

PRACTICA 12. Configurar un Servidor de FTP (Revista de HackXCrack)

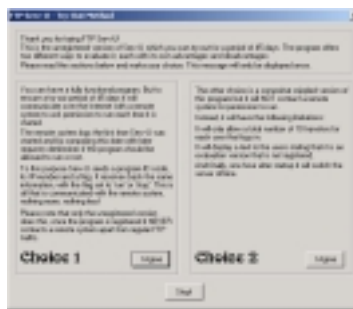
Para la realización de ésta práctica he elegido el programa Serv-U

¿Por qué este?

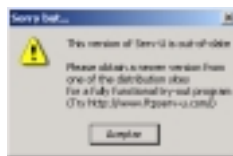
Efectivamente en existen más, incluso de “mejor” aspecto, se ha elegido éste (y esta versión concretamente) por que con algunas pequeñas modificaciones lo convertiremos en un troyano que no será detectado por ningún antivirus del mercado.

Aunque se trata de una versión bastante antigua, si deseas utilizarlo sin limitación en el tiempo debes registrar su uso y pagar por él, aún así lo podemos usar durante 45 días sin límite para nuestros propósitos, espero que consigas entender todo esto antes de esa fecha.

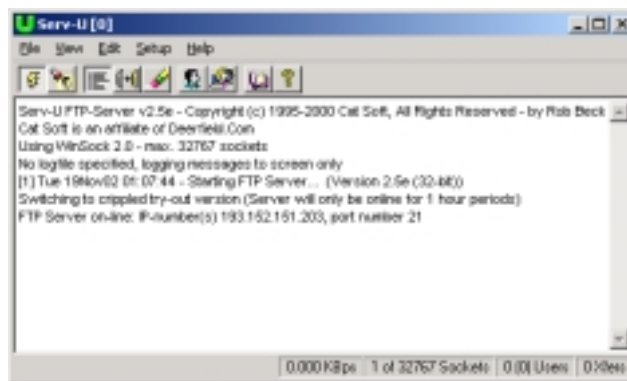
Primero vamos a crear una carpeta en la unidad que quieras para copiar el programa e instalarlo, por ejemplo **C:\SRVFTP**, y luego copia el programa, a esta carpeta y lo ejecutas



Haz clic en **I agree** dentro de **Choice 1**, te saldrá una ventana indicando que este programa está fuera de fecha, etc.. Este aviso saldrá siempre hasta que registres el producto, pulsa **Aceptar**



Se iniciará el programa y mostrará algo así:



El **icono con forma de rayo** inicia o detiene el servidor FTP, haz clic sobre él para detener el servicio antes de nada.

IMPORTANTE

Srv-U utiliza por defecto el puerto 21 (*FTP*) y nada más ser ejecutado intenta conectarse, si dispones de otro programa que use ese puerto NO PODRA abrirlo y el servidor no se estará ejecutando, también si tu equipo dispone de un Firewall personal o es XP, y no permite que se use este programa, desactiva el *Firewall*.

Si utilizas *Windows 2000 Server* o tienes instalado los *Servicios de Internet*, ya se estará ejecutando el servidor FTP de los servicios de IIS, *para el servicio o deshabilítalo mejor*.

INFORMACIÓN ADICIONAL

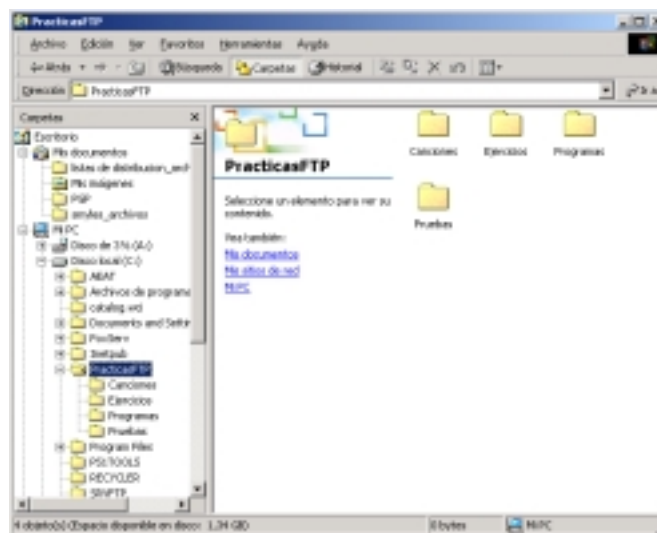
Cuando se instala *Windows 2000 Server*, se instala *IIS* por defecto, es decir, que tienes abiertos los puertos a la escucha *80-HTTP*, *119-NNTP*, *25-SMTP*, y también otros: *443*, *4605*, *6787*, *3456*, *4611* y depende de los servicios instalados tendrás más, y todo ello *SIN QUE TE ENTERES*, por que la instalación por defecto de *Windows 2000 Server* ya incluye la instalación de estas aplicaciones aunque no las uses.

