# El NMAP

# Herramienta de exploracion de red y escaner de seguridad.

SINOPSIS nmap [Tipos(s)de escaneo] [Opciones] <servidor o red>

Nmap ha sido disenado para permitir a administradores desistemas y gente curiosa en general el escaneo de grandesredes para determinar que servidores se encuentran activosy que servicios ofrecen. nmap es compatible con un grannumero de tecnicas de escaneo como: UDP, TCP connect (),TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYNsweep, and Null scan. Vease la seccion Tipos de Escaneopara mas detalles. nmap proporciona tambien caracteristi-cas avanzadas como la deteccion remota del sistema operativo por medio de huellas TCP/IP , escaneo tipo stealth(oculto), retraso dinamico y calculos de retransmision,escaneo paralelo, deteccion de servidores inactivos pormedio de pings paralelos, escaneo con senuelos, deteccionde filtrado de puertos, escaneo por fragmentacion yespecificacion flexible de destino y puerto.Se han hecho grandes esfuerzos encaminados a proporcionarun rendimiento decente para usuarios normales (no root).Por desgracia, muchos de los interfaces criticos del ker-nel ( tales como los raw sockets) requieren privilegios deroot. Deberia ejecutarse nmap como root siempre que seaposible.

OPCIONES

En general, pueden combinarse aquellas opciones que tengansentido en conjunto. Algunas de ellas son especificaspara ciertos modos de escaneo. nmap trata de detectar yadvertir al usuario sobre el uso de combinaciones deopciones sicoticas o no permitidas.


Tambien puede ejecutar el comando nmap -h para una paginade referencia rapida con un listado de todas las opciones.Tipos de Escaneo-sT Escaneo TCP connect(): Es la forma mas basica deescaneo TCP. La llamada de sistema connect() pro-porcionada por nuestro sistema operativo se usapara establecer una conexion con todos los puertosinteresantes de la maquina. Si el puerto esta a laescucha, connect() tendra exito, de otro modo, elpuerto resulta inalcanzable. Una ventaja importantede esta tecnica es que no resulta necesario tenerprivilegios especiales.

Cualquier usuario en lamayoria de los sistemas UNIX tiene permiso parausar esta llamada.Este tipo de escaneo resulta facilmente detectabledado que los registros del servidor de destinomuestran un monton de conexiones y mensajes deerror paraaquellos servicios que accept() (acep-tan) la conexion para luego cerrarla inmediata-mente.-sS Escaneo TCP SYN: A menudo se denomina a estatecnica escaneo "half open" (medio abierto), porqueno se abre una conexion TCP completa. Se envia unpaquete SYN, como si se fuese a abrir una conexionreal y se espera que llegue una respuesta. UnSYN|ACK indica que el puerto esta a la escucha. UnRST es indicativo de que el

puerto no esta a laescucha.

Si se recibe un SYN_ACK, se envia un RST inmediatamente para cortar la conexion (en realidades el kernel de nuestro sistema operativo el quehace esto por nosotros). La ventaja principal deesta tecnica de escaneo es que sera registrada pormuchos menos servidores que la anterior. Por desgracia se necesitan privilegios de root para con-struir estos paquetes SYN modificados.
-sF -sX -sNModos Stealth FIN, Xmas Tree o Nul scan: A veces nisiquiera el escaneo SYN resulta lo suficientementeclandestino. Algunas firewalls y filtros de paque-tes vigilan el envio de paquetes SYN a puertosrestringidos, y programas disponibles como Synlog-ger y Courtney detectan este tipo de escaneo. Estostipos de escaneo avanzado, sin embargo, puedencruzar estas barreras sin ser detectados.La idea es que se requiere que los puertos cerradosrespondan a nuestro paquete de prueba con un RST,mientras que los puertos abiertos deben ignorar lospaquetes en cuestion (vease RFC 794 pp 64). Elescaneo FIN utiliza un paquete FIN vacio (sorpresa)como prueba, mientras que el escaneo Xmas treeactiva las flags FIN, URG y PUSH. El escaneo NULL desactiva todas las flags.

