Laboratorio 1

Análisis y obtención de tráfico mediante Wireshark
Laboratorio de Redes 2016, UTFSM

Valparaíso, 28 de marzo de 2016

1. Introducción

Se entiende como protocolos de comunicación al conjunto de reglas que permiten el flujo de información entre distintos equipos. Cada uno de estos protocolos de la capa de aplicación ha sido diseñado para cumplir una función en específico, ofreciendo a las aplicaciones la posibilidad de acceder a servicios, por ejemplo: navegación a través de Internet (HTTP/HTTPS), envío de correos electrónicos (SMTP, POP3), llamadas mediante VoIP (SIP/H.323), streaming (RTP), transferencia de archivos (FTP), etc.

Por otro lado, Wireshark es una poderosa herramienta de análisis utilizada para inspeccionar datos obtenidos desde cualquier interfaz de red, como Ethernet, WiFi o incluso Bluetooth. Wireshark tiene la capacidad mostrar de manera ordenada y esquematizada lo paquetes capturados en procesos de envío y recepción de información, a su vez esta dotado de múltiples herramientas que permiten realizar un completo análisis de la comunicación capturada.
En esta experiencia usaremos esta herramienta para obtener y analizar información usando las opciones de organización y filtrado que ofrece.

2. Objetivo general del laboratorio

Familiarizarse con Wireshark poniendo énfasis en la información obtenida con esta herramienta, además de destacar conceptos, detalles y aspectos de la implementación de protocolos.

3. Objetivos específicos del laboratorio

- Aprender a obtener información de un tráfico de red usando esta herramienta.
- Reconocer los protocolos presentes usando opciones de filtrado.
- Interpretar información desde un tráfico dado.

4. Descripción del laboratorio

En esta experiencia se le presentarán tres ejercicios que debera desarrollar usando Wireshark. Para esto el alumno deberá tener instalado Wireshark en su computador y se le pedirá que descargue el archivo 'exp1.tar.gz' de la página `https://scm.labit.inf.utfsm.cl/trac/redes16?`.

5. Actividades y/o Preguntas

Ejercicio 1 Se realizarán una serie de preguntas de investigación, esperando que el grupo estudie, comente y concluya (**brevemente**) sobre ellas.

1. Suponga que usted esta viendo la página web del curso de Redes de Computadores (moodle) desde el computador de su casa. Describa la conectividad de la red y su arquitectura entre su computador y los servidores de la universidad (e informática), si no encuentra información especifica de la red de departamento describa la red con un entorno comparable. Utilice la herramienta Wireshark e incluya los protocolos típicos para esta comunicación e identifique la capa que lo utiliza.

2. Realizando una conexión en un sitio con HTTP y otro con HTTPS, realice un filtrado (opción Filter en Wireshark) de tal forma que identifique el tráfico que se realiza desde/hacia los host específicos visitados y el tipo de protocolo mayormente utilizado. Adjunte en su informe los filtros utilizados y una breve explicación de su captura (adjunte archivo .pcap obtenido bajo el nombre grupoXX.pcap, si tiene grupo designado o nombre-apellido.pcap si realiza la experiencia individualmente).
   Se le recomienda al alumno realizar un ingreso (login/logout) en un sitio HTTP y luego, en un sitio HTTPS, previamente seleccionados, manteniendo sólo estos dos sitios en su navegador y utilizando una conexión por red, recuerde analizar solamente las frames relacionadas con el ejercicio.

3. Según la información recopilada, ¿Qué inconvenientes tienen las páginas HTTP(form) y a que se debe su inseguridad?.

Ejercicio 2 Abrir Wireshark, y abrir el archivo "EjercicioDos-N", donde 'N' corresponderá al número de grupo asignado.

En el siguiente ejercicio se le proporciona un extracto de trafico de red, en el cual se desarrollaron actividades en un servidor. Bajo este escenario, se solicita al alumno que analice a grandes rasgos cuales fueron las actividades que se desarrollaron, los host que se vieron involucrados y los rangos de tiempo en los cuales se desarrollaron las tareas. Por ultimo, se le solita al alumno que logre rescatar algun/os objetos involucrados en el trafico de red (imagenes, paginas web, etc).

Hint: Utilice la herramienta Static del menú y conteste preguntas como:

- ¿Cuantos paquetes en total estuvieron involucrados en el tráfico de red?
- ¿Cual es el tiempo involucrado en cada actividad?
- ¿Cual es el tiempo total del tráfico presentado, considerar tiempo total entre el primer y el último paquete?
- ¿Cual es el porcentaje obtenido por la conexión de cada protocolo utilizado?

- ¿Cuales son los host involucrados?, ¿cual es la dirección? y ¿cual es el cliente? (relacionar con número de paquetes)
- Gráfique el tráfico por paquetes involucrados y analice el comportamiento de la curva obtenida.

Ejercicio 3 Para este ejercicio, revise en la carpeta de descarga el archivo EjercicioTres.pcap el cual es un archivo de Wireshark con paquetes capturados durante una llamada VoIP hecha con un servidor levantado con Asteriks y utilizando la aplicación de android CSipSimple. Para este ejercicio se espera que pueda utilizar Wireshark de manera de recuperar la información de la llamada e identificar las herramientas que se presentan.

1. Analice la petición a modo general e identifique el audio.
2. Analice el flujo de la llamada; considere tiempos y forma gráfica del envío de paquetes.
3. ¿Cuál fue la duración de la llamada? ¿Cuántos paquetes fueron transferidos?
4. Identifique la dirección de los dos interlocutores.
5. Identifique los protocolos que están involucrados solo en la llamada y su función general

6. Entrega

El informe realizado se deberá entregar a más tardar el día XX de XXXXXXX en el buzón de LabIT. Por cada día de atraso se descontarán 20 puntos de la nota final. Respecto al trabajo realizado en el trac, no se podran efectuar modificaciones pasada la fecha de entrega (en caso de detectar alguń cambio posterior se sancionará con nota 0).