

PRACTICA 15. Convertir el Serv-U en un troyano. (Revista HackXcrack)

¿Recuerdas el Servidor?. A leerlo de nuevo...

Vamos a convertir a éste programa en un troyano, haciendo menos sospechosa su ejecución y colocándolo en algún sitio interesante.

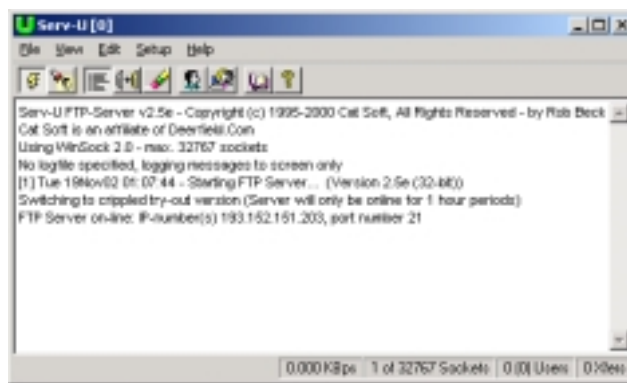
Lo primero es crear una carpeta en dónde “probar” nuevas funciones, p.e. Tro_SU, no te apures, en “la víctima” no colocaremos ese nombre que “canta” mucho.

Copiamos el Serv-U (limpito, es decir, sin haberlo ejecutado anteriormente) o sea, que lo descomprimimos directamente a esa carpeta, para que no haya dudas: Olvídate de la instalación anterior del programa.

Antes de ejecutarlo, vamos a cambiar de nombre al exe, por ejemplo yo lo he llamado mdsn32.exe, puedes elegir otro cualquiera, pero que sea discretito, no le pongas troyano.exe ni ftpserve.exe o explorer.exe ni nada de eso, échale imaginación: adobeview.exe, udmadv.exe o lo que sea.

Explicación número 1: ¿Por qué cambiar el nombre? Claro, “la víctima” puede conocer el archivo srv-U, no es un buen nombre para “esconder” nuestro troyano.

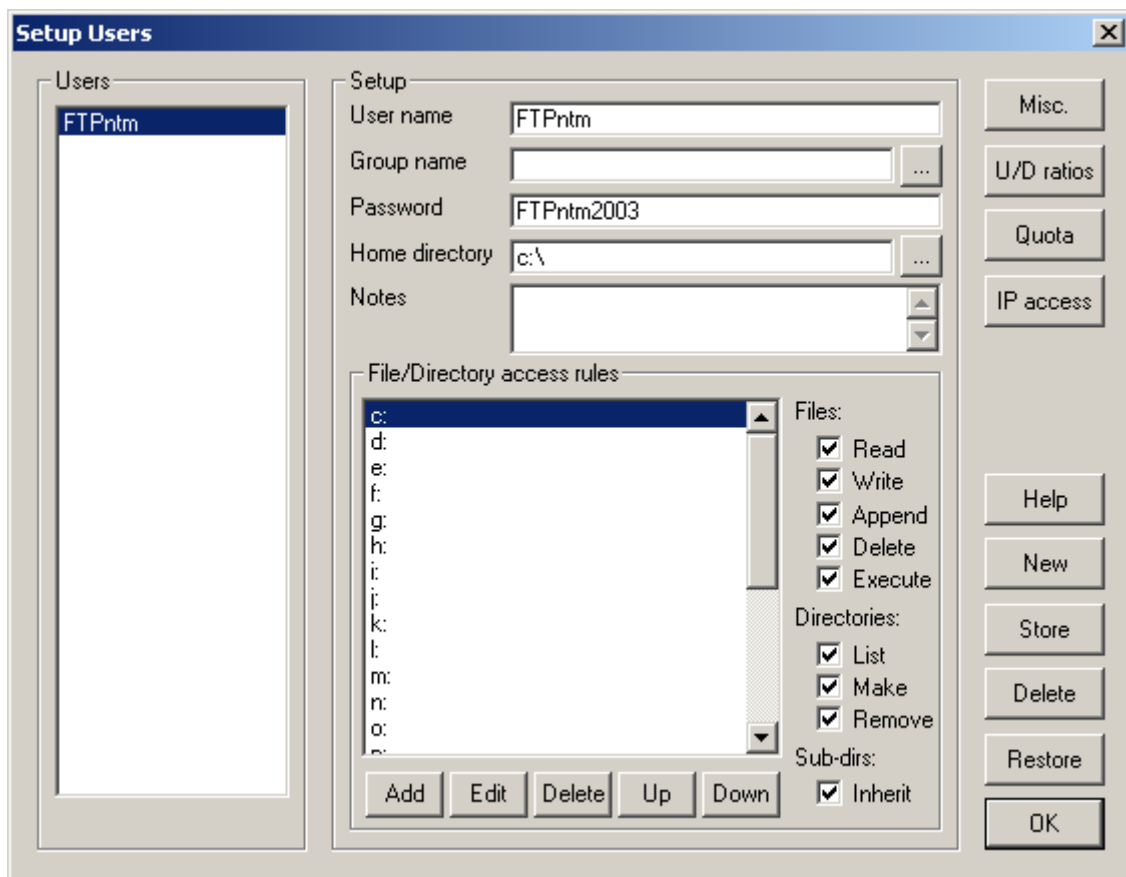
Ahora ejecutamos el mdsn32.exe (que en realidad es el serv-U) y seguimos los pasos descritos anteriormente, lo ejecutamos, elegimos la opción 1 **Choice 1** y Aceptamos, nos saldrá la pantalla principal del Serv-U, como vimos anteriormente



