PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC2333 — Sistemas Operativos y Redes — 2/2018

# Tarea 3

Miércoles 24-Octubre-2018

**Experiencia práctica: Miércoles 24 de Octubre de 2018, 8:30-9:50, Sala E10**
**Fecha de Entrega: Miércoles 31-Octubre-2018 a las 23:59**
**Composición: Individual o en parejas**

## Objetivo

En esta tarea efectuaremos una experiencia práctica de monitoreo en una LAN. Deberán analizar el tráfico de tipo HTTP y TCP de una LAN conectada por *switches*. Para analizar el tráfico, utilizaremos la herramienta de análisis de redes en *Wireshark*. Posteriormente, deberán elaborar un informe con sus observaciones y responder a las preguntas propuestas.

## Pasos previos

Para el día de la experiencia necesitarán:

- Saber cómo configurar una dirección IP estática, **de manera manual** (no con DHCP) en su sistema operativo.
- Tener instalado *Wireshark* en su computador.
- Saber cómo aplicar filtros y guardar capturas con *Wireshark*. Puede encontrar más información en la ayudantía realizada para esta tarea.

# Actividad de laboratorio

## Parte (a)

1. Identifique el nombre de su interfaz de red dentro de su sistema operativo.
2. Configure su interfaz de red de acuerdo a la IP y subred indicados por los ayudantes.
3. Limpie la tabla ARP de su computador.
4. Abra un cliente *web* y borre su *caché*.
5. Inicie una captura de paquetes con *Wireshark* **sin aplicar un filtro inicial**.
6. Acceda al sitio `http://192.168.1.9:3000/register`.
7. Acceda al sitio `http://192.168.1.9:3000/`.
8. Vuelva a acceder al sitio `http://192.168.1.9:3000/`.
9. Acceda al sitio `http://192.168.1.9/big.txt`.
10. En *Wireshark*, encuentre el paquete GET de la imagen que sale en la página y guarde la dirección que usa para obtenerla.
11. Usando la dirección encontrada en el punto anterior, reemplace el nombre de la imagen por `win98.mp3` y acceda desde su navegador.
12. Acceda al sitio `http://192.168.1.9/meme`.

13. Limpie la tabla ARP de su interfaz de red y obtenga el estado de la tabla.
14. Acceda al sitio `http://192.168.1.9/power`, y realice lo que indica la página.
15. Tome nota del contenido de la tabla ARP de su interfaz de red.
16. Tome nota de la arquitectura de la red construida en la sala: modelos de *switch* y *Access Point* inalámbricos, cantidad de puertos, y cómo están conectados.
17. **Guarde el resultado de su captura (*dump*). Verifique que está correctamente guardado, de lo contrario no podrá completar el resto de la experiencia**.

**Usando los datos capturados** y aplicando los filtros que necesite, responda las siguientes preguntas. Puede utilizar tablas cuando sea conveniente para mostrar la información.

1. ¿Qué *browser* hace la solicitud?
2. Para cada acceso, ¿en qué formato se transfieren los datos?
3. Para cada acceso, ¿cuál es el código HTTP de respuesta?
4. ¿Cuál es la dirección obtenida de la imagen de la primera vista?
5. ¿Qué tipo de paquetes se registraron cuando abrieron la dirección reemplazando el nombre de la imagen por `win98.mp3`? ¿Por qué existen múltiples paquetes de este tipo luego de acceder? ¿Cuántos *bytes* se transmitieron del archivo?
6. Para cada acceso de la captura, ¿cuántos *byte* retorna el *browser* en cada acceso?
7. Para cada acceso, ¿cuántos GET se efectúan en cada caso y por qué?
8. ¿Podría indicar si las imágenes de `http://192.168.1.9/meme` se descargan en forma serial o si esta operación se realiza en paralelo?
9. ¿Qué método (de HTTP) se usa en el caso de la *request* `http://192.168.1.9/power` y por qué? ¿Qué inconvenientes podría provocar el no usar ese método?

## Parte (b)

**Usando los datos capturados** y aplicando los filtros que necesite, para monitorear su tráfico con el protocolo TCP. Para cada acceso de la parte **(a)** agregue la siguiente información:

1. ¿Cuántos segmentos TCP se transmiten en cada acceso?
2. ¿Cuáles son los rangos de segmentos TCP que corresponden a cada mensaje HTTP?
3. ¿Hubo paquetes perdidos, dañados, o duplicados? Indique cuántos hubo de cada caso y cómo los identificó.
4. Identifique **una** secuencia de *handshake*. Indique en qué paquetes se efectúa y los números de secuencia de cada lado.

## Parte (c)

**Usando los datos capturados** y aplicando los filtros que necesite, filtre los resultados de acuerdo al protocolo ARP.

1. Construya una lista que incluya los miembros observados en la red. cada entrada de la lista debe incluir: dirección MAC, dirección IP y fabricante de tarjeta de red.
2. Explique por qué podrían existir direcciones IP sin información dentro de la tabla ARP de su interfaz de red.
3. Para una de las direcciones obtenidas luego del *ping*, identifique los paquetes que se envían por la red y que permitan descubrir la dirección MAC de ese miembro de la red.

### Referencias

- Funcionamiento del protocolo HTTP[1]
- Funcionamiento del protocolo ARP[2]

## Informe

Debe entregar la captura de paquetes (*packet dump*) de su ejecución y un reporte donde se aborden los siguientes aspectos:

- Diagrama de la red. Debe incluir descripción de la subred y equipos involucrados.
- Respuestas parte **(a)**. Puede utilizar una tabla para resumir los paquetes HTTP y los byte.
- Respuestas parte **(b)**. Puede utilizar una tabla para asociar los mensajes HTTP con los paquetes TCP correspondientes.
- Respuestas parte **(c)**.

## Entrega

A cada alumno se le asignó un nombre de usuario y una contraseña para el servidor del curso (`iic2333.ing.puc.cl`). Para entregar su tarea usted deberá crear una carpeta llamada `T3` en el directorio de su carpeta personal y subir su tarea a esa carpeta. Puede ser realizada en forma individual, o en grupos de 2 personas, donde basta que uno de los integrantes se encargue de subir lo solicitado. En cualquier caso, recuerde indicar en el informe los autores de la tarea con sus respectivos números de alumno.

En su carpeta `T3` se debe incluir:

- Informe en formato PDF.
- Captura de los paquetes (archivo de *Wireshark*).

Se revisará el contenido de dicha carpeta el día Miércoles 31 de octubre de 2018 a las 23:59.

## Evaluación

Se evaluarán los siguientes aspectos.

- 10 % Formato: Formalidad en la presentación, presencia de items requeridos.
- 10 % Entrega de paquetes capturados.
- 20 % Diagrama de la red
- 20 % Respuestas parte (a)
- 20 % Respuestas parte (b)
- 20 % Respuestas parte (c)

[1] https://code.tutsplus.com/tutorials/http-the-protocol-every-web-developer-must-know-part-1--net-31177
[2] http://securityxploded.com/basics-nic-mac-and-arp-tutorial.php

## Política de atraso

Se puede hacer entrega de la tarea con un máximo de 2 días de atraso. La fórmula a seguir es la siguiente:

$$N_{T_3}^{\text{Atraso}} = N_{T_3} - 1{,}5 \cdot d$$

Siendo $N_{T_3}$ la nota obtenida a partir de los elementos descritos y $d$ la cantidad de días de atraso.

## Preguntas

Cualquier duda preguntar a través del foro.