Carlos Mateos Iglesias

PARP401-Sniffers

Sniffers

CFGS – ASIR1

Contenido

[Wireshark 2](#_Toc159972061)

[Network Miner 3](#_Toc159972062)

[Microsoft Network Monitor 7](#_Toc159972063)

[TCPDUMP 8](#_Toc159972064)

[Netsh trace 11](#_Toc159972065)

# OBJETIVOS DE LA PRÁCTICA

* Conocimiento de algunos sniffers comunes.
* Determinar las condiciones necesarias para la escucha de la red
* Determinar las condiciones necesarias para la escucha de la red

# MATERIALES NECESARIOS

Necesitaremos una Máquina virtual con Windows en el que usaremos el software de Microsoft Network Monitory el NetworkMiner .

También necesitaremos una máquina virtual con Ubuntu en el la que descargaremos el software Wireshark.

# Wireshark

Empezaremos por la instalación de Wireshark en Ubuntu 22.0.4

Para ello ejecutamos el comando “sudo apt install wireshark”Texto

Descripción generada automáticamente

Para arrancar el programa ejecutamos “sudo wireshark” así lo estaremos ejecutando con permisos elevados



Se abrirá una ventana nueva con el programa, debemos darle al botón azul para empezar a esnifar

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez abierto, si procedemos a lanzar un ping, contra la ip 192.168.1.1 (en mi caso a mi propio router) podemos ver que lo está interceptando y mostrando, las.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

# Network Miner

Accedemos a la página oficial de WinPcaP, que son las dependencias de Network Miner y debemos instalarlas antes de instalar el Network Miner.

<https://www.winpcap.org/>

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ahora debemos acceder a la carpeta donde hayamos descargar el NetworkMiner (<https://www.netresec.com/?page=NetworkMiner>) y lo ejecutamos como administrador

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora debemos conocer nuestra interfaz de red, para ello nos fijamos en la esquina inferior derecha en busca de un cuadrado con un cable, y haremos click derecho, configuración de red Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Aquí se nos abrirá los ajustes y podremos ver el nombre del adaptador de internet.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ahora accedemos a “Configuración de red avanzada”

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Pinchamos en Ethernet0 y podemos ver la descripción

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

La seleccionamos en el programa.

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

A continuación, realizaremos un ping hacia cloudfare.com generando así trafico en la red, para que el programa pueda detectarlo.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ahora navegamos a dell.com para ver que nos devuelve el programa

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

# Microsoft Network Monitor

Accedemos a la página oficial <https://www.microsoft.com/en-us/download/details.aspx?id=4865> y descargamos la herramienta, la descomprimimos, e instalamos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Debemos presionar el botón “New Capture” para una nueva captura.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora se nos abrirá una nueva interfaz, en blanco para que empecemos a sniffar la red, debemos decirle al programa que empiece, para ello pulsamos el botón “Start”

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez iniciada la escucha de paquetes, probamos realizando un ping contra mi dominio. Podemos comprobar como enviar paquetes y recibe la respuesta

Una captura de pantalla de una computadora

Descripción generada automáticamente

# TCPDUMP

Por problemas en la instalación no pude correr el programa, intenté realizar la instalación mediante Docker-compose, apt y tienda y nada.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente con confianza baja

Imagen que contiene Texto

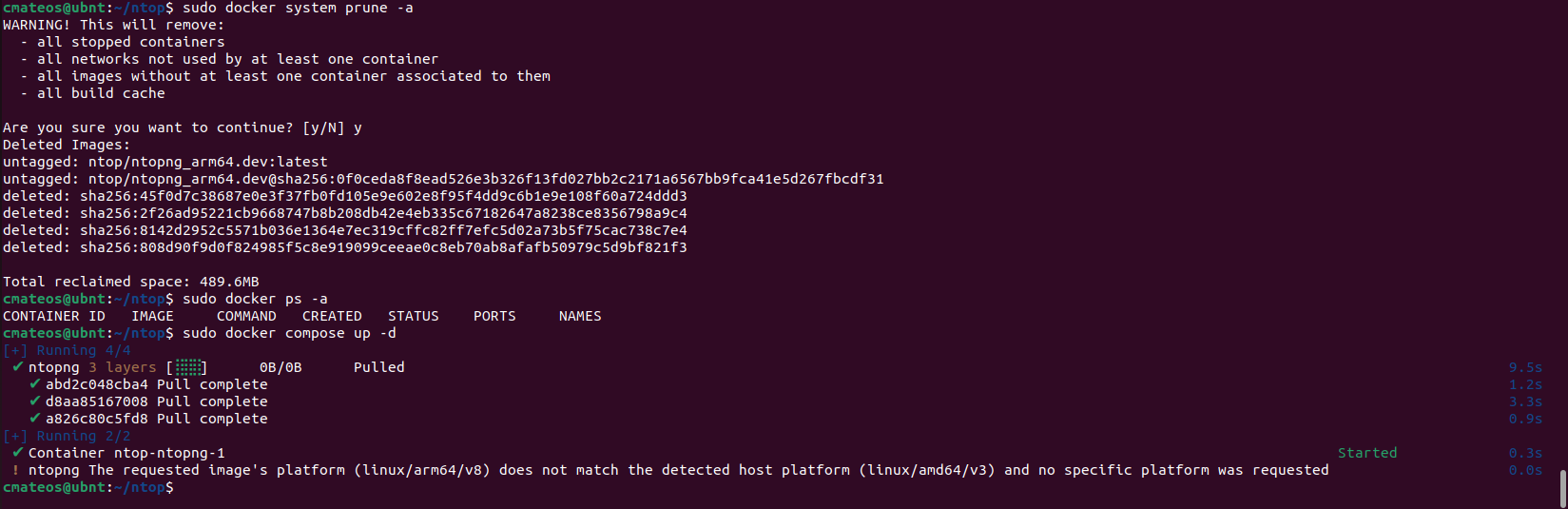
Descripción generada automáticamente

<https://www.ntop.org/get-started/download/>

<https://packages.ntop.org/apt/>

Interfaz de usuario gráfica

Descripción generada automáticamente



Texto

Descripción generada automáticamente

Imagen que contiene Texto

Descripción generada automáticamente

# Netsh trace

Para ejecutar este programa que viene instalado con Windows, debemos ejecutar una terminal CMD con permisos de administrador.

Nos dirigimos a C con el comando

“cd /”

Creamos el directorio donde se guardará los archivos de la captura netsh trace.

“mkdir netsh” (en este caso está creado en C:\)

Para empezar a capturar debemos correr el comando=

“netsh trace start persitent=yes capture=yes tracefile=c:\netsh\trace.etl”

Texto

Descripción generada automáticamente

Para terminar de capturar los paquetes debemos ejecutar el comando

“netsh trace stop”

Texto

Descripción generada automáticamente

Ahora accedemos a la pagina web de Microsoft y descargamos su herramienta ADK - Windows Performance Toolkit (<https://learn.microsoft.com/en-us/windows-hardware/get-started/adk-install>)

Importamos el archivo guardado en la carpeta que creamos de netsh en C:Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Y vemos todos los archivos que nos exporta el programa, debemos fijarnos en el report

Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza media

Lo abrimos y podemos ver este archivo de reporte

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente