RESUMEN

Hardening es una acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador del sistema operativo o la red para reforzar al máximo posible la seguridad de los equipos del Ministerio de Trasporte y Obras Públicas del Ecuador. Ante la problemática de no tener conocimiento sobre este proceso, el presente artículo propone la implementación de una herramienta informática que permita su uso apropiado para el Ministerio de Trasporte y Obras Públicas, la seguridad de cada uno de los sistemas operativos ha sido delimitada por la que viene por defecto, programada por Microsoft y no más allá de sus necesidades reales; para ello se determinan las áreas de vulnerabilidad de los sistemas con sus respectivas acciones y afectaciones a través de herramientas de testeo, para mediante un manual de configuración de seguridad Hardening se pueden crear sistemas operativos más efectivos a la hora de contraatacar invasores y con mayor necesidad e importancia de cuando se trata de información por parte de un Ministerio de Gobierno. Su propósito es entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad mediante la configuración de todas las áreas de seguridad. Una de las primeras cosas que hay que dejar en claro del Hardening de sistemas operativos Microsoft es que no necesariamente logrará forjar equipos invulnerables sino equipos más seguros.

CAPÍTULO I

PLAN DE TESIS

TEMA:

Afinamiento de los sistemas operativos plataforma Microsoft mediante la utilización de Hardening, para resolver problemas de seguridad en el Ministerio de Transporte y Obras Públicas del Ecuador

Introducción

Windows se ha caracterizado por ser un sistema operativo inseguro, lo cierto también es que finalmente Microsoft ha encausado su estrategia vertiendo importantes mejoras en su nueva línea de sistemas operativos Windows XP / Windows 2008, sobre todo con la distribución de SP 2 y SP 1 respectivamente.

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

"Firewall Activado por defecto en XP SP2", "IIS Desactivado por defecto en Windows 2003", etc.

A pesar de esto, quienes tienen la posibilidad de ir un poco más allá, no deben desconocer aquellas configuraciones que pueden elevar en gran medida la de seguridad respecto del sistema operativo. Cierto es que Microsoft hace su esfuerzo intentando mejorar sus productos, pero como usuarios, también tenemos la responsabilidad al momento de conectar a la red uno de nuestros equipos.

Aún después de mejoras existen algunas características que a menudo no suelen ser tomadas en cuenta a la hora de llevar a la práctica procedimientos de "Hardening" en la plataforma Microsoft.

Debido a tales situaciones existen algunas técnicas o herramientas de las cuales se pueden aprovechar sobre la instalación de Windows.

"Haciéndole la vida difícil al atacante". Es el concepto que está detrás del Hardening de sistemas operativos. Hardening es una acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo.

_____ Roberta Bragg USA

Justificación e Importancia

Hardening es una acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo.

Para el Ministerio de Trasporte y Obras Públicas la seguridad en los equipos ha sido aplicada solo a nivel básico; es decir las configuraciones de cada uno de los sistemas operativos han sido delimitadas por la que viene por defecto, programada por Microsoft.

Teniendo así sistemas operativos medianamente seguros; en muchas ocasiones es muy difícil determinar el nivel de seguridad debido a que las personas tienen su sistema operativo pero solo saben el 50% de sus programas; la mayoría de programas dentro de Plataforma Microsoft sirven para configurar al mismo, pero muy pocos lo usan o simplemente usan las configuraciones por defecto.

Por ello es importante, no sólo tener las herramientas de control sino saber para qué? y por qué? Utilizarlas. Mediante un manual de configuración de seguridad Hardening se pueden crear sistemas operativos más efectivos a la hora de contraatacar invasores y con mayor necesidad e importancia cuando se trata de información por parte de un Ministerio de Gobierno.

Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

¿Hasta qué punto el Hardening es una ayuda y no una molestia? En este punto, es importante considerar un paradigma muy interesante que tiene la seguridad.

Al parecer, la seguridad por un lado, y la versatilidad y facilidad de uso de los sistemas por otro, son como dos grupos de personas tirando de ambos extremos de una cuerda. En pocas palabras, a medida que se busca una seguridad mayor en los sistemas, la versatilidad y facilidad de uso del mismo se ven limitados, puesto que la cantidad de decisiones que puede tomar el usuario se reduce y la cantidad de posibilidades ajenas al propósito inicial del sistema en sí disminuye drásticamente. Por otro lado, el aumentar la versatilidad y la facilidad de uso de los sistemas pareciera estar muy relacionado con el aumento en las decisiones y posibilidades del usuario, lo que por consiguiente aumenta la probabilidad del mismo de equivocarse y poner en peligro la seguridad de todo el sistema. Y el debate sobre el punto exacto de equilibrio en cuanto a la cantidad de decisiones que deben pasar por manos del usuario final es bastante extenso y no está del todo resuelto.

Objetivos

Objetivo General

- Resolver los problemas de seguridad en los sistemas operativos Microsoft, mediante la utilización de Hardening en el Ministerio de Trasporte y Obras Públicas del Ecuador.

Objetivos Específicos

- Realizar pruebas sobre sistemas operativos Microsoft para determinar sus vulnerabilidades, mediante herramientas de testeo (Software).

- Determinar áreas de vulnerabilidad de los sistemas operativos con sus respectivas acciones y afectaciones.

- Elaborar manual de hardening que permita al usuario configurar su sistema operativo, para contrarrestar las áreas de vulnerabilidad.

- Elaborar e implementar archivos de tipo registro estándar con configuración de hardening, para uso en equipos de similares características con sistemas operativos iguales.

Situación Actual

En los últimos años, la seguridad ha pasado de ser una ocurrencia tardía en los departamentos de TI a ser la principal prioridad. En este movimiento, no sólo ha calificado la necesidad de que el aumento de profesionales de la seguridad, pero la seguridad ha convertido en un requisito básico de trabajo para casi todos los administradores de TI.

Lamentablemente, para El MTOP, no hay suficientes horas en el día para realizar sus tareas, y mucho menos cavar a través de pilas de libros blancos, sitios web tratando de encontrar información sobre el endurecimiento de Windows, especialmente si la red de su organización tiene usos múltiples versiones de Windows.

La mayoría de los libros sólo se refieren a una o dos versiones de Windows, pero muy pocos de ellos cubren todos. Esto, combinado con su relajado, divertido estilo de escritura, lo convierte en un verdaderamente único y especial de recursos de seguridad.

Mientras que la seguridad es de por sí sobre el ordenador, a veces los mayores vulnerabilidades de seguridad provienen de personas, el control de usuarios al ingreso de los sistemas que maneja El MTOP es adecuado, pero el ingreso al Sistema Operativo como tal es muy poco controlado en lo que se refiere a contraseñas y usuarios.

Esto NO significa que el proceso de Hardening contemple tan solo estos puntos, pero SI significa que tan solo con este MINIMO esfuerzo de 5 pasos, el sistema podrá ser considerado más confiable.

Dicho de otro modo... debería ser considerado como un REQUERIMIENTO MINIMO, que muy pocos o casi nadie lo aplica dentro de las medidas que se deben tomar a la hora de decidirse por el uso de un Sistema operativo Microsoft.

Aunque el Gobierno haya determinado como medida el uso de Sistemas de tipo Software Libre, estos sistemas usados en El MTOP cuentan con licencias propias, razón por la cual son usados, y no ven la posibilidad de migrar a otros.

Tomando en cuenta esto, lo que queda por hacer es fortalecer los Sistemas que se tienen tanto por economía como por seguridad.

Alcance

Una de las primeras cosas que hay que dejar en claro del Hardening de sistemas operativos Microsoft es que no necesariamente logrará forjar equipos invulnerables. Es importante recordar que, según el modelo de defensa en profundidad, el host es sólo una capa de éste. En otras palabras, un factor más a considerar dentro del gran número de puntos a ser tomados en cuenta para defender globalmente un sistema.

Tomar un enfoque proactivo para la seguridad de la red por el endurecimiento de su sistemas Windows contra ataques antes de que ocurran. Está en manos de recursos proveer medidas concretas que puede tomar de inmediato, así como las acciones en curso para garantizar la seguridad a largo plazo. Con cobertura de Windows 95/98/NT 4.0/2000/XP y Windows Server 2008, Como una herramienta esencial para la seguridad en el trabajo a los profesionales de TI.

Mediante la elaboración de un manual de seguridad con Hardening, los usuarios estarán mucho mejor equipados para endurecer la organización cliente y servidor de los equipos que ejecutan Windows.

Determinando sus vulnerabilidades y creando barreras de ayuda.

Se tendrá que trabajar juntos y por sí solo para generar una cultura de la seguridad, endurecer todos los componentes de nuestras redes, la construcción de sistemas de seguros, capacitar a nuestra gente.

Para el manual de seguridad se determinarán los siguientes puntos:

- Uso de herramientas de identificación de vulnerabilidades
- Determinación de Niveles de seguridad
- Determinación de requisitos indispensables de cada uno de los sistemas operativos.
- Controles de seguridad y activaciones
- Protecciones de seguridad
- Seguridades adicionales
- Generación de archivos de configuración para sistemas operativos Microsoft con similares características.

Limitaciones

La investigación proporcionará un manual con una lista maestra de las medidas necesarias para endurecer los sistemas Windows. Windows 98, Windows 95, Windows NT 4.0, Windows 2000, Windows XP y Windows Server 2003.

No pretende ser una guía completa de la seguridad de la información, ni siquiera la única información que necesita para comprender y la práctica seguridad de Windows. Sin embargo, es sencilla y detallada.
Endurecimiento cada paso va acompañado de paso a paso las instrucciones. Para algunos, que proporciona un punto de partida, para otros, una lista de control que se puede juzgar su programa actual, y para otros, una base sólida de seguridad en Windows.

Metodología de aplicación

La investigación

Existen muy diversos tratados sobre las tipologías de la investigación. Las controversias para aceptar las diferentes tipologías sugieren situaciones confusas en estilos, formas, enfoques y modalidades. En rigor, y desde un punto de vista semántico, los tipos son sistemas definidos para obtener el conocimiento.

Se pretende presentar una síntesis de los tipos de investigación que van a ser usados, con la intención de sistematizar lo que se va a usar para poder desarrollar la misma.
Según la fuente de información se aplicará:

- Investigación documental.
- Investigación de campo.
- Experimental.

El método para la obtención del conocimiento denominado científico es un procedimiento riguroso, de orden lógico, cuyo propósito es demostrar el valor de verdad. La amplitud de criterios en las formas de investigar ha producido diferentes métodos para obtener el conocimiento. Los que se usarán son:

- Inducción-deducción.
- Análisis-síntesis.

- Experimento.
- Explicación.
- Mecanicismo.
- Funcionalismo.
- Sistemas.

Herramientas de Desarrollo

HERRAMIENTAS DE DETECCIÓN DE VULNERABILIDADES

La determinación de vulnerabilidades de los sistemas será a través del empleo de herramientas de tipo tester (software libre).

Que ofrecerán una mejor proyección de los problemas que se sucinta en los sistemas operativos.

- La existencia de libros sobre Hardening es casi nula, debido a que se han desarrollado temas de seguridades informáticas en general, pero que aplican operaciones de seguridad que deben ser de tratados como Hardening por su contenido.

  Esto hace que se pueda utilizar material ya escrito como una opción de recopilación de información para ponerlo como actividades que se realiza dentro de lo que es Hardening.