Al igual que antes, lo primero que hacemos es parar el servicio (*el icono del rayo*), nos vamos a **Setup** y eliminamos el Usuario por defecto (**Default**)

Recuerda lo que se ha dicho más de una vez en este texto, Dejar las configuraciones “por defecto” de programas, aplicaciones, routers, etc. es uno de los errores más graves que puede cometer un administrador o simple usuario, lo primero que probará un atacante es “entrar” por la configuración por defecto en el servicio, programa o dispositivo.

Te creas un nuevo usuario, el nombre lo eliges tu, yo elegí: FTPntm

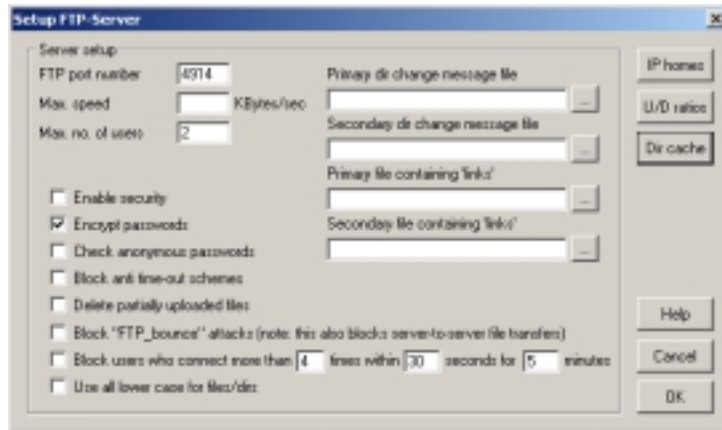


Explicación número 2: Si observas, se han seleccionado TODAS las letras del abecedario de la A a la Z, mejor de la C: a la Z:, lo de acceder a la disquetera puede ser algo demasiado perceptible por nuestro objetivo. Se han habilitado TODOS los permisos a ficheros y directorios. ¿Por qué? ¿Es que acaso no vamos a encontrar una máquina con tantas unidades?

