

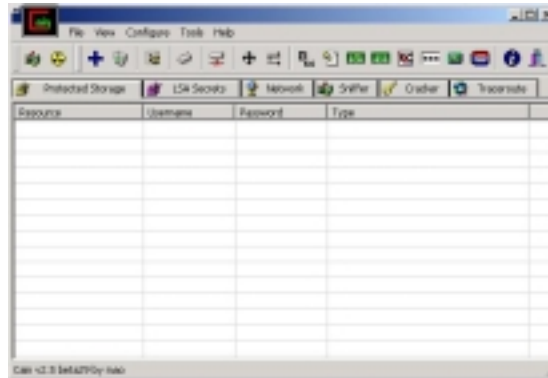
Práctica 37. Esnifer y craqueo de contraseñas. CAIN (Por HxC Mods-Adm)

Lo primero, claro, instalar Cain, no tiene ningún misterio, sólo una cuestión, Se necesita tener instalado WinPcap 2.3, No, no te preocupes, ya viene incluido.

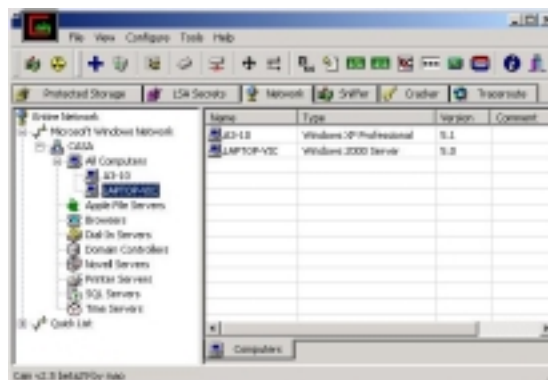
<http://www.oxid.it/cain.html>

Qué es Win Pcap, pues en pocas palabras: Un driver para captura de paquetes.

Al ejecutar *Cain*, verás esta pantalla:



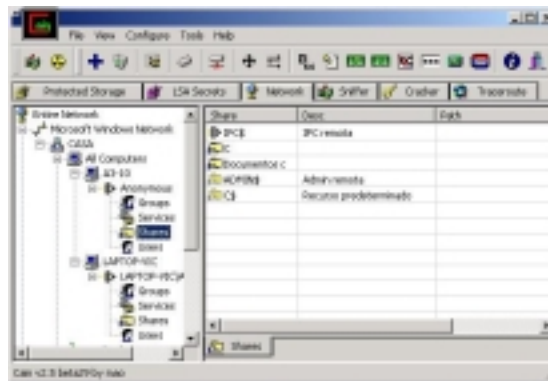
Vamos a inspeccionar nuestra red, Pinchas la ficha NetWork y expande el árbol de Microsoft NetWork....



Aparecen los equipos que pertenecen al dominio o grupo de trabajo, incluso si alguno “no está” o pertenece a otro segmento de red puedes añadirlo en Quick List.

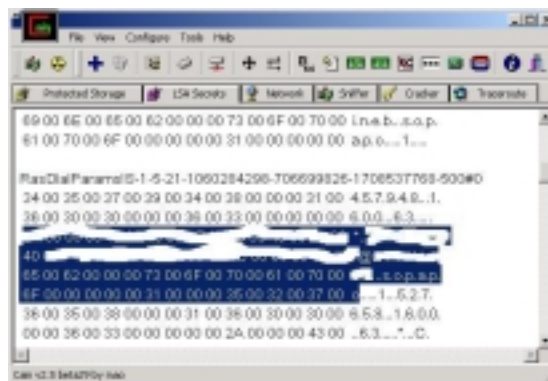
Foro de HackXcrack

Como ya se dijo antes, Cain puede enumerar recursos, usuarios, etc. Vamos a probar sobre uno de los equipos Expandiendo el arbol y pinchando en Shared



Interesante, tiene compartido Toda la unidad C, pero no importaría que no tuviese nada compartido, IPC\$ siempre está....

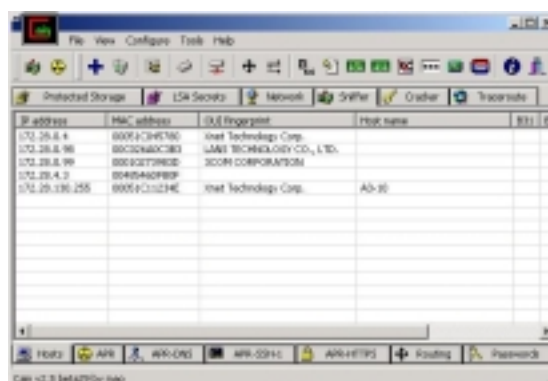
La curiosidad nos mata y es que suena bien, Secretos LSA, ¿Qué es?, al final lo sabrás, pero ahora vamos a probar algo....



