



EDUCACIÓN 

Seguridad en Redes: Network Hacking

Programa de Estudio

Seguridad en Redes: Network Hacking

Aprende a atacar y defender las infraestructuras tecnológicas de las organizaciones, conociendo los distintos tipos de ataques y herramientas que pueden ser utilizados para vulnerar una red. Sabiendo esto, podrás defenderte de los distintos tipos de ataques y peligros que pueden afectar a las redes de las organizaciones.

Contenido del curso

El curso comienza con el análisis de tráfico de red, utilizando herramientas conocidas como ¿sniffers?. Luego, vamos a introducir el concepto de escaneo de puertos, para detectar qué servicios se encuentran habilitados en los dispositivos. Más adelante, veremos cómo identificar las versiones de software y sistema operativo para cada equipo escaneado. A continuación analizaremos los firewalls y sistemas IPS, para la detección y prevención de intrusos. También analizaremos las infraestructuras de clave pública, el funcionamiento del protocolo HTTPS y los certificados SSL. Por último, aprenderemos a realizar y detectar ataques de envenenamiento ARP, que nos permitirán interceptar el tráfico de red entre dos o más equipos dentro de una red local.

PRÁCTICAS EN CLASE ::

En este curso se analizará el tráfico de red con Wireshark, para comprender mejor los protocolos de red. Se realizarán escaneos de puertos con Nmap y se utilizarán varias de sus opciones, entre ellas, las de reconocimiento de versiones y sistemas operativos. Se implementará el IPS Suricata, y se crearán reglas personalizadas para entender cómo funcionan y sus diferentes operadores. Se creará una Autoridad Certificante para emitir certificados digitales. Por último, se realizarán ataques ARP Poisoning, con herramientas como Ettercap y Cain & Abel.

Público

El curso de Network Hacking está orientado a toda persona que esté interesada en comprender las medidas de seguridad que deben implementarse en las redes, tanto en las organizaciones pequeñas y medianas, como en las grandes compañías.

Salida Laboral

Al finalizar este curso podrás aplicar a puestos que estén buscando Soporte en Redes.

Requisitos

Se requieren conocimientos sólidos en: Seguridad Informática o haber realizado el curso Introducción a la Seguridad Informática Armado de redes o haber realizado el curso Redes Nivel Introducción

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

En este curso aprenderás a

- Capturar tráfico de una red para su posterior análisis.
- Analizar paquetes para detectar posibles anomalías en la red.
- Detectar qué sistemas se encuentran activos dentro de una red.
- Buscar puertos abiertos en un sistema utilizando diferentes técnicas.
- Identificar el software y sistema operativo que ejecuta un equipo remoto.
- Determinar qué tipo de dispositivo de protección es adecuado para cada red.
- Comparar y elegir diferentes tipos de firewalls de acuerdo a sus características.
- Implementar dispositivos para el filtrado de conexiones y la detección de ataques.
- Crear una conexión segura entre dos equipos para proteger la transferencia de datos.
- Proponer la implementación de diferentes topologías VPN de acuerdo a cada caso
- Emitir solicitudes de firma de certificados y certificados para utilizar con HTTPS.

Plan de Estudios



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

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
- Perfiles de Firewall (Público, Privado, Dominio)
- Reglas creadas automáticamente
- Configuración de la Creación Automática de Reglas
- Crear una nueva regla de entrada
- Comportamiento Firewall On/Off
- Configuración de Logs
- Introducción a las VPN
- Creación de una VPN Host to Host

3. Infraestructuras de Clave Pública y GPG

- Instalación de GPG4Win
- Creación de un Par de Claves
- Importar Claves de un Tercero
- Cifrar y Firmar Archivos
- Descifrar y Validar Archivos
- Instalación de XCA
- Creación de un CA con XCA
- Creación de un CSR con XCA
- Firmar un CSR con XCA
- CSR con OpenSSL y Firma de Certificado para HTTPS
- Creación de un CSR con OpenSSL
- Firma del CSR utilizando XCA
- Instalación del Certificado SSL
- Editar el almacén de CA de Confianza de Mozilla Firefox
- Instalación de Mozilla Thunderbird
- Generación de un archivo PKCS12 personal
- Instalación de PKCS12 en Mozilla Thunderbird
- Configuración de OpenPGP con Mozilla Thunderbird

4. Sistemas de Prevención de Intrusos (IPS)

- Instalación de Suricata
- Revisión de Configuración e Inicio del Demonio
- 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 umbrales (thresholds)
- 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

5. ARP Poisoning, DHCP Spoofing 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

EDUCACIÓN IT

Centro de Capacitación y Desarrollo Profesional



Lavalle 648 Piso 8, Microcentro, CABA

0810-220-8148

info@educacionit.com

EducaciónIT. Copyright 2005-2020