

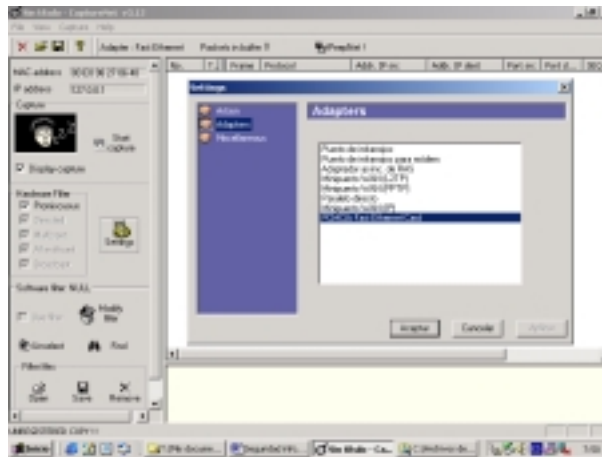
PRÁCTICA 5. ESNIFAR SESIONES DE NAVEGACIÓN (Por HxC Mods-Adm)

Como ya expliqué antes, *SpyNet* es un programa que te permitirá capturar el tráfico de tu Red sin moverte de tu PC, obviamente puede ser algo prohibido en tu empresa o lugar de trabajo, advierte de tus intenciones al administrador de la Red o podrás encontrarte en un serio problema si eres descubierto.

En esta práctica no se contempla la posible solución o contramedidas para evitar el “*esnifado*” eso se verá más adelante cuando se trate más profundamente el tema de *Sniffers*, como este programa lo es, entonces pondremos solución al problema, por ahora debes conformarte con que si tienes instalado un cortador de *cookies*, como *Cookie Pal*, al menos las *cookies* pueden estar a salvo de la captura realizada por *CaptureNet*.

Voy a realizar una sencilla práctica en la que capturaremos de una red, y observaremos más tarde, la navegación de otro usuario, para ello una vez instalado en tu PC el programa *SpyNet*, ejecuta *CaptureNet* y sigue los siguientes pasos:

- Pulsa sobre el icono de **Settings** y en la ventana que aparece, selecciona el apartado **Adapters** y elige de la lista la tarjeta de Red que tengas instalada en tu equipo, en el ejemplo **PCMCIA Fast Ethernet Card** y luego Aceptar.

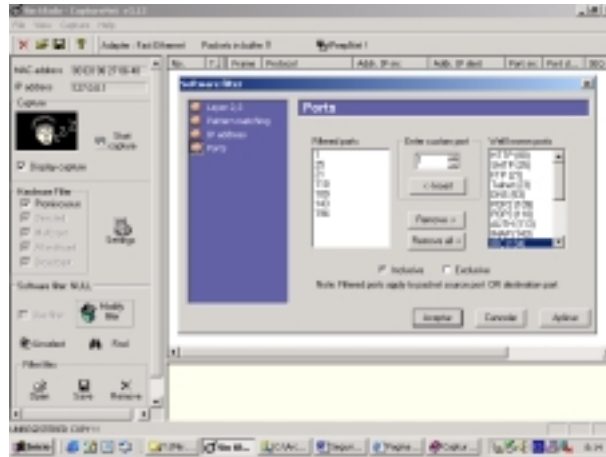


- Desde *CaptureNet* se pueden usar dos tipo de Filtros para conseguir “*esnifar*” sólo lo que nos interese, estos filtros son:
 - **Filtros Hardware:** Que establecen el tipo de direcciones que permite el Adaptador de Red u otro que tengas instalado, switches, routers, hubs, etc.
 - **Filtros Software:** Que te permite seleccionar el tipo de tráfico capturado dependiendo del tipo de protocolo, cadenas de caracteres buscadas, direcciones IP origen-destino y Puertos usados.

Todos estos filtros se pueden combinar entre ellos para restringir el ámbito de la captura y no encontramos con un enorme fichero de datos, en nuestro caso haremos lo siguiente:

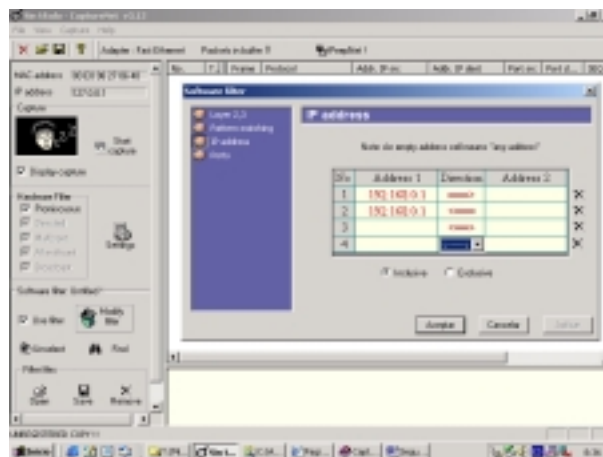
Nos aseguraremos que el **Filtro Hardware** está en **Promiscuous**

