TALLER DE SNIFFERS

Juan David González Suarez

Administración de Redes de Computadores

Modulo de Seguridad

20112

Fernando Quintero

SENA Servicio Nacional de Aprendizaje CESGE

Medellín

2010

Sniffers

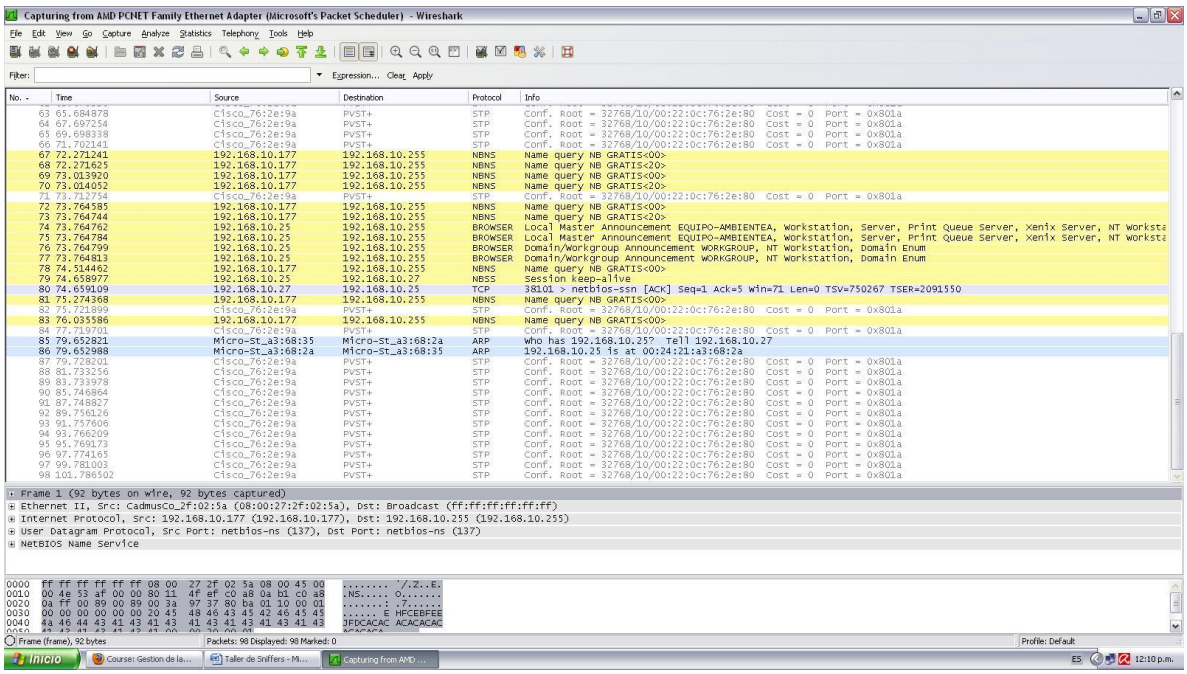
Un sniffer es un programa informático que captura los paquetes que se envían dentro de la red; Al estar en una red local, ya sea por un medio guiado o no guiado, es posible que una de las estaciones de trabajo pueda capturar las tramas que no estén destinadas a él, esto se hace cuando la tarjeta de red está en *modo promiscuo,* esto se hace voluntariamente y existen diferentes tipos de software para hacer esto, el más conocido de ellos es *Wireshark.*

Ejercicios

1- Analizar el tráfico de la red donde se encuentre su aula de clases o desde la conexión desde su casa y tratar de interpretar los datos y las conexiones que cruzan por ella.

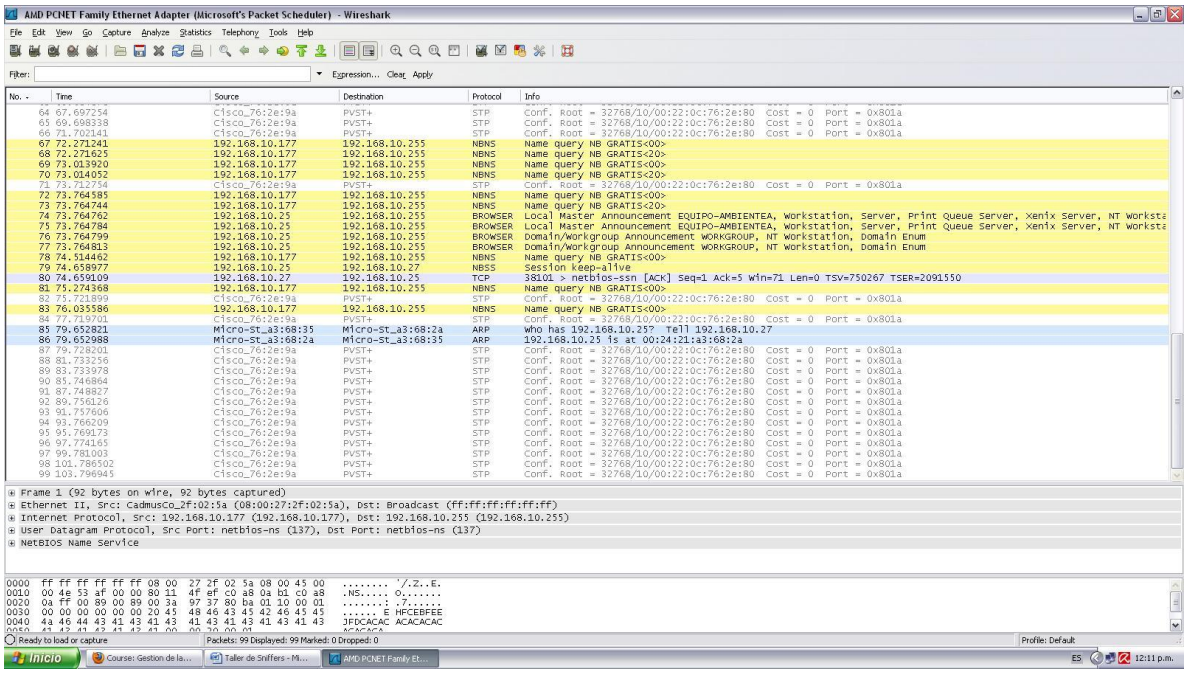
Solución,

Después de capturar trafico de red por 60 segundos, tomamos dos Screenshot y las analizaremos brevemente.



Screenshot 1

Vemos muchos paquetes a la dirección de broadcast de la red, con el protocolo STP y ARP y algunos al navegador.



Screenshot 2

Es muy parecida a la primera captura, aunque en esta es evidente que hay mas paquetes hacia el broadcast, pero con destino a internet, ya que son con el protocolo del navegador, http y DNS.

Ejercicios:

1- ¿Cuántas sesiones FTP y SSH se realizaron?

Se realizaron 4 sesiones FTP correctas, una como usuario anónimo y otras 3 que requería de un Login, en una ocasión se intento iniciar sesión con una contraseña incorrecta; se iniciaron el mismo número de sesiones SSH.

2- La máquina de origen tiene como dirección IP 10.0.0.9.
3- El usuario es *nando* y el password es *hssujs* por el puerto *21*
4- El tamaño más común es de 1448 bytes.
5- La versión del servidor FTP es 6.6 y corre en OpenBSD
6- El usuario es *nando* y la contraseña es *cantinflas.*
7- El Archivo se llama **logo.jpg** y pesa **40119 bytes**
8-
9- Se realizan dos descargas de dos archivos llamados cap*.pdf y cap00.pdf.
10- El archivo no captura por que el proceso de captura se hizo en una red con otro direccionamiento y ya se cerraron las sesiones FTP.