FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

2ª FAQ de como de conseguir las contraseñas de usuarios remotos en una LAN utilizando un sniffer.

Escenario:

Una LAN con:

1 Windows 2000 Server como servidor de dominio
1 XP con el sniffer a la escucha
x Clientes Windows (variedad)
1 Switch 10/100

Software

Cain & Abel 2.5 beta 29, está calentito, ha salido en éste mes

Lo primero Bajarse el Cain. http://www.oxid.it/cain.html

¿Por qué Cain y no otros?

a) Es gratis, sin patch, no keygen ni leches.
b) Dumpea Secretos LSA
c) Enumeración de usuarios, grupos, recursos compartidos
d) Escanea SID
e) Envenenamiento ARP, DNS, ARP-HTTPS y ARP-SSH
f) Permite Filtros para HTTP-BASIC, HTTP-FORM, HTTP-COOKIE, POP3, IMAP, FTP, VNC, HSRP, SMTP, NNTP, TDS (Sybase and MS-SQL), MS-Kerberos5 Pre-Auth, VRRP, RIPv2, OSPF, SMB (ClearText, NTLMv1, NTLMv2), NTLMSSP (NTLMv1, NTLMv2), RADIUS, ICQ y MSN
g) Esnifa Sesiones Telnet y SSH-1
h) Descubre Automáticamente IP-MAC
i) Escanea la red en modo promiscuo basado en ARP
j) Revienta contraseñas Access (9x/2000/XP) Database Passwords Decoder Base64, Cisco type-7 y VNC
k) Craquea contraseñas de hashes de MD2, MD4, MD5, SHA-1 y RIPEMD-160
l) Craquea contraseñas de Ficheros PWL files, Cisco-IOS Type-5, Cisco PIX , APOP-MD5, CRAM-MD5, NT HASHES & NTLMv1, NTLMv2, RIPv2-MD5, OSPF-MD5, VRRP-HMAC-96, VNC-3DES, MS-Kerberos5 Pre-Auth), MSN Messenger, RADIUS Shared Secrets
m) Dimpea NT Hash incluso con Syskey habilitado
n) Revelación de contraseñas de asteriscos- Box Revealer
o) Mantenimiento de la Tabla de Rutas
p) Visor de puertos TCP/UDP
q) Trazado de rutas TCP/UDP/ICMP con DNS y cliente WHOIS

Seguro que me he dejado más de una, pero como veis es un programa específico para obtener Contraseñas, sus hashes y romperlas por fuerza bruta o diccionario, se pueden importar/exportar SAM, pwdump, etc., vamos una JOYA.

De todo esto y lamentablemente, esta ocasión, sólo vamos a utilizar El envenenamiento ARP, Volcado de Hashes de equipos remotos mediante un servidor SMB fraudulento, descubrir por fuerza bruta la contraseña de “todo aquel bendito” que se conecte a nuestro PC y como no, la escucha de contraseñas y autentificaciones. POR HOY YA ES BASTANTE, ¿no?

Triste pero necesario, lo primero hay que saber Cómo es el proceso de autentificación en Windows.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Aprendiendo como se autentifican las sesiones en Windows 2000

La autenticación local en un equipo Windows 2000/NT/XP es mediante la señal Ctrl+Alt+Supr

La autenticación en red se realiza mediante protocolos de red.

Las contraseñas de un equipo local se guardan en un archivo llamado SAM del equipo local

Las contraseñas de una red se guardan en Active Directory del controlador de dominio en ntds.dit

Las base de datos de contraseñas y ellas mismas, pueden estar cifradas o no y en algunos casos, las contraseñas pueden almacenarse en el disco local, en el registro o en un disquete, esto se consigue mediante la utilidad Siskey

Si alguno de vosotros conoce "*algo más*" de Windows 2000, estará pensando ¡Esto es mentira!, y cierto, no es del todo verdad, las contraseñas realmente no se almacenan, sino que se le aplica un formato codificado que convierte la contraseña (por ejemplo: perro) en otro valor que se llama Hash, y es ese valor el que se guarda en la SAM junto con el nombre de la cuenta de usuario.

El algoritmo de Hash se aplica a la contraseña y da como resultado un valor que no puede ser descifrado (por lo menos actualmente yo no conozco ningún mecanismo que realice la función inversa), es decir, la función hash es de un solo sentido y no se puede resolver a la inversa.

