CYBERIUM ARENA

Descripción

La Forense de Redes ofrece una inmersión profunda en el análisis de redes y la detección de intrusiones. Los participantes dominarán el análisis de paquetes con herramientas como Wireshark, explorarán el marco de análisis de red Zeek y abordarán investigaciones de casos del mundo real, desde la detección de anomalías en la red hasta ataques MiTM. El curso concluye con un enfoque en estrategias de mitigación, enfatizando la configuración y operación de sistemas IPS e IDS como Sysmon y Snort.

NX213 - FORENSE DE REDES

Módulo 1: Detección de Intrusiones

Sumérgete en el núcleo de las redes con una exploración profunda de los protocolos de red y las estructuras de paquetes. Domina herramientas y técnicas avanzadas, desde el análisis de Wireshark y TShark hasta la integración de GeoIP y aplicaciones del módulo Scapy. Mejora tus habilidades en detección de intrusiones, creación de paquetes y trabajo con IPv6.

Redes
Protocolos de Red
Estructura de Paquetes
Netstat y ProcMon
SysInternal
Métodos de Detección de Intrusiones
Wireshark Avanzado: Ataques de Red
Análisis de TShark
Integración de GeoIP
Usando el Módulo Scapy
Creación y Análisis de Paquetes
Trabajando con IPv6

Módulo 2: Análisis de Red

Sumérgete en el mundo de Zeek, un marco dinámico de análisis de red. Domina el arte de automatizar procesos, monitorear datos en logs y utilizar el parsing Zeek-Cut. Mejora las habilidades investigativas al reproducir paquetes y crear cronogramas detallados.

Zeek
Logs de Salida
Automatización de Procesos
Monitoreo de Datos en Logs
Parsing de Zeek-Cut
Reproducción de Paquetes para Investigar
Creación de un Cronograma

Módulo 3: Investigación de Casos

Emprende un viaje completo a través de investigaciones de redes, desde entender el ataque MiTM e identificar anomalías en la red hasta dominar el análisis de flujo. Profundiza en herramientas como NetworkMiner y file carvers, y navega por las complejidades del Wi-Fi, desde capturar tráfico inalámbrico hasta gestionar modos de acceso a la red.

Proceso de Investigación
Ataque MiTM
Encontrar Anomalías en la Red
Análisis de Flujo
Carving de Archivos de Red
NetworkMiner
File Carvers
Captura de Tráfico Inalámbrico
Ganando Acceso a través de Wi-Fi
Tráfico HTTPS

Módulo 4: Mitigación

Profundiza tu comprensión de la seguridad de la red con sistemas IPS e IDS, enfocándote en su operación y configuración. Sumérgete en el mundo de Sysmon, desde la instalación hasta la captura de eventos de red. Mejora tu experiencia con herramientas como Snort, un pilar en la detección de intrusiones.

IPS e IDS
Sysmon
Instalación y Configuración de Sysmon
Eventos de Red
Proceso de Operación de IDS/IPS
Configuración de IDS/IPS
Snort

Defensa NX | NIVEL: 4 | DURACIÓN: 40h