

Las novedades de Windows Vista en Seguridad

Estos documentos han sido escritos y publicados por las siguientes personas.

Chema Alonso, MVP de Windows Security y escribe diariamente en su blog de ["Un Informático en el lado del mal"](#).

Juan Luís Rambla, MVP De Windows Security. Es especialista en Seguridad, sistemas, en Windows Vista y Longhorn. Impartió los primeros [Hans On Lab](#) de Windows Vista en España.

Joshua Saenz, especializado en Windows Server y Exchange.

Julian Blázquez, MCSA. Recorre España impartiendo seminarios de Windows Vista y Longhorn en Torrelavega, Galicia, Canarias, Sevilla, Madrid, Barcelona.

Juanfran Arrabe, imparte Hands On Labs MCSA y es amante de la seguridad informática.

Todos ellos trabajan en [Informática 64](#) y escriben en los blogs [Un Informático en el lado del mal](#) y [vista-tecnica](#)

Recopilación: Cristian Borghello, Director de www.segu-info.com.ar

V1.0 – 070320

V1.1 – 070519

Indice

Las novedades de Windows Vista en Seguridad	1
Indice	2
Control de Cuentas de usuario (UAC)	4
Control de Cuentas de Usuario (I de III)	4
Control de Cuentas de Usuario (II de III)	5
¿Cómo Deshabilitamos UAC?	5
¿Qué ocurre cuando deshabilito UAC?	5
Firmado de Drivers	6
Fortificación de Servicios.....	6
Control de Cuentas de Usuario (III de III).....	7
Configuración de UAC para los Usuarios	7
La protección contra Desbordamientos de Buffer en Windows Vista (I de IV)	9
Desbordamiento de Buffer.....	9
Explotación de un Desbordamiento de Buffer.....	10
Tecnologías de protección	11
La protección contra Desbordamientos de Buffer en Windows Vista (II de IV)....	11
Primera protección: Prevención.....	11
Segunda Protección: Detección	12
La protección contra Desbordamientos de Buffer en Windows Vista (III de IV) ..	13
Tercera Protección: No ejecución de Datos	13
Configuración en Vista	15
La protección contra Desbordamientos de Buffer en Windows Vista (IV de IV) ...	16
Cuarta Protección: Ocultación de Información.....	16
Bitlocker (I): Seguro más allá de su uso	18
Bitlocker (II): La Concienciación para la Seguridad de los Discos	19
Bitlocker (III): Escenarios para la implementación	20
Chequeo Médico	22
Bitlocker (IV): Algoritmos de autenticación para el cifrado de Disco.....	24
Autenticación MAC	24
Autenticación de "Poor-man"	25
Referencias Externas	25
Bitlocker (V): AES - CBC + Difusor.....	25
Referencias Externas	26
SuperFetch (I de IV)	26
SuperFetch (II de IV)	27
SuperFetch (III de IV)	29

SuperFetch (IV de IV): ReadyBoost y ReadyDrive ★★★★★	30
GPOs en Windows Vista (I de IV): Múltiples políticas locales	33
Un repaso general	34
LGPO en Windows Vista	34
Firewall de Windows Vista I de II	35
Firewall de Windows Vista II de II	41

Control de Cuentas de usuario (UAC)

Uno de los principios de la fortificación de sistemas es que todo se ejecute con el menor privilegio posible, así que, UAC nos permite, aunque estemos ejecutando nuestra sesión como Administradores de la máquina, que todas nuestras acciones se ejecuten como un usuario no privilegiado. Cada vez que se requiera el uso de privilegios se recibirá un aviso que nos informará de que esto se va a producir. Algunos lo tildan de “pesado” pero es mejor eso a que no diga nada, ¿no? Para los amantes del riesgo se puede deshabilitar (usando privilegios, claro)

Control de Cuentas de Usuario (I de III)

<http://geeks.ms/blogs/vista-tecnica/archive/2007/02/02/control-de-cuentas-de-usuario.aspx>

UAC – Control de cuentas de usuario es la tecnología que Microsoft ha incorporado en su nuevo sistema operativo Windows Vista. Es una tecnología revolucionaria que nos va a ayudar a mejorar la seguridad de nuestros sistemas.

Esta nueva tecnología proporciona al sistema el complemento que le faltaba para cumplir con el [principio del menor número de privilegios](#) posibles. Ahora solo falta esperar y ponerlo a prueba, para comprobar si al final aporta tantos beneficios como está empezando a demostrar.

El [objetivo principal de UAC](#) es minimizar el número de ataques que cada día más sufren nuestros sistemas y proteger el equipo ante los usuarios (amenaza en ocasiones más peligrosa que cualquier malware).

Para proteger el sistema y la información almacenada en el mismo, esta nueva tecnología realiza una reducción automática de los privilegios de todos los usuarios, convirtiéndolos en usuarios estándar por defecto.

¿Pero que ocurre cuando el sistema necesita de permisos superiores? El sistema notificará al usuario que la tarea que desea realizar (ya sea ejecutar una aplicación o realizar cambios sobre la configuración del sistema) necesita de privilegios superiores y requiere de su aceptación. Si el usuario acepta el incremento de permisos la tarea podrá realizarse, en caso contrario, la tarea se finalizará.



De este modo conseguimos que cualquier ejecución de las aplicaciones se haga de forma segura para el sistema. En definitiva, consigue que el trabajo diario de los usuarios, incluidos los administradores, no supongan un riesgo para nuestros equipos.

Para aquellos pocos administradores que tenían dos cuentas de usuario en el sistema, una con privilegios y otra sin ellos (que digo pocos..... casi ninguno), se

acabo la tortura de tener que estar lanzando las tareas administrativas mediante el comando **runas**.

En definitiva, **UAC sustituye a runas**, con el fin de hacerlo más sencillo para el usuario y mejorándolo hacia los nuevos avances que requiere cualquier sistema operativo en la actualidad.

En los siguientes post iremos ahondando cada vez en esta fascinante tecnología que nos va a proporcionar un gran control de lo que realizan nuestras aplicaciones en el sistema.

Control de Cuentas de Usuario (II de III)

La primera impresión de la gente al utilizar Windows Vista es lo "cansino" y molesto que puede llegar a ser el control de cuentas de usuario. Yo personalmente os tengo que decir que ya me he acostumbrado (algunos estarán pensando que no sé lo que digo), pero es verdad.

Al principio me resultaba un poco incomodo tener que aceptar cualquier acción que necesitara de privilegios administrativos o ejecutara un aplicación no reconocida por el sistema, pero con el uso acabas acostumbrándote.

Como ya habíamos comentado en post anteriores, esta tecnología viene a cubrir el poco uso o ninguno del comando RUNAS por parte de los administradores. Esta carencia provocaba en nuestros sistemas, agujeros de seguridad que lo convertían en mucho más vulnerables.

Hoy vamos a comentar como se puede deshabilitar el control de cuentas de usuario y sus consecuencias, para que los administradores que decidan no contar con esta tecnología tengan claro los riesgos que están corriendo.

¿Cómo Deshabilitamos UAC?

Para deshabilitar el control de cuentas de usuario de Windows Vista simplemente consiste en desactivar una casilla de verificación. Esta casilla de verificación se encuentra en el módulo de cuentas de usuario del panel de control en el link Activar o desactivar el control de cuentas de usuario.

Cuidado con activar o desactivar UAC, ya que es necesario reiniciar la máquina para que los cambios surjan efecto.

¿Qué ocurre cuando deshabilito UAC?

Desde el momento en que decidimos dejar de utilizar el control de cuentas de usuario el sistema operativo empieza a ser vulnerable a los riesgos que tantos problemas nos acarreaban en Windows XP.

Sin UAC, Windows Vista deja de virtualizar los registros para cualquier usuario. Obligándonos a dar de nuevo privilegios de administrador a los usuarios estándar. A aquellos usuarios que utilizan aplicaciones que requieren de credenciales de administrador. ¿Queremos correr ese riesgo? ¿Un usuario con privilegios administrativos? (¡Eso nunca!)

Otro de los inconvenientes de desactivar UAC es que un usuario administrador utilizará todos sus privilegios para lanzar aplicaciones como el solitario y navegar por internet. ¿Estamos convencidos de dejar esa puerta trasera abierta?

Otra problemática es la pérdida de seguridad en la ejecución de aplicaciones. Me explico, ¿quién no ha sufrido en alguna ocasión la ejecución de una aplicación que venía encapsulada en una imagen o se ha descargado desde una página web,...o desde cualquier otro modo? Pues bien gracias al control de cuentas podemos

controlar dichas aplicaciones e impedir que se instalen y se ejecuten en nuestro sistemas.

Estos son algunos ejemplos de los riesgos más comunes que podemos sufrir si desactivamos el UAC. Toda seguridad empieza protegiendo el acceso y control que los usuarios y las aplicaciones tienen de nuestro sistema.

Personalmente os recomiendo encarecidamente seguir utilizando UAC y no hagáis caso a esos post que lo único que hacen es vetarlo sin conocer todas sus ventajas.

En el siguiente post hablaremos del modo que tenemos de configurar el control de cuentas de usuario para adaptarlo a nuestras necesidades. Por ejemplo, como seguir utilizando UAC sin tener que sufrir los mensajes de aceptación.

Firmado de Drivers

El firmado de los drivers que se exige en las plataformas de 64 bits tiene como principal objetivo garantizar la no inclusión de rootkits o troyanos no deseados en modo kernel en el sistema operativo, pero al mismo tiempo busca obtener una garantía de calidad de aquellos que sí deben ser instalados y así mejorar la fiabilidad del sistema.

Fortificación de Servicios

Para los servicios se han realizado tres acciones, una primera en la que se han reducido los permisos necesarios de los mismos para evitar que corran de manera privilegiada en el sistema. En segundo lugar se les ha identificado a cada uno con un SID del sistema que permite la gestión de sus permisos de forma individual y en tercer lugar, son acompañados de un manifiesto que les restringe los objetos a los que tiene acceso cada servicio, para, en caso de un eventual compromiso, esté limitada la supervicie vulnerada.

Mandatory Integrity Control

Windows Vista ha dividido en cuatro niveles de integridad las características de todos los procesos y objetos del sistema, con lo que ningún objeto o proceso de nivel de integridad inferior podrá acceder a ningún otro objeto que tenga un nivel de integridad superior. Esto lleva a que por ejemplo, ningún programa que esté corriendo con nivel de Integridad Medio, ejecutado por un administrador, podrá acceder a un objeto de nivel de Integridad Alto de Sistema. Para ello se tendría que hacer correr el proceso con el nivel de Integridad Alto de Sistema. Esto tiene su expresión más visible en el Modo Protegido de Internet Explorer 7, que corre dos procesos, uno con nivel de integridad bajo, que es el expuesto a Internet y otro con nivel de integridad medio que es el que controla al primero.

User Interface Privilege Isolation

UIPI, que así se luce acrónimo esta tecnología, realiza una protección utilizando los niveles de integridad para los procesos. En este caso, niega que un proceso de nivel de integridad inferior realice una llamada o envíe un mensaje de ventana o se ponga en la lista de eventos de un proceso que se ejecuta en un nivel de integridad superior. Con esto se intentan evitar los ataques de inyección de código para realizar elevaciones de privilegios tan utilizados en muchas de las herramientas de ataque.

Protecciones contra desbordamiento de buffer

Siempre han sido un punto fuerte de los ataques aprovechar los desbordamientos de buffer en los parámetros de llamadas a procedimiento. En Windows XP ya contamos con la protección DEP (Data Execution Prevention), ofrecida por los microprocesadores, para evitar que se inyecten códigos ejecutables en los

parámetros. Esto evita que se inyecte un programa como parámetro, pero siempre se puede ejecutar un programa ya cargado en memoria, para evitar esto, los programas ya no se cargan en las mismas direcciones de memoria. En cada ejecución se cambia la dirección. A esta tecnología se llama Address Space Layout Randomization (ASLR).

Es uso de BitLocker ([I](#), [II](#), [III](#)), para cifrar los discos, el uso de los chips TPM (Trusted Platform Module) para garantizar la integridad en arranque del sistema, el firmado de dlls del sistema, la integración de IPSec con LDAP, el firewall de doble dirección, la integración del sistema con [NAP](#) (Network Address Protection) el monitor de fiabilidad y las herramientas de diagnostico son algunas otras características que acompañan las novedades de Windows Vista en Seguridad.

Si a estas tecnologías le unimos las ya existentes de Windows XP SP2, los filtros Antiphishing de IE7, el acompañamiento de Windows Defender para proteger el sistema contra Spyware, el sistema de actualizaciones automáticas, etc... podremos decir que el sistema tiene un buen aspecto. ¿Invulnerable? No lo creo, pero... ¿Hay algo invulnerable?

Y aun nos quedarían las otras tecnologías, el Superfetch de memoria ([I](#), [II](#), [III](#)) para conseguir un uso más aprovechado de la memoria y mejorar la experiencia del usuario, el Readyboot para conseguir el arranque eficiente, el ReadyBoost para añadir memorias caché flash en caliente y aumentar la velocidad de acceso a disco en accesos aleatorios y... ¿Cómo se llama eso de las ventanas en 3D? Ah sí, el Aero.

Control de Cuentas de Usuario (III de III)

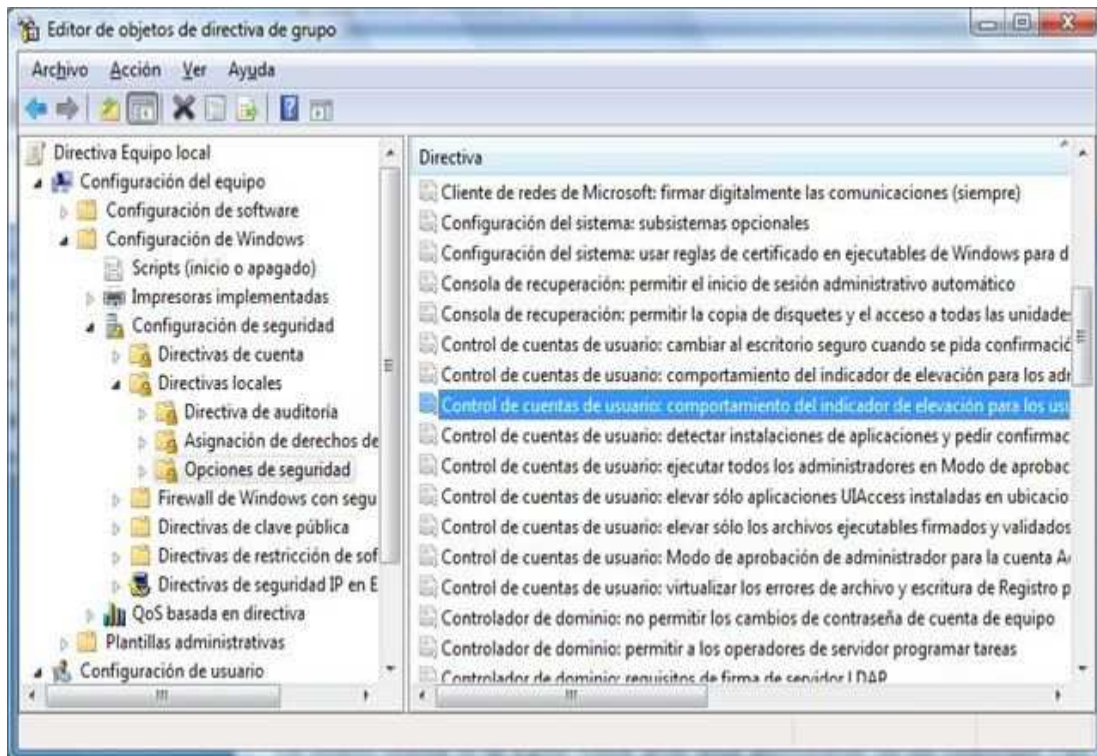
En estos nuevos posts hablaremos de las posibles configuraciones que permite realizar el Control de Cuentas de Usuarios, para poder adaptarlo a nuestras necesidades. Iremos viendo ante todo los posibles riesgos ([no tan graves como deshabilitarlo](#)) que conlleva cada configuración. El administrador no puede conseguir asegurar nunca un sistema operativo al máximo, pero si puede asumir los riesgos que corre.

Las posibles configuraciones del UAC la vamos a dividir en dos grandes grupos, los usuarios estándar y los administradores. Windows Vista nos proporciona la posibilidad de definir su comportamiento de forma independiente a ambos tipos de usuarios. En este post lo dedicaremos a la configuración de UAC para los usuario estándar.

Configuración de UAC para los Usuarios

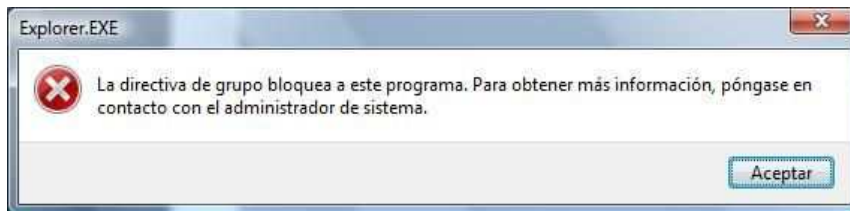
Los usuarios estándar no van a poder realizar jamás tareas administrativas con sus credenciales. Pero ¿Qué ocurre si el administrador necesita realizar una tarea administrativa cuando se encuentra bajo la sesión de uno de estos usuarios?. Ante este tipo de situación antes, utilizabamos el comando runas para ejecutar la acción, pero no siempre resultaba lo suficientemente cómodo y rápido.

Ahora mediante políticas (locales o de grupo) vamos a poder definir el comportamiento del UAC, para favorecer la operativa del sistema operativo en el escenario anteriormente descrito. Para ello debemos abrir la política que deseemos configurar y acceder a la directiva que se encuentra en la ruta: Configuración del Equipo --> Configuración de Windows --> Configuración de Seguridad --> Directivas Locales --> Opciones de Seguridad. En dicha ruta existen una directiva con el nombre "Control de cuentas de usuario: Comportamiento del indicador de elevación para los usuarios estándar".



Esta directiva proporciona dos posibles configuraciones:

Rechaza solicitudes de elevación automáticamente. Esta configuración impide a los usuarios realizar cualquier tipo de tarea administrativa, ya que su usuario no posee privilegio para ello.



Pedir credenciales. Esta configuración permite proporcionar al usuario nuevas credenciales para realizar la tarea administrativa, dando mayor funcionalidad al equipo a la hora de su administración. Pero nos muestra por defecto todos los nombres de las cuentas que pueden realizar dicha configuración.

Cuidado con esto, ya que nos acabos de saltar uno de los dos niveles de seguridad que tienen la cuentas de usuarios. ¡Ya tenemos el nombre de una cuenta válida, ahora solo nos queda adivinar su contraseña!



Estas son las dos posibilidades que nos proporciona Windows Vista a la hora de configurar el comportamiento de UAC con los usuarios estándar (que carecen de privilegios). En el post de la semana que viene (y prometo que sea el viernes) hablaremos de la configuración para los administradores.

La protección contra Desbordamientos de Buffer en Windows Vista (I de IV)

El problema de los desbordamientos de Buffer en las aplicaciones que corren sobre un sistema operativo ha sido un tema recurrente. Desde hace tiempo se intenta encontrar una forma eficiente de realizar comprobaciones en el código fuente que se programa para evitarlos. Muchos de los lenguajes de alto nivel que se utilizan hoy en día tienen este tipo de protecciones, pero cuando se desarrollan módulos en lenguajes de bajo nivel siguen apareciendo estas debilidades.

