



IIC2333 — Sistemas Operativos y Redes — 2/2021

Tarea 4

6 de diciembre, 2021

Fecha de entrega: 13 de diciembre, hasta las 23:59

Fecha de ayudantía: Por definir, 2021

Composición: en parejas (2 personas)

Objetivos

En esta tarea deberán monitorear y analizar paquetes de datos de la red a través del programa [Wireshark](#). La tarea consiste de distintos casos que les permitirán familiarizarse con el programa y conocer más sobre los dispositivos conectados a la red y protocolos de red.

En el caso de la actividad **presencial**. Deberán configurar sus computadores y conectarlos a la red como les indican los ayudantes. Esta conexión es estática y será una subred que no conecta con Internet.

Caso 1: Servidor UDP (15 puntos)

Junto con este enunciado se les entregó un archivo ejecutable: `broadcast_OS`, en donde `OS` corresponde a su sistema operativo. Este archivo permite correr un servidor UDP que hace **broadcast** de mensajes constantemente. Deberán correr este servidor y mientras esté corriendo deben encontrar y analizar los paquetes correspondientes usando el programa Wireshark. En específico, deberán realizar lo siguiente:

- Ejecuten el archivo `broadcast_OS` a través del siguiente comando en consola:

```
$ ./broadcast_OS <numero_de_alumno_sin_último_dígito>
```

Esto ejecutará el servidor UDP, el cual comenzará a hacer *broadcast* de mensajes.

- Usando Wireshark, notarán que aparecen muchos paquetes de tipo UDP. Cree un filtro de forma que solo se capturen paquetes cuya IP de destino sea `255.255.255.255` y que el protocolo sea UDP. ¿Cuál es este filtro?
- ¿Cuál es el tamaño en bytes del paquete completo? ¿Cuántos de estos corresponden a UDP? ¿A qué se debe esta diferencia?
- ¿Cuál es el mensaje que emite el servidor? ¿Cuál es su largo en bytes en el paquete?
- Si quisieras enviar un mensaje broadcast a todos los usuarios de la red `192.168.0.0/24`. ¿Cuál debería ser la IP de destino del mensaje?

Caso 2: Servidor HTTP (30 puntos)

Para esta parte deberán conectarse a un servidor y capturar los distintos paquetes que se envían hacia y desde este. Notar que este caso es distinto dependiendo del tipo de actividad que desean realizar (remota o presencial).

Actividad Presencial

1. Abra un cliente web y borre su caché.
2. Inicie una captura de paquetes con Wireshark sin aplicar un filtro inicial.
3. Acceda al sitio `http://192.168.0.7:8080/`.
4. Acceda al sitio `http://192.168.0.7:8080/big.txt`.
5. Acceda al sitio `http://192.168.0.7:8080/small.txt`.
6. Vuelva a acceder al sitio `http://192.168.0.7:8080/`.
7. En Wireshark, encuentre el paquete GET de la imagen que sale en la pagina y guarde la dirección que usa para obtenerla.
8. Usando la dirección encontrada en el punto anterior, reemplace el nombre de la imagen por `win98.mp3` y acceda desde su navegador.
9. Acceda al sitio `http://192.168.0.7:8080/meme`.
10. **Guarde el resultado de su captura (dump). Verifique que está correctamente guardado, de lo contrario no podrá completar el resto de la experiencia**

Preguntas actividad presencial

Utilizando los datos obtenidos anteriormente deberán responder las siguientes preguntas.

1. ¿Qué browser hace la solicitud? Agregue al informe una captura de pantalla de *Wireshark* indicando donde se muestra el navegador.
2. Para los accesos con finalización `/big.txt` y `/small.txt` ¿cuales son los códigos HTTP de respuesta? ¿Qué significan?
3. ¿Cual es la dirección obtenida de la imagen de la primera vista? Agregue al informe una captura de pantalla de *Wireshark* indicando donde se muestra.
4. Para cada acceso de la captura, ¿cuántos byte retorna el browser en cada acceso?
5. Para cada acceso, ¿cuántos GET se efectúan en cada caso y por qué?

Actividad Remota

1. Abra un cliente web y borre su caché.
2. Inicie una captura de paquetes con Wireshark sin aplicar un filtro inicial.
3. Acceda al sitio `http://iic2333.ing.puc.cl/`.
4. Acceda nuevamente al sitio `http://iic2333.ing.puc.cl/`.
5. Acceda al sitio `http://iic2333.ing.puc.cl/images/figures/logo1.gif`.
6. Acceda al sitio `http://iic2333.ing.puc.cl/images/figures/logo2.gif`.
7. Acceda al sitio `http://iic2333.ing.puc.cl/slides/7-net.html/`.

Preguntas actividad remota

Utilizando los datos obtenidos anteriormente deberán responder las siguientes preguntas.

1. ¿Qué browser hace la solicitud? Agregue al informe una captura de pantalla de *Wireshark* indicando donde se muestra el navegador.
2. Para los accesos con finalización `/logo1.gif` y `/logo2.gif` ¿cuales son los códigos HTTP de respuesta? ¿Qué significan?
3. ¿Cual es la dirección del servidor donde está almacenada la imagen de *linux power*? Agregue al informe una captura de pantalla de *Wireshark* indicando donde se muestra.
4. Para cada acceso de la captura, ¿cuantos byte retorna el browser en cada acceso?
5. Para cada acceso, ¿cuántos GET se efectúan en cada caso y por qué?

Caso 3: Protocolos de mensajes (15 puntos)

Dentro de una red se envían mensajes pertenecientes a variados protocolos. En los casos anteriores nos enfocamos principalmente en UDP y HTTP. En este caso observaremos otro protocolos que se suelen utilizar.

- Mande un `ping` desde su dispositivo al *default gateway*. Para esto deberá buscar la IP de su *default gateway* y luego escribir en consola el comando `ping [IP_DESTINO]`. Wireshark capturará paquetes de un protocolo en particular. ¿Cual es el protocolo de estos paquetes según Wireshark? ¿Para qué se utiliza generalmente este protocolo?
- Si no utilizan ningún filtro, cada cierto tiempo va a recibir un paquete de protocolo ARP. ¿Cuál es la finalidad de este protocolo?
- Indique utilizando Wireshark si el servicio DHCP está habilitado en su red local. Esto lo puede comprobar observando lo que ocurre en Wireshark cuando se conecta a su red local. Describa lo que realizó para llegar a su respuesta.

Entrega y formalidades

Deberán subir un archivo .pdf a la carpeta T4 de su directorio en el servidor del curso. Este archivo deberá contener sus respuestas a todas las preguntas de los puntos anteriores.

El nombre del archivo debe tener el siguiente formato: t4_[numalumno_1]_[numalumno_2].pdf. Por ejemplo, si el número de alumno del integrante 1 es 12345678 y el del integrante 2 es 22446688, su archivo a subir tendrá por nombre t4_12345678_22446688.pdf.

En caso de ser un solo alumno, el archivo debe tener el formato: t4_[numalumno].pdf. Por ejemplo, si su número de alumno es 12345678, su archivo a subir tendrá por nombre t4_12345678.pdf.

Nota final

La nota final de la tarea entregada a tiempo se calcula de la siguiente manera:

$$N = 1 + \frac{\sum_i p_i}{10}$$

Siendo p_i el puntaje obtenido en caso i de la tarea.