Por desgracia Microsoft(como de costumbre) decidio ignorar el estandarcompletamente y hacer las cosas a su manera. Debidoa esto, este tipo de escaneo no funcionara con sis-temas basados en Windows95/NT. En el lado positivo,esta es una buena manera de distinguir entre lasdos plataformas. Si el escaneo encuentra puertos cerrados, probablemente se trate de una maquinaUNIX, mientras que todos los puertos abiertos es indicativo de Windows. Excepcionalmente, Cisco,BSDI, HP/UX, MVS, y IRIX tambien envian RSTs en vezde desechar el paquete.

-sPEscaneo ping:

A veces unicamente se necesita saberque servidores en una red se encuentran activos.Nmap puede hacer esto enviando peticiones derespuesta ICMP a cada direccion IP de la red que seespecifica. Aquellos servidores que responden seencuentran activos. Desafortunadamente, algunossitios web como microsoft.com bloquean este tipo depaquetes. Nmap puede enviar tambien un paquete TCPack al puerto 80 (por defecto). Si se obtiene porrespuesta un RST, esa maquina esta activa. Una ter-cera tecnica implica el envio de un paquete SYN yla espera de de un RST o un SYN/ACK.

Para usuariosno root se usa un metodo connect().Por defecto (para usuarios no root), nmap usa lastecnicas ICMP y ACK en paralelo. Se puede cambiarla opcion -p descrita mas adelante.

Notese que el envio de pings se realiza por defectode todas maneras y que solamente se escanean aquel-los servidores de los que se obtiene respuesta. Usee sta opcion solamente en el caso de que desee unping sweep (barrido ping) sin hacer ningun tipo deescaneo de puertos.-sU Escaneo Udp: Este metodo se usa para saber quepuertos UDP (Protocolo de Datagrama de Usuario, RFC768) estan abiertos en un servidor.
La tecnica con-siste en enviar paquetes UCP de 0 bytes a cada puerto de la maquina objetivo. Si se recibe un men-saje ICMP de puerto no alcanzable, entonces elpuerto esta cerrado. De lo contrario, asumimos queesta abierto.Alguna gente piensa que el escaneo UDP no tienesentido. Normalmente les recuerdo el reciente agu-jero Solaris rcpbind. Puede encontrarse a rcp bin descondido en un puerto UDP no documentado en algunlugar por encima del 32770. Por lo tanto, noimporta que el 111 este bloqueado por la firewall.Pero, quien puede decir en cual de los mas de30000 puertos altos se encuentra a la escucha elprograma? iCon un escaner UDP se puede! Tenemostambien el programa de puerta trasera cDc Back Ori-fice que se oculta en un puerto UDP configurable en las maquinas Windows, por no mencionar los muchosservicios frecuentemente vulnerables que usan UDPcomo snmp, tftp, NFS, etc.Por desgracia, el escaneo UDP resulta a vecestremendamente lento.

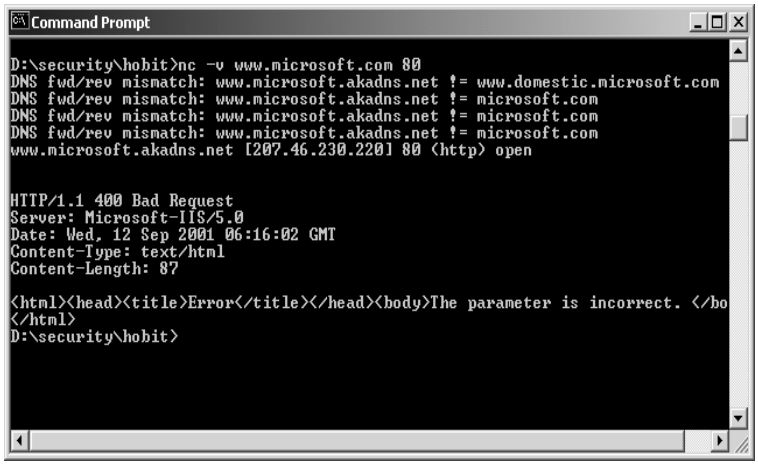
Tomado de Internet...