Desbordamiento de Buffer

El objetivo de una explotación de desbordamiento de buffer es sobrepasar la longitud de memoria reservada para los parámetros de una llamada a un procedimiento con el fin de sobrescribir la dirección de retorno del contador de programa. Es decir, se buscan parámetros en procedimientos que no son correctamente comprobados antes de ser utilizados.

Imaginemos este entorno de memoria:



Imagen 1: Memoria

En esta sección de memoria vemos como se ha apilado una dirección de retorno para cuando se acabe de ejecutar el procedimiento que tiene actualmente el control del programa y encima se ha reservado espacio para que se apilen los parámetros locales de dicho procedimiento. A la hora de cargar los parámetros en ese espacio reservado, estos deberían ser comprobados, si no se produjera esta comprobación tendríamos un problema de buffer overflow.

Explotación de un Desbordamiento de Buffer

El atacante introduce como parámetro el código que quiere que se ejecute y luego escribe información nula hasta que sobrepasa el espacio que tiene reservado. Una vez que ha llegado a la dirección de retorno escribe la dirección de memoria donde ha introducido su programa.



Imagen 2: Desbordamiento de Buffer

Con esto consigue haber introducido un programa que se va a ejecutar. Este es un ejemplo típico para los programas que devuelven una shell o crean un interfaz de comandos.

Tecnologías de protección

Las tecnologías para evitar que se produzca una explotación de una vulnerabilidad de buffer overflow son varias, pero hay dos que son especialmente significativas: DEP (Data Execution Prevention) y ASLR (Address Space Layout Randomization). Ambas incluidas en Windows Vista y ...lo vemos en el próximo post!.

La protección contra Desbordamientos de Buffer en Windows Vista (II de IV)

¿Como podemos proteger Windows Vista contra los desbordamiento de buffers? Esto es algo que se lleva estudiando largo tiempo, por ello existen diferentes aproximaciones. La primera de ellas es una respuesta bastante sencilla. Utilizar técnicas de prevención.

Primera protección: Prevención

Herramientas de Análisis Estático de Código. FxCod

El objetivo es que si todos los parámetros están bien controlados y no se pasan a la pila de memoria sin haber comprobado correctamente su longitud no tendríamos desbordamientos de buffer, luego intentemos que no salga ningún programa sin haber sido correctamente evaluado. Para ello se utilizan desde hace tiempo las herramientas de Análisis Estático de Código realizan un chequeo del código del programa mientras este no se está ejecutando, buscando patrones de fallos de

seguridad (incluidos los desbordamientos de buffer) en códigos en ensamblador, código fuente o código manejado. FxCod es una herramienta de análisis de estático de código manejado que se puede utilizar en todos los desarrollos que se realizan con Visual Studio 2005. Es una herramienta que permite detectar, no solo desbordamientos de buffer, si no un amplio abanico de fallos de seguridad en las aplicaciones. Todo programa debe estar comprobado para evitar desbordamiento de buffers. Una de las características importantes es que estas herramientas se pueden usar para validar la fiabilidad y seguridad de un software. Microsoft, para las versiones de Windows Vista de 64 bits ya para Longhorn obliga a que los drivers que se instalen en el sistema operativo vayan firmados por Microsoft o una compañía autorizada. Para conseguir la firma del driver es necesario pasar unos test de seguridad que evalúan con herramientas de análisis estático el código del driver.

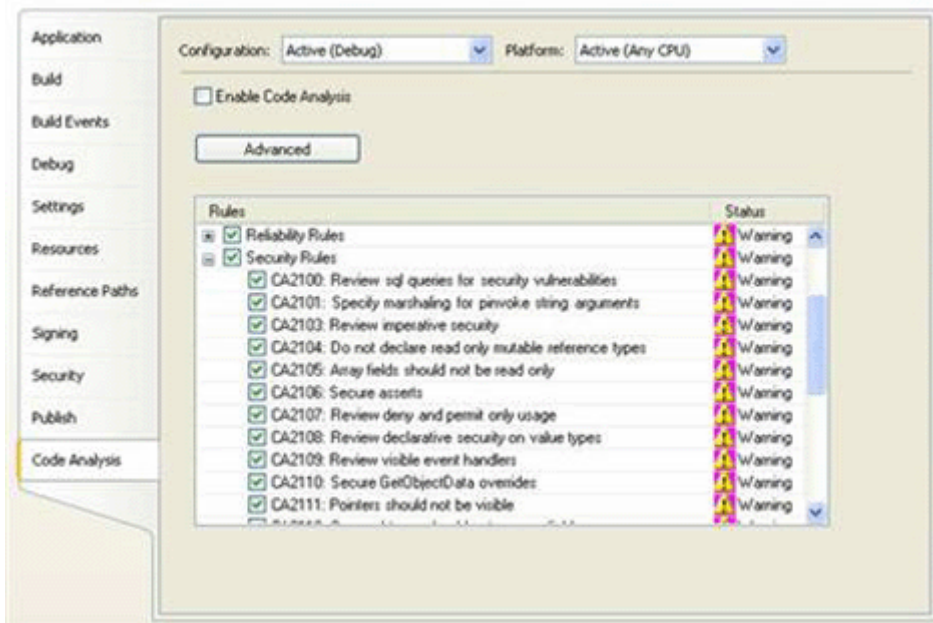


Imagen: Opciones de Análisis de Código en Visual Studio.

Segunda Protección: Detección

Los Canarios y la opción /GS

Una de las ideas, propuesta por uno de los grandes expertos de la seguridad, Crispin Cowan, fue utilizar lo que el denomina canarios. Los canarios son utilizados en las minas y en las cocinas de gas, para detectar gases nocivos, si el canario muere, algo malo sucede. En el caso de los desbordamientos de Buffer esta es una idea similar. Consiste en apilar unos determinados valores en la pila de llamada al procedimiento justo después de apilar la dirección de retorno. Cuando se va a pasar el control a esa dirección de retorno, se comprueba previamente si los valores en los canarios son los correctos. Si no lo son, hemos de asumir que se ha producido una violación de la zona de memoria. Se llama Stack-Smashing Protection. El uso de estas tecnologías no garantiza que los parámetros no sufran de desbordamiento de buffer, pues se pueden sobrescribir, no la dirección de retorno, pero sí, el resto de estructuras y, si el atacante puede descubrir el valor de la dirección de memoria o del canario, puede intentar simular un canario correcto. Para ello, se usan canarios no predecibles.

En Visual Studio la opción del compilador de comprobación de seguridad del búfer de Visual C++ se llama /GS. El funcionamiento de la opción /GS consiste en

establecer un valor cifrado (a veces denominado "chivato") al final de un búfer. Este valor se comprueba durante la ejecución del código y si ha cambiado, se detiene la ejecución del programa y se genera una excepción de seguridad. La opción /GS no evita la saturación del búfer, pero protege contra el posible secuestro del código al detener la ejecución del programa.

La protección contra Desbordamientos de Buffer en Windows Vista (III de IV)

Tercera Protección: No ejecución de Datos

DEP (Data Execution Prevention) Bit NX (Non Execute)

La tecnología DEP está disponible en Windows XP SP2, Windows Server SP1, Windows Server 2003 R2 y además viene incluida también en Windows Vista y puede aplicarse tanto por Software como por Hardware. ¿Qué quiere decir que puede aplicarse por Hardware o por Software? ¿Funcionan igual?

DEP por Hardware

Para activar DEP por hardware es necesario que el microprocesador que estemos utilizando venga con esta característica, ya que éste es un avance tecnológico de la industria de microprocesadores que es aprovechada por los sistemas operativos. El objetivo es evitar que un programa pueda ser inyectado en un sistema por medio de un desbordamiento de buffer. Para ello se dividen, en tiempo de ejecución, las páginas de la memoria en dos clases: Páginas de ejecución en las que se cargarán los procesos o páginas de NO ejecución donde se van a almacenar datos y/o parámetros de llamada a procedimientos. Para realizar esto las páginas de memoria llevan asociadas un NX (Non eXecute) que indica si se puede ejecutar lo que esté allí o si por el contrario, nada que esté almacenado en esa zona de memoria puede ser ejecutado.

El realizar esta división y marcado de las páginas permite, que, aunque se produzca un desbordamiento de buffer, este nunca podrá ser utilizado para inyectar un código a través de un parámetro, con lo cual estamos garantizando que el sistema no ejecuta nada que no esté ya introducido previamente.



Imagen 1: Desbordamiento de Buffer

Aplicar DEP por hardware previene que se pueda introducir código inyectado, si el contador de programa se quedara apuntando a una zona de memoria marcada como NX el sistema intentaría recuperarse y si no pudiera se produciría una parada. Debido a esto, es posible que ciertas aplicaciones, que utilicen la inyección de código como forma normal de trabajar dejen de funcionar correctamente. No es una práctica correcta de desarrollo pero en algunos casos se utiliza. Para intentar garantizar la compatibilidad de aplicaciones de este tipo se pueden crear listas blancas en Windows Vista.

DEP por Software

Como protección adicional, DEP en Windows Vista, tiene una versión basada solo en software que vino ya en XP SP2 y cuyo objetivo es garantizar la integridad de las funciones que son invocadas en el tratamiento de los mensajes de excepciones que deben ser gestionados por el sistema operativo. Para ello se comprueba la integridad de los binarios del sistema que se encargan del tratamiento de los mensajes de error.

SafeSEH (Safe Exception Handler)

Esta es una opción del linkador que se puede usar en Visual C++ para poder comprobar, de forma segura, que las funciones de tratamiento de excepciones de un determinado programa son las correctas. Para ello el ejecutable lleva almacenada la tabla de las funciones con las referencias a las funciones que deben procesar cada uno de los mensajes de excepción. El sistema operativo comprobará

si el manejador de esa excepción corresponde con el que marca el programa en la tabla de manejadores y si no es así, matará el proceso. Estas opciones son utilizadas en conjunción de la protección DEP por software.

Configuración en Vista

Para configurar las opciones de DEP en Windows Vista deberemos acceder a la opción de configuración en:

1. Panel de Control
2. Sistema y Mantenimiento
3. Sistema
4. Configuración Avanzada
5. Avanzadas
6. Opciones de Rendimiento
7. Data Execution Prevention

Tras una petición de Microsoft y en concreto de Michael Howard, todos los equipos que vendrán con Windows Vista en versión OEM vendrán por defecto con DEP Activado.



Imagen 2: Prevención de Ejecución de Datos

La protección contra Desbordamientos de Buffer en Windows Vista (IV de IV)

Cuarta Protección: Ocultación de Información

Con las tecnologías vistas hasta el momento se ha pretendido, en primer lugar que no se produzcan los fallos en el código que originan los desbordamientos de buffer, que no se puedan sustituir las funciones de tratamiento de errores y que no se puedan meter códigos en la zona de memoria destinada a datos para evitar la inyección de programas no deseados dentro del sistema. Sin embargo un atacante no necesita inyectar un troyano si puede abrir una conexión desde dentro del sistema que le conecte contra un socket en su equipo, es decir, si puede configurar una conexión reversa. Y para eso no necesita inyectar ningún código, le basta con invocar una función del sistema operativo para abrir un socket.

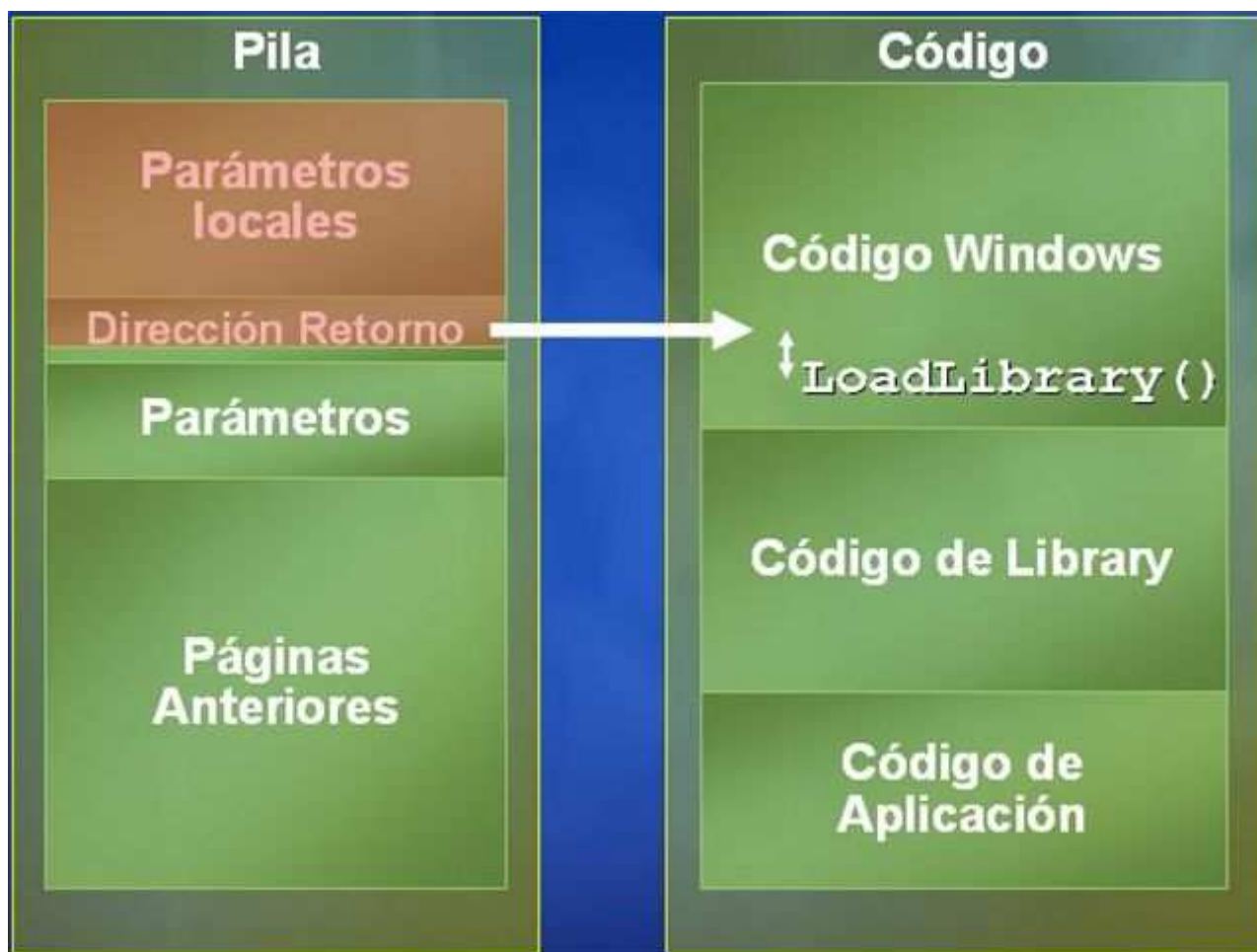


Imagen: Invocación de una función conocida del sistema

Pointer ofuscation

La primera tecnología de protección para evitar que se invoquen funciones conocidas se añadió en Windows XP SP2 y Windows Server 2003 SP1. Por supuesto esta tecnología también funciona en Windows Vista.

La idea es evitar que se vea la dirección de cualquier función que se usa en el cuerpo de un programa, por ello, se utilizan las funciones: `EconcePointer` /

DecodePointer y EncodeSystemPointer / DecodeSystemPointer para ofuscar la información en el código.

Las funciones EncodePointer y EncodeSystemPointer generan una dirección ofuscada a partir de realizar un XOR entre la dirección real de la función que se desea invocar y un número dinámico generado por el sistema operativo.

Cuando se desea realizar la llamada a la función se hace mediante las funciones DecodePointer y DecodeSystemPointer. Si un atacante desea suplantar la llamada a una función por una suya debe saber como codificarla para que cuando sea decodificada corresponda con la función que él quiere llamar. Nada sencillo.

El uso de estas tecnologías no previene solo contra los ataques de desbordamiento de buffer sino contra todos aquellos que, no pudiendo modificar la dirección de retorno de la llamada buscan obtener el control mediante la modificación de cualquier llamada a función que vaya a ser invocada, ya que cogerá el control del programa.

ASLR (Address Space Layout Randomization)

Para evitar que el atacante sepa la dirección de memoria dónde se encuentra una función que desea invocar, la tecnología ASLR intenta cambiar en cada ejecución la posición exacta de la misma dentro de la memoria. Para ello se utiliza una función que se denomina de entropía (máximo desorden) que le asigna en cada ejecución de la aplicación una dirección diferente dentro de un rango de 256 posibles.

Es decir, se ejecuta el programa A y se carga en la dirección FF000FFF, se cierra el programa y se vuelve a ejecutar. Cuando se carga en memoria ASLR le asigna la dirección FF000ABB, por ejemplo.

Con esto se intenta que no se pueda predecir la dirección donde se pueden encontrar los programas que tiene en ejecución un determinado sistema.

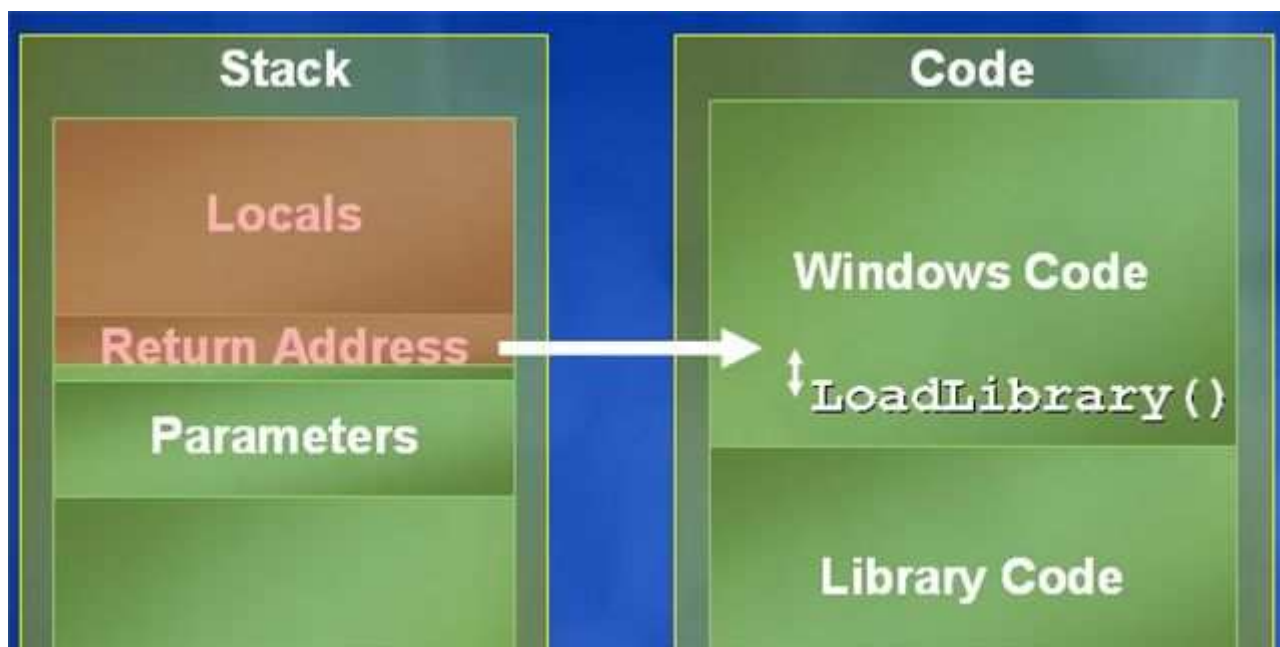


Imagen: ASLR le asigna una dirección diferente en cada ejecución

Conclusión

Garantizar que un sistema no va a tener fallos de desbordamiento de buffer en alguna de los millones de líneas que conforman el sistema operativo es mucho

decir, pero el uso de el SDL (Secure Development Lifecycle), la compilación con /FxCod y /SafeSEH, la aplicación de DEP (Data Execution Prevention) con el bit NX (Non Execute) por Hardware y por Software para la protección de integridad en el tratamiento de errores, la ofuscación de los punteros a funciones y la ejecución aleatoria con ASLR ayudan a que el sistema se encuentre mucho más fortificado contra los fallos de Buffer Overflow.

