Instituto Politécnico Nacional

Escuela Superior de Computo
(ESCOM)

Proyecto final

“Analizador de protocolos”

REDES DE COMPUTADORAS

Profesor:

- Morales Cervantes Axel Ernesto

Integrantes:

- Pacheco Bautista Gerardo
- Reyes Saucedo Cesar Augusto

Grupo: 2CM11

Introducción

Un sniffer captura todos los paquetes que pasan por delante del equipo en el que está instalado, es decir, que sólo podrá capturar los paquetes de información que salgan o lleguen a su máquina. Se utilizan ya que muchos de los protocolos de acceso remoto a las máquinas se transmiten las claves de acceso como texto plano, y por lo tanto, capturando la información que se transmite por la red se puede obtener este tipo de información. Cuando la tarjeta o adaptador de red se configura en modo promiscuo, captura todos los paquetes que pasan por delante de él. La forma de funcionamiento de este tipo de programas suele basarse en almacenar en un fichero toda la información para recuperarla en el futuro.

Muchas de estas herramientas disponen de la capacidad de interpretar los paquetes recibidos, e incluso las cabeceras asociadas a protocolos que se en encuentra por debajo de IP, y mostrarlas de forma más sencilla de interpretar para los seres humanos. Cuando los sniffers se utilizan de esta forma son llamados **Analizadores de protocolo.** Utilizados de esta forma, resultan una herramienta extremadamente potente para comprender en profundidad el funcionamiento de los protocolos de comunicaciones y, en cierto modo, visualizar, localizar y obtener una solución para ataques remotos utilizando este software (o hardware en algunos casos).

Ethernet

Ethernet/IP es un protocolo de red en niveles para aplicaciones de automatización industrial. Basado en los protocolos estándar Protocolo de Control de Transmisión (TCP), el Protocolo Internet (IP) y las tecnologías de acceso mediático y señalización disponibles en todas las tarjetas de interfaz de red (NICs). Ethernet utiliza los ya bastante conocidos hardware y software para establecer un nivel de protocolo para configurar, acceder y controlar dispositivos de automatización industrial. Ethernet/IP clasifica los nodos de acuerdo a los tipos de dispositivos preestablecidos. El protocolo de red Ethernet/IP está basado en el Protocolo de Control e Información (Control and Information Protocol - CIP).

Las tramas Ethernet tienen la siguiente estructura:

6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
MACd	MACo	Tipo	Datos	CRC

LLC

El protocolo LLC (control lógico de enlace, Logic Link Control por sus siglas en inglés) es un protocolo de la capa de enlace de datos derivado de HDLC (High-Level Data Link Control, control de enlace de datos de alto nivel), del cual hereda su campo de control.

Las tramas LLC tienen la siguiente estructura:

6 bytes	6 bytes	2 bytes	1 byte	1 byte	1 ó 2 bytes	Variable	Variable
Dir. Destino	Dir. Origen	Tamaño SAP	Destino SAP	Origen	Control	Información	Relleno

El funcionamiento de LLC es independiente del método de acceso de la red al medio de transmisión y por ello sus principales funciones son:

1. Habilitar la transferencia de datos entre la capa de red y la subcapa de acceso al medio.

2. Controlar el flujo de datos.

3. Efectuar enlaces para los servicios orientados a la conexión entre aplicaciones situadas en distintos puntos de red.

4. Puede ser configurado como un protocolo sin conexión utilizando las tramas no numeradas de información.

Desarrollo

Se hizo una aplicación en NetBeans con el lenguaje de programación java sobre un sniffer que captura paquetes al vuelo o paquetes desde un archivo de más de 20 tipos distintos de protocolos, entre ellos IP, LLC, ARP, Ipv6, AT&T, RARP, PUP, entre otros. Así mismo, se hace el análisis de los bytes de las tramas capturadas con este tipo de protocolos para saber cómo están estructuradas y conocer su función, por ejemplo si son respuestas o peticiones. Este sniffer puede leer automáticamente las tarjetas de red presentes para poder analizar los datos recibidos y que el usuario elija la que planea usar para leer la información recabada. Esto se logró gracias a la combinación de los analizadores creados anteriormente a lo largo del curso.

Además de recuperar la información de los paquetes, el sniffer también crea un archivo con la información y sus respectivas gráficas.