# El NETCAT “NC”

Sacandole Provecho a una exelente Utilidad.por: Kliber.Netcat es un pequeño programa creado para uso de losadministradores de redes (y por supuesto para los Hackers) :), esteproggie fué creado originalmente por Hobbit y porteado a Win95 y NT porWeld Pond de L0pht , tiene mas de un año desde que fué Liberado y muypoco se ha escrito sobre este Programita; Principalmente porque la estructurade sus comandos es poco familiar para el usuario medio. Netcat tiene infinidad de funciones, aunque se deja que sea el usuario quien las averigue :P, y en el archivo de ayuda ponen algunos ejemplitos muy elementales solamente...La especialidad de NetCat es el Protocolo tcp/ip, y le dá a lamáquina de windows, cierto poder sobre este protocolo que solo teníaUNIX, trabaja con lineas de comandos desde MS-DOS (o desde el Shell de Linux), y según parece, puede hacer casi cualquier cosa sobre TCP/IP. El comando principal es nc con su respectiva variable u opción al mas puro estilio Unix.Cabe destacar que la información sobre Netcat y sus usosespecificos es bastante limitada; aunque Hobbit en su documento aclara muchas cosas, cita algunos ejemplos y dice que NetCat puede ser utilizado para mas de 1001 vainas... Netcat puedeser encontrado en:

http://www.atstake.com/research/tools/ en WinX "actualizado!"

Este es el resultado de el comando de ayuda de netcat en una máquina windows




c:>nc -h
para conectrase:
**nc [-opcion] nombre_pc puerto[s] [puertos]**
c:\nc -h 192.168.0.1 21

para escuchar:
**nc -l -p port [options] [hostname] [port]**
c:\nc -l -p 21

-d (Modo Stealth o encubierto) Esta opción desvincula al Programa de la consola, haciendolo trabajar en el BackGround.

-e <prog> (Ejecuta un programa cuando se conecta) Puede ser utilizado para ejecutar incluso un Shell tanto en WinX como en *NIX.-l (Escuchando conecciones)

-l Deja a un puerto abierto en espera de una conección

-L (lo mismo queanteriormente pero sigue escuchando aún cuando laconección es cerrada Esta opción es incluida en la versión de Weld Pond de L0pth, y es muy util para seguir escuchando en el puerto, a diferencia de:
-l (que la conección cerrada termina con el proceso de nc) esta opción
-L permite seguir escuchando en el mismo puerto (la rutina de nc -l es reiniciada).

-n (Dirección numerica especifica; no hace un DNS Lookup) Netcat tiene lafacultad de resolver nombres de dominio mediante un DNS Lookup, con esta opción le especificamos que no lo haga, y use solamente direcciones IP.

-o<logfile> (obtiene un archivo log en Hex de la acción) Genera un Log de las actividades de netcat en código Hexadecimal.

-p<puerto> (Puerto para pegarse) Algunas veces debes especificarle con estaopción el puerto a realizar una acción.

-s<ip addr> (pegarse a un IP especifico) Netcat puede utilizar IP de una redcomo fuente local.

-t (Funciona como un pequeño demonio telnet) Con esta opción le especificasa netcat que debe realizar negociaciones telnet.

-u specify UDP (Utilizar Protocolo UDP) Con esta opción le dices a netcat quetrabaje con protocolo UDP en vez de TCP.

-v (modo verbose, mas información, se le puede añadir otra -v para masinfo todavia) Bastante util y necesario, sobre todo para estudiar demonios en profundidad y observar todos los detalles en un Sniffing.