Bitlocker (I): Seguro más alla de su uso

Ante todo un saludo a todos aquellos que se aventuren a leernos a través de estos post, en los que iremos desgranando diferentes temas, y algunos de ellos muy curiosos. Para este primer post os propongo una reflexión tras la cual iremos desentrañando alguna tecnología de seguridad interesante que incorpora Windows Vista.

Cuando finalizamos el ciclo de vida de un equipo, ¿qué hacemos?, simplemente nos deshacemos de él. Pero realmente tenemos en cuenta cuál es el destino del mismo, quien lo puede manipular,..., total si nosotros no lo vamos a utilizar que más da, ya tenemos una copia de los datos y los habremos pasado a nuestro nuevo y flamante equipo. Otras veces un equipo estropeado es enviado a un servicio técnico y desconocemos quien va a manipular la información; o simplemente hemos dejado olvidado nuestro equipo portátil en cualquier lugar o nos lo han [robado](#), ofreciendo eso sí, un acceso total a la información que este contiene (claro y en muchas circunstancias como no con un descriptivo fichero llamado password o con fotos comprometidas,... ya podemos imaginar las consecuencias).

Algunas veces es posible que el propietario de un equipo que se va deshacer de él pudiera llegar a formatear el disco (las menos), pero desconoce realmente, que este mecanismo no garantiza que alguien pudiera llegar a extraer los datos que él tuviera anteriormente almacenado. Algunos estudios revelan informaciones alarmantes que determinan que un gran número de datos médicos, de cuentas corrientes, datos financieros, de empleados, clientes, etc., acaban en cubos de la basura junto a los equipos deshechados o bien camino de algún supuesto país, tras haber hecho una importante donación de los mismos a una nueva Fundación que ha aparecido vaya usted a saber donde, requiriendo de mi empresa los ordenadores en deshuso, y todo esto claro está sin que hagamos ningún tratamiento para la eliminación de los datos almacenados (Dios mío mis datos médicos o financieros camino de... y quien habrá detras de estos envíos).

Dos graduados del Instituto Tecnológico de Massachussets realizaron un [estudio](#) con objeto de determinar el alcance de esta problemática, para lo cual compraron 150 discos duros de segunda mano y le aplicaron técnicas de análisis forense para extraer los datos almacenados. En muchas de las circunstancias estos datos no se encontraban ni eliminados y en los que así era, pudieron extraerlos mediante aplicaciones para la recuperación de ficheros. De los discos duros consiguieron extraer una cantidad significativa de datos de tipo confidencial.

Y ahora ¿qué?

Windows Vista en sus versiones Enterprise y Ultimate, incorpora una nueva funcionalidad que entre otras posibles características podría paliar los anteriores escenarios que habíamos planteado: Bitlocker. Este nuevo sistema garantiza la confidencialidad de los datos almacenados en el disco mediante cifrado. Bitlocker utiliza AES (Advance Encryption Standard) como algoritmo de cifrado en modo CBC (Cypher Block Chaining) y con objeto de evitar los ataques por manipulación de datos cifrados se incorpora un difusor adicional independiente de AES-CBC.

Los mecanismos de seguridad implementados por Bitlocker se complementan mediante unas nuevas especificaciones de seguridad hardware Trusted Platform Module (TPM). Este nuevo chip TPM proporciona una plataforma segura para el

almacenamiento de claves, password o certificados, haciendo más difícil el ataque contra las mismas. Aunque nuestros equipos no dispusieran de este mecanismo de seguridad las especificaciones de Bitlocker admiten su funcionalidad sin el chip TPM, pero ¿funciona igual?

En post posteriores trataremos los diferentes aspectos técnicos empleados para el cifrado de la información, destriparemos Bitlocker y las funcionalidades que nos reporta el uso del Chip TPM si disponemos del mismo.

Bitlocker (II): La Concienciación para la Seguridad de los Discos

Bitlocker proporciona mecanismos para garantizar tanto el cifrado de la unidad que contiene el sistema operativo, proporcionando de esta manera, seguridad adicional frente a amenazas externas directas o indirectas. De esta forma [nadie](#) ajeno al sistema podría conseguir la información almacenada en la partición del disco duro cifrado mediante Bitlocker. A pesar de las mejoras que este mecanismo proporciona no hay que obviar otras metodologías como [EFS](#) o [Right Management Services](#), puesto que Bitlocker solo condiciona este mecanismo de seguridad, a la información almacenada sobre el disco cifrado y en ninguna instancia a todos los datos que salen fuera de él como ficheros compartidos, almacenados en discos externos, etc. El cifrado del sistema se puede combinar mediante cifrado de mecanismos Software y/o Hardware.

¿Combinar Hardware y Software?

[Bitlocker](#) proporciona un filtro en el Stack del sistema de Windows Vista encargado de realizar los procesos de cifrado y descifrado de una forma totalmente transparente, cuando se escribe o se lee en un volumen protegido. Este mismo mecanismo interviene también cuando el equipo entra en el modo de hibernación. Mediante este mecanismo se garantiza también la seguridad del fichero de paginación, los ficheros temporales y resto de elementos que puedan contener información sensible. Una vez que el mecanismo de cifrado ha sido puesto en marcha, la clave de cifrado es eliminada del disco y posteriormente almacenada en el Chip TPM. Con objeto de garantizar que un posible ataque al sistema hardware mediante posibles vulnerabilidades, se proporcionan mecanismos de autenticación mediante sistemas adicionales tales como el uso de Token (llave USB) o una password (PIN) para evitar esta posibilidad.

El uso combinado de mecanismos hardware y software evitan determinados ataques que tienen como objetivo la modificación de datos que aunque cifrados podrían provocar una vulnerabilidad en el sistema, siendo explotado posteriormente para poder acceder al sistema. La implementación de Bitlocker requiere de la existencia de condiciones para su implementación. Un factor importante es que el sistema necesita dos particiones NTFS una de las cuales, la partición activa, que albergará el sistema de arranque no se encontrará cifrada. Bitlocker también proporciona mecanismos para garantizar que no se han producido modificaciones en el sistema de arranque del sistema, tales como los que pueden provenir de ataques tipo malware que pudieran producir un ataque colateral o el control del acceso al sistema.

Puesto que bitlocker proporciona diferentes mecanismos de implementación, cada escenario dependerá de determinados factores, algunos de los cuales pueden ser tan curiosos como la predisposición a la seguridad de sus usuarios. Imaginemos que se implementa bitlocker con autenticación por Token (almacenada en un Memory Stick USB) para un portátil y cuando pierdes o te roban el portátil ¿qué?, pues resulta que el USB iba en el mismo maletín y a rezar para que el que nos haya robado el portátil cuando vea el USB y que Vista no arranque en una situaciones. Aunque alguno piense menuda tontería, eso es imposible que pase... tampoco pensaba que iba a ver nunca en una SmartCard el código PIN escrito con rotulador

indeleble y lo he visto (sino tiempo al tiempo, y es que más de uno se planteará donde llevar el Memoty Stick). En el siguiente post analizaremos estos escenarios.

Bitlocker (III): Escenarios para la implementación

¿Dónde implementaremos Bitlocker?

Uno de los problemas que se nos plantea cuando decidamos implementar Bitlocker, es cual es el escenario previsible en el que podemos implementarlo y como será la forma idónea para realizarlo. Evidentemente cuando decidimos por la implementación de un mecanismo de seguridad como el cifrado deberemos tener presente si es necesario el mismo o para que lo vamos a hacer, si esta es una máquina convencional usada solamente como soporte de aplicaciones pero no almacenamos en ella ningún dato de interés.

Supongamos los equipos estándar de una empresa. Estos por regla general son utilizados solo como soporte para la ejecución de las aplicaciones, ya que los datos importantes de la empresa se encuentran almacenados en un servidor bien resguardado en el CPD (o así debería ser...) Habrá que tener presente también los elementos adicionales que pudieran quedar almacenados en la máquina que por comodidad pudiéramos dejar almacenados, tales como contraseñas de navegación, de aplicaciones enmascaradas por los dichosos asteriscos, los correos, etc. Cual importante es esta información en manos de alguien que busca datos de nuestra empresa, implicaría prever la opción para el cifrado de estos discos. Una de las mejoras que nos reporta el sistema de Bitlocker en máquinas coexistiendo en un Dominio, es que los mecanismos para la recuperación de las contraseñas, obtienen ventaja de las funcionalidades aportadas por el Directorio Activo.

Si la circunstancia la evaluamos desde el punto de vista de una persona que viaja muy a menudo, con un portátil que parece ya una extensión más de su propio cuerpo (alguno se sentirá identificado seguramente), el hecho de tenerlo cifrado sería una opción más que interesante, máxime cuando puedan llevar informes de clientes, datos de la empresa, etc. Un eventual robo o pérdida, solo significaría precisamente eso: el robo o la pérdida, pero pasaría a un significativo segundo plano los datos que portaran. La implementación dependerá fundamentalmente si el dispositivo presenta o no Chip TPM. Si no lo lleva la única opción posible es el uso del almacenamiento de la clave en un USB (cuidado donde lo llevamos no sea que se rían de nosotros).

¿Y el usuario doméstico? Salvo para algunos casos significativos, resulta evidente que este método no será el empleado en los hogares, principalmente porque la orientación de los sistemas operativos de índole doméstico no portan esta funcionalidad. Un elemento previsible aunque negativo, es que este sistema pudiera dificultar elementos para el análisis de un equipo donde es requerido determinar si desde él, se ha cometido un posible delito.

Y en todos estos posibles escenarios, ¿tengo que equiparme con un nuevo PC, para soportar la infraestructura de Bitlocker? La respuesta es NO, aunque podremos obtener mejoras significativas si optamos por utilizar un equipo que cuente con el Chip TPM. Para todos aquellos que desean utilizar el cifrado y no poseen el Chip, encontramos una directiva de seguridad bajo la cual podemos condicionar el uso de Bitlocker sin el citado Chip. Por defecto el sistema solo admite la configuración de Bitlocker si el equipo cuenta con el Chip.

Configuración de Bitlocker sin TPM en Vista

Para utilizar Bitlocker sin TPM

1. MMC

2. Directiva Equipo Local
3. Configuración del equipo
4. Plantillas Administrativas
5. Componentes de Windows
6. Cifrado de Unidad BitLocker

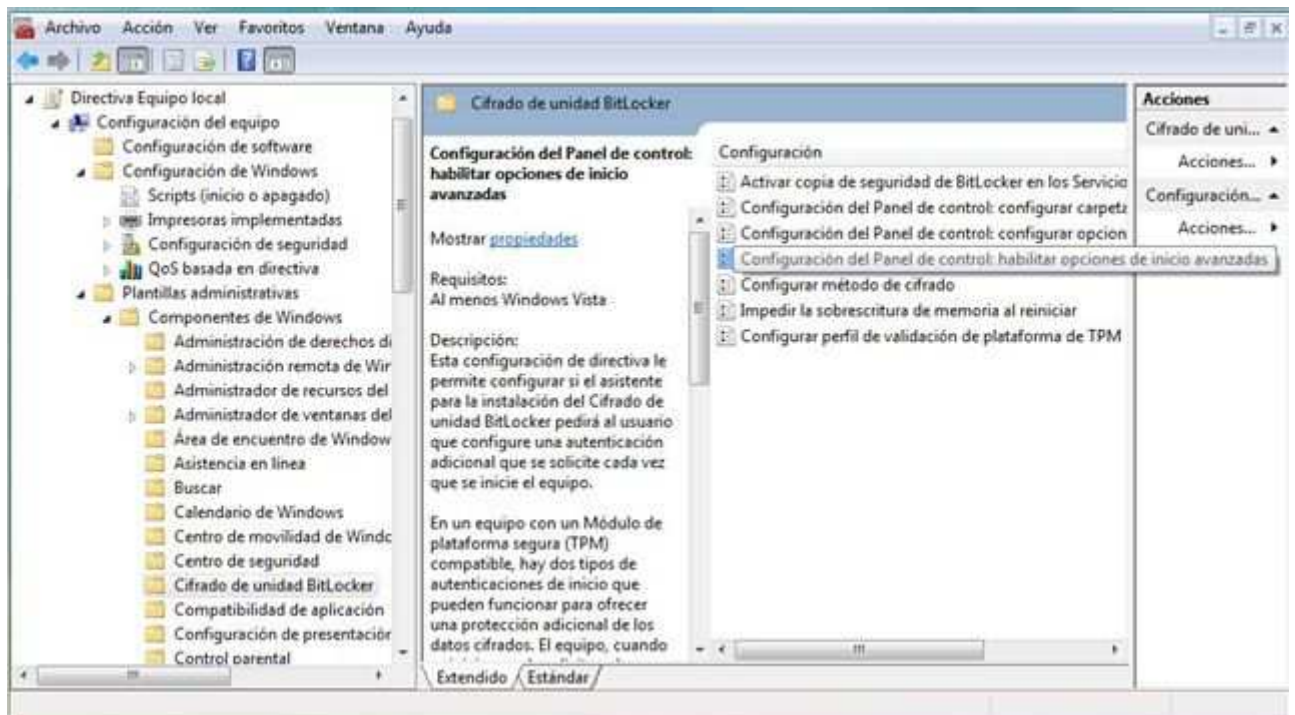


Imagen 1: Directiva de Seguridad

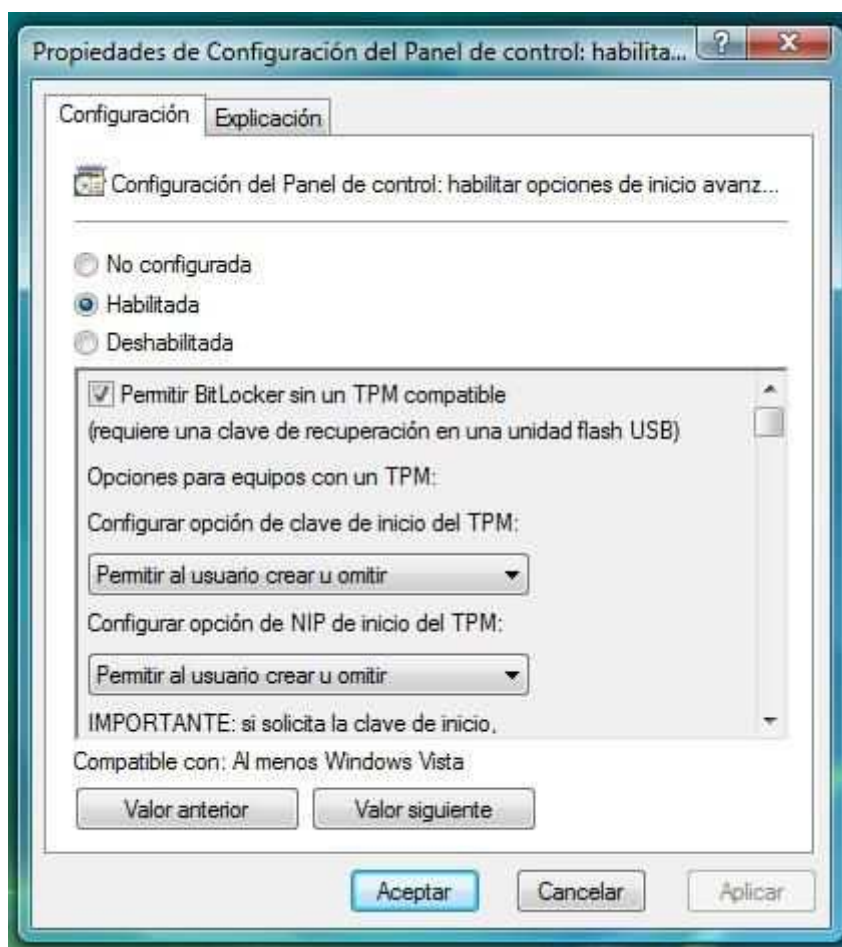


Imagen 2: Configuración Bitlocker sin TPM

Chequeo Médico

Al finales del año 2004, gracias a ser MVP de Seguridad en Microsoft fui invitado a asistir al Security Summit que nos ofreció durante una semana la gente de Seguridad en Redmond. Allí, entre muchas cosas, nos contaron el funcionamiento de SenderID, lo que sería el WSUS y también el NAP. NAP son las siglas de Network Access Protection y es de lo que quería hablar este mes porque ya casi está aquí, entre nosotros.

La idea de Microsoft con respecto a esta tecnología consiste en aunar en la industria una forma avanzada y extensible de controlar la configuración segura de todas las máquinas que se le conectan a un sufrido administrador en su red. La idea proviene de las Redes de Cuarentena (Quarantine Networks) de las que disponíamos en las conexiones VPN. En esta tecnología, Redes de Cuarentena, cuando un cliente VPN se intenta conectar a la red principal se lanzan una serie de scripts en la máquina cliente que comprueban la configuración de la misma para ver si cumple la "Política de Salud" exigida por el administrador. A ningún administrador le gusta que se conecte a su red un equipo portátil que está rodando por el mundo, sin parchear, sin tener el firewall conectado o sin las firmas del antivirus actualizadas ya que puede ser un foco de problemas en la red principal.

Si el cliente VPN no cumple la Política de Salud marcada por el administrador entonces no se le conecta a la red principal sino a una red paralela, llamada "Red de Cuarentena" donde va a poder acceder a los "Servidores de Remediación" (Remediation Servers) que serán, lógicamente, los necesarios para arreglar aquello que hace que un equipo no cumpla la política, es decir, el WSUS para que

actualice los parches, el servidor de gestión de software si la distribución está controlada por el administrador, el correo mediante acceso Web por si es una "urgencia", el servidor de antivirus o lo que el administrador considere necesario.

Esta idea de Redes de Cuarentena estaba bastante avanzada también por Cisco y Trend Micro, así que lo mejor sería trabajar de forma conjunta para poder ofrecer una solución interoperable de futuro. Network Admission Control de Cisco-Trend Micro y Network Access Protection de Microsoft son la evolución de las Redes de Cuarentena y son interoperables como ya nos anticiparon a principios de Septiembre de este año.