- La creación de archivos de tipo registro para plataformas Windows no presenta ningún tipo de restricción a la hora de implementarlos, por lo tanto se podrá hacer pruebas significativas sobre los diferentes tipos de sistemas operativos Microsoft, que posean permisos de administrador

Investigación de Aplicación del Hardening

I. Endurecimiento de sistemas Windows.

   i. Recolección de la información sobre seguridad aplicada en los sistemas de operativos Microsoft.

   ii. Aplicación de Testers para análisis de riesgos.

      - Manejo de herramientas

   iii. Análisis de vulnerabilidades.

   iv. Sectores de afectación

   v. Manejo del Editor de Registros de Windows

   vi. Análisis de áreas

II. Vulnerabilidad

i. Niveles de seguridad Hardening

ii. Ciclos de vida de Hardening

iii. Usos de Servicepacks

iv. Análisis de Configuraciones básica por defecto

v. Requisitos básicos de los sistemas en el campo de seguridad

vi. Configuraciones que causan problemáticas

III. Aplicación Hardening

i. Creación de listas de control por áreas de riesgo

ii. Service Packs y actualizaciones de seguridad

- Gran Service Pack y actualización de seguridad Requisitos
- Servicio de Menores Pack y Requisitos de la actualización de seguridad

iii. Auditoría y políticas de cuentas

- Principales características de Auditoría y de políticas de cuenta y Requisitos
- Menores características de Auditoría y de políticas de cuenta y Requisitos

iv. Configuración de seguridad

- Grandes Configuraciones de seguridad
- Menores Configuraciones de seguridad

v. Protección de Seguridad Adicional

- Servicios del sistema
- Derechos del Usuario
- Otros Requisitos del sistema
- Permisos de archivos y entradas del Registro

vi. Plantillas administrativas

- Sistema
- Red
- Componentes de Windows

IV. Resultados

i. Elaboración de registros ejecutables con configuraciones predeterminadas para Sistemas Operativos Microsoft, con similares características de uso.

ii. Aplicaciones de tipo ejemplo de configuración de registros.

iii. Aplicaciones de tipo ejemplo de configuraciones especiales

- Manejo de servicios
- Manejo se software
- Manejo de sistema
  - Tiempos
  - Mejoras

Factibilidad

Factibilidad técnica

- Inmunizar el sistema contra ataques conocidos
- Maximizar el tiempo necesario para llevar a cabo
- un ataque en la plataforma
- Evitar el robo de información en el sistema
- Fortificación de cuentas de usuario
- Definición de roles restringidos
- Política de contraseñas eficiente
    - Fortificación del sistema operativo
- Gestión periódica de parches
- Política de auditoría eficaz
    - Auditar inicios de sesión
    - Auditar cambios de políticas
    - Auditar Accesos a objetos
- Auditar el acceso a cuentas falsas de usuario
    - Administrador / Administrador
- Desinstalación de componentes no necesarios
    - Software del sistema operativo
    - Productos de terceros
    - Servicios innecesarios
- Deshabilitar servicios del sistema no necesarios
    - Evaluar la funcionalidad del sistema.
- Limitación de acceso al sistema de ficheros
    - Lectura: robo de credenciales

Factibilidad económica

- Protección de Hardware y Software
- Protección de manejo de información
- Dispositivos y prevención de acceso físico

- Protector de pantalla
- Limitar uso de dispositivos USB
- Limitar acceso remoto a cdrom/floppy
- Deshabilitar dispositivos de Hardware
  - Pantalla
  - Teclado
- Ejecución automática.
  - autorun
- Instalación de drivers no firmados

Factibilidad operativa

Es muy factible el proyecto de tesis para poder desarrollar un manual de automatización y mejora, completamente funcional y en el menor tiempo posible.

Presupuesto y Cronograma de Trabajo

PRESUPUESTO

Presupuesto Software

Existe diversidad de programas que sirven como Testers de sistemas operativos, claro que muchos de ellos no analizan algunas vulnerabilidades, pero se las pueden determinar con inspección directa en el sistema.

La mayoría de estos programas son de software libre.

Las pruebas en los diversos sistemas operativos Microsoft, por ser de carácter investigativo y no lucrativo, no será necesario adquirir las licencias., ya que las pruebas serán realizadas en una sola máquina de propiedad del estudiante, luego se procederá la aplicación de los archivos de configuración de tipo registro en cada una de las máquinas del MTOP; las cuales poseen sus propias licencias.

Presupuesto Hardware

Tabla 1.1 Computador para estudiante

Procesador	MIC INTEL C2D E8400 3.00/6/1333
Memoria	MEM NOT MVISION D2-800 4GB
Disco duro	D DURO SAMSUNG 500GB SATA
Mainboard	MB INTEL D965SSCK VSR 775 BOX
Tarjeta gráfica	Aceleradora 3D, 64 MB/SDRAM
Unidad Lectora de Tarjetas	SD-MicroSD-USB
DVD-WRITER	52x
Módem interno	Fax-Módem interno 56K
Monitor LCD	19"
Micrófono	De sobremesa

Teclado	Botones adicionales navegar por Internet
Ratón	Intellimouse de Microsoft
Software	Microsoft Windows XP Professional Microsoft Windows Vista Bussines Microsoft Windows 2003 Server

Total presupuesto hardware: **980 USD**

Las licencias para uso del software van a ser gratuitas por lo que se puede encontrar en el internet sin costo alguno.

Los costos serán cubiertos por el desarrollador. El software en su versión ejecutable.

Presupuesto de Aplicación

Gastos para Investigación y Pruebas

- Internet 256 Kbps 3 meses $ 81,00

Gastos para Implementación

- Trasporte 2 meses $ 70,00

TOTAL..... $ 151,00

Costo Total: $ 1131,00

CRONOGRAMA

Bibliografía utilizada en Plan de Tesis

El centro para la seguridad de Internet [ONLINE] http://www.cisecurity.org

[2] El instituto de SANS [ONLINE] http://www.sans.org

[3] [ONLINE] http://www.nsa.gov/ia

[4] Departamento de las recomendaciones de defensa no corrientemente disponible en línea.

Microsoft Windows Security [ONLINE] http://www.microsoft.com/security

[5] [ONLINE] http://tipsdeseguridad.spaces.live.com/blog/cns!779AF69CE6408BD1!2273.trak

[6] [ONLINE] http://labs.dragonjar.org/xmlrpc.php?rsd

[7] [ONLINE] http://geeks.ms/blogs/vista-tecnica/archive/2007/12/24/sistemas-de-integridad-en-win

[8] [ONLINE] http://www.fistconference.org/data/presentaciones/hardeningaltaseguridadbajow32.pdf

[9] [ONLINE]

http://www.aibarra.org/investig/tema0.htm#INVESTIGACI%D3Nhttp://tipsdeseguridad.spaces.live.com/blog/cns!779AF69CE6408BD1!2273.trak

CAPÍTULO II

MARCO TEÓRICO

HARDENING DE MICROSOFT WINDOWS

Introducción

Para entender sobre como Endurecer la seguridad de los Sistemas Operativos Microsoft Windows, se ha organizado la siguiente información en capítulos, los mismos que se enfocan en los diferentes aspectos del Hardening de Sistemas Microsoft. Los Capítulos 2 y 3 describen procedimientos relacionados con las versiones específicas de Windows. Es decir que las técnicas descritas en un capítulo sobre el proceso de Hardening aplicado sobre una versión de Windows pueden ser usadas en otra versión. Es simplemente una forma de organizar el flujo de Aplicación Hardening, así es que se puede aprovechar todo de cada capítulo para cualquier tipo de sistema operativo.

Los capítulos se enfocan en los diferentes asuntos que afectan la seguridad e integridad de los sistemas y redes. Al final, se encontrará una lista de los puntos de control y de las configuraciones que se pueden hacer de forma directa a través del editor de registros.

Existen, por supuesto, muchos métodos de endurecimiento, y muchas opiniones y cuán utilizables son estos; pero Hardening de Windows está enfocado directamente a las vías probadas, para lograr la protección máxima del sistema en menor tiempo, donde la respuesta será encontrarse con los resultados más aceptables.

La seguridad de la computadora parece ser parte principal de las noticias, hoy en día en el mundo de la informática por la invasión de especialmente zonas web. Las compañías pierden millones de dólares y sufren daños a los sistemas de computadora, como un ejemplo de esta consecuencia New York gasta miles de dólares en los sistemas y

productos de seguridad para proteger las puertas de ingreso a sus redes corporativas anualmente.

Por otro lado Microsoft estanca al usuario con una simple configuración de seguridad la cual se refiere a corregir las propiedades de red del computador. El resultado de esta configuración es horas de tiempo muerto y la confianza del cliente disminuida. Muchas veces por no decirlo siempre es duro saber cuál es el número de intrusos que son amenazantes para el reino de la computadora, algunos de ellos hasta son indetectables, y no es suficiente controlarlos mediante una simple configuración.

Muchos sistemas de tipo administradores y usuarios han construido un sistema que soluciona en parte el problema mediante una forma de tolerancia al hurto de información, contenida en ordenadores que almacenan basura como información, para que el intruso pase su tiempo intentado burlar dicho servidor. Ellos han aceptado intrusos de forma normal y tranquila como si fuesen usuarios reales del sistema y como la información alojada que sufre el ataque es solo basura (colocada a propósito), entonces esta parte son sólo los subproductos de un sistema unido al servidor verdaderamente importante. Y de alguna forma si solucionan y principalmente protegen la información. Pero muchos de los intentos, sin éxito o no, son inadvertidos por los usuarios mediante este método. Los expertos de seguridad de Internet coinciden en esto y que el número de intentos a las roturas de seguridad está aumentando, al igual que la eficiencia y sofisticación de los intentos. Entonces cada vez que haya más seguridad habrá más ataques.

Para mantener su presencia con las ventas, los vendedores y fabricantes de hardware de seguridad luchan por simplemente distraer al atacante con sus productos, mientras que el atacante después de muchos intentos por ingresar termina por colapsar al sistema y finalmente consigue su objetivo, ya sea por sus métodos o las herramientas usadas.

Un ataque de intruso, es sólo una faceta de la seguridad que se debe proteger. Los virus son otra amenaza a la seguridad; el hecho de que se esparcen fácilmente hace que se generen las infestaciones rápidamente, por ello no es sólo un área la que hay que proteger sino todas.

Por ejemplo, los virus de gusano esparcen cuando los usuarios abren correo electrónico con enlaces de cadenas, que causa que el virus pueda enviarse por correo electrónico a la lista de contactos entera del usuario, Otros virus de tipo caballo de Troya puede entrar a su sistema y dar permisos de puertos para intrusos que usarán su computadora para hacer innumerables ataques en las máquinas de otros usuarios.

Enseñar cómo proteger su entorno de informática de éstas varias amenazas es el propósito de Hardening. Los administradores de sistemas de todo el mundo saben que la Internet es un entorno hostil. No pueden decir cuando un intruso intentará tener acceso al servidor, pero si pueden apostar que habrá un intento en algún momento que el usuario esté conectado. Y esto es porque el atacante sabe que el sistema operativo es vital para el funcionamiento de una computadora, y porque es el nexo principal entre los recursos disponibles de la máquina y sus lasos conexos.

Hardening

Es el proceso de proteger un sistema contra las amenazas desconocidas. Los administradores de sistemas los endurecen contra cualquiera que pueda ser la amenaza, pero hay una gran diferencia entre proteger el sistema de uso empresarial y el Sistema Operativo sobre el cual trabaja dicho sistema; entonces se está quedando pendiente e incompleto el trabajo sobre protección y al hablar de seguridad al hacer esto, es como no haber hecho nada para proteger nuestra máquina.

Para aplicar el Hardening se necesitara endurecer la seguridad de los sistemas operativos, Windows NT, 2000, XP, y 2003 -2008 Server que al final son resultantes de una misma configuración, pero con diferentes parámetros de medición en contra de las amenazas.

¿Qué es la seguridad?

Para proteger el bienestar o integridad de algo, para asegurar la propiedad o intereses de un objeto en contra de la infiltración, o para mantener un concepto u objeto privado; necesitará asegurar el sistema en donde se hallan dichos elementos. En el entorno hostil de la Internet, administradores de sistema necesitan restringir acceso a los bienes comunes, para otorgar acceso a un grupo escogido de usuarios necesita saber de quién fiarse y cómo verificar las credenciales de autentificación de lo contrario no hay forma de ingresar al mismo, peor aún lograr hacer uso de dicha información.

La norma de actuación sobre la seguridad incluye lo siguiente:

- ★ Retiro o la habilidad para mantener las cosas en privado y de forma confidencial.
- ★ La autenticidad o verificación de que los contactos son hechos por las personas que están representando exactamente la identidad que dicen ser.
- ★ Integridad o el proceso de aseguramiento en que el sistema no ha sido comprometido y estará seguro.

Hardening se enfocará totalmente en los aspectos prácticos de endurecer una computadora basada en Microsoft Windows, es decir de la forma más fácil a través del usuario y sus necesidades sobre seguridad. Entonces hay que moverse en las consideraciones prácticas, que no necesariamente son el limitar al Sistema Windows y no seguir las sugerencias que no son apropiadas para ninguna máquina.

El dilema de la seguridad

La seguridad depende de dos cosas: En primer lugar, una persona debe definir lo que la seguridad significa para él, y secundar en que necesariamente se debe comunicar para poder trabajar, que la idea clara y competente de su trabajo se desarrolla o está reflejada en la comunidad alrededor de él. La seguridad padece de tal problema en estos días debido a asuntos relacionados directamente con estas dos necesidades.

La Seguridad para cada persona; es totalmente diferente, sin embargo una persona puede ser satisfecha con una contraseña de BIOS y un disco flexible, mientras que otro individuo puede tener el doble de problemas por esta medida y otro el triple si codifican estos

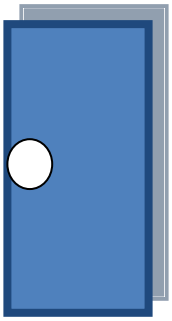
archivos. Y porque la definición, significado y valor intrínseco de la seguridad difieren así violentamente entre las partes, es difícil comunicar una norma de actuación sobre seguridad que sea clara a la comunidad de usuarios de un sistema operativo y en especial cuando cada uno de ellos realiza un trabajo diferente dentro de su empresa.

Dentro de la empresa u organización de a poco crece un problema crítico cuando el sistema no tiene protección y sólo se puede tener la seguridad utilizable y entendible como solución, es decir no hay otra salida que, proteger o perder la integridad del Sistema, pero siempre y cuando todos comprenden cual es el nivel de seguridad requerido y cuando todos acuerdan que la seguridad es estrictamente necesaria; y es que el acuerdo mutuo ayuda a la efectividad de la misma. Y en la práctica, como se podría imaginar, una comprensión de la seguridad de parte del usuario es de alguna forma importante y esta es generalmente deficiente.

La misma existencia de la seguridad reside en la confianza. En realidad, se puede argumentar que cada problema de seguridad queda reducido a una pregunta de confianza, por ello cada sector confiable se vuelve de ese modo por una sola razón y es que es seguro. La idea de la seguridad es introducida para el propósito único de protegerse contra alguien que no se confía, debido a sus intenciones maliciosas o debido a su competencia cuestionable. Para hacer esto, normalmente cierta tecnología lo que hace es ir al lugar, para modificar la confianza de una "zona" arriesgada e ir o llevarla a un área más tranquila o confiable (asegurada).

Un excelente ejemplo es una cerradura de puerta de entrada: No confía al público general, y por lo tanto es cuidadoso para con las personas que pueden ser enemigos potenciales y pueden terminar tomando sus pertenencias sin su conocimiento para lo cual

se instala una cerradura en la puerta de entrada de su casa la cual sin duda protegerá su ingreso y determina que no confía en el público general, pero si se confía en la cerradura para hacer su trabajo, el de mantener en el exterior a las personas intrusas.


Se tiene obviamente un problema menos pero No se puede confiar enteramente en la cerradura, así que se instala un sistema de alarma que notifica la policía si alguien entra en la casa y ahora se ha desplazado su desconfianza del público a la policía, del sistema de alarma, y la cerradura.

Cada día, que procede sobre su negocio, poniendo su confianza semiconsciente en los bancos, cajeros automáticos, los sitios de tienda en línea, la policía, siempre está pendiente que puede que esta seguridad también se rompa y también sabe que esto no significará ser el fin de todo. Pero entonces porque no tomar una medida de seguridad antes que aguardar a ver qué sucede.

Por ejemplo, cuando un joven aprende a manejar un automóvil, pone vidas en riesgo. Debido a este riesgo, la mayor parte de los municipios y gobiernos requieren que el joven tenga que pasar un examen para demostrar su maestría al manejo. Los sistemas de computadora son igualmente capaces de causar daño, aunque ellos no son conscientes. Su vida normal es interrumpida cuando los sistemas de computadora funcionan mal, y esto indica una confianza decreciente en ellos. Su confianza en computadoras y sus usuarios son a menudo bastante desatendidos. Ahí es donde los problemas verdaderamente vienen.

Enemigos de la seguridad

Para lograr la seguridad más verdadera y eficiente, los administradores del sistema necesitan examinar un método para analizar sistemas, para sondear sus debilidades y detallar sus propias suposiciones sobre esas protecciones del sistema, antes de poner ciegamente la confianza en ellos. Si la seguridad va a ser discutida en una vía más seria, lo que se necesita es:

- ★ Identificación de lo que uno está tratando de proteger.
- ★ La evaluación de las fuentes principales del riesgo y donde está ubicada toda el área de confianza
- ★ La suposición de medida preventiva ante posibles ataques potenciales

Se puede definir un sistema seguro, como uno en que todas las amenazas han sido analizadas y uno en que la medida preventiva está en su lugar apropiado para todas las amenazas.

Unos cuantos obstáculos se crean en los sistemas seguros.

El primero es la complejidad: los usuarios se volverán impacientes y el trabajo alrededor de la seguridad se vuelve demasiado pesado para su estilo de trabajo y flujo.

Después será la necesidad de la compatibilidad hacia el software. A menudo la seguridad es atrapada en las revisiones posteriores del software, pero para permanecer operable con la versión previa de un paquete, las restricciones de seguridad se pueden disminuir.

El problema, sin embargo, es cómo saber cuáles son todas las amenazas posibles contra un sistema, y ahí es donde Hardening entra es acción. No se puede siempre saber todas sus amenazas; es imposible en cierta medida tener todo el conocimiento. Pero si se puede asegurar las estradas y pre cautelar para impedir todas las infiltraciones futuras.

Lo que a Windows le hace falta

La parte para identificar todos los problemas de valor garantizado es mirar al producto en conjunto. ¿Dónde están sus debilidades y lo que es lo más vulnerable en cada parte?

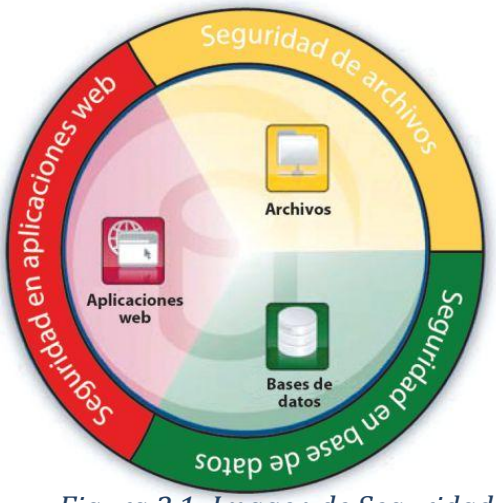


Figura 2.1: Imagen de Seguridades sobre Windows

Los tres problemas de Windows que son notables son:

Internet Explorer es el talón de Aquiles de clientes de Windows, y es desafortunado que el visor de navegación sea demasiado básico para algunos entornos de negocio. Aunque Windows XP Service Pack 2 ha hecho mucho para mejorar algunos detalles de la versión más reciente de Internet Explorer, Microsoft ha manifestado públicamente muchas veces que es incapaz para mejorar o reparar el conjunto de problemas de Internet Explorer sobre las versiones previas de Windows, incluyendo Windows 2000-- un cliente de negocio OS que es el usuario significativo evidentemente en empresas alrededor del mundo.

¿Qué puede hacer para mitigar este riesgo? unas cuantas cosas se aclaran para tener cuidado: Por supuesto, se pueda fomentar el uso de Windows XP. (Recuerde al comprar nuevos sistemas con un acuerdo de licencia de volumen de Microsoft, puede especificar una licencia de XP, pero con ello usted consigue bajar el nivel de derechos para correr

Windows 2000 mientras lo necesita. Así el gasto de las licencias ascendentes es alto). También, investigar otros tipos de navegadores bajo Windows como Mozilla y firefox ya que ambos son los visores más seguros.

El protocolo de llamada de procedimiento remoto (RPC) es una reliquia hoy en día ido por un método de comunicaciones depreciado que tiene intenciones para ser usado en una red en que todo lo que están compartiendo los anfitriones es de confianza.

¿Cuántas décadas han sido desde que era el caso? RPC esencialmente no tiene ningunos medios para ser protegido de los ataques con base en protocolos más simples de transmisión, y los anfitriones en uno u otro fin de una transacción de RPC no son a menudo bastante endurecidos para resistirse a la penetración. Por supuesto, los esfuerzos han sido hechos en las últimas liberaciones del cambio y seguridad de Internet y servidor de aceleración (ISA) para proporcionar unos medios más seguros para "incluir" RPC dentro de otros protocolos. Aunque desplegando el cambio 2003 y servidor de ISA 2004 son las vías buenas para disminuir el riesgo de RPC en la Internet, tales sistemas están tratando simplemente los síntomas y no el problema. Nosotros necesitamos lanzar RPC al exterior - como una cinta de beta en un mundo de Dvd, es simplemente no adecuado - y encontrar otra vía para transmitir un paquete pequeño de máquina a máquina.

Para en resumidas cuentas, cualquier contraseña con 14 o menos caracteres se codifican en aleatoriamente con un algoritmo de cálculo de clave que ha sido descifrado y así es simple para infiltra. Esta vulnerabilidad, aunque reducida, esté presente en 2003-- de servidor de Windows de modo supuesto el sistema operativo seguro. Esta era una equivocación en la parte de Microsoft, y aunque no puede esperar el propio producto Manager de LAN ha debido subir con una mejor forma las vías más rápidas para mitigar este riesgo para inhabilitar estos tipos de infiltraciones por la vía del grupo Policy, o para ordenar las contraseñas de 15 caracteres o más largas. Obviamente esta última elección

ha muchos benefició.

¿Qué podemos conseguir realmente?

- ★ Evitar el robo de información en el sistema
- ★ Inmunizar el sistema contra ataques conocidos
- ★ Maximizar el tiempo necesario para llevar a cabo un ataque en la plataforma

Imponer cambios que se ponen en práctica de mejor manera en un entorno manejado, que son diseñados para limitar la comunicación entre computadoras, para identificar y autorizar positivamente el personal, este es un cambio de la manera de pensar normal en un mundo de Windows.

Los sistemas principales deben todavía funcionar, pero probar otra forma de configuración en un entorno controlado es esencial para lograr un cambio efectivo.

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

Una de las primeras cosas que hay que dejar en claro del Hardening de sistemas operativos es que no necesariamente logrará forjar equipos invulnerables, sino sistemas operativos más seguros, que simplemente ayudaran a prevenir el 95% de las amenazas a las que el equipo se encuentra sujeto.

Y aquí es donde nace una pregunta que debería ser más o menos obvia. ¿Hasta qué punto el Hardening es una ayuda y no una molestia? En este punto, es importante considerar un paradigma muy interesante que tiene la seguridad.

Al parecer, la seguridad por un lado, y la versatilidad de uso de los sistemas por otro, son como dos grupos de personas tirando de ambos extremos de una cuerda. En pocas palabras, a medida que se busca una seguridad mayor en los sistemas, la versatilidad y facilidad de uso del mismo se ven limitados, puesto que la cantidad de decisiones que puede tomar el usuario se reduce y la cantidad de posibilidades ajenas al propósito inicial del sistema en sí disminuye drásticamente.

Por otro lado, el aumentar la versatilidad y la facilidad de uso de los sistemas pareciera estar muy relacionado con el aumento en las decisiones y posibilidades del usuario, lo que por consiguiente aumenta la probabilidad del mismo de equivocarse y poner en peligro la seguridad de todo el sistema. Y el debate sobre el punto exacto de equilibrio en cuanto a la cantidad de decisiones que deben pasar por manos del usuario final es bastante extenso y no está del todo resuelto.

Por lo tanto, la respuesta a la pregunta planteada es la siguiente:

El Hardening es una ayuda hasta el momento exacto en que entorpece el objetivo inicial que tiene el sistema. Por citar un ejemplo, si un sistema trabaja con impresoras, redes inalámbricas y además con correo electrónico, no es recomendable deshabilitar la cola de impresión, el servicio de redes inalámbricas ni bloquear los puertos de SMTP y POP. En otras palabras, en cada acción de Hardening que se vaya a ejecutar en el sistema operativo, hay que tener especial cuidado en que dichas acciones no afecten el propósito del sistema en sí.

Es debido a este tipo de situaciones que existen los niveles de seguridad, que son aplicados dependiendo no sólo del tipo de información que maneje ya sea importante o no, sino que también depende del área de acción o desarrollo en la que se encuentre ubicado el equipo.

Características generales de HARDENING

Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

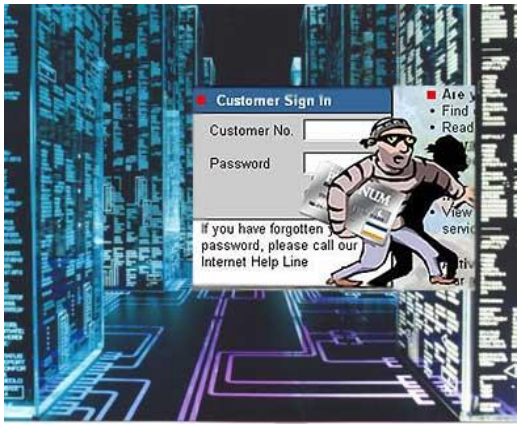
Una de las primeras cosas que hay que dejar en claro del Hardening de sistemas operativos es que no necesariamente logrará forjar equipos invulnerables. Es importante recordar que, según el modelo de defensa en profundidad, el host es sólo una capa de éste. En otras palabras, un factor más a considerar dentro del gran número de puntos a ser tomados en cuenta para defender globalmente un sistema.

Lo que podemos conseguir es:

- ☑ Proteger el sistema contra ataques y accesos no autorizados
- ☑ Prevenir el mal uso del sistema de los usuarios,
- ☑ Prevenir la pérdida de información y caídas del sistema.
- ☑ Evitar vectores de ataques conocidos
- ☑ Limitar el impacto de vulnerabilidades 0day
- ☑ No perder totalmente la funcionalidad del sistema
- ☑ Mejorar el rendimiento global

Los procesos de Hardening, a menudo se componen de una serie de pasos a seguir, los cuales involucran diferentes niveles de personalización acorde a la tarea del sistema operativo.

Haciéndole la vida difícil al atacante!!!



Ése es el concepto que está detrás del Hardening de sistemas operativos. Hardening es una acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo la seguridad de su equipo, con características que pueden ser de tipos básicas o elevadas.

Existen pasos de índole general, aplicables a cualquier dispositivo, sistema o aplicación, como por ejemplo: la instalación de services packs, la disposición de elementos de seguridad física y/o del entorno, etc. y también aquellos mas puntuales referidos específicamente al recurso que se está intentando asegurar (Software de Base de Datos Oracle, Software de Base de Datos SQL Server, Windows SO en cada una de sus variantes, Linux SO en cada uno de sus sabores, IOS de Cisco, etc.)

- Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

Mantener secretos (Principio básico de seguridad)

- Aprender a no revelar sus secretos, es una práctica buena para la seguridad, negarse a hablar sobre esas cosas que podría comprometer la misma. Otra forma de revelar las debilidades de su sistema es decir cualidades del mismo. Hay que darse cuenta lo que se está diciendo a las personas, hay que considerar la seguridad de sus sistemas de información como si se estuviese protegiendo su familia o a su país.

- Entre las actividades de Hardening se pueden contar las siguientes, las mismas que pretenden mitigar los ataques a áreas de mayor vulnerabilidad.

Esto NO significa que el proceso de Hardening contemple tan solo estos puntos, pero SI que tan sólo con este MINIMO detalle de configuración, el sistema podrá ser considerado más confiable.

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

Endurecimiento de sistemas Microsoft Windows

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

Windows propone varias soluciones para la seguridad de su sistema, y aunque el usuario en un comienzo trate de potenciarlas al máximo haciendo uso de éstas, la mayoría de opciones se quedan olvidadas o simplemente no utilizadas y es que Windows lo propone de esta manera el afinamiento de la seguridad de su sistema; es decir “Asegurar el sistema a su voluntad”.

Razón por la cual Microsoft no las muestra como opciones de configuración para el usuario, y simplemente están ahí, algunos casos configurados por defecto y en otros simplemente inhabilitados (vulnerables).

Reconociendo finalmente que no todos los usuarios son capaces de seleccionar el tipo de configuración que mejor se adapte a la seguridad a su sistema, una de las mejoras producidas en estos nuevos sistemas operativos, se conoce como “Mejor configuración por defecto”, un ejemplo de esta política es:

“Firewall Activado por defecto en XP SP2”, “IIS Desactivado por defecto en Windows 2003”.

A pesar de esto, no debemos desconocer de aquellas configuraciones que pueden elevar en gran medida el listón de seguridad, respecto de nuestro sistema operativo. Microsoft hace su esfuerzo intentando mejorar sus productos, pero como usuarios, también tenemos responsabilidad al momento de conectar a la red uno de nuestros equipos.

En lugar de aumentar la seguridad es mejor hacerse preguntas de " cómo puedo reducir el riesgo". Recordar que "perfeccionar " es el enemigo de " bastante" no hay que preocuparse sobre presentar la solución más perfecta, más bien concentrarse en la solución más práctica.

Las herramientas para la protección del sistema operativo Windows están ahí, solo es necesario saberlas manejar, y lo más importante saber cuándo aplicar.}

Hardening para Windows no es simplemente una herramienta que hay que aplicar, es un proceso por el cual se realiza un afinamiento de las opciones de configuración que Microsoft Windows ya definió previamente en cada uno de sus sistemas operativos.

Consideraciones de software

Los paquetes de servicio son las aplicaciones que son puestas en circulación después de la liberación pública de un paquete de software o parches a defectos que son encontrados después de la disponibilidad de corriente principal de una aplicación. La mayor parte de estos paquetes de servicio incluyen seguridad para corregir las áreas del código de programa que eran no aseguradas por los desarrolladores y por lo tanto eran vulnerabilidades.

Después en la lista son los virus, una irritación rápidamente en crecimiento. Como usted puede ser consciente, muchos nuevos virus son puestos en circulación semanalmente. Debe mantener al día en una base regular para con su antivirus. Para protegerse, de una mirada a esta guía:

- Cada software descargado de la Internet debe ser guardado e instalado en sistemas de prueba antes de cada producción, y el sistema se debe proteger de virus después de que el software haya sido examinado.

- Búsqueda con seguridad, no descargue software de las fuentes desconocidas; Esto causa peligro no solo el ordenador base sino también la red entera. Recientemente, los virus se están comenzando a esparcirse después de poner iníciales en la red compartida y los virus pueden causar muchas horas del tiempo muerto

- Para obtener el mejor resultado, se debe configurar el software de virus con el más restrictivo nivel, con eso se está asegurando que cada virus y su contenido en una computadora pierda su capacidad de infectar la red.

- La mayor parte de los programas de antivirus modernos incluyen la opción al interior para reparar un archivo infectado tendrá probablemente los resultados mezclados con este rasgo. Es aceptable reparar el archivo infectado pero por un período de tiempo de modo que el sistema pueda volverse operacional.

- Como una forma de práctica, siempre se recomienda que el disco duro infectado sea formateado a cero, para poderlo volver a reinstalar. Puesto que no se sabe exactamente la proporción de la infección.

- Restrinja los archivos con extensiones, tales como VBS, EXE, JPG, PCX, COM, y SCR, de su servidor de correo. Estos tipos de archivo son raramente usados para el negocio legítimo pueden ejecutarse accidentalmente por los usuarios confiados. Esta puede comprometer la red entera. ¿Recuerda el virus de melisa?

Esto asegura que un virus no se escabulle más allá de su cortafuego.

Consideraciones de hardware y red

Windows depende tanto de los dispositivos de hardware externos para la seguridad como de sus propios mecanismos internos.

La pieza más obvia del rompecabezas de dispositivos físicos es el cortafuego, una parte integral de cada red que es unida a la Internet. Sin un cortafuego, cualquier máquina de Internet puede estar unida o negada del servicio (DoS) ataques, los ataques de servicio, con esfuerzos de penetración de red son fichados junto con otros acontecimientos malos. Todos estos ataques son muy difíciles de encontrar su origen para lo cual es importante considerar las siguientes sugerencias de cortafuego:

- Bloquee los puertos de TCP 135,139 y 445, y puertos de UDP 135,137 y 445. Estos puertos de red de Microsoft Windows han sido tradicionalmente susceptibles a gran número de ataques de Servicios, y allí está el uso pequeño para ellos sobre la Internet.

- Bloquee todos los puertos no usados. Cada vez que usted abre un puerto crea un hueco pequeño alrededor de su red y lo reemplaza con una ventana. Los puertos abiertos invitan a ataques.

El hermano del cortafuego en la seguridad familiar es un sistema de detección de infiltraciones (IDS), otra parte vital de endurecer una red basada en Windows. Un IDS "rastrea" o inspecciona el trafico de ida en y que viene de fuera de una red, y distingue adentro de ese tráfico algo que puede indicar una actividad sospechosa.

Un IDS difiere de un cortafuego en que una pared de fuego mira a las intrusiones a fin de detenerlas en su accionar. El cortafuego limita el acceso entre redes a fin de prevenir entremetimiento y no comunicar un ataque del interior la red. Un IDS, por otra parte, evalúa un entremetimiento sospechoso una vez que ha tomado lugar, y comunica una alarma. Un IDS también vela para ataques que se originan de adentro de un sistema. Es una adición beneficiosa para la red. El acceso remoto queda como uno de los enlaces más débiles en la seguridad de red si se pone en práctica incorrectamente.

Si se permite el acceso remoto a la red o por las conexiones en línea o por una conexión de red (VPN) privada virtual, debe restringir el acceso en línea a los usuarios confiados en y limitar la funcionalidad de esos usuarios de las localizaciones remotas. Las políticas pueden ser diseñadas en tal vía que la actividad del usuario se trace, se recomienda una conexión de VPN: Los datos que viajan sobre un VPN son mucho menos susceptibles a la interceptación qué punto a punto normalmente protocoliza (PPP) conexiones sobre las redes de teléfono viejas sencillas.

Si sus datos son particularmente críticos, podría considerar poner sistemas en su lugar apropiado que requieren la validación credencial para cualquier recurso que se accede remotamente, como certificados de cliente lateral y los métodos de autenticación de contraseña fuertes.

Recolección de la información sobre seguridad aplicada en los sistemas de operativos Microsoft

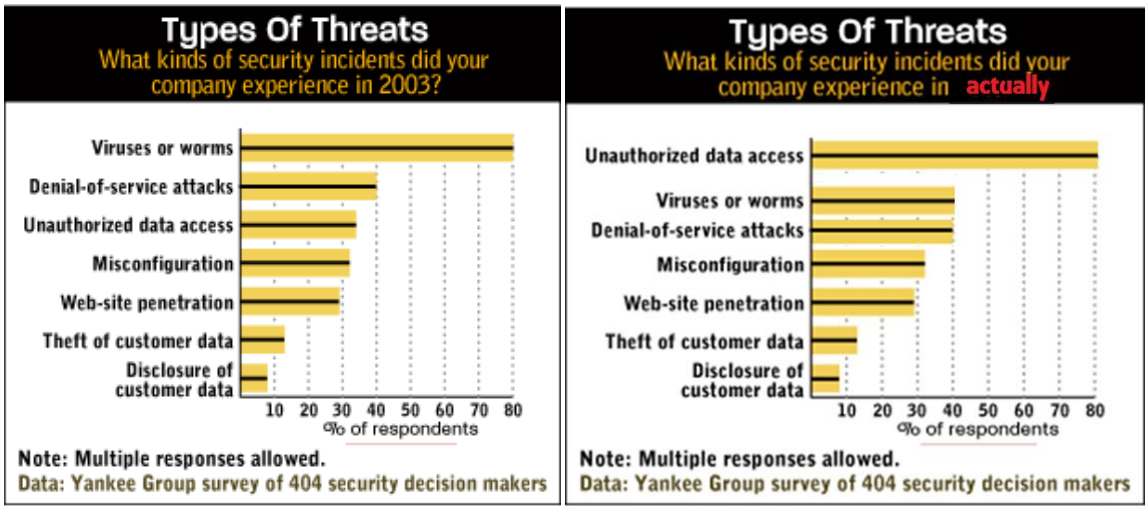


Figura 2.2: Estadísticas sobre ataques a sistemas operativos Windows.

Sólo hace siete años los ataques eran producidos por virus o los llamados gusanos, que ocasionaban perdida de información, y por ende retraso en el desarrollo de la empresa.

Hoy en día los ataques han dejado de ser sólo una molestia en retraso del tiempo de trabajo, ahora se han vuelto ataques de tipo infiltración y robo de información, ya sea externa o internamente.

Es decir, que los sistemas operativos ya no son forzados a romper sus seguridad con el uso de virus, sino que ahora los atacantes buscan sectores de libre circulación para ingresar sin sospecha ni forzamiento, esto es debido a algún as causas tales como:

- Falta de conciencia de usuarios finales.
- Presupuesto para implementación de medios de seguridad física o lógica.
- Falta de apoyo de la alta gerencia.
- Falta de Entrenamiento.
- Pobre definición de responsabilidades.
- Falta de herramientas.
- Aspectos legales.

La falta de conocimiento hace que no se defina correctamente la labor que debe asumir el sistema operativo para servir como tal.

Aplicación de Testers para análisis de riesgos

La herramienta TESTER es diseñada para medir el estatus de su sistema contra una norma. La herramienta no hará cambios a la seguridad, debe ser instalado como una aplicación y manejada como tal.

Existe más de una vía para poner en práctica las colocaciones y sugerencias descritas.
La meta de cada prueba de características y las herramientas asociadas son dar a los usuarios una vista en tiempo real de donde los sistemas están siendo situados en relación con la norma corrientemente aceptada. Esta "cuenta" producida por la herramienta es un número entre el cero y diez, y es derivado de las siguientes áreas.

Los criterios usados para analizar están divididos en cuatro categorías:

(1) ServicePacks y Hotfixes,
(2) las políticas,
(3) la forma de seguridad,
(4) servicios disponibles, derechos de usuario, archivos y permisos de registro, y otras necesidades de sistema.

Las aplicaciones o servicios adicionales pueden disminuir la cuenta completa, justo cuando los servicios adicionales disminuyan la seguridad de estos sistemas en el entorno de producción. Algunos tipos de pruebas de características de nivel II son desarrolladas para cubrir tales aplicaciones.

Cada una de las primeras tres categorías tienen un limitado el número de las necesidades principales y muchas necesidades menores. Por ejemplo, en el área de los paquetes de servicio y Hotfixes, la corriente Service Pack es un requerimiento principal, mientras que el otro Hotfixes puede ser considerado menores.

Debido al uso de estos parámetros de análisis de vulnerabilidades, se podría decir que el uso de herramientas para testear un sistema en cuanto a su seguridad, es eficaz siempre y cuando el análisis se haga por separado; es decir búsqueda de vulnerabilidades por sectores, archivos, servicios, configuraciones, etc. , teniendo como resultado negativo al empleo de esto ya que en el mercado no existen herramientas de este tipo; simple y llanamente evalúan un sistema por completo en algunos casos con resultados específicos y en otros generalizados.

Entonces lo importante es saber analizar esas áreas generalizadas para poderlas expandir y escarbar en su totalidad cuando una de las áreas es de suma importancia. Dependiendo claro del nivel de seguridad que portará ese equipo.

Un test de intrusión es una evaluación de las medidas de protección de una organización y de los servicios expuestos a Internet.

El objetivo es vulnerar la seguridad de los mecanismos Implantados para conseguir por ejemplo un acceso no autorizado a la organización, obtener información sensible, interrumpir un servicio, todo depende del alcance del test.

Un test de intrusión es diferente de una revisión de seguridad exhaustiva.

Comprobación del sistema

Este punto se basa en comprobar la robustez del sistema de autenticación en base a distintas técnicas.

- Pruebas de diccionario
- Fuerza Bruta
-

Evasión del sistema de autenticación (predicción de ID de sesión, SQL Injection, modificación de parámetros,..)

- PathTraversal
- Recordatorio de contraseña débil
- Análisis de gestión de la caché y salida de sesión

Prueba de gestión de sesiones

La gestión de sesiones comprende todos los controles que se realizan sobre el usuario, desde la autenticación hasta la finalización de la aplicación.

Los elementos a evaluar son los siguientes:

- Análisis del esquema de gestión de sesiones
- Manipulación de cookies y testigos de sesión.
- Variables de sesión expuestas
- Abuso de sesión

Las herramientas para pruebas dan soporte al usuario para determinar falencias en el sistema que no siempre son detectadas a simple vista, cada una de las herramientas esta creada para determinar sectores de afectación y se basan en la fase de la seguridad (EVALUACIÓN) y es de esta forma como se realizan los análisis en base a lo siguiente:

Evaluación (Assess):

- Análisis de Riesgos basados en el OCTAVE method.
- Debilidades en Seguridad Informática (auditorías, evaluación de Vulnerabilidades, pruebas de penetración, revisión de aplicaciones)

RESULTADOS

El Análisis de Riesgos a través de estos testers nos permitirá:

Realizar acciones:

- Proactivas
- Reactivas

Administrar el Riesgo:

- Identificar
- Analizar
- Evaluar
- Determinar el tratamiento a seguir.

Existen tester en el mercado tales como MBCA, Benchmarking CIS, que se pueden conseguir fácilmente y que suelen ser de gran ayuda a la hora de buscar vulnerabilidades; el único inconveniente es saber interpretar los resultados de los mismo.

Manejo de herramientas

Microsoft en su intento por hacer software para todas las necesidades de los informáticos. Presenta una actualización de su aplicación de administración de vulnerabilidades **Microsoft Baseline Security Analyzer** (MBSA).

Puede ser que no sea la mejor (de hecho no lo es) pero para las personas que quieren empezar a conocer de que se trata las vulnerabilidades o que desean hacer un muy rápido vistazo de su red esta herramienta puede que le ayude a examinar de manera superficial y así hacerse a una idea de la seguridad en su entorno.

Es una herramienta gratis que incluye interface tanto grafica como de línea de comandos (poco a poco Microsoft entiende de esta necesidad). **MBSA no está en nuestro idioma**, pero realmente no es un inconveniente.

Tiene cosas malas como que necesita conectarse a internet para descargar las "recomendaciones" de Microsoft, solo funciona obviamente para "escanear" maquinas que ejecuten sistemas operativos de Microsoft.

NOTA: MBSA NO es una herramienta profesional y probablemente NUNCA lo sea. Sin embargo para las personas que DESEAN EMPEZAR pueden hacerlo con este software.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) es una herramienta fácil de usar diseñada para los profesionales de TI que ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad según las recomendaciones de seguridad de Microsoft y ofrece orientación de soluciones específicas. Mejore el proceso de administración de seguridad utilizando MBSA para detectar los errores más comunes de configuración de seguridad y actualizaciones de seguridad que falten en sus sistemas informáticos.

MBSA 2.1

MBSA 2.1 es la última versión de la herramienta de análisis gratuita de evaluación de seguridad y vulnerabilidades de Microsoft para administradores, auditores de seguridad y profesionales de TI.

MBSA 2.1 ofrece compatibilidad con Windows Vista y Windows Server 2008, una interfaz de usuario revisada, compatibilidad de 64 bits, compatibilidad mejorada con Windows Embedded y compatibilidad con las últimas versiones del Agente de Windows Update (WUA) basadas en Microsoft Update.

MBSA 2.1 también es compatible con Microsoft Update, Windows Server UpdateServices 2.0 y 3.0, la herramienta SMS InventoryToolfor Microsoft Update (ITMU) y SCCM 2007.
Para obtener una lista completa de los productos que admite MBSA 2.1 basado en las tecnologías de Microsoft Update (MU) y Windows Server UpdateServices (WSUS).

Compatibilidad con productos anteriores:

Los usuarios que tengan los siguientes productos en su entorno pueden usar ShavlikNetChkLimited para aumentar los resultados de MBSA 2.0.1 con el fin de obtener una detección exhaustiva de las actualizaciones de seguridad.