Cuando Pinchamos en LSA Secrets y después en el Signo + que hay en azul, se nos llena una pantalla con datos ¿incomprensibles?, Fíjate bien, He resaltado (en azul) parte del volcado de RAS DIAL, es decir, el equipo tiene un MODEM (Es mi portátil, cuidadín. Por eso he borrado la conexión pero he dejado la contraseña) SE VE, SE VE EL PASS de conexión del módem pone **s.o.p.a.p.o** , esa ERA mi contraseña hasta hoy, sopapo (sin los puntos)

Hay más acerca de LSA, pero es sólo para hacer boca.

Vamos a la Ficha Sniffer,

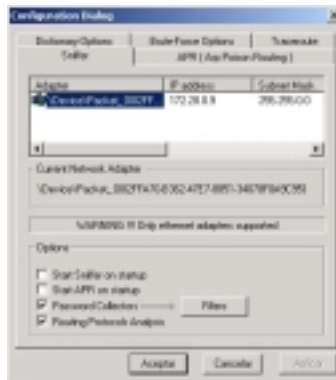


Foro de HackXcrack

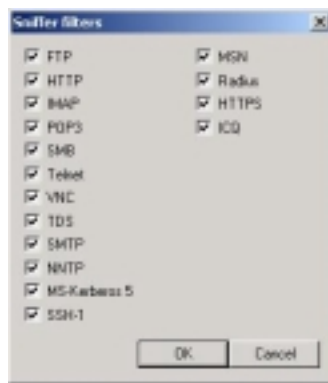
En la zona inferior de la pantalla de Cain, tenemos Host (lo que ves en la pantalla anterior), ARP, ARP-DNS.....y al final Password

Una puntualización, Tu no verás lo mismo que yo en Host, de hecho la primera vez que uses *Cain* no verán NADA, hay que agregar los equipos a esnifar, pero antes hay que poner en marcha el Esnifer, vamo a ello.

Pinchamos en el Menú Configure



Aparecerán las tarjetas de Red que dispones (ficha Sniffer de Configure) y un Botón que pone Filters: Los protocolos y/o autentificaciones a esnifar:



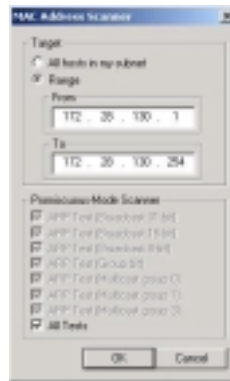
Creo que no hacen falta muchos mas comentarios, lo dejamos todo seleccionado o si queremos alguno en especial pues quitamos los que nos sobren.

En la Ficha APR (ARP Poison Routing) Envenenamiento ARP:



Fíjate bien, mi IP real es la 172.28.0.9, sin embargo “suplanto” la identidad de 172.28.0.44 e incluso la dirección MAC, en este caso, el IP Spoofing corresponde al mismo segmento, ojo la IP envenenada no debe existir en la red, sino ya sabes....

Ahora es cuando podemos usar el signo + en azul para escanear las máquinas de la Red, aparecerá algo así:

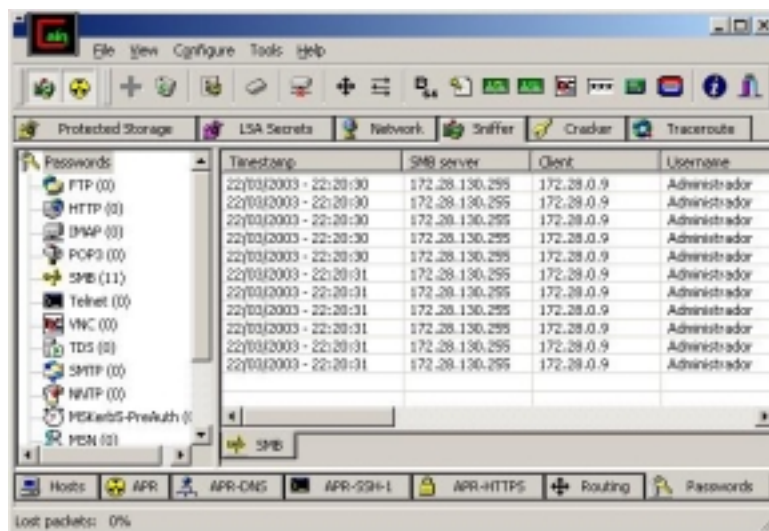


Puedo escanear todo el rango Uff, qué pesado

Puedo escanear un Rango, mejor. Ahora advierte una cosa, los esnifer sólo escanean efectivamente el rango de la tarjeta de red a que pertenecen, pero como hemos envenenado la dirección ARP y nuestra dirección MAC aunque perteneciésemos al rango 192.168.xxx.xxx (dirección real de la tarjeta de Red) podríamos esnifar el rango 172.28.xxx.xxx, puesto que anteriormente en Configure-APR le indicamos a Cain que nuestra IP Spoofing era 172.28.0.44