Dicho de otra forma, si tienes un equipo en tu red o en casa, que no es un servidor Web, ni de correo, ni de noticias, etc. Lo primero que debes hacer es desinstalar los servicios que no uses, puesto que aunque no estén configurados LOS PUERTOS ESTAN A LA ESCUCHA y cualquiera (no te creas que hacen falta grandes conocimientos) puede usarlos para efectuar conexiones sin tu consentimiento.

Lo he comentado muchas veces en lo que va de libro (y las que faltan) **Nunca instales un Servicio que no vas a utilizar, Nunca dejes “tal cual” la configuración por defecto** al instalar un programa sea de lo que sea y esto incluye por supuesto al mismo Sistema Operativo.

Parece una cosa obvia, nadie en su casa compra una lavadora que no piensa utilizar, nadie compra un módem sin tener línea de teléfono, en fin, otra vez: LAS CONFIGURACIONES POR DEFECTO se deben revisar cuidadosamente y NUNCA SE INSTALA ALGO QUE NO SE USA O NO SE SABE USAR.

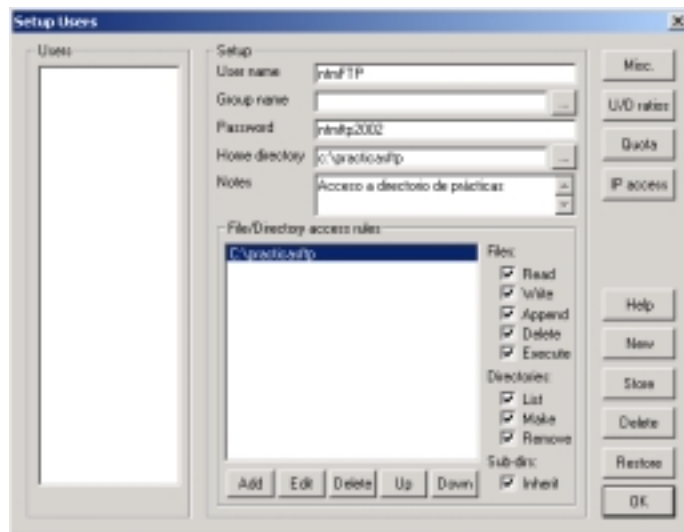
Para poder practicar con el servidor y con el cliente (próxima práctica) crearemos una estructura de directorios (carpetas) con la “supuesta” información que queremos ofrecer, si quieres puedes utilizar lo mismo que apareced en la siguiente pantalla o definirte una estructura personal.



Dentro de la carpeta “canciones” y “ejercicios” hay varios archivos, las otras están vacías.

Foro de HackXcrack

Lo primero que haremos es crear un nuevo usuario, **Menú Setup-Users**, Selecciona el usuario Default y elimínalo con el botón **Delete** el de la fila de la derecha), después créate un nuevo usuario con los datos que siguen:



User name: es el nombre de la persona que se conectará al servidor

Group Name: Grupo, podemos establecer usuarios y grupos como en windows 2000 ó XP

Password: Contraseña que pedirá el servidor cuando se conecte User Name.

