Artículo publicado en la revista @RROBA # 98
Suplemento *"Hack Paso a Paso"* #29 – Enero 2006
(Material Sin Editar)

Hardening Windows: IPFront

Introducción

Windows ha cargado por años la cruz de ser un sistema operativo inseguro, y si bien es cierto que originalmente la empresa de Redmond no ha sido lo suficientemente eficiente al momento de encarar este aspecto esencial de toda plataforma de cómputo, lo cierto también es que finalmente Microsoft ha encausado su estrategia vertiendo importantes mejoras en su nueva línea de sistemas operativos Windows XP / Windows 2003, sobre todo con la distribución de SP 2 y SP 1 respectivamente.

Reconociendo finalmente que no todos los usuarios son capaces de seleccionar el juego de configuración que mejor se adapte desde el punto de vista de la seguridad a su sistema, una de las mejoras producidas en estos nuevos operativos, pasa por lo que se conoce como "Mejor configuración por defecto", ejemplos de esta política pueden ser: "Firewall Activado por defecto en XP SP2", "IIS Desactivado por defecto en Windows 2003", etc.

A pesar de esto, quienes tenemos la posibilidad de ir un poco más allá, no debemos desconocer aquellos seteos o configuraciones que pueden elevar en gran medida el listón de seguridad respecto de nuestro sistema operativo. Cierto es que Microsoft hace su esfuerzo intentando mejorar sus productos, pero como usuarios, también tenemos nuestra cuota de responsabilidad al momento de conectar a la red uno de nuestros equipos.

Por este motivo, es que me he decidido a escribir este artículo de tan solo unas pocas líneas, con la intención de mostrarte algunas características que a menudo no suelen ser tenidas en cuenta a la hora de llevar a la práctica procedimientos de "Hardening" en nuestra plataforma.

A tal efecto, en las próximas secciones encontraras algunos tips, técnicas o herramientas de las cuales te podrás aprovechar a la hora de echar manos a la obra sobre tu instalación de Windows.

Hardening... que es eso?

Generalmente, se conoce como "Hardening" al proceso por medio del cual, es posible realizar una serie de ajustes pormenorizados sobre un dispositivo, sistema o aplicación, con el fin de elevar su nivel de seguridad.

Los procesos de hardening, a menudo se componen de una serie de pasos a seguir, los cuales involucran diferentes niveles de customización. Existen pasos de índole general, aplicables a cualquier dispositivo, sistema o aplicación, como por ejemplo: la instalación de hotfix y services packs, la disposición de elementos de seguridad física y/o del entorno, etc. y también aquellos mas puntuales referidos específicamente al

recurso que se esta intentando asegurar (Software de Base de Datos Oracle, Software de Base de Datos SQL Server, Windows SO en cada una de sus variantes, Linux SO en cada uno de sus sabores, IOS de Cisco, etc.)

Al mismo tiempo, y yendo puntualmente al tema principal de este artículo, el proceso de hardening de Windows, suele incluir aspectos relacionados con: Networking, Servicios, Aplicaciones, etc.

Ya escuche hablar de eso...

Encarar el proceso completo del hardening de Windows en general, tomaría varios artículos. Puesto que existen excelentes guías al respecto y entendiendo que probablemente ya hayas tenido oportunidad de leer alguna de ellas en algún momento, no espero aburrirte comentando cosas que sabes o a las que podrás acceder en alguno de los tantos buenos recursos on-line. En cambio, me tomare el atrevimiento de tan solo enunciar aspectos generales que deberás tener en cuenta en el camino de asegurar tu sistema Windows, para luego profundizar dos o tres puntos relacionados con seguridad a nivel IP que a menudo suelen pasar desapercibidos en tales procesos.