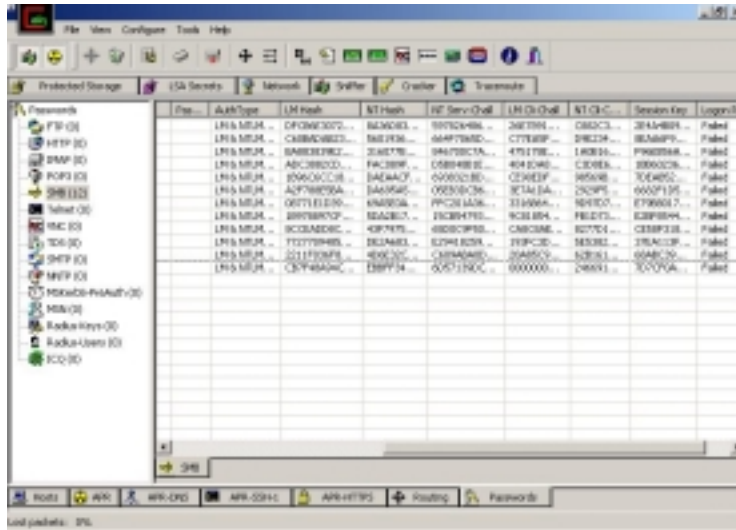
Lo de los test multicast, broadcast, etc. es largo y tendido, así que propongo que primero se esnife si test y si no escuchamos nada, pues marcamos todos los test (all test), me cuesta adivinar las distintas topologías de red que tengáis cada uno....

El caso es que una vez realizados los test o no ya podemos empezar, la primera es muy simple, Supongamos que el Administrador (que soy yo en el portátil) se conecta a un recurso compartido del equipo donde está el esnifer (el XP) qué hace nuestro esnifer, observa:



Foro de HackXcrack

Ha capturado algo, ¿Dónde? En el protocolo SMB (parte izquierda), como esto es interesante, voy a poner otra pantalla más que corresponden a otras columnas que están más a las derecha de las que vemos...



He ajustado las columnas para que se vean “todas un poquito”, ¿Decepcionado? La columna Password (la primera que vemos en la vista de esta pantalla) está vacía, QUE ESPERABAS.

Pero tenemos los Hashes de desafío-respuesta.

Quiero que prestéis atención a la última columna Logon Request, aparece Failed, y esto lo he hecho a propósito, para que no haya trampas ni cartón, pero ¿Qué quieres decir?

Pues que el Administrador del equipo Server se ha intentado conectar a un recurso compartido del equipo XP (el del sniffer) y NO HA CONSEGUIDO CONECTARSE, de otra forma el usuario y contraseña que puso no era válido.

Seguro que estás perdido, (yo ya lo estoy) lo que quiero decir es que NO HACE FALTA que se complete la conexión ni que tenga éxito, que por el SIMPLE HECHO de INTENTARLO ya le cazamos su hashes.

¿Por qué es importante? Pues porque según esta experiencia, lo que debemos hacer es montar un servidor SMB Fraudulento (ya lo tenemos es nuestro XP + el esnifer) e invitar al resto de la red a que “nos visiten”, no hará darles usuarios ni contraseñas, bastará que simplemente intenten conectarse a un recurso compartido en nuestro equipo, de hecho no hace falta ni que compartamos NADA, tenemos a nuestro querido IPC\$.

Y cómo conseguimos eso, pues aquí es donde vuestra imaginación y práctica empiezan, (o es que os creáis que os lo iba a dar todo), bueno, apunto alguna:

Podemos crear una página web con un hiperenlace a un recurso de nuestro equipo QUE NO EXISTA, por ejemplo a nul.gif, por que lo de que no exista, pues porque simplemente le dirá que esa página no existe y tal y tal y el tío NI SE ENTERARÁ que le hemos birlado la contraseña.

Si disponemos de correo interno, mejor aún, le enviamos la misma página por mail (recuerda que un correo con formato HTML no es más que una web por correo) lo que pasa es que si utiliza IMAP o Webmail no nos funcionará.

