técnica: Técnicas de Pivoting y Movimiento Lateral**
  Comprensión del tránsito interno, la importancia del host pivote y el valor ofensivo de encadenar accesos para ampliar el compromiso.

Algunas herramientas, sin limitarse a:

SSH, ProxyChains, Chisel, Ligolo, Socat, Netcat, túneles SOCKS, reenvío local y remoto de puertos, rutas estáticas, agentes de pivoting, clientes VPN, escaneo a través de host pivote y herramientas de reconocimiento interno.

ESPECIALIZACIÓN 6

Descubrimiento, Análisis de Vulnerabilidades y Explotación de Servicios Web

Cobertura integral de reconocimiento web, fallas de desarrollo, explotación ofensiva y uso profesional de plataformas de análisis HTTP.

- **Introducción al Descubrimiento, Análisis de Vulnerabilidades y Explotación de Servicios Web**
  Panorama general de la seguridad web, flujo ofensivo, identificación de superficie expuesta y comprensión de aplicaciones vulnerables.
- **Relación: Laboratorios del Módulo vs OWASP Top 10**
  Vinculación entre escenarios prácticos y categorías de riesgo ampliamente reconocidas en seguridad de aplicaciones.
- **Laboratorio Práctico: Descubrimiento de Directorios Web**
  Identificación de rutas ocultas, exposición de recursos sensibles y entendimiento de la arquitectura funcional de la aplicación.
- **Laboratorio Práctico: Funcionalidades Mal Diseñadas y Directorios Públicos**
  Errores de diseño, lógica insegura y exposición de contenidos por controles inexistentes o deficientes.
- **Laboratorio: Análisis de Vulnerabilidades Web**
  Revisión integral de comportamiento, análisis de entradas y respuestas, y correlación entre debilidad técnica e impacto.
- **Lógica Formal y Álgebra Booleana**
  Bases lógicas necesarias para comprender validaciones, filtros, condicionales y manipulación de parámetros en aplicaciones.
- **Bases de Datos Relacionales (RDBMS)**
  Modelo relacional, organización de la información y relación entre aplicaciones y almacenamiento estructurado.
- **Laboratorio Práctico: RFI (Remote File Inclusion) – Cargando Código Malicioso Remoto**
  Incorporación insegura de contenido externo y compromiso de la lógica de ejecución del lado servidor.
- **Laboratorio Práctico: Open Redirect – Redireccionando Víctimas a Sitios Maliciosos**
  Abuso de flujos de navegación, confianza del usuario y manipulación de rutas para fines maliciosos.
- **Laboratorio Práctico: Brute Force & Credential Stuffing – Rompiendo Autenticaciones con Fuerza Bruta**
  Ataques contra autenticación, debilidad de contraseñas, reutilización de credenciales y compromiso de cuentas.
- **Laboratorio Práctico: IDOR (Insecure Direct Object References) – Acceso No Autorizado a Datos Privados**
  Ruptura del control de acceso, manipulación de identificadores y exposición de información entre usuarios.
- **Laboratorio Práctico: Sensitive Information Disclosure – Exposición de Información Confidencial**
  Divulgación involuntaria de datos sensibles, malas configuraciones y fuga de información relevante para el atacante.
- **Laboratorio Práctico: Configuración Inicial de Burp Suite**
  Comprensión del flujo HTTP, preparación del entorno de análisis y visualización de tráfico entre cliente y aplicación.
- **Lenguaje SQL (Structured Query Language)**
  Consultas, manipulación de datos, interacción con tablas y comprensión del impacto de una consulta insegura.
- **Ingeniería del Software (Malas Prácticas de Desarrollo)**
  Errores comunes de diseño e implementación, ausencia de validaciones y consecuencias de una seguridad débil desde origen.
- **Información y Codificación**
  Representación de datos, transformación de entradas, formatos comunes y relevancia para análisis ofensivo y evasión básica.
- **Laboratorio Práctico: SQL Injection – Explotación de Consultas**
  Manipulación de consultas, validación insuficiente de entradas y acceso no autorizado a información persistente.
- **Laboratorio Práctico: XSS – Inyectando Código en Respuestas Dinámicas**
  Ejecución de contenido no confiable, abuso del contexto del usuario y efectos sobre sesiones y navegación.
- **Laboratorio Práctico: Command Injection – Control Total del Sistema**
  Ruptura de límites entre aplicación y sistema operativo, ejecución de instrucciones no previstas y toma de control funcional.
- **Laboratorio Práctico: File Upload Vulnerability – Subiendo Archivos Peligrosos**
  Validaciones insuficientes, carga de contenido malicioso y abuso del almacenamiento expuesto por la aplicación.
- **Laboratorio Práctico: LFI (Local File Inclusion) – Accediendo a Archivos Sensibles**
  Acceso indebido a recursos locales, revelación de configuraciones y obtención de información interna del sistema.
- **Laboratorio Práctico: Interceptación HTTP con Burp Suite (Análisis y Mapeo)**
  Inspección de solicitudes y respuestas, mapeo de funcionalidad y observación de parámetros clave de la aplicación.
- **Uso de Repeater en Burp Suite**
  Repetición controlada de peticiones, prueba de variaciones y análisis fino del comportamiento del servidor.
- **Laboratorio Práctico: Ataque de Fuerza Bruta con Intruder en Burp Suite**
  Automatización de pruebas de entrada, validación masiva de parámetros y análisis de respuestas diferenciales.
- **Tutorial: Uso de Repeater en Burp Suite**
  Profundización en análisis manual, ajuste de parámetros y exploración lógica de funcionalidades vulnerables.
- **Laboratorio Práctico: Decodificación y Codificación con Burp Suite Decoder**
  Transformación de datos, interpretación de formatos y apoyo al análisis de entradas y salidas de la aplicación.
- **Laboratorio Práctico: Análisis de Diferencias con Burp Comparer**
  Comparación de respuestas, identificación de cambios sutiles y apoyo a la detección de comportamientos anómalos.
- **Descubrimiento y Explotación de Servicios Web**
  Integración de reconocimiento, explotación, análisis de lógica insegura y consolidación del compromiso de aplicaciones web.

