CYBERIUM ARENA

Descripción

Este programa de ingeniería inversa, específicamente diseñado para el experto en ciberseguridad moderno. Este programa meticulosamente diseñado se adentra en el análisis de ejecutables tanto de Windows como de Linux. Desde los principios fundamentales de las estructuras binarias hasta las técnicas prácticas de mitigación de amenazas de software en el mundo real, los participantes estarán equipados con un conjunto de habilidades robusto, dominando una plétora de herramientas y estrategias que aseguran la competencia en descifrar, comprender y contrarrestar vulnerabilidades de software y amenazas maliciosas.

NX233 - INGENIERÍA INVERSA

Módulo 1: Ingeniería Inversa

Comienza con una inmersión profunda en los pilares fundamentales de la ingeniería inversa, entendiendo su papel pivotal en el panorama actual de la ciberseguridad. Los participantes configurarán un entorno de laboratorio dedicado, asegurando un enfoque práctico desde el principio. El módulo también introducirá los conceptos básicos de estructuras binarias, formatos de archivo y las sutilezas de varios lenguajes de ensamblaje, sentando las bases para una exploración avanzada.

Fundamentos de la Ingeniería Inversa
Configuración del Laboratorio
Herramientas y Software Esenciales
Aislamiento del Laboratorio y Aseguramiento de la Integridad de Datos
Introducción a Ejecutables y Bibliotecas
Comprensión de Estructuras Binarias y Encabezados
Primer de Lenguaje de Ensamblaje
Fundamentos de x86, x64 y ARM

Módulo 2: Análisis Estático/Dinámico

Transición al mundo del análisis de código, tanto desde una perspectiva estática, donde el código se disecciona sin ejecución, como dinámicamente, observando el comportamiento del software en tiempo real. Este módulo está diseñado para proporcionar a los participantes una comprensión completa de herramientas y metodologías de ingeniería inversa renombradas. Se pondrá especial énfasis en técnicas como desempaquetado y desofuscación, cruciales para descifrar construcciones de software complejas y ofuscadas.

Introducción al Desensamblado de Código
Comprensión de Grafos de Flujo de Control
Esenciales del Análisis Dinámico
Configuración de un Depurador
Puntos de Interrupción, Pasos e Inspección de Memoria
Monitoreo de Llamadas al Sistema y Actividad de Red
IDA Pro: Características, Atajos y Plugins
Ghidra: Potencia de Código Abierto
OllyDbg, GDB y Radare2
Desempaquetado y Desofuscación
Introducción a Código Empaquetado y Ofuscado
Técnicas y Herramientas para Desempaquetar

Módulo 3: Ingeniería Inversa Avanzada

Este módulo ofrece una exploración comprensiva tanto de los sistemas operativos Windows como Linux, centrándose en sus desafíos y amenazas únicos. Los participantes analizarán malware específico de la plataforma, entenderán llamadas al sistema y API, y se sumergirán en las complejidades de la ingeniería inversa a nivel de kernel, asegurando una comprensión holística de ambas plataformas.

Profundización en Windows
Comprensión de Llamadas API de Windows
Bibliotecas del Sistema y Su Significancia
Técnicas de Análisis de Malware
Ingeniería Inversa del Kernel de Windows
Profundización en Linux
Monitoreo de Llamadas al Sistema de Linux
Bibliotecas Compartidas
Detección de Malware y Rootkits en Linux
Técnicas de Análisis de Binarios ELF

Módulo 4: Ingeniería Inversa del Mundo Real

El módulo introducirá el arte de identificación de vulnerabilidades a partir de parches de software, ofreciendo perspectivas sobre el mundo de las actualizaciones de software y sus implicaciones de seguridad. Además, una parte significativa se dedicará a las dimensiones éticas de la ingeniería inversa, asegurando que los participantes estén bien versados en los límites morales y legales de su experiencia.

Escenarios Prácticos
Análisis de Muestras de Malware del Mundo Real
Bypass de Protecciones

Defensa NX | NIVEL: 7 | DURACIÓN: 40h