

INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO



REDES

Práctica 1 : Captura de tramas

Integrantes:

- Hernández Escobedo Fernando
- Meza Zamora Abraham Manuel

12 de septiembre de 2019

1. Introducción

En informática, un *Sniffer* es un programa de captura de las tramas de una red de computadoras.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el analizador pone la tarjeta de red en un estado conocido como "modo promiscuo".^{en} el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta; de esta manera se puede capturar (sniff, "olfatear") todo el tráfico que viaja por la red. .

2. Desarrollo

- En C

1. Simplemente, leímos el pdf, y seguimos las instrucciones paso a paso para llevar a cabo la instalación.
2. Compilamos el programa y observamos la salida (fig1) y (fig2).

- En Java

1. Seguimos las instrucciones de instalación del pdf.
2. Observé la salida. A diferencia del ejemplo en C, mostraba la trama sin formato.
3. Basado en el ejemplo de encabezados vistos en clase, hicimos una modificación al código de captura, iterando un ciclo `for` sobre la trama. Inicializando `i` de manera adecuada para mostrar de manera adecuada:
 - a) MAC destino
 - b) MAC destino
 - c) MAC tipo
4. Finalmente compilamos el código y observamos las tramas capturadas. (fig3).

3. Pruebas

Figura 1: Captura de tramas en C

Figura 2: Formato de captura de tramas

Figura 3: Captura de tramas en Java, encabezado sin formato

Figura 4: Trama con formato adecuado

4. Conclusiones

- Fernando: Este tipo de aplicaciones tienen la responsabilidad de realizar la captura de distintos paquetes que se encuentran en circulación a través de una red informática. Además de esto, los sniffers tienen un uso fundamental, que viene a ser el de analizar los paquetes de la red y estudiarlos, no solo capturarlos.
- Abraham :La práctica realizada tuvo como objetivo sentar las bases para poder interpretar los mensajes que utilizan los dispositivos para comunicarse, además analizadores de paquetes tienen diversos usos, como monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.