Ejercicios de captura de tráfico

1. Durante la realización de las prácticas, será muy común disponer de una consola donde ejecutaremos comandos que mandan y reciben tramas por un interfaz de red. En paralelo tendremos en ejecución a Wireshark, que estará capturando el tráfico que nos interese. Este ejercicio muestra un ejemplo típico a realizar en prácticas posteriores:

1.Abra una consola o shell, y déjela abierta en espera de ejecutar algún comando.

2.Ejecute Wireshark y seleccione y configure el interfaz por el que se capturará el tráfico (habitualmente será eth0) Acuérdese de seleccionar las opciones de visualización que más le convenga.

3.Inicie la captura de tráfico pulsando en el botón 'Start'.

4.Vuelva a la consola y ejecute el siguiente comando (tecléelo y pulse <enter>): $ sudo hping3 -S -p 80 www.uam.es

5.Detenga la captura de tráfico mediante el botón 'Stop'.

6.Analice el tráfico capturado (aunque no lo entienda en detalle)

7.Guarde la traza en un fichero (Importante: no utilizar el formato pcap-ng).

8.Cierre Wireshark, y vuelva a abrirlo.

9.Abra el fichero almacenado y compruebe que se almacenó correctamente.

10.Utilizando las columnas que se han añadido durante el tutorial, ordene con respecto al campo 'PO' en sentido descendente y contabilice el número de paquetes en el que este campo tiene valor 53.

Discuta los problemas que haya encontrado durante la realización del ejercicio.

Durante el ejercicio hemos ido siguiendo los pasos del tutorial uno a uno, sin encontrar problemas, cabe añadir que aparte de los pasos tal cual, hemos tomado la precaución de desmarcar las casillas pertinentes antes de iniciar la captura.

En nuestra traza no encontramos ningún paquete con el número 53 en su campo PO.

Hemos guardado esta traza en ejercicio1.pcap

2.Tras haber leído las documentación online facilitada, empiece a capturar tráfico. Abra un navegador y visualice un vídeo en youtube. Pare la captura, y añada un filtro en el interfaz de modo que solo se visualicen paquetes que sean de tipo IP y que tengan un tamaño de paquete mayor a 1000 Bytes.

1.Copie el filtro realizado.

ip.len>1000

2.¿Cómo almacenaría en una captura solo los paquetes mostrados?

Para almacenar dichas capturas, hemos tenido que hacer click izquierdo en Edit->Mark all displayed packets para marcar todos los paquetes con longitud mayor de 1000, y posteriormente, para almacenarlo, clickar en File->Export specified Packets donde marcamos la casilla «Marked packets only» y damos a aceptar, y lo guardamos.

Podemos ver que ha sido guardado correctamente en ejercicio2.pcap

3.Compare el tamaño del primer paquete IP, y el campo 'length' del protolo IP del mismo. Repita para los primeros 5 paquetes, ¿qué relación encuentra?

Podemos apreciar que el tamaño del paquete capturado tiene 14b de longitud más que los del length del protocolo IP, esto es posible que sea debido al hecho de que el paquete va pasando por las diferentes capas de la «arquitectura en capas» por las que pasa un paquete al ser enviado, y que el protocolo IP haya recibido el paquete con menos bits en la cabecera, puesto que no le corresponde interpretarlos.

3.Añada una columna custom que muestre el tiempo entre paquetes consecutivos. Explique brevemente que menús y opciones ha seleccionado.

Simplemente creamos una columna de tipo delta time llamada custom tal y como creamos las columnas PO y PD

4.Modifique la forma en que Wireshark muestra la información en la columna 'Time' de cada paquete. En concreto muestre los tiempos en formato para humanos, y en tiempo Unix con resolución en segundos. Explique brevemente los pasos realizados.

Por ejemplo podemos hacer click derecho en Time y luego clicamos en edit column details→utc date and time, y así nos muestra el tiempo con fecha y hora.

5.Inicie una captura en Wireshark pero aplicando filtros de captura, en concreto solo queremos capturar tráfico UDP. Mientras captura tráfico visualice brevemente un vídeo en youtube, ejecute en una consola el comando

$ sudo hping3 -S -p 80 www.uam.es.

Compruebe que solo se capturan paquetes UDP, y describa brevemente los pasos realizados.

Vemos, que correctamente se muestran sólo los paquetes de tipo UDP si escribimos en el filtro UDP.
Hemos guardado la traza capturada con solo paquetes de tipo UDP en ejercicio5.pcap