

Práctica 43. Una de Servicios....Marchando!!!! (Por HxC Mods-Adm)

Antes de nada, se debe aclarar algo importante!!

Una cosa es un **servicio** y otra es un **proceso**.

Sin entrar en tecnicismos, algo muy simple que entenderéis a la perfección:

Pongamos un programa cuyo nombre de archivo es *ntsvrc.exe* (este nombre se repite a lo largo de todo éste documento, sirve como ejemplo, es un *back-door* de verdad, pero con otro nombre)

Cuando se ejecuta el programa se verá un proceso con el mismo nombre (*ntsvcr.exe*, en nuestro caso) pero eso no quiere decir que esté instalado como servicio y si lo estuviese, podría tener un nombre diferente como servicio, por ejemplo, el programa se llama *ntsvrc.exe* y el servicio podría ser *Servicio de Proteccion de Archivos de Windows*, incluso podremos tener nombres diferentes para los procesos, los servicios y los archivos que los ejecutan, veamos el ejemplo:

Proceso en ejecución: *ntsvcr.exe*
Archivo físico: *msntfs.exe*
Servicio: *Servicio de Proteccion de Archivos de Windows*

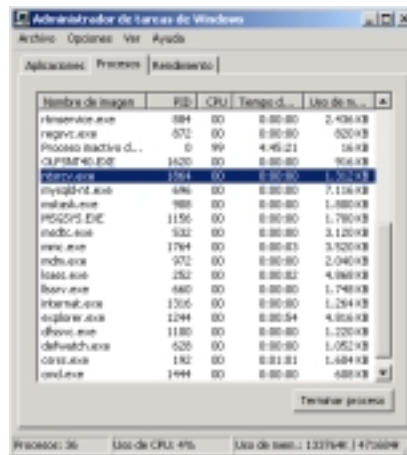
El engaño está servido, también es importante conocer qué otros procesos-servicios están en ejecución, sus nombres y descripciones, no vaya a ser el nuestro el único en español, o en inglés, vamos que hay que jugar con el objetivo e intentar “*despistar*” porque ocultar totalmente el servicio es difícil.

Por ejemplo, si en nuestro destino se ejecutan servicios con nombres en inglés (o si éstos son mayoría) pues podemos llamarlo como *Windows Protect File System* o similar.

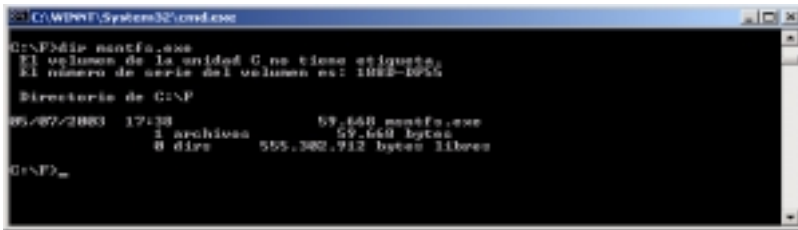
La forma de listar procesos, servicios, etc. Las veremos más adelante, tiempo al tiempo.

Antes de comenzar veamos unas pantallas de cómo quedará todo,

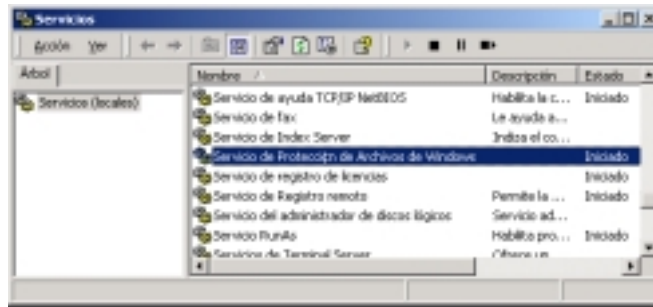
CTRL.-ALT-SUPR y pinchamos en procesos....



La siguiente pantalla sin comentarios....



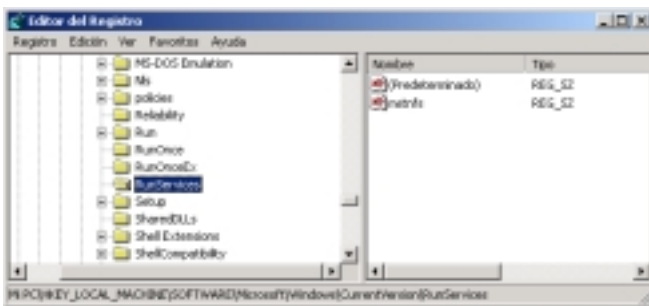
Inicio-Configuración-Panel de control-servicios



nombres diferentes para una misma cosa... un nombre, un servicio y un proceso, todo listo....

Todavía queda algo más.... el Registro

Inicio-Ejecutar: regedit



Hombre, alguno no sabrá nada del registro de windows..., Merecería la pena un artículo enterito, de momento nos vamos a creer que en la clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

se sitúan las aplicaciones y programas que se instalan como servicios en la máquina.

Todo lo que se ponga allí, se ejecutará como un servicio al iniciar Windows....

En nuestro caso observamos que hay una entrada de nombre *msntfs* y tipo **REG_SZ**, qué complicación, **REG_SZ** tradúcelo como un valor alfanumérico, si pulsáis dos veces con el ratón sobre el nombre *msntfs*, saldrá esto:



Entendiendo....

Mstnfs es el NOMBRE DEL SERVICIO
C:\WINNT\System32\ntsrcv.exe es LA RUTA Y EL NOMBRE DE ARCHIVO que se ejecutará

Y qué fue de lo del *Servicio de Protección de Archivos de Windows*?

Pues nada, eso es simplemente un nombre que describe MEJOR al servicio *msntfs*, por si fuera poco, se podría “documentar” más el servicio y ponerle algún texto de lo que hace o deja de hacer, vease la pantalla de servicios anterior la columna Descripción (en nuestro caso no pone nada..., ya pondremos algo si nos apetece más adelante)

Bueno, pues ya sabemos que un proceso es aquello que se está ejecutando en este preciso momento, que un servicio es algo que se ejecuta al iniciar Windows y que el nombre del archivo o aplicación es lo que hace que cualquiera de esas cosas se ejecute y no tiene por qué coincidir con nada de ello.

¿Qué nos faltaría?

Pues copiar el archivo *ntsrcv.exe* al directorio *C:\winnt\system32*, porque sino no lo encontraría nuestro servicio

Matando el tiempo... digo procesos

PULIST Y KILL

Hombre de Dios, si esto son herramientas del kit de recursos y son archi-conocidas, ¿por qué? ¿para qué?

Pues primero por que nos vendrán bien más adelante y segundo porque así daremos gusto a algunos que preguntan cómo “matar” procesos en ejecución.

Pulist.exe muestra los procesos en ejecución
Kill.exe los mata

Ej: (la salida puede ser muy larga, así que la recorté un poquito)

C:\>pulist

Process	PID	User
Idle	0	
System	8	
smss.exe	168	NT AUTHORITY\SYSTEM
csrss.exe	192	NT AUTHORITY\SYSTEM
winlogon.exe	212	NT AUTHORITY\SYSTEM
services.exe	240	NT AUTHORITY\SYSTEM
lsass.exe	252	NT AUTHORITY\SYSTEM
svchost.exe	404	NT AUTHORITY\SYSTEM
svchost.exe	452	NT AUTHORITY\SYSTEM
ntsercv.exe	976	NT AUTHORITY\SYSTEM
.....		
.....		
WINWORD.EXE	456	LAPTOP-VIC\Administrador
pulist.exe	1912	LAPTOP-VIC\Administrador

Como podéis ver por columnas se muestra el *nombre del proceso un ID y quién lo está ejecutando...*

Caramba, me llama la atención el proceso 976 (ntsercv.exe), eso es un troyanito que he instalado ahora mismo, vamos a matarlo....

```
C:\>KILL 976
process ntsercv.exe (976) - " killed
```

No pondré de nuevo el resultado de *pulist*, pero lo mató....

Adiós troyanito, adiós...

En la columna nombre veo cómo se llama, en ID un número que lo IDentifica y en user, quien lo ejecuta.

Muchos de ellos pertenecen al mismo S.O, (*NT/AuthoritySystem*) esto significa que es el mismísimo Sistema Operativo el encargado de ejecutarlo con independencia del usuario que esté logeado...

Vaale, y en remoto?

Pues **psinfo.exe** y **pskill.exe** (de sysinternals, los del **psexec...**)

Echadle un vistazo a **pslist.exe** y también a **tlist.exe**, vosotros mismos....

AppToService

Pues eso, instala una aplicación “normal” como un servicio de Windows, con la ayuda de la propia utilidad será suficiente....

AppToService v2.4a - Shareware
Copyright (C) 1996-2001 Basta Computing, Inc. All rights reserved.
Internet web site: <http://www.basta.com>

Synopsis: Runs regular applications as Windows services.

Usage: AppToService /? |
 /Install [options] "application" |
 /Remove "application" |
 /RemoveAll | /ShowAll
 /Password:xxx

Commands Description:

/? Display this screen.
/Install Install a service.
/Remove Remove a service.
/RemoveAll Remove all AppToService services.
/ShowAll Display all AppToService services with their status.
application The executable file you would like to run as a service.

MENU 1:General 2:/Install options 3:Examples 4:About

Ejemplo:

C:\>apptoservice /install ntsrv.exe

Se supone que el archivo ntsrv.exe existe en el directorio por defecto

El mayor problema de ésta utilidad es que es un tanto “cantona” pero puede servir en un apuro...

Psservice

Otra de sysinternals...

Permite parar-reiniciar-preguntar-etc sobre un servicio determinado o de todos.

Psservice query para listar los servicios en instalados

Psservice stop ntsrv para parar el servicio ntsrv

Psservice query ntsrv información del servicio en cuestión...

CMDINFO

Una bobada, o no..., dependerá de para qué...

C:\>cmdinfo

Version type	Full Version
Installation date	16 May 2003, 01:57:18
Owning Org	lap
Owner name	lap
Build number	2195
System root	C:\WINNT
OS type	Microsoft Windows 2000
Plus version	Not Available
Service Pack	Not available
Processor Type	Uniprocessor Free
Product Type	Windows 2000 Server
Source Path	E:\I386
Expiry date	Not Applicable

Y qué?

Pues si obtenemos una shell de un equipo remoto y le subimos el archivito, veremos rápidamente el directorio de instalación (systemRoot), si tiene o no service Pack instalados, la versión del Sistema, etc...

Nada, para ir conociendo a los amigos..

Otra buena y con mayor detalle es *psinfo*, lo dejo para vosotros

Problemas que nos pueden surgir hasta ahora...

P: Cuando intento matar un proceso, no me deja...