En el proyecto de NetBeans se encontrarán 5 clases:

1. **Captura**
   Es la clase principal del proyecto pues aquí es donde aparecen todas las ventanas de opción del usuario para que éste decida la tarjeta de red a elegir, el modo en el que quiere la captura de paquetes y el modo en el que desea que la información recolectada sea mostrada (gráfico/consola) y donde analiza las tramas tipo Ethernet pues regresa todos los elementos de un mensaje Ethernet como la longitud, MAC destino, MAC origen, SSAP, DSAP, etc.

2. **ConvertidorBinDec**
   Esta clase es utilizada para analizar más fácilmente las tramas LLC pues debido a que regresan un número en binario, es necesario convertirlo a decimal para saber qué significa y por lo tanto saber qué operación está realizando.

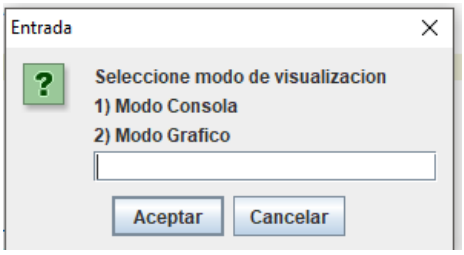
3. **Vista**
   Es la interfaz gráfica del proyecto, donde se pueden observar las tramas capturadas y elegir la opción de graficar si se desea. Además, muestra el valor de los campos que conforman cada tipo de trama.

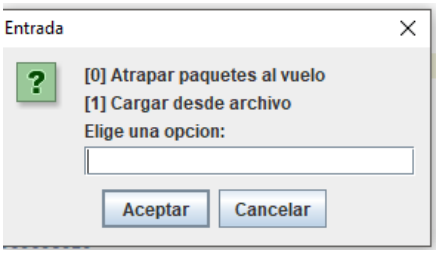
4. **AnalizadorLLC**
   Aquí es donde se realiza el análisis de los mensajes del protocolo LLC, es decir, donde se analiza poco a poco cada tramo para identificar qué tipo de trama es (U,S,I) y analizar otros elementos como su pool/final, N(S), N(R).

5. **BibliotecaP**
   Es la clase donde están todos los tipos de protocolos que podrían aparecer al hacer la captura de los paquetes. Cada tipo tiene un número asignado dentro de un arreglo. Además, contiene la función para obtener el protocolo del que se trata a partir de la longitud obtenida.

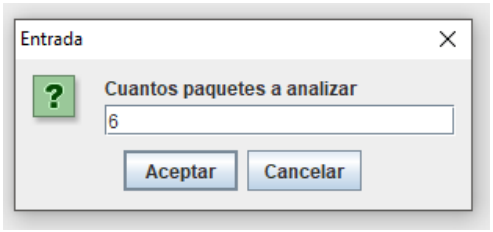
Pruebas

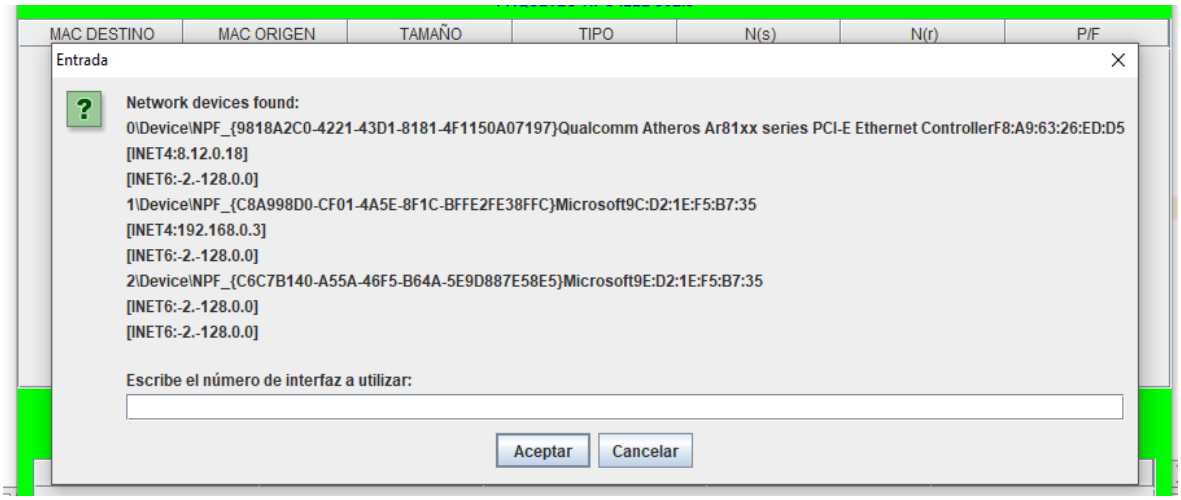
para el funcionamiento de la práctica se despliega esta primera pantalla que nos muestra las 2 opciones que tenemos para correr el programa en modo consola o modo gráfico. En este caso es necesario seleccionar una de las 2 opciones que se nos despliegan en la parte superior.





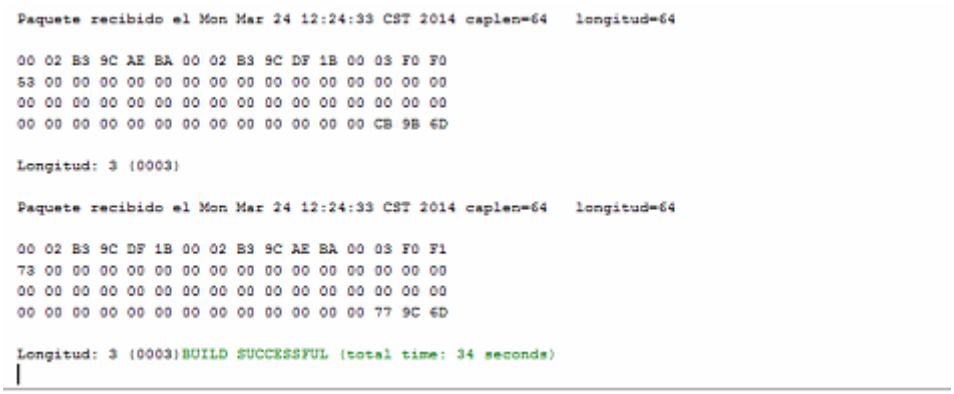
Para el caso en que se seleccione la opción 0 entonces se capturan paquetes al vuelo, te preguntara que red se utilizara una vez seleccionada alguna se muestra la interfaz gráfica correspondiente, a continuación te preguntara el número de paquetes a capturas y una vez indicados procede a mostrar correspondientes datos a capturar.





Por el contrario, al seleccionar la opción 1 se capturan paquetes de un archivo y estos son cargados para a la interfaz. Este tipo de paquetes tiene otras características desplegadas en el menú. Para este tipo de captura se termina una vez encontrado el fin del archivo. Y se termina muy rápidamente.

También el programa ofrece la solución de que mientras se realiza por medio de la interfaz gráfica la captura de paquetes se realiza también desde la parte de consola. Con lo cual se corrobora cada uno de los paquetes desplegados en la parte de la interfaz.



Conclusión

Gracias a este proyecto fue posible conocer otro tipo de protocolos que no fueron profundamente estudiados pero que es importante conocer su existencia pues hay una gran cantidad actualmente y este pequeño sniffer sólo detecta los más importantes, además de analizar a fondo las tramas tipo Ethernet y LLC. De la misma manera, gracias a este análisis profundo, se conocieron las partes que conforman los mensajes de este tipo de protocolos, cómo es que son analizados por los equipos, sus dimensiones (número de bytes) y las acciones que realiza en cada uno de sus campos. Con los datos obtenidos por el sniffer también se pudo observar de manera gráfica la información recibida para que su comprensión sea más sencilla para el usuario. Finalmente, se puso en práctica la opción de permitirle cierta libertad al usuario al poder la tarjeta de red que desee dependiendo de las disponibles en el equipo.

Referencias

- Esteso, Mario Pérez. "Redes - El Protocolo ARP." *Redes - El Protocolo ARP*. N.p., n.d. Web. 11 Dec. 2016.
- "Ethernet/IP." *Ethernet/IP - Siemon*. N.p., n.d. Web. 12 Dec. 2016.
- Sergio Untiveros. "AprendaRedes.com." *Artculo De Redes - Networking*. N.p., n.d. Web. 12 Dec. 2016.