CYBERIUM ARENA

Descripción
Sumérgete en módulos avanzados de ciberseguridad, comenzando con ataques a dominios y dominando herramientas como Mimikatz y técnicas de post-explotación. Explora operaciones de equipos rojos, enfatizando técnicas de dominio, persistencia e ingeniería social. Profundiza en la seguridad del IoT, comprendiendo vulnerabilidades y extracción de datos. Finalmente, sumérgete en sistemas operativos embebidos, aprendiendo sobre emulación de firmware, automatización de despliegue y diversos métodos de explotación de IoT.

ZX310 - GUERRA CIBERNÉTICA

Módulo 1: Ataques a Dominios

Adéntrate en la seguridad de red comprensiva, comenzando con técnicas avanzadas de reconocimiento y escaneo pasivo. Domina herramientas como Mimikatz, comprende las sutilezas de los ataques sin archivos y desbordamientos de búfer. Profundiza en estrategias de post-explotación, desde configurar payloads hasta automatizar procesos, asegurando un entendimiento completo de la escalada de privilegios e inyección de procesos.

Análisis de la Red
Reconocimiento Avanzado y Escaneo
Trabajando con CVE
Mimikatz
Explotación Manual
Ataques sin Archivos
Desbordamiento de Búfer
Configuración de Payloads
Análisis de Explotaciones Locales
Escalada de Privilegios
Inyección de Procesos
Automatización de Post-Ataques

Módulo 2: Técnicas de Equipo Rojo

Domina el reenvío de puertos y la exfiltración de datos hasta comprender los movimientos laterales. Sumérgete en estrategias de equipos rojos, aprovechando marcos como C2, y fortalece defensas contra amenazas. Mejora habilidades en ingeniería social, configurando servidores de phishing y creando archivos maliciosos para una preparación comprensiva en ciberseguridad.

Movimiento Lateral
Reenvío de Puertos y Exfiltración
Técnicas de Persistencia
Detección y Defensas
Marcos de Equipo Rojo
Marco C2
Persistencia
Técnicas de Ingeniería Social
Configuración de Servidores de Phishing
Creación de Archivos Maliciosos

Módulo 3: Introducción a la Seguridad del IoT

Aprende a recopilar y extraer datos cruciales, identificar vulnerabilidades del IoT y comprender conceptos fundamentales. Profundiza en las complejidades de sistemas operativos embebidos, comprensión de firmware y mapeo de superficies de ataque. Mejora tu experiencia configurando máquinas virtuales, montando sistemas de archivos y detectando secretos codificados.

Encontrando Dispositivos IoT
Uso Avanzado de Shodan
Recopilación y Extracción de Datos
Identificando Vulnerabilidades del IoT
Conceptos Fundamentales
Configurando tu VM
Introducción a Sistemas Operativos Embebidos
Comprensión del Firmware
Superficie de Ataque
Mapeo de la Superficie de Ataque del IoT
Montando Sistemas de Archivos
Identificando Secretos Codificados

Módulo 4: Sistemas Operativos Embebidos

Adéntrate en el análisis de archivos de sistemas IoT, emulación de firmware y el despliegue de Firmadyne. Mejora tus habilidades en la militarización y puertas traseras en firmware. Profundiza en técnicas de explotación del IoT, desde utilizar Burp hasta dominar inyecciones de comandos y ataques de fuerza bruta.

Introducción a Sistemas Operativos Embebidos
Trabajando con SquashFS
Análisis de Archivos de Sistemas IoT
Emulación de Binarios de Firmware
Trabajando con QEMU
Desplegando Firmadyne
Automatizando los Despliegues
Militarizando Firmware
Colocando una Puerta Trasera en Firmware
Explotación del IoT con Burp

ZX Ofensiva | NIVEL: 6 | DURACIÓN: 40h