- Office 2000
- ISA Server 2000
- Extensiones de servidor de FrontPage 2000/2002
- Visual Studio .Net 2002/2003
- SQL Server 7.0/2000

NG ScoringTool

La herramienta de CIS Scoring habilitan usuarios finales para verificar que la configuración de seguridad de sistemas antes de despliegue de red, sistemas de monitor y dispositivos de red para la conformidad progresiva con las pruebas de características, y demuestre a oyentes y socios de negocio su sumisión con las normas internacionalmente aceptadas para la configuración de seguridad.

CIS produce los informes que guían a los usuarios y administradores de sistema para asegurar ambas nuevas instalaciones y sistemas de producción.

La herramienta de NG lee un archivo Benchmark configurado previamente y la configuración de Windows, verifica los archivos, ambos archivos están en el formato de XML. Los archivos Benchmark expresan las recomendaciones de configuración de consenso. Ellos instruyen la herramienta de NG para verificar la seguridad técnica de un sistema controles e informe en la sumisión de esos controles con las recomendaciones de prueba de características.

La configuración verifica los archivos que expresan el método de la herramienta de NG que usa para verificar el sistema para los controles recomendados técnicos.

Instruyen la herramienta de NG en cómo ejecutar la configuración verifican los datos detallados los cuales indican lo generado por el proceso de comprobación de sumisión que habilitan los usuarios para comparar la configuración de sus sistemas con las recomendaciones de prueba de características (definido como “items” de prueba de características).

Para las configuraciones de sistema que es de acuerdo con las recomendaciones de prueba de características, la herramienta de NG relata esos artículos de prueba de características como “pass.” Para las configuraciones de sistema NO de acuerdo con las recomendaciones de prueba de características, la herramienta de NG relata ésos artículos de prueba de características como “fail.” Los informes también guían a los usuarios en cómo configurar los controles recomendados en artículos de “failed”, con eso mejorando la configuración de seguridad del sistema escudriñado y lo crie en la sumisión más cercana con la norma de configuración de consenso.

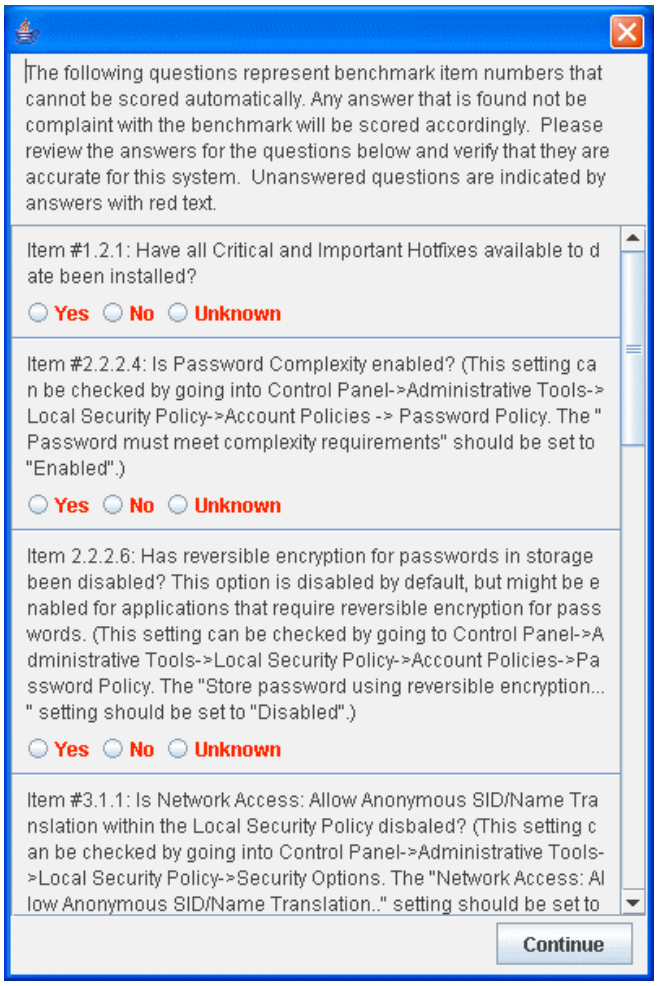


Figura 2.3: Grafico ejemplo de tabla de cuestionario para comparación de archivos.

Análisis de vulnerabilidades - Sectores de Acción y afectación

La meta de cada prueba de características y el uso de las herramientas asociadas son dar a usuarios una vista del punto en el tiempo de donde los sistemas están situados en relación con la norma con la que fue evaluado.

Este "score" producido por la herramienta es un número entre el cero y diez, y es derivado de la tabla de abajo figura 3.

Los criterios usados para determinar estos sectores están divididos en cuatro categorías:

(1) Service Packs y Hotfixes
(2) Políticas
(3)Valores de Seguridad y
(4) Servicios disponibles, Derechos de usuario, Archivo, permisos de registro, otras necesidades del sistema.

Cada categoría explica un cuarto de cuadrante. Las aplicaciones o servicios adicionales pueden disminuir el cuadrante, justo cuando los servicios adicionales disminuyen la seguridad de estos sistemas en el entorno de producción también lo hace.

Cada una de las primeras tres categorías tienen un limitado el número de las necesidades principales y muchas necesidades menores. Por ejemplo, en el área de los ServicePacksy Hotfixes, el último Service Pack es un requerimiento principal, mientras que Hotfixes puede ser considerado menor.

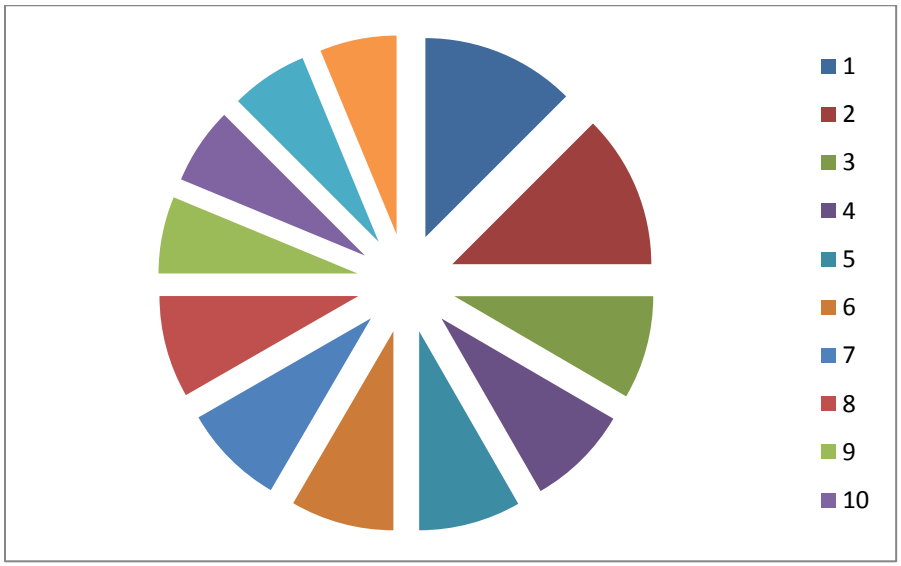


Figura 2.4: Sectores de afectación (4 Cuadrantes)

Tabla 2.1: Especificaciones de cuadrantes

1	Service Packs y Hotfixes: último Service Pack Instalado
2	Service Packs and Hotfixes: Otros Hotfixes
3	Políticas de cuenta y de examen de cuentas: Ninguna contraseña expirada
4	Las políticas de cuenta y de examen de cuentas: Políticas en base a estandares
5	Las políticas de cuenta y de examen de cuentas: Valores de acceso
6	Opciones de seguridad: Restricciones de cuenta de anónimo
7	Opciones de seguridad: Las opciones de seguridad en base a normas
8	Opciones de seguridad: Valores adicionales de seguridad
9	Servicios disponibles
10	Derechos de usuario
11	Otras necesidades del sistema
12	Los permisos de archivo y de registro

Manejo del Editor de Registros de Windows

Introducción al registro de Windows

Una base de datos jerárquica central utilizada en Microsoft Windows 98, Windows CE, Windows NT y Windows 2000 con el fin de almacenar información necesaria para configurar el sistema para uno o varios usuarios, aplicaciones y dispositivos de hardware.

El Registro contiene información que Windows utiliza como referencia continuamente, por ejemplo los perfiles de los usuarios, las aplicaciones instaladas en el equipo y los tipos de documentos que cada aplicación puede crear, las configuraciones de las hojas de propiedades para carpetas y los iconos de aplicaciones, los elementos de hardware que hay en el sistema y los puertos que se están utilizando.

El Registro reemplaza la mayoría de los archivos .ini basados en texto que se utilizan en los archivos de configuración de Windows 3.x y MS-DOS, como Autoexec.bat y Config.sys. Aunque el Registro es común a varios sistemas operativos Windows, existen algunas diferencias entre ellos.

Una sección del Registro es un grupo de claves, subclaves y valores del Registro que cuentan con un conjunto de archivos auxiliares que contienen copias de seguridad de sus datos. Los archivos auxiliares de todas las secciones excepto HKEY_CURRENT_USER están en la carpeta %SystemRoot%\System32\Config en Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 y Windows Vista. Los archivos auxiliares para HKEY_CURRENT_USER están en la carpeta %SystemRoot%\Profiles\nombreDeUsuario. Las extensiones de los archivos de estas carpetas indican el tipo de datos que contienen. A veces, la falta de extensión también puede indicar el tipo de datos que contienen Vease Figura 4.

Sección del Registro	Archivos auxiliares
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Figura 2.5: Secciones del registro de Windows

En Windows 98, los archivos del Registro se denominan User.dat y System.dat. En Windows Millennium Edition, los archivos del Registro se denominan Classes.dat, User.dat y System.dat.

Nota: las características de seguridad de Windows NT, Windows 2000, Windows XP, Windows Server 2003 y Windows Vista permiten que un administrador controle el acceso a las claves del Registro.

La siguiente tabla (Figura 5) enumera las claves predefinidas que utiliza el sistema. El tamaño máximo del nombre de una clave es de 255 caracteres.

HKEY_CURRENT_CONFIG	Contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.

Figura 2.6. Claves que usa el sistema

Carpeta o clave predefinida	Descripción
HKEY_CURRENT_USER	Contiene la raíz de la información de configuración del usuario que ha iniciado sesión. Las carpetas del usuario, los colores de la pantalla y la configuración del Panel de control se almacenan aquí. Esta información está asociada al perfil del usuario. Esta clave a veces aparece abreviada como "HKCU".
HKEY_USERS	Contiene todos los perfiles de usuario cargados activamente en el equipo. HKEY_CURRENT_USER es una subclave de HKEY_USERS. HKEY_USERS puede aparecer abreviada como "HKU".
HKEY_LOCAL_MACHINE	Contiene información de configuración específica del equipo (para cualquier usuario). Esta clave a veces aparece abreviada como "HKLM".
HKEY_CLASSES_ROOT	Es una subclave de HKEY_LOCAL_MACHINE\Software. La información que se almacena aquí garantiza que cuando abra un archivo con el Explorador de Windows se abrirá el programa correcto. Esta clave a veces aparece abreviada como "HKCR". En el caso de Windows 2000, esta información se almacena en dos claves: HKEY_LOCAL_MACHINE y HKEY_CURRENT_USER. La clave HKEY_LOCAL_MACHINE\Software\Classes contiene la configuración predeterminada que se puede aplicar a todos los usuarios del equipo local. La clave HKEY_CURRENT_USER\Software\Classes contiene la configuración que invalida la configuración predeterminada y que se aplica únicamente al usuario interactivo. La clave HKEY_CLASSES_ROOT proporciona una vista del Registro que combina la información de estos dos orígenes. HKEY_CLASSES_ROOT también proporciona una vista combinada para los programas diseñados para versiones anteriores de Windows. Para cambiar la configuración del usuario interactivo, se deben realizar los cambios en HKEY_CURRENT_USER\Software\Classes en lugar de en HKEY_CLASSES_ROOT. Para cambiar la configuración predeterminada, se deben realizar los cambios en HKEY_LOCAL_MACHINE\Software\Classes. Si escribe valores en una clave de HKEY_CLASSES_ROOT, el sistema almacena la información en HKEY_LOCAL_MACHINE\Software\Classes. Si escribe valores para una clave en HKEY_CLASSES_ROOT y la clave ya existe en HKEY_CURRENT_USER\Software\Classes, el sistema almacenará la información ahí, en lugar de en HKEY_LOCAL_MACHINE\Software\Classes.