No creo, eso es improbable, pero como no conocemos cuántas tiene ni cómo se llaman (Recuerda que Windows 2000 permite cambiar la unidad, por ejemplo un sistema con tres particiones, éstas pueden ser perfectamente C: T: y X:, además del CD y/o grabadora, que podrían ser D: y G:, si además es un equipo conectado a una LAN puede tener unidades de Red, p.e K:, I: etc., etc., etc. El por qué se habilitan todos los permisos está claro, ¿no?. Lo de no poner la Ñ: también se entiende....

Foro de HackXcrack

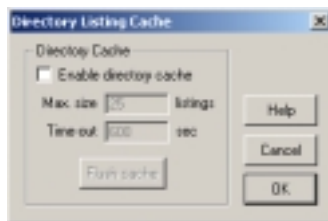
Ahora lo que debemos hacer es acceder a Setup-FTP Server... y seleccionar las mismas opciones que se muestran a continuación:



Explicación número 3: cuando configurábamos el serv-U se verificaban otras casillas, Enable Security, Block Time..., Block Users..., etc. claro, claro, eso era antes, cuando queríamos que nuestro servidor FTP fuese lo que debería ser, pero ahora no queremos eso, ja, ja.

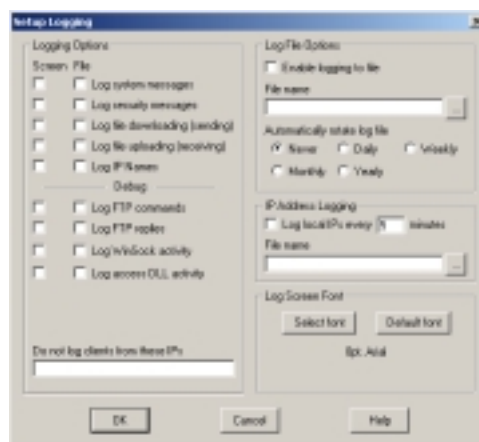
El FTP port number, yo elegí el 4914, pon el que te de la gana, ya sabes más allá del 1023 mejor, si lo dejamos en el 21 nuestra víctima será rastreada por miles de escáneres de todo el mundo.

Ahora pincha en Dir caché y deshabilítalo.



Pulsa OK y de nuevo OK volverás a la pantalla inicial del serv-U, ejem. Del mdsn32.exe

En el menú Setup-Login DESACTIVA TODO si no quieres que cuando te conectes al servidor registre TU PROPIA IP, después de dedicarle un montón de páginas a cómo ocultar la IP, no se te vaya a ocurrir que te logges tu sólo. Sin comentarios.



Vale ya está, ahora accedes a la carpeta en cuestión y OBSERVA: apareció otro fichero SERV-U.INI

Explicación número 4: Los archivos .ini suelen ser los archivos de configuración, en la mayoría de los casos son de tipo texto y se pueden ver simplemente con el bloc de notas.

Estos archivos guardan los cambios de configuración del programa a que pertenecen, es decir, todas esas opciones que se han deshabilitado, la lista de recursos, etc. están almacenadas en ese archivo. Como no existía en el momento de la ejecución del programa (recuerda que empezamos diciendo lo de una instalación limpia...) pues nuestro mdsn32.exe ha creado el suyo propio.

El archivo serv-u.ini es al serv-U.exe como el registro de Windows es al propio sistema operativo, además en los archivos .ini podemos encontrar claves ocultas y configuraciones que no se pueden configurar desde el propio programa ¡IGUAL QUE EN EL REGISTRO DE WINDOWS!. Imagino que vas comprendiendo la importancia de conocer más de cerca el archivo .ini y el registro de windows.

