CYBERIUM ARENA

Descripción

El programa de Investigación de Redes está diseñado para introducir a los aprendices en los aspectos fundamentales de la seguridad de la información, utilizando Linux como herramienta principal y brindando exposición a diversas amenazas de seguridad.

NX201 - INVESTIGACIÓN DE REDES

Módulo 1: Introducción a Linux

Este módulo ofrece una mirada en profundidad a la virtualización, enfocándose en Linux. Comienza con una visión general de la virtualización y las distribuciones de Linux, guías de instalación de Linux y uso de VMWare. Aborda configuraciones de red, temas de administración de Linux como estructuras de directorios, gestión de usuarios, paquetes, comandos de manipulación de archivos y concluye con scripting y automatización en Linux.

Virtualización
Introducción a la Virtualización
Acerca de la Distribución de Linux
Instalación de Linux
Trabajando con VMWare
Bridged vs. NAT
Trabajando con Linux
Directorios de Linux
Usuarios de Linux
Paquetes
Comandos de Manipulación de Archivos
Técnicas de Manipulación de Texto y Archivos
Scripts de Linux y Automatización

Módulo 2: Redes

Este módulo ofrece una inmersión profunda en protocolos y servicios de red clave. Comienza explorando el modelo TCP/IP, seguido de exámenes detallados de los protocolos DNS, DHCP y ARP, luego hace la transición a servicios de red, proporcionando conocimientos sobre el funcionamiento de SSH, FTP y el servidor web Apache. Este estudio comprensivo de redes equipa a los aprendices con conocimientos cruciales para la gestión y seguridad de redes digitales.

Protocolos
Modelo TCP/IP
DNS
DHCP
ARP
Servicios de Red
SSH
FTP
Apache

Módulo 3: Seguridad de Red

Este módulo se sumerge en técnicas de escaneo de redes y ataque. Comienza con Nmap y Masscan, herramientas poderosas para el escaneo de redes, luego cubre estrategias de ataque de fuerza bruta y ataques sin conexión. Este curso ofrece habilidades invaluables para pruebas de seguridad de redes.

Escaneo
Nmap
Masscan
Fuerza Bruta
Ataques sin Conexión
Creación de Listas de Palabras
Wireshark
Filtrado y Análisis
Extracción de Objetos

Módulo 4: Ciberseguridad

Este módulo profundiza en varios ataques de red y técnicas de defensa. Cubre estrategias de Hombre en el Medio (MiTM) y Envenenamiento ARP, fuerza bruta de servicios y análisis de ciberataques. Los aprendices son introducidos a cargas útiles de reversa y enlace, y entrenamiento práctico con Msfvenom y Msfconsole. Finalmente, explora la operación de firewalls, incluyendo bloqueo de puertos y monitoreo de dispositivos, impartiendo habilidades críticas para la seguridad de la red.

Ataques de Red
MiTM
Envenenamiento ARP
Fuerza Bruta de Servicios
Análisis de Ataques
Ciber Ataque
Cargas Útiles de Reversa y Enlace
Trabajando con Msfvenom
Trabajando con Msfconsole
Firewall
Acerca de la Operación del Firewall
Bloqueo de Puertos
Monitoreo de Dispositivos

Defensa NX | NIVEL: 2 | DURACIÓN: 6-8 semanas (autoaprendizaje) / 40h (con instructor)