Iniciación al Hacking Ético y Ciberseguridad

La ciberseguridad es la práctica ofensiva o defensiva de proteger los sistemas, redes y datos contra ataques digitales.

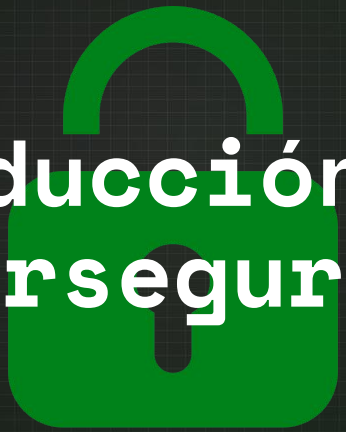
Manuel Márquez Morenilla

Objetivos del Curso

1. Comprender los fundamentos de la ciberseguridad.
2. Configurar un entorno seguro y configurarlo en Hack The Box (HTB).
3. Identificar y documentar vulnerabilidades en un documento.
4. Resolver retos en Hack The Box y herramientas básica.

HACKTHEBOX

Introducción a la Ciberseguridad



¿Qué es la Ciberseguridad?

- La ciberseguridad es la protección de sistemas, redes y datos frente a ataques cibernéticos, como robos de información o daños. En nuestra vida digital, es esencial para asegurar nuestra privacidad

Ejemplos

El **ransomware WannaCry** (2017), que paralizó hospitales, el ataque a **SolarWinds** (2020), que **afectó a agencias gubernamentales**, y la filtración de datos de **Facebook** (2019), que **expuso millones de usuarios**. Estos ataques demuestran la gravedad de las amenazas digitales y la importancia de protegernos.

Conceptos Clave

Amenazas: Son posibles eventos o acciones que pueden causar daño a los sistemas, redes o datos, como los ciberataques o el robo de información.

Vulnerabilidades: Son debilidades en un sistema que pueden ser explotadas por los atacantes para acceder a datos o causar daños.

Principales ciberataques:

Malware: Software malicioso que daña o infecta un dispositivo, como virus o troyanos.

Phishing: Engaños que intentan obtener información personal (como contraseñas) a través de correos electrónicos o sitios web falsos.

DDoS (Denegación de Servicio Distribuida): Ataques que saturan un sitio web o servidor con tráfico para hacerlo inaccesible.

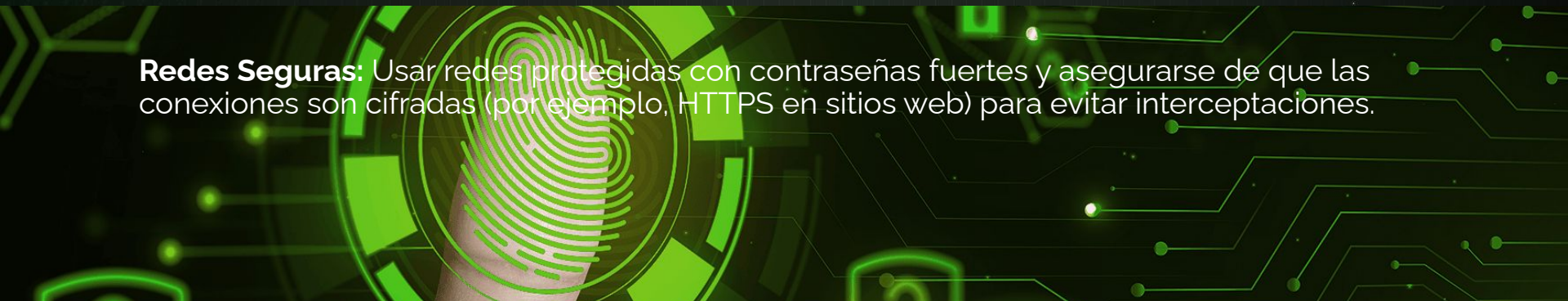
Técnicas de Protección Básicas

Contraseñas Seguras: Contraseñas complejas, largas y únicas para cada cuenta, lo que dificulta su adivinación o descifrado.

Autenticación de Dos Factores (2FA): Añade una capa extra de seguridad, pidiendo una segunda verificación, como un código enviado a tu teléfono, además de la contraseña.

VPN (Red Privada Virtual): Cifra tu conexión a internet, ocultando tu dirección IP y protegiendo tu privacidad al navegar, especialmente en redes Wi-Fi públicas.

Redes Seguras: Usar redes protegidas con contraseñas fuertes y asegurarse de que las conexiones son cifradas (por ejemplo, HTTPS en sitios web) para evitar interceptaciones.



