CYBERIUM ARENA

Descripción
El Análisis de Malware es el estudio y examen detallado del malware para entender sus orígenes, propósito e impacto potencial en el sistema. Los analistas de malware realizan sus tareas usando diversas herramientas y conocimientos de nivel experto para comprender qué puede hacer un malware y cómo lo hace.

NX232 - ANÁLISIS DE MALWARE

Módulo 1: Introducción al Análisis de Malware

El Análisis Estático Básico examina el código de un programa sin ejecutarlo, permitiendo la identificación temprana de amenazas potenciales. El Análisis Dinámico Básico se refiere al examen de un programa durante su ejecución, proporcionando conocimientos sobre su comportamiento en tiempo real y vulnerabilidades potenciales.

Análisis Estático Básico
Tipos de Malwares
Entendiendo el Formato PE
Librerías y Procesos de Windows
Configurando un Sandbox
Construyendo y Configurando Máquina Virtual
Herramientas de Análisis de Malware
Análisis Dinámico Básico
Identificando Máquinas Virtuales
Buscando Puertos
Probando Tráfico de Red
Analizando Procesos
Análisis del Registro
Simulando Servicios de Internet

Módulo 2: Cargas Útiles de Malware

Las Cargas Útiles de Malware se refieren a la parte del malware que realiza acciones maliciosas, como la exfiltración de datos o daños al sistema. Entender las cargas útiles ayuda en la evaluación de amenazas y la estrategia de defensas. Por otro lado, YARA es una herramienta poderosa utilizada para crear descripciones para identificar y clasificar malware basado en patrones textuales o binarios, mejorando las capacidades de detección de malware.

Cargas Útiles (*payloads*)
Diferentes Métodos de Propagación
Viendo Actividades de Malware
Ejecutando Persistencia
Visión General del Malware en Linux
Detección
Reglas YARA
Trabajando con IMPHash

Módulo 3: Análisis General

Analizar Conexiones de Red implica monitorear y revisar el tráfico de red para detectar anomalías o amenazas potenciales. Identificar Actividades Maliciosas equipa a los aprendices para reconocer comportamientos del sistema inusuales que indican posibles brechas de seguridad. Análisis de Memoria es el estudio de datos en la memoria de un sistema, a menudo utilizado para detectar malware sofisticado o investigar incidentes en forense digital.

Analizando Conexiones de Red
Extrayendo Archivos
Analizando HTTP y HTTPS
Identificando Descargas de Malware
Identificando Actividades Maliciosas
Ataques de Malware
Análisis de Memoria
Identificando Malware
Extrayendo Malware

Módulo 4: Análisis Avanzado

Los Fundamentos del Lenguaje Ensamblador proporcionan una comprensión básica de la programación de bajo nivel crítica para tareas como la ingeniería inversa. El componente Desensamblador permite la traducción del lenguaje de máquina a código ensamblador, permitiendo una mejor comprensión de la función de un programa. El Análisis Dinámico Avanzado implica estudiar programas en ejecución, un método valioso para entender el comportamiento complejo del malware.

Fundamentos del Lenguaje Ensamblador (*Assembly*)
Arquitectura del Procesador x86
Llamadas al Sistema
Programación Básica en Ensamblador x86
Desensamblador
Analizando Malware con IDA Pro
Análisis Dinámico Avanzado
Entendiendo Depuradores
Ejecutando Malware en OllyDbg

Defensa NX | NIVEL: 6 | DURACIÓN: 40h