Práctica 2 - Análisis de Tráfico
Criptografía y Seguridad 2023-2

Anayanzi Delia Martínez Hernández
anayanzi@ciencias.unam.mx

Ivan Daniel Galindo Perez
ivangalindo@ciencias.unam.mx

Luis Fernando Yang Fong Baeza
fernandofong@ciencias.unam.mx

Enero 2023

1 Introducción

El propósito de esta práctica es el analizar de manera efectiva el tráfico de una red local, es decir, el intercambio de información entre direcciones IP viendo como se realiza el uso de distintos protocolos de Red como lo son TCP, ICMP, SSH o TLS.

Para tener la resolución y la calificación completa de la práctica, antes que nada se debe de descargar la herramienta conocida como Wireshark, una herramienta que facilita el análisis del tráfico permitiendo que se pueda descargar y abrir cualquier archivo con extensión `.pcap` (proveniente de packages captured).

2 Procedimiento

El programa de Wireshark puede ser instalado para sistema operativo Windows, Linux y OS X, sin embargo, en el caso de Linux el super usuario es el que debe de abrir el programa puesto que está interfiriendo directamente con la tarjeta de red.

2.1 Link de instalación

https://www.wireshark.org/download.html

En el link anterior, se debe de descargar el programa de acuerdo al sistema operativo correspondiente.

3 Antecedentes de la práctica

Para esta práctica se van a requerir los 4 archivos `.pcap` para responder las preguntas hechas a continuación, la idea es utilizar algún filtro de Wireshark para facilitar la búsqueda entre los archivos, así como la historia cronológica de la misma.

Las respuestas de las preguntas deberán de ser entregadas en el archivo `Respuestas.txt` llenando la información que se pide puesto que esta práctica se califica de manera automática (Mediante un programa de Python).

3.1 Historia de la práctica

Estás trabajando como especialista en seguridad en el taller de Santa Claus, en particular, en el equipo del SOC donde se detecta el tráfico inusual de la red y sabes que ha habido una alerta, el equipo de respuesta, te ha otrogado estos 3 archivos `.pcap` para que puedas decirles la información necesaria con respecto al incidente sucedido, ¿Crees poder ayudarlos?

3.2 Preguntas

1. Abre el archivo `uno.pcap`, ¿cuál es la dirección IP que inicia una conexión del protocolo ICMP?
2. Si solo se quisiera obtener los mensajes del protocolo HTTP que lleven el verbo GET, ¿Qué filtro usaríamos?
3. Aplica el filtro de la pregunta pasada al archivo `uno.pcap` y contesta. ¿Cuál es el nombre de la página que visita la dirección IP **10.10.67.199**?
4. Abre el archivo `dos.pcap`, mira el tráfico del protocolo FTP, ¿Qué password fue filtrada durante el proceso de login? (Hint, trata de usar algún filtro).
5. En el mismo archivo, ¿cuál es el protocolo en él que está encriptado?
6. Abre el archivo `tres.pcap` y recupera *la Navidad*. ¿Qué objeto está en la lista de deseos de Elf McSkidy para reemplazar a Elf McEager?

Recuerda responder estas preguntas en el archivo `Respuestas.txt`, todas tus respuestas deberán de estar escritas inmediatamente después del signo sin espacios, comas y/o puntos, al igual que sin puntos espacios y/o comas al final.

4 Entrega

La entrega de los archivos se hara en el classroom antes de las 23:59:59.