Ejemplo:

Contraseña----------✍ Algoritmo Hash ----------✍ Valor Hash
Perro----------Algortimo Hash ----------✍ b59f51c4456ad5679900

El valor del hash para la contraseña "perro" no puede ser reutilizado, es decir, por cada nuevo acceso se genera otro hash diferente que relaciona unívocamente a esa contraseña con ese nombre de usuario.

Vamos a olvidarnos por el momento de la autentificación contra un servidor remoto, y veamos qué pasa en el equipo local.

Una vez obtenido el hash, éste se guarda en la SAM junto con el nombre de la cuenta del usuario, por tanto la única forma de asaltar por fuerza bruta las contraseñas de un equipo local es atacando la SAM, bueno me refiero a probar contraseñas, si tenemos acceso al equipo local podemos poner keylogers, sniffers, usar algún bug, exploit, etc.

¿Dónde se guarda la SAM?

Ya se ha posteado anteriormente (de la desaparecida **Nikkyta**) , en un archivo llamado SAM, que estará en:

%systemroot%system32\config\sam.

Ese archivo es "intocable" mientras se esté ejecutando Windows, por lo que un atacante con acceso local "restringido" tendrá que buscar "en otros lugares"

El archivo SAM también se guarda en:

Disquetes de reparación del sistema
%systemroot%repair\sam._
En el registro HKM\SAM

Por tanto para conseguir la SAM de un equipo al que tenemos acceso físico, podemos:

1.- Arrancar con otro Sistema Operativo con soporte NTFS y copiarnos el archivo SAM
2.- Copiar el archivo sam_ del disco de reparación (carpeta o disquete) si es que se hizo.
3.- Extraer los hashes directamente del archivo SAM
4.- Poner sniffers o keylogers para obtener la contraseña.

Las contramedidas no son muy difíciles de implementar:

1.- Deshabilitar el arranque desde disquetes o CD
2.- Borrar el archivo sam._ del directorio winnt\repair una vez hecha la copia del sistema
3.- Restringir el acceso de cuentas con privilegios de administrador, los hashes no se pueden extraer de la SAM sin no se dispone de permisos administrativos.
4.- vigilancia y chequeo de aplicaciones instaladas.
5.- En cualquier caso, utilizar syskey para cifrar doblemente los hashes y la SAM

Otra posibilidad que puede intentar un atacante es detener el sistema de protección de archivos de Windows, lo cual no es sencillo aunque se pueda conseguir...

No obstante, casi todas estos mecanismos son bastante agresivos, ¿Qué pensará un administrador u otro empleado, cuando ve un equipo con “la pantallita negra”, arrancando el equipo de la oficina?

Es muy importante el segundo punto, el archivo que guarda la copia de la SAM de un equipo del que se ha efectuado un disco de reparación (winnt\repair\sam._) NO ESTA PROTEGIDO y es posible llevárselo en un disquete a casa para “pasarle” un craqueador por fuerza bruta.

Ese archivo suele estar comprimido, pero eso no es problema con la herramienta del propio sistema operativo llamada expand.

Además de todo esto, es probable que la contraseña del administrador local no sea la del administrador del dominio (al menos nunca debería de ser iguales) o puede que simplemente NO TENGAMOS cuenta de acceso local (otra cosa que deberia ser de obligado cumplimiento), así que, seguiremos pensando en lo de los sniffers y otros.

Comprendiendo la autentificación en Red

Windows 2000 utiliza de forma predeterminada un mecanismo de autentificación basado en desafío/respuesta para validarse ante un controlador de dominio, de ese modo NI LA CONTRASEÑA NI EL HASH aplicado viajan por el cable de conexión, de esa forma es el servidor quien provoca un desafío aleatorio que envía al cliente para que aplique la función hash a la contraseña, luego el cliente responde al servidor con el desafío haseado y lo reenvía al Servidor quien compara la respuesta con el hash del desafío y entoces otorga o deniega la sesión.

1º El cliente Solicita una sesión al servidor
2º El Servidor emite un desafío al cliente
3º El cliente hasea el desafío con el hash de la contraseña de usuario y lo envía al Servidor
4º El servidor compara la respuesta y permite o no el inicio de sesión

Los hashes son generados en el momento de la creación de la cuenta de usuario, por lo que se limita a ese momento la obtención de los mismos.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Este es un típico caso de autentificación desafío/respuesta en LM/NTLM que es el método predeterminado en sistemas Windows.