R: Puede ser que se trate de un servicio en ejecución y por eso no puede, se necesitaría detener o matar el servicio y luego el proceso...

R: Puede ocurrir que esté en ejecución por otros servicios o procesos, tendríamos que ver de quién depende y quienes son sus otros procesos-servicios que dependen de él

P: Mato un proceso y de repente vuelve a aparecer

R: En muchos casos se pueden programar servicios que ejecutan procesos que se auto-reinician, el caso más simple es IIS, está pensado para restaurarse si pasa algo... por tanto deberíamos cambiar su prioridad y/o su estado de auto-restauración.

Recomiendo que se hagan mil y una prácticas con estas herramientas, parar, suspender, iniciar, matar, listar, etc. Siempre el socorrido bloc de notas, **notepad.exe**, es uno de los candidatos a elegir, copiadlo con otro nombre, pe. **Notas.exe** y probad a instalarlo como servicio, etc...

Ni que decir tiene que muchas de éstas herramientas precisan de privilegios administrativos, probad también como simples usuarios, en algún caso encontraréis problemas, nada mejor que cometer errores y que “salgan” errores para entender todo mejor y aplicar las soluciones...

Ahora a por el Registro....

Vamos a usar *regini.exe*, *regfind.exe* y *regshell.exe*, bueno otras también....

La primera nos permitirá añadir-borrar-modificar claves del registro

La segunda verificar la existencia de claves y/o buscar en el registro

La tercera es como una shell del registro, podremos “navegar” por sus claves desde la línea de comandos, también podremos editarlas, manipularlas y/o borrarlas...

Hombre hay muchas otras, pero estas son simples, efectivas, rápidas y se pueden usar remotamente o si lo preferimos, subirlas al destino y ejecutarlas desde allí.

Voy a explicar “un poco” el registro....

En este apartado voy a tratar cómo cualquier programa, incluso virus y troyanos pueden incluirse en el **Registro de Windows** para que cuando el equipo reinicie se vuelvan a activar y así poder continuar con su capacidad de infección o lo que le corresponda, a esta operación se le conoce como “*abrir una puerta trasera*”.

La forma de tratar al **Registro** es muy diferente dependiendo de la versión del Sistema Operativo que se utilice, yo me voy a limitar a Windows 2000, aunque la mayor parte de las explicaciones sean válidas para otras versiones, es posible que existan diferencias (a veces importantes) entre unas y otras.

¿Qué es el Registro?

Y como te lo explico, ¿Definición técnica? ¿Recurrimos a explicaciones tipo Microsoft? ¿Buscamos un buen Diccionario Informático? Seguramente esta no sea la mejor definición de lo que es, pero seguro que será una de las más prácticas:

El Registro de Windows es una gran Base de Datos que guarda TODA la información de TODO lo que tienes instalado en tu PC, desde la configuración Hardware hasta los programas que tienes instalados, los perfiles de los usuarios, las propiedades de las carpetas e iconos y LOS PUERTOS en uso.

El **Registro** es una parte fundamental del Sistema Operativo, sin él Windows NO PUEDE arrancar, es igual o más importante que los propios programas que componen el Sistema Operativo.

Dada la importancia del mismo sólo los Administradores o usuarios con privilegios de Administrador puede acceder y modificar el **Registro**, luego ya tenemos otro motivo por el que los intrusos deben ganar el acceso como Administradores, sin ello no podrían modificar el registro o instalar una puerta trasera, en la práctica:

Si lees el correo y/o navegas por Internet con cuenta de Administrador, una página o correo malicioso como los aprendidos lo de los mails y html maliciosos, podrían ejecutar cualquier cosa con privilegios de Administrador y si “el bicho” intenta modificar el registro lo conseguirá sin más.

El acceso al **Registro** se puede Auditar, por tanto aquí debemos añadir otro buen hábito del Administrador, CONTROLAR LOS ACCESOS AL REGISTRO.

Cuando un programa se ejecuta, busca los parámetros de inicio en el registro (entre otros sitios), así que si “*tocamos*” en el registro algunos valores podremos modificar algunas opciones del programa que se está ejecutando, otro motivo por lo que nos interesa conocer el funcionamiento del registro: Modificar el comportamiento de un programa, desde el tipo de inicio hasta opciones ocultas que pueda disponer si es el caso.

Foro de HackXcrack

No todos los programas que se ejecutan en el PC se “registran” en el **Registro**. Por ejemplo las aplicaciones que se ejecutan desde una ventana de comandos, no suelen modificar los valores del registro para “incluirse” en el mismo como una aplicación más, este tipo de aplicaciones disponen de sus propios archivos de configuración, recuerda el Servidor FTP (Server-U) no necesitaba “instalarse”, simplemente lo ejecutábamos y punto, en lugar de usar el registro, necesitaba un archivo de configuración, recuerda....

Windows 2000 permite la administración remota del **registro**, no podremos acceder a todo pero sí a lo más importante, por tanto un intruso que llegue a convertirse en el Administrador del Sistema podrá modificar el registro de las máquinas de una Red Local como si estuviese sentado en la misma máquina.