Dicho esto, y antes de comenzar debes conocer que los aspectos mencionados a continuación, te ayudaran a prevenir el 95% de las amenazas a las que tu equipo se encuentra sujeto. Por si acaso alguien no hubiera entendido este concepto, esto NO significa que el proceso de Hardening contemple tan solo estos puntos, pero SI significa que tan solo con este MINIMO esfuerzo de 5 pasos, tu sistema podrá ser considerado mas confiable. Dicho de otro modo... considéralo como un REQUERIMIENTO MINIMO:

-Asegurar tu secuencia de booteo y Verificar la seguridad a nivel BIOS de tu equipo.
-Instalar todos los Service Packs y Hotfix para tu plataforma en tiempo y forma.
-Instalar o Habilitar las características de Firewall.
-Desactivar/Renombrar las cuentas Guest y Administrator y Utilizar una política fuerte de contraseñas.
-Instalar Software Antivirus.

Vayamos a lo importante

Ahora que ya he podido explicar lo básico, pasemos a revisar algunos seteos que deberías implementar en tu Windows Box!!!!

Un aspecto de suma importancia en todo sistema actual que requiera interactuar de algún modo con una red TCP/IP, es aquel que se encuentra relacionado precisamente con el aseguramiento de la Pila TCP/IP o mejor dicho, con su implementación.

Cuando hablamos de seguridad a nivel TCP/IP, a menudo nos estamos refiriendo a la prevención contra amenazas tales como el spoofing, la denegación de servicios o DoS e incluso en algunos casos la actividad de port scanning.

Dejando de lado las medidas básicas y lógicas a saber:

- Deshabilitar siempre que sea posible "Compartir Impresoras y Archivos", digamos SMB (Server Message Block), quitando el *bind* desde la sección correspondiente en las propiedades de la placa de red...
- Deshabilitar siempre que sea posible NetBT o dicho de otro modo NetBIOS sobre TCP/IP, no solo desinstalándolo sino también quitando el *bind* desde la sección avanzadas de la placa de red...
- Eliminar la capacidad de Windows para registrar su nombre de Host en forma automática en un DNS, para aquellos equipos dispuestos en una DMZ o eventualmente una red de acceso público. (Sencillamente desmarcando la opción correspondiente en las propiedades DNS de la placa de red tal como se muestra en la **Figura 1**)

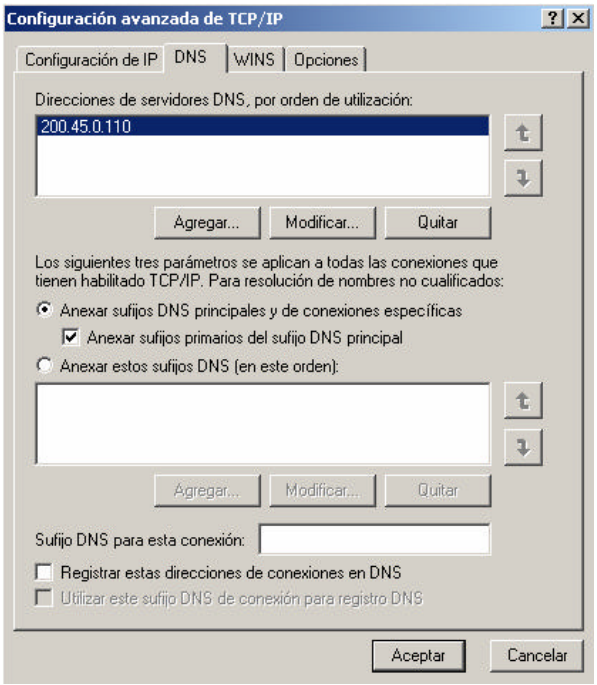

Figura 1

Los ataques de Denegación de Servicios (DoS), a menudo son difíciles de evitar cuando se originan de modo distribuido (DDoS), a pesar de ello, el administrador de Windows tiene a su alcance la posibilidad de customizar y/o optimizar, el modo en el cual el equipo establece y administra conexiones TCP/IP a través de su pila.

