1 Objetivos

- Aplicar los conocimientos sobre redes de computadoras en el análisis estadístico de tráfico de red, para detectar anomalías en el comportamiento de la red.

2 Preámbulo

Las herramientas sniffer (pasivas) como Wireshark permiten la captura de tráfico de red para su posterior análisis. Con esta información se puede analizar aspectos de la red como la eficiencia y optimización del rendimiento (cuellos de botella), pero también se pueden detectar anomalías que sugieren un análisis profundo para descartar posibles ataques.

3 Desarrollo

Para este ejercicio se utilizará el archivo analisis_paquetes.pcap, disponible en CANVAS. Trabaje el laboratorio en un jupyter notebook.

Preámbulo

1. Instale la librería scapy: https://scapy.net/
2. Tutorial de uso: https://guedou.github.io/talks/2022_GreHack/Scapy%20in%200x30%20minutes.slides.html#/
3. Verifique que la herramienta fue correctamente instalada:
    a. Capture 25 paquetes de su red doméstica (no de la red de la UVG) y asígnelos a una variable.
    b. Imprima el tipo de variable, la longitud y el contenido de la variable.
    c. Imprima el tipo de dato del primer paquete capturado.
    d. Imprima el contenido de 5 paquetes.

Análisis estadístico

1. Descargue e archivo analisis_paquetes.pcap y asignelo a una variable.
2. Convierta la variable a un DataFrame.
3. Muestre el contenido de las primeras 5 filas del dataset.
4. Muestre los valores de las columnas: Src Addres, Dst Address, Src Port y Dst Port.
5. Estadísticas
    a. Muestre todas las IP origen
    b. Muestre todas las IP destino
    c. ¿Cuál es la IP origen más frecuente?
        i. ¿A qué IP destino se comunica con más frecuencia?
        ii. ¿A que puerto destino se comunica? ¿Cuál es el propósito de este puerto?

iii. ¿Desde que puertos origen se comunica?

6. Gráficas
    a. Genere una gráfica de barras 2D horizontales, en el eje Y las IPs origen, y en el eje X la suma de los payloads (bytes) enviados desde dichas direcciones.
    b. Genere una gráfica de barras 2D horizontales, en el eje Y las IP destino, y en el eje X la suma de los payloads (bytes) recibidos en dichas direcciones.
    c. Genere una gráfica de barras 2D horizontales, en el eje Y los puertos origen, y en el eje X la suma de los payloads (bytes) enviados de dichos puertos.
    d. Genere una gráfica 2D de barras horizontales, en el eje Y los puertos destino, y en el eje X la suma de los payloads (bytes) recibidos en dichos puertos.
    e. Genere una gráfica de barras 2D verticales, en el eje Y la suma de los payload, en el eje X el tiempo, para la IP origen más frecuente.
    f. Utilizando la información de las estadísticas y la información del comportamiento del tráfico que las gráficas muestran, describa que es lo que está sucediendo. ¿Es común el comportamiento?
7. Investigación del payload
    a. Cree un nuevo DF que incluya únicamente las conexiones con la dirección IP origen más frecuente.
    b. Cree un nuevo DF que utilice el DF anterior con las columnas src, dst y payload y agrúpelas por dst y la suma del payload,
    c. Obtenga la IP destino que más ha intercambiado bytes con la IP más frecuente. Esta IP es sospechosa por la cantidad de bytes intercambiados, entre todas las direcciones.
    d. Cree un nuevo DF con la conversación entre la IP más frecuente y la IP sospechosa.
    e. Obtenga los payloads del DF del inciso anterior, y añada cada uno en un array.
    f. Muestre el contenido del array.
    g. Observe los primeros bytes del contenido, ¿encuentra algún tipo de dato que no haga sentido que se envíe al puerto destino? Describa lo que encontró.