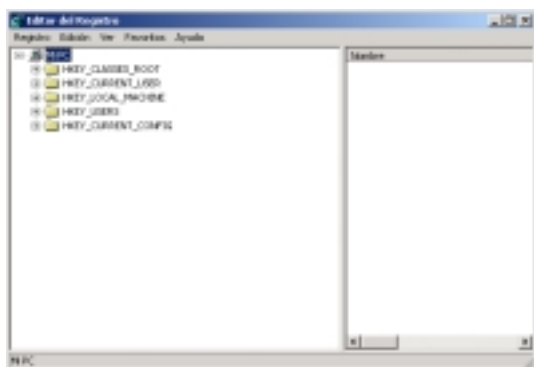
La información que contiene el **Registro** está organizada en “partes”, llamadas árboles, la siguiente tabla informa de cada uno de los *árboles del registro* y está sacada directamente de la ayuda de Windows 2000:

HKEY_LOCAL_MACHINE	Contiene información sobre el sistema del equipo local, incluyendo datos del hardware y del sistema operativo tales como el tipo de bus, la memoria del sistema, los controladores de dispositivo y datos de control de inicio.
HKEY_CLASSES_ROOT	Contiene información utilizada por diversas tecnologías de vinculación e incrustación de objetos (OLE) y de asociación archivo-clase, equivalente al Registro de Windows para MS-DOS. En HKEY_CLASSES_ROOT hay una clave o un valor determinado si existe la clave o valor correspondiente en HKEY_LOCAL_MACHINE\SOFTWARE\Classes o en HKEY_CURRENT_USER\SOFTWARE\Classes . Si hay una clave o un valor en los dos directorios, la versión HKEY_CURRENT_USER es la que aparece en HKEY_CLASSES_ROOT .
HKEY_CURRENT_USER	Contiene el perfil del usuario que ha iniciado la sesión actual de modo interactivo (no remoto) e incluye las variables de entorno, la configuración del escritorio, las conexiones de red, las impresoras y las preferencias para los programas. Este subárbol es un alias del subárbol HKEY_USERS y hace referencia a HKEY_USERS\ Id. de seguridad del usuario actual.
HKEY_USERS	Contiene información acerca de los perfiles de usuario activos cargados y del perfil predeterminado. Se incluye información que también aparece en HKEY_CURRENT_USER . Los usuarios con acceso remoto al servidor no tienen perfiles en esta clave del servidor. Sus perfiles se cargan en el Registro de sus propios equipos.
HKEY_CURRENT_CONFIG	Contiene información sobre el perfil de hardware que utiliza el equipo local al iniciarse. Esta información se usa para configurar opciones tales como los controladores de dispositivo y la resolución de pantalla que se va a utilizar. Este subárbol forma parte del subárbol HKEY_LOCAL_MACHINE y hace referencia a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current .

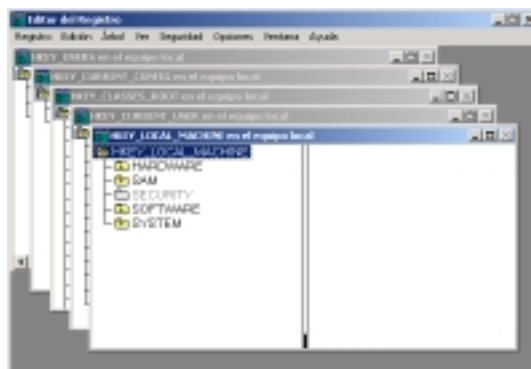
Foro de HackXcrack

Para acceder o modificar el registro en Windows 2000 puedes usar los programas que suministra el propio Sistema Operativo, estas son: Regedit y Regedt32

REGEDIT.EXE



REGEDT32.EXE



En cada árbol encontrarás claves que a su vez contienen valores que contienen datos, NO CAMBIES NADA de lo que no estés totalmente seguro del registro o puedes dejar fuera de combate al Sistema Operativo, ya llegará el momento de modificarlo. Realiza copias de seguridad del estado del sistema de forma periódica, con ello podrás entre otras cosas recuperar un registro dañado, perdido o modificado sin permiso.

Hasta ahora todo “muy bonito” y ya tenemos claro que hay que proteger al registro, pero ¿Qué “pinta” el registro y los servicios-troyanos-backdoor, etc?

Muy sencillo, la idea es que comprendas la importancia que tiene el Registro en lo que tiene que ver con la instalación de programas y la ejecución de los mismos, sobretodo lo que se refiere a la ejecución “automática” por cada vez que se inicie el Sistema.

En estos momentos me voy a ocupar de enseñarte en qué lugares deben instalarse los programas para que se ejecuten cuando Windows se inicia, mejor dicho, las claves del registro que se deben crear y dónde se deben crear para que determinados programas se ejecuten al inicio, estos son:

En las carpetas:

C:\Documents and Settings\nombre_usuario\Menú de Inicio\Programas\Inicio\programa_a_ejecutar
C:\Documents and Settings\All User\Menú de Inicio\Programas\Inicio\programa_a_ejecutar
C:\Documents and Settings\Default User\Menú de Inicio\Programas\Inicio\programa_a_ejecutar