Algunas herramientas, sin limitarse a:

Burp Suite, Repeater, Intruder, Decoder, Comparer, Gobuster, Dirsearch, Dirb, Nikto, SQLmap, curl, wget, ffuf, navegadores con extensiones de análisis, proxys interceptores, validadores HTTP, fuzzing web, utilidades de codificación y herramientas de inspección de parámetros.

ESPECIALIZACIÓN 7

Descubrimiento, Análisis de Vulnerabilidades y Explotación de Infraestructura Windows (Active Directory)

Reconocimiento, abuso de servicios, captura de credenciales, escalada y control ofensivo de entornos corporativos Windows.

- **INTRODUCCIÓN: Active Directory y su Rol en Pentesting**
  Arquitectura básica, importancia del directorio en empresas, relaciones de confianza y superficie de ataque en entornos Windows.
- **Laboratorio Práctico: Shadow SMB – Explorando Recursos Ocultos en la Red**
  Descubrimiento de recursos compartidos, revisión de exposición y análisis de accesos no controlados dentro del dominio.
- **Laboratorio Práctico: DNS Recon – Descubriendo Secretos del Directorio Activo**
  Reconocimiento de nombres, resolución interna, descubrimiento de activos y visibilidad de la infraestructura del dominio.
- **Laboratorio Práctico: Deep Lookup – Espionaje Avanzado en LDAP**
  Enumeración de objetos, lectura estructurada de datos del directorio y entendimiento del valor ofensivo de la información centralizada.
- **Laboratorio Práctico: Silent Scan – Escaneo de Puertos y Servicios**
  Reconocimiento sigiloso, detección de servicios críticos y construcción progresiva del mapa técnico del entorno Windows.
- **Laboratorio Práctico: Breaking Kerberos – Accediendo a la Fortaleza del Dominio**
  Comprensión del modelo Kerberos, exposición de cuentas y relevancia ofensiva del servicio de autenticación central.
- **Laboratorio Práctico: Hidden Shares – Infiltración en Recursos Compartidos SMB**
  Acceso a comparticiones no evidentes, revisión de permisos y exploración de datos internos con valor estratégico.
- **Laboratorio Práctico: AS-REP Roasting – Explotando Usuarios Kerberos sin Preautenticación**
  Abuso de configuraciones débiles en cuentas, obtención de material sensible y análisis del riesgo asociado a políticas laxas.
- **Laboratorio Práctico: Kerberoasting – Robo de Credenciales de Servicios**
  Enumeración de servicios asociados a cuentas privilegiadas y aprovechamiento de configuraciones delegadas de autenticación.
- **Laboratorio Práctico: Bruteforce Blitz – Rompiendo Contraseñas en Active Directory**
  Evaluación de fortaleza de credenciales, repetición controlada de autenticación y consecuencias del uso de contraseñas débiles.
- **Laboratorio Práctico: Relay Wars – Ataques SMB y NTLM en Redes Windows**
  Abuso de mecanismos de autenticación heredados, redirección de confianza y obtención de acceso indirecto dentro del entorno.
- **Laboratorio Práctico: Espionage MITM (Man in the Middle) – Captura de Credenciales**
  Intercepción de tráfico, captura de material autenticador y entendimiento del riesgo de protocolos inseguros o mal segmentados.
- **Laboratorio Práctico: Privilege Escalation – Escalada de Privilegios en Windows**
  Abuso de permisos locales, configuraciones débiles y ampliación del control sobre sistemas del dominio.
- **Laboratorio Práctico: Credential Hunter – Robo de Credenciales y Archivos Sensibles**
  Localización de secretos, lectura de información crítica y aprovechamiento de almacenamiento inseguro en estaciones y servidores.
- **Laboratorio Práctico: Post-Explotación en WinRM – Manteniendo Persistencia**
  Consolidación del acceso, mantenimiento operativo de la sesión y persistencia funcional en sistemas comprometidos.
- **Laboratorio Práctico: Domain Takeover – Dominación Total del Directorio Activo**
  Encadenamiento de debilidades, elevación de privilegios a nivel dominio y toma de control completa de la infraestructura.