Configuración del Entorno de Hacking

En nuestro caso usaremos el entorno de Hack The Box pero hay muchas más.

Configuración del Entorno de Hacking

Software necesario: Para realizar pruebas de seguridad o investigaciones cibernéticas, herramientas como **Kali Linux o Parrot** y plataformas de virtualización como **VirtualBox o VMware** son esenciales para crear entornos aislados y controlados.

Instalación y configuración de OpenVPN: Para asegurar la conexión en redes no confiables, OpenVPN se debe instalar y configurar adecuadamente, creando una red privada virtual (VPN) que cifra el tráfico y protege la privacidad en las conexiones remotas.

Conexión a Hack The Box (HTB)

En este módulo aprenderás a conectarte a **Hack The Box (HTB)** mediante una **VPN** y cómo asegurar tu entorno de trabajo.

Conexión mediante OpenVPN: Te enseñaré cómo descargar y configurar OpenVPN para conectarte de forma segura a los servidores de HTB.

Recomendaciones de seguridad: Veremos cómo proteger tu entorno de pruebas usando máquinas virtuales y buenas prácticas de seguridad como la actualización constante del sistema y el uso de redes privadas.

Reconocimiento con Nmap

También aprenderás a utilizar **Nmap** para realizar **escaneos de puerto**s y descubrir servicios activos en un objetivo. **Nmap es una herramienta fundamental** en pruebas de penetración y auditorías de seguridad, ya que permite mapear la red y obtener información valiosa sobre los sistemas.

Introducción a Nmap: Te enseñaré cómo funciona Nmap y cómo usarlo para identificar puertos abiertos y servicios en un objetivo.
Importancia para el escaneo de puertos: Veremos cómo Nmap te permite detectar vulnerabilidades potenciales al escanear puertos, lo que es crucial para planificar un ataque o evaluar la seguridad de un sistema.

Al finalizar, serás capaz de realizar un escaneo básico de puertos, una habilidad clave en cualquier proceso de reconocimiento previo a una prueba de penetración.

Fundamentos de Redes

Protocolos de Red

Descubrirás los protocolos de red esenciales que permiten la comunicación entre dispositivos en una red. Estos protocolos son fundamentales para asegurar que los datos se transmitan de manera correcta y eficiente a través de Internet y redes locales.

TCP/IP (Transmission Control Protocol/Internet Protocol): Aprenderás sobre el protocolo TCP/IP, que es la base de Internet. TCP se encarga de garantizar que los datos lleguen correctamente a su destino, mientras que IP se encarga de direccionar esos datos a través de las redes.

HTTP/HTTPS (Hypertext Transfer Protocol/Secure): Veremos cómo HTTP y su versión segura HTTPS permiten la comunicación entre tu navegador y los servidores web. HTTPS cifra los datos para proteger la privacidad y seguridad de las transacciones en línea.

DNS (Domain Name System): Comprenderás el funcionamiento del DNS, que traduce los nombres de dominio (como "www.ejemplo.com") en direcciones IP que las computadoras pueden entender, facilitando la navegación por Internet.

Análisis de Tráfico de Red

En esta sección, te enseñaré cómo **analizar el tráfico** que circula por una red para **detectar problemas y posibles amenazas.**

Uso de herramientas: Aprenderás a utilizar herramientas como Wireshark para capturar paquetes de datos y examinar la información de la red, incluyendo protocolos, puertos y direcciones IP.

Objetivos del análisis:

Detectar problemas de rendimiento como congestión de red o dispositivos con un alto consumo de ancho de banda.

Identificar actividades sospechosas, como tráfico anómalo que pueda indicar un ataque cibernético.

Al dominar el análisis de tráfico, serás capaz de mantener una red más eficiente y detectar posibles incidentes de seguridad a tiempo.

Identificación de Vulnerabilidades

Aquí aprenderás a identificar las **vulnerabilidades en una red o sistema** que puedan ser explotadas por atacantes. Esto es clave para prevenir intrusiones y proteger los datos.

Herramientas y técnicas: Te enseñaré a usar herramientas como **Nmap** para **escanear puertos** y **detectar servicios activos**, o **Nessus** para realizar **escaneos** de **vulnerabilidades** en sistemas y aplicaciones.

Métodos para identificar vulnerabilidades:

Escaneo de puertos: Encontrar puertos abiertos que puedan ser puntos de entrada.
Análisis de vulnerabilidades: Detectar fallos de seguridad en sistemas o aplicaciones.
Pruebas de penetración: Simular ataques reales para evaluar las debilidades de seguridad en la infraestructura.