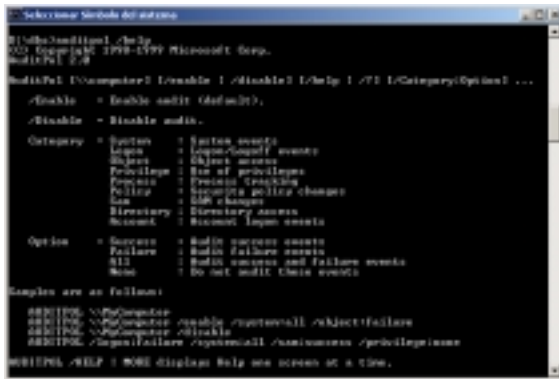
Como una tarea programada,

Configuración-Tareas Programadas

En las claves del Registro

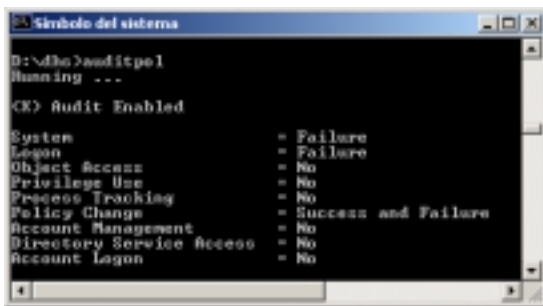
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows NT\CurrentVersion\policies\Explorer\Run
HKLM\Software\Microsoft\Windows NT\CurrentVersion\AeDebug
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKLM\System\CurrentControlSet\Services
HKEY_CLASSES_ROOT\exefile\shell\open\command

Su uso es muy simple:



Para conocer el estado de la auditoría de tu propio equipo puedes usar simplemente la sintaxis auditpol y se mostrará el estado y los objetos o categorías auditadas, cuando lleguemos al escaneo de redes encontraremos herramientas que nos permitirán conocer el estado de la auditoría sin necesidad de contar con privilegios administrativos, lo de modificar la auditoría es otro asunto.

Ejemplo:



Auditoría Activa, registros de sistema y logon activados contra accesos erróneos y auditar cambios en la política de auditoría, también activados.

¿Qué significa esto? Pues que el administrador del sistema ha activado la auditoría para el equipo local de tal forma que se registrarán los accesos con nombre de usuario y/o contraseña inválidos, así como, los cambios efectuados en la política del sistema, esto es, que si desactivamos la auditoría se registrará un suceso que así lo indica, lo cual delatará lo que ocurre con un simple vistazo al registro de sucesos.

Existen aplicaciones de seguridad que además pueden enviar una alerta (vía mail o correo interno) al administrador de ello, en tiempo real.

La buena noticia es que el Registro de Sucesos de Windows advertirá de los cambios, pero en el mejor de los casos sólo mostrará el usuario y/o el nombre Netbios de la máquina del que proviene la orden, NO LA IP.

La mala noticia es que existen aplicaciones de terceros que sí registrarán la IP remota en esas situaciones.

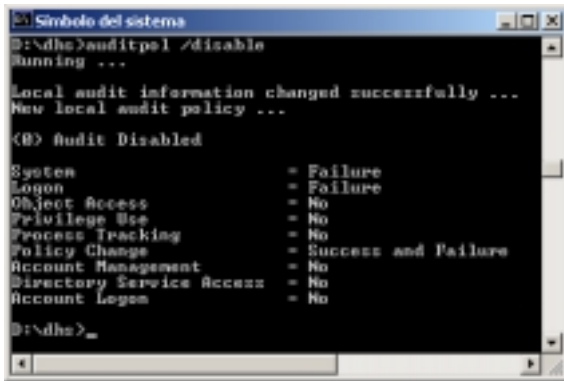
Resumiendo, aún contando con los medios y conocimientos para acceder a un equipo remoto “atravesando” su sistema de seguridad, antes hay que conocer a fondo los servicios, aplicaciones instaladas o en ejecución, mecanismos de seguridad, etc., aunque nuestras intenciones no sean las mismas que las de un ladrón al atracar un banco, podríamos decir que nadie “asalta un banco” sin haber estudiado previamente algunos puntos básicos: Cámaras de seguridad, Vigilantes, Número de empleados, horario de apertura/cierre, tránsito de clientes, “recompensa” a obtener, vías de escape, etc.

Aquellos que un buen día deciden escanear una red y “colarse” en un equipo remoto por el simple hecho

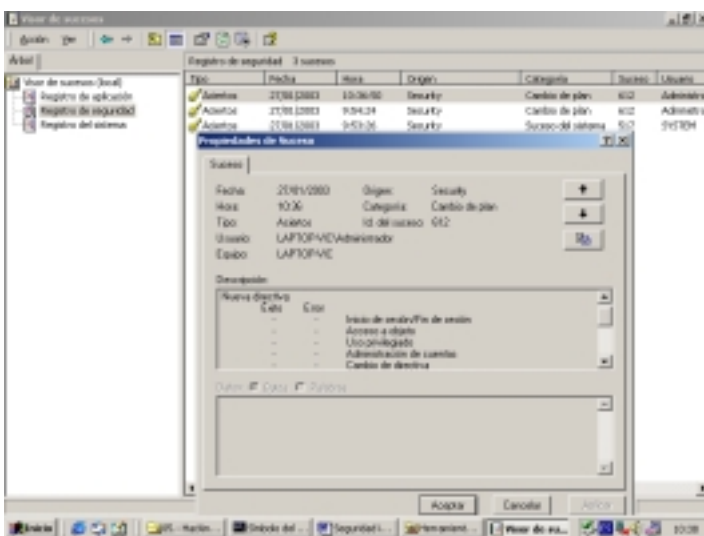
que encuentran un puerto abierto o un servicio vulnerable consiguen el rechazo general de todos, son unos lamers, que simplemente piensan que ya son dioses por conocer cómo ocultar su IP y unas cuantas herramientas, seguro que no aprenderán nada más, hasta que un día se equivoquen en el destino y los pasarán por la piedra.

En la siguiente página se muestran unas capturas de pantalla de lo que el administrador vería cuando se deshabilita la auditoría, no creo que sea necesario explicar cómo se muestra el registro de sucesos, ¿no?