Realizando los seteos correspondientes, las chances de que nuestro equipo pueda tolerar un ataque DoS simple, crecen exponencialmente. Lo cierto es que dichos seteos, al igual que gran parte de las configuraciones importantes en Windows, no se encuentran accesibles a través de la GUI. Por tal motivo, a continuación presentaremos algunos Hack al Registro, que podas implementar con el objeto de mejorar algunos aspectos relacionados con la seguridad de TCP/IP en tu equipo:

> Antes de continuar, debo recordarte que todo cambio en el registro de Windows, puede causar resultados adversos, por tal motivo no olvides tener una copia de resguardo actualizada de tu sistema en general y del registro en particular.

El procedimiento es sencillo:

Desde el menú "Inicio" deberás señalar la opción "Ejecutar" y una vez allí llamar a la utilidad "RegEdit 32" escribiendo tan solo "regedt32" y dando enter. Por medio de RegEdit 32, editaremos los valores correspondientes básicamente a dos claves, por un lado aquella correspondiente a los parámetros generales de TCP/IP:

```
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters"
      DisableIPSourceRouting = 2
      EnableDeadGWDetect = 0
      EnableICMPRedirect = 0
      EnablePMTUDiscovery = 0
      KeepAliveTime = 300000
      NoNameReleaseOnDemand = 1
      PerformRouterDiscovery = 0
      SynAttackProtect = 1
      TcpMaxConnectResponseRetransmissions = 2
      TcpMaxDataRetransmissions = 3
      TCPMaxHalfOpen = 500
      TCPMaxHalfOpenRetired = 400
      TCPMaxPortsExhausted = 5
```

Y por el otro si así lo deseáramos, podríamos customizar algunos de los valores de Windows Sockets, de modo tal que podamos especificar la forma en la que operarán aplicaciones tales como FTP o Web servers. Puesto que este tipo de operaciones, interactúan con el controlador AFD.SYS, la clave sobre la cual realizaremos cambios, será precisamente la siguiente:

```
HKLM\System\CurrentControlSet\Services\AFD\Parameters"
EnableDynamicBacklog = 1"
DynamicBacklogGrowthDelta = 10"
MaximumDynamicBacklog = 20000"
MinimumDynamicBacklog = 20"
```

Ok... habiendo realizado estos cambios nuestro sistema debería encontrarse bastante mas seguro que al comenzar. Si eres alguien que realmente entiende TCP/IP, quizás hasta puedas ir testeando los valores seleccionados a fin de ir variándolos a fin de mejorar aspectos relacionados con la performance, aunque estos valores

(Recomendados por MS) probablemente se ajusten a tus necesidades. Si no fuera así, aún tienes tiempo de restaurar las llaves modificadas a su estado original.

Por ultimo, si estas interesado en obtener mas información respecto de estos cambios, quizás sea buena idea echar un ojo a los artículos ID 315669 y 324270 en la Microsoft Knowledge Base.

Seguridad en Profundidad: IPSec al rescate

Antes de terminar, me gustaría comentar un aspecto sumamente interesante respecto del uso de IPSec en Windows (2000/XP/2003), al momento de implementar "Seguridad en Profundidad".

Si bien es cierto que Windows XP y Windows 2003 a partir de sus nuevas ediciones poseen algunas características mejorados respecto de la implementación de reglas de firewalling como parte del propio sistema operativo, aún quedan algunas situaciones en las que la utilización de los mismos no se encuentra a nuestra disposición.

