INF-256/ILI-256: Redes de Computadores

Experiencia 1
"Sockets y Análisis de tráfico"

Laboratorio de Integración Tecnológica

Marzo - Abril 2017

1. Introducción

Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiar un flujo de datos, generalmente de manera fiable y ordenada. El término socket es también usado como el nombre de una interfaz de programación de aplicaciones (API) para la familia de protocolos de Internet TCP/IP, provista usualmente por el sistema operativo. Los sockets de Internet constituyen el mecanismo para la entrega de paquetes de datos provenientes de la tarjeta de red a los procesos o hilos apropiados. La primera parte de este laboratorio consistirá en implementar un cliente que utilice un Socket TCP.

Por otro lado, cuando hablamos de redes de computadores, es importante saber cómo ocurre la comunicación entre estas a nivel de aplicación. Los protocolos de comunicación corresponden un 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: navegar por internet por *HTTP/HTTPS*, envío de correos electrónicos (SMTP, POP3), llamadas mediante VoIP (SIP/H.323), streaming (RTP), transferencia de archivos (FTP), etc. En la segunda parte del laboratorio se deberán identificar y reconocer las características anteriormente mencionadas utilizando una poderosa herramienta de análisis de trafico llamada *Wireshark*.

2. Objetivo general del laboratorio

Estudiar y comprender los conceptos de socket, análisis de paquetes de red a través de *Wireshark*, e introducir al alumno al mundo de las tecnologías VoIP.

3. Objetivos específicos del laboratorio

- Comprender el funcionamiento de un socket TCP.

- Familiarizarse con *Wireshark*, poniendo énfasis en la información obtenida con esta herramienta, además de destacar conceptos, detalles y aspectos de la implementación de protocolos.
- Comprender qué es *Asterisk* y cómo funciona.

4. Descripción del laboratorio

Esta experiencia entrega herramientas para trabajar con *sockets* y el software *Wireshark*, complementando este último con tecnologías *VoIP*.

El laboratorio se divide en dos partes:

1. Trabajo Previo
2. Trabajo en el laboratorio

5. Actividades y preguntas

5.1. Trabajo previo

5.1.1. Comunicación por Socket

Se deberá implementar un cliente que utilice un *Socket TCP*, desarrollado en lenguaje *Python*, para comunicarse con un servidor y obtener una clave secreta, la cual será requisito para poder realizar el posterior trabajo en el laboratorio.
Esta comunicación tendrá siempre la estructura iterativa:

1. Mensaje Servidor
2. Respuesta del cliente

La comunicación debe terminar cuando el servidor retorne un 0.

Un ejemplo de output de una comunicación exitosa con el servidor sería el siguiente:

```
[Servidor]: Bienvenido al LabIT, ingrese su numero de grupo de dos digitos
> 01
[Servidor]: Su clave secreta es: "0000000". Envie cualquier caracter no vacio para terminar...
> x
```

Una vez desarrollado el código y obtenida la clave, se deberá subir el archivo fuente a la plataforma *Docencia*, el cual debe estar disponible antes de dar la segunda parte de la experiencia (en caso contrario, esta no se podrá rendir).

5.1.2. Investigación

Para un correcto desarrollo del trabajo en el laboratorio, se recomienda estudiar de forma personal y no obligatoria, los siguientes temas:

- ¿Qué es VoIP? ¿Qué es la telefonía IP? ¿Que programas lo utilizan?

- ¿Qué es una central teléfonica PBX? ¿Qué diferencias hay con una central telefónica común?
- ¿Qué es y para qué se usa el software *Asterisk*?
- ¿Qué es el software *Ekiga* y cómo uno se registra en una central PBX a través de este?
- ¿Qué es y para qué se usa el software *Wireshark*?
- ¿Cómo se capturan paquetes a través de *Wireshark*?
- ¿Cómo se analiza un archivo generado en *Wireshark*? ¿Cómo se aplican filtros? ¿Qué tipos de filtros existen?

5.2. Trabajo en el laboratorio

Como prerequisito para este trabajo, el grupo deberá llegar en el bloque inscrito con su clave secreta (obtenida en la primera parte) y haber subido con anterioridad su código del cliente socket en *Docencia*.

Luego de que el ayudante corrobore que lo anterior se hizo correctamente, se da inicio a la experiencia práctica.

5.2.1. Creación PCAP

Se pondrán a disposición de los alumnos un teléfono VoIP *Grandstream GXP1400*, junto a un computador con el cliente VoIP *Ekiga* instalado (los cuales ya se encontrarán registrados y configurados con el servidor de *Asterisk*).