Deshabilitamos la auditoría:



Visor de Sucesos:



Luego, para rizar el rizo, no estaría demás alguna utilidad que elimine los logs de sucesos, tipo rmlogs, elsave o similar....

Esto se complica, no veo la forma de terminar, así que vamos a por todas...

En lugar del archivo *serv-u.exe* lo llamaremos *mdsn32.exe*

En lugar del *.ini* que necesita el server-U, lo llamaremos *usbkeyb.dll*

Arrancando el Serv-U automáticamente

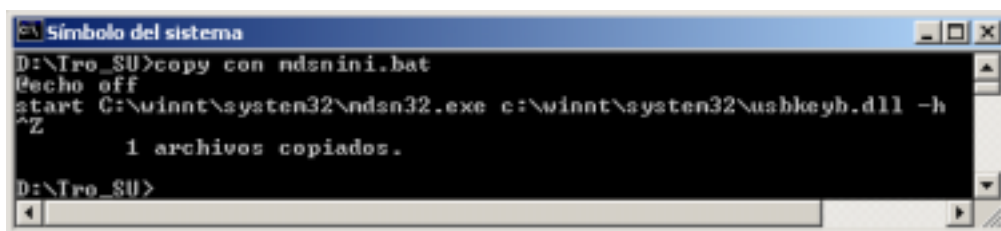
Los más espabiladillos seguro que estáis pensando (lo más probable que ya lo habréis hecho) es idear la forma para que nuestro servidor FTP, ahora llamado *mdsn32.exe* y *usbkeyb.dll*, se ejecute solito cada vez que el equipo donde lo hemos colocado se inicie, no tendrá alguna opción oculta para que se inicie como servicio...

Como no disponemos de ningún otro, mejor dicho, como no queremos usar ningún otro, vamos a ver cómo ponerle preparadito y en condiciones para que se auto ejecute.

Para ello supongamos que tenemos copiados los ficheros *mdsn32.exe* (el ejecutable) y *usbkeyb.dll* (el archivo de configuración) dentro de la carpeta `C:\winnt\system32`, ocultos o no eso no importa, para ésta práctica

Arrancando el FTP desde la carpeta de inicio:

Nos creamos un archivo *.bat* como el siguiente, por ejemplo:



* Para los que no uséis *copy con*, el signo *^Z* se consigue pulsando *F6*, corresponde al fin de archivo, *copy con* es copiar desde consola..., podéis usar el bloc de notas o el edit o lo que sea de texto claro.

Ahora lo copiamos, ¿dónde? Pues en la carpeta de Inicio de All users, es decir:

Copy mdsini.bat `C:\Documents and settings\All Users\Menu de inicio\Programas\Inicio`

De esta forma cada vez que un usuario inicie una sesión se cargará nuestro troyano....

Bueno, no es muy elegante pero efectivo, claro que bastaría que cualquier usuario accediese a ese lugar para descubrir el engaño, además fácilmente conocerá el archivo ejecutable y el de configuración, basta con que lo edite con el bloc de notas, vamos que está bien pero deja que desear.

Una opción si insistimos en éste lugar sería “convertir” el archivo *mdsini.bat* en un archivo *.com*, lo seguirá viendo igual pero al menos lo podrá visualizar en texto claro, si además le cambiamos un poco el nombre “*despistaremos un poco más*”, si se da cuenta lo eliminará de la carpeta pero los archivos que pusimos en `winnt\system32` podrían seguir, no se sabe, depende de lo experto del usuario para descubrirlos.

¿Cómo, convertir un *.bat* a *.com* o *.exe*? Sí, hay infinidad de aplicaciones que lo permiten, seguro que dispones de más de una de ellas....

Vamos a usar turbobat, haremos lo que sigue:

Nos creamos un nuevo fichero .bat como sigue:

```
Copy con prueba.bat
@echo off
C:\winnnt\system32\mdsnini.exe C:\winnnt\system32\usbkeyb.dll -h
^Z
```

recuerda que ^Z sale al pulsar la teclade función F6...

Compilamos:

```
Turbobat /B- prueba.bat
```

Renombramos y copiamos:

```
Ren prueba.com adobeldr.com
Copy adobeldr.com C:\winnnt\system32
```

Creamos un nuevo bat:

```
Copy con adobegama.bat

@echo off
start /B adobeldr.com
^Z
```

lo copiamos a la carpeta All users:

```
Copy adobegama.bat C:\Documents and settings\All Users\Menu de inicio\Programas\Inicio
```

Explicación

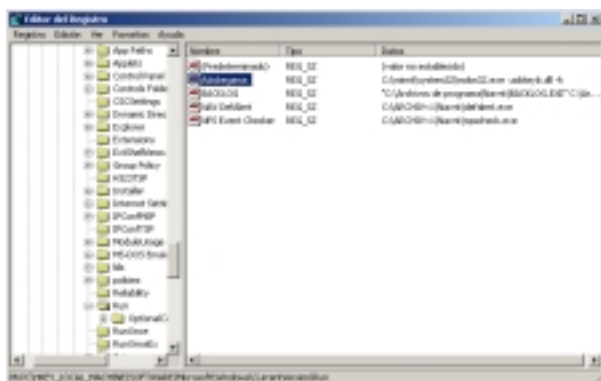
Bien, turbobat “no acepta” el comando start, si te fijas el archivo prueba.bat no incluye la instrucción start, por ello nos creamos dos archivos *.bat, siendo el ultimo (adobegama.bat) el que nos llevamos a la carpeta destino, que es el que incluye la instrucción start, la opción /B le indica a la orden start que no abra una nueva ventana de msdos, a estas alturas deberías haber empezado a investigar el mandato start, si no lo has hecho prueba a escribir start /? Desde la línea de comandos.