Aunque las contraseñas y sus hashes no viajen por la línea, debido a la debilidad del hash LM es posible adivinarlo, para ello los sistemas Microsoft puede utilizar otros métodos aunque todos tienen sus ventajas e inconvenientes, el mayor de todos, la compatibilidad con sistemas de versiones anteriores

Autenticación	Clientes Soportados
LANMan	Todos
NTLM	NT+ SP3, Windows 2000
NTLMv2	NT + SP4 y Windows 2000
Kerberos	Windows 2000

Existen utilidades y parches (DSClient) que permiten a versiones más antiguas de Windows 2000 utilizar tipos de autentificación específicos, sin embargo si un cliente no puede usarlos Windows 2000 asume el tipo de autenficación necesaria para ello.

¿Pero cómo se obtiene el hash LM?

Ya hemos dicho que el verdadero hash y por supuesto la contraseña no viajan por el cable de conexión, pero sí la respuesta al desafío, y de ahí vienen los problemas, el algoritmo LM divide en dos grupos el hash del usuario, en bloques de 8 bytes.

Primeros 8 Bytes	Segundos 8 Bytes

Los primeros 8 Bytes guardan los 7 primeros caracteres de la contraseña haseada
Los segundos 8 Bytes guardan los caracteres 8 y sucesivos de la contraseña

Por ese motivo es igual de seguro o de inseguro utilizar contraseñas de 7 u 8 caracteres

Una vez obtenidos los hashes, bastará con probar por fuerza bruta todas las combinaciones posibles e ir comparando y aplicando la función hash en el equipo local hasta encontrar uno que cumpla el resultado, en ese momento ya tendremos el hash verdadero y por pura combinación la contraseña.

El tiempo que esto puede tardar varía dependiendo de la longitud de la contraseña y de su complejidad, pero con un ordenador “modernito” probar todas las combinaciones numeros-letras, por ejemplo, para una contraseña de 7 caracteres puede ser una labor de pocos minutos, a lo peor de un par de horas.

Para evitar esto, se creó NTLMv2 que es bastante más robusto, pero que también ha sido descubierto el método de craquearlo, sólo nos queda Kerberos, bastante más difícil de desencriptar y muchísimo más seguro, aunque ya circulan vulnerabilidades, no veremos ninguna, pero siempre te queda google.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

Envenenamiento ARP

Medios Conmutados y Medios Compartidos

También se ha posteado en ocasiones anteriores e incluso **LorD_d4Rk355** puso un excelente link de lo que es un sniffer, y sus fechorías, no se te olvides descargarlo y leerlo, no obstante aclararemos:

Muchas redes locales son configuradas compartiendo un mismo segmento de red Ethernet (HUB's), en este tipo de redes todas las tarjetas de red reciben todos los paquetes de datos y descartan las que no son para ellas, de otra forma, en una LAN compartida los paquetes de datos se envían por toda la red sin importar si la información debe ser entregada a esa máquina o a otra, cuando se recibe la información la tarjeta la descarta o no dependiendo si va dirigida a ella.

Para que un sniffer tenga éxito hay que obligar a la tarjeta de red que acepte toda la información y que "registre" los paquetes transmitidos ya sean para esa máquina o no, esto es lo que se conoce como poner la tarjeta de red en modo promiscuo

Los medios conmutados (switches) son más seguros al snifado, teóricamente los datos no son retransmitidos por toda la red y sólo viajan de/hacia las máquinas que se comunican, es decir, el resto de tarjetas "no se enteran" de la conversación aunque formen parte del mismo segmento de red.

Por suerte o por desgracia, existen "otros métodos" para espiar en redes conmutadas, el principio básicamente es el mismo, se trata de poner la tarjeta de red en modo promiscuo, analizar el protocolo y descifrar la información, a "esos métodos" se les suele denominar envenenamiento ARP

Analizando el tráfico de la Red

Como estarás pensando, capturar todo el tráfico de una red puede ser una tarea tediosa, larga y con demasiada información, por ello, los sniffers actúan monitorizando el flujo de comunicación entre las maquinas de la red para descubrir cuando alguien utiliza los servicios de la red mencionada anteriormente.

Cada uno de estos servicios utiliza un protocolo que define como una sesión se establece, como se identifica y autentifica una cuenta y de como los servicios son utilizados.

Los dos párrafos anteriores quieren decir que podemos filtrar el tráfico de datos en nuestra red indicando al sniffer que escuche solamente determinados protocolos, por ejemplo podemos poner a nuestro espía a oir únicamente los protocolos que nos interesen (Filtros)

Por ejemplo, si deseamos "capturar" las contraseñas de correo (y por qué no, los correos en sí mismos) podremos un filtro al sniffer para que escuche únicamente los protocolos POP-POP3 y SMTP.

