Jose Benjumeda Rubio y Jorge Santisteban Rivas

**Ejercicios de captura de tráfico**

Ejercicio 1.

Configuramos la interfaz para llevar a cabo la captura de tráfico: eth0. Desmarcamos las opciones que no nos interesan, es decir, la casilla Use pcap-ng format y las casillas de Name Resolution, y empezamos la captura del tráfico.

A continuación, ejecutamos en la terminal el comando

**$ sudohping3 -s -p 80 www.uam.es**

Esperamos unos segundos y terminamos la ejecución.

Guardamos la traza en un fichero con la extensión pcap. Entonces cerramos wireshark y lo volvemos a abrir, y al seleccionar abrir fichero encontramos el fichero que hemos guardado como p1ej2. Se ha guardado correctamente.

Para ordenar los paquetes hacemos clic derecho sobre el campo que hemos creado en el tutorial (Edit -> Preferences -> User Interface -> Columns -> + Añadir con Field type Src Port (Undefined) y nombre PO) y seleccionamos Sort Descending. Llegamos hasta el primer valor 53 y vemos que también es el último: solo hay 1. Hasta ahora no ha habido ningún problema ni ningún momento en el que hayamos tenido que tomar ninguna decisión más que seguir al pie de la letra las instrucciones dadas.

Ejercicio 2.

Capturamos tráfico mientras visualizamos algunas páginas web en el navegador. Para filtrar, clicamos sobre el icono “Edit/apply display filter…”, seleccionamos “IP only” y en el campo expresión escribimos ip.len > 1000.

Para almacenar esta captura con el filtro aplicado, es decir, que no se nos guarden todos los paquetes sino únicamente los que son de tipo IP y de mas de 1000 bytes, tenemos que hacer File -> Export Specified Packets… y seleccionar, en Packet Range, la casilla Displayed. Aquí vemos que las dos opciones son Captured, que en este caso son 10921, y Displayed, que son solo 5453; es decir, los que nos quedan tras quitar todos los que no son de tipo IP o tienen menos de 1000 Bytes. Queda así guardada la traza con el filtro aplicado tras darle un nombre al archivo, asegurarnos de que la extensión es pcap y hacer clic en Save.

El primer paquete, el 10, tiene 1514 bytes de tamaño, como vemos en la columna Packet length (bytes), pero luego haciendo doble clic sobre el paquete, vemos que nos sale más información: Frame 10, Ethernet II, Internet Protocol Version 4 Src, Transmission Control Protocol Src Port y Secure Sockets Layer. El que nos interesa es Internet Protocol Version 4, Src, que es “IP”. Dentro de este apartado encontramos un campo Total Length, en el que dice 1500 bytes. Vemos que hay una diferencia de 15 bytes entre los dos tamaños.

Repetimos este proceso en los 4 siguientes paquetes, el 12, el 33, el 35 y el 39. Todos tienen 1514 bytes de tamaño en Packet length (bytes) y 1500 en

el campo Total Length del campo IP. Se conserva la relación de 14 bytes menos en uno que en otro. Vemos que el campo Header length tiene 20 bytes, cosa que puede estar relacionada, aunque no directamente ya que 1514 - 20 no es 1500.

Ejercicio 3.

Para añadir una columna hacemos igual que para añadir las columnas PO y PD, solo que esta vez, en Field type tenemos que seleccionar Delta time.

Esto básicamente lo he hecho probando con todos los campos que contenían la palabra time: empecé con UTC date and time, luego UTC time, Time (format as specified), Absolute Date and time, Absolute time y finalmente probé delta time con el que sí que obtuve una diferencia de tiempo y no un tiempo normal. Qué pasa, que la diferencia de tiempo no coincide con la diferencia de tiempo que obtenemos restando los tiempos de la columna Time, y esto es un poco raro, pero lo que hay que hacer es quitar el filtro. Esto se debe a que la diferencia de tiempo que estamos representando no es entre los paquetes de tipo IP y más de 1000 bytes, sino entre un paquete y el siguiente tal cual se capturaron al principio. Haciendo esto sí que obtenemos la misma diferencia de tiempo que vemos en el campo Time.

Ejercicio 4.

Modificar el formato de la columna time para que no marque el tiempo que tarda cada paquete respecto del tiempo en el que llega el primero (este sería tiempo = 0), sino que nos lo de en formato de humanos, es decir con horas minutos segundos... Aquí tenemos dos opciones, UTC date and time, con el que nos dan fecha y hora, y UTC time, con el que solo obtenemos hora (sin la fecha).

Ejercicio 5.

Hacer una captura en wireshark utilizando filtros de captura para obtener solo tráfico UDP (User Datagram Protocol) y mientras capturamos, visitar algunas páginas web y ejecutar el mismo comando de antes en la terminal.

Para aplicar un filtro de captura, tenemos que seleccionarlo en el panel de Wireshark: Capture Options. Marcamos eth0, modo promiscuo, desmarcamos pcap-ng format y las opciones de name resolution como siempre, pero además clicando en el botón Capture Filter, seleccionamos el filtro UDP only, y comenzamos a capturar.

Obtenemos muchos paquetes, todos con las siglas DNS (Domain Name System) en la columna Protocol. Hacemos doble clic para ver la decodificación e información que nos da wireshark de los datos de este paquete, y vemos que efectivamente aparece el campo User Datagram Protocol. Ha funcionado.