Vamos a echar un vistazo al contenido del archivo serv-u.ini

<pre>[GLOBAL] TryOut=Full Version=2.5.5.2 RegistrationKey=6YOctAJ1fWY,Su,25 Window=174,202,500,300 StartIconic=Yes StartMaximized=No ShowToolBar=Yes ShowBmpMenus=Yes MaxNrUsers=2 PortNr=4914 AntiHammer=FALSE AntiHammerWindow=30 AntiHammerTries=4 AntiHammerBlock=300 DirCacheEnable=NO DirCacheSize=25 DirCacheTime=600 Security=OFF LogGETs=OFF LogPUTs=OFF LogSystemMes=OFF LogSecurityMes=OFF LogFTPCommands=OFF LogFTPReplies=OFF LogIPNames=OFF LogDirtyDetails=OFF LogAccessDLL=OFF LogFileGETs=OFF LogFilePUTs=OFF LogFileSystemMes=OFF LogFileSecurityMes=OFF LogFileFTPCommands=OFF LogFileFTPReplies=OFF LogFileIPNames=OFF LogFileDirtyDetails=OFF LogFileAccessDLL=OFF Logging=OFF IPLog=0</pre>	<pre>[USER=FTPntm] Password=gt4aQhtABjnDc HomeDir=c:\ Access1=c:;RWAMCDLEP Access2=d:;RWAMCDLEP Access3=e:;RWAMCDLEP Access4=f:;RWAMCDLEP Access5=g:;RWAMCDLEP Access6=h:;RWAMCDLEP Access7=i:;RWAMCDLEP Access8=j:;RWAMCDLEP Access9=k:;RWAMCDLEP Access10=l:;RWAMCDLEP Access11=m:;RWAMCDLEP Access12=n:;RWAMCDLEP Access13=o:;RWAMCDLEP Access14=p:;RWAMCDLEP Access15=q:;RWAMCDLEP Access16=r:;RWAMCDLEP Access17=s:;RWAMCDLEP Access18=t:;RWAMCDLEP Access19=u:;RWAMCDLEP Access20=v:;RWAMCDLEP Access21=w:;RWAMCDLEP Access22=x:;RWAMCDLEP Access23=y:;RWAMCDLEP Access24=z:;RWAMCDLEP</pre>
--	--

Lo he puesto en dos columnas para que se vea mejor y he resaltado tres líneas interesantes...

Observa que en éste archivo están todas las configuraciones anteriores, nombre de usuario, puerto, número de conexiones, unidades de acceso, permisos de acceso para cada unidad, etc. Interesante, verdad.

Las líneas que he resaltado son las que vamos a cambiar sus valores:

Valor Actual	Nuevo valor
StartIconic=Yes	StartIconic=No
ShowToolBar=Yes	ShowToolBar= No
ShowBmpMenus=Yes	ShowBmpMenus=No

Explicación numero 5:

StartIconic permite o no la visualización del icono en la bandeja del sistema
ShowToolBar: permite o no que se muestre la barra de herramientas
ShowBmpMenus: permite o no que se muestren iconos a la izquierda de las opciones del menú.

IMPORTANTE.

No lo ejecutes todavía, si lo haces StartIconic se pondrá de nuevo a Yes por sí sólo, antes de ejecutar el programa con esta configuración tenemos que hacer “otras cosas”. Por cierto, no se si lo he dicho pero si se está ejecutando nuestro serv-U, antes de seguir debes “matarlo”, pulsa el botón derecho sobre la U verde que verás en la Bandeja del sistema y selecciona Shutdown.

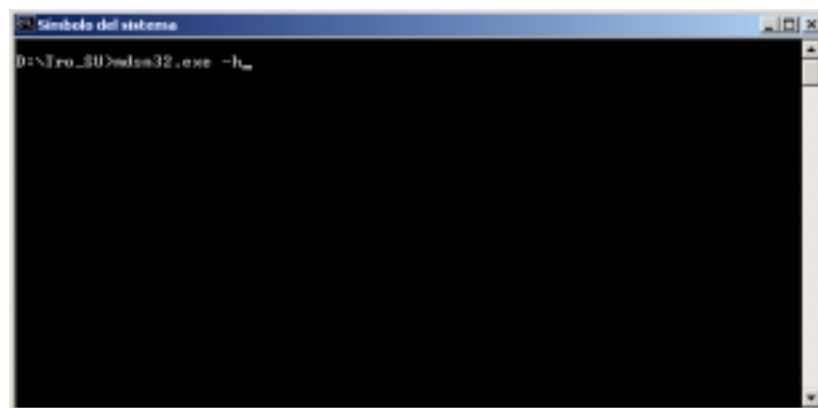
Bueno, estamos terminando, vamos a ejecutar el mdsn32.exe desde la ventana de comandos. ¿por qué?, ahora mismo lo entenderás.

