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

IIC 2333 — Sistemas Operativos y Redes — 1/2018

Tarea 5

Profesor: Cristian Ruz

Ayudantes: Lukas Svicarovic (lsvicarovic@uc.cl), Jurgen Dieter Heysen Palacios (jdheysen@uc.cl)

Experiencia práctica: Miércoles 13 de junio de 2018, 10:00-11:20, Sala E10
Entrega reporte: Miércoles 20 de junio de 2018, 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 su sistema operativo.
- Tener instalado *Wireshark* en su sistema operativo
- Saber cómo aplicar filtros y guardar capturas con *Wireshark*

Actividad de laboratorio

Parte (a)

- Identifique el nombre de su interfaz de red dentro de su sistema operativo
- Configure su interfaz de red de acuerdo a la IP y subred indicados por el ayudante.
- Limpie la tabla ARP de su computador.
- Abra un cliente web y borre su caché.
- Inicie una captura de paquetes con *Wireshark* **sin aplicar un filtro inicial**
- Acceda al sitio `http://192.168.1.9:3000/register`
- Acceda al sitio `http://192.168.1.9:3000/`
- Vuelva a acceder al sitio `http://192.168.1.9:3000/`
- Acceda al sitio `http://192.168.1.9/big.txt`
- Acceda al sitio `http://192.168.1.9/meme`
- Acceda al sitio `http://192.168.1.9/power`, y complete el formulario. Luego realice lo que indica la página.
- Limpie la tabla ARP de su interfaz de red y obtenga el estado de la tabla.

- Utilice la herramienta *ping* para enviar paquetes *ICMP Echo Request* a 6 direcciones IP distintas dentro de la subred, y que no sea la dirección propia. Asegúrese que al menos 4 de ellas respondan y que una corresponda a un computador que no esté conectado al mismo *switch* o *Acces Point*.
- Tome nota del contenido de la tabla ARP de su interfaz de red.
- 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.
- Guarde el resultado de su captura (*dump*)

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. ¿Qué sistema operativo y *web server* responden?
3. Para cada acceso, ¿en qué formato se transfieren los datos?
4. Para cada acceso, ¿cuál es el código HTTP de respuesta?
5. Para cada acceso, ¿cuántos byte retorna el *browser* en cada acceso?
6. Para cada acceso, ¿cuántos GET se efectúan en cada caso y por qué?
7. ¿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 información de:

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 ted 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 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).

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 `T5` en el directorio `Entregas` de su carpeta personal y subir su tarea a esa carpeta. Puede ser realizada en forma individual, o en grupos de 2 personas. En cualquier caso, recuerde indicar en el informe los autores de la tarea con sus respectivos números de alumno.

En su carpeta `T5` se debe incluir:

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

Se revisará el contenido de dicha carpeta el día Lunes 18 de junio de 2018 a las 23:59.

Evaluación

Se evaluará, con una escala de 1.0 a 7.0 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.
- 30 % Respuestas parte (a)
- 25 % Respuestas parte (b)
- 25 % Respuestas parte (c)

Preguntas

Cualquier duda preguntar a través del foro.

[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