Laboratorio 8. Analizador de protocolos Wireshark. Pila de protocolos TCP/IP. Órdenes **ping** y **traceroute**.

Objetivos:

- Familiarización con la herramienta de análisis de protocolos Wireshark
- Comprensión del apilamiento de protocolos y el encapsulado de Protocol Data Units (PDUs) en la pila TCP/IP.
- Identificación de información relevante en las PDUs y sobre el comportamiento de los protocolos: direcciones IP origen y destino, longitudes de cabeceras IP y TCP.
- Uso de la orden traceroute para obtener la ruta que siguen los paquetes IP. Uso de la orden ping para obtener la misma información.

Realización:

- La práctica se realizará en Linux y en el laboratorio del DIT (los resultados que se piden dependen de en qué ordenadores se realiza la práctica, por lo que **debe hacerla en el laboratorio del DIT**).
- La duración estimada es de una hora, pero antes de acudir al laboratorio **debe** haber realizado aquellas partes que no dependan de datos indicados por el profesor en la sesión de laboratorio.
- Antes de realizar la práctica, el alumno habrá leído la sección del capítulo 1 del libro "Computer Networking: a Top Down Approach" dedicada a la orden traceroute. También debe haber leído la introducción y la sección "Sample ping test" de este artículo dedicado a la orden ping: https://en.wikipedia.org/wiki/Ping_(networking_utility)

Resultados:

- En el portal moodle se proporciona un formulario en el que se pide incluir determinados resultados pedidos en el enunciado (los que aparecen subrayados). Debe subir a moodle un fichero ZIP que incluya el formulario con los resultados pedidos, así como dos ficheros con captura de pantalla que se piden en las tareas 4 y 5. En la tarea de entrega se indican los detalles de la subida de resultados.
- En el formulario de entrega aparecen menos cuestiones que en este enunciado. Sin embargo, debe ser capaz de responder todas las cuestiones del enunciado, pues dichas cuestiones también pueden aparecer en los exámenes.

Tareas a realizar:

Tarea 1. Obtención de la dirección IP de su ordenador y del enrutador que está usando.

- Abra una ventana de terminal y en ella dé la orden **`netstat -rn`**
- Se le muestra una tabla con varias filas. Busque la fila con destino ("Destination") 0.0.0.0 y máscara de red ("Genmask") 0.0.0.0. Anote la dirección IP de la pasarela ("Gateway"). Es la dirección IP del enrutador por defecto de su ordenador.
- En esa fila observe también cuál es la interfaz de red que se está usando (columna "Iface"). La interfaz viene identificada por un código de letras y números como enp0s25 u otro código similar. En el resto del enunciado se supondrá que es enp0s25, pero **en su caso debe utilizar el código de interfaz que le muestre su ordenador al ejecutar la orden citada antes.**
- En la ventana de terminal dé la orden **`ifconfig`** ***enp0s25***
- La salida de dicha orden muestra varias informaciones. El texto a continuación de "inet addr" es la dirección IP (versión 4) de su ordenador. Anote la dirección IP de su ordenador.

Tarea 2. Arranque del analizador e inicio de la captura de tráfico.

- Arranque el navegador web (se pide que se haga antes de iniciar la captura con Wireshark para evitar capturar el tráfico de la página web de inicio).
- Vaya al menú de Aplicaciones→Laboratorios docentes del DIT y encontrará una entrada para el programa Wireshark. Inícielo.
- Si le aparece una ventana que le avisa de que está ejecutando el programa como "root", indique que no desea volver a recibirlo y pulse el botón de OK (mientras no lo haga, el analizador no responderá a ningún otro tipo de orden). Si le aparece alguna otra ventana inicial con avisos de error ignórelos también pulsando el botón OK. Al final del enunciado se muestra una captura de pantalla con el interfaz de usuario de Wireshark. Algunos detalles del interfaz como la apariencia o la posición de algún botón de acción que se menciona más abajo pueden variar ligeramente dependiendo de la versión del programa Wireshark que esté utilizando.
- En la ventana del analizador, a la izquierda, aparece una lista de conexiones de red (interfaces) de las que puede capturar. Arranque una captura de tráfico marcando con el ratón la interfaz de red *enp0s25* y pulsando a continuación el botón "Start" (aleta de tiburón azul).

Tarea 3. Generación de tráfico y su captura.

- Tras arrancar la captura, vaya con el navegador a la página

`http://www.dit.upm.es/~ftel/lab8.php`

- Cuando la página se haya mostrado, detenga la captura de tráfico en el analizador pulsando el botón rojo cuadrado, que está en la parte superior.
- Aplique un filtro de presentación para mostrar sólo el tráfico con el servidor web. Para ello escriba **`http and ip.addr == 138.4.2.56`** en el espacio junto a "Filter" y pulse "Apply".

Tarea 4. Estudio del protocolo IP.

- En el panel superior del analizador, donde se muestran los paquetes capturados, busque los paquetes cuya dirección IP origen sea la de su ordenador.
- Examine el análisis la cabecera del protocolo IP del primero de dichos paquetes. Tendrá que usar la información que proporciona el panel intermedio; el detalle de cada protocolo se consigue picando con el ratón sobre los signos ▷ que apuntan a cada protocolo; para ocultar de nuevo la información, se vuelve a picar sobre el ▷ que se expandió).
- Para ese paquete anote la longitud de la cabecera IP y la longitud total del paquete IP.
- En el panel intermedio, pique con el ratón sobre la línea que empieza con "▽ Internet Protocol version 4". Observe que en el panel inferior se marcan en azul varios octetos. Son la cabecera IP. Haga una captura de pantalla en la que el analizador muestre dichos octetos pulsando la tecla ImprPant. Renombre la imagen capturada a **`tarea4.png`**.
- Como ya sabe, una dirección IP (v4) es un número de 32 bits que se suele representar con la notación punto (ej.: 138.4.1.193). En el panel intermedio busque la línea que empieza por "Source:" y pulse sobre ella. En el panel inferior se marcan los octetos que en la cabecera IP llevan la dirección origen del paquete IP. Indique en qué posición dentro de la cabecera IP se encuentran. Indique justificadamente si al transmitirse por la red los octetos de la dirección IP se envían en el orden del convenio extremista mayor o el extremista menor.

