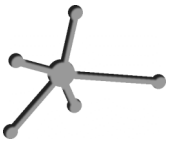
Universidad Pública de Navarra

Grupo de Redes, Sistemas y Servicios Telemáticos



Redes de Ordenadores

Práctica 2: Introducción a Ethereal

Fecha: 13 de Octubre de 2006

Práctica 2: Introducción a Ethereal

1. Introducción

El objetivo de esta práctica es familiarizarse con el laboratorio de telemática, los terminales de red que utilizaremos en las prácticas y la herramienta que se utilizará en una parte de las prácticas.

Con ésta herramienta, llamada Ethereal, podremos capturar los paquetes que circulan por la red, lo cuales nos permitirán una mejor comprensión de las comunicaciones.

2. El laboratorio

El puesto de trabajo consiste en PC´s con sistemas operativos Windows y Linux. Realizaremos las prácticas utilizando ambos.

- Al arrancar el ordenador verá una pantalla de selección de sistema operativo. Para esta primera práctica se utilizará Linux con lo cual seleccionará la opción *Fedora*.
- Introduzca su usuario y contraseña.
- Una vez en el escritorio cambiaremos la contraseña. Para ello abriremos un Terminal pulsando en Programas -> System Tools -> Terminal. Teclee el comando yppasswd. Le pedirá que introduzca la actual contraseña y a continuación la contraseña nueva. De esta manera, se habrá cambiado su contraseña para la cuenta de Linux.

3. Ethereal: herramienta de sniffing

La herramienta a utilizar para capturar paquetes intercambiados en la red se denomina sniffer de paquetes. Se trata de una aplicación que captura los paquetes enviados y recibidos desde nuestra máquina y los analiza mostrándonos su contenido. Es una herramienta de libre distribución que corre sobre Windows, Linux/Unix y Mac OS. Para mayor información podéis visitar la página Web de esta aplicación http://www.ethereal.com. Allí encontrareis una guía de usuario que os explica como conseguir, instalar y utilizar esta herramienta.

4. Utilizando Ethereal

Lanzadlo desde el menú principal. (Programas -> Internet -> Ethereal)

Los menús de comandos son menús desplegables que contienen las acciones elementales de la aplicación. En nuestro caso nos interesa de momento Capture.

El campo Filter permite especificar parámetros requeridos a los paquetes a capturar. Por ejemplo, puede seleccionarse que sólo capture paquetes del protocolo HTTP.

De momento no se observa nada. Capturemos los primeros paquetes y veamos que sucede.

- Arranca el navegador de Internet.
- Para comenzar la captura abre el menú Capture y selecciona Start. Ahí aparecen todas las opciones de captura.
- Dejamos las opciones por defecto y pulsamos OK.
- A continuación aparecerá una ventana de seguimiento de la captura. Indica los tipos de paquetes encontrados y el botón de parada de la captura.
- Una vez hecho esto vaya al navegador y visite la página Web http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html.
  Para conseguir esta página, el navegador (cliente) contactará con un servidor Web mediante el protocolo HTTP (nivel de aplicación de la torre OSI), e intercambiará mensajes con él. Ethereal los capturará.
- Cuando consigáis la página en el navegador id a Ethereal y pulsar STOP. Ethereal nos mostrará los paquetes capturados y podremos ver su contenido.

Observe que en la columna de tipo de protocolo aparecen algunos otros distintos de HTTP, lo que muestra que el hecho de bajar una página involucra otros mecanismos de comunicaciones de los que aparentemente no se tiene constancia. En el campo Filter escribid http.

El primer mensaje HTTP debe ser un mensaje HTTP GET, enviado por nuestra máquina al servidor solicitando la página.

Vea ahora el contenido de cada paquete y conteste a las siguientes cuestiones:

- ¿Cuál es la versión HTTP que usa el navegador? ¿Y el servidor?
- ¿Qué lenguajes acepta el servidor?
- ¿Cuáles son las direcciones IP de su máquina y del servidor Web visitado?
- ¿Cuántos bytes de contenido "pesa" la página?

Pruebe a hacer la misma operación con otra página.

5. Obtención de páginas con protección de autenticación

Veamos ahora que ocurre cuando se requiere un fichero HTML protegido por contraseña.

- Lo primero que debemos hacer es vaciar la caché de nuestro navegador. Para ello vaya a Edit > Preferentes > Advanced > Cache y pulse Clear Cache
- Arranque Ethereal
- Solicite la página

  http://gaia.cs.umass.edu/ethereal-labs/protected_pages/HTTP-ethereal-file5.html
- El navegador le pedirá un usuario y contraseña que son:

  Usename: eth-students

  Password: networks
- Detenga Ethereal
- Examine los mensajes recogidos.

¿Ha encontrado la cadena de caracteres ZXRoLXN0dWRlbnRzOm5ldHdvcmtz? Es una representación codificada en Base64. Visite la Web HTTP://securitystats.com/tools/base64.php y decodifique dicha cadena. ¿Qué obtiene?

Mostrar a la profesora los resultados obtenidos.