También podemos simplemente no hacer nada y esperar, seguro que alguien pasa por nuestro SMB

Podemos enviar un mensajito (Net send o similar) al grupo o al dominio diciendo que en la carpeta compartida [lomejordelaweb](#) tienes yo qué sé.....

Foro de HackXcrack

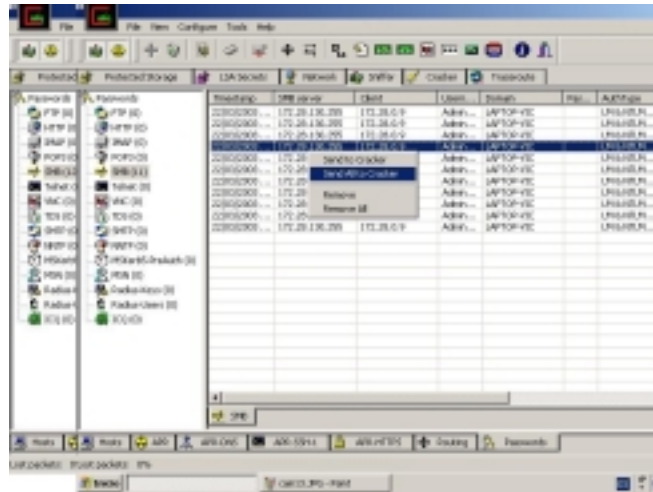
Ahora, los hashes que esnifas son los de los usuarios que se conectan, es decir, que si el administrador de la red “te visita” pero utiliza una cuenta restringida, pillarás ese hash, por eso hay una máxima en seguridad: La cuenta de administrador para Administrar.

Ahora puedes empezar a entender lo peligroso que es Navegar por la Red con privilegios administrativos...

Bueno seguro que se te ocurren muchas otras más, Animo.

Todavía no tenemos todo ganado, nos falta averiguar la contraseña, pero eso es coser y cantar.

Sobre cualquiera de las capturas SMB pulsa el botón derecho del ratón y selecciona Send All to Cracker...



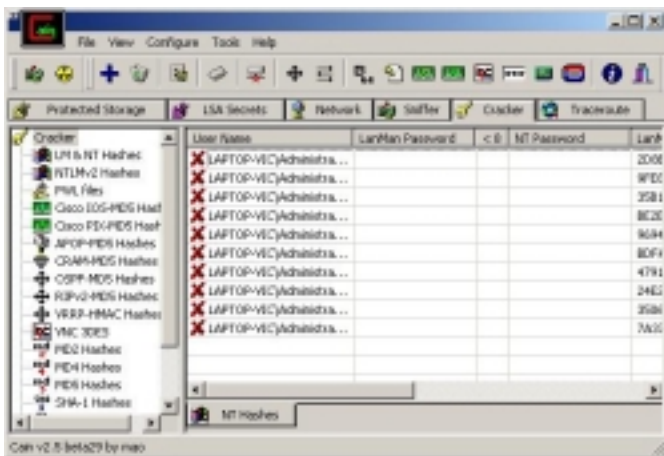
Y se pasarán todos los Hashes al craqueador, para que no tarde mucho yo he puesto una contraseña muy simple (kaka)

El tiempo que puede tardar depende de la longitud y caracteres empleados en la contraseña, pero como se van a dumpear en un equipo local como mucho serán unas horas....

Incluso una vez en pasados los hashes a Cracker, podemos exportar los hashes, guardarlos en un disquete y llevárnoslos a casa y el fin de semana mientras vemos el fútbol nos ponemos a reventarlos con más calma y sin “ojos que nos vean”

Vamos a ello, paramos el sniffer para ello volvemos a pulsar en los iconos Start/Stop esniffer (los de la parte superior izquierda, el verde y el amarillo/negro)

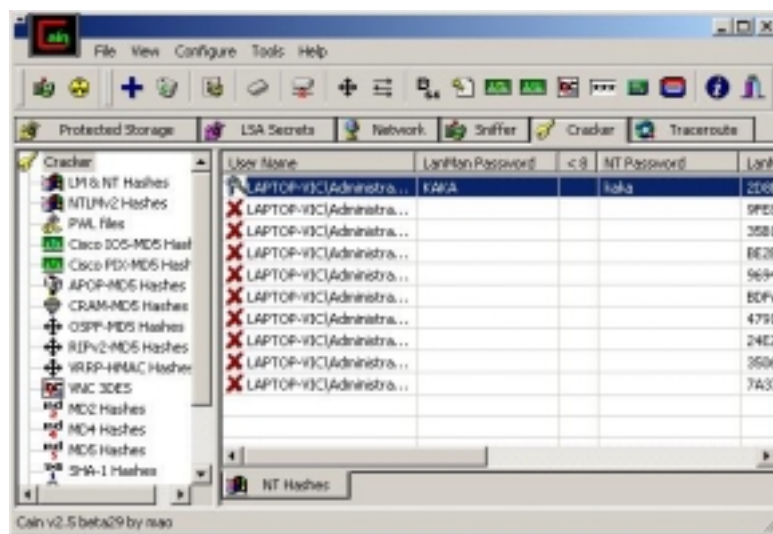
Como ya hemos pasado mediante send all to carcker los hashes, pinchamos en la ficha Cracker (que tiene una llave amarilla)