El usuario ahora podrá editar el archivo adobegama.bat y verá que ejecuta a su vez el archivo adobeldr.com, se descubre fácilmente como antes, pero ahora no sabe cuales son los archivos que a su vez ejecuta éste último, es decir nuestros archivos mdsn32.exe y usbkeyb.dll están algo más protegidos.

Si además hubiésemos utilizado un joinner que “uniese” el archivo adobeldr.com con, por ejemplo, un archivo del tipo adobe acrobat o photoshop o “algo así”, en el caso de que el usuario ejecutara por su cuenta el archivo “juntado” vería lo que es y no el troyano.

De todas formas, NO HEMOS OCULTADO el proceso, sigue siendo visible desde el administrador de tareas, un administrador experimentado se dará cuenta en seguida de lo que ocurre, es más, si se ejecuta varias veces los ficheros “troyanizados” se abrirán tantos procesos en el administrador de tareas como veces se ejecuten, vamos que “canta por soleares”, aun así, te puedo asegurar que en un gran tanto por ciento de casos es muy, muy efectivo y simple.

Y añadimos lo siguiente:



Para ello, pulsamos sobre la ventana de la derecha (en un lugar en blanco) con el botón derecho del ratón, elegimos Nuevo-Valor alfanumérico, le cambiamos el nombre que nos pone por el de Adobegama.

Después pulsamos de nuevo con el botón derecho sobre el valor adobegama y seleccionamos Modificar, entonces escribimos:



Y pulsamos Aceptar.

La próxima vez que el equipo reinicie cargará y ejecutará nuestro troyano.

¿Y si el equipo no se reinicia nunca o tarda demasiado?

Bueno, podemos forzarlo, Un ataque por denegación de servicio (DoS, Denial of Service) sería interesante, también podemos probar con la herramienta shutdown del propio Windows o de terceros...

Ahora si que empiezas a entender el por qué no sólo los ataques DoS pretenden poner fuera de servicio a una máquina, no es sólo por fastidiar.....

Ejemplo:

- Shutdown /? Para "ir entendiendo"
- Shutdown /L /R /C para reiniciar le equipo local YA!

Si eres aplicado puedes experimentar con las otras claves del registro, prueba y comprueba, no dejes de estudiar, en estos momentos “has subido” muchos escalones en el conocimiento, no lo desperdices limitándote a copiar y “probar” únicamente con lo expuesto aquí.

Estarás pensando: ¿Para qué necesitamos shutdown si estamos en el equipo local?, bastaría con Inicio-Apagar...-Reiniciar. Sí Correcto.

También puedes pensar: Aunque no se trate del equipo local ¿Para qué necesitamos shutdown si debemos acceder el registro mediante Regedit?. Sí correcto.

Pero, vamos a ver, ¿Se podrá manipular un registro remoto de una máquina Windows? SIIIIII.

Disponemos de Regedt32, como vimos anteriormente y TAMBIEN disponemos de “otras” herramientas para hacerlo, ya lo verás, ahora mismo.

Manipulando el Registro de Windows.

Ya sabemos cómo editar, modificar y/o añadir nuevas claves con regedit, pero eso supone “estar sentado” físicamente en la máquina objetivo o disponer “de control remoto” de la misma y eso todavía no sabemos hacerlo, ¿Se podrá?

Lo que vamos a usar en esta práctica son determinadas utilidades que nos van a facilitar la tarea a la hora de manejar el Registro prescindiendo de Regedit o de Regedt32.

Conociendo la misión:

Se trata de escribir las nuevas claves a añadir o modificar, podemos utilizar el bloc de notas o algún editor ascii, NO USES WORD o cualquier otro tipo de Tratamiento de Textos que incluya “formatos extraños”, lo que necesitamos es que sea texto claro y limpio del tipo bloc de notas o similar.

Una vez escritas las claves a añadir o modificar, “colocarlas” en el Registro como si lo hubiésemos hecho directamente.

Necesitamos y disponemos de



Como eres bastante observador, imagino que empiezas a conocer de qué van.

Regback: Copia el Registro

Regdmp: Muestra/Vuelca el contenido del registro

Regfind: Busca valores y/o datos en el registro

Regini: añade, modifica o elimina claves, valores y datos en el registro

Regrest: restaura una copia del registro

Ya tenemos todo, nos falta aprender su uso, sintaxis y experimentar.

Todas estas herramientas en definitiva hacen lo mismo que la interface gráfica de Regedit, pero no necesitaremos regedit...

Bien, por ahora el que nos interesa es regini.exe, vamos a explicar como funciona:

- Por un lado hay que tener un archivo de texto con extensión *.ini con los valores a modificar
- Por otro lado hay que conocer cómo se interpretan los valores
- Por último hay que conocer la sintaxis del programa

Interpretación de regini.exe de las claves principales del registro

HKEY_LOCAL_MACHINE es convertida a **\Registry\Machine**.

