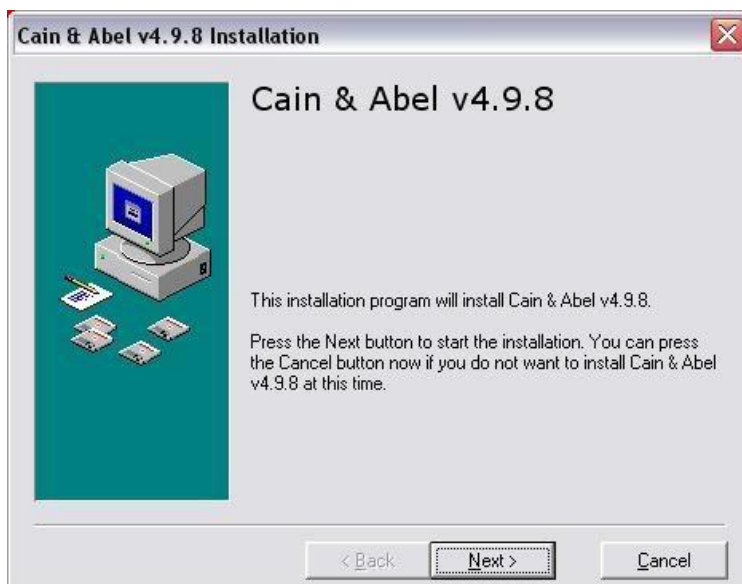


## Sniffing: Cain & Abel (by Zykl0n-B)

Saludos, como he visto que se interesan bastante por el Packet Sniffing, pues, hoy les enseñaré a Sniffar paquetes con una Maravilla de herramienta multiusos, Cain & Abel.

Pueden descargarla directamente desde <http://www.oxid.it/cain.html>

Bien, lo bajamos, y obtendremos un archivo llamado "Ca\_Setup.exe", ese es el Launcher, lo abrimos, y nos saldrá la ventana roja de Instalación, seleccionamos "Next" en todos:

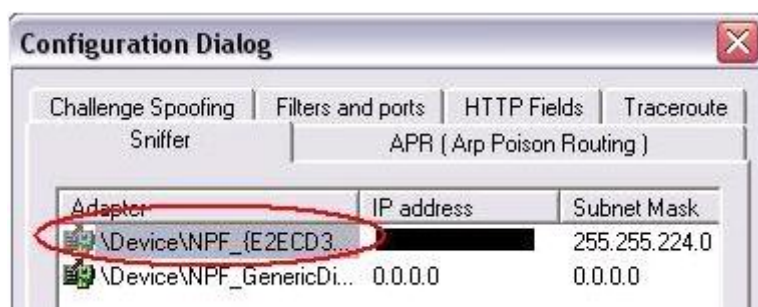


Luego nos pedirá Instalar el Paquete de Winpcap 4.0.1, le decimos que sí:



Una vez terminado, reiniciamos el Ordenador, y estaremos listos.

Caín, Necesita ser configurado, para eso abrimos el programa, y nos dirigimos al Menú "Configure", ahí seleccionamos nuestro adaptador de red, y en la pestaña "APR (Arp Poison Routing)" tenemos opciones de utilizar nuestras direcciones IP y MAC reales, o spoofearlas:

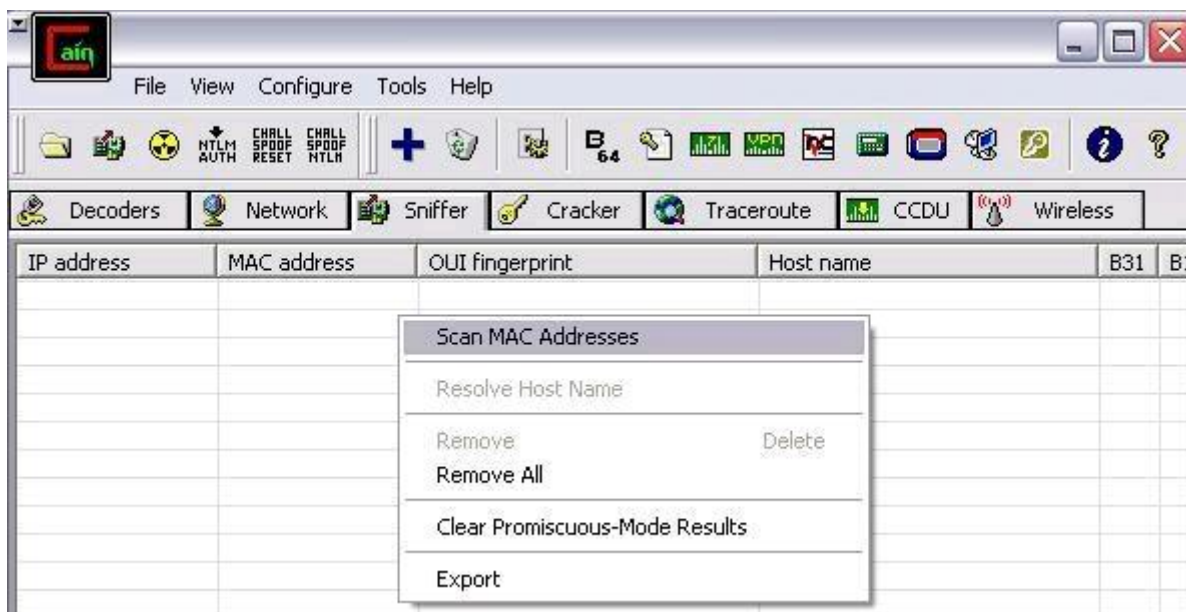


Bien, una vez hecho ésto, clickeamos en <Aceptar> y tendremos frente a nosotros a Caín. Hoy sniffaremos de todo lo que salga, Contraseñas Encriptadas, Texto Plano, Ftp, Http, Myspace, Hi5, etc.,.