Prácticamente cualquier ordenador de esta red puede ejecutar un programa sniffer para robar las claves de los usuarios.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

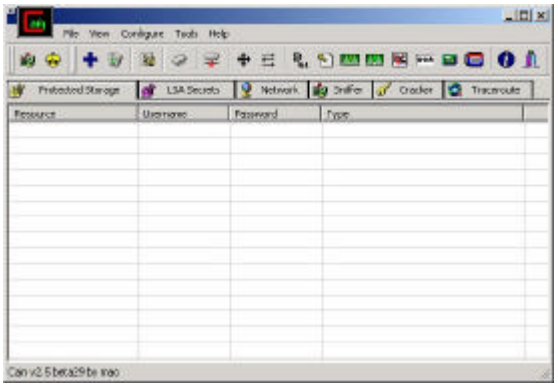
POR FIN, ¡¡¡LA PRACTICA!!!!

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.

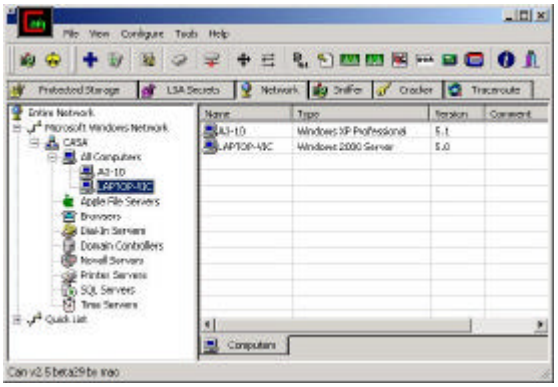
Qué es Win Pcap, pues en pocas palabras: Un driver para captura de paquetes.

Al final del documento te pondré algunos links para que consultes que es WinPcap

Al ejecutar Cain, verás esta pantalla:

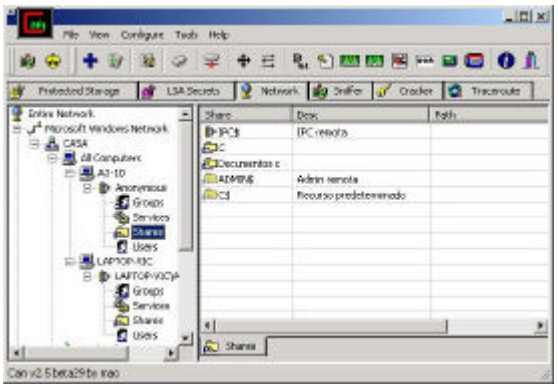


Vamos a inspeccionar nuestra red, Pinchas la ficha NetWork y expande el árbol de Microsoft NetWork....



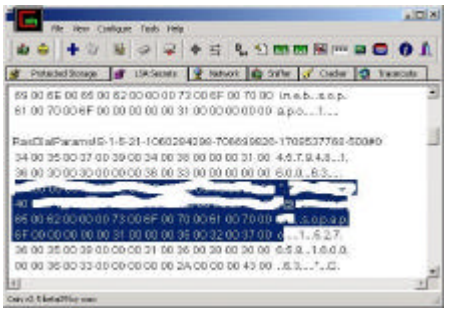
Aparecen los equipos que pertenecen al dominio o grupo de trabajo, incluso si alguno “no está” o pertenece a otro segmento de red puedes añadirlo en Quick List.

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....

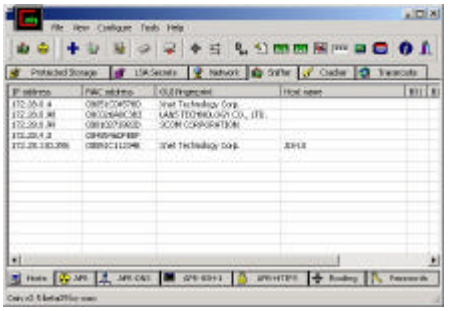
La curiosidad nos mata y es que suena bien, Secretos LSA, ¿Qué es?, al final lo sabrás, pero ahora vamos a probar algo....



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.