Junto con lo anterior, en esta sección se deberá crear, a través del software *Wireshark* (ya instalado), un archivo *.pcap*, el cual debe contener el tráfico de paquetes generado por las siguientes actividades:

- El grupo deberá realizar una llamada desde el teléfono VoIP hacia el computador con el cliente *Ekiga* instalado, con una duración mínima de 5 segundos.
- Se deberán abrir dos páginas web dentro del computador. La primera será la página de *Docencia*, en la cual se deberá iniciar sesión con una cuenta que será entregada por el ayudante en ese momento. La segunda página web a ingresar debe ser *Facebook* en la cual deberán iniciar sesión con una cuenta a elección.

Finalmente, el archivo *.pcap* creado deberá ser subido a *Docencia*, para su posterior revisión. Las restricciones para esta sección se definen más adelante.

5.2.2. Análisis PCAP

Luego de terminada la creación del archivo *.pcap*, se pondrá a disposición otro telefono VoIP (mismo modelo anterior), a través del cual el grupo deberá registrarse con los datos obtenidos por socket, ingresando:

- Usuario (Número del grupo, de dos dígitos)

- Contraseña (Clave secreta obtenida en el trabajo previo)
- IP Servidor Asterisk

Una vez registrados, a través del teléfono se deberán responder preguntas basadas en el archivo recién creado, analizando este último a través de *Wireshark*. Para esto, se encontrarán habilitados dos números:

- 6666: El grupo deberá llamar a este número para escuchar las 9 preguntas sobre el archivo generado, enumeradas del 1 al 9.
- 6667: El grupo deberá llamar a este número para responder las preguntas escuchadas en el número anterior, indicando primero el número de pregunta que desea responder, y luego decir en voz alta la respuesta.

Una vez respondidas las 9 preguntas, o terminado el bloque asignado, se da por finalizada la experiencia.

6. Consideraciones

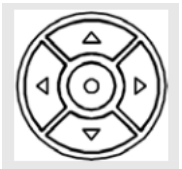
- La dirección IP del servidor para comunicarse a través de sockets será la 204.87.169.107, el cual estará escuchando en el puerto 9999.
- La dirección IP del servidor que estará corriendo *Asterisk* para registrar los teléfonos VoIP será la 10.10.14.22.
- El nombre del código fuente con el cliente socket a subir a *Docencia* debe seguir el formato *EXP1_Sockets_XX.py*, donde *XX* corresponde al número de grupo.
- El nombre del archivo pcap que se subirá a *Docencia* con los paquetes capturados en la parte práctica del laboratorio, debe seguir el formato *EXP1_Wireshark_XX.pcap*, donde *XX* corresponde al número de grupo.
- En el trabajo en el laboratorio, las respuestas de la sección *5.2.2* quedarán guardadas en carpetas identificadas con el usuario registrado (número de grupo), para posteriormente revisarlas junto al archivo *.pcap* creado y subido presencialmente a *Docencia*, por lo que el grupo deberá asegurarse que los datos ingresados sean los correctos.
- El trabajo en el laboratorio se desarrollará entre el Lunes 17 de Abril y Viernes 21 de Abril.
- Cabe destacar que este laboratorio está sujeto a las reglas generales publicadas en la página del laboratorio en *Docencia*.
- Si tiene dudas con el desarrollo del laboratorio, no dude en consultar al correo labit@listas.inf.utfsm.cl, en plataforma *Docencia* o directamente en el LabIT.

7. Anexos

7.1. Configuración Teléfono VoIP Grandstream GXP1400

Para ingresar los datos en el teléfono VoIP y registrarse en el servidor *Asterisk*, se deben seguir los siguientes pasos:

1. Presionar el botón de al medio para acceder al menú del teléfono.



2. Dirigirse a *Config* > *SIP*. Luego en *Account*, seleccionar *Account 2*.
3. Después, ingresar los datos de registro:
    - *SIP Proxy*: IP Servidor Asterisk

- *SIP User ID* y *SIP Auth ID*: Usuario
- *SIP Password*: Contraseña

4. Una vez ingresados los datos, presionar *Save* y esperar a que el mensaje *Applying new configuration* aparezca y termine.

5. Finalmente, realizar la llamada. Asegurarse que al momento de marcar el número, se llama por la línea denominada *exp1*. En caso contrario, presionar el botón *LINE1* para utilizar la configuración de la cuenta ingresada.