-w <segundos> (Especifica un tiempo para terminar) Con esta opción le especificas un tiempo determinado para realizar conecciones .

-r (Genera un Patron Ramdom de puertos locales o remotos) Muy util para evitarpatrones lógicos de Scanning.

-g <gateway> (especificar Gateways) Una de las opciones más interesantes de netcat, permite utilizar Routers como "puentes" de conección.

-G <numero> (Especificar puntos de Routing), Con esta opción podemos crear una cadenaaleatoria de hosts para crear un ruta perdida para tus paquetes (Spoofing).

-i <segundos> Especifica un intervalo de segundos entre puertos Scaneados.

Extraido de Internet

# SATAN

## (herramienta del administrador de la seguridad para analizar redes)

SATAN fue hecho por la razon que los sistemas informáticos están llegando a ser más y más dependientes en la red, y en igual forma a ser más y más vulnerable al ataque por vía de esa misma red.

SATAN es una herramienta para los administradores de sistemas. Reconoce varios problemas establecimiento de una red-relacionados comunes de la seguridad, y divulga los problemas sin realmente explotarlos.

Para cada tipo o problema encontrado, las ofertas Satan da una respuesta en particular que explica el problema y qué podría ser de impacto. El resultado particular también explica qué se puede hacer sobre el problema: corrija un error en un archivo de la configuración, instale un bugfix del vendedor, utilice otros medios de restringir el acceso, o inhabilite simplemente el servicio.

SATAN recoge la información que está disponible para cada uno encendido con el acceso a la red. Con un cortafuego apropiado-configurado en lugar, ésa debe ser información cercana-cero para los forasteros.

Hemos hecho una cierta investigación limitada con SATAN.con SATAN encontrarán inevitables problemas. Aquí está la lista actual del problema:

- Sistemas de ficheros del NFS exportados a los anfitriones arbitrarios
- Sistemas de ficheros del NFS exportados a los programas no privilegiados
- Sistemas de ficheros del NFS exportados vía el portmapper
- Acceso del archivo de la contraseña del NIS de los anfitriones arbitrarios
- Viejas (es decir antes de 8,6,10) versiones del sendmail
- Acceso de REXD de los anfitriones arbitrarios
- El control de acceso del servidor X inhabilitó
- archivos arbitrarios accesibles vía TFTP
- acceso alejado de la cáscara de los anfitriones arbitrarios
- directorio casero del Anonymous FTP escribible

Éstos son problemas bien conocidos. Han sido tema del CERT, CIAC, u otros advisories, o se describen extensivamente en manuales prácticos de la seguridad. Los problemas han sido explotados por la comunidad del intruso durante mucho tiempo.

Se hizo que SATAN sea una espada de doble filo como muchas herramientas, puede ser utilizado para los propósitos buenos y para malvados. También puede hacer que los intrusos (wannabees y Newbie's incluyendo) tengan herramientas mucho más capaces (de intrusion) ofrecidas por SATAN.

Extraido de Internet

# El AccessDiver (AD)

Es probablemente el programa mas usado por la mayoría de los crackers. Para ingresar a un sitio basa su actuación en la "fuerza bruta"; es decir, bajo el principio de probar diferentes combinaciones de usuarios (user) y claves (password) hasta que encuentra alguna que el sitio acepta como válida. Esta acción la realiza en forma automática y a una velocidad que manualmente nunca lograríamos.

Es un programa muy versátil que posee varias opciones de configuración, de manejo de proxy, generación y administrador de wordlist, tipos de ataques, automatismos, historial, etc.
La versión mas actualizada del AccessDiver puede descargarse del sitio oficial: http://www.accessdiver.com/downloads.htm.
En los apartados que siguen a continuación se indica como configurar el AD versión 4.84 para dejarlo en condiciones de iniciar un ataque. Esta es una configuración básica que sirve en la mayoría de los casos y tiene como propósito ilustrar acerca de su utilización. Dependiendo de la velocidad de conexión a Internet que se tenga, del sitio que se desea ingresar o de otros factores, será necesario realizar los ajustes que correspondan.