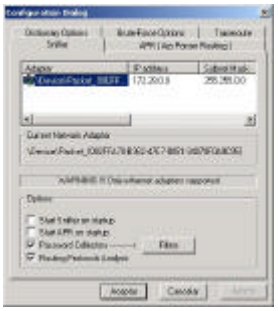
Vamos a la Ficha Sniffer,



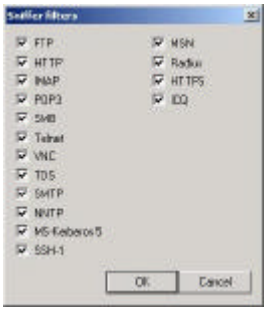
En la zona inferior de la pantalla de Cain, tenemos Host (lo que ves en la pantalla anterior), ARP,ARP-DNS.....y al final Password

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:



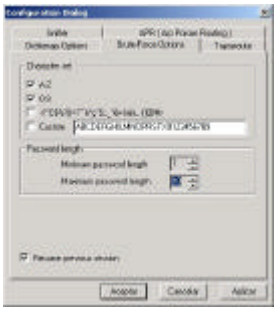
Creo que no hacen falta muchos mas comentarios, lo dejamos todo seleccionado o si queremos alguno en especial pues quitamos los que nos sobren.

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, pero eso no tiene por qué ser así, ojo, la IP envenenada no debe existir en la red, sino ya sabes....

También hubiese sido posible actuar con la IP real.

Las fichas Dictionary Options y Brute Force options, pues eso, podemos especificar el directorio en donde se encuentran los diccionarios a usar para craquear la contraseña y/o los signos, letras, números, etc. que intervendrán en el ataque por fuerza bruta (por defecto sólo letras y números) y la posible logitud de la contraseña (hasta 32), lo pondremos a 12 (que ya está bien) y los signos cada uno a su bola.



La ficha TracerRoute, nos permite resolver el nombre NetBios, consultar Whois, etc.. mejor lo probáis cuando terminemos.

Por último Aplicamos y aceptamos y volveremos a la pantalla inicial (la de la ficha Sniffer-Host)

Para poder añadir los equipos a esnifar, debemos poner en marcha el sniffer, esto podemos hacerlo de dos formas:

1º) Esnifar en un medio compartido (no necesita envenenamiento ARP)
2º) Esnifar en un medio conmutado (Envenenando ARP)

Cada uno de ellos corresponde a los iconos que hay en el extremo superior izquierdo de la pantalla de caín, en la barra de herramientas, el de la tarjeta de red verde y el amarillo/negro (como el de los residuos tóxicos o nucleares)

Si pulsamos en el icono amarillo/negro (Start/Stop ARP) se activará el otro automáticamente, si pulsamos sólo en el de la tarjeta verde no usaremos Envenenamiento ARP

Ahora es cuando viene el desahogo, Menos mal que ya expliqué lo de los Hub's y Switch....

Bueno, aunque todavía falta por explicar mas cosas del envenenamiento ARP, vamos a probar...

Pinchamos en el icono APR (el amarillo/negro) y el esniffer se pone en marcha

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

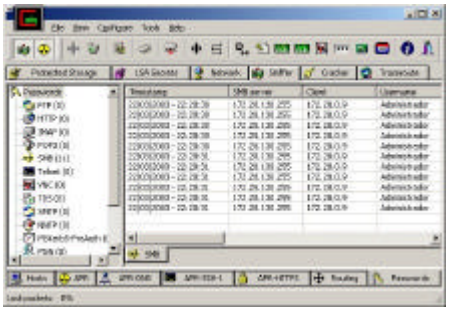
Puedo escanear todo el rango Uff, qué pesado

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

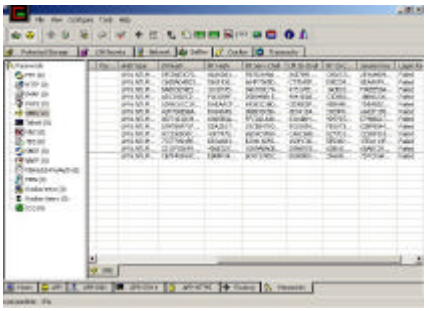
Lo de los test multicast, broadcast, etc. es largo y tendido, así que propongo que primero se esnife si test y si no escuchamos nada, pues marcamos todos los test (all test), me cuesta adivinar las distintas topologías de red que tengáis cada uno....

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:

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR



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$ (mira la FAQ I de las contraseñas)

Y cómo conseguimos eso, pues aquí es donde vuestra imaginación y práctica empiezan, (o es que os creíais 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 tio 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

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

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

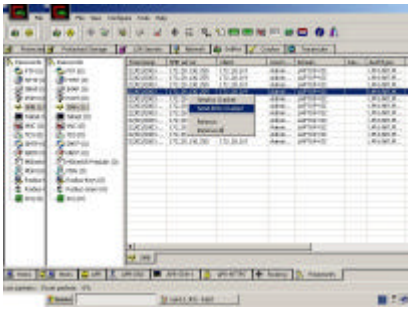
Ahora, los hashes que esnifas son los de los usuarios que se conectan, es decir, que si el administrador de la red "te visita" pero utiliza una cuenta restringida, pillarás ese hash, por eso hay una máxima en seguridad: La cuenta de administrador para Administrar.