Home directory: Es el directorio que mostrará el servidor, fíjate que apunta a la estructura creada (C:\practicasftp), eso quiere decir que sólo tendrá acceso a ese directorio y siguientes, si en lugar de ese directorio hubiésemos puesto C:\, tendría acceso a TODA la unidad C:

Notes: comentarios, puedes olvidarlos si no quieres perder tiempo, aunque son muy útiles cuando tienes muchos usuarios con distintos *Home Directory* y diferentes permisos.

En el marco de la ventana **File/Directory access rules**, se añadió (botón **Add**), el mismo directorio y si observas a su derecha se han verificado TODAS las casillas, esto quiere decir que ese usuario tendrá CONTROL TOTAL sobre esa carpeta, puede leer, escribir, ejecutar,... bien creo que no hace falta más explicación.

Quizá las únicas que te creen dudas sean **inherit** y **append**, sirven para:

Append: Que no es añadir como se puede pensar, permite reanudar la descarga en el caso de que se haya perdido la conexión con el cliente, desde el lugar dónde se quedó la última vez. ¿No os ha pasado alguna vez que al descargar un archivo de 5 Mb habéis perdido la conexión (cuando se llevaban 40 minutos) y al volver a intentarlo de nuevo el “*maldito*” empieza desde el principio otra vez?, Bueno pues esto se resuelve si se verifica esta opción, reanudará la descarga desde dónde se quedó.

Inherit: Asigna todas las opciones seleccionadas (leer, escribir, etc..) a los subdirectorios y archivos sucesivos, o sea, habilita la herencia de propiedades y permisos que se definieron en el directorio padre.

Foro de HackXcrack

El resto de botones, tienen la siguiente función, son bastante comprensibles y no me extenderé mucho:

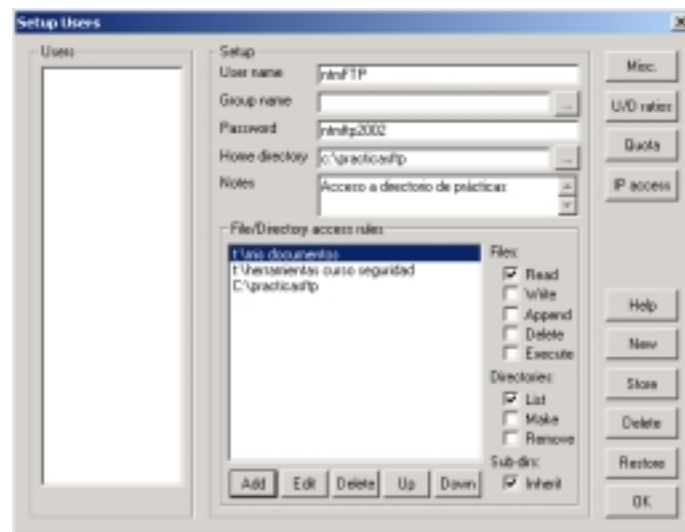
Misc: Miscelánea, permite configurar entre otras cosas, el número de accesos simultáneos, la velocidad de transferencia, si se muestran o no los archivos ocultos, etc...

U/D Ratios: Mide la tasa de transferencia, archivos descargados, bytes, etc..

Quota: Especifica el límite para cada usuario del espacio en disco disponible. FUNDAMENTAL si permitimos la escritura, NOS PUEDEN LLENAR el disco si no la establecemos.

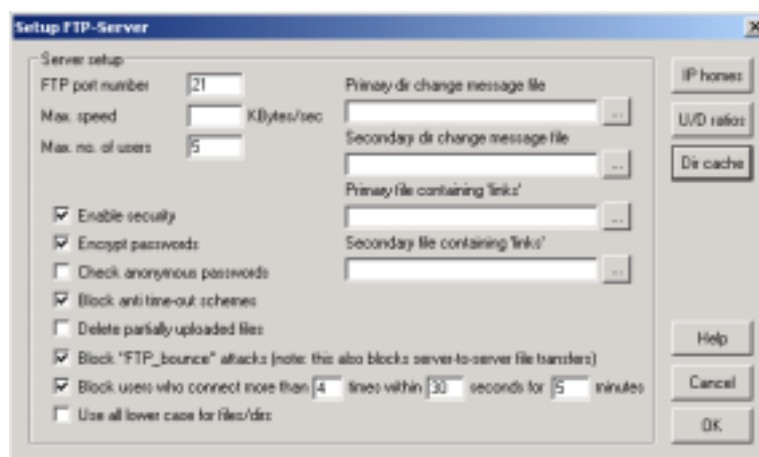
IP Access: Establece las reglas para aceptar o rechazar las conexiones a este servidor dependiendo de la dirección IP (puede ser un rango de IP) Es muy útil si montamos un servidor en una red local y deseamos impedir a ciertas máquinas el acceso al mismo aunque se identifique como usuarios registrados, o si es Internet a ciertas direcciones que no deseamos que se conecten.