En esta nueva tecnología ya no pensamos en una conexión de un Cliente VPN sino en una conexión a nuestra red, ya sea en un Switch, en un Punto de Acceso Wireless, mediante una conexión VPN o de cualquier otra manera. En el momento que la máquina se conecta a la red el Cliente NAP que debe correr en la máquina genera un documento del "Estado de Salud" (Statement of Health "SoH") de la máquina. Éste es enviado al "Servidor de Política de Red" (Network Policy Server "NPS"), que es el sustituto en Windows Server "Longhorn" de IAS (Internet Authentication Server) en Windows Server 2003. El "Doctor" NPS comprueba con los Servidores de Políticas si el Estado de Salud (SoH) de nuestro "paciente" es correcto para poder estar conectado a la red a la que quiere conectar. Si es un Estado de Salud correcto se le permite la conexión y si no, pues decidimos que hacer. O bien le situamos en una red de remediación o bien optamos por no permitirle la conexión o en otro caso, directamente, en reconfigurar de forma "sana" la máquina en el acto.

Esta rápida descripción del funcionamiento nos permite hacernos dos preguntas. La primera: ¿Depende de donde conectemos la máquina cliente podremos tener diferentes requerimientos de salud? La respuesta es: Por supuesto, es genial, podemos definir la red como zonas distintas de seguridad que nos exigen distintos niveles de salud. La segunda pregunta que seguro que a todos nos viene a la cabeza es: ¿Cómo forzamos la política para que no se conecte una máquina cliente que no cumple el estado de salud requerido? Para ello tenemos varias formas de hacerlo.

1.- Servidor DHCP: Es la forma más sencilla y menos "segura" pero la tecnología NAP intenta ayudar a los administradores y usuarios a no ser vulnerables, no es una tecnología para luchar contra usuarios maliciosos, aunque ayude a ello. En este entorno cuando el cliente DHCP realiza la petición el servidor comprueba el SoH y si no cumple el nivel de salud, se le configura para trabajar en la red de remediación o directamente no se le concede una configuración de red válida.

2.- Servidor VPN: Para aquellas máquinas que se conectan mediante clientes VPN se aplica un funcionamiento similar al de las predecesoras Redes de Cuarentena. Usamos el servidor VPN para configurar al cliente dentro de una red de remediación o directamente no le permitimos la conexión.

3.- 802.1x: En todos los switch de la conexión Lan o VLAN de la organización, cuando algún cliente se conecta a un puerto de un switch o a un Punto de Acceso Wireless, mediante el protocolo 802.1x se envía al servidor NPS el SoH de la máquina cliente. Si no cumple la Política de Salud entonces se deniega la conexión al puerto o se le configura de forma dinámica en otra VLAN para la remediación.

4.- IPSec: En este caso el certificado X.509 para IPSec se emite de forma dinámica cuando una máquina es conectada. El proceso es sencillo, primero, el agente NAP genera el SoH que es enviado al NPS que a su vez comprueba si es válido o no con el Servidor de Políticas (PS). Si la cumple un Certificador de Salud genera un

certificado X.509 para comunicaciones IPSec que deberá usar el cliente. En el momento que tenga el certificado podrá comunicarse con todos equipos de la red que también tienen el certificado IPSec y si no, quedará aislado.

Al final la idea es ver como restringir a las máquinas que no están sanas de comunicarse con las sanas. Sencillo.

La solución NAP viene con Windows Server "Longhorn" para la parte servidora y preparada para clientes Windows Server "Longhorn" y Windows Vista aunque se tiene prevista una implementación NAP para Windows XP SP2. No obstante clientes compatibles NAC existen ya para Windows 2000/XP SP2. ¿Muchas Siglas? ¡Cómo los médicos!

Más info: [Technet](http://technet.microsoft.com)

Bitlocker (IV): Algoritmos de autenticación para el cifrado de Disco

Cuando se determina la necesidad de implementar un mecanismo para establecer un cifrado, así como el mecanismo para su descifrado tiene que cumplir ciertas normas y criterios para no hacerlo inviable:

- No debe repercutir de forma muy negativa en el rendimiento general en procesos de escritura y lectura.
- Debe ser transparente para los mecanismos de funcionalidad de las aplicaciones con las que trabajamos.
- Debe ser lo suficientemente robusto para evitar ataques mediante ataques de permutación o por manipulación de datos y obtención de resultados en texto plano.

A la hora de determinar un sistema de implementación para el cifrado de la unidad de disco para bitlocker, Microsoft tuvo en cuenta determinados factores y evaluó la posibilidad de implementar algunos de estos sistemas de implementación de cifrado. Uno de los elementos que se tuvieron en cuenta es que Bitlocker no debería consistir solamente en un elemento de cifrado, sino que debería garantizar mediante un sistema de autenticación de datos, el evitar que una manipulación de los datos cifrados pudieran introducir una modificación a ciegas, en el código del S.O., provocando una debilidad en el mecanismo de arranque con Bitlocker o para conseguir una escalada de privilegios en el sistema. Además debería evitar el permitir la predicción de la función de cifrado mediante la manipulación de datos cifrados y la obtención de datos en texto plano.

Autenticación MAC

El mecanismo natural de implementación de cifrado para evitar estos mecanismos de ataque, es la utilización de MAC (Message Authentication Code) a cada bloque de datos del disco. El problema que plantea el uso de este mecanismo es que necesitaríamos establecer una reserva de sectores para almacenar el MAC, con lo cual tendríamos un uso limitado en la capacidad de almacenamiento de hasta un posible 50% de almacenamiento. Además bajo las condiciones actuales de implementación de este mecanismo en sistema de altos procesamiento de datos con accesos de lectura y escritura, podremos encontrarnos con problemas de rendimiento o la corrupción de sectores. Si no queremos escribir en sectores x , sin dañar $x+1$ $x-1$ en procesos de caída del sistema no controlados o por pérdida de energía, tendremos que tener en cuenta que en el caso de escribir en un sector x el sistema deberá leer el sector, descriptarlo, encriptarlo y nuevamente escribir todos los sectores que correspondan al bloque. Si falla el sistema cuando se

escriben sectores, en el nuevo bloque pero quedan pendientes otros, entonces todo el bloque puede quedar corrompido.

Autenticación de “Poor-man”

Este es otro de los posibles mecanismos para la implementación de seguridad que permite generar bloques cifrados con un tamaño entre 512-8192 bytes, de tal forma que una leve modificación en uno de los caracteres del bloque modifica de forma aleatoria todo el bloque. Con objeto de evitar el mecanismo de secuenciación moviendo datos cifrados de un sector a otro sector, se generan cambios del algoritmo para cada sector.

De este forma aunque el potencial atacante tuviera acceso a los datos tanto cifrados como en texto plano, la variedad del mecanismo de secuenciación y los cambios en el algoritmo evitan los mecanismos de predicción del sistema de cifrado.

En el siguiente post evaluaremos diferentes mecanismos de cifrado y el mecanismo empleado para Bitlocker: AES-CBC + difusor.

Referencias Externas

[MAC authentication](#)

[Cifrado bloques de disco](#)

Bitlocker (V): AES - CBC + Difusor

Como planteé en el anterior post, existen numerosos elementos necesarios aplicar a la hora de determinar un mecanismo de cifrado, y estos deben garantizarse, de tal forma que el acceso a los datos cifrados deben ser controlados, tanto a nivel lógico, como el impedir los ataques que mediante manipulación arbitraria permitiera el acceso aleatorio a los datos y la obtención del mecanismo de cifrado.

Por mecanismos de rendimiento el mejor sistema que se puede emplear para el cifrado de datos de disco es AES-CBC, pero ya advertimos anteriormente el riesgo de posibles ataques al utilizar únicamente este mecanismo. La decisión finalmente establecía la utilización de AES-CBC para la encriptación primaria y una clave difusor independiente para texto plano. Este difusor tiene como objetivo fortificar frente a los ataques de manipulación, mejor que lo que puede realizar de forma única el algoritmo de AES-CBC.

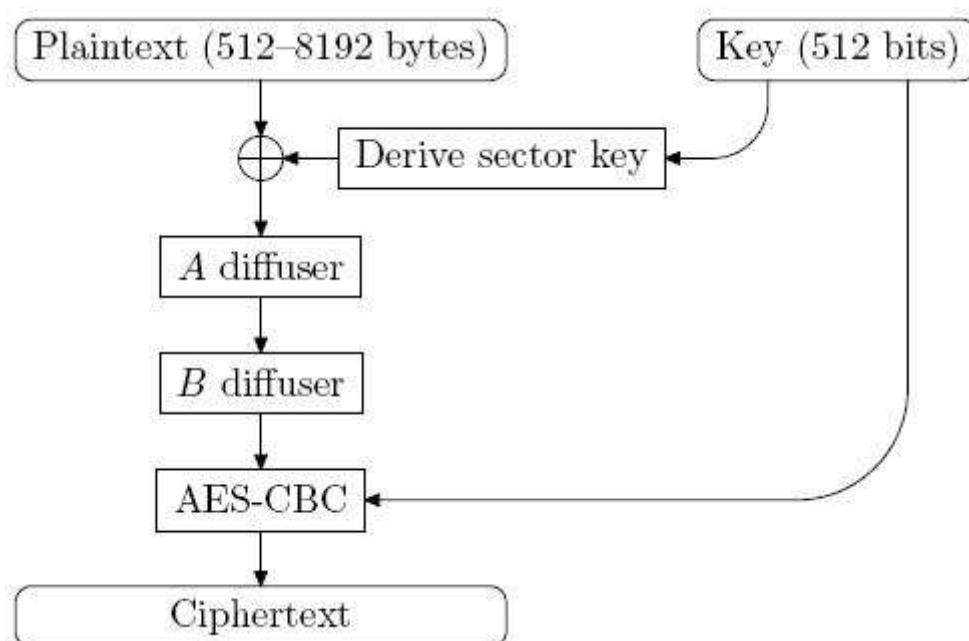


Figura 1 - Funciones de cifrado mediante AES-CBC + Difusor

La figura anterior describe los mecanismos empleados para el cifrado de los datos. Los datos en texto plano son corred con una clave del sector. Posteriormente se le aplican los difusores y finalmente se encripta con el modo AES-CBC. La clave del sector viene definida por la siguiente función:

$$K_S := E(K_{SEC}, e(s)) \parallel E(K_{SEC}, e'(s))$$

donde $E()$ es la función AES de encriptación, K_{SEC} es la clave utilizada (128 o 256 bits, según lo elegido) y $e(s)$ y $e'(s)$, es la función de codificación utilizada en la capa AES-CBC teniendo en cuenta que e' es como e solo que el último byte tiene el valor 128. La clave K_S se repite tantas veces como sea necesario hasta completar una clave del tamaño del bloque y se aplica una función corred sobre el texto plano.

El uso de dos difusores, muy similares pero aplicados en direcciones opuestas, permite la propiedad de difusión correcta en ambas direcciones. Los difusores vienen determinadas en una función donde intervienen el número de palabras del sector y un operador de 4 constantes (diferentes para cada difusor) en un array que especifica la rotación. Este mecanismo tiene como objetivo minimizar el impacto del cifrado en el rendimiento al utilizar un menor uso de ciclos por segundo para realizar el mismo.

Referencias Externas

[RFC 3602 AES - CBC](#)

[Algoritmo AES - CBC + Elephant](#)

SuperFetch (I de IV)

El motivo de este BLOG es desgranar Windows Vista, dar a conocer sus nuevas características, funcionalidades y tecnologías de manera que como profesional dedicado al tema no he podido evitar poner mi granito de arena y mis conocimientos técnicos ante este proyecto al servicio de todos aquellos que deseen leernos y aprender más acerca del nuevo sistema operativo de Microsoft. Por todo ello quizás la mejor manera de empezar este POST es daros las gracias a todos por dedicarnos algo de vuestro tiempo.

Cuando tuve que decidir el tema a tratar en este BLOG pensé en un principio algún tema de seguridad, sin embargo teniendo en el equipo a dos expertos MVP en seguridad hubiera sido un error privar a dichos expertos (Chema y Juan Luís) de atender dichos temas con el valor añadido de toda su experiencia, amplios conocimientos y por qué no, repertorio de anécdotas. Así que he decidido probar suerte con otro de los pilares de Windows Vista junto con la seguridad: el rendimiento. Concretamente en estos días hablaré sobre el nuevo gestor de memoria de Windows Vista: SuperFetch.

Mucha gente le tiene miedo al uso o consumo de la memoria: es un recurso caro, limitado y en ocasiones con una capacidad de expansión escasa, y además, y quizás el elemento más importante de esta ecuación, se encuentra una de las leyendas urbanas más difundidas en el mundo de la informática: "cuanto más consumo de memoria, peor rendimiento", algo que como veremos no siempre es cierto, y menos aun si hablamos de Windows Vista. La polémica está servida por tanto cuando Windows Vista recomienda como mínimo 1GB de RAM, nuestra mente nos engaña surcada por la siguiente deducción: "Si Sistema Operativo recomienda 1GB de RAM como mínimo significa que dispondremos de menos espacio en memoria para nuestras aplicaciones con la consiguiente reducción del rendimiento, aumento del uso de la memoria virtual, lectura del disco duro etc.". Por supuesto mucho técnico no informado y sin conocimiento de causa se echa las manos a la cabeza y alardea de la poca memoria que consume su distribución de linux, un ejemplo de este debate lo encontramos en el siguiente POST del Blog de elladodelmal:

<http://elladodelmal.blogspot.com/2006/11/expertos-no-tecnico-less.html>

Pero la respuesta es fácil: si la principal ventaja de la RAM es que su velocidad de lectura/escritura es muy superior a la de un disco duro, ¿no es lógico pensar que cuanto más información de los programas que vayamos a utilizar tengamos en memoria mejor será el rendimiento? ¿Y si además de lo anterior añadimos que algo fuera capaz de predecir qué vamos a ejecutar en cada momento y cargará previamente la información de esos programas en memoria? Bien, pues ese algo es SuperFetch, un proceso de bajo consumo que gracias a sus capacidades predictivas mejora el rendimiento de nuestro sistema y el tiempo que tardan en abrirse nuestras aplicaciones basándose en nuestras propias pautas de comportamiento (a veces es de agradecer que el ser humano sea un animal de costumbres).

En próximos POST iremos desgranando esta tecnología y otras relacionadas con el fin de obtener una visión general de las mejoras de rendimiento de Windows Vista y para desterrar para siempre aquellos falsos rumores que pudieran circular sobre los requisitos y la optimización de este nuevo sistema operativo, mientras tanto y si queréis ir alimentando vuestra curiosidad os dejo el enlace oficial de Microsoft sobre las nuevas características de rendimiento de Vista.

<http://www.microsoft.com/windows/products/windowsvista/features>

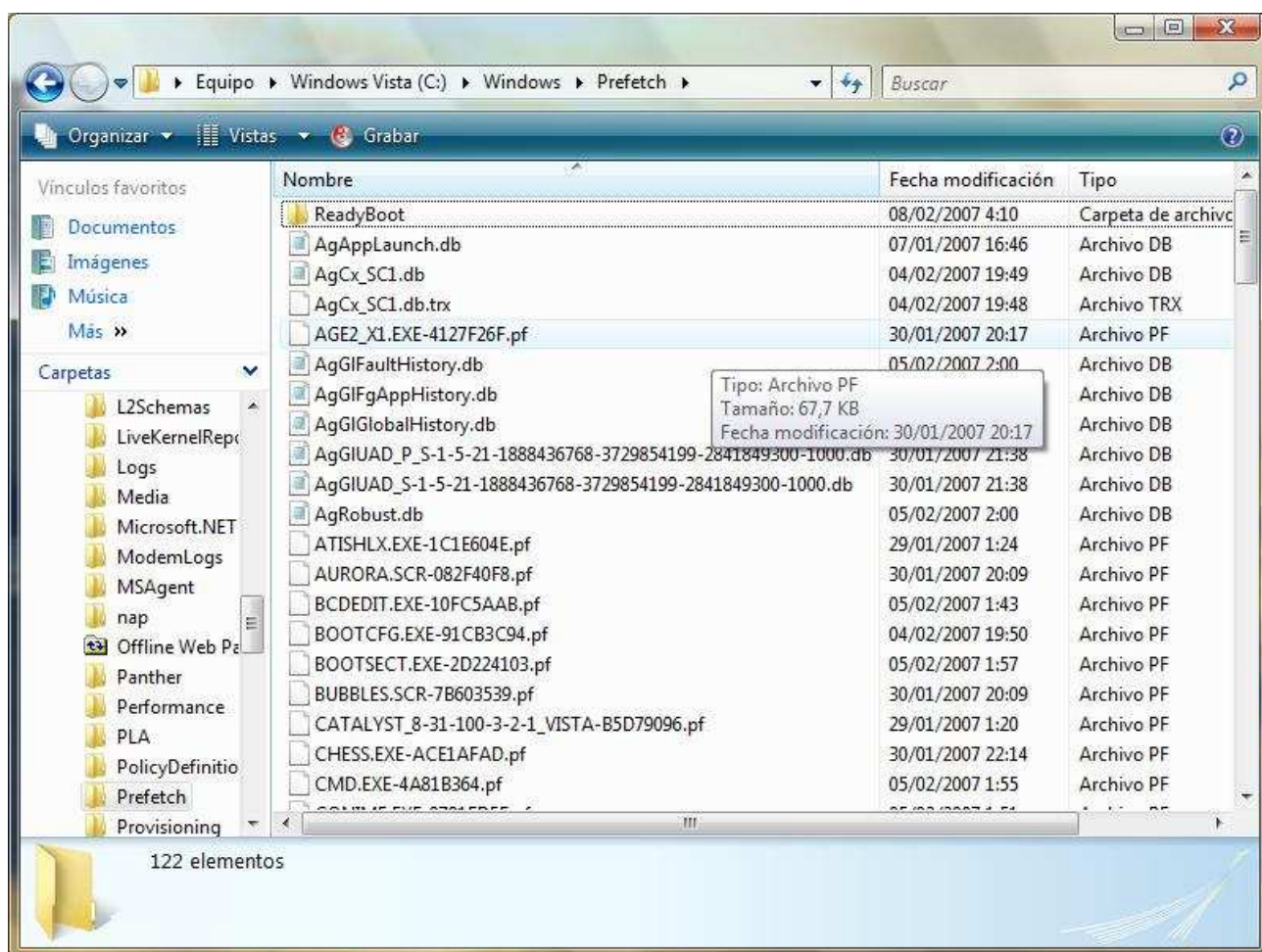
SuperFetch (II de IV)

SuperFetch no es una tecnología que parta de cero, sino que complementa a otra ya existente en Windows XP llamada Prefetch y que en español vendría a significar "precarga".

Prefetch es un término usado en diferentes ámbitos de la informática, por ejemplo se habla de prefetch refiriéndose a las capacidades de los microprocesadores de cargar anticipadamente datos en la cache L1 durante la ejecución de una instrucción con el fin de acelerar al ejecución de aplicaciones, en el ámbito de los navegadores WEB se conoce como Prefetch (concretamente como Link Prefetching) a la capacidad de estos de cargar en caché información de las páginas WEB enlazadas cuando el navegador esta inactivo con el fin de acelerar la navegación

(pudiendo realizar esto de manera agresiva o solo cuando le es indicado en el código html de link), en programación se hace referencia a este termino apuntando a la precarga de información en memoria antes de que sea necesaria con el fin de ganar tiempo de ejecución y por último en sistemas hablamos de Prefetch como un sistema de gestión de memoria usado en varios sistemas operativos (también esta disponible en Linux) que permite optimizar notablemente la carga de aplicaciones y servicios especialmente al arranque del equipo precargando la información de estos en memoria y reduciendo por tanto el tiempo de inicio.

