EDUCACIÓN IT

Seguridad en Redes: Network Hacking

Programa de Estudio

Contenido del curso

El curso comienza con el anÃ¡lisis de trÃ¡fico de red, utilizando herramientas conocidas como ?sniffers?. Luego, vamos a introducir el concepto de escaneo de puertos, para detectar quÃ© servicios se encuentran habilitados en los dispositivos. MÃ¡s adelante, veremos cÃ³mo identificar las versiones de software y sistema operativo para cada equipo escaneado. A continuaciÃ³n analizaremos los firewalls y sistemas IPS, para la detecciÃ³n y prevenciÃ³n de intrusos. TambiÃ©n analizaremos las infraestructuras de clave pÃºblic, el funcionamiento del protocolo HTTPS y los certificados SSL. Por Ãºltimo, aprenderemos a realizar y detectar ataques de envenenamiento ARP, que nos permitirÃ¡n interceptar el trÃ¡fico de red entre dos o mÃ¡s equipos dentro de una red local.

PRÃ•CTICAS EN CLASE ::

En este curso se analizarÃ¡ trÃ¡fico de red con Wireshark, para comprender mejor los protocolos de red. Se realizarÃ¡n escaneos de puertos con Nmap y se utilizarÃ¡n varias de sus opciones, entre ellas, las de reconocimiento de versiones y sistemas operativos. Se implementarÃ¡ el IPS Suricata, y se crearÃ¡n reglas personalizadas para entender cÃ³mo funcionan y sus diferentes operadores. Se crearÃ¡ una Autoridad Certificante para emitir certificados digitales. Por Ãºltimo, se realizarÃ¡n ataques ARP Poisoning, con herramientas como Ettercap y Cain & Abel.

Público

El curso de Network Hacking estÃ¡ orientado a toda persona que estÃ© interesada en comprender las medidas de seguridad que deben implementarse en las redes, tanto en las organizaciones pequeÃ±as y medianas, como en las grandes compaÃ±Ã-as.

Salida Laboral

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

Requisitos

Se requieren conocimientos sÃ³lidos en: Seguridad InformÃ¡tica o haber realizado el curso IntroducciÃ³n a la Seguridad InformÃ¡tica Armado de redes o haber realizado el curso Redes Nivel IntroducciÃ³n

Modalidad de cursado

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

En este curso aprenderás a

- Cómo capturar el tráfico para su análisis
- Analizar paquetes para identificar posibles anomalías
- Conocer las técnicas para encontrar los puertos abiertos de un sistema
- Cuál dispositivo de protección es el adecuado para mi red
- Tipos de Firewalls y características específicas de cada uno
- Implementar dispositivos para el filtrados de conexiones y la detección de ataques
- Topologías VPN: Cuándo usar cada una
- Crear una Autoridad Certificante para el uso interno de una organización

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
Configuracion 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

Captura de Tráfico en la VPN

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
Instalacion de Mozilla Thunderbird
Generacion de un archivo PKCS12 personal
Instalación de PKCS12 en Mozilla Thunderbird
Configuración de OpenGPG 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 deteccion 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
TEL_PRINCIPAL
info@educacionit.com