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...



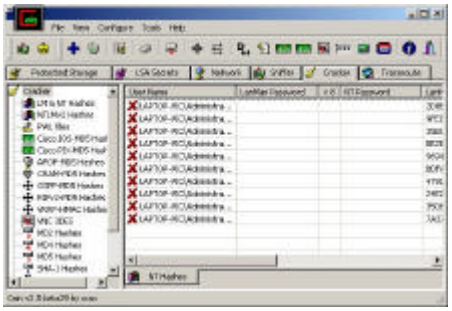
Y se pasarán todos los Hashes al craqueador, para que no tarde mucho yo he puesto una contraseña muy simple (kaka)

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 o paseamos por el Foro de HxC 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)

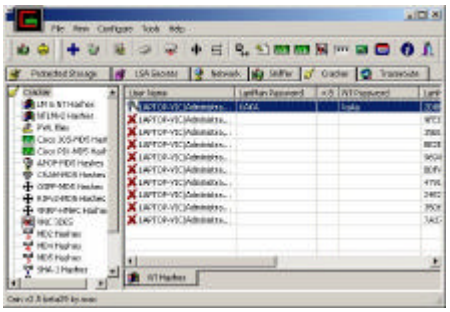


Seleccionamos cualquiera de esas entradas, mejor la que ponga Administrador como nombre de usuario, que a mi solo me aparecen esas...

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.

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR

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



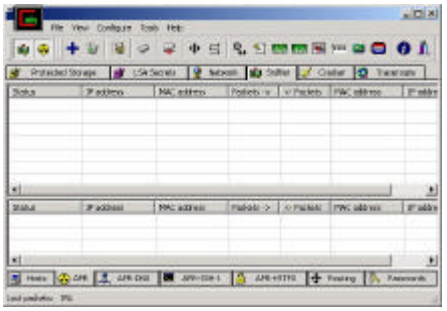
Como verás se muestran las contraseñas reveladas LANMan y NTPassword, es la misma una en mayúsculas y otra en minúsculas, como ya sabemos que se trata de un W2K debemos usar la de las minúsculas,.

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

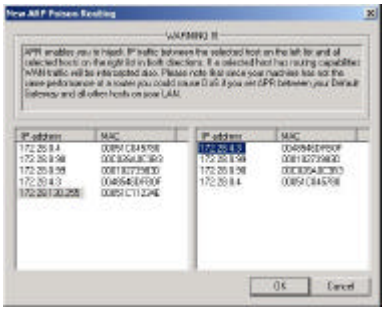
FIN DE LA PARTIDA.

Si queréis "trastear" algo más, os cuento, es posible "escuchar" el tráfico de autentificación 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



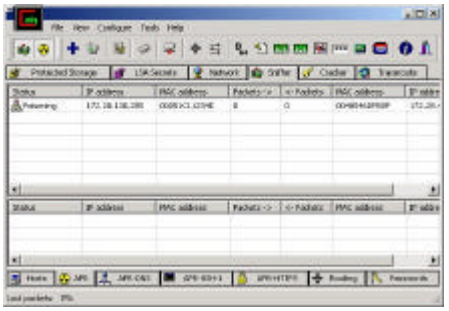
Pulsamos en el signo + que hay en azul en la barra de herramientas



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

FAQ CONSEGUIR LA CONTRASEÑA DEL ADMINISTRADOR



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..

ESPERO QUE OS GUSTE, y perdonad por las faltas de ortografía

LINKS RECOMENDADOS

FAQ 1 A por la contraseña de Windows 2k (posteado por **Vic_Thor**)

www.hackxcrack.com/phpBB2/viewtopic.php?t=3856

FAQ de la SAM (posteado por **Nikkyta**)

www.hackxcrack.com/phpBB2/viewtopic.php?t=2987

Sniffers Espías en la Red (posteado **por LorD_d4Rk355**)

www.hackxcrack.com/phpBB2/viewtopic.php?t=3410&highlight=espias

WinPcap

http://winpcap.polito.it/install/default.htm#Developer

Cain & Abel (Oxid)

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