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

IIC 2333 — Sistemas Operativos y Redes — 1/2016

Tarea 6

Fecha de Entrega: Martes 5-Julio de 2016, 12:00 (mediodía)

Composición: grupos de n personas, donde $n \leq 2$

En esta tarea analizaremos un protocolo de capa de aplicación mediante el software *Wireshark*, que ya hemos usado en la tarea 4.

Sobre la nota de tareas (N_T)

Recuerden que la nota de tareas del curso es requisito de aprobación, y se calcula como: $N_T = (T_1 + T_2 + T_3 + T_4 + T_5 + T_6 - min(T_1, T_2, T_3, T_4, T_5, T_6)/5$.

Usando `nslookup`

Para esta tarea es necesario utilizar la herramienta `nslookup`, disponible a través de las consolas de Windows, Linux y MacOS. Pruebe ejecutando nslookup de manera sencilla con comandos como:

```
nslookup hercules.ing.puc.cl
nslookup www.ing.puc.cl
nslookup www.ca2016.com
```

Ejecute la misma instrucciones anteriores, pero agregando el flag `-type=NS`. Observe la diferencia e investigue qué significa este resultado.

```
nslookup -type=NS hercules.ing.puc.cl
nslookup -type=NS www.ing.puc.cl
nslookup -type=NS www.ca2016.com
```

Finalmente agregue un segundo argumento de la siguiente manera:

```
nslookup www.ing.puc.cl 146.155.4.4
nslookup www.ing.puc.cl 8.8.8.8
nslookup www.ca2016.com 146.155.4.4
nslookup www.ca2016.com 8.8.8.8
```

Averigüe el significado de este llamado y note las diferencias.

Actividad

Para esta parte debe utilizar el software *Wireshark* de manera similar a la Tarea 4, y analizar el funcionamiento del protocolo DNS luego durante el acceso a un sitio web. Luego analiará brevemente el protocolo DHCP utilizando este mismo software.

Parte (a)

1. Borre el caché DNS. Averigüe cómo hacerlo en su sistema operativo. (keywords: *flush dns cache*).
2. Abra un navegador web y borre su cache.
3. Abra *Wireshark* y configúrelo para monitorear su tráfico de salida (`ip.addr == miDireccionIP`)
4. Visite 3 sitios web en dominios distintos (ej: www.ing.puc.cl, www.ca2016.com, www.ietf.org)

5. Guarde el resultado de su captura (*dump*)

Debe ejecutar estas instrucciones desde una misma ubicación, ya sea su casa, la red de la universidad, o alguna red pública u oficina. Si accede algunos sitios desde redes de origen distintas puede distorsionar los resultados.

Parte (b)

A continuación ejecute las consultas a los mismos sitios elegidos previamente usando `nslookup`, con y sin el flag `-type=NS`, y experimente también usando servidores DNS explícitos. Obtenga respuesta de servidores *autoritativos* y *no-autoritativos*.

Parte (c)

Investigue sobre las prácticas habituales para desplegar un servicio DNS. ¿Es posible asegurar continuidad de servicio? Indague sobre los *root servers*, indicando qué son, cuál es su relevancia y dónde se encuentran.

Parte (d)

A continuación conéctese a una red que asigne sus IPs mediante protocolo DHCP, identifique los paquetes asociados y hosts involucrados en la comunicación. Puede provocar una comunicación DHCP utilizando el comando `ipconfig /renew` en Windows o `ifconfig --renew` en Unix.

Informe

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

- Parte (a). Identifique la secuencia de mensajes DNS para cada conexión web. Para esta secuencia de mensajes debe identificar el protocolo de transporte, puerto usado, tipo de mensajes de acuerdo al protocolo DNS, cuáles servidores DNS son consultados.
- Parte (b). Identifique la secuencia de mensajes DNS para cada conexión hecha con `nslookup`. Identifique las diferencias entre usar o no `-type=NS`, y cuáles son las diferencias entre usar o no servidores *autoritativos*.
- Parte (c). Responda las preguntas planteadas utilizando referencias relevantes. Indique claramente sus fuentes.
- Parte (d). Identifique la secuencia de mensajes DHCP, indique Hosts involucrados, protocolos de transporte, puertos, origenes y destinos de los paquetes. Indique claramente el servidor DHCP que responde y obtenga información relevante de él. ¿Hay diferencias en DHCP para IPv4 e IPv6? Fundamente su respuesta utilizando fuentes oficiales.

Evaluación

Para la evaluación deberá subir en un cuestionario un archivo zip que incluya su informe en formato PDF.

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
- 30 % Identificación de ítems requeridos en parte (a)
- 30 % Identificación de ítems requeridos en parte (b)
- 15 % Investigación sobre prácticas de deployment para servidores DNS.
- 15 % Identificación de estructura de mensajes DHCP