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

IIC 2333 — Sistemas Operativos y Redes — 1/2017

**Tarea 5**

**Experiencia práctica: Lunes 12-Junio de 2017, 08:30-09:50, Sala C201**
**Entrega reporte: Lunes 19-Junio de 2017, 23:59**
**Composición: grupos de $n$ personas, donde $n \leq 2$**

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 *Wireshark*. Posteriormente deberán elaborar un informe con sus observaciones.

### Pasos previos

Para el día de la experiencia necesitarán:

- Saber cómo configurar una dirección IP estática, de manera manual (no con DHCP) en el sistema operativo de su computador.
- Tener instalado Wireshark en su sistema operativo
- Saber cómo aplicar filtros y guardar capturas con Wireshark

## Actividad de laboratorio

### Parte (a)

- Abra un cliente web y borre su caché.
- Configure *Wireshark* para monitorear el tráfico bajo el protocolo `http`
- Acceda al sitio `http://192.168.1.9/`
- Acceda al sitio `http://192.168.1.9/build/slides/5-disk.html`
- Vuelva a acceder al sitio `http://192.168.1.9/build/slides/5-disk.html`
- Acceda al sitio `http://192.168.1.9/big.txt`
- Acceda al sitio `http://192.168.1.9/up.html`, y complete el formulario
- Guarde el resultado de su captura (*dump*)

Usando los datos capturados responda las siguientes preguntas:

1. ¿Qué browser hace la solicitud?
2. ¿Qué sistema operativo y web server responde?
3. ¿En qué formato se transfieren los datos en cada caso?
4. ¿Cuál es el código HTTP de respuesta en cada caso?
5. ¿Cuántos byte retorna el browser en cada caso?
6. ¿Cuántos GET se efectúan en cada caso y por qué?
7. ¿Qué método se usa en el caso de la *request* `http://192.168.1.9/up.html` y por qué?

### Parte (b)

Utilice la captura de la parte (a) y agregue el filtro para monitorear su tráfico con el protocolo tcp.
Para cada uno de los casos de la parte (a) agregue la información de:

1. ¿Cuántos segmentos TCP se transmiten en cada caso?
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.
4. Identifique una secuencia de *handshake*. Indique en qué paquetes se efectúa y los números de secuencia de cada lado.
5. Calcule el *throughput* (bytes por unidad de tiempo) de cada *request* y *response HTTP*. Describa brevemente cómo calculó este valor.

### Parte (c)

Utilice la captura de la parte (a), y ejecute las instrucciones obtenidas después de acceder a `http://192.168.1.9/up.html`.
A continuación filtre los resultados de acuerdo al protocolo ARP, y construya una lista que incluya los miembros observados en la red. Cada entrada de la lista debe incluir: dirección MAC, dirección IP, fabricante de tarjeta de red.

### Parte (d)

Analice el resto de la captura, e identifique si hubo otro tipo de tráfico. En caso que lo haya, mencione a lo más 3 tipos de tráfico distintos que haya en su captura, la cantidad de paquetes vistos de cada caso, y a qué protocolo corresponden. Estos tráficos no pueden ser HTTP, TCP ni ARP.

### Referencias

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

## Informe

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

- 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).
- Respuestas parte (d).

[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

## Evaluación

Para la evaluación deberá subir en un cuestionario de SIDING un archivo zip que incluya su informe en formato PDF, y la captura de paquetes.

Se evaluará, con una escala de 1 a 7, los siguientes elementos. La nota final de la tarea será el promedio ponderado de ellas.

- 10 % Formato: Formalidad en la presentación, presencia de items requeridos.
- 10 % Entrega de paquetes capturados.
- 25 % Respuestas parte (a)
- 25 % Respuestas parte (b)
- 15 % Respuestas parte (c)
- 15 % Respuestas parte (d)