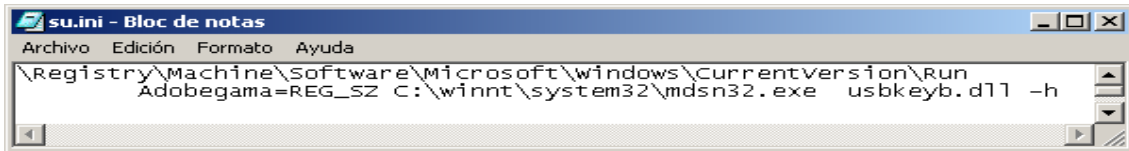
HKEY_USERS equivale a **\Registry\User**.

HKEY_CURRENT_USER se convierte en **\Registry\User\User_SID**

Observa todas las entradas comienzan por \Registry, a nosotros nos interesa la primera \Registry\Machine

Lo que queremos es realizar la misma operación que en la práctica anterior, modificar el registro añadiendo los valores necesario tal y como se hizo utilizando regedit.

Vamos a crear el archivo .ini, le llamaremos su.ini, abrimos el bloc de notas y escribimos:



Observa la segunda línea es exactamente lo mismo que escribimos cuando se hizo manualmente mediante regedit, en la siguiente tabla se muestran los valores y tipos de dato que aceptan las claves y valores del registro para ser usadas mediante scripts del tipo *.ini

Tipo de Dato	Valor	Entrada al Registro	Notas
REG_SZ	Cadena Caracteres	REG_SZ	REG_SZ tipo de dato por defecto
REG_EXPAND_SZ	Cadena Caracteres	REG_EXPAND_SZ	
REG_MULTI_SZ	Una o más cadenas entrecorilladas	REG_MULTI_SZ	
REG_MULTI_SZFI	Ruta del fichero	REG_MULTI_SZ	Abre el archivo que indica
REG_DWORD	Número decimal	REG_DWORD	0x para Hexadecimal 0o Octal 0b Binario True, False se convierte a 0x00000001 y 0x00000000
REG_BINARY	Dos o mas números decimales.	REG_BINARY	El primer valor es el número de bytes de los datos que siguen. El resto se convierte en formato de 32 bytes
REG_BINARYFIL	Ruta hacia un fichero	REG_BINARY	Se abre el fichero y su contenido se almacena en el registro como valor. La longitud del valor es la longitud del fichero
DELETE	Sin valor	Sin valor	Elimina la entrada.

Para añadir el archivo su.ini que acabamos de crear a la entrada correspondiente del registro, hay que

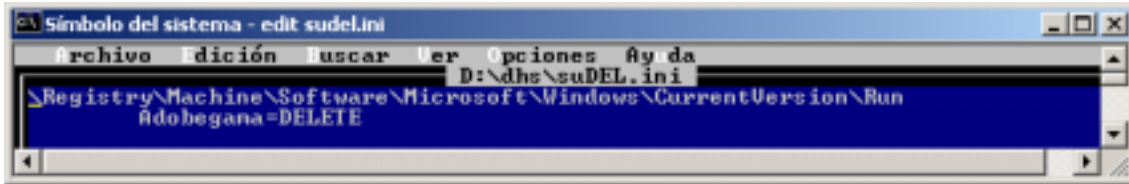
escribir:

Regini.exe [dirección_IP] archivo.ini, es decir:

Regini.exe su.ini, para nuestro equipo local o

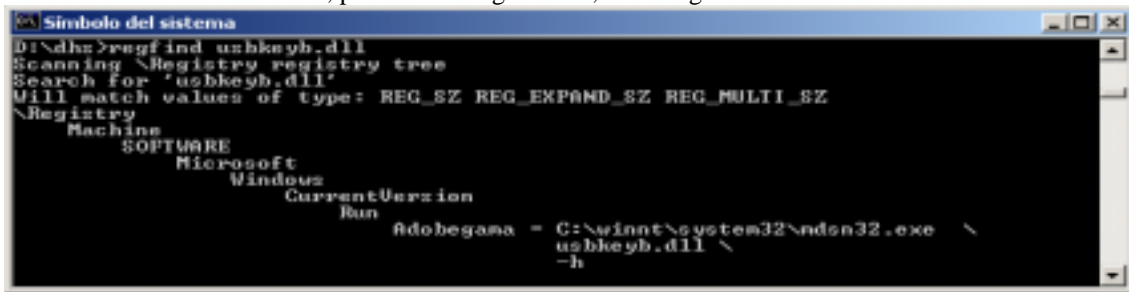
Regini.exe [\\192.168.0.1](http://192.168.0.1) su.ini, si la ip remota fuese 192.18.0.1

Para eliminar la entrada, crearíamos un archivo.ini, como este:



Lo grabamos, con el nombre sudel.ini y ejecutamos: Regini.exe [\\192.168.0.1](http://192.168.0.1) sudel.ini

Para encontrar un dato o valor, puedes usar regfind.exe, como sigue



Sugerencias

Podemos crear un script o fichero *.bat con los pasos para instalar la clave, “subirlo” o guardarlo en la máquina objetivo para que se auto ejecute y “cargue” el troyano, después que se auto elimine. Atrévete.

NOTA FINAL

Para manipular el registro, matar procesos, iniciarlos, tareas programadas, etc. Debemos tener permisos de administrador, por lo que antes de lanzar sin más las herramientas contra el destino hay que “explicarle” que somos administradores, para ello previamente nos conectaremos al recurso IPC\$ como administradores, después ya se podrán usar. Ejemplo:

Net use [\\ip.del.objetivo/IPC\\$](http://ip.del.objetivo/IPC$) contraseña /u:administrador

Después de la “tarea” no olvidar desconectarse... net use * /delete