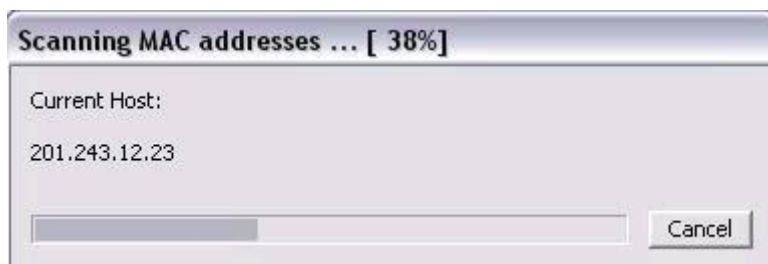
Venga, nos vamos a la Pestaña Superior "Sniffer" y luego a la Pestaña inferior "Hosts", Una vez ahí, Arrancamos el Sniffer, ¿Cómo?, pues en el Segundo botón que aparece arriba, al lado de una carpeta:



Listo, ahora Hacemos click secundario sobre Caín y seleccionamos "Scan Mac Addresses" como en la Imagen:



Esto buscará direcciones MAC de ordenadores en nuestra Red, así que esperamos...

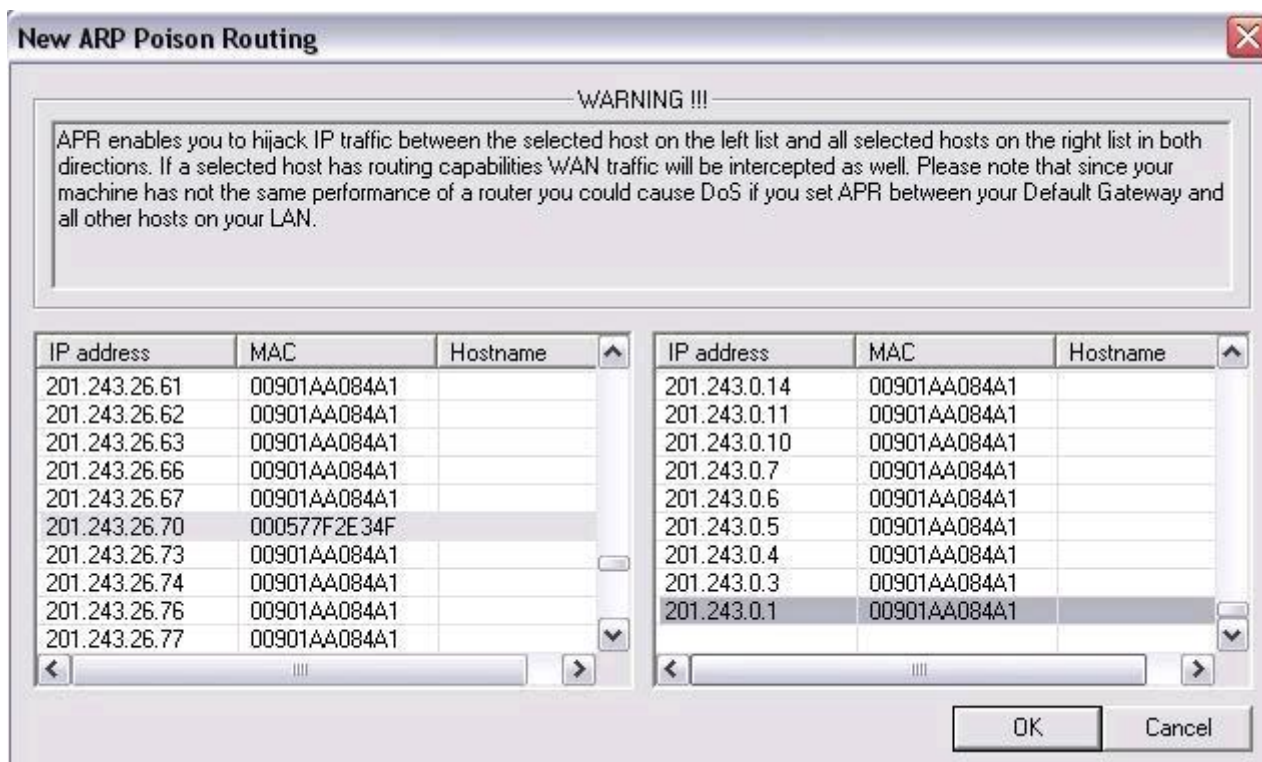


Pasado un tiempo, Caín ya habrá escaneado toda la Red, así que seleccionamos las direcciones IP de los "Targets" u objetivos que queremos sniffar, para eso nos vamos a la pestaña inferior "APR" y clickeamos sobre el botón "Add to list":