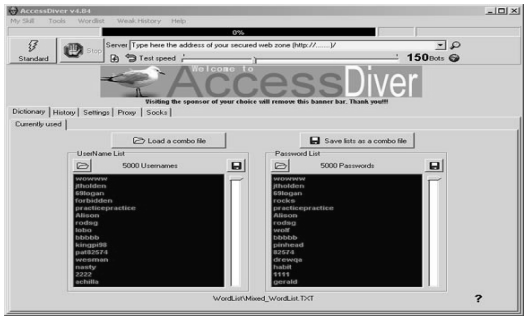
**PROXYS Y WORDLISTS**

Al AccessDiver se le debe proporcionar una lista de proxys para que pueda rotarlos y una lista con las diferentes combinaciones de palabras que se usarán como claves de acceso. El éxito o fracazo de un ataque dependerá en gran medida de lo adecuado que sean estas dos listas.

Casi todos los sitios poseen protecciones para detectar intentos de acceso -evidentemente, no autorizados- manteniendo vigilancia acerca de las direcciones IP desde donde provienen los ingresos de User/Pass. Típicamente admiten hasta tres intentos consecutivos antes de bloquear una IP.

De lo anterior se deduce la importancia de contar con una lista de proxys, que aparte de otorgarnos anonimato, al rotarlos con el AccessDiver nos permitirá realizar muchísimas pruebas de combinaciones de User/Pass, haciendo creer al servidor del sitio que las solicitudes de ingreso provienen de diferentes orígenes (diferentes IP) sin que nos bloquee.

La lista de proxys tiene que estar en el formato siguiente:
PROXY_HOST:PROXY_PORT
Por ejemplo:
15.35.135.52:8080
Las wordlist son simplemente combinaciones de user/passwords que se agrupan en un archivo. El formato es:
username:password
Por ejemplo:
wnwz:isgo




Extraido de Internet

# L0phtCrack

## 1.- Introducción :

L0phtcrack es una herramienta cuya finalidad es conseguir descifrar contraseñas de Windows NT. Después de varias versiones la herramienta ha quedado bastante bien, y seguro que concido en el gusto de muchas personas al decir que es el mejor crackeador de passwords NT para Windows.

Esta herramienta básicamente tiene tres funciones:

1.- Extraer / importar ficheros SAM.

2.- Capturar / Sniffar paquetes de autentificaron SMB ( contraseña cifrada ).

3.- Crackear *hashes* NT (Contraseñas).

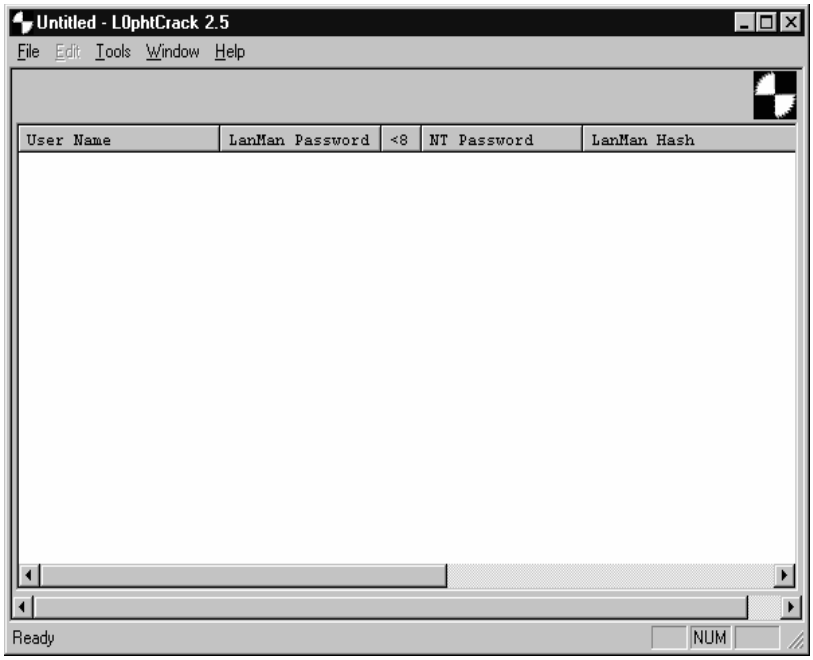
## 2.- Instalando la aplicación:

Como creo que es bastante trivial solo decir que como cualquier aplicación Windows, dar al enter un par de veces y ya está.

Si no sabéis de donde sacar el L0phtcrack. pues muy fácil de www.l0pht.com

## 3.- Toma de contacto con L0phtCrack.

Este es el aspecto que tiene el l0pht cuando se abre



**Menús:**

| **File** | |
|---|---|
| Open password file. | Abre una sesión guardada de crackeo (*.lc) |
| Open wordlist file. | Seleccionamos el diccionario a utilizar |
| | |
| Import SAM file. | Importar un fichero .SAM. |
| | |
| Save | Para Guardar la sesión actual |
| Save As. | Guardar como. |
| | |
| Exit | Salir |

| **Tools** | |
|---|---|
| Dump Passwords from the registry | Coger las pass de nuestra SAM local *. |
| SMB Packet Capture | Se activa el modo sniffer. |
| Run Crack | Comienza a crackear. |
| Stop Crack | Detiene el crackeo |
| | |
| Options | Opciones para crackear. Ver sección. |

| **Window** | |
|---|---|
| Minimize to tray | Deja la aplicación sólo con su proceso así: |
| | |
| Hide Ctrl+Alt +L to show | Deja la aplicación funcionado exclusivamente como proceso y oculta. Solo se puede ver con el administrador de tareas o dando a ctrl+alt+l. |

**Importando ficheros SAM.**

Vamos a empezar por las caracteríscas mas sencillas de l0pht, que es importar y volcar ficheros SAM.

Para conseguir los ficheros .SAM lo podemos hacer de dos formas coger un fichero SAM e importarlo; o coger el registro de nuestra máquina o una máquina remota.

1.- Localizar ficheros SAM:

%windir%\repiar\sam. -> c:\winn\repair\sam.

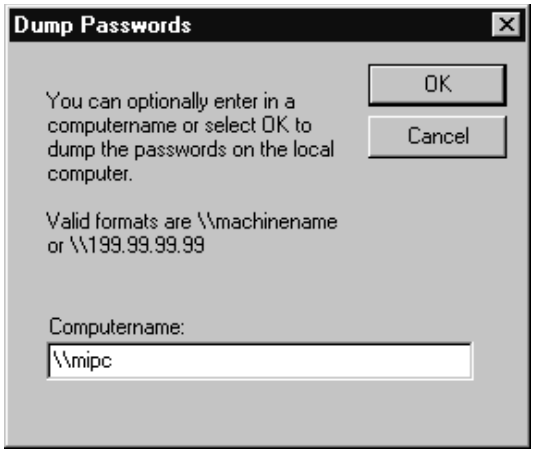
Por defecto el directorio de c:\winnt\repair\sam. Tiene permisos de lectura para el grupo : todos, pero no suele estar actualizado. ( Nota: estos ficheros los general el rdisk, disco de reparación)

%windir%\system32\config\sam. -> c:\winnt\system32\config\sam.

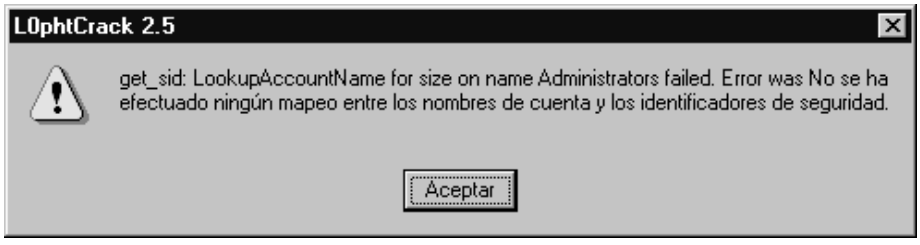
La forma más rapida de tomarlos es usando el ntfsreader (www.sysinternals.com ) o siendo administrador local y arrancando en modo msdos.