A partir de ahora irás descubriendo que “la pantallita” de msdos va a ser una de nuestras mejores aliadas, herramientas como netcat, enum, nat, los comandos net, y cientos, miles de aplicaciones incluso con interface gráfica, se pueden iniciar desde la ventana de comandos, algunas de las que he citado sólo pueden ser ejecutadas desde ésta.

Bien, pero todavía no lo entiendo, ¿por qué? Pues porque vamos a ejecutar el serv-U (ahora es mdsn32.exe) en modo silencioso, no lo verás, no aparecerá el icono en la bandeja del sistema ni tampoco la interface gráfica del programa. Creo que no hace falta explicar la necesidad de todo esto, si nuestra “víctima” ve una U verde en el extremo inferior izquierdo de su pantalla “de repente” seguro que se mosquea, amén que intentará probar qué es eso y abrirá el serv-U. No te digo nada si lo que ve es la pantalla de inicio del serv-U.

Lo has cogido, ¿no? Lo que queremos es que el programa se ejecute sin que se den cuenta de ello.

A nuestra tarea, abrimos la ventana de comandos y escribimos: mdsn32.exe -h, no se te olvide cambiar primero a la unidad y directorio de la carpeta que te creaste, cd\troj_su

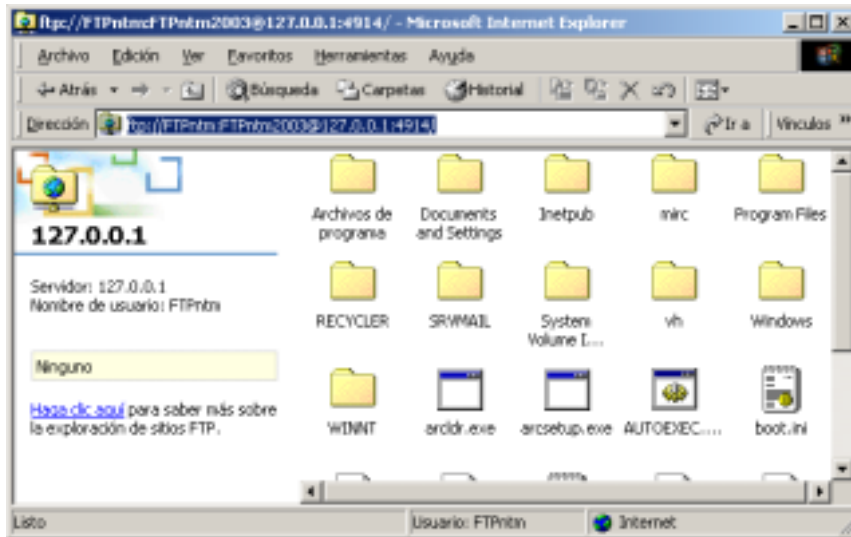


¿No ha pasado nada?, ¿Estás seguro? Pues aunque no te lo creas se ha ejecutado el serv-U, nuestro mdsn32.exe, y está escuchando por el puerto 4914 tal y como le dijimos, esperando que “alguien2 se conecte y cumpla su función: SERVIDOR FTP

¿No te lo crees? Haz varias pruebas:

inicia el Internet explorer y pon lo siguiente en la dirección:

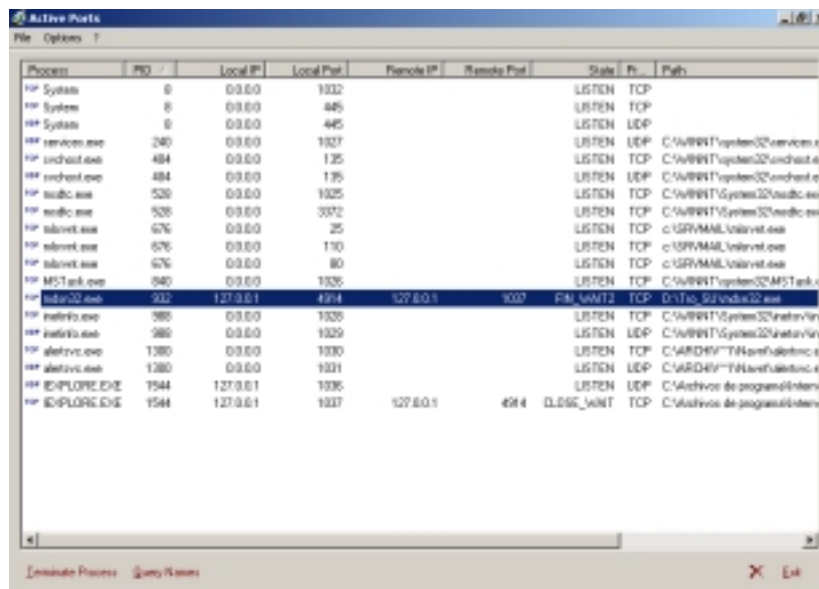
<ftp://FTPmtm:FTPmtm2003@127.0.0.1:4914> y verás la luz....



Explicación número 6: Internet Explorer 5 y posteriores incluyen un cliente FTP (algo cutre), contiene la parte mínima e imprescindible para poder “bajarse” archivos sin necesidad de salir del Explorador., por si lo quieres usar la sintaxis es:

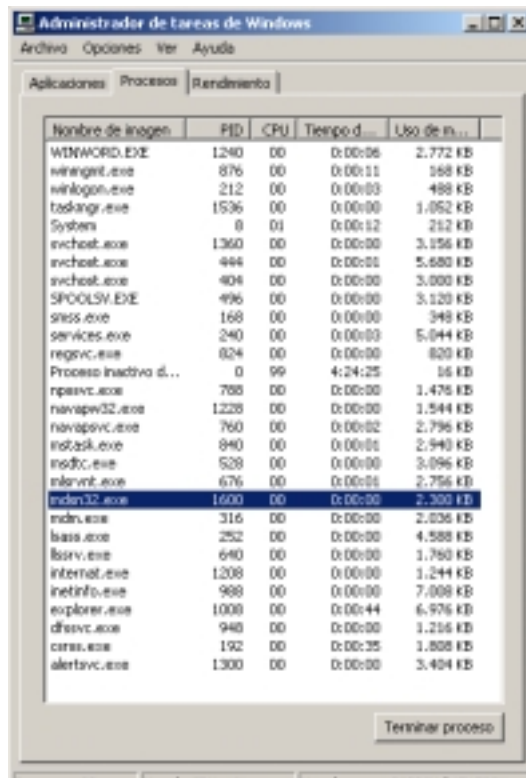
ftp://nombre_de_usuario:contraseña@ip_servidor:puerto

La segunda prueba es utilizar la herramienta Active Ports, fíjate bien he resaltado la línea que muestra que el programa mdsn32.exe se está ejecutando y abre el puerto 4914



