Mayo de 2021

Contenido

Práctica 5: TCP, DNS

Resumen

En esta práctica continuaremos aprendiendo sobre el funcionamiento básico del **protocolo de nivel de transporte TCP**, así como también sobre el **servicio DNS**

⚠️ **Nota importante**: Al cargar capturas en Wireshark es necesario **ordenar los paquetes** por su **marca de tiempo**. Para ello, pulsa en la pestaña **Time** , de esta forma podremos analizar lo que ha ocurrido ordenadamente, siguiendo el eje temporal

Descargas

- **Guión de la práctica en PDF**: P5-guion.pdf (opcional) (es lo mismo de esta wiki)
- **Información adicional**: herramientas-conexiones.pdf: Herramientas para el análisis de comunicaciones TCP/UDP

Ficheros que debes **descargar** para realizar la práctica:

- **Captura 1**: captura-1-tcp.cap
- **Captura 2**: captura-2-tcp-mss-pmtu.cap
- **Captura 3**: captura-3-tcp-window.cap
- **Captura 4**: captura-4-tcp-timeout-probes.cap
- **Captura 5**: captura-5-nav-web-browser.pcap

1. Comunicación de aplicaciones usando el protocolo TCP

1.1 Análisis inicial de la captura de TCP

Utilizando Wireshark, abre la captura 1 (captura-1-tcp.cap). En ella se muestra una comunicación TCP entre dos aplicaciones

Contesta a las siguientes preguntas:

1. ¿Cuál es la dirección IP y el puerto del cliente TCP y la dirección IP y el puerto del servidor TCP?
2. ¿Cuántos segmentos TCP se han enviado desde el cliente al servidor?
3. ¿Cuántos segmentos TCP se han enviado desde el servidor al cliente?
4. Indica qué extremo cierra antes la conexión (cliente o servidor)

1.2. Números de secuencia

Sigue analizando la captura 1

En el menú de Wireshark, seleccionando en el menú Edit → Preferences → Protocols → TCP, puedes desactivar la opción **Relative Sequence Numbers & Window Scaling**. De esta forma podrás observar los números de secuencia reales, en lugar de los números relativos que muestra por omisión Wireshark

1. ¿Cuántos bytes de datos envía el servidor al cliente? Razona la respuesta. Indica cuáles son los números de secuencia del SYN y del FIN que envía el servidor, y qué relación tienen con la cantidad de datos enviada por el servidor al cliente

2. ¿Cuántos bytes de datos envía el cliente al servidor? Razona la respuesta. Indica cuáles son los números de secuencia del SYN y del FIN que envía el cliente, y qué relación tienen con la cantidad de datos enviada por el cliente al servidor

Cuando hayas observado los números de secuencia reales, **vuelve a activar** la opción **Relative Sequence Numbers & Window Scaling** para que resulte más fácil analizar la captura en los siguientes apartados

1.3. RTT

Continúa analizando la captura 1

1. Para cada uno de los segmentos de datos que envía el cliente al servidor, indica cuál es el RTT. Observa para ello los tiempos de envío de los segmentos y los de recepción de sus correspondientes asentimientos

1.4. MSS

Abre ahora el archivo de captura 2 (captura-2-tcp-mss-pmtu.cap). En ella se muestra el principio de una comunicación TCP. Ordena en Wireshark los paquetes por la columna Time

Contesta a las siguientes preguntas:

1. Indica cuál es el **valor anunciado** de **MSS** en las cabeceras opcionales de los **paquetes SYN** de los dos sentidos de la conexión. Dados estos dos valores, indica qué tamaño de datos crees usarán ambos sentidos de la conexión si tienen que enviar datos

2. Mira los **tamaños de las cabeceras** de los distintos segmentos, medidos en palabras de **4 bytes** y razona por qué no todos los segmentos tienen el mismo tamaño. ¿Crees que el tamaño de la cabecera puede influir en el tamaño máximo de datos que posteriormente utilizará TCP para enviar segmentos?

3. Teniendo en cuenta que en el instante en el que se envía el **segmento número 4**, la máquina 11.0.0.11 tenía más de 2.000 bytes de datos que enviar a la máquina 12.0.0.12, ¿por qué envía menos? ¿Cuántos bytes envía en ese segmento 4? ¿Cómo se justifica el número de bytes de datos que contiene el segmento 4 dados los valores de MSS anunciados en los segmentos SYN?

4. Explica qué tipo de paquete son los **paquetes 5** y **7** de la captura. ¿Qué significan y cuál puede ser la razón de que se hayan enviado? ¿Qué campo de la cabecera IP de los paquetes 4 y 6 ha provocado que se envíen los paquetes 5 y 7?