Windows XP y Vista guardan la información de traza de Prefetch en la carpeta %Windir%\prefetch en unos archivos con extensión .pf cuyo nombre esta compuesto por el nombre de la aplicación, un guión y un hash en hexadecimal de la ubicación de dicho archivo, como por ejemplo "NOTEPAD.EXE-2F2D61E1.pf" ("NTOSBOOT-B00DFAAD.pf" en el caso del archivo de arranque) y cuyo contenido no es más que una serie de referencias a los ficheros y directorios que leen las aplicaciones al iniciar, así como sus metadatos. Para crear estos archivos de traza el sistema de gestión memoria comprueba las consultas a las entradas de la MFT (Master File Table) del sistema de archivos NTFS sabiendo de este modo qué archivos son los que se intentan cargar y de esta manera poder precargarlos previamente a la próxima apertura de la aplicación. Así mismo Prefetch se combina con el programador de tareas para realizar una defragmentación y colocación de manera contigua y según el orden de uso de aquellos archivos que vayan a ser utilizados al iniciar las aplicaciones o durante el arranque del equipo; estos ficheros a colocar de manera contigua vienen señalados en el archivo layout.ini de la propia carpeta Prefetch realizándose la labor de defragmentación con una periodicidad de 3 días en momentos de baja actividad del equipo.



Sobre la carpeta Prefetch y sus propiedades existen diferentes leyendas urbanas en forma de trucos para mejorar el rendimiento de Windows, podéis echar un vistazo a algunas de ellas en el siguiente enlace:

<http://mywebpages.comcast.net/SupportCD/XPMyths.html#Optimization>

Este sistema de Prefetch de XP combinado con SuperFetch es el usado por Windows Vista si disponemos de menos de 700MB de memoria RAM, si disponemos de una mayor cantidad de memoria se continua usando el sistema Prefetch y SuperFetch pero añadiendo a la ecuación el sistema ReadyBoot (no confundir con ReadyBoost).

ReadyBoot es otro añadido al rendimiento de Windows Vista y es el sistema utilizado para reducir el tiempo de arranque en caso de disponer de más de 700MB de RAM. ReadyBoot guarda su información en una carpeta con ese mismo nombre dentro del directorio Prefetch de Windows Vista y realiza un seguimiento de los 5 últimos arranques cuyos archivos de traza (de extensión .fx) guarda en el directorio anteriormente citado con el objetivo de usarlos posteriormente para generar un plan de arranque optimizado. Los parámetros de configuración de ReadyBoot los podemos encontrar en la siguiente clave de registro:

HKLM\System\CurrentControlSet\Services\Ecache\Parameters

Bueno, a toda esta ecuación sobre precargas en memoria habría que añadir la inclusión en la carpeta prefetch de archivos de traza de aplicaciones enteras en función del comportamiento del usuario, es decir: SuperFetch.

SuperFetch es un servicio disponible en todas las versiones de Windows Vista y hace un uso intensivo de la memoria partiendo del concepto de que es muy común hoy en día trabajar con gran cantidad de memoria libre en los equipos modernos, para resolver este desaprovechamiento de memoria Windows Vista carga en esta toda aquella información que probablemente utilizará el usuario, para ello mantiene un historial de su comportamiento por días de la semana e incluso por horas de tal manera que cuando desee abrir alguna aplicación concreta esta se encuentre ya cargada en memoria y el proceso de apertura sea mucho más rápido, aun que como es obvio para uso efectivo de SuperFetch se requiere memoria libre suficiente (de ahí las recomendación de 1GB de RAM). Superfetch está completamente integrado con Prefetch y con el layout.ini, interviene en los procesos de suspensión e hibernación y es un proceso de baja prioridad y consumo que no repercute negativamente en el rendimiento del equipo sino que lo mejora gracias a la innovadora gestión de memoria que realiza. Los archivos de traza de Superfetch se guardan como Ag*.db en el directorio Prefetch.

Superfetch también esta relacionada con la gestión de la memoria virtual relacionándose y gestionando otras dos tecnologías referentes en Windows Vista: el READY BOOST y el READY DRIVE que describiré en mi próximo post.

SuperFetch (III de IV)

Para finalizar el tema de SuperFetch en estos dos últimos post vamos a comprobar dos de sus funcionalidades más interesantes: la gestión de los procesos en segundo plano, y la gestión de caché de disco desde un punto de vista innovador con READYBOOST y READYDRIVE.

Es algo común que dejemos aplicaciones en segundo plano cuando por ejemplo abrimos el explorador o el Messenger mientras estamos editando un documento de Office o abrimos un juego mientras se esta ejecutando cualquier otro programa, y es también común que notemos una reducción en el rendimiento del sistema al intentar retomar dichas aplicaciones y pasarlas a primer plano; esto se debe a que los programas en segundo plano son preferentes para pasar al archivo de paginación del disco duro, lo cual, en caso de falta de memoria, supone que cada vez que deseemos volver a traer dicha aplicación a primer plano obtengamos una

considerable reducción en el rendimiento del sistema. La situación anterior también es aplicable cuando hacemos uso de la característica "[cambio rápido de usuario](#)" y deseamos volver a la sesión que dejamos iniciada anteriormente ya que la información de la sesión inactiva es paulatinamente trasladada a la memoria virtual según se va necesitando más memoria. Superfetch gestiona los procesos en segundo y primer plano para reducir en todo lo posible esta pérdida de rendimiento, la manera en que logra esto es bastante intuitiva: vuelve a cargar la información del proceso en memoria cuando volvemos a tener disponibilidad de esta (normalmente al cerrar un programa) lo cual supone que por ejemplo en un entorno de escasa memoria, volver de Internet Explorer a Microsoft Word tras haber cerrado Windows Mail (el programa que viene a sustituir a Outlook Express en Windows Vista) sería mucho más rápido que con sistemas operativos anteriores, y de nuevo esto también sería aplicable al sistema de cambio rápido de usuario siendo ideal por ejemplo para volver a la sesión en la que se está ejecutando la mula para aquellos amigos del P2P que tienen que compartir su equipo; pero quizás la aplicación práctica más evidente de todo esto es no ver reducido el rendimiento tras largos momentos de inactividad, como por ejemplo al ir comer en el trabajo o cuando nos llaman por teléfono. Hasta ahora tras habernos ausentado un tiempo notábamos una ralentización de nuestras aplicaciones debido a que la actividad de los servicios y procesos en segundo plano tomaban el control de la memoria RAM relegando a la aplicación inactiva de primer plano al archivo de paginación; aun que esto es el comportamiento ideal (mantiene al microprocesador ocupado al servicio de procesos en segundo plano como la ejecución de un antivirus) tras la finalización de estos procesos la aplicación principal continuaba en el archivo de paginación hasta que sus funciones eran requeridas por el usuario al volver, con la consabida reducción de rendimiento, Windows Vista corrige esta situación gracias a que Superfetch va colocando denuevo en memoria la información del programa en primer plano cuando se libera suficiente memoria RAM por ejemplo al finalizar una aplicación en segundo plano, de esta manera la aplicación queda completamente disponible para el usuario a su regreso.

Bueno, a parte de lo comentado en este post también existe otra manera de aumentar el rendimiento del equipo a la hora de tener que acceder al disco, esta manera es mediante los sistemas ReadyBoost y ReadyDrive, que veremos en mi próximo post.

Por cierto, se están publicando en TechNet Magazine una serie de artículos sobre las mejoras en el Kernel de Windows Vista, yo estoy a la espera de que publiquen la sección de administración de memoria por si pudiera ofreceros aun más información de lo visto hasta ahora. Os dejo el enlace:

<http://www.microsoft.com/technet/technetmag/issues/2007/02/Vista>

SuperFetch (IV de IV): ReadyBoost y ReadyDrive ★★★★★

Como todos sabemos, la desventaja de usar el disco duro como memoria virtual es la significativa reducción en las tasa de transferencia con respecto a la memoria RAM, sobretodo si estamos hablando de acceso aleatorio a la información como suele ser el caso cuando hablamos de información de memoria, de esta manera en disco duros modernos tenemos tasas de transferencia E/S de 80MB/s. en acceso secuencial al disco duro y 1MB/s en el caso de acceso aleatorio (por el movimiento de los cabezales en búsqueda de información), existe no obstante una solución intermedia entre el disco duro y la memoria RAM que nos ofrece una tasa de transferencia de unos 10MB/s en acceso aleatorio a información.: La memoria Flash.

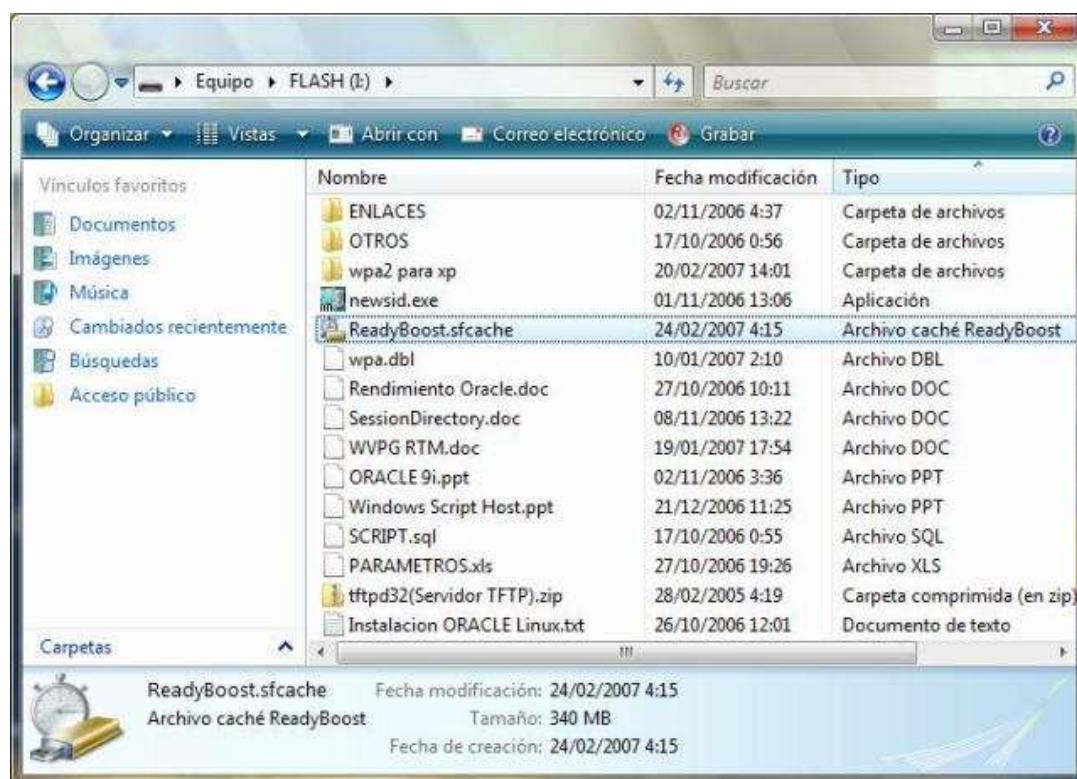
ReadyBoost es un nuevo sistema incluido en Windows Vista que consigue mejorar el rendimiento del equipo haciendo uso de la mayor tasa de transferencia en búsquedas aleatorias y menor latencia de la memoria flash con respecto al disco

duro, de este modo podemos usar dispositivos como llaves USB, memorias SD o Compact Flash para guardar información de caché del disco duro.



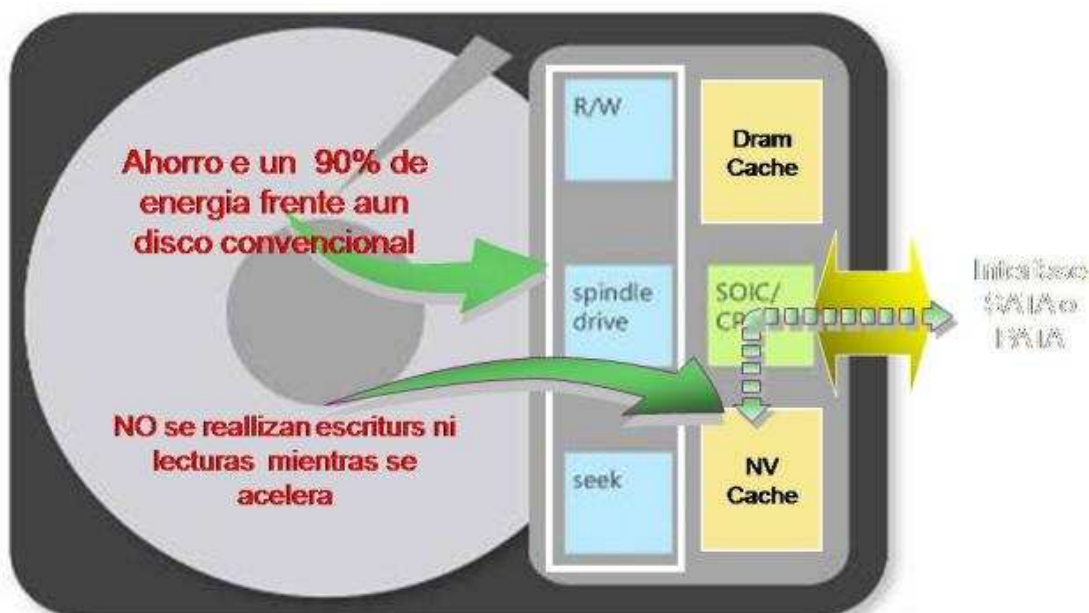
Para poder hacer uso de ReadyBoost nuestra memoria flash debe disponer de al menos 235 MB de espacio libre y ser de rápido acceso (es decir, con una tasa de transferencia adecuada como para ser útil como caché). Como podréis ver en las imágenes añadidas, activar ReadyBoost en una memoria USB es tan sencillo como entrar en sus propiedades e indicar que cantidad de memoria deseamos utilizar para esta funcionalidad, esto quiere decir que no tenemos por qué usar todo el espacio de la memoria flash para almacenar información de caché sino que podemos indicar una cantidad determinada de memoria y continuar usando el resto del espacio para nuestros ficheros, aun que no obstante Microsoft recomienda usar una cantidad de memoria 3 veces superior a la RAM para disfrutar de todas las ventajas de esta tecnología. Otra característica de ReadyBoost es el uso de un algoritmo de escritura optimizado para mantener el tiempo de vida de las celdas de la memoria flash, de hecho, gracias a este algoritmo, si usáramos una memoria flash actual exclusivamente para el uso de ReadyBoost su tiempo de vida oscilaría entre 19,4 y 1823 años. Pero ¿y como se protege esta caché de disco de intentos de lectura no autorizados? pues usando el algoritmo de encriptación AES de 128 bits de tal manera que nos aseguramos que el archivo de caché de ReadyBoost (llamado ReadyBoost.sfcache) solo puede ser leído en el equipo que lo generó inicialmente, y todo esto además con un factor de compresión de 1.8X a 2.3X que garantiza un almacenamiento eficiente al poder guardar más información en menos espacio. Por último quedaría añadir que retirar la memoria flash cuando se esta haciendo uso de ReadyBoost no causa ningún tipo de problema en el equipo ya que es una caché de solo lectura que hace uso del sistema "Write-through" que garantiza que toda la información de la caché del dispositivo flash se encuentra presente en el disco duro, no siendo por tanto necesaria para que el equipo siga

funcionando correctamente.



Sobre estos sistemas de administración de caché de disco duro que realiza SuperFetch hay que hacer mención especial a ReadyDrive que aplica un concepto semejante al de ReadyBoost pero a los discos duros híbridos (discos duros provistos de una caché flash).

Los discos duros híbridos continúan la línea de evolución actual de los discos duros de mejorar el rendimiento y el consumo de energía (hasta el 90% menos de consumo que los discos duros actuales en portátiles) al añadir una caché flash no volátil o NVRAM adicional, que no se pierde la información al apagar el ordenador, a la caché DRAM ya existente. Esto permite, a parte de una mejora en el acceso aleatorio a información como ya se explico anteriormente, realizar lecturas y escrituras en disco mientras este se encuentra acelerando, con la consecuente mejora en rendimiento, especialmente tras la hibernación del equipo.



Superfetch se suma a este tipo de dispositivos híbridos gestionando su memoria flash y aplicando los patrones de uso de aplicaciones para aumentar aun más el rendimiento, así como para mejorar los tiempos de arranque del sistema operativo y de recuperación tras hibernación, todo esto gracias a que al realizar alguno de estos procesos la información necesaria para el arranque o la recuperación es volcada en la NVRAM. ReadyDrive requiere de un mínimo de 50MB de NVRAM, siendo recomendable más de 120MB.

Conclusión:

Como habéis podido comprobar a lo largo de estos post SuperFetch es sin duda una de las grandes novedades incluidas en Windows Vista y un referente en cuanto a tecnologías de rendimiento, de hecho al usar Windows Vista por primera vez a menudo sorprende que, al contrario de lo que esperamos, lleguemos a apreciar una mejoría en el rendimiento de nuestro equipo con respecto a sistemas operativos anteriores.

Continuaré desglosando los aspectos de rendimiento de Windows Vista en próximos artículos, hasta entonces espero haber conseguido despertar vuestra curiosidad sobre esta tecnología y otras muchas que se irán mencionando en este blog.

GPOs en Windows Vista (I de IV): Múltiples políticas locales

En esta nueva serie de POST iremos tratando las mejoras en Windows Vista relacionadas con las políticas de grupo. En el presente post trataremos sobre el soporte de Windows Vista de varias políticas de grupo locales (LGPO).

Un repaso general

Las políticas de grupo o GPO son una de las características más interesantes del directorio activo y de personalización del comportamiento de nuestro equipo o de los equipos de una red. Gracias a las GPO podemos controlar desde qué herramientas están disponibles para los usuarios hasta que permisos NTFS deseamos establecer en nuestras unidades, es decir podemos modificar aspectos como el comportamiento de protocolos, auditorías del sistema, difusión de certificados, restricciones de contraseñas, restricciones de usuario, comportamiento de componentes del sistema y un largo etc. tanto a nivel local como a nivel de dominio, siguiendo la regla de prioridad LSDOU (del inglés **L**ocal, **S**ite, **D**omain, **O**rganizational **U**nit). En el fondo la mayoría de las configuraciones de una GPO son cambios en el registro de Windows del equipo final, el cual va a permitir o restringir ciertas acciones siendo todo ello configurable, con las explicaciones oportunas, a través del MMC (Microsoft Management Console) de edición de políticas de grupo (**gpedit.msc**).

LGPO en Windows Vista

Windows Vista trae consigo una serie de mejoras relativas al funcionamiento y uso de las políticas de grupo que iremos desgranando en sucesivos post, hoy partiremos de la posibilidad de usar varias políticas locales permitiendo así una personalización de estas por usuario o según se pertenezca o no al grupo administradores.

En Windows XP cuando creábamos alguna LGPO esta se aplicaba al equipo y a todos los usuarios, algo que no siempre es lo más óptimo según las configuraciones que deseemos realizar, de manera que por Internet podemos encontrar formas de hacer que las políticas configuradas no afecten a los administradores como se puede comprobar en el siguiente artículo de Microsoft.