Se pueden incluir más de un directorio de FTP (aunque sólo uno será *el Home directory*), es decir, podemos dar acceso mediante FTP, por ejemplo a lo que sigue:



Por cada entrada en *File/Directory access rules*, puedes establecer los permisos *Read*, *Write*, *Delete*, etc. específicos, como verás en el ejemplo la carpeta de Mis documentos de la unidad T: sólo puede ser leída y recorrida para este usuario.

Bueno una vez establecidas las configuraciones pulsa en el botón *Store* y luego *OK*, vamos al menú *Setup* y selecciona *FTP-Server*



Explicación

Enable security: Habilita la seguridad de acceso al Servidor

Encrypt Password: Codifica las contraseñas

Check Anonymous Password: Comprueba las contraseñas para usuarios anónimos

Block Anti line-out schemes: Desconecta a un usuario que no hace nada

Block FTPBounce attacks : Activa la posibilidad de transmisión FTP servidor a servidor.

Block user who connect more...: Evita posibles ataques por fuerza bruta

Use all lowers case for files/dir: Estructura de directorios en minúsculas

Son de especial interés las opciones *Block FTP Bounce attacks* y *Block user who connect...*

Block FTP Bounce attacks permite (si está desactivada) hacer lo que se llama FXP, esto lo veremos con más detalle en la próxima práctica, por ahora piensa en esto:

Supongamos un servidor en EEUU con un buen ancho de banda de conexión

Supongamos otro servidor en Francia con otro gran ancho de banda

Nosotros desde España con una conexión pobre (28.800 baudios) podemos hacer que entre los servidores anteriores se transfieran datos entre ellos utilizando sus anchos de banda, no el nuestro, podremos mover grandes volúmenes de información rápidamente.

La otra opción interesante es *Block user who connect...*, si la activamos desconectará a todos los usuarios durante 5 minutos, que no se identifiquen correctamente (usuario y contraseña) y lo intenten más de 4 veces en 30 segundos. Podemos variar las cantidades, esto evitará ataques de diccionario o fuerza bruta de nuestro servidor, por que a la cuarta ocasión que falle el registro de usuario “*le echará*” durante 5 minutos.

Los botones que hay en la derecha son:

IP Home: Permite especificar varias direcciones IP de nuestro servidor, por ejemplo si tenemos varias tarjetas de red en el mismo equipo

U/D Ratios: Permite seleccionar ficheros a descargar

Dir Cache: Habilita un caché de disco para la descarga optimizando los accesos a ficheros

Help, Cancel y Ok No hace falta explicarlos, ¿o sí?

Bueno una vez configurado el Servidor, en **IP Home, Ratios y Dir caché** no pondremos nada, pulsamos **OK** y volveremos a la pantalla inicial del servidor y pulsaremos de nuevo en **el icono del rayo para iniciar el servidor**.

La versión sin registrar desconecta automáticamente el servidor al cabo de una hora, si eso ocurre, debes reiniciar el servicio, esto es cerrando el servidor y volviéndolo a ejecutar.

En la bandeja del sistema, observaremos una U verde que indica que srv-U está corriendo en la máquina...

Para comprobar que funciona teclea esto: <ftp://mtmftp:mtmftp2002@127.0.0.1> desde Internet Explorer, y accederás desde el navegador al sitio ftp hemos creado. IE dispone de una versión “descafeinada” de cliente FTP, no explicaré nada más porque normalmente se usan otros programas para ello.