**Volcando ramas de registro:**

En el menú 'tools \ dump passwords from registry' nos aparece esta ventana para seleccionar el equipo del que volcaremos los *hashes*. Por defecto aparece el nombre la máquina local.




Si te aparece esto.




. no te vuelvas loco. Esto aparece por que se cree que somos del grupo local ADMINISTRATORS ( versión inglesa ) en vez de **ADMINISTRADORES** (versión castellano ).

Para ello l0phtcrack necesita que se cambie un valor en una cadena del registro.

Podemos hacer un fichero .reg de la siguiente forma:

```
REGEDIT4
[HKEY_CURRENT_USER\Software\L0pht\L0phtCrack]
"AdminGroupName"="Administradores"
```

Necesitaremos cerrar el l0pht y lo volvemos a abrir para que coja los cambios. Y sin duda funcionará.

**¿ Que hacer si quieremos coger el de una máquina remota ?**

Si simplemente nos conectamos nos aparecerá esto :


Lo que quiere decir que no tenemos privilegios de administración sobre esa máquina. Para ello nos chequeamos contra su pc con privilegios de administrador ( consecuentemente necesitamos la contraseña ). Por ejemplo :

C:\> net use k: \\maquina_remota\c$ /user:maquina_Remota\administrador

Luego nos pedira la contraseña y se la damos. Una vez que nos chequeamos. probamos y. funciona perfectamente.

**Menú FILE**

En cuanto al menu file no hay nada complicado:

*Open password file. :* Son los ficheros de sesión de contraseña son de extensión *.lc. En estos ficheros es donde guardamos las sesiones, por que hay veces que se debe cortar un crackeo .

*Open wordlist file . :*Los ficheros de word-list ( lista de palabras) cualquier fichero de tipo texto con nuestras palabras. Seleccionar uno.

*Import sam file :* Seleccionar un fichero SAM a importar para trabajar con él.

Nota : Si importamos el fichero del directorio '*repair*', esta comprimido; son los ficheros de tipo '*sam._'* no es necesario descomprimirlo en maquinas NT. Sin embargo si trabajamos con Windows 9x tendremos que usar :

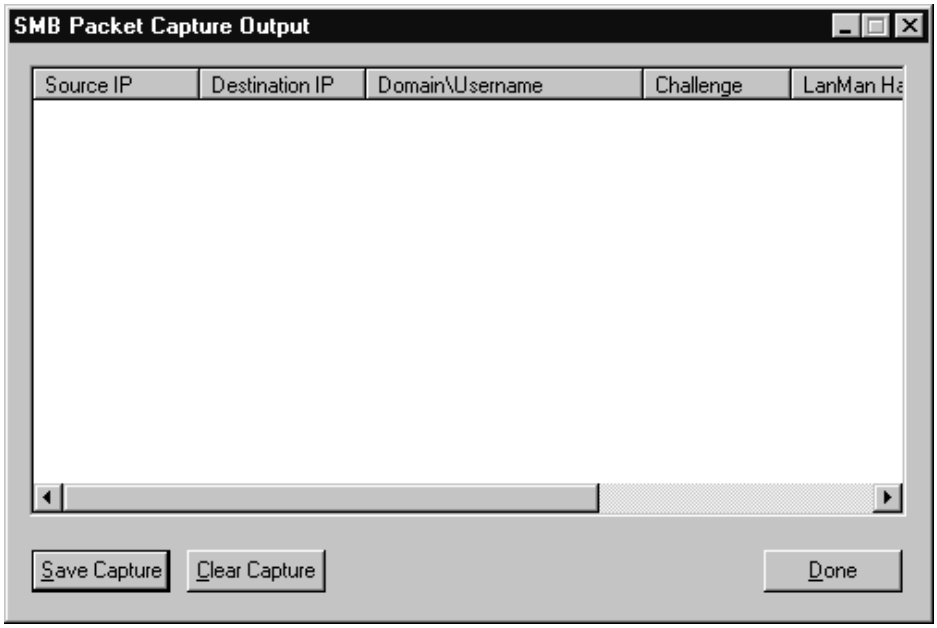
C:\>expand sam._ sam.

