CYBERIUM ARENA

Descripción

La forense de Windows desempeña un rol crucial en la ciberseguridad. Los aprendices comprenderán los mecanismos de almacenamiento de datos del sistema operativo Windows y adquirirán las habilidades para llevar a cabo investigaciones durante y después de incidentes cibernéticos.

NX212 - FORENSE DE WINDOWS

Módulo 1: Datos Digitales

Este módulo explora el manejo de archivos y discos, la codificación y los sistemas numéricos, profundizando en los tamaños digitales y las características de las unidades de estado sólido (SSD). Incluye formación práctica con un editor hexadecimal y enseña técnicas de visualización de discos y archivos. La sección continúa para abarcar el carving automático y métodos para examinar archivos del sistema y metadatos en Windows.

Archivos y Discos
Codificación
Sistemas Numéricos
Tamaños Digitales
Características de la Unidad de Estado Sólido (SSD)
Editor Hexadecimal
Trabajo con Desplazamientos
Visualización de Archivos
Visualización de Discos
Carving Automático
Métodos de Carving
Carvers Automáticos
Archivos del Sistema de Windows
Metadatos
Visualización de Metadatos
Modificado Accedido Creado
Edición de Datos Exif

Módulo 2: Forense de Archivos

Este módulo se adentra en la esteganografía, enseñando a identificar, extraer y crear archivos ocultos. Transita al análisis de discos duros, centrándose en los archivos del sistema y el análisis de la Tabla Maestra de Archivos (MFT). También brinda experiencia práctica con el Forensic Toolkit (FTK), una herramienta esencial para la forense digital. Este módulo equipa a los aprendices con habilidades vitales en ocultamiento de datos y análisis de discos.

Esteganografía (Análisis de Artefactos Digitales)
Identificación de Archivos Ocultos
Extracción de Archivos Ocultos
Creación de Archivos Ocultos
Análisis de Disco Duro
Archivos del Sistema
Análisis de MFT
Trabajo con FTK

Módulo 3: Recolección de Evidencia

Este módulo profundiza en el análisis de artefactos digitales. Se enfoca en el análisis de registros, incluyendo la extracción de datos y el examen de archivos NTUSER.DAT. El módulo concluye con técnicas para realizar búsquedas generales y el uso de visualizadores de registros, mejorando así la comprensión de los aprendices sobre la investigación de artefactos digitales.

Artefactos
Directorios de Artefactos
Navegadores
Copias en la Sombra
Análisis de Registros
Extracción de Datos
Análisis de NTUSER.DAT
Búsqueda General
Visualizadores de Registros

Módulo 4: Análisis

Este módulo se adentra en los complejos ámbitos del análisis de memoria, eventos, red y malware. Proporciona habilidades clave para inspeccionar la memoria del ordenador, investigar eventos del sistema, analizar interacciones de red y examinar software malicioso, dotando a los aprendices con capacidades críticas para investigaciones forenses cibernéticas.

Análisis de Memoria
Creación de una Imagen
Trabajo con Volatility
Extracción de Datos de la RAM
Análisis de Eventos
Visualizadores de Eventos
Establecimiento de Política de Auditoría
Búsqueda Personalizada
Análisis de Red
Análisis de Protocolos de Servicio
Identificación de Conexiones Darknet
Análisis de Malware
Análisis Estático Básico
Análisis Dinámico Básico

Defensa NX | NIVEL: 3 | DURACIÓN: 10-12 semanas (autoaprendizaje) / 40h (con instructor)