Para estas circunstancias, quizás sería bueno tener en cuenta que tienes la posibilidad de implementar tus propias reglas, a partir de la línea de comando de Windows. Veamos un ejemplo sumamente sencillo para que tengas idea de que va su sintaxis:

```
:Windows 2003 – Definimos la Política General
netsh ipsec static add policy name="Packet Filters - IIS" description="Server
Hardening Policy" assign=yes

:Windows 2003 – Definimos la Lísta de Filtrado
netsh ipsec static add filterlist name="HTTP Server" description="Server
Hardening"
netsh ipsec static add filter filterlist="ALL Inbound Traffic" srcaddr=any
dstaddr=me description="ALL Inbound Traffic" protocol=any srcport=0 dstport=0

:Windows 2003 – Definimos las Acciones del Filtro (Permitir o Bloquear)
netsh ipsec static add filteraction name=SecPermit description="Allows Traffic
to Pass" action=permit
netsh ipsec static add filteraction name=Block description="Blocks Traffic to
Pass" action=block

:Windows 2003 – Definimos los Filtros
netsh ipsec static add filter filterlist="HTTP Server" srcaddr=any dstaddr=me
description="HTTP Traffic" protocol=TCP srcport=0 dstport=80
netsh ipsec static add filter filterlist="All Inbound Traffic" srcaddr=any
dstaddr=me description="All Inbound Traffic" protocol=ANY srcport=0 dstport=0

:Windows 2003 – Definición de Reglas
netsh ipsec static add rule name="HTTP Server Rule" policy="Packet Filters -
IIS" filterlist="HTTP Server" kerberos=yes filteraction=SecPermit
netsh ipsec static add rule name="ALL Inbound Traffic Rule" policy="Packet
Filters - IIS" filterlist="ALL Inbound Traffic" kerberos=yes
filteraction=Block
```

No hace falta demasiada explicación verdad, en este caso tenemos un sencillo script por medio del cual seteamos un par de reglas tendientes a solo dejar ingresar a nuestro equipo, tráfico destinado a nuestro puerto 80 (Web) y denegamos el resto del tráfico.

Claro está que no es funcional y se encuentra lejos de ser óptimo para proteger un webserver, pero a los efectos del ejemplo es sumamente funcional.

Ahora bien... no importa si eres de los que prefieren todo servido, o por el contrario te consideras parte de aquellos a quienes les interesa aprender cada día mas, en cualquiera de los casos, te recomiendo eches un vistazo a una pequeña herramienta que he desarrollado hace algunos años, tendiente a automatizar el proceso de hardening de servidores Windows 2000/2003, y en la cual se hace uso tanto de los hacks de registro mencionados al inicio del artículo, como de filtrado por medio de IPSec: IPFront.

IPFront

Tal como se menciona en su "Acerca de" **(Figura 2)**, IPFront es una herramienta (GPL) desarrollada con el objeto de facilitar la tarea de usuarios y administradores encargados del hardening de servidores Microsoft Windows 2000 o Microsoft Windows Server 2003 (Su utilización en Windows XP merecería tan solo algunas modificaciones para funcionar).

Figura 2

En resumen, IPFront no es mas que un pequeño *Front End* encargado de recibir directivas por parte del usuario, transformando las mismas en pequeños scripts que

pueden ser ejecutados desde la misma aplicación o bien utilizados mas tarde en otros equipos. **(Figura 3)**