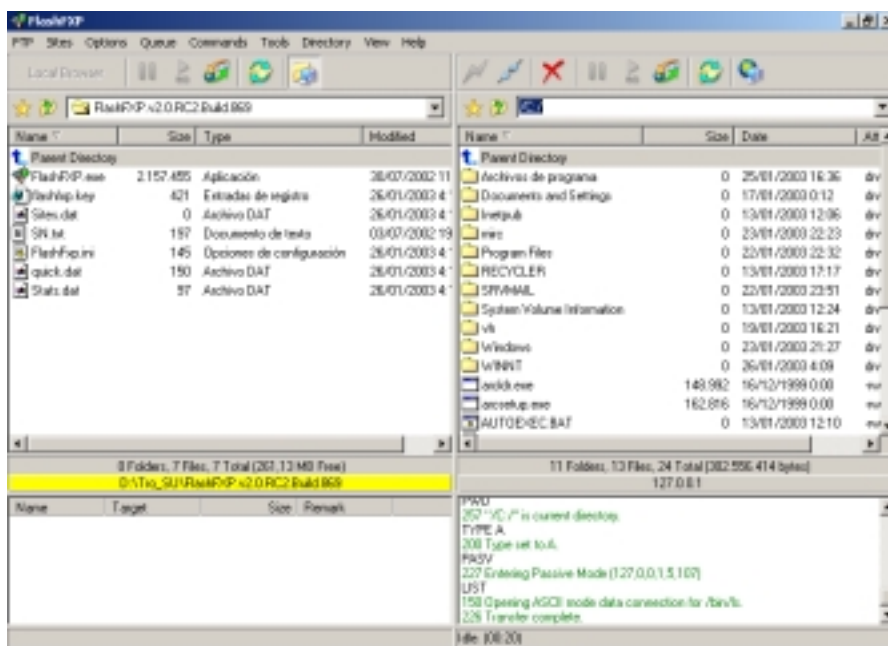
Prueba 3:

Pulsa Ctrl+Alt+Del y accede al administrador de tareas ficha de procesos, verás que el programa mdsn32.exe se está ejecutando....



Prueba número 4:

Arranca tu cliente preferido de FTP y realiza una conexión con el servidor:



Finalizando la práctica:

Hemos conseguido ocultar el icono y la pantalla de inicio del programa pero cuidado, el proceso sigue apareciendo y aunque hemos resuelto el problema del nombre del ejecutable todavía hemos de solventar el problema de la “llamada” al archivo SRV-U.INI, quien delata la existencia del “troyano”.

Todavía no es el momento de resolver el asunto de la aparición de nuestro mdsn32.exe en el administrador de tareas o en Active Ports, lo solucionaremos más adelante, no muy lejos,

Sí es interesante poner solución a lo del archivo .INI. Bien al igual que antes vamos a renombrar el archivo SRV-U.INI con el nombre, ummmmm, ya está: usbkeyb.dll, ya sabes, puedes elegir otro, a mi me gusta éste.

Problema: si renombramos éste archivo, el ejecutable no lo encontrará a menos que se lo digamos explícitamente, para ello y desde la ventana de comandos escribe:

Start mdsn32.exe usbkeyb.dll -h, y el Serv-U se ejecutará silenciosamente utilizando como archivo de inicio el contenido de usbkeyb.dll que es precisamente el SRV-U.INI renombrado.

Para rematar la tarea podemos ocultar los archivos, no te confundas, sólo los archivos no el proceso en sí mismo, mediate la orden:

```
Attrib -s mdsn32.exe  
Attrib -s usbkeyb.dll
```

Bueno, no es demasiada protección, si “la víctima” habilita la opción de mostrar archivos ocultos los verá, pero son bastante discretos y colocados en carpetas como c:\winnt\system32 pueden pasar desapercibidos.

Para finalizar la práctica nos falta colocar los archivos a “la víctima”, un mail? Un zip? Un empaquetado? Un rootkit? Un stream? Un camuflage? Un joiner? Un disquete?, calma, todo llegará, de momento confórmate con “pasárselo” a alguien que conozcas y que te deje su pc unos minutos, te lo llevas en un disquete se lo colocas en una carpeta discretita y se lo ejecutas. Luego te vas a casa y te conectas a su IP.

¿Y si no se la IP de la víctima o simplemente se “enchufa” a Internet mediante un módem con IP dinámica?, calma, todo llegará, (lo he dicho antes?)