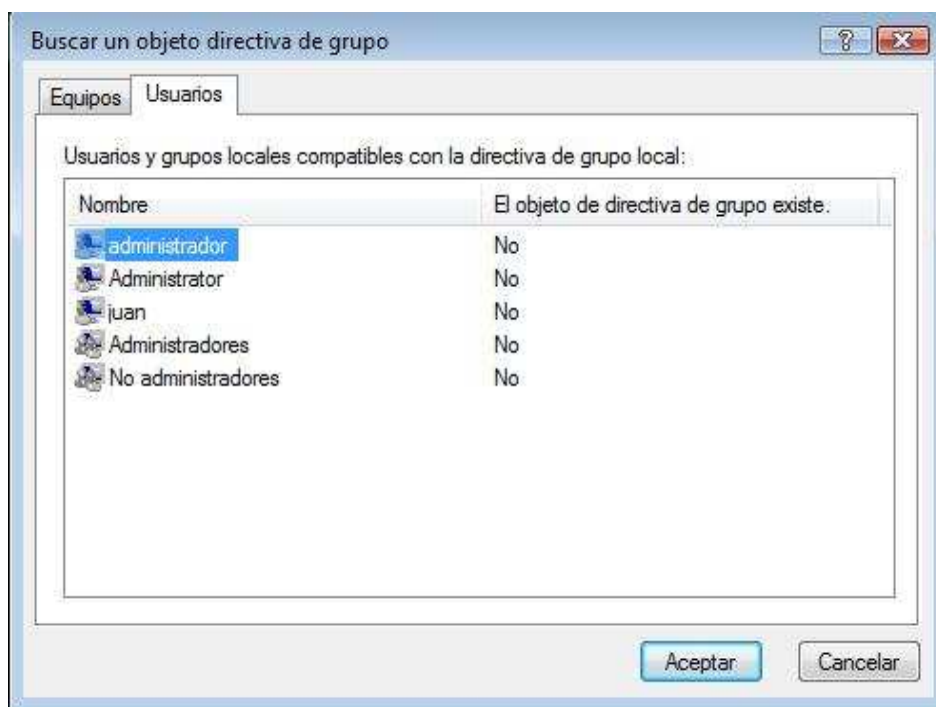
<http://support.microsoft.com/kb/q293655/>

En Windows Vista ya tenemos implementada la posibilidad de realizar una gestión de políticas diferenciada, para ello debemos seguir el siguiente proceso:

Ejecutar MMC > Archivo > Agregar o quitar complementos > Editor de objetos de directiva de grupo

Nota: No confundir "editor de objetos de directiva de grupo" con el complemento de "administración de directivas de grupo" también conocido como GPMC y que ya viene integrado como parte de Windows Vista para administración de directivas en un dominio.

Al pulsar en agregar el complemento y antes de seleccionar cualquier otra opción debemos hacer clic sobre el botón "Examinar" donde además de la posibilidad de aplicar la LGPO a otro equipo distinto desde la pestaña "equipos" nos aparecerá una nueva pestaña llamada "usuarios" donde podremos seleccionar entre las cuentas de usuario existentes o los grupos "administradores" para aplicar políticas propias a usuario con privilegios administrativos y "no administradores" para la creación de políticas que afecten al resto de los usuarios; finalmente solo tenemos que pulsar en aceptar para empezar a editar las políticas de usuario correspondientes (obviamente esto no afecta a las políticas de equipo que se aplican a todos por igual).



Alguno ya habrá caído en la cuenta de que mediante este método existe la posibilidad de existencia de conflictos entre políticas, por ejemplo tendríamos un conflicto al aplicar una política concreta sobre un usuario corriente llamado Pablo y esa misma política con una configuración diferente para todos los usuarios no administradores. Para resolver este tipo de situaciones y partiendo de que quien edita las políticas locales en conflicto es normalmente la misma persona, se concluye que normalmente la configuración deseada es la ultima modificación realizada, de tal manera que Windows Vista aplica aquella configuración que haya sido editada la última.

¿A quien le apetece restringir las funciones del Panel de Control de sus usuarios o modificar el comportamiento de Internet Explorer sin afectar a algún usuario específico? Con Windows Vista ya podeis hacerlo.

En el próximo POST trataremos sobre el cambio en el formato de las plantillas administrativas y su independencia del idioma.

Firewall de Windows Vista I de II

El tiempo parece que avanza cada día más rápido, y junto a él, estamos nosotros. Nunca antes el mundo había sido tan pequeño. Y esto se lo debemos en gran parte a las comunicaciones. Mensajería corporativa, correo interno, streaming para reuniones que antes serían imposibles, VOIP, gente que viene de otras empresas, ejecutivos con sus portátiles que van de una oficina a otra, etc...

Todo esto sería maravilloso si pasase exactamente así. Pero la realidad no es siempre de color de rosas y una red, por pequeña que sea, se puede convertir en un campo de batalla, si no tomamos las debidas precauciones.

Vivimos en un tiempo en el que las redes corporativas y las no corporativas son cada día más complicadas de administrar. Comerciales que conectan sus PDA a los portátiles o equipos de sobremesa, conexión de dispositivos de almacenamiento externo, tener que realizar operaciones en distintas redes, como por ejemplo, aeropuertos, ejecutivos que van de oficina en oficina y necesitan conectarse a la Red, etc..

Desgraciadamente, junto a este tipo de comportamiento, pueden venir a veces acompañados de la mano ciertas amenazas de seguridad como pueden ser Malware, Exploits, Spyware, DOS, Script-Kiddies, etc..

Y aquí es donde entra en acción un Firewall. Algo que ayude a minimizar los riesgos, sin perder un ápice de experiencia.

Antiguamente (y no hablo de mucho tiempo atrás) poniendo firewalls en el perímetro, podíamos permitirnos el lujo de tener a nuestros clientes sin firewall, pero hoy en día, con las nuevas técnicas de ataque, es casi de obligado cumplimiento defender en profundidad tanto a nuestros servidores como a nuestros clientes. Al fin y al cabo ellos serán los que utilicen la tecnología que les podamos proporcionar. Y por qué no aportarles tecnología y seguridad?

Dicho esto, en esta ocasión vamos a hablaros del nuevo Firewall de Windows Vista.

El Firewall de Windows Vista ayudará a mitigar estos desafíos que hemos comentado en líneas anteriores. Y por qué decimos mitigar? Pues porque un Firewall no es una panacea. La seguridad al 100% nunca está, ni estará garantizada. Un Firewall podrá reducir la superficie de ataque a una computadora, pero nunca asegurarla al 100%.

Dicho esto y sin haberme cogido los dedos J, vamos a ver las nuevas características o features del nuevo Firewall de Vista.

- Soporte para IPV6.- Gracias a la nueva pila TCP/IP integrada en Vista y Longhorn, se integra el soporte para esta evolución de TCP/IP.
- **Posibilidad de controlar tanto el tráfico entrante como saliente.**
- **Nueva consola de seguridad basada en MMC (Microsoft Management Console)**
- **NetWork Access Protection (NAP)**
- **Hardening de servicios**
- **Integración con IPSEC**
- **Reglas aplicables a perfiles determinados**
- **Reglas basadas en AD, usuarios, grupos y computadoras**

Profundizaremos en ellos más adelante.

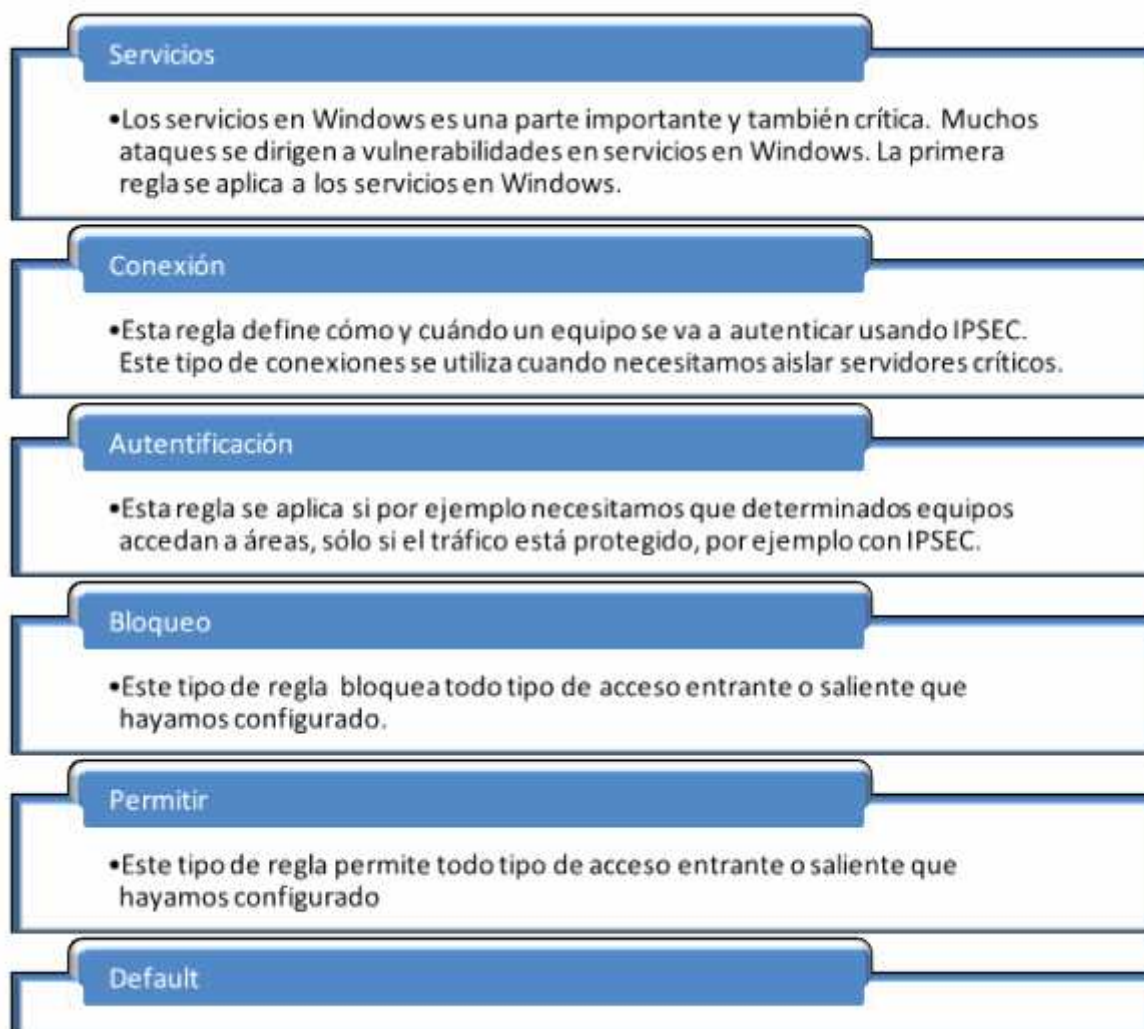
Gracias a la nueva consola de administración del Firewall basada en mmc, se mejora bastante la administración del mismo, pudiéndose crear reglas tanto de entrada como de salida, y configurarlas hasta en el más mínimo detalle.

Los tipos de configuración varían en función de lo que queramos permitir o denegar:

- **Por nombre de aplicación.**- Podemos restringir o permitir a una aplicación la conexión con el exterior
- **Puertos.**- Restringir o permitir a todos o a un número determinado de puertos la conexión
- **Direcciones IP.**- Restringir o permitir a una dirección IP o un rango entero la conexión con algún tipo de aplicación o servicio
- **ICMP o ICMPV6.**- Restringir o permitir algún servicio de este tipo como por ejemplo ping
- **Servicios.**- Restringir o permitir la conexión al exterior de algún servicio
- **Usuarios AD, locales, grupos o máquinas.**- Restringir o aplicar reglas en base a un determinado grupo de usuarios, usuarios de directorio activo o locales

- **Tipos de Interface.**- Aplicar o restringir las reglas en base al tipo de interfaz que tengamos en el equipo, ya sea Wireless, Ethernet, etc...

Las reglas se pueden aplicar de dos formas. A través de una política local, o a través de una GPO, si lo configurásemos desde Directorio Activo. El orden de aplicación de reglas es el siguiente:

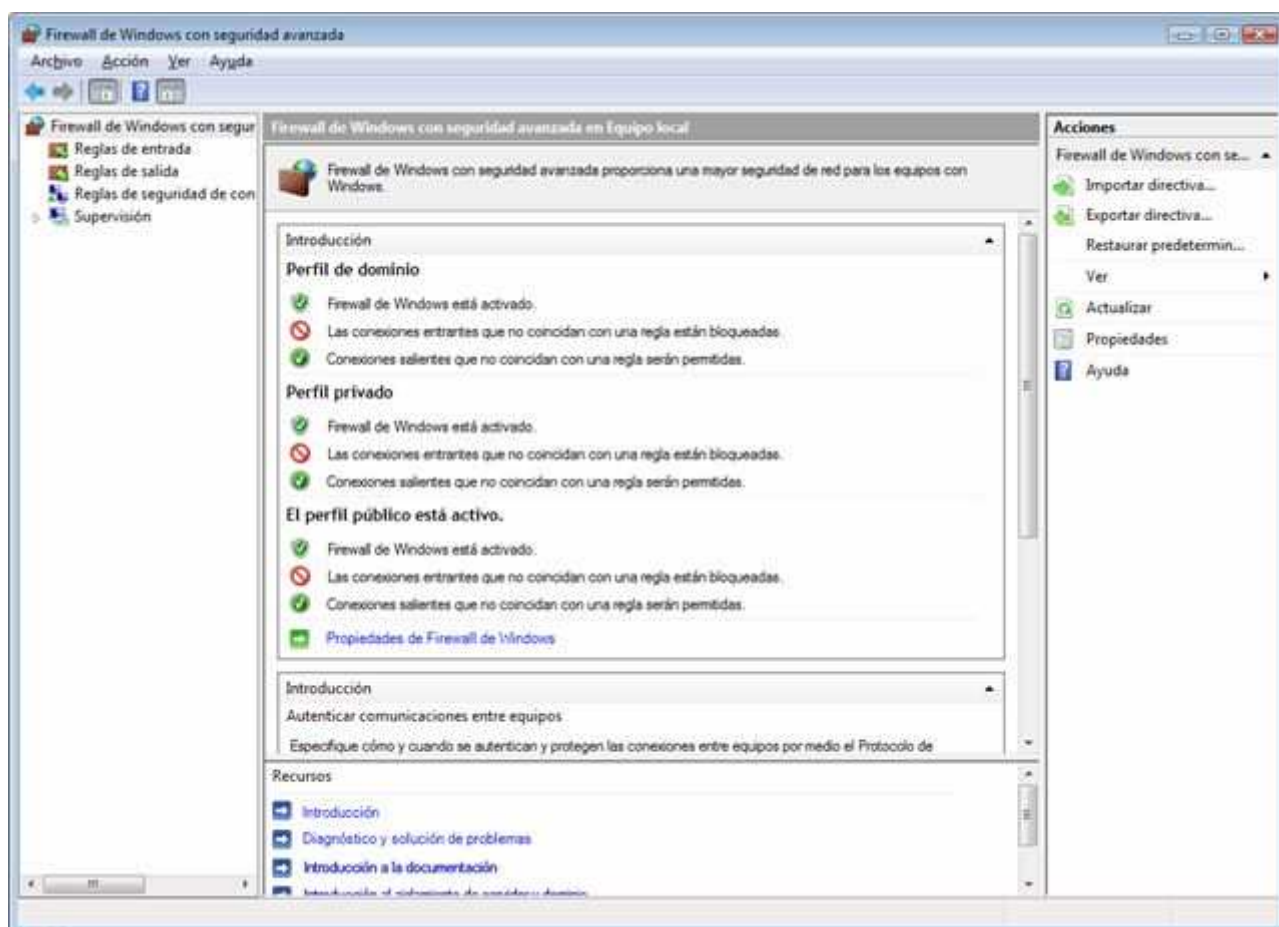


Para acceder a la consola de Windows Firewall podremos seguir varios caminos:

- Desde el buscador de Windows, tipeando **WF.msc**
- Desde Inicio --> Ejecutar --> mmc --> Añadir complemento --> Windows Firewall
- Desde Inicio --> Panel de Control --> Herramientas administrativas --> Windows Firewall
- Desde Inicio --> Ejecutar --> control.exe /name Microsoft.AdministrativeTools -> Windows Firewall

Por caminos que no quede... 😊

Cuando abrimos la consola de administración de Windows Firewall, éste es el aspecto que presenta:



Este es el nuevo aspecto de las consolas MMC 3.0. A los administradores les resultará más fácil adaptarse a este tipo de consolas, ya que por defecto se mantendrá el mismo diseño en otras aplicaciones, como las nuevas versiones de ISA Server y los nuevos productos de la familia Forefront por ejemplo, que traerán un aspecto parecido.

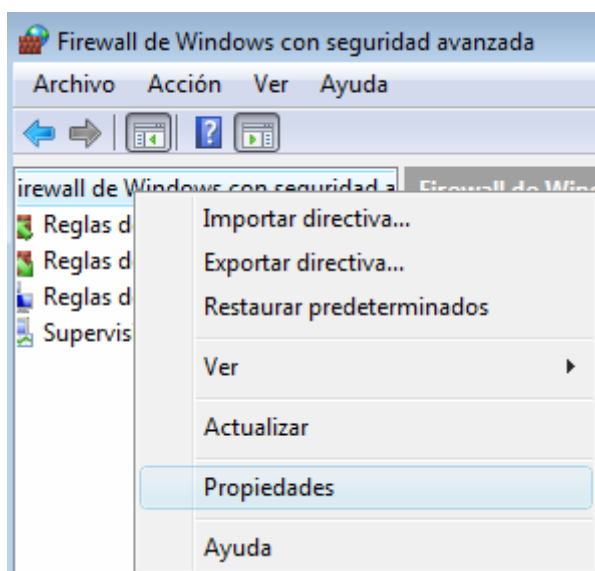
Por un lado vemos la parte derecha, que nos presenta varias opciones. Desde exportar/importar directivas, hasta establecer filtros en base al perfil, estado de conexión o por grupos.

En la parte izquierda tenemos las opciones de configuración y monitorización de reglas. Podremos configurar tanto las reglas de entrada como las de salida, y monitorizar el estado de conexiones y actividad del Firewall.

