Miguel Ángel Liaño
Francisco Javier Nanclares

EJERCICIOS DE CAPTURA DE TRÁFICO-WIRESHARK

Ejercicio1:

Comenzamos abriendo la shell y ejecutamos wireshark con el comando **$ sudo wireshark-gtk** para poder realizar una captura en vivo, una vez abierto elegimos la interfaz por donde vamos a capturar el tráfico de paquetes.
Comenzamos a capturar dicho tráfico pulsando el botón 'Start' y en una nueva terminal ejecutamos el comando **$ sudo hping3 -S p 80 www.uam.es**, tras unos segundos paramos la captura pulsando el botón 'Stop', analizamos el tráfico a partir de la información facilitada por wireshark como el número del paquete, tiempo, fuente, destino, protocolo… A continuación guardamos la traza en un fichero con extensión .pcap (no pcapng).
Cerramos wireshark y lo volvemos a abrir con el fichero guardado previamente, donde se muestra de nuevo la información anterior, añadimos dos nuevas columnas (PO y PD) y ordenamos en orden descendiente con respecto a PO, en mi caso uno de los paquetes tiene el valor PO=53, con la siguiente información:
No. = 4, Time = 0.006123, Source = 192.168.27.2, Destination = 192.138.27.128, Protocol = DNS, Length = 97, PO = 53, PD = 54150, Info = Standar Query response 0x3245 A www.uam.es A 150.244.214.237 OPT.

Ejercicio2:

En este apartado nos solicitan capturar tráfico, para ello iniciamos la captura y comenzamos a generar tráfico con el navegador, para realizar el filtrado solicitado (por ip y tamaño del paquete mayor a 1000 bytes) para ello usamos la siguiente expresión, es importante destacar que es necesario añadir la columna ip ya que por defecto no se encuentra visible:

1.- frame.len > 1000 && ip

2.- Para este apartado abría que realizar el mismo filtro realizado en el apartado anterior pero en este caso se aplicaría un filtro de captura (en el caso anterior era de visualización) , para ello antes de realizar la captura usaremos la opción **"Capture Filter"** obteniendo así los paquetes deseados.

3.-El primer paquete tiene una longitud de 95 bytes la cual es mucho mayor a la de los siguientes 5 paquetes: 95, 253, 277, 74 y 60 bytes respectivamente, por lo general este primer paquete tendrá una longitud similar a los siguientes paquetes.

Ejercicio3:

En este apartado nos solicitan añadir una nueva columna, para ello tras generar tráfico procdemos añadir una nueva columna a partir de la opción edit→preferences→columns, creando una columna que llamaremos interarrival, cuyo tipo será UTC time de esta forma se mostrará una columna que muestre el tiempo de llegada de los paquetes tras su captura, éste nos permitirá diferenciar el tiempo de llegada entre paquetes consecutivos.

Ejercicio4:

En este apartado nos solicitan modificar la columna Time para mostrar los tiempos en formato para humanos, para ello hemos realizado los siguientes pasos:

1.-Click derecho sobre el nombre de la columna Time.

2.-Seleccionamos la opción Edit Column Details…

Se abrirá una nueva pestaña:

3.-En Field type, seleccionamos la opción UTC date, as YYYY-MM-DD, and time

4.-Aceptamos

Como se puede observar en la columna se muestra la fecha, la hora, los minutos y segundos de captura del paquete.

Ejercicio5:

Para este apartado comenzaremos realizando la captura de tráfico, para ello seleccionamos la opción "Show the capture options…," se abrirá una nueva pestaña, elegiremos el interfaz deseado (en este caso ens192) y pulsaremos la opción "Capture Filter:", de nuevo se abrirá otra pestaña donde selecionaremos la opción "UDP only" bajando un poco con la barra de scroll y aceptamos, seguidamente comenzamos la captura pulsando el botón "Start" y abriremos una nueva terminal donde teclearemos el comando $sudo hping -S -p 80 **www.uam.es**, además abriremos un navegador para generar más tráfico.

Una forma de comprobar que solo se ha capturado tráfico UDP, es por ejemplo filtrar tráfico a partir de un protocolo distinto a UDP, como se podrá observar no se obtiene ningún resultado.