Seguridad en Redes: Network Hacking

Duración: 3 días (24 hrs)

Descripción general

El curso comienza con el análisis de tráfico de red, utilizando herramientas conocidas como esnifes. Luego, vamos a introducir el concepto de escaneo de puertos, para detectar que servicios se encuentran habilitados en los dispositivos. más adelante, veremos cómo identificar las versiones de software y sistema operativo para cada equipo escaneado.

Objetivos

- Capturar tráfico de una red para su posterior análisis.
- Analizar paquetes para detectar posibles anomalías en la red.
- Detectar que sistemas se encuentran activos dentro de una red.
- Buscar puertos abiertos en un sistema utilizando diferentes tácticas.
- 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.
- Crear una Autoridad Certificante preparada para el uso interno en una organización.
- Realizar y detectar ataques ARP Poisoning utilizando diferentes herramientas.
- Utilizar herramientas de monitoreo de tablas ARP.

Prerrequisitos del curso

Se requieren conocimientos en:

- Seguridad Informática o haber realizado el curso Introducción.
- Armado de redes o haber realizado el curso Redes Linux.

Esquema del curso

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
- 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
- Generación 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