Nota: el Registro en las versiones de 64 bits de Windows XP, Windows Server 2003 y Windows Vista se divide en claves de 32 y de 64 bits. Muchas de las claves de 32 bits tienen los mismos nombres que sus homólogas de 64 bits y viceversa. La versión de 64 bits predeterminada del Editor del Registro que se incluye con las versiones de 64 bits de Windows XP, Windows Server 2003 y Windows Vista muestra las claves de 32 bits bajo el nodo siguiente:

HKEY_LOCAL_MACHINE\Software\WOW6432Node

Ampliación de información sobre registro en Windows de 64 bits. Véase Anexos

¿Para qué utilizar el registro de Windows?

El conocimiento de las bases del registro de Windows puede ser muy importante a la hora de resolver un problema o para personalizar el comportamiento del sistema operativo o de las aplicaciones. También puede ser necesario para hacer respaldos de nuestra configuración.

Básicamente sirve para dar soporte a los sistemas operativos y programas de Microsoft y muchos de los contenidos tratan sobre modificaciones en el registro.

¿Qué es el registro?

Es la base de datos de todas las versiones de Windows donde se guarda la información sobre la configuración y el comportamiento del sistema operativo, hardware instalado y las aplicaciones.

Precauciones que debemos tomar

El registro es fundamental para el sistema operativo y si se corrompe o si lo dañamos cuando lo editamos podemos tener serios problemas e incluso el sistema operativo puede llegar a ser inservible. Por eso siempre debemos tener mucho cuidado a la hora de

manejar el registro. Deberíamos tener la costumbre de guardar copias de seguridad del registro. La forma de hacerlo es distinta para cada versión de Windows. Si eres usuario de Windows 95 te recomiendo que utilices ERU.EXE, la pequeña utilidad escondida en algún lugar del CD de Windows que nos puede salvar la vida en más de una ocasión. Si eres usuario de Windows 98 es suficiente que ejecutes scanreg desde Inicio/Ejecutar para hacer una instantánea del registro. Los usuarios de Windows ME lo tienen aún más fácil con SystemRestore que encontrarán en Inicio/Programas/Accesorios/Herramientas de sistema. Solo se necesita crear un nuevo punto de restauración cada vez que vamos a manipular el registro o instalar un programa.

¿Cómo editamos el registro?

Para eso utilizaremos el editor del registro de Windows (regedit.exe). Vamos al menú Inicio/Ejecutar y escribimos "regedit" (sin comillas). Se abrirá una ventana parecida a ésta:

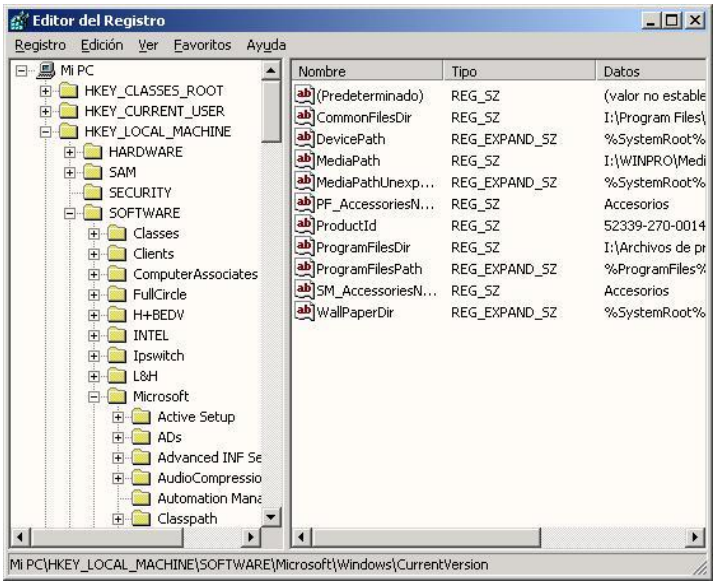


Figura 2.7: Registro de Windows RegEdit

En el panel izquierdo veremos el árbol del registro con Mi PC a la cabeza y debajo los seis subárboles. Los subárboles se componen de claves y las claves a su vez se componen de subclaves. Esto puede parecer un poco complicado, por eso, normalmente se utiliza la palabra "rama" para referirse a cualquier nivel del registro. Podemos expandir y contraer cada rama pulsando "+" que está junto a su nombre. En el panel derecho veremos dos o tres columnas, a la izquierda están los nombres de los datos y a la derecha sus valores.

Buscar en el Registro

Utilizaremos para ello el menú "Edición/Buscar" (o Ctrl+F) y escribimos en el diálogo el nombre que queremos encontrar, por ejemplo una dll que nos da problemas y queremos. Regedit la buscará y nos mostrará el primer resultado. Para seguir buscando, utilizaremos el botón "Buscar siguiente" o simplemente pulsaremos F3.

Agregar o eliminar subclaves.

Es algo que debemos hacer con muchísimo cuidado:

Para agregar:

1. Seleccionamos la rama donde queremos agregar la subclave.
2. Vamos a Edición/Nuevo/Clave o pulsamos con el botón secundario la clave y seleccionamos "Nuevo/Clave" del menú contextual. Se creará una clave con el nombre de "Nueva clave".
3. Cambiamos el nombre por el deseado.

Para eliminar:

1. Seleccionamos la subclave que queremos eliminar.
2. Pulsamos "Eliminar" desde el menú "Edición" o desde le menú contextual.

Modificar los valores de una clave (figura 7.)

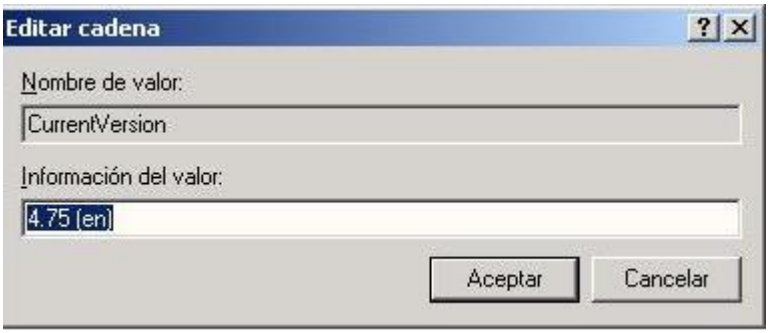


Figura 2.8: Menú cambio de clave

Agregar o eliminar valores a subclaves

Tenemos tres tipos principales de valores: Cadena, Binario, DWord. Windows NT tiene además Cadena Expandible y Cadena Múltiple. Para agregar el valor a una clave primero la seleccionamos y después pulsamos "Nuevo" en el menú "Edición" o en el menú contextual y seleccionamos el tipo del valor que queremos agregar.

Para eliminar un valor, lo seleccionamos y pulsamos "Eliminar" en el menú "Edición" o en el menú contextual.

Exportar y combinar claves

Es la característica más útil del editor de Windows. Nos permite:

1. Hacer respaldos de una clave antes de modificarla y así nos aseguramos que el registro estará a salvo si las cosas no funcionan después de modificarlo.
2. Hacer respaldos de nuestra configuración para reproducirla en otra máquina o después de formatear el disco y reinstalar Windows. Debemos tener en cuenta que puede haber diferencias entre los registros de diferentes versiones de Windows o

distintas versiones de programas, por ejemplo entre Outlook Express 4 y Outlook Express5.

Para exportar una clave, primero la seleccionamos y después pulsamos "Exportar archivo del registro" en el menú "Registro". El archivo exportado se guardará con la extensión *.reg, nosotros le ponemos un nombre. Debemos tener en cuenta que si queremos exportar una clave de Windows 2000 o Windows XP a Windows 9.x, la debemos guardar en formato de Regedit 4 que seleccionamos de la lista desplegable "Tipo" del cuadro de diálogo "Guardar".

Y para introducir la clave guardada es suficiente con hacer un doble click sobre el archivo guardado o seleccionar "Combinar" en el menú contextual".
Como se puede identificar, cada clave principal comienza con un "HKEY_" que iene de "Key Handle".

HKEY_CLASSES_ROOT

Esta rama se guarda en el archivo System.dat y contiene los nombres de todos los tipos de archivo registrados y también los manejadores de las hojas de las propiedades y otros componentes ActiveX. Esta rama es un puntero hacia la subclave HKEY_LOCAL_MACHINE\SOFTWARE\Classes y contiene a su vez dos tipos de claves:
Las claves de las extensiones de los tipos de archivo que contiene definiciones de los conocidos tipos de archivo (por ejemplo, .txt, .doc, etc) y *las claves de definición de clase* que especifican las propiedades de *shell*y OLE de una clase o tipo de documento. Entre estas claves se encuentran los CLSID (ClassIdentifier) de los controles ActiveX.

HKEY_CURRENT_USER

Contiene la información de perfil del usuario que está usando la máquina en este momento. Esta clave es muy útil para nosotros ya que ahí están todas nuestras configuraciones personales y nuestras preferencias.

HKEY_LOCAL_MACHINE

Contiene los datos de configuración del equipo local. Esta información está utilizada por las aplicaciones, controladores de dispositivos y su configuración es la misma para todos los usuarios.

HKEY_USERS

Contiene la información de los perfiles de todos los usuarios y además la subclave "Default" que es para los usuarios que no tengan un perfil configurado.

HKEY_CURRENT_CONFIG

Contiene la información acerca la configuración del sistema actual.

HKEY_DIN_DATA

Contiene la información de configuraciones que se almacenan en la RAM para optimizar el desempeño del sistema. La información contenida en esta subclave se crea cada vez que Windows arranca.

El registro de Windows posee una estructura inmensa y muy compleja y no existe ningún "Catálogo general" de todas sus claves, subclaves y datos. Aquí solo se ha descrito las partes claves del editor.

Realizar una copia de seguridad del Registro

Antes de modificar el Registro, exporte las claves del Registro que desee modificar o haga una copia de seguridad de todo el Registro. Si se produce algún problema, puede seguir los pasos descritos en la sección "Restaurar el Registro" para restaurar el Registro a su estado anterior. Para realizar una copia de seguridad de todo el Registro, emplee la utilidad Copia de seguridad para hacer una copia de seguridad del estado del sistema. El estado del sistema incluye el Registro, la Base de datos de registro de clases COM+ y sus archivos de inicio.

