IS23 Mantenimiento de Instalaciones Informáticas
Práctica 9. Análisis de redes

Ingeniería Técnica Informática de Sistemas
Curso 2005/2006

1 – Objetivos

En la presente sesión se pretende familiarizar al alumno con la instalación y el uso de aplicaciones destinadas a monitorizar y analizar el tráfico de una red informática.

2 – Material

Para el desarrollo de la práctica se va a utilizar un ordenador PC con sistema operativo *Windows 2000* y la aplicación ***ethereal***.

3 – Introducción teórica

Las redes de comunicaciones son, en la actualidad, un elemento fundamental dentro de cualquier sistema informático. La compartición de dispositivos (impresoras, unidades de almacenamiento para copias de seguridad, etc.) o de archivos, la mera interacción para enviar correos electrónicos o ejecutar sesiones remotas hace que el funcionamiento de la red sea crítico para el buen funcionamiento de todo el sistema.

Para analizar el funcionamiento de las redes existen una serie de aplicaciones (vulgarmente conocidas como *sniffers*) que son capaces de capturar y analizar la información que circula a través de ellas (con las lógicas limitaciones impuestas por la topología de la red) ofreciendo al usuario datos de diversa índole acerca del tráfico de la red. A estas aplicaciones nos referiremos como **analizadores de tráfico de red**.

Como es habitual, existe una gran variedad de analizadores de tráfico de red, tanto comerciales como de dominio público.

Para la presente práctica se ha elegido la aplicación ***ethereal*** por las siguientes razones:

- Es probablemente el analizador de tráfico de red más utilizado bajo el sistema operativo *linux*.
- Existe una versión idéntica que funciona bajo entorno *Windows*.
- Es de dominio público.

La aplicación tiene su propia página web http://www.ethereal.com desde la que se pueden descargar tanto fuentes como ejecutables para una gran variedad de sistemas operativos.

Inicialmente la aplicación se diseñó como un entorno gráfico (*front-end*) para la aplicación de consola `tcpdump`, presente comúnmente en las distribuciones *linux*. Debido a su popularidad se desarrollaron posteriormente versiones para diferentes plataformas, entre ellas *Windows*. En esta práctica se empleará dicha versión (la de

Windows) dado que la distribución de *linux* instalada en el laboratorio carece de `tcpdump` y la instalación de ***ethereal*** para *linux* en este caso es demasiado laboriosa.

4 – Desarrollo de la práctica

La práctica consiste en la instalación de ***ethereal*** y la realización de distintas pruebas. Los pasos a seguir se describen a continuación.

3.1 – Instalación y prueba de la aplicación

La aplicación debe encontrarse instalada en los equipos del laboratorio. De no ser así se procederá a descargarla de la dirección habitual de software de prácticas y a instalarla.

Durante el proceso de instalación se nos solicitará que seleccionemos el tipo de interfaz de usuario a emplear entre el GTK1 y el más avanzado GTK2. Una vez cumplimentado este requisito la instalación se completará de forma automática. En caso de utilizar el sistema operativo *Windows NT* ó *2000* (circunstancia que se da en esta ocasión) será necesario instalar también el módulo *WinPcap* para permitir el acceso al hardware del sistema por parte de la aplicación.

Una vez instalada, se puede ejecutar ***ethereal*** mediante el enlace que la instalación ha ubicado en el escritorio. El manual completo (en inglés) está disponible en www.ethereal.com/distribution/docs/user-guide.pdf y en su *capítulo 3* ofrece toda la información necesaria para el uso de la aplicación.

3.1.1 – Primera prueba de captura

Una vez ejecutada la aplicación se efectuará una primera prueba de captura. Previamente se describe el formato de la ventana principal de visualización de datos. Se puede apreciar que ésta se divide en tres secciones horizontales.

En la sección superior aparecerá una lista de tramas de red capturadas, con su información más relevante. En la sección intermedia aparece en forma de árbol la pila de protocolos (conocidos por ***ethereal***) presente en el mensaje. En la sección inferior aparecen los datos sin formatear, es decir, los bytes de que se compone el mensaje, que se muestran en hexadecimal. Se observará posteriormente que, al seleccionar en la ventana intermedia un protocolo (o parte del mismo), se destacarán en la inferior los bytes del mensaje relacionados con aquél.

Pasemos ahora a realizar la captura. Utilizando la opción *Capture* y luego *Start* del menú, aparecerá una ventana que nos permitirá seleccionar ciertas opciones de captura. Entre ellas cabe destacar:

- La ***interfaz de red*** (en caso de que el sistema disponga de varias) desde la que se va a realizar la captura. Deberemos asegurarnos de que está relacionada con la tarjeta de red.
- El ***filtro de captura***, que se comentará posteriormente.
- Los ***límites*** para detener la captura, que pueden fijarse según tiempo, bytes o número de tramas.

- La ***resolución de direcciones*** que se utiliza para mostrar la información en pantalla y que también se comenta más adelante.