Algunas herramientas, sin limitarse a:

Impacket, BloodHound, SharpHound, CrackMapExec, Responder, enum4linux, smbclient, rpcclient, kerbrute, GetUserSPNs, GetNPUsers, Evil-WinRM, ldapsearch, nbtscan, Nmap, herramientas de relay NTLM, captura de credenciales y análisis de relaciones de privilegio en Active Directory.

ESPECIALIZACIÓN 8

Seguridad en Cajeros Automaticos ATM y prevención de fraude bancario

Cobertura integral sobre seguridad en cajeros automáticos, evolución de ataques, fraude financiero, malware ATM, manipulación física, protocolos críticos, auditoría técnica en escenarios reales.

- **Fundamentos de Seguridad en Cajeros Automáticos**
  Historia y evolución de ataques a ATM, arquitectura, topología, tipología de cajeros, ciclo de transacción financiera, normativas globales y fabricantes/software.
- **Compromiso del PIN y Seguridad del Teclado**
  Ingeniería social, interceptores electromagnéticos, esteganografía en teclados falsos, cifrado de PIN, biometría y mecanismos de detección de manipulación.
- **Skimming y Robo de Tarjetas**
  Reverse engineering de skimmers, lectura sin contacto, decodificación de pistas magnéticas, exfiltración de datos y mecanismos de detección de alteraciones físicas.
- **Trampas de Efectivo y Fraudes de Reversión**
  Análisis de sensores de billetes, manipulación de logs, dispositivos cash-trap, controles de verificación y revisión de firmware de dispensadores.
- **Ataques de Malware y Caja Negra**
  Análisis estático y dinámico de malware ATM, cadenas de infección USB, anti-debugging, manipulación de módulos XFS y ejecución remota vía command & control.
- **Seguridad Física y Manipulación de Cerraduras**
  Bypass electromagnético, cámaras ocultas, cerraduras vulnerables, ataques físico-lógicos combinados, sensores de vibración y roleplay de intrusiones físicas.
- **Fraudes de Extracción Ilimitada de Efectivo**
  Ataques coordinados con tarjetas clonadas, simulación de escenarios bancarios, transacciones válidas no autorizadas, ofuscación de logs y respuesta ante ATM cashout.
- **Manipulación de Mensajes de Autorización**
  Ingeniería inversa de ISO 8583, spoofing de mensajes, redirección de transacciones, ARP poisoning, TLS mutuo y simulación de corrupción de mensajes.
- **Gestión de Crisis y Delitos Asociados**
  Escenarios de crisis coordinada, activación de CSIRT financiero, análisis post-mortem, fraude interno, simulacros en tiempo real y perfil criminal en delitos ATM.
- **Auditoría Técnica y Cumplimiento Normativo**
  Auditoría Red Team vs Blue Team, herramientas de compliance, validación de cifrados EMV, simulación de informes, auditoría de logs/firmware/BIOS y métricas de madurez.
- **Laboratorio Práctico: Análisis de ATM Comprometido – Reconstrucción Forense Integral**
  Evaluación inicial del sistema comprometido, identificación de artefactos, correlación de eventos y análisis del contexto operativo del incidente.
- **Laboratorio Práctico: Extracción de Información de un Firmware Dump – Análisis Estructural de Firmware**
  Desmembramiento de binarios, identificación de estructuras internas, extracción de datos sensibles y mapeo lógico del sistema embebido.
- **Laboratorio Práctico: Exfiltración USB desde ATM con Malware – Implante Autónomo de Exfiltración**
  Simulación de malware persistente capaz de recolectar y exfiltrar información financiera mediante dispositivos periféricos.
- **Laboratorio Práctico: Explotación de Vulnerabilidades en ATM y Exfiltración de Logs – Acceso y Análisis de Registros Críticos**
  Compromiso de servicios expuestos, extracción de logs operacionales y decodificación de eventos sensibles del sistema.
- **Laboratorio Práctico: Análisis Estático de Malware ATM – Ingeniería Inversa de Binarios**
  Inspección de archivos maliciosos mediante técnicas estáticas, identificación de funciones, firmas e indicadores de compromiso.
- **Laboratorio Práctico: Análisis Dinámico de C2 ATM – Simulación de Canal de Comando y Control**
  Ejecución controlada de backdoors, interacción con servicios persistentes y análisis del comportamiento en tiempo real.

Algunas herramientas, tecnologías y áreas abordadas, sin limitarse a:

Kali Linux, Netcat, Python, Wireshark, tcpdump, scripts C2, análisis forense, análisis de memoria, firmware, sandboxing, recolección de evidencias, herramientas ofensivas, XFS, ISO 8583, debugging, reversing, sensores de integridad, detección de skimmers, validación EMV, análisis de malware, command & control, protocolos criptográficos, correlación de logs, laboratorio ATM, auditoría técnica, fraude bancario, controles de seguridad físicos y lógicos.