5. Mira el **paquete 8** de la captura. ¿Por qué se retransmite este segmento? Comprueba el tamaño de su campo de datos. Explica la relación de este valor con la información contenida en los paquetes 5 y 7

1.5. Funcionamiento básico de la ventana anunciada

En la **captura 3** (captura-3-tcp-window.cap) se muestra el **principio** de una **comunicación TCP**. Para este apartado, utiliza en Wireshark los números de secuencia relativos al principio de la conexión. Ayudándote de la gráfica `tcptrace` (Consulta el documento *Herramientas para el análisis de comunicaciones TCP/UDP*), en la segunda sección Análisis de gráficas tcptrace de conexiones TCP, contesta a las siguientes preguntas relativas al sentido de comunicación 12.0.0.100 → 13.0.0.100:

1. ¿Cuál es el número de secuencia del primer byte de datos contenido en el paquete número 6?

2. ¿Cuál es el número de secuencia del último byte de datos contenido en el paquete número 6?

3. El paquete número 7, ¿cuántos bytes de datos asiente?

4. En el momento de enviar el paquete número 8, ¿cuál es el último valor de ventana anunciada por el receptor que ha recibido el emisor? ¿En qué número de paquete venía anunciado? ¿Cuántos bytes de

datos puede enviar como máximo el emisor en ese momento, en uno o más segmentos, antes de volver a recibir otro ACK del receptor?

5. En el momento de enviar el paquete número 13, ¿cuál es el último valor de ventana anunciada por el receptor que ha recibido el emisor? ¿En qué número de paquete venía anunciado? ¿Cuántos bytes de datos puede enviar como máximo el emisor en ese momento, en uno o más segmentos, antes de volver a recibir otro ACK del receptor?

6. ¿Podría haber enviado el emisor un segmento con datos nuevos en el instante 0.321000 segundos? ¿Por qué?

7. Identifica en la gráfica tcptrace de este sentido de la comunicación en qué otro periodo de tiempo se produce una situación similar a la que ocurre al enviarse el paquete número 13

1.6. Retransmisiones y asentimientos

En la **captura 4** (captura-4tcp-timeout-probes.cap) se muestra el **principio** de una **comunicación TCP**. Para este apartado, utiliza en Wireshark los números de secuencia relativos al principio de la conexión. Ayudándote de la gráfica tcptrace , contesta a las siguientes preguntas relativas al sentido de comunicación 12.0.0.100 → 13.0.0.100:

1. El paquete **número 16** es una retransmisión, aunque Wireshark no lo etiqueta como tal:

- a) Mirando la gráfica tcptrace , ¿cómo puede identificarse que dicho paquete 16 es una retransmisión?
- b) ¿Qué número de paquete es la primera transmisión de los bytes de datos que viajan en este paquete 16?
- c) ¿Cuál ha sido el plazo de retransmisión aplicado a esa primera transmisión del paquete?
- d) Mirando la gráfica tcptrace , ¿vuelve a ser retransmitido este paquete en la conexión? ¿Con qué plazo de retransmisión? ¿Por qué?

2. Identifica en la gráfica tcptrace otros segmentos que son retransmisión
3. En el momento de transmitir el paquete 18, ¿cuántos bytes están transmitidos y pendientes de que llegue su asentimiento? ¿Y cuántos paquetes (indica su número de paquete)?
4. El paquete 19 es un asentimiento. ¿Cuántos bytes asiente? ¿Y cuántos segmentos?
5. Identifica con ayuda de la gráfica tcptrace otros asentimientos que asienten varios paquetes a la vez

2. Tráfico DNS y HTTP

Tal y como hemos visto en teoría, el **servicio DNS** ofrece mecanismos para poder **descubrir la dirección IP** que corresponde a una máquina con la que queremos establecer un diálogo a nivel de transporte (con TCP o UDP). Uno de los ejemplos más típicos de uso de este servicio es al utilizar un navegador web

El archivo de **captura 5** (captura-5-nav-web-browser.pcap) contiene un extracto de una captura original de tráfico de red con Wireshark. Abre ese archivo con Wireshark y contesta a las siguientes preguntas:

1. ¿Cuántas solicitudes de resolución de la IP correspondiente a un FQDN se realizan en esta captura? Identifica, concretamente, cuáles son los FQDN cuya dirección IP se solicita, así como la IP que el

servicio DNS informa que corresponde a esos nombres de dominio. ¿Qué dirección IP tiene el servidor DNS que contesta?

2. Dibuja un pequeño diagrama en el que se indique cúantos diálogos TCP puedes idetificar en esta captura. Para cada diálo TCP debes indicar:

- La IP de la máquina cliente y la IP del servidor, así como el puerto de comunicación empleado en ambos extremos
- Los números de secuencia anunciados en la apertura de cada conexión por ambos extremos
- ¿Cuántos de los diálogos TCP abiertos finalizan correctamente? Indica, concretamente, el número de trama capturada en Wireshark que corresponde a los segmentos TCP intercambiados para cerrar cada conexión