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

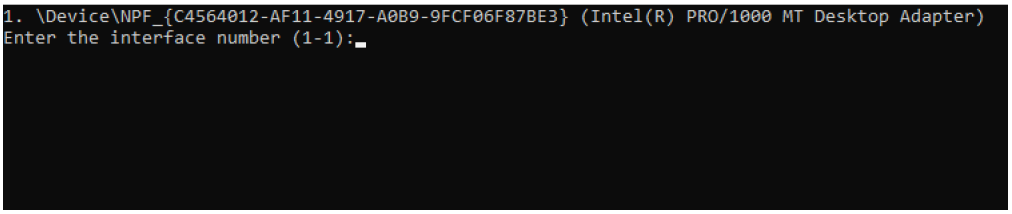

Figura 1: Captura de tramas en C

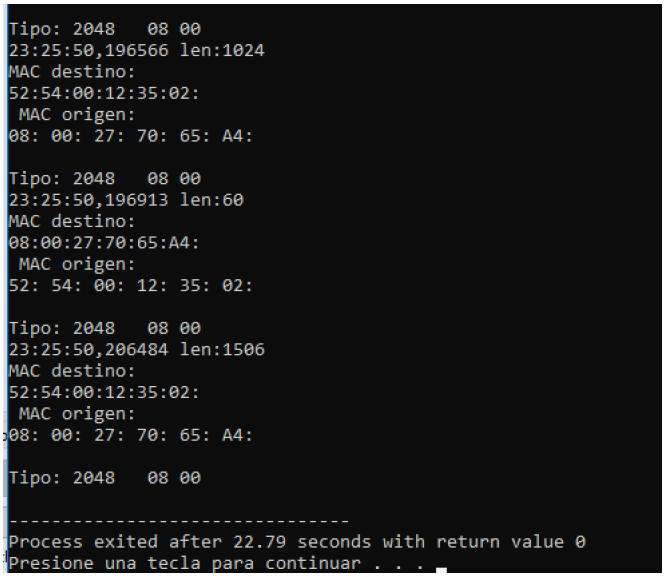

Figura 2: Formato de captura de tramas

```
Encabezado: 0000:*08 00 27 70  65 a4 52 54  00 12 35 02  08 00*45 00    ..'pe.RT..5...E.
0010: 05 a0 5a 43  00 00 40 06  ab 75 bd f7  a5 99 0a 00    ..ZC..@..u......
0020: 02 0f*00 50  c3 32 05 fa  f1 2f cb eb  54 96 50 18    ...P.2.../..T.P.
0030: ff ff 23 c2  00 00*ce a7  4a a2 26 92  78 71 d5 95    ..#.....J.&.xq..
0040: 97 01 7c 01  cd 15 58 ce  aa 24 4b b1  6f 28 87 55    ..|...X..$K.o(.U
0050: 58 e5 27 e0  48 a4 65 e5  51 03 c3 c0  b6 c2 74 8e    X.'.H.e.Q.....t.
0060: c0 7a 48 0d  cc 06 6d 16  ec d9 fe c0  54 ed dd 54    .zH...m.....T..T
0070: 54 37 15 a1  4f 66 94 6a  ec 06 50 72  6f b3 88 96    T7..Of.j..Pro...
0080: b7 54 aa 2e  64 b2 e1 0e  51 e8 16 d8  d3 06 6b 54    .T..d...Q.....kT
0090: 2a b8 45 c4  b3 e5 57 5a  32 00 5f 99  1d 22 ee 3f    *.E...WZ2._.."."?
00a0: b1 af 14 67  8a 51 d1 a1  7e 05 66 5e  4f 9a b8 b7    ...g.Q..~.f^O...
00b0: 4f 36 92 9a  32 f5 bd d4  57 e0 5b 17  fa 47 be aa    O6..2...W.[..G..
00c0: 8c f7 64 bc  02 4e 3e b5  e1 3f 58 7d  5e 45 ca 7b    ..d..N>..?X}^E.{
00d0: 52 5e 01 a4  75 d1 bf 8c  97 e7 54 9b  f0 0e 8b 47    R^..u.....T....G
00e0: c2 cb df 04  18 70 c9 df  b2 5c a7 7e  91 b5 d1 ef    .....p...\.~....
00f0: 24 3c a2 df  00 7d b5 a8  f2 38 c7 b4  2b 86 ca 15    $<...}...8..+...
0100: 95 bb 39 d3  16 f3 7c be  cb 1b 15 3a  5f 39 eb f3    ..9...|....:_9..
0110: 02 91 c4 65  47 b4 1c 47  b3 ec 9d 91  e5 2d d2 65    ...eG..G.....-.e
0120: 63 ef e2 12  92 2e 01 cc  56 56 96 d5  e5 67 97 4a    c.......VV...g.J
0130: e5 89 f9 ba  c9 0a 10 23  1e e7 95 a1  dc 7a 2c 14    .......#.....z,.
0140: 02 ac 9b 6d  43 6b c4 63  fe 30 66 d5  6c 09 59 61    ...mCk.c.0f.l.Ya
0150: 81 58 27 c1  29 b3 4c 42  9c c1 9b fa  9d cb 8d ce    .X'.).LB........
0160: ea 4c 48 e2  de ad 6c 6f  0a 2b 3a be  34 a8 11 c7    .LH...lo.+:.4...
0170: 16 a4 9c f4  1c 63 69 c0  ea fe b4 8a  6c 69 2c b4    .....ci.....li,.
0180: 29 7c f8 ac  2c c9 c2 19  a6 e0 d2 8b  5d f6 68 d7    )|..,.......].h.
0190: cb 82 9c 77  4b e8 b5 25  ad 8e 87 04  8e da 28 9c    ...wK..%......(.
01a0: 49 43 83 c9  44 d0 37 d7  7f 96 33 d9  0d 24 64 c7    IC..D.7...3..$d.
01b0: 47 ff 21 21  d5 a1 f5 ea  7d ea 68 d3  41 19 0e e1    G.!!....}.h.A...
01c0: 68 fc 58 37  7c ae 99 c5  a3 d2 c5 67  43 33 29 f3    h.X7|......gC3).
01d0: 11 cb ef e5  40 91 93 54  0b 87 98 57  81 e7 2d 58    ....@..T...W..-X
```

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

```
+MAC DESTINO
08 00 27 70 65 A4

+MAC ORIGEN
52 54 00 12 35 02

+TIPO
08 00 BUILD SUCCESSFUL (total time: 1 second)
```

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.