Acto seguido aparecerá una ventana doble, En la izquierda seleccionamos el objetivo "A" de la lista de IPs, ésto

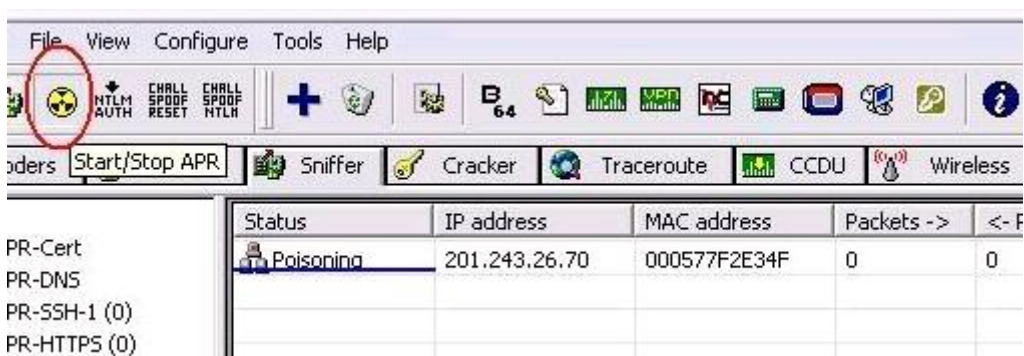
Llenará el lado derecho con otras direcciones IP, en ese lado debemos seleccionar la IP del objetivo "B" (El Gateway), Justo como un 'Man In The Middle':



¿Por qué debo llenar esa estúpida tabla? Simple, esa es la tabla en la que le indicaremos a Cain cómo deberá envenenar las tablas ARP (Address Resolution Protocol) de las víctimas.

Nota: Si estás en una red concentrada (Conectada por Hubs), no es necesario envenenar las tablas ARP de nadie, ya que los paquetes llegan solos, en cambio, si estás en una red conmutada (Switch), sí es necesario envenenar las tablas ARP de la red.

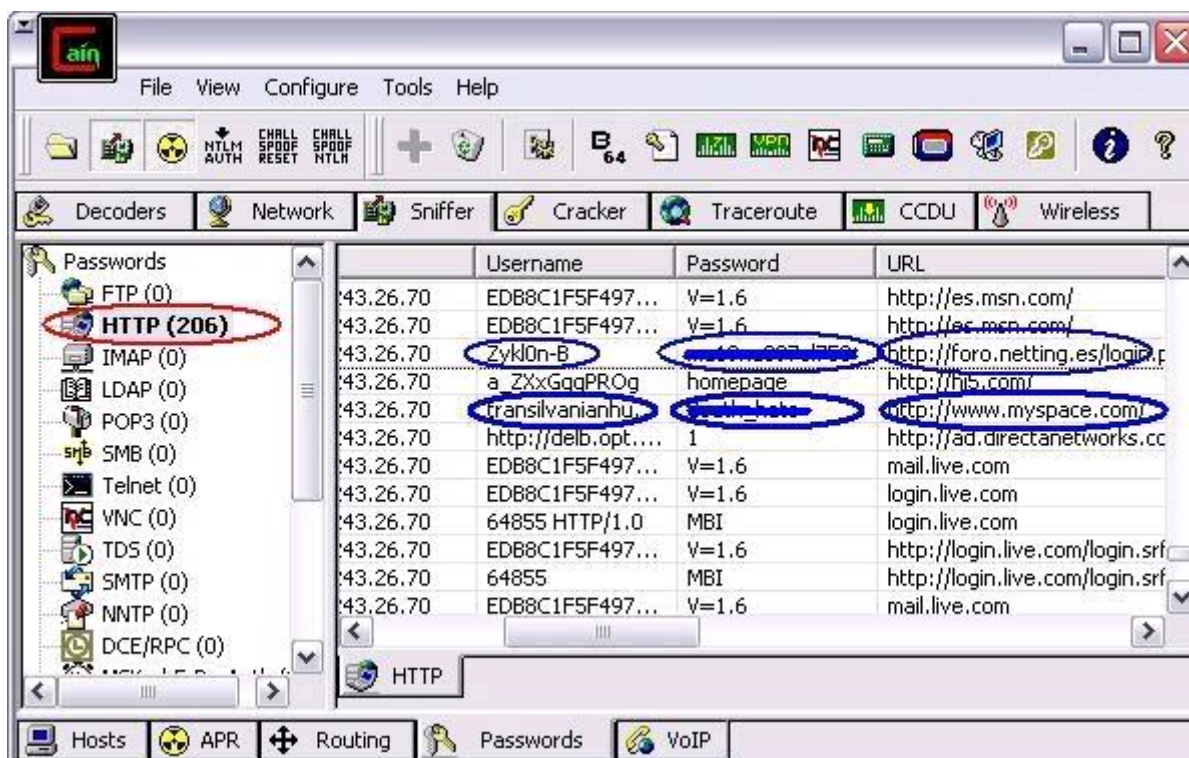
Hecho esto, debemos empezar a envenenar las tablas ARP de nuestra Red (porque estoy bajo un Switch, mi red es conmutada), para eso hacemos click sobre el botón amarillo de "APR", marcado en la Imagen, también he marcado en azul la indicación de Cain de que está "Poisoning" es decir, envenenando:



Ya ha empezado el ataque, ya sólo nos queda tomarnos un café, ligar con una tía y esperar a que nuestra víctima introduzca todas sus contraseñas como lo haría todos los días, ya que no se dará cuenta del envenenamiento...

