Fecha:	
Descripción:	Captura de paquetes de red
Nombre:	

Práctica

Introducción

Como introducción a la seguridad informática y con el objetivo de visualizar los paquetes que circulan por la red, se propone presentar al alumnos esta actividad en la que realizará un análisis de los paquetes que circulan por la red (network sniffing).

Contenidos

En esta práctica se introducirán al alumnos los siguientes contenidos:
-Analizador de red.
-Esnifar paquetes.
-Modo promiscuo de las interfaces de red.

Actividad

El alumno debe tener un conocimiento inicial suficiente que le permita comprender que por las redes de datos circulan paquetes de datos, con una estructura y un contenido.
Estos paquetes obviamente, no son visibles de forma directa a nosotros.
Usando el paralelismo con el uso del microcospio explicaremos a los alumnos cómo vamos a utilizar una herramienta que nos permita 'ver' todo lo que va circulando por la red.

La herramienta que vamos a utilizar es wireshark. Es de libre distribución y es un estándar de facto para la realización de esta tarea.
El alumno descargará e instalará esta herramienta en su PC como parte de la práctica.

La herramienta se puede descargar de la siguiente dirección:

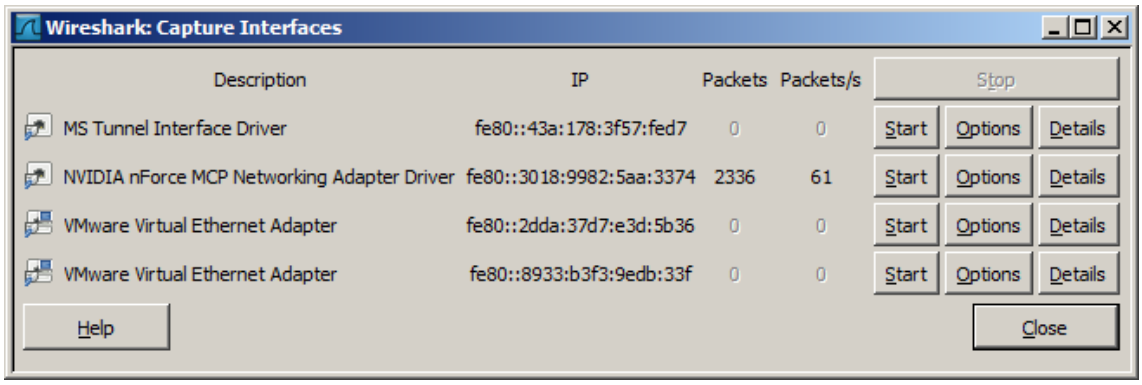
http://www.wireshark.org/download.html

Una vez instalada, se activará la misma y se comenzará la monitorización de la red local.
El programa está en inglés, por tanto habrá que ayudar a los alumnos con la traducción de los conceptos.
Vamos a realizar una monitorización sin filtro.