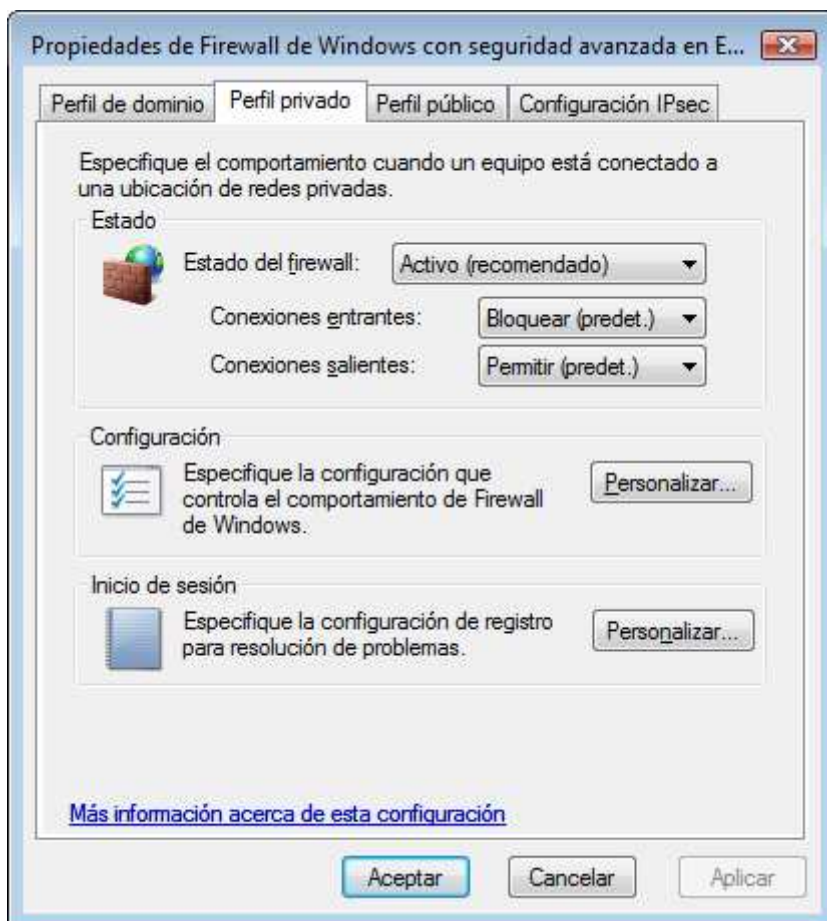
En la parte central podremos ver el estado en que se encuentra nuestro Firewall. Podremos ver los perfiles de conexión que trae por defecto Windows. Perfil de dominio, perfil privado y perfil público, accesos para crear reglas de entrada o salida y un apartado de recursos y documentación.

Para acceder a las propiedades del Firewall de Windows con seguridad avanzada, podremos hacerlo de dos formas.

Pinchar con el botón derecho del ratón en Firewall de Windows con seguridad avanzada, tal y como se muestra en la imagen:



O directamente pulsando en Propiedades, en la parte derecha de la consola (Acciones).



En las propiedades podemos ver 3 tipos de perfiles:

- **Perfil de Domino:** Equipo que se conecta a una red corporativa, como directorio activo

- **Perfil privado:** Equipo que se conecta a una LAN privada, como nuestra casa, por ejemplo
- **Perfil público:** Equipo que se conecta a una red en la que no tenemos control ninguno sobre ella. Cibercafés, aeropuertos, etc...

Cuando conectamos nuestro Vista a una red, automáticamente debe poder detectar el tipo de red a la que nos estamos conectando, y según como tengamos configurado nuestro Firewall, se aplicarán las reglas en base al perfil que tengamos.

Por ejemplo, si tengo una aplicación que conecto libremente en casa pero no en la oficina, puedo crear una regla que diga que se puede conectar libremente a internet cuando esté bajo el perfil privado, pero que no se pueda conectar cuando estemos en un perfil de dominio. Esto facilita mucho la labor a los administradores, creando la misma regla pero con ámbitos de acción diferentes en base al perfil.

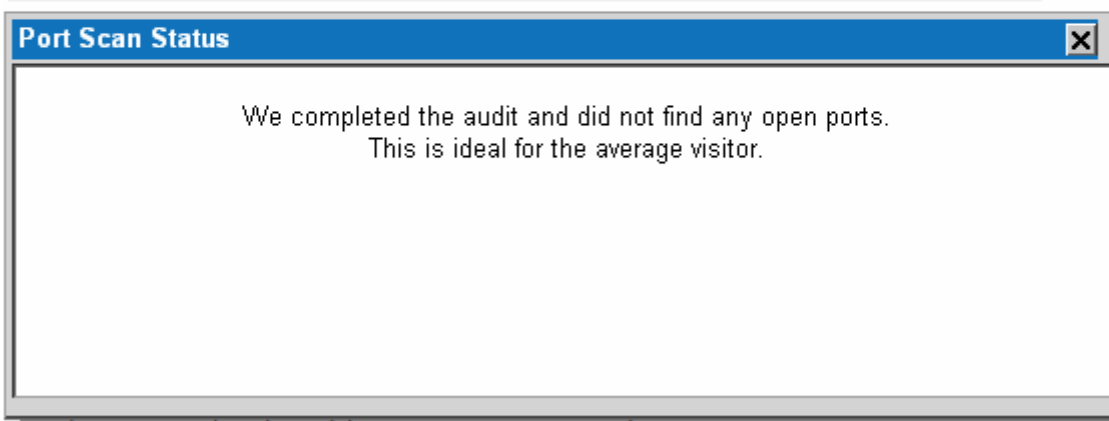
Cada perfil es totalmente configurable, pudiendo desactivarlo o activarlo a nuestro gusto, creando archivos de logs para cada uno de ellos, mostrando notificaciones de bloqueo, etc....

Y para terminar esta primera parte, vamos a someter a nuestro Firewall a una sencilla prueba de escaneo de puertos, para ver cómo reacciona.

Le he hecho un par de test de pruebas en dos Webs distintas. Una en HackerWatch y la otra en AuditMyPC. Los resultados:

Port Scanner

This Port Scanner will help you find holes (open ports) on your firewall and provide information related to those ports.



the world is useless if your browser's security is improperly configured!

Resultado Test 2:

Traffic Sent

Packets were successfully sent to your computer. The server was unable to obtain a connection or any traffic from your computer. This generally indicates that your firewall blocked the traffic successfully.

If you did *not* see an event warning it may indicate that the traffic did not reach your computer at all.

This could be due to any of the following reasons:

- You are connecting to the Internet through a proxy server. When we attempted to connect back to the IP address your web traffic came from we actually were connecting to the proxy server, not your computer.
- You are behind a corporate firewall which is redirecting traffic in an unexpected manner.
- You are connecting to the Internet through a NAT (network address translator). When we attempted to connect back to the IP address your web traffic came from we actually were connecting to the proxy server, not your computer.

In any of these cases you will not see an event notification on your computer because our connection attempt did not reach your computer. In any case, **your computer is secure**.

Podéis hacer la comprobación en alguna de estas Webs y comprobar ustedes mismos los resultados. Siempre hay que hacer las debidas pruebas antes de postear resultados, porque puede ser que pasen cosas como estas:

<https://www.securinfos.info/english/the-week-of-vista-bugs-the-truth.php>

Y administradores **mal informados** publiquen cosas como estas:

<http://www.kriptopolis.org/node/3970>

Lo que puede generar en una cadena de noticias mal documentadas y contrastadas, y al final, todos salimos perdiendo.

Firewall de Windows Vista II de II

Vamos a terminar este pequeño repaso al firewall de Windows Vista repasando las opciones que nos quedaban por cubrir, las cuales son:

- NAP (Network Access Protection)
- Configuración básica
- Creación y personalización de reglas
- Administración a través de la Shell
- Jugar un poco con él

Empezaremos hablando sobre Network Access Protection. NAP o protección de acceso a la red, no es más que una serie de políticas que nos van a ayudar a los administradores a garantizar que los equipos que se conecten a nuestra red, cumplen con una política de salud aceptable. Si para nosotros una buena política de salud es no tener un resfriado, hacer ejercicio de forma constante, etc., para un equipo una buena política de salud sería tener el antivirus en pleno funcionamiento y con las firmas actualizadas, tener instaladas todas las actualizaciones de

seguridad, etc.. Si nuestro equipo no cumpliera con la política de seguridad establecida por la empresa, podrían pasar dos cosas. La primera que no se pudiese conectar a nuestra red, y una segunda podría ser que sí nos pudiésemos conectar, pero en una red aislada de toda la corporación, con acceso sólo a algunos recursos, y a la espera de poder cumplir con los requisitos mínimos de salud.

Recordemos que esto es sólo una medida más de seguridad, al igual que los antivirus, las políticas, DEP, UAC, MIC, etc...

En el artículo anterior veíamos cómo estaba configurado el firewall por defecto, los diferentes perfiles a los que nos podemos enfrentar (dominio, público, privado) y el tipo de comportamiento que tendrá nuestro firewall cuando nos conectemos con un determinado perfil. Por defecto están los 3 configurados iguales:

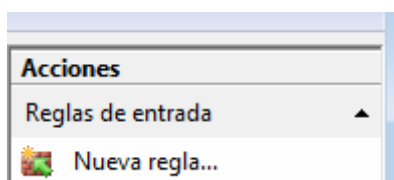
- Estado del Firewall : Habilitado
- Conexiones entrantes: Bloquear
- Conexiones salientes: Permitir

Por defecto el firewall está habilitado para todos los perfiles, las conexiones entrantes se bloquean si no cumplen con una determinada regla, pero las conexiones salientes no. Yo particularmente recomiendo que se habilite esta regla (**Conexiones salientes: Bloquear**), y así cubrimos dos campos, los cuales son las conexiones entrantes, y las salientes. Si activamos esta opción, toda acción de salida que no cumpla con una determinada regla será bloqueada. Cualquier aplicación que necesite salir al exterior, tiene que tener una regla para salir, si no la tiene, no sale. Cabe decir que si aplicamos esta opción, tendremos que configurar a mano las aplicaciones que necesiten salir a Internet, como por ejemplo nuestro navegador.

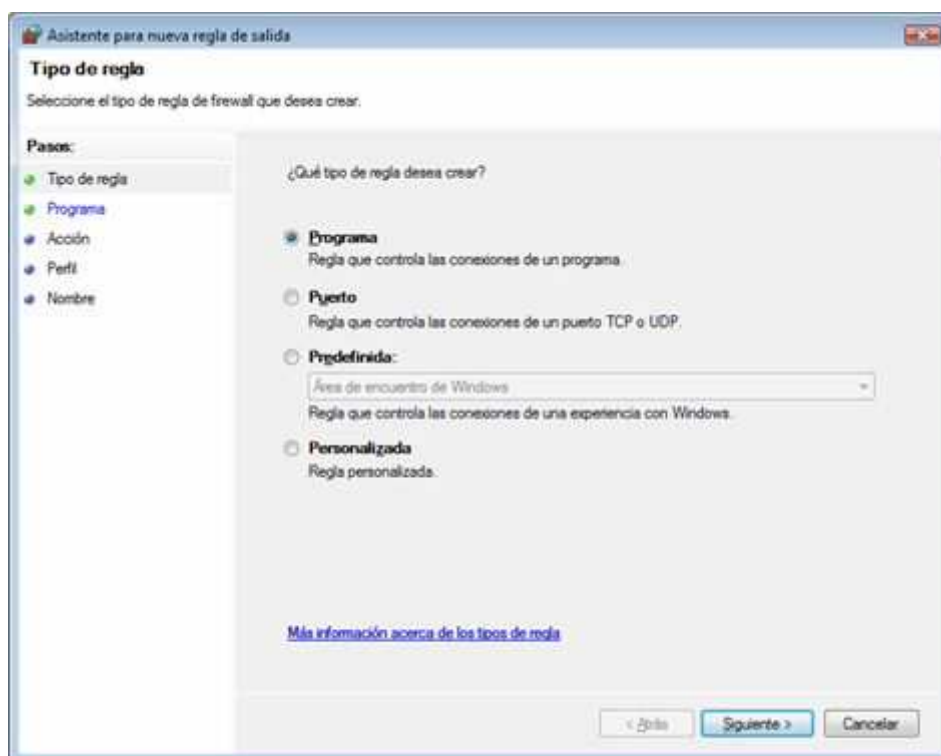
Esto lo vamos a ver muy bien con dos ejemplos de aplicaciones que necesiten salir al exterior.

Una vez que hayamos aplicado esta opción, nuestro PC estará automáticamente aislado de toda comunicación desde el interior al exterior, y desde el exterior al interior. Esto quiere decir que si iniciamos nuestro navegador para navegar por Internet, éste no podrá salir, al no tener una regla de salida asignada. Tampoco podremos hacer comprobaciones de conectividad, como por ejemplo ping, etc.... Así que vamos a crear una regla de salida, como por ejemplo nuestro navegador.

Crear una regla de salida en el Firewall es tan sencillo como picar en la opción **Nueva regla**, la cual la podemos encontrar en dos puntos de nuestra consola. En la parte superior derecha o pulsando con el botón derecho del ratón en las pestañas **Reglas de entrada** y **Reglas de salida**.

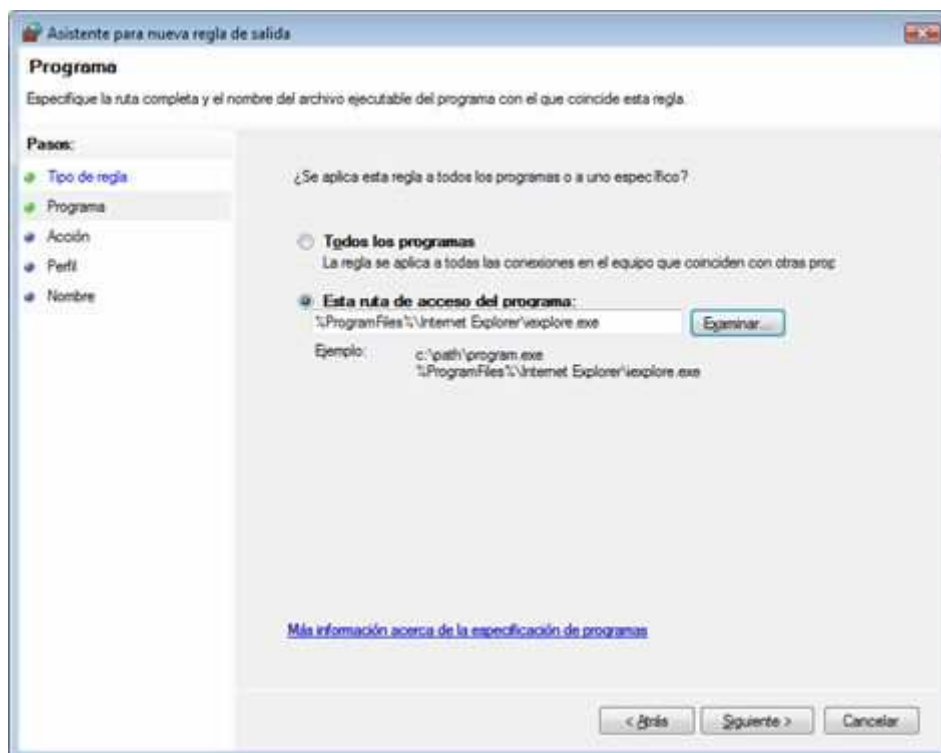


Al pulsar en **Nueva Regla** nos saldrá un asistente que nos guiará en todo momento a crear una nueva regla.

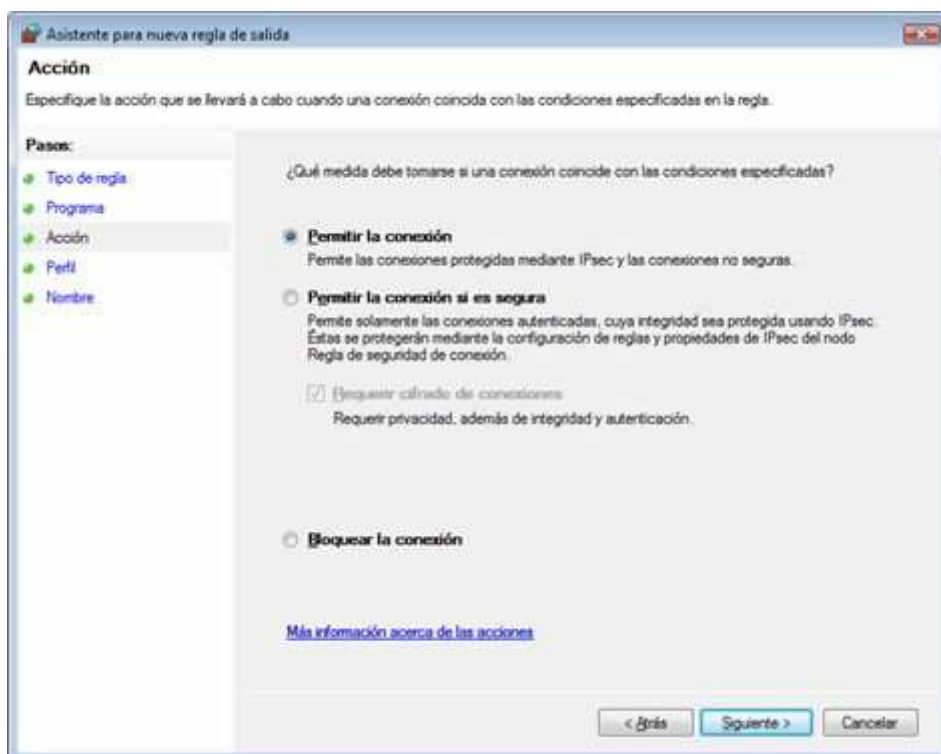


Como podréis observar, la regla no solo se limita al ámbito de una aplicación, sino que podremos crear reglas por número de puerto, servicios, reglas predefinidas, etc... Podremos personalizar las reglas a nuestro gusto.

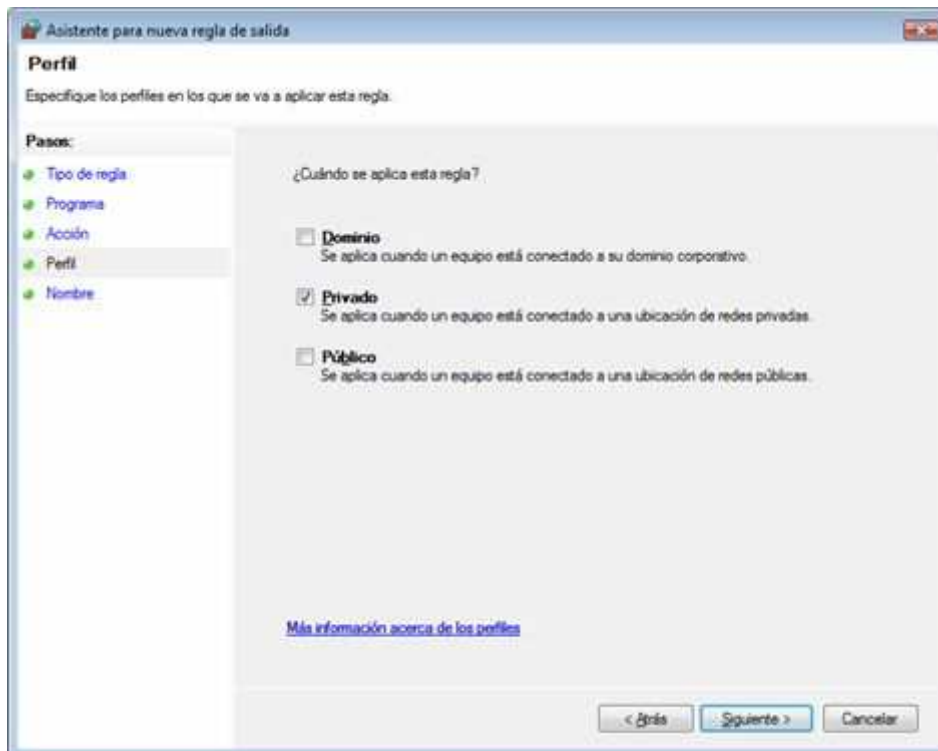
Como en nuestro caso vamos a darle salida a nuestro navegador, elegiremos la opción **Programa** y pulsaremos **Siguiente**.