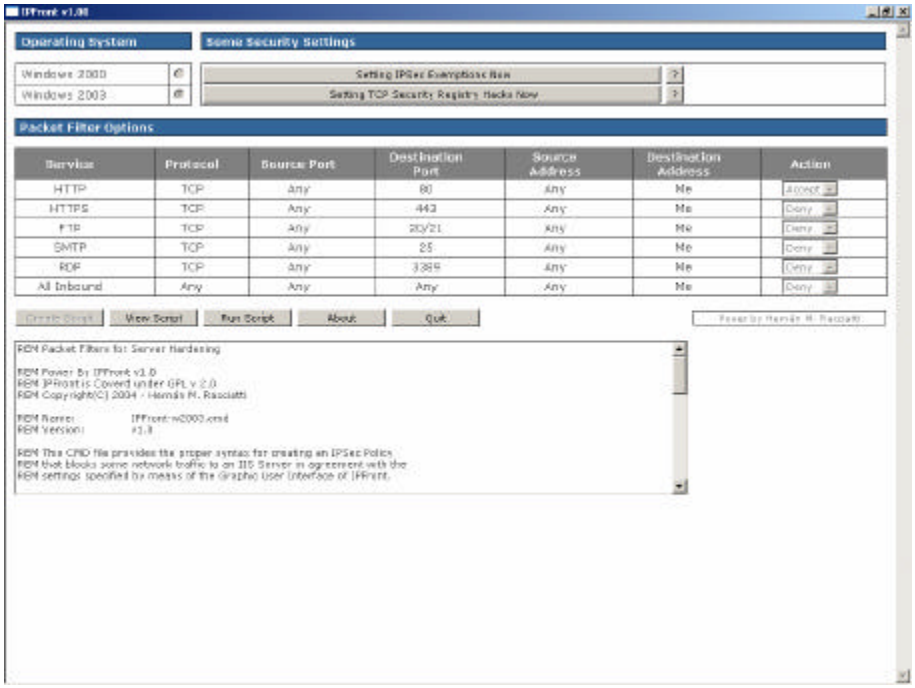

Figura 3

Figura 4

IPFront, cuenta también con dos botones, mediante los cuales es posible realizar algunos cambios en el registro de Windows (Como los descriptos al inicio de este artículo), a efectos de realizar el hardening de algunos aspectos del tratamiento de paquetes por parte de la pila TCP/IP en un caso **(Figura 4)**, y eliminar las excepciones existentes en la implementación de IPSec en Windows en el otro (Quizás puedas referirte a la ayuda del programa para saber mas acerca de las excepciones IPSec). **(Figura 5)**

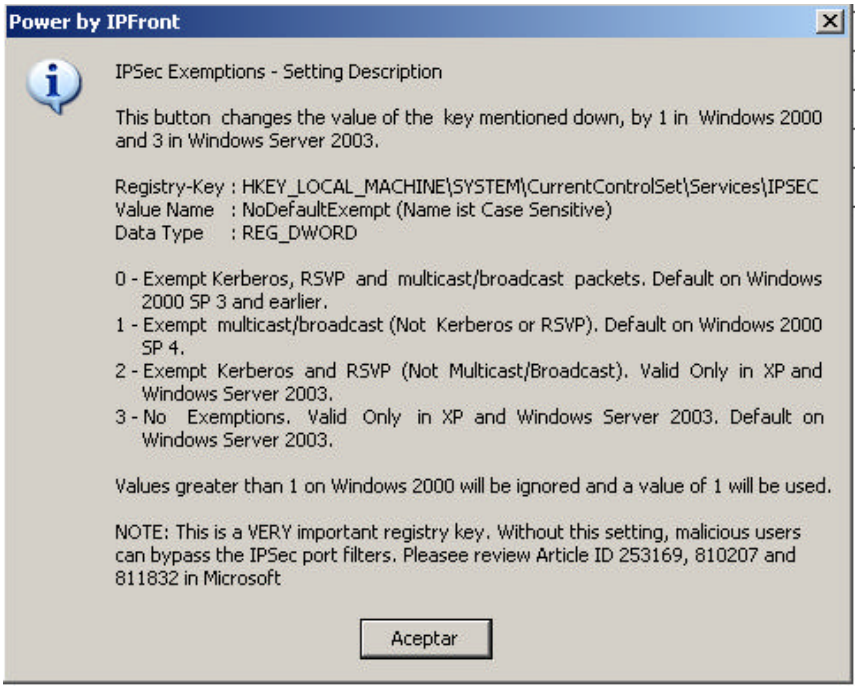

Figura 5

Como habrás podido notar, son muchos los aspectos de Windows que pueden ser mejorados sin siquiera hacer un solo click :D Espero que sepas aprovechar los conceptos vertidos en este artículo, que los mismos sean tan solo otro disparador para incentivarte a investigar más sobre estos temas y que disfrutes de IPFront! Hasta la próxima!!

IPFront puede ser descargada de:

http://www.ipfront.com.ar
http://www.hernanracciatti.com.ar/papers.html (IPFront link)

Hernán Marcelo Racciatti
http://www.hernanracciatti.com.ar

Referencias

Windows Security Resource Kit ISBN 0-7356-1868-2
http://www.hernanracciatti.com.ar
http://www.ipfront.com.ar
http://www.microsoft.com/security