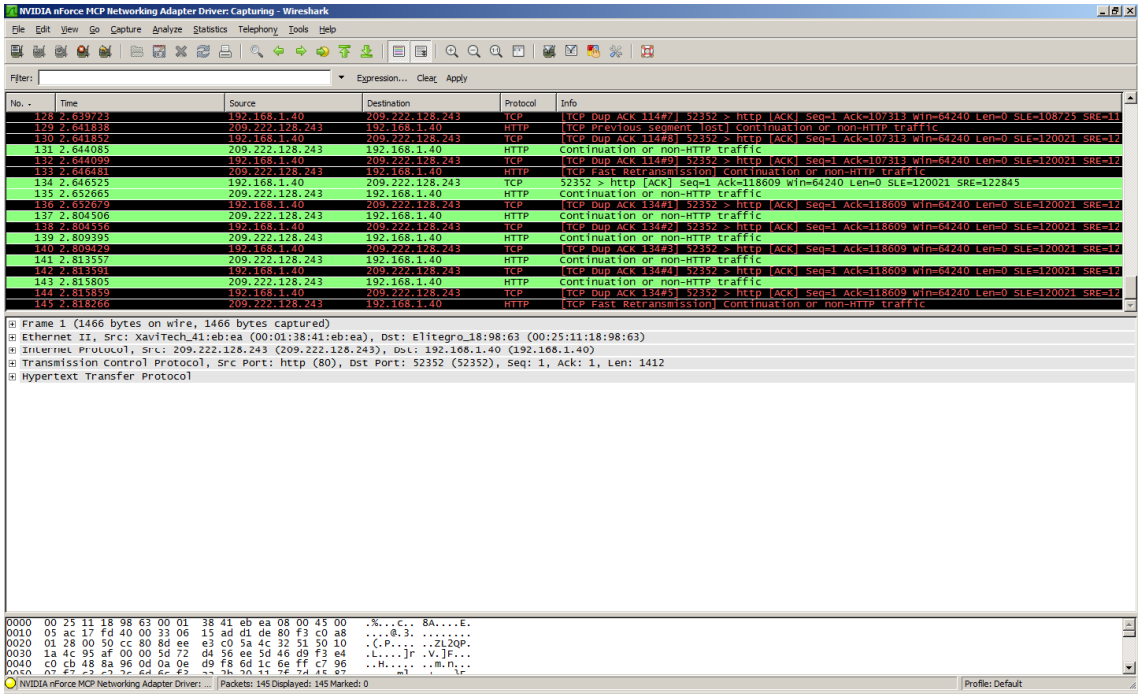
Capture > Interfaces

Esta pantalla nos muestra un listado de las interfaces de red con las que contamos y habrá que elegir una para que se comience la monitorización en esa interfaz.

Fecha:	
Descripción:	Captura de paquetes de red
Nombre:	



Una vez se comienza la captura de paquetes, explicaremos a los alumnos las dos partes diferenciadas de la pantalla, la parte donde aparecen los paquetes y la parte donde se muestra la estructura de un paquete.

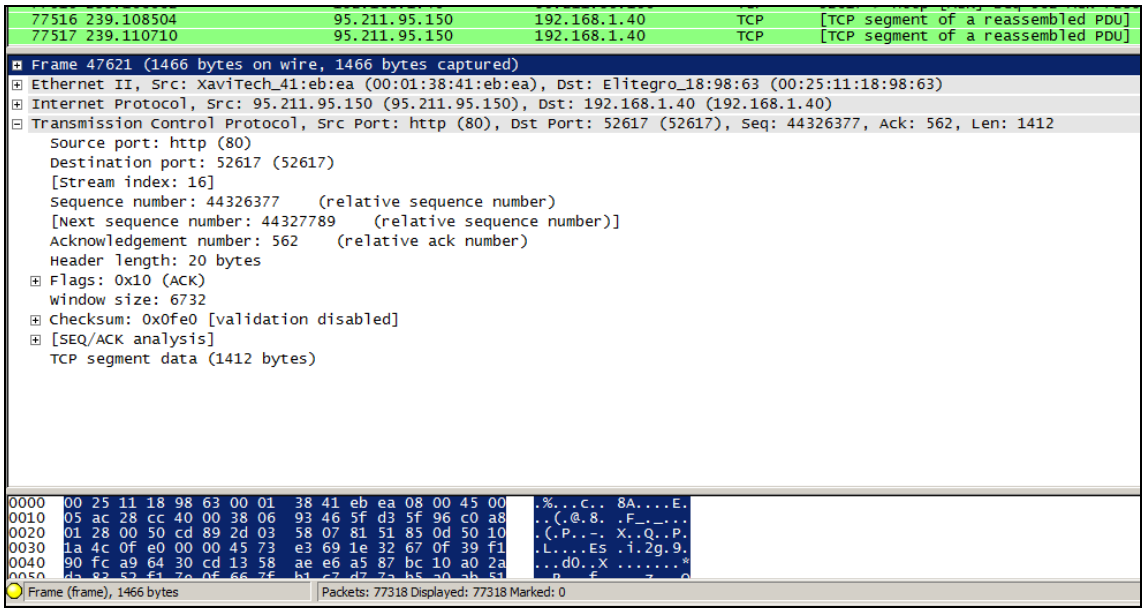


En este punto se dejará que los alumnos exploren libremente la herramienta durante unos minutos.
A continuación pasaremos a explicar los filtros.
Explicaremos los filtros por la necesidad de reducir el número de paquetes que aparecen por pantalla y afinar más en la búsqueda.
Los alumnos aplicarán filtros para:

-Detectar paquetes http
-Detectar paquetes ICMP
-Detectar paquetes ARP

Los alumnos pincharán sobre un paquete y se analizará la estructura del mismo, desde el nivel de enlace al nivel de aplicación.

Fecha:	
Descripción:	Captura de paquetes de red
Nombre:	



Por último y trabajando en parejas de PCs, los equipos de trabajo se mandarán paquetes entre ellos, provocándolos mediante el comando ping o mediante el comando telnet a un puerto determinado.
Se filtrará la captura de paquetes por la ip de la pareja con la que estamos haciendo las pruebas.

Por último, y como una especie de juego, dejaremos que los alumnos se manden paquetes de datos de unos a otros en la red de forma que vayan viendo cómo es posible tener la información de lo que circula por la red en un momento dado.