Guía Actividades - Taller Nº3 Escaneo

*Taller de Hacking Ético – II Semestre - 2024*

*Prof. Marco Aravena, Ayudante Juan Larenas*

**Objetivo**: Utilizar comando nmap e identificar protocolo.

**Entregable**: documento con captura de pantalla ilustrando lo solicitado en la sección actividades.

**Herramienta**: IMUNES - KALI.

Actividades:

**Parte 1: IMUNES**

1. Replique la red de la imagen 1 en IMUNES (las direcciones IP se colocan automáticamente, no requiere configuración). Para ello inicie IMUNES y en modo diseño (sin iniciar el experimento) coloque los elementos de la imagen 1

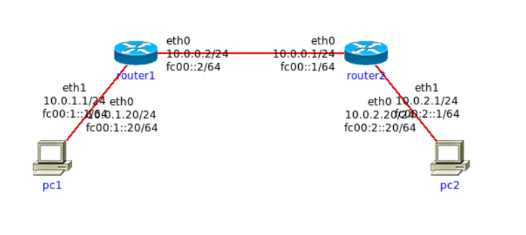


Imagen 1: red para análisis.

* 1. Ejecute el experimento. Capture paquete con Wireshark en pc1. En pc2 ejecute el comando “netserver” y en pc1 “netperf -H *ipdelpc2* ” (NOTA: las ip’s pueden ser distintas a las de la imagen 1).¿ Qué se evidencia en Wireshark? ¿ Qué banderas detecta? Registro el dato de Throughput para compara con b)
  2. Reinicie el ejercicio, haga click derecho en el enlace entre los dos router’s y seleccione configurar. En el parámetro BER indique el número 1000 (ello indica que se pierde 1 de cada 1000 bits) y repita lo indicado en a) para obtener los resultados bajo este nuevo escenario con pérdida de bits. Ejecutes otros escenarios con BER 10.000 y 100.000

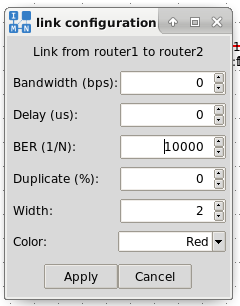


Imagen 2: configuración de enlace

**Parte 2: Kali**

En esta segunda parte debe realizar un escaneo utilizando Kali-Linux.

**IMPORTANTE**: La red de la máquina virtual atacante (Kali) y víctima (Cybersploit) debe estar configuradas en modo “adaptador sólo anfitrión”.

Las credenciales de la máquina Kali son usuario: kali y contraseña: kali

Se sugiere utilizar el terminal (intérprete de comando) de Kali en modo root, para ello utiliza la interfaz gráfica tal como se indica en la imagen 3

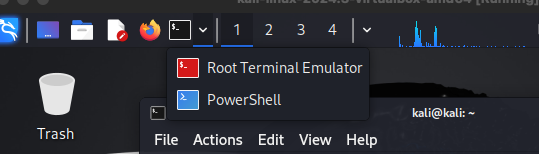


Imagen 3: terminal en modo root

**Actividades.**

1. Dado que se desconoce la IP de la víctima, realice un escaneo de la red con nmap, utilizando “nmap red/mascara”, por ejemplo “nmap 10.11.12.0/24” . Determine la numeración de red utilizando el comando ifconfig en Kali. Identifique la máquina con ssh y http en funcionamiento.
2. Determine las versiones de los servicios de la máquina víctima con nmap, utilizando “nmap -sV IP”, por ejemplo “nmap -sV 10.11.12.123 ”
3. Determine la versión de sistema operativo de la máquina víctima con nmap, utilizando “nmap -O IP”, por ejemplo “nmap -O 10.11.12.123”
4. Determine las vulnerabilidades de la máquina víctima con nmap, utilizando “nmap –script=vuln IP”, por ejemplo “nmap –script=vuln 10.11.12.123”