Con estas habilidades, podrás identificar las brechas de seguridad antes de que los atacantes las encuentren y las exploten.

Técnicas de Ataque

No se puede hackear en sitios públicos ya que es totalmente ilegal. Los ataques solo ocurren en redes controladas o con acceso autorizado mediante contrato.

Tipos de Ataques Comunes

Exploraremos algunos de los ataques más utilizados por los ciberdelincuentes y cómo afectan a los sistemas y aplicaciones.

Inyección SQL: Este ataque se produce cuando un atacante inserta comandos maliciosos en un formulario web o parámetro de URL para manipular una base de datos. Aprenderás a reconocer cómo los atacantes pueden acceder, modificar o eliminar datos sensibles a través de una vulnerabilidad en el código SQL de una aplicación web.

Cross-Site Scripting (XSS): En este ataque, el atacante inserta scripts maliciosos en una página web que luego se ejecutan en el navegador de otro usuario, lo que puede robar información como cookies o credenciales. Te enseñaré cómo se explotan estas vulnerabilidades y cómo proteger las aplicaciones web contra XSS.

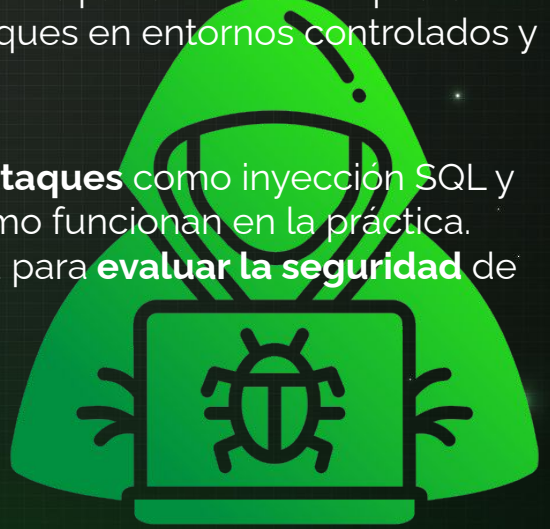
Otros ataques comunes: También revisaremos ataques como Cross-Site Request Forgery (CSRF), Denegación de Servicio (DoS/DDoS) y Ransomware, y cómo pueden comprometer la seguridad de los sistemas.

Cómo Ejecutar Ataques en Entornos Controlados

Aquí aprenderás cómo ejecutar estos ataques de **manera ética y en un entorno seguro**, sin comprometer redes o sistemas reales.

Uso de entornos virtualizados: Te enseñaré cómo utilizar máquinas virtuales o plataformas como **Hack The Box (HTB) o TryHackMe** para realizar ataques en entornos controlados y **legales**.

Simulación de ataques: Realizaremos **simulaciones de ataques** como inyección SQL y XSS en **plataformas de pruebas** para que puedas ver cómo funcionan en la práctica. Aprenderás a ejecutar estos ataques de forma controlada para **evaluar la seguridad** de aplicaciones web y redes.



Ejemplos Prácticos

A lo largo del curso, realizaremos ejemplos prácticos de cada uno de los ataques que hemos revisado:

Inyección SQL: Realizaremos un ataque de inyección SQL en una base de datos vulnerable para aprender a explotarla y cómo protegerla.

XSS: Simularemos un ataque XSS en una aplicación web vulnerable, demostrando cómo un atacante podría robar información de usuarios.

También practicaremos ataques de fuerza bruta, CSRF, DoS/DDoS y algunos más.

Al finalizar este módulo, comprenderás las técnicas de ataque más comunes, cómo ejecutarlas de manera controlada y cómo defender los sistemas contra ellas. Esto te brindará las habilidades necesarias para realizar pruebas de penetración y reforzar la seguridad de aplicaciones web y redes.

Resolución de Máquinas en Hack The Box

Metodología de Resolución de Máquinas

También te enseñaremos procesos para ayudarte a resolver tus máquinas:

Reconocimiento: Escanea la maquina para identificar puertos y servicios abiertos con herramientas como Nmap.

Enumeración: Examina los servicios encontrados para buscar posibles vulnerabilidades.

Explotación: Usa las vulnerabilidades detectadas para obtener acceso a la máquina.

Escalada de privilegios: Una vez dentro, intenta obtener acceso de administrador para comprometer totalmente la máquina.

Errores comunes a evitar:

No hacer un buen reconocimiento.

