Descripción

Emprende un viaje comprensivo hacia la ciberseguridad basada en Python. Adéntrate en la red de Python, cubriendo sockets, obtención de banners y herramientas avanzadas como Nmap y Shodan. Concéntrate en la creación de paquetes, enseñando las complejidades de Scapy, sniffing de paquetes y creando herramientas de seguridad. Introduce la Seguridad de Aplicaciones Web, explorando la programación HTTP, medidas de seguridad de aplicaciones web y técnicas como spidering. Finalmente, desvela las poderosas características de Metasploit, desde trabajar con payloads y shells reversos hasta ataques locales y keylogging.

ZX322 - PYTHON OFENSIVO

Módulo 1: Redes Python

Sumérgete en los aspectos fundamentales de la red con una introducción a sockets y conexiones a través de TCP y UDP. Explora herramientas y técnicas de seguridad, desde la obtención de banners y escaneo de puertos hasta aprovechar bibliotecas como Cymruwhois y Faker. Domina métodos de cracking de contraseñas, utilizando herramientas como Nmap, Shodan y ataques de fuerza bruta especializados.

Introducción a Sockets
Conectando con TCP y UDP
Obtención de Banners
Escáner de Puertos
Bibliotecas Útiles para Seguridad
Cymruwhois
Faker
Ataques de Fuerza Bruta
Ataques de Fuerza Bruta a Zip
Cracker de FTP
Escáneres
Nmap
Shodan

Módulo 2: Creación de Paquetes

Profundiza en el mundo de Scapy, una herramienta poderosa para la manipulación de paquetes y análisis de red. Domina el arte del sniffing, investigación de archivos pcap y automatización de tareas con Scapy. Mejora tu conjunto de herramientas de seguridad creando y enviando paquetes, desplegando escáneres de puertos, ejecutando ataques MiTM y diseñando herramientas de seguridad a medida.

Scapy
Sniffing con Scapy
Investigación de Archivos Pcap
Creación de Paquetes
Envío de Paquetes
Automatización con Scapy
Escáneres de Puertos
Ataque MiTM
Creación de Herramientas de Seguridad

Módulo 3: Seguridad de Aplicaciones Web

Programación HTTP, explorando la creación de servidores web simples y aprovechando bibliotecas como Urllib, BeautifulSoup y Requests. Profundiza en la seguridad de aplicaciones web, dominando técnicas como configuración de agentes de usuario, manejo de cookies, utilización de proxies web y el arte de hacer spidering.

Programación HTTP
Servidor Web Simple
Urllib
BeautifulSoup
Requests
Seguridad de Aplicaciones Web
Configuración del Agente de Usuario
Configuración de Cookies
Uso de Proxy Web
Spidering

Módulo 4: Características de Metasploit

Navega el complejo mundo de payloads, desde dominar MSFVenom hasta entender payloads específicos de Python. Profundiza en la mecánica de shells reversos, incluyendo variantes TCP y HTTP, y comprende la importancia de la persistencia en operaciones cibernéticas. Mejora tu conjunto de habilidades con técnicas como mejorar shells, ejecutar ataques locales, envenenamiento DNS, extracción de contraseñas de Chrome y despliegue de keyloggers.

Trabajando con Payloads
MSFVenom
El Payload de Python
Shell Reverso TCP Explicado
Shell Reverso HTTP Explicado
Persistencia Explicada
Shell Reverso DDNS
Envenenamiento DNS
Extracción de Contraseñas de Chrome
Keylogger

ZX Ofensiva | NIVEL: 5 | DURACIÓN: 40h