Tarea - Análisis de Protocolos de Red

mvaras@inf.utfsm.cl

UTFSM - JMC - Redes de Computadores
1 Oct 2015

Objetivos y puntaje otorgado por la tarea:

- Observar los protocolos que intervienen en las redes de datos en forma práctica, estableciendo sus relaciones de dependencia.
- Aprender a usar un sniffer como herramienta de administración de redes.
- Sensibilizarse respecto a la seguridad.
- Puntaje ponderado 20 %

1. Introducción

Una forma simple de entender las redes de computadores, es entender los protocolos que estructuran su arquitectura.
El presente trabajo consiste precisamente en observar las secuencias de mensajes que intercambian dos entidades de protocolos cuando son forzados a realizar determinadas acciones.

La herramienta básica para experimentar con protocolos es el llamado Sniffer.
Un Sniffer de paquetes es una herramienta que permite observar mensajes recibidos y generados por protocolos en un computador.

Los componentes principales de un Sniffer son los módulos de captura de paquetes y el módulo de análisis. El módulo de captura recibe una copia de cada frame (capa de enlace) generado y recibido por el computador donde está instalado.
El módulo de análisis muestra los campos de los paquetes capturados. Como el analizador conoce la estructura de los mensajes, es posible ver todos los protocolos encapsulados jerárquicamente.

Para la experiencia se utilizará el Sniffer Wireshark de distribución gratuita y multiplataforma.
Un Sniffer es un elemento pasivo. Observa mensajes enviados y recibidos por aplicaciones y protocolos en un computador. No altera el flujo normal de paquetes porque sólo procesa copias de mensajes.

2. Descripción de la Experiencia.

(**a**) Los pasos a seguir son:

1.Bajar e instalar el binario Wireshark en su computador. El sitio es http://www.wireshark.org.
2.Bajar la documentación (Wireshark user guide)
3.Iniciar Wireshark estableciendo las interfases de red para la captura
4.En un Browser seleccionar alguna página
5.Iniciar la captura (establecer Capture Options)
6.Mientras la captura está activa, seleccionar distintos URL. Filtrar por http. Seleccionar páginas seguras, por ejemplo de un banco y escribir la password.
7.Salvar en un archivo datos capturados
8.Bajar desde un sitio algún archivo grande e iniciar una nueva captura. Filtrar por tcp.

(**b**) Ayudas para la experiencia:

```
Qué mensaje envía su computador al servidor http?.
Qué responde el servidor? Qué protocolos están
involucrados?
Qué información se puede extraer?
Cuáles son los números de secuencia de los segmentos SYN en TCP?
Comparar las siguientes aplicaciones y/o protocolos:

 - Skype v/s msg
 - pop v/s imap
 - telnet v/s ssh
 - http v/s https
```

(**c**) Informe:

```
La estructura del informe es la correspondiente a un informe
técnico.Como máximo 7 páginas en total.

El informe debe contener al menos:
 - Introducción.
 - Desarrollo
 - Resultados

Conclusiones respecto a:

 - El Sniffer

 - Proceso de instalación ,configuración y uso.

 - Seguridad de redes.

 - Estructura de protocolos.
```