

Tarea 2

CC51C Comunicación de Datos

25 de Junio de 2001 - Plazo: 1 semana (vence el 2 de Julio de 2001)

1 Descripción

Se cuenta con un archivo que contiene datos capturados desde una Ethernet. Se le pide que conteste las siguientes preguntas basándose exclusivamente en esos datos. El archivo de datos se encuentra en `anakena:~cc51c/T2/tarea2.dump`.

Para poder analizar el stream capturado, deberá usar el analizador de protocolos de su preferencia (ej: `tcpdump`, `ethereal`). La recomendación es `ethereal`. Es válido usar los filtros y demases características de los programas (puede facilitar bastante las respuestas a algunas preguntas)

1. ¿Cuántas conexiones TCP se establecen y terminan? (Hint: no quedan conexiones pendientes y no hay conexiones que se hayan iniciado antes de la captura)
2. Identifique cada una de las conexiones TCP y describa en no más de dos líneas de qué se trata (servicio involucrado, éxito/fracaso, etc).
3. ¿Cuál es la password del usuario 'test'?
4. Durante la sesión FTP: ¿Por qué no se inicia una conexión desde el servidor al cliente para el envío del listado de directorio, que es como lo especifica el RFC?
5. ¿Cuántos *paquetes* (no conexiones ni interacciones) UDP están capturados?
6. De los paquetes UDP, cuántas interacciones (requerimiento-respuesta) puede identificar? Describalas en no más de dos líneas por cada una.
7. De los dos primeros paquetes capturados, qué se puede concluir acerca de las direcciones Ethernet y las direcciones IP?
8. Los paquetes 83 y 84 muestran un intento de conexión a un puerto que no está siendo escuchado por ninguna aplicación. Cómo interpretaría los flags TCP seteados en el paquete 84?
9. Si ya ha habido interacción entre los hosts 10.1.1.10 y 10.1.1.3 (y por lo tanto debieron haber sabido los mapeos de direcciones IP a direcciones Ethernet), explique por qué tiene sentido que en el paquete 13 y 14 se vuelvan a intercambiar estas informaciones.
10. ¿Qué User-Agent es el que se usa en la(s) conexión(es) a servidores web?
11. ¿Qué página(s) web se solicita(n) en la(s) conexión(es) a servidores web?
12. ¿Es posible determinar cuál es el router de la red en base a los paquetes enviados a una red distinta? Si la respuesta es afirmativa, cuál es el router?

2 Entrega

La entrega se hará por mail a `cc51c@dcc.uchile.cl`, con Subject "Entrega Tarea 2 CC51C".

3 Hints

En `anakena:/u/a/cursos/cc51c/T2` está una copia del programa `ethereal`, y la `manpage`. Para ver esta última, basta usar el comando

```
nroff -man /u/a/cursos/cc51c/T2/ethereal.1 | less
```

(o sustituya `less` por el pager de su preferencia). Si desea bajar y compilar el software, puede hacerlo desde la URL <http://www.ethereal.com/>.

Es altamente recomendable revisar la `manpage` para usar filtros y demás capacidades y evitar revisiones a mano de los paquetes (aunque esto último es posible y aceptable).