Sólo 2 minutos después, revisemos el resultado de Cain, para eso nos dirigimos a la pestaña superior Sniffer y a la pestaña inferior Passwords...

Veamos:



¡Vaya, 206 passwords! , Pero no se emocionen, sólo son paquetes, pero he resaltado en azul los passwords que sí son verdaderos, y para colmo, viajan en texto plano.

Un ejemplo:

Id...	C...	Username	Password	URL
6...	2..	zyklon.mv@gmail.com	mat3nacc3f@1337	https://www.google.com/accounts/L
2...	2..	transilvanianhunger1@hotmail...	mat3nacc3f@1337	http://www.myspace.com/
2...	2..	m-villasana@hotmail.com	mat3nacc3f@1337	http://hi5.com/friend/importer/displa

Ahí podemos ver las contraseñas de Myspace, Google y Hi5, todas en texto plano. Vaya seguridad, ¿eh?

Así sucede con los passwords en FTP, SMTP, HTTP, POP3, VNC, MYSQL, ICQ, Hi5, Photobucket, Yahoo, Hotmail, Gmail, etc.. Y además, Cain contiene "Certificados de Autenticidad" falsos. Para hacerle creer a la víctima que todo anda bien y legal, como verán, "Hackear contraseñas" no es nada del otro mundo cuando disponemos de Cain.

Ahora, ¿qué sucede cuando el Cain detecta passwords encriptados? ¿Los desecha? Pues no, Cain, automáticamente los lleva a la pestaña superior "Cracker" ¿Qué es eso? ¡Hombre! es lógico lo que es, un crackeador múltiple de contraseñas. Ahí tenemos una lluvia de opciones, podemos desencriptar contraseñas a través de diversos modos, Bruteforce, Criptoanálisis, Ataque por Diccionario, etc..

Cain, también funciona Sniffando paquetes Wireless, y hasta tiene herramientas de Wep Cracking y demás, y puede ser combinado con otras herramientas tales como Aircap, Airdump, etc..

Nota: Les recomiendo que cuando se encuentren sniffando no abran en sus ordenadores páginas ni ningún tipo de conexiones, ya que ésto les dificultará más el trabajo, recuerden que estamos "Husmeando" los paquetes que llegan a nuestra tarjeta de Red, y si nosotros metemos más paquetes ni les cuento...

¡Ah! que se me olvida, para poder cerrar Cain deben parar el envenenamiento APR y detener el Sniffer.

## Cain & Abel (II) - DNS Poisoning

Saludos, hoy les enseñaré a realizar un ataque bastante divertido, un ataque de DNS Poisoning, y también les mostraré la otra mitad de Caín, su hermano Abel. Podrán empezar y detener servicios de la víctima, obtendrán una Shell remota (gracias a Abel), etc.. Pero no me extenderé mucho, será necesario haber hecho la práctica pasada con Caín.