Seleccionamos cualquiera de esas entradas, mejor la que ponga Administrador como nombre de usuario, que a mi solo me aparecen esas...

Pulsamos el botón derecho del ratón y le damos a Start Brute-Force Attack (Iniciar el ataque por fuerza bruta), podemos usar el diccionario, si tenemos uno bueno, pero por ejemplo mi contraseña (kaka) no figurará en ninguno y mira que es simple.

Pasado un tiempo (muy poquito para este pass) se nos mostrará



Como verás se muestran las contraseñas reveladas LANMan y NTPassword, es la misma una en mayúsculas y otra en minúsculas, como ya sabemos que se trata de un W2K debemos usar la de las minúsculas,.

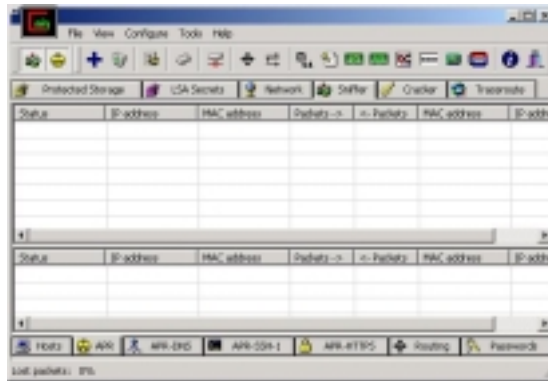
LanMan no distingue entre Mayúsculas y minúsculas, NTLM sí lo hace.

FIN DE LA PARTIDA.

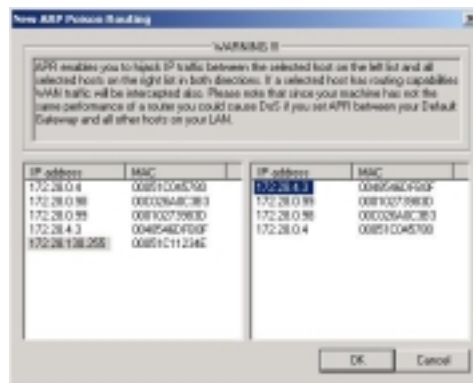
Foro de HackXcrack

Si queréis “trastear” algo más, os cuento, es posible “escuchar” el tráfico de autenticación entre dos ordenadores con la técnica Hombre en medio (nuestro PC), de tal forma que lo que haremos es obligar a que “las conversaciones” de esos equipos pasen primero por el nuestro (con el esnifer preparado) podremos escuchar sus autenticaciones, robar sus hashes y así no necesitamos “invitar” a nadie a visitarnos.

Cómo se hace eso, superfácil: Con el esnifer a la escucha y envenenamiento ARP en marcha, seleccionamos la ficha APR de la zona inferior de la pantalla

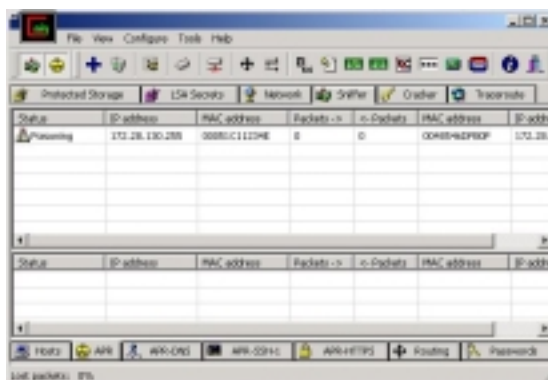


Pulsamos en el signo + que hay en azul en la barra de herramientas



Y eliges de la zona izquierda y derecha las Ip's de los equipos a escuchar...

Repite el mismo paso si deseas escuchar más equipos, para finalizar pulsa en OK



Como ves se ha puesto a esnifar el tráfico entre esos dos equipos y nosotros lo oiremos... Luego repite los pasos anteriores de captura SMB, Cracker, etc.