Sin modificar ninguno de los parámetros por defecto (excepto tal vez la interfaz de red) se procederá a iniciar la captura pulsando el botón OK. Veremos que aparece una ventana con información diversa acerca de los paquetes que se están capturando. Ejecutemos ahora el *explorer* para conectarnos a Internet y detengamos la captura mediante el botón Stop cuando hayamos capturado algo más de una veintena de tramas.

1 - Analícese el contenido de las ventanas que se han descrito anteriormente.

Repitamos ahora la captura (conexión a Internet incluida) pero seleccionando la opción de resolución de nombres de red (***Enable network name resolution***)

2 - ¿Qué diferencias se observan respecto de la captura anterior?

3.1.2 – Captura de una sesión `ftp`

En segundo lugar se va a capturar una sesión de descarga de archivos mediante del protocolo **`ftp`**. Para ello nos conectaremos a un servidor **`ftp`** anónimo (por ejemplo ftp.rediris.es) usando como nombre de usuario ***anonymous*** y cualquier texto como password. Una vez conectados procederemos a descargar el archivo **`welcome.msg`** del directorio **`mirror`**.

Se observará que, si se efectúan las operaciones anteriores tras haber lanzado una captura como en el apartado anterior, se encontrarán paquetes que no son parte (o al menos no lo parecen) de la sesión **`ftp`**. Para evitar capturar estos paquetes se puede emplear un filtro que se creará mediante la opción *Capture filters* del menú *Edit*.

Cumplimentaremos los recuadros nombre y string como sigue:

Nombre: **`ftp_rediris`**
String: **`tcp port 21 and host ftp.rediris.es`**

Pulsaremos sobre New, Save y Quit para dar de alta el filtro, guardarlo y salir de la ventana de edición de filtros respectivamente, e iremos a iniciar nuevamente la captura.

3 - ¿Cuál es el significado de los textos introducidos en el filtro?

Ahora vamos a analizar los resultados que aparecen en las ventanas de datos. Es interesante responder a las siguientes preguntas:

4 - ¿Se puede encontrar, entre los datos de las tramas capturadas, el contenido del archivo descargado?

5 - ¿Parece **`ftp`** un protocolo seguro para transferencia de datos?

6 - ¿Por qué? Compárese con lo obtenido al hacer las captura de la sesión **`ftp`** sin filtro.

3.2 – Evaluación de la seguridad de aplicaciones en red

En esta sección se utilizará ***ethereal*** para verificar la seguridad (y en general el protocolo) de dos aplicaciones de finalidad similar: **`telnet`** y **`ssh`**.

3.2.1 – Captura de una sesión `telnet`

El objetivo es capturar una conexión **`telnet`** y analizar el protocolo utilizado y la seguridad del mismo. En primer lugar se editará un filtro de captura (según lo visto anteriormente) con el ***string***:

```
tcp port 23 host "nombre del host"
```

Se lanzará una captura con este filtro y se realizará una conexión a la máquina **`labtec16.act.uji.es`** siendo **`userXX`** el texto a introducir como nombre de usuario y **`XXuserXX`** el password, donde **`XX = 01...15`** es el número de puesto de prácticas que se ocupa. Realícense algunas acciones (**`ls`**, **`vi`** *fichero*, etc.) y ciérrese la sesión. Analícense a continuación las tramas capturadas.

7 - ¿Es posible reconocer el password en las tramas capturadas?
8 - ¿Cómo se realiza en el protocolo **`telnet`** la transferencia de datos desde el cliente al servidor?
9 - ¿Y desde el servidor al cliente?

3.2.2 – Captura de una sesión `ssh`

Se repetirá una sesión como la anterior pero mediante el protocolo **`ssh`**. Para ello se cambiará el filtro anterior para que el número de puerto sea el **`22`** y se realizará la conexión y captura de forma similar a la del apartado anterior. Se puede usar **`putty.exe`**, un cliente **`ssh`** que se puede descargar desde:
http://lorca.act.uji.es/933/apps/ethereal/putty.exe

10 - Compárense los datos de la captura (tanto en lo que a seguridad como a protocolo se refiere) con los obtenidos en el apartado anterior.

3.3 – Estadísticas y otras características añadidas

En la opción *Tools* del menú aparecen ciertas utilidades para realizar seguimiento de datos, estadísticas de uso, etc. Es interesante probar algunas de ellas e intentar deducir qué están haciendo exactamente (puede resultar complicado si se carece de suficientes conocimientos de redes)

4 - Conclusiones

En esta práctica se ha visto una aplicación capaz de analizar el tráfico de la red visible a nuestra máquina. Es interesante responder a las siguientes preguntas:

11 - ¿Todos los mensajes que se pueden capturar van dirigidos explícitamente a nuestra máquina?
12 - ¿En qué medida depende la respuesta anterior de la topología de la red?

IS23 Mantenimiento de Instalaciones Informáticas
Práctica 9. Análisis de redes
HOJA DE RESPUESTAS

Práctica realizada por:

Estudiante	Firma