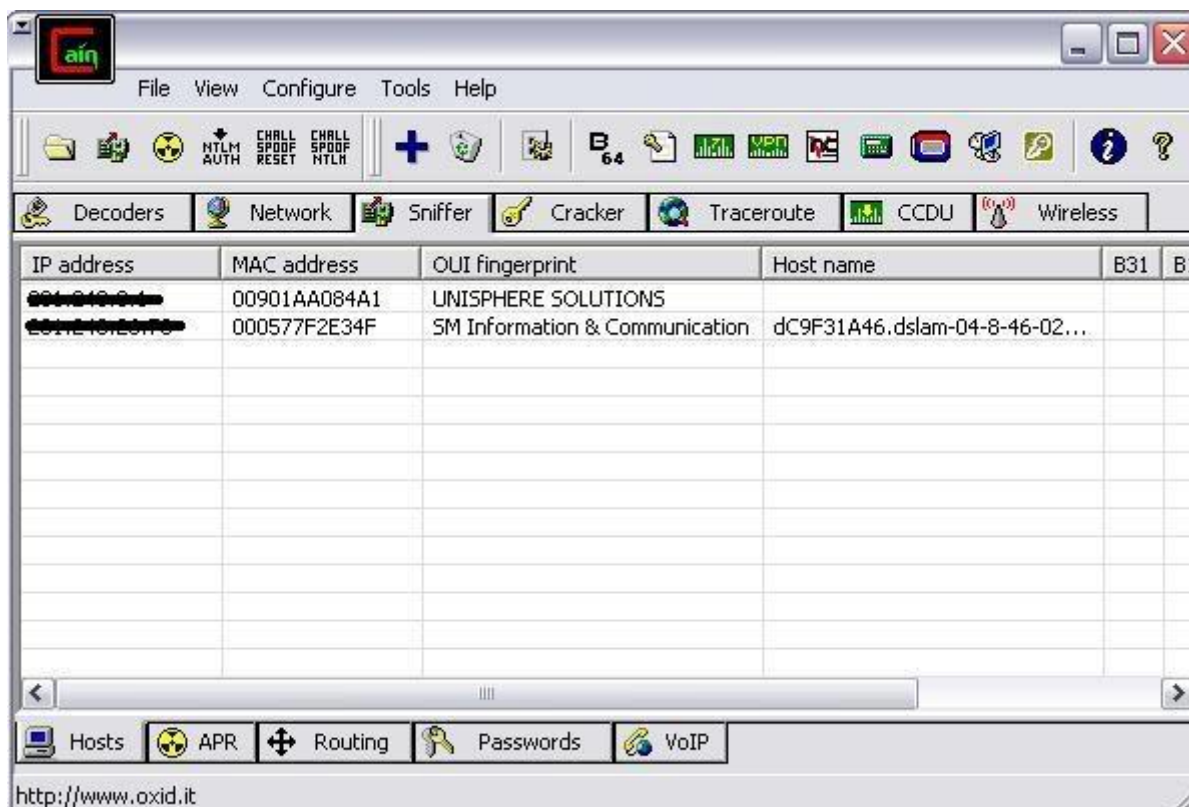
Nota: Para utilizar a Abel en un equipo remoto es necesario conocer un User y Password válidos, y haber copiado a Abel previamente en el equipo remoto (todo esto lo puedes hacer leyéndote las prácticas).

### ¿Qué es un ataque DNS Poisoning?

Como su nombre indica, es un ataque basado en el "Envenenamiento" de la Caché DNS de la víctima, es decir, agregaremos valores de relación Dominio-IP de su Caché DNS.

Vale vale, no entiendes aún, imagínate que cambiáramos la Caché DNS de la víctima, y le dijéramos que al nombre de dominio "www.microsoft.com" le corresponde la dirección IP de una página XXX cualquiera. ¿Qué pasará cuando la víctima escriba en su Navegador "www.microsoft.com"? Exacto, irá directamente a la página XXX que le hemos indicado a la Caché. Interesante, ¿no? Y lo mejor es que podemos hacer ésto con cuantos nombres de dominio se nos ocurran.

Vale, abran su Caín, configúrenlo como les parezca necesario, hagan un Host Scanning, y encuentren las direcciones de la víctima y del Router (Gateway, puerta de enlace) de la red:



Hagan exactamente lo mismo que en la práctica pasada, un ataque tipo "Man In The Middle". Envenenen las tablas ARP. ¿Listo?

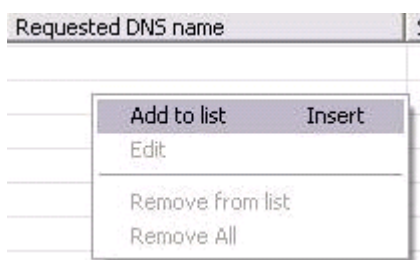
Yo ya encontré a mi víctima y al Router de la Red, ahora arrancaré el Sniffer y envenenaré las tablas ARP de ambos, justo como el MITM pasado, para poder realizar el ataque DNS Poisoning.

Listo. Mientras Caín se encuentra "poisoning", nosotros podemos "agregarle condimentos" a ese veneno. Hoy le agregaremos a la caché DNS valores "spoofeados".

Bien, ya estoy sniffando los paquetes que viajan entre la víctima y el Router, ahora en la pestaña superior [Sniffer], me dirijo a la pestaña inferior [APR]. A la Izquierda vemos varias opciones, pero la que nos interesa a nosotros es "APR-DNS":



Una vez ahí, del lado derecho nos saldrá un campo vacío llamado "Requested DNS name". Hacemos click secundario ahí y seleccionamos la opción "Add to list Insert", como en la imagen:



Esto hará que se nos abra una ventana nueva llamada "DNS Spoofer for APR" pidiéndonos un nombre de dominio y una dirección IP. En el campo del Nombre de dominio escribimos el de la página que queremos "Spoofer", por ejemplo, "www.microsoft.com", y en el campo de dirección IP escribimos la IP a la cuál queremos que vaya la víctima cuando intente conectarse con [www.microsoft.com](http://www.microsoft.com). ¿Qué fácil no?

Yo he colocado la Dirección IP de una página Basura, así que cada vez que la víctima intente ir a [www.microsoft.com](http://www.microsoft.com), irá directamente a la página "Limpia basura" (así se llama):



Listo. Pulsamos <OK> y ya estará envenenada la víctima.

Este es el resultado:



Jaja, por algo dije que era divertido este ataque, puedes Spoofear cualquier página que quieras.

Ahora pasemos a ver a Abel, que creo que en la práctica pasada no expliqué lo qué era en Realidad y no quedó claro.

Caín & Abel es el nombre del programa, pero no son el mismo programa. Me explico, Caín es el Sniffer que tanto hemos estado usando, pero Abel es otra aplicación, es un Servicio NT aparte.