En *Software Filter*, pulsaremos en *Modify Filter* y dentro del apartado *Ports*, *Insertaremos* los puertos **80, 21, 25, 109, 110, 143, 194**. Si conocemos que se usa una aplicación específica para *Chat, Icq, Irc*, etc y conocemos el puerto de datos lo podríamos insertar simplemente escribiendo el número de puerto (1 al 65534) ya debes conocer lo que son los puertos TCP y UDP, no obstante en otros capítulos de este libro se explica brevemente.

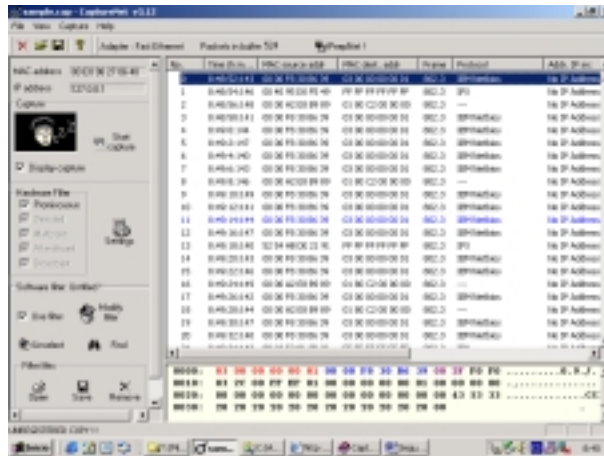


- Después de insertar los filtros de puertos, pulsamos en *Ip Address* y seleccionamos la dirección IP del equipo a espiar, si no la conocemos podemos dejarlo todo en blanco, lo que producirá una captura de todo nuestro segmento de red, podemos incluir una IP, un Rango, etc. , incluso podemos filtrar la *Dirección* de los datos , si son de entrada (<---), salida (--->) o de entrada-salida (< --- >).

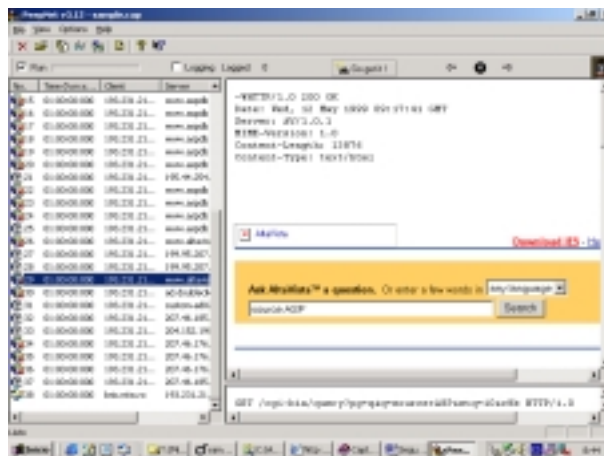
En nuestro ejemplo hemos monitorizado todos los paquetes de datos que “salen” (→) de la dirección IP 192.168.0.1 con destino a cualquier sitio, y todos los paquetes de datos que “entran” (< ---) a la misma dirección desde cualquier otra. Si quisiéramos observar “la conversación” entre dos equipos podríamos haber seleccionado sus direcciones IP correspondientes en *Address1* y *Address2* respectivamente y la dirección (< -- >). Nuestro caso es el que se muestra en la siguiente pantalla.



- Una vez configurado los *filtros*, *Settings*, etc, sólo queda pulsar sobre *Start Capture* y esperar a que se transmitan datos del o hacia el equipo objetivo, una vez que lo hemos conseguido paramos la captura con *Stop Capture* y guardamos el archivo de captura mediante el menú de *File-Save As*



Por último sólo nos queda llamar a *PeepNet*, observa que tienes un botón desde el mismo *CaptureNet* para hacerlo, y abrir el archivo capturado que guardamos anteriormente para luego pulsar *Go Get it!* Para obtener un reflejo de toda la navegación de la máquina objetivo durante el proceso de captura



Esta es una práctica muy sencilla y pro supuesto no pretende una explicación detallada del funcionamiento de *CaptureNet*, no obstante con algo de habilidad y claro conocimiento puedes capturar contraseñas de red, decodificar paquetes de datos, etc. Vuelvo a remitirme al momento en el que aprenderemos algo más sobre los *Sniffers*, para explicarlo.