Tarea 5. Estudio del protocolo de transporte.

- Identifique el protocolo de transporte que se está usando en el paquete examinado.
- En el panel intermedio, pulse sobre la línea que empieza por "▷" correspondiente a la capa de transporte y observe la cabecera de transporte en el panel inferior. Haga una captura de pantalla en la que se muestren los octetos de la cabecera de transporte. Renombre el fichero de la imagen capturada a **`tarea5.png`**.
- Examine ahora la cabecera de transporte del paquete estudiado en el apartado anterior. Dé la longitud de su cabecera.
- Anote los puertos origen y destino del paquete examinado. ¿Qué protocolo de aplicación está asociado al puerto destino?
- ¿Cómo están colocadas entre sí las cabeceras de los protocolos IP, transporte y aplicación?

Tarea 6. Uso de la orden traceroute. Esta orden nos va a permitir conocer la ruta que sigue el tráfico IP entre su ordenador y la máquina que se especifica como destino.

- En una ventana de terminal dé la orden siguiente: **`traceroute -N 1 www.dit.upm.es`**
- ¿A cuántos saltos se encuentra la máquina www.dit.upm.es de su ordenador?
- ¿Cuál es la dirección IP del equipo que se encuentra a un salto de distancia de su ordenador? ¿En qué tarea anterior le ha aparecido esta dirección? ¿Por qué aparece aquí también?
- Pregunte a un compañero la dirección IP de su puesto de laboratorio y haga un traceroute a esa dirección (**`traceroute`** ***direcciónIPdesuCompañero***). ¿A cuántos saltos está dicha máquina de su ordenador? ¿La máquina que está a un salto de distancia es la misma que en el apartado anterior? ¿Por qué?

NOTA: la opción -N de traceroute permite controlar el número de mensajes de sonda que se envían simultáneamente por el programa traceroute. Por defecto, traceroute envía un número grande, que en algunos cortafuegos se puede descartar. Al limitar ese número, los cortafuegos no ven un tráfico tan agresivo y baja la probabilidad de descarte.

Tarea 7. Uso de la orden ping.

- La orden ping admite varias opciones, como el tamaño de los mensajes que se envían, cuántos mensajes de sonda se envían, o controlar cuántos saltos como máximo puede dar el paquete en su ruta hacia el destino especificado. En esta tarea se usarán las dos últimas opciones. Indicaremos a la orden ping que envíe tres mensajes de sonda con la opción **`-c 3`**. Si *N* es el número máximo de saltos que permitimos, en Linux se especifica con la opción **`-t`** *N*. En una ventana de terminal ejecute la orden siguiente para hacer ping al sitio www.esa.int:

```
ping -c 3 -t 1 www.esa.int
```

- En esta orden la opción de número máximo de saltos *N* toma el valor inicial 1 y se envían 3 paquetes de sonda. ¿Qué mensajes presenta ping? ¿Ve alguna información relacionada con la respuesta de la tarea 1?
- Repita la orden ping incrementando de uno en uno el valor de *N* hasta obtener contestación de www.esa.int. En todo caso, tome nota de las direcciones IP de las máquinas que generan los mensajes de respuesta que recibe para cada valor de N que va probando, aunque no sean de www.esa.int.
- ¿Con qué valor del número de saltos obtiene respuesta del sitio www.esa.int?
- Tome nota de la dirección IP que le responde finalmente.
- Haga un traceroute, con la opción -N 1, a la dirección IP anotada en el punto anterior. Compare las direcciones IP que le va mostrando asociadas a cada número de saltos con las direcciones que le han aparecido en los pings que ha hecho en esta tarea y explique las coincidencias.
- ¿Qué tipo de equipos ("hosts" o "routers") deben ser las máquinas que contestan con el mensaje de número de saltos insuficiente para llegar al destino final?
- A la vista de lo estudiado en esta tarea, tiene información suficiente para deducir cómo el programa traceroute consigue obtener la ruta que siguen los paquetes entre su ordenador y la máquina destino del traceroute. Explíquelo.

Tarea 8. Traceroute a un servidor web.

Este punto se debe realizar en la sesión de laboratorio planificada en su grupo. En el laboratorio el profesor indicará el nombre de un servidor web al que debe realizar el traceroute. En la ventana de terminal dé la orden:

`traceroute -N 1` ***servidorDeSuGrupo***

- Incluya la salida de dicha orden en el formulario de respuesta. ¿A cuántos saltos se encuentra de su ordenador el servidor indicado? ¿Entre qué máquinas (dé sus nombres y direcciones IP) se produce el mayor incremento del RTT? Indique una posible explicación de este incremento.

Apéndice. Pantalla principal de Wireshark.

Como orientación, la imagen siguiente muestra el aspecto del analizador tras haber terminado una captura, viendo el detalle del protocolo IP de paquete nº 23 que aparece seleccionado en el panel superior.