¿Cómo es eso?

Cuando Instalamos Caín, también se copia Abel, pero no se Instala, nosotros tenemos que Instalarlo, ya sea local o remotamente.

Abel consta de 2 archivos: "Abel.exe" y "Abel.dll". Una vez instalado corre como un servicio NT de Windows, y nos ofrece una shell remota que manipulamos mediante Caín y otras cosas como las tablas TCP/UDP remotas, la tabla de Routing, puede volcar los Hashes de usuarios de la base de datos SAM remotos, etc.,.

Los datos transmitidos entre Caín y Abel se encriptan utilizando el método de Cifrado RC4, el cual también utilizan los protocolos WEP, SSL, WPA, ...

Bien, veamos cómo instalar Abel localmente.

Abre una shell y dirígete al directorio de Caín, que por defecto es C:\Archivos de Programa\Caín\.  
Ahí es donde se encuentra Abel.

La instalación de Abel es algo complicadísimo que no sé si entenderán, pero igual se lo explico.

Para instalarlo, escriban el siguiente comando desde el directorio de Caín:

C:\Archivos de programa\Caín\ > Abel



Y para desinstalarlo:

C:\Archivos de programa\Caín\ > Abel -r



¿Ven lo difícil que es?

Bien, Abel está instalado pero no corriendo. Para arrancarlo debemos ir a Caín y dirigirnos a la pestaña superior [NETWORK], allí desplegamos la pestaña [Entire Network] y luego le damos click secundario a la opción "Quick List", y en ella seleccionamos la opción "Add to Quick List":



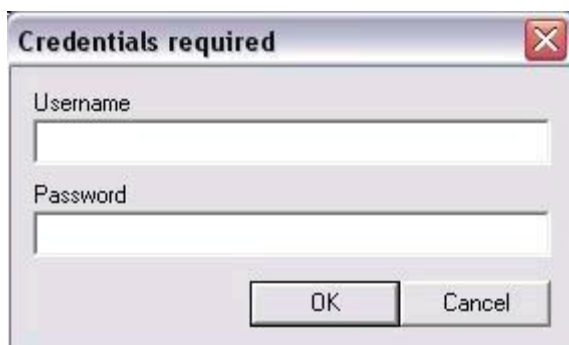
Esto hará que nos salga una ventana nueva pidiéndonos la dirección IP ó el nombre de la máquina a la que nos queremos conectar. Lo informamos y presionamos <OK>:



Ahora desplegamos "Quick List" y nos aparece el ordenador que acabamos de agregar, Para conectarnos a él hacemos click Secundario sobre su nombre y elegimos la opción "Connect as". Nos aparecerá una



ventana pidiéndonos un nombre de usuario y una password válidos para ese ordenador, si no los tenemos, estamos fritos... ¡Pero, hombre! ¿Para qué tienes el Sniffer? Para dar con los Passwords...



Vale, nos logueamos en la máquina remota y tendremos acceso a varios recursos, tales como los Grupos de Usuarios, los Servicios, los recursos compartidos y los nombres de usuario.

Pero nosotros necesitamos arrancar Abel (que lo hemos subido e instalado previamente), así que nos vamos a "Services" donde se mostrarán TODOS los servicios del ordenador remoto. En esa lista debemos buscar a Abel, que debería aparecer como "Stopped". Para arrancarlo simplemente hacemos click secundario sobre su nombre y seleccionamos la opción "Start":



Una vez que ha arrancado Abel, contraemos el nombre del ordenador, lo volvemos a desplegar y vemos que hay algo nuevo... ABEL.

Al desplegar a Abel nos encontramos con varios servicios:

- Console
- Hashes
- Lsa Secrets
- Routes
- TCP Table
- UDP table

### Console

Nos da una Shell remota con permisos de System:



## Hashes

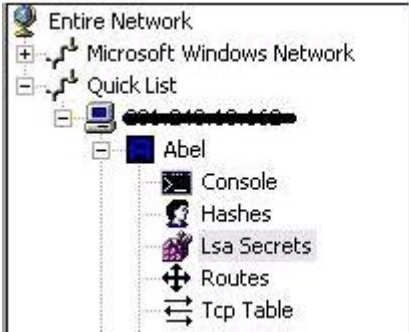
Nos da los Hashes de todos los usuarios del ordenador remoto:



User Name	RID	< 8	LanMan Hash
Administrador	500	*	AAD3B435B51404EEAAD3.
Asistente de ayuda	1000		49029D54ED2360DCC0B9.
Invitado	501	*	AAD3B435B51404EEAAD3.
SUPPORT_388945a0	1002	*	AAD3B435B51404EEAAD3.
user	1003	*	AAD3B435B51404EEAAD3.
_vmware_user__	1010	*	AAD3B435B51404EEAAD3.