**Capturando paquetes :**

La captura de paquetes de autentificación se realiza con el '*SMB packet capture',* es un pequeño módulo que pone la tarjeta de red ethernet en modo promiscuo para capturar paquetes. Recordar que

es necesario ser administrador para poder poner el sniffer, por lo menos la primera vez. Si tenemos instalados otros capturadores de paquetes puede dar problemas, así que es mejor eliminarlos ( asmodeus y ISS packet capture ).

Este es el aspecto de la ventana de capturación de paquetes :



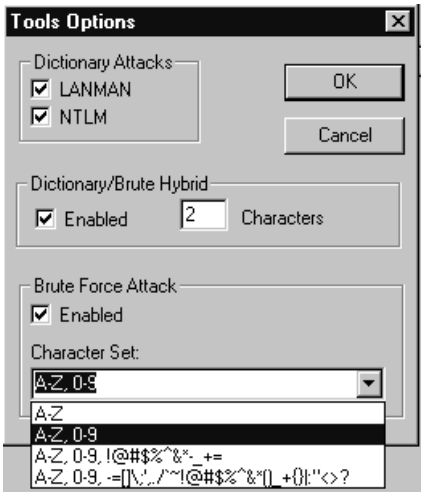

Nos aprece esta ventana en la cual irán apareciendo los paquetes capturados, con información de la ip de origen, ip de destino, nombre de usuario/dominio y los hashes. Podemos grabar y comenzar a crackear o eliminar la captura.

Lo mejor de esto es que se puede estar crackeando y capturando paquetes a la vez.

## Crackeando

Este es el menú (tools \ config ) de crackeo, para elegir de que forma vamos a crackear.

Además se realiza una secuencia de modos de crackeo si no se consigue encontrar la contraseña, se continua con cada de crackeo a cual más lento.




- Ataque por diccionario o lista de palabras:

Los ataques de diccionario atacan directamente al sistema de encriptado LANMAN y NTLM. Para eso necesitamos que esté seleccionado un fichero de diccionario

- Ataque Híbrido:

Mezcla los valores de la lista de palabras con valores que se posponen al final de la palabra. Esta opción coloca caracteres numéricos y alfanuméricos al final de cada palabra; por defecto son 2. Un ejemplo de esto es : juanjo21. Si tenemos una palabra en nuestro diccionario con *juanjo*, el mismo coloca valores de tipo :

juanjo11

juanjo12

juanjo1a

...

juanjo21

- Ataque de fuerza bruta:

Es el ataque clásico, incremental, podemos seleccionar el rango de valores, aunque es mejor seleccionar los valores que ya vienen en la lista, ya que por experiencia propia no funciona bien si introducimos nosostros los rangos manualmente.

Los tiempos según la documentación son de : 24-72 horas con Pentium II/450 a Pentium 166, para un crackeo completo por fuerza bruta de tipo a-z,0-9.

Hay que tener una máquina potente y tiempo, sobre todo mucho tiempo.

Si se quiere practicar, se incluyen algunas capturas, un diccionario y alguna cosa mas.

Extraido de el hacker.net

Esta guia esta extraida en su totalidad desde Internet, Fue tomada desde diferentes paginas y foros, esta informacion ha sido recolectada por mi para fines educativos.

por: BlackShadow

Salu2s!