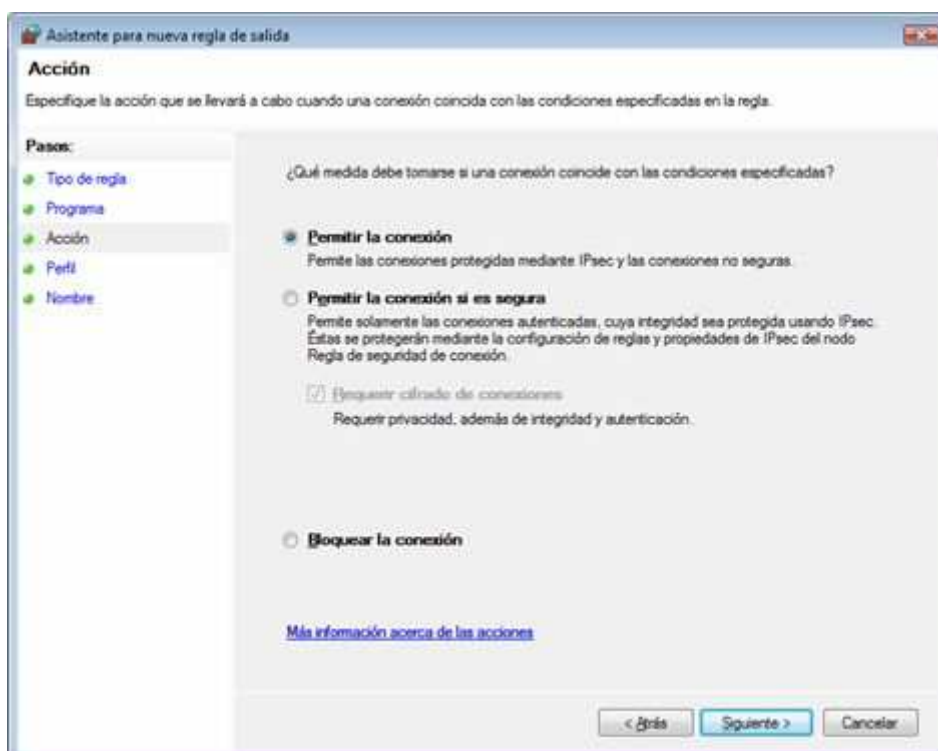
Aquí nos está pidiendo el asistente que le indiquemos la aplicación que va a coincidir con la regla de salida. Marcaremos la ruta de nuestro navegador y pulsaremos **Siguiente**.



Aquí nos pregunta por el tipo de conexión que vamos a permitir o denegar. Si os fijáis, el firewall, al estar integrado con IPSEC, nos da la opción de permitir sólo las conexiones seguras y autenticadas, en el caso de que nuestra red estuviese configurada con IPSEC. Marcamos **Siguiente**.



En esta parte de la regla, nos preguntará en qué ámbito se aplicará esta regla. Como mi PC sólo va a estar en casa, marcaré la opción **Privado**. Si fuésemos un administrador de sistemas y tuviésemos que configurar el Firewall para el portátil de un directivo podríamos marcar los 3 ámbitos, así nuestro directivo tendría conectividad tanto en el trabajo, como en su casa, pasando por una red pública, como podría ser un aeropuerto, etc...



La última regla es solo para poner un nombre y una descripción. Tendremos que ser consecuentes con el nombre que pongamos si queremos llevar una monitorización óptima. Pulsamos **Finalizar** y listo! Tenemos nuestra primera regla de salida!

Un problema menos, podemos navegar por la Red. Pero al cabo de un rato me veo en la necesidad de hacer una prueba de conectividad entre varios equipos, y al intentar una prueba con el comando **ping**, veo que el Firewall me está denegando la salida.



```
Símbolo del sistema
D:\Users\Silverhack>ping microsoft.com

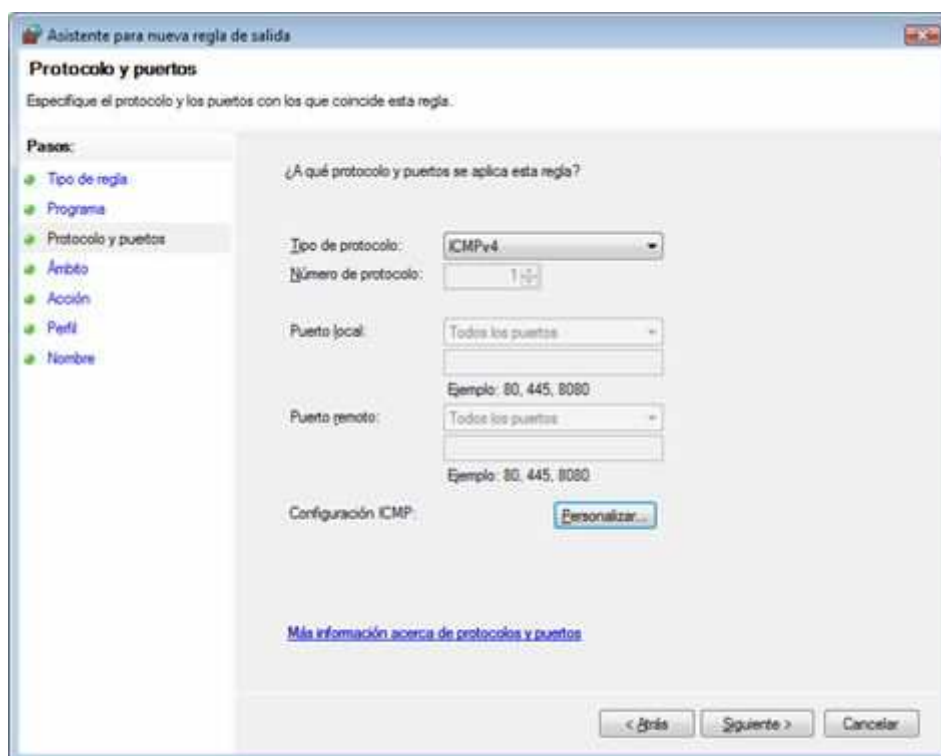
Haciendo ping a microsoft.com [207.46.197.32] con 32 bytes de datos:
Error general.
Error general.
Error general.
Error general.

Estadísticas de ping para 207.46.197.32:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos),
D:\Users\Silverhack>
```

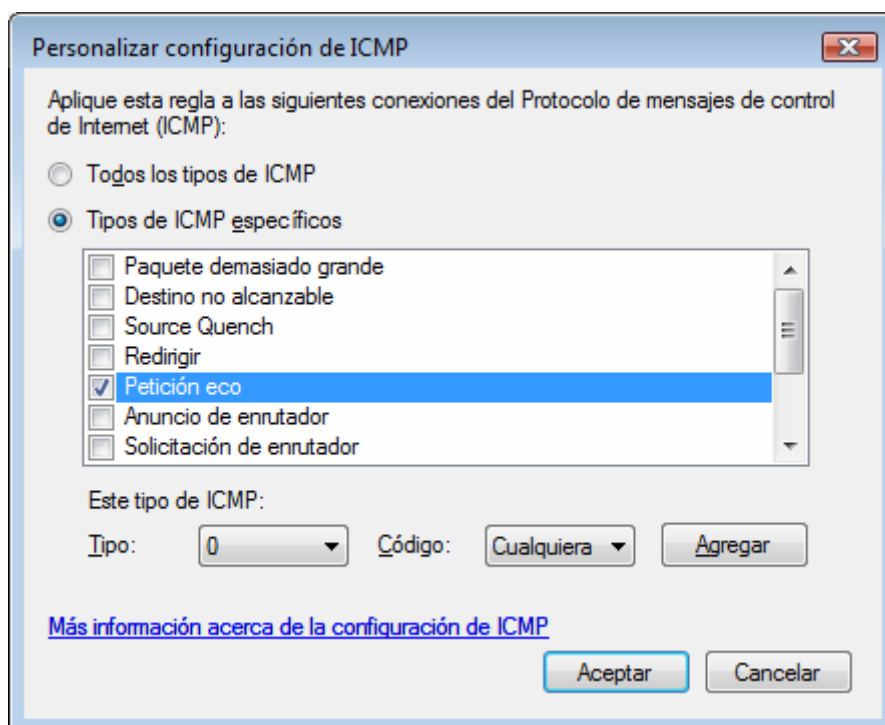
Para cerciorarnos de que no es un error de conexión, podemos mirar el log de nuestro Firewall para ver qué registra, y esto es lo que nos encontraremos:

```
2007-04-25 12:43:45 ALLOW UDP 192.168.1.50 192.168.1.255 138 138 0 - - - - - RECEIVE
2007-04-25 12:44:17 DROP ICMP 192.168.1.151 207.46.197.32 - - 0 - - - - 8 0 - SEND
2007-04-25 12:44:18 DROP ICMP 192.168.1.151 207.46.197.32 - - 0 - - - - 8 0 - SEND
2007-04-25 12:44:19 DROP ICMP 192.168.1.151 207.46.197.32 - - 0 - - - - 8 0 - SEND
2007-04-25 12:44:20 DROP ICMP 192.168.1.151 207.46.197.32 - - 0 - - - - 8 0 - SEND
```

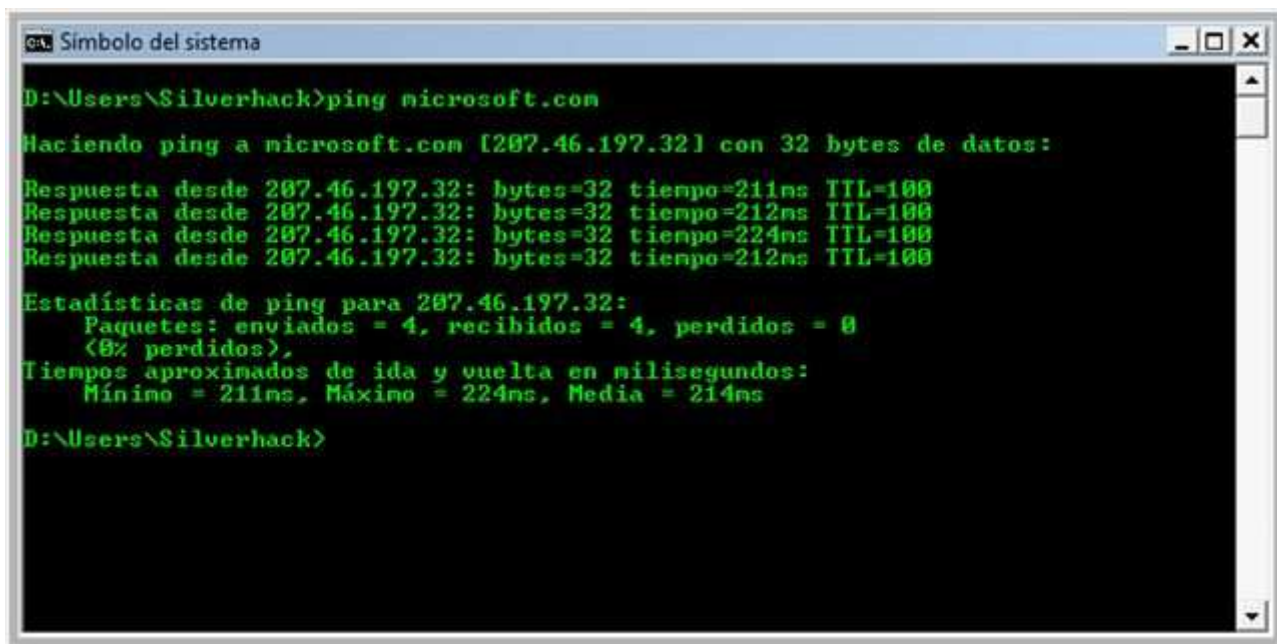
Como podéis comprobar, me está denegando toda salida ICMP. Lo único que nos queda por hacer es crearnos una nueva regla de salida, pero esta vez personalizada, que se aplique a todos los programas. Lo único que tenemos que cambiar es la configuración del protocolo. La regla sólo se aplicará al protocolo ICMP, tal y como aparece en la imagen:



Si os fijáis, el firewall de Windows también nos permite configurar el protocolo ICMP, lo cual nos viene de perlas, porque yo sólo quiero **peticiones de eco** para poder hacer **pings**, lo que nos quedaría:



Una vez configurada nuestra regla y habilitada, podremos comprobar que ya tenemos conectividad ping.



```
D:\Users\Silverhack>ping microsoft.com

Haciendo ping a microsoft.com [207.46.197.32] con 32 bytes de datos:

Respuesta desde 207.46.197.32: bytes=32 tiempo=211ms TTL=100
Respuesta desde 207.46.197.32: bytes=32 tiempo=212ms TTL=100
Respuesta desde 207.46.197.32: bytes=32 tiempo=224ms TTL=100
Respuesta desde 207.46.197.32: bytes=32 tiempo=212ms TTL=100

Estadísticas de ping para 207.46.197.32:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 211ms, Máximo = 224ms, Media = 214ms

D:\Users\Silverhack>
```

Y la administración bajo línea de comandos? Es posible? Claro que sí!

Muchos administradores se quejaban de que Windows era una gran plataforma en entorno gráfico, pero que la línea de comandos estaba bastante descuidada. Esto es y no es cierto. Me explico. Desde Windows 2000/XP ya se podía administrar en un 100% un equipo bajo línea de comandos, lo que no había en Internet eran manuales al respecto. Ahora con la nueva [PowerShell](#) de Windows la experiencia se multiplica de forma exponencial. Veamos cómo podemos administrar nuestro Firewall a través de la Shell.

Vamos a utilizar la herramienta nativa de Windows **netsh**. Netsh es una aplicación bajo línea de comandos que nos permite la administración de la configuración de red de un equipo. Este tipo de administración lo podemos hacer tanto de forma local como remota.

Este comando no sólo sirve para administrar el Firewall de Windows, sino que podremos administrar un 100% de nuestra configuración. Podremos administrar NAP, HTTP, RPC, configuraciones IP, etc...

El comando en cuestión es el siguiente:

Netsh advfirewall firewall

Imaginemos que tenemos una aplicación que se llama **juanito.exe** que necesita salir al exterior. Necesitamos crearle una **regla de salida** sólo para el perfil **privado**. Lo que nos deja el comando siguiente:

Netsh advfirewall firewall add rule name=" Permitir aplicación Juanito.exe" dir=out program="C:\Archivos de programa\Aplicación de Juanito\juanito.exe" profile=private action=allow

En donde el apartado **dir** refleja la naturaleza de la regla (si es de salida o de entrada), el apartado profile refleja el ámbito de la regla (perfil público, privado o dominio) y la acción que va a tomar esa regla (permitir o denegar).

Con la aplicación netsh podremos crear, eliminar, crear backups de las reglas, etc... Recomendando echarle un vistazo, ya que es una herramienta muy potente que puede ayudar a muchos administradores.

Y para jugar un poco con él, vamos a intentar poner una Shell a la escucha con la aplicación netcat.

El comando que vamos a utilizar es el siguiente:

nc.exe -l -e "cmd.exe" -p 1234

Al pulsar **Enter** podremos ver como nuestro firewall se cosca de que hay una aplicación que quiere salir a escuchar, y que incluso si desbloqueamos esa aplicación, el control de cuentas de usuario nos pide aprobación para iniciar la consola de nuestro Firewall.



La segunda prueba que vamos a hacer es un escaneo típico con la herramienta **nmap**. En este caso vamos a probar dos tipos de escaneo. El escaneo SYN y el escaneo connect.

SYN Scan

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrador\nmap>nmap -v -A -sS 192.168.1.151

Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-25 14:15 Hora de verano ro
mance
Initiating ARP Ping Scan at 14:15
Scanning 192.168.1.151 [1 port]
Completed ARP Ping Scan at 14:15, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:15
Completed Parallel DNS resolution of 1 host. at 14:15, 0.00s elapsed
Initiating SYN Stealth Scan at 14:15
Scanning 192.168.1.151 [1697 ports]
Completed SYN Stealth Scan at 14:16, 38.13s elapsed (1697 total ports)
Initiating Service scan at 14:16
Warning: OS detection for 192.168.1.151 will be MUCH less reliable because we d
id not find at least 1 open and 1 closed TCP port
Initiating OS detection (try #1) against 192.168.1.151
Host 192.168.1.151 appears to be up ... good.
All 1697 scanned ports on 192.168.1.151 are filtered
MAC Address: 00:00:00:00:00:00 (Xerox)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http:
//insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 39.487 seconds
Raw packets sent: 3419 (152.714KB) | Rcvd: 1 (42B)

```

Connect Scan

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrador\nmap>nmap -v -A -sT 192.168.1.151

Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-25 14:18 Hora de verano ro
mance
Initiating ARP Ping Scan at 14:18
Scanning 192.168.1.151 [1 port]
Completed ARP Ping Scan at 14:18, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:18
Completed Parallel DNS resolution of 1 host. at 14:18, 0.00s elapsed
Initiating Connect() Scan at 14:18
Scanning 192.168.1.151 [1697 ports]
Connect() Scan timing: About 39.16% done; ETC: 14:19 (0:00:46 remaining)
Completed Connect() Scan at 14:20, 85.12s elapsed (1697 total ports)
Initiating Service scan at 14:20
Warning: OS detection for 192.168.1.151 will be MUCH less reliable because we d
id not find at least 1 open and 1 closed TCP port
Initiating OS detection (try #1) against 192.168.1.151
Host 192.168.1.151 appears to be up ... good.
All 1697 scanned ports on 192.168.1.151 are filtered
MAC Address: 00:00:00:00:00:00 (Xerox)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http:
//insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 86.665 seconds
Raw packets sent: 25 (3378B) | Rcvd: 1 (42B)

```

Incluso podríamos ver la reacción de nuestro Firewall mirando de nuevo el Log

```

2007-04-25 14:20:50 DROP ICMP 192.168.1.100 192.168.1.151 -- 148 - - - - 8 9 - RECEIVE
2007-04-25 14:20:50 DROP ICMP 192.168.1.100 192.168.1.151 -- 178 - - - - 8 0 - RECEIVE
2007-04-25 14:20:50 DROP ICMP 192.168.1.100 192.168.1.151 -- 148 - - - - 8 9 - RECEIVE
2007-04-25 14:20:50 DROP ICMP 192.168.1.100 192.168.1.151 -- 178 - - - - 8 0 - RECEIVE
2007-04-25 14:20:50 DROP ICMP 192.168.1.100 192.168.1.151 -- 148 - - - - 8 9 - RECEIVE
2007-04-25 14:20:51 DROP ICMP 192.168.1.100 192.168.1.151 -- 178 - - - - 8 0 - RECEIVE
2007-04-25 14:20:51 DROP ICMP 192.168.1.100 192.168.1.151 -- 148 - - - - 8 9 - RECEIVE
2007-04-25 14:20:51 DROP ICMP 192.168.1.100 192.168.1.151 -- 178 - - - - 8 0 - RECEIVE

```

```

2007-04-25 14:20:24 DROP TCP 192.168.1.100 192.168.1.151 4121 135 48 S 1479575993 0 65535 - - - RECEIVE
2007-04-25 14:20:24 DROP TCP 192.168.1.100 192.168.1.151 4124 135 48 S 1912892793 0 65535 - - - RECEIVE
2007-04-25 14:20:26 DROP TCP 192.168.1.100 192.168.1.151 4213 139 48 S 2534774270 0 65535 - - - RECEIVE
2007-04-25 14:20:26 DROP TCP 192.168.1.100 192.168.1.151 4218 139 48 S 3970565409 0 65535 - - - RECEIVE

```