## Lsa Secrets

Vuelca del registro de Windows las llaves Lsa Secrets (Local Security Authority) que se encuentran en el directorio HKEY\_LOCAL\_MACHINE\Security\Policy\Secrets:




```
=== Cain's LSA Secrets Dumper ===
=====

0083343a-f925-4ed7-b1d6-d95d17a0b57b-Remot
64 00 45 00 3D 00 33 00 50 00 70 00 46 00 71 00
4E 00 55 00 66 00 52 00 67 00 69 00 00 00    N

0083343a-f925-4ed7-b1d6-d95d17a0b57b-Remot
```

## Routes


Nos devuelve un "Route print" del ordenador remoto:



Destination	SubnetMask	Def.Gateway	Interface
0.0.0.0	0.0.0.0	201.243.0.1	201.243.10.16
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
201.243.0.0	255.255.224.0	201.243.10.162	201.243.10.16
201.243.10.162	255.255.255.255	127.0.0.1	127.0.0.1
201.243.10.255	255.255.255.255	201.243.10.162	201.243.10.16
224.0.0.0	240.0.0.0	201.243.10.162	201.243.10.16
255.255.255.255	255.255.255.255	201.243.10.162	201.243.10.16

## TCP Table

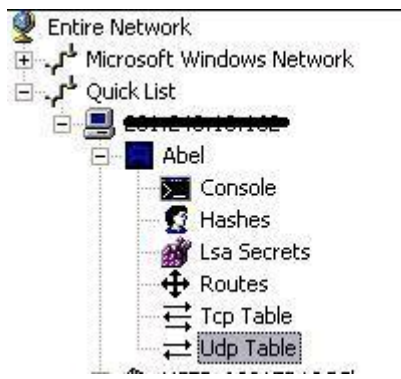
Nos muestra una tabla con las conexiones TCP del ordenador remoto:



Process	Protocol	Local Address	Local Port	Rer
Not supported	TCP	0.0.0.0	80	0.0
Not supported	TCP	0.0.0.0	135	0.0
Not supported	TCP	0.0.0.0	443	0.0
Not supported	TCP	0.0.0.0	445	0.0
Not supported	TCP	0.0.0.0	636	0.0
Not supported	TCP	0.0.0.0	990	0.0
Not supported	TCP	0.0.0.0	993	0.0
Not supported	TCP	0.0.0.0	995	0.0
Not supported	TCP	0.0.0.0	3306	0.0
Not supported	TCP	0.0.0.0	7614	0.0

## UDP Table

Nos muestra una tabla con las conexiones UDP del ordenador remoto:



The screenshot shows the Windows Network Explorer interface. On the left, the tree view is expanded to show the 'Udp Table' for the remote computer 'Abel'. The main pane displays a table with the following data:

Process	Protocol	Local Address	Local Port
Not supported	UDP	0.0.0.0	445
Not supported	UDP	0.0.0.0	500
Not supported	UDP	0.0.0.0	1025
Not supported	UDP	0.0.0.0	1111
Not supported	UDP	0.0.0.0	1112
Not supported	UDP	0.0.0.0	1487
Not supported	UDP	0.0.0.0	3375
Not supported	UDP	0.0.0.0	3376
Not supported	UDP	0.0.0.0	3377
Not supported	UDP	0.0.0.0	3378
Not supported	UDP	0.0.0.0	3379
Not supported	UDP	0.0.0.0	3380

Bueno, ya lo que queda es de parte de ustedes. Espero haber aclarado las dudas que existían con respecto a Abel y que hayan entendido y disfrutado todo esto.

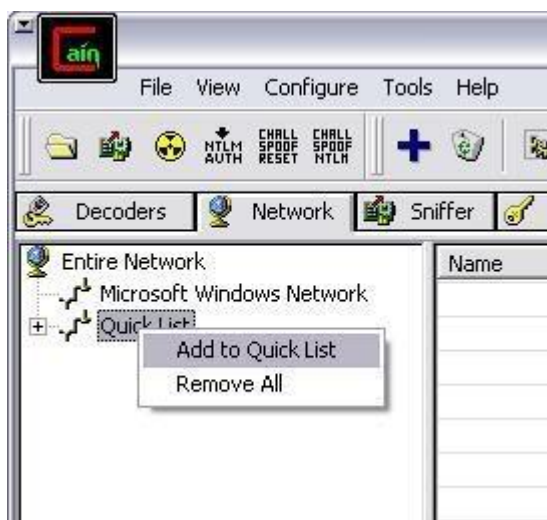
Saludos.

## Cain & Abel (III) - Instalando Abel remotamente

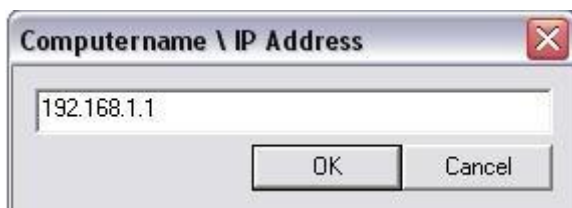
Saludos, en la práctica pasada vimos qué demonios era Abel, vimos qué nos ofrece y las utilidades que trae y vimos cómo instalarlo LOCALMENTE. Y eso a nosotros no nos gusta, porque tener contacto físico con el PC víctima "canta" demasiado, además tenemos que copiarle e instalarle Abel y bla, bla, bla....

Hoy aprenderemos cómo instalar el servicio Abel de manera remota, algo bastante fácil la verdad, ya que Caín hace casi todo por nosotros...

