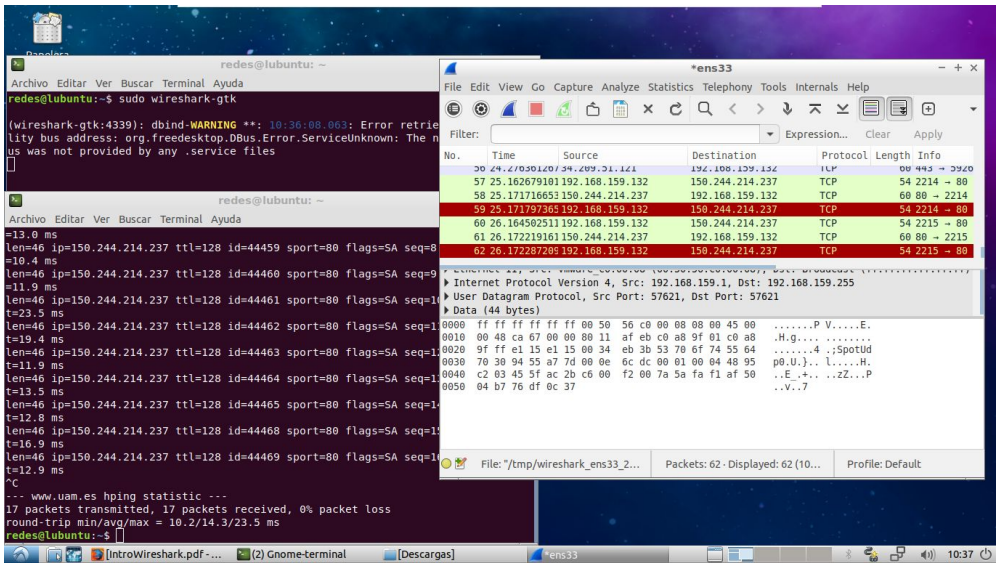
Carlos García Toledano y S. Xiao Fernandez Marin
G. 1392

PRÁCTICA 1

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:

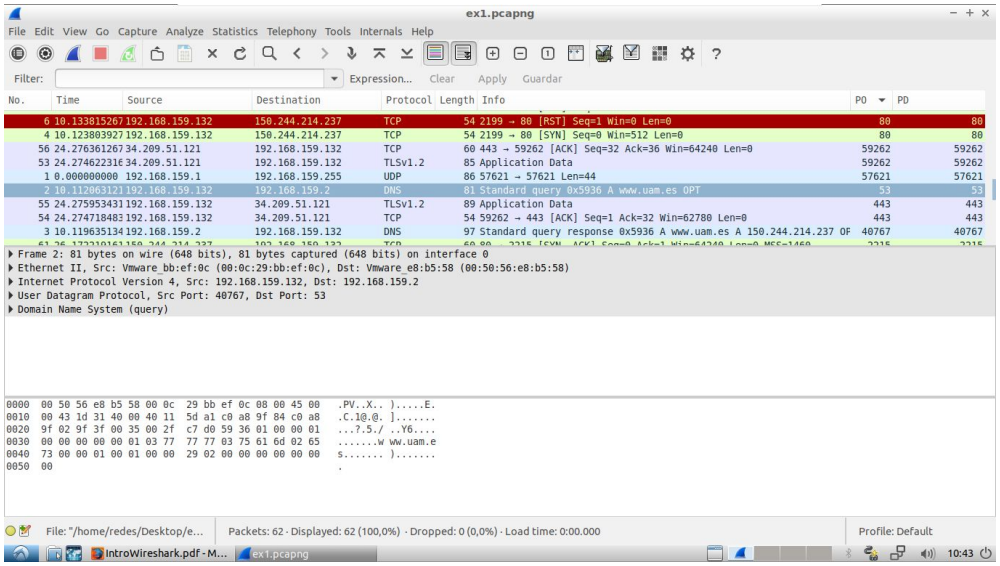
1. Abra una consola o shell, y déjela abierta en espera de ejecutar algún comando.
2. Ejecute Wireshark y seleccione y configure el interfaz por el que se capturará el tráfico (habitualmente será eth0) Acuérdese de seleccionar las opciones de visualización que más le convenga.
3. Inicie la captura de tráfico pulsando en el botón 'Start'.
4. Vuelva a la consola y ejecute el siguiente comando (tecléelo y pulse):
   $ 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.

Describa el proceso realizado y discuta los problemas que haya encontrado durante la realización del ejercicio.



Como podemos ver en la captura de pantalla, se han capturado 67 paquetes, 17 de ellos procedentes de uam.es, ya que el comando Hping3 nos permite abrir un puerto (en este caso el 80, el cual nos permite transferir información de una world wide web) a una IP destino (uam.es) y analizar los paquetes que pasan por ahí.

Además de capturar esos 17 paquetes, los cuales sabemos de donde proceden, ha capturado otros 50 más de los cuales podemos saber su dirección ip mirando en la columna “source”.



Se ha encontrado un solo puerto origen con valor 53. Este es el puerto que es utilizado para servicios DNS. En este caso, hemos especificado que fuese el dominio uam.es.
Hemos seguido los pasos y nos ha costado entender la información del tráfico capturado que nos daba wireshark y el cómo entenderla. Seguimos sin saber entenderla al 100%.

2. Tras haber leído las documentación online facilitada, empiece a capturar tráfico. Abra un navegador y genere tráfico a partir de la visualización de páginas web. 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 && frame.len > 1000

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

Con el filtro ya puesto, Edit > Mark all displayed packets. File > Export specified packets…

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

El tamaño total es sin incluir el relleno de la capa del Ethernet, por lo que va a ser siempre menor al tamaño de la columna “Length”.

Paquete	Tamaño total (Internet protocol version > Total length)	Length
1	72	86
2	72	86

3	333	347
4	40	60
5	707	721

3. Añada una columna llamada interarrival que muestre el tiempo entre paquetes consecutivos. Explique brevemente qué menús y opciones ha seleccionado.
Edit > Preferences > Column > Añadir > Delta Time

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.
Edit > Preferences > Column > Time > Absolute Time

5. Inicie una captura en Wireshark pero aplicando **filtros de captura**, en concreto solo queremos capturar tráfico UDP. Mientras captura tráfico, genere durante algunos instantes tráfico a partir de la visualización de páginas web, y ejecute al mismo tiempo 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.
Capture Options > Capture filters > udp