

# Curso seguridad en redes: network hacking

 Cantidad de Horas: 12hs



## Objetivo

Conoce las herramientas para la defensa y ataque de las infraestructuras. Identifica las vulnerabilidades en tu web, redes para iniciar un plan de protección.

## Requerimientos

Contar con conocimiento general en Redes.

## 1. Análisis de Tráfico y Escaneo de Puertos

- Captura de Tráfico con Wireshark
- Instalación de Wireshark
- Captura de Tráfico
- Filtros de Visualización
- Filtros de Captura
- Instalación de Nmap
- Especificación de objetivos
- Selección de puertos a escanear
- Escaneo TCP y UDP
- Opciones de escaneo personalizadas
- Detectar que un equipo está activo
- Escaneo de Ping
- Opciones de Tiempo y Rendimiento
- Formatos de Salida
- Detección de Sistemas Operativos y Software
- Detección de Sistema Operativo
- Detección de Versiones de Software
- Introducción a los scripts de Nmap
- Utilización de Scripts de escaneo
- Categorías de Scripts

## 3. Sistema de Prevención de Intrusos

- Instalación de Suricata
- Configuración de Reglas
- Configuración de Logs
- Creación de una Regla Básica
- Regla con Análisis de Contenido y nocase
- Regla ICMP y tamaño de payloads
- Reglas con análisis de DNS (dns\_query)
- Reglas para detección de protocolos
- Descarga de reglas con oinkmaster
- Reputación de Direcciones IP
- Modo en línea (IPS)
- Regla para detección de escaneos web con Nikto

## 2. Firewalls y Redes Privadas Virtuales

- Introducción a los Firewalls
- Capacidades de un Firewall de Red
- Ubicación de un Firewall de Red
- Modelos y Capacidades de Firewalls
- Perles de Firewall (Público, Privado, Dominio)
- Reglas creadas automáticamente
- Configuración de la Creación Automática de Reglas
- Crear una nueva regla de entrada
- Comportamiento Firewall On/Of
- Configuración de Logs
- Introducción a las VPN
- Creación de una VPN Host to Host
- Captura de Tráfico en la VPN

## 4. ARP Poisoning, DHCP Spoong y DNS Poisoning

- Detección Manual Desde Linux
- Manipulación de la Tabla ARP (Windows)
- Manipulación de la Tabla ARP (Linux)
- Captura de Tráfico ARP
- Instalación de Cain & Abel
- Ataque ARP Poisoning con Cain & Abel
- Captura de Tráfico SSL con Cain & Abel
- Instalación de Bettercap
- Ataque ARP Poisoning con Bettercap
- Captura de Tráfico SSL con Bettercap
- Bloquear Ataque en Linux con ARPon
- Detectar Ataque en Windows con ARP Monitor
- DHCP Starvation