Asegúrate de no omitir ninguna fase del proceso.

En el curso haremos también ejemplos prácticos para que sepáis como hacerlo al 100%

Documentación e Informes

Importancia de Documentar los Ataques

Documentar cada ataque es **crucial** para varias razones:

Rastreabilidad: Permite llevar un registro de los pasos seguidos durante una prueba de penetración o un ataque ético.

Revisión y análisis: Ayuda a analizar qué se hizo bien, qué se pudo mejorar y cómo prevenir futuras vulnerabilidades.

Comunicación clara: Facilita que el equipo de seguridad, los desarrolladores o los clientes comprendan las amenazas y soluciones implementadas.

Cómo Redactar un Informe de Vulnerabilidad

En este módulo, te enseñaremos cómo redactar un informe de vulnerabilidad estructurado y profesional. Un buen informe debe incluir:

Resumen ejecutivo: Una descripción breve y clara del ataque o vulnerabilidad, y el impacto potencial en el sistema.

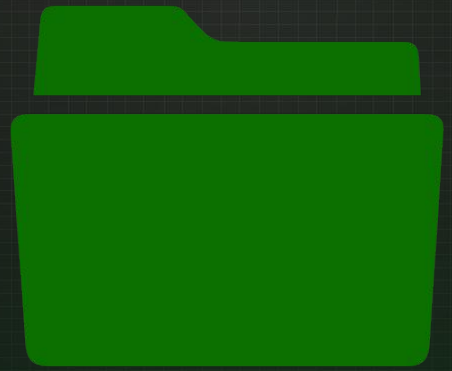
Detalles técnicos: Explicación de la vulnerabilidad, cómo se encontró, herramientas utilizadas y los pasos seguidos para explotarla.

Recomendaciones de mitigación: Sugerencias claras sobre cómo corregir la vulnerabilidad y evitar que vuelva a ocurrir.

Impacto: Las consecuencias de no corregir la vulnerabilidad y los riesgos asociados.

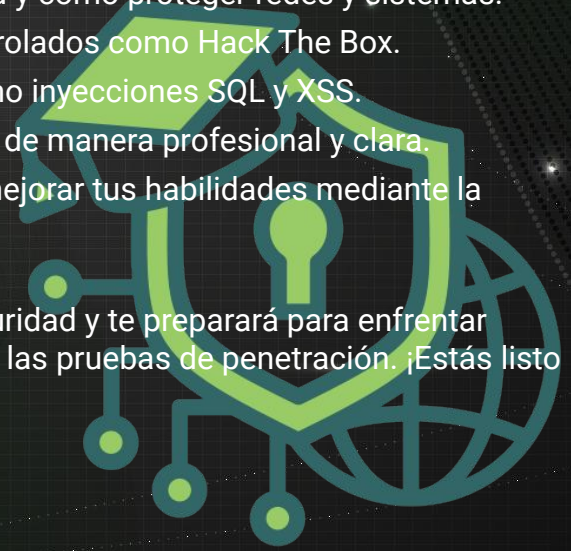
Ejemplos de Informes

Te proporcionaremos ejemplos prácticos de informes de vulnerabilidades bien estructurados. Estudiarás cómo se presentan los hallazgos de manera concisa y profesional, para que puedas aplicarlo en tus propios proyectos de ciberseguridad.



Al finalizar este curso, serás capaz de:

- Comprender los fundamentos de la ciberseguridad y cómo proteger redes y sistemas.
- Ejecutar pruebas de penetración en entornos controlados como Hack The Box.
- Detectar y explotar vulnerabilidades comunes como inyecciones SQL y XSS.
- Documentar y redactar informes de vulnerabilidad de manera profesional y clara.
- Aplicar estrategias de resolución de máquinas y mejorar tus habilidades mediante la práctica constante.



Este curso te proporcionará una base sólida en ciberseguridad y te preparará para enfrentar desafíos más avanzados en el campo del hacking ético y las pruebas de penetración. ¡Estás listo para comenzar tu viaje en el mundo de la ciberseguridad!

Nos Vemos en el Curso

Recuerda que la ciberseguridad es un campo dinámico y en constante cambio. La práctica constante y la curiosidad te permitirán seguir mejorando. Te animo a continuar explorando plataformas como Hack The Box y a participar en la comunidad, donde siempre encontrarás nuevos desafíos que te ayudarán a crecer.

¡El viaje ha comenzado! ¡No dejes de aprender y seguir avanzando en tu carrera en ciberseguridad!

¡Nos vemos en el próximo desafío! 🚀🔐