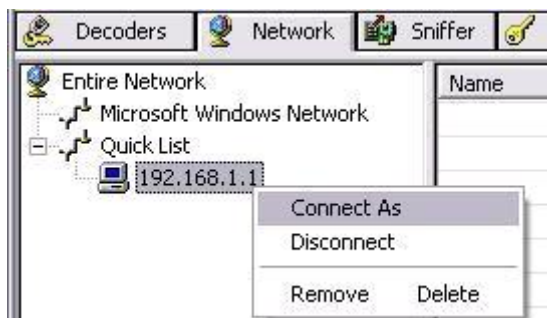
Abrimos nuestro Caín, lo configuramos como siempre, y nos dirigimos a la pestaña superior [Network]. A la izquierda seleccionamos el menú desplegable "Quick List" (Lista rápida), hacemos click secundario y seleccionamos la Opción "Add to Quick List":



Ésto hará que nos aparezca una ventana nueva solicitando el nombre y/o la dirección IP del PC que queremos agregar a Caín. Se los damos y pulsamos <OK>:



Listo. Desplegamos el menú "Quick List" y aparecerá el PC víctima agregado. Ahora debemos conectarnos con él, para eso hacemos click secundario sobre el nombre del PC y seleccionamos la Opción "Connect as":



Esto desplegará una ventana nueva llamada "Credentials Required". Lógico, ¿no esperarías tener acceso tan fácilmente...?

En el campo Username escribimos un nombre de usuario válido en el PC víctima y en el campo Password, escribimos la contraseña para dicho usuario.



**Nota:** Dado que Abel proporciona una Shell remota con privilegios de System (súperusuario) y nos brinda acceso a diferentes servicios del PC remoto, debemos loguearnos con permisos de Administrador, ya que de otro modo, al instalar Abel quedarían inutilizadas la mayoría de sus opciones, así que ponte a Sniffar para capturar el password del Admin.

Vale, ya nos hemos logueado como Admin, ahora a lo que vinimos, a instalar Abel. Para ello desplegamos el menú de la dirección IP de la víctima y nos aparecerá un nuevo menú con el nombre del PC. Lo desplegamos también. Luego nos aparecerán las 4 opciones por defecto que nos da Caín sin usar Abel, que son:



### Groups

Nos muestra los grupos de usuarios del ordenador remoto, tales como Administradores, Invitados, Usuarios Avanzados, Operadores de Red, etc.,.

### Services

Nos muestra y da acceso a todos los servicios que están corriendo en el PC remoto, tales como servidores Telnet, Ftp, Antivirus, servicios de Red, Firewall, etc.,.

### Shares

Muestra las unidades y/o recursos que está compartiendo el ordenador remoto. ¿Quién necesita un Scanner NetBIOS cuando Caín te da esto?:

Share	Desc	Path
IPC\$	IPC remota	
print\$	Controladores de impresora	C:\WINDOWS\system32\
ADMIN\$	Admin remota	C:\WINDOWS
C\$	Recurso predeterminado	C:\

Users

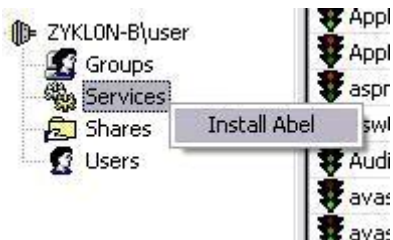
Muestra y enumera los usuarios remotos, al seleccionar esta opción solicita permiso para enumerarlos:



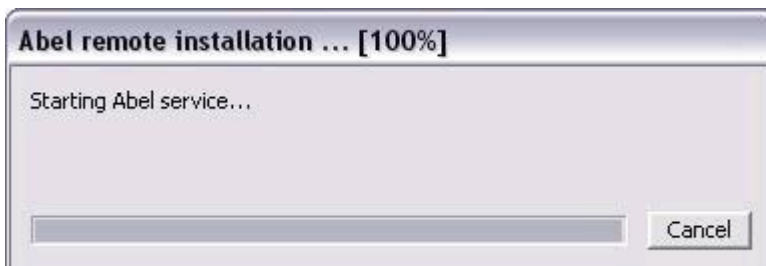
Vale, vale, que nos vamos por donde no es...

En la práctica pasada dijimos que Abel era un SERVICIO de Windows, ¿cierto? Pues, si te fijas bien, Caín nos ha dado acceso a los servicios remotos, así que, ¿por qué no instalarle el servicio Abel?

Seleccionamos el menú "Services", hacemos click secundario y seleccionamos la opción "Install Abel", así de fácil:



Al hacerlo, se nos mostrará una ventana de diálogo indicándonos el proceso de instalación:



Listo. Ahora, si revisamos los servicios, veremos que Abel se encuentra el último, instalado y corriendo. Ya podemos utilizarlo.

Nota1: Para desinstalar Abel, debemos escribir en la misma shell que él nos proporciona el siguiente comando:

```
C:\Windows\System32\>Abel -r
```

Bueno, espero que les sirva. Luego veremos qué más hacer y nos adentraremos al Sniffing en Redes Wireless.

Saludos.