Modificar el Registro

Para modificar datos del Registro, un programa debe utilizar las funciones del Registro definidas en el siguiente sitio web de MSDN:
http://msdn2.microsoft.com/es-es/library/ms724875.aspx
Los administradores pueden modificar el Registro con el Editor del Registro (Regedit.exe o Regedt32.exe), Directiva de grupo, Directiva del sistema o archivos del Registro (.reg), o bien ejecutando scripts como los archivos de scripts de Visual Basic.

Utilizar la interfaz de usuario de Windows

Se recomienda que utilice la interfaz de usuario de Windows para cambiar la configuración del sistema, en lugar de modificar el Registro manualmente. Sin embargo, modificar el Registro puede ser a veces el método mejor para resolver un problema del

producto. Si el problema está documentado en Microsoft Knowledge Base, dispondrá de un artículo con instrucciones paso a paso para modificar el Registro en relación con ese problema. Recomendamos que siga exactamente esas instrucciones.

Utilizar el Editor del Registro

Advertencia: pueden producirse problemas graves si modifica incorrectamente el Registro mediante el Editor del Registro o con cualquier otro método. Estos problemas pueden requerir que reinstale el sistema operativo. Microsoft no puede garantizar la solución de esos problemas. Modifique el Registro bajo su responsabilidad.

Puede utilizar el Editor del Registro para hacer lo siguiente:

- Buscar un subárbol, clave, subclave o valor
- Agregar una subclave o un valor
- Cambiar un valor
- Eliminar una subclave o un valor
- Cambiar el nombre de una subclave o un valor

El área de navegación del Editor del Registro muestra carpetas. Cada carpeta representa una clave predeterminada del equipo local. Cuando se obtiene acceso al Registro de un equipo remoto, sólo aparecen dos claves predefinidas: HKEY_USERS y HKEY_LOCAL_MACHINE.

Utilizar Directiva de grupo

Microsoft Management Console (MMC) hospeda herramientas administrativas que puede utilizar para administrar redes, equipos, servicios y otros componentes del sistema. El complemento Directiva de grupo de MMC permite a los administradores definir la configuración de la directiva aplicada a equipos o a usuarios. Puede implementar Directiva de grupo en equipos locales utilizando el complemento de directiva de grupo local de

MMC, Gpedit.msc (Figura 8). Puede implementar la directiva de grupo en Active Directory utilizando el complemento Usuarios y equipos de Active Directory de MMC.

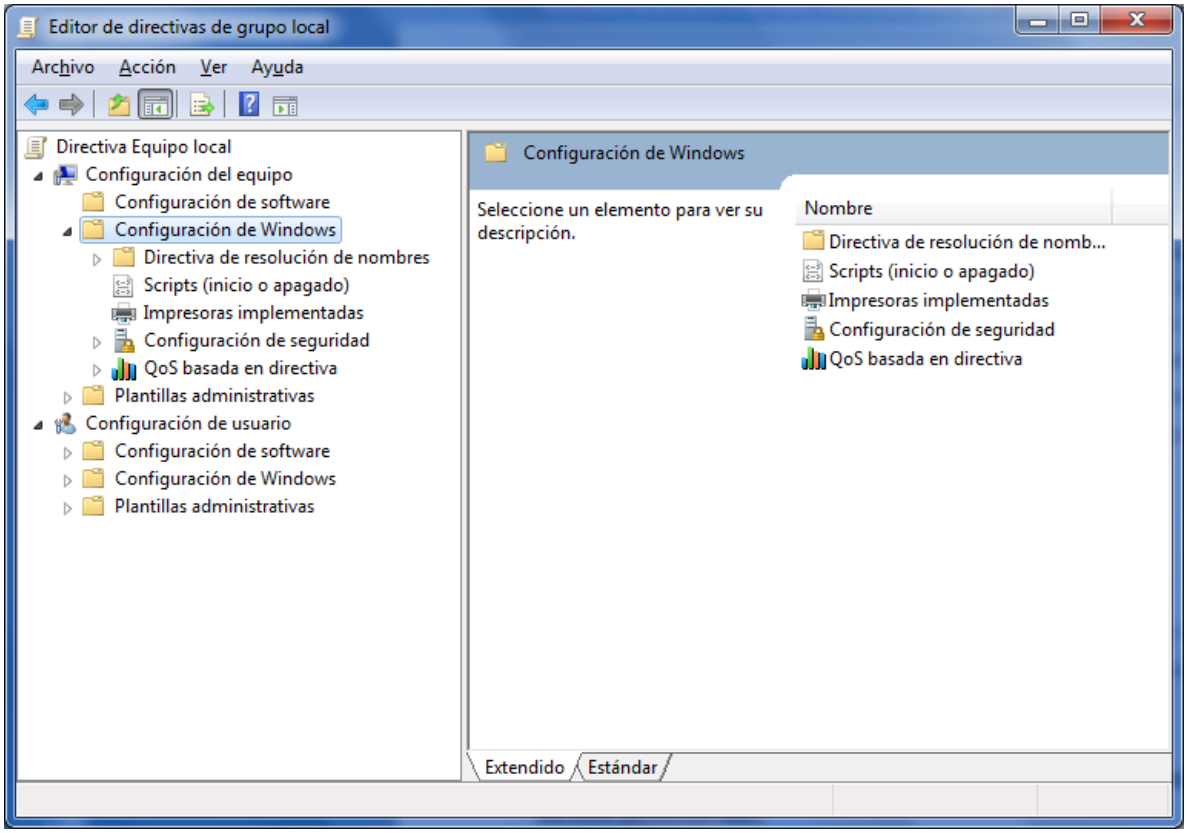


Figura 2.9: Menú de opciones de directivas de grupo

- **Utilizar un archivo de entradas del Registro (.reg)**

Cree un archivo de entradas del Registro (.reg) que contenga los cambios del Registro y ejecute el archivo .reg en el equipo en el que desee realizar los cambios. Puede ejecutar el archivo .reg manualmente o mediante un script de inicio de sesión.

Cómo agregar, modificar o eliminar subclaves y valores del Registro mediante un archivo de entradas de registro (.reg)

ADVERTENCIA: si utiliza incorrectamente el Editor del Registro, puede causar serios problemas que tal vez requieran volver a instalar el sistema operativo. Microsoft no garantiza que pueda solucionar los problemas resultantes del uso incorrecto del Editor del Registro. Utilice el Editor del Registro bajo su responsabilidad.

Aquí se describe cómo agregar, modificar o eliminar subclaves y valores del Registro mediante un archivo de entradas de Registro (.reg). Regedit.exe utiliza archivos .reg para importar y exportar las subclaves y valores del Registro. Puede utilizar estos archivos .reg para distribuir de forma remota los cambios del Registro en varios equipos basados en Windows. Cuando ejecuta un archivo .reg, su contenido se combina en el Registro local. Por consiguiente, debe distribuir los archivos .reg con precaución.

Sintaxis de los archivos .Reg

Un archivo .reg tiene la sintaxis siguiente:

versiónEditorRegistro
línea en blanco
[*rutaRegistro1*]
"*nombreDato1*"="*tipoDatos1*:*valorDatos1*"
nombreDato2"="*tipoDatos2*:*valorDatos2*"
línea en blanco
[*rutaRegistro2*]
"*nombreDato3*"="*tipoDatos3*:*valorDatos3*"

donde:

versionEditorRegistro es cualquier "Editor del Registro de Windows versión 5.00" para Windows 2000, Windows XP y Windows Server 2003 o "REGEDIT4" para Windows 98 y Windows NT 4.0. El encabezado "REGEDIT4" también funciona en equipos basados en Windows 2000, Windows XP o Windows Server 2003.

línea en blanco es una línea en blanco. Esto identifica el inicio de una nueva ruta del Registro. Cada clave o subclave es una nueva ruta del Registro. Si tiene varias claves en el archivo .reg, las líneas en blanco pueden ayudarle a examinar y solucionar problemas del contenido.

rutaRegistrox es la ruta de la subclave que contiene el primer valor que va a importar. Agregue la ruta entre corchetes y separe cada nivel de la jerarquía con una barra diagonal inversa. Por ejemplo:
[HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\Microsoft\Windows\System]

Un archivo .reg puede contener varias rutas de Registro. Si la parte inferior de la jerarquía en la instrucción de ruta no existe en el Registro, se crea una nueva subclave. El contenido de los archivos de Registro se envía al Registro en el orden en que se especifica. Por consiguiente, si desea crear una nueva subclave con otra por debajo de ella, debe escribir las líneas en el orden correcto.

nombreDatox es el nombre del dato que desea importar. Si un dato del archivo no existe en el Registro, el archivo .reg lo agrega (con el valor del dato). Si un dato existe, el valor del archivo .reg sobrescribe el existente. Las comillas contienen el nombre del dato. Un signo igual (=) sigue inmediatamente al nombre del dato.

tipoDeDatosx es el tipo de datos del valor del Registro y sigue inmediatamente al signo igual. Para todos los tipos de datos distintos de REG_SZ (un valor de cadena), un signo de dos puntos sigue inmediatamente al tipo de datos. Si el tipo de datos es REG_SZ, no incluya el valor de tipo de datos ni los dos puntos. En este caso, Regedit.exe supone REG_SZ para el tipo de datos. En la tabla (figura 9.) siguiente se muestran los tipos de datos del Registro típicos:

Tipo de datos	Tipo de datos en .reg
REG_BINARY	hexadecimal
REG_DWORD	dword
REG_EXPAND_SZ	hexadecimal (2)
REG_MULTI_SZ	hexadecimal (7)

Figura 2.10: Tipos de datos

valorDatosx sigue inmediatamente al signo de dos puntos (o al signo igual con REG_SZ) y debe estar en el formato adecuado (por ejemplo, cadena o hexadecimal). Utilice el formato hexadecimal para los datos binarios.

Nota: puede escribir varias líneas de datos para la misma ruta del Registro.

Agregar subclaves del Registro o agregar y cambiar valores del Registro

Para agregar una subclave o agregar o cambiar un valor del Registro, realice los cambios adecuados en el Registro y, a continuación, exporte la subclave o subclaves adecuadas. Las subclaves del Registro exportadas se guardan automáticamente como archivos .reg. Para realizar cambios en el Registro y exportarlos a un archivo .reg, siga estos pasos:

1. Haga clic en **Inicio** y en **Ejecutar**, escriba **regedit** en el cuadro **Abrir** y haga clic en **Aceptar**.

2. Busque la subclave que contenga el elemento o elementos del Registro que desee cambiar y haga clic en ella.
3. Haga clic en **Archivo** y, después, en **Exportar**.

   De este modo se hace una copia de seguridad de la subclave antes de realizar cualquier cambio. Puede importar de nuevo este archivo en el Registro después si sus cambios provocan algún problema.
4. En el cuadro **Nombre de archivo**, escriba un nombre de archivo para guardar el archivo .reg con los elementos del Registro originales y, a continuación, haga clic en **Guardar**.

   Nota: use un nombre de archivo que le recuerde al contenido, por ejemplo, una referencia al nombre de la subclave.
5. En el panel derecho, agregue o modifique los elementos del Registro que desee.
6. Repita los pasos 3 y 4 para exportar de nuevo la subclave, pero use un nombre de archivo diferente para el archivo .reg. Puede utilizar este archivo .reg para realizar cambios en el Registro de otro equipo.
7. Pruebe sus cambios en el equipo local. Si ocasionan algún problema, haga doble clic en el archivo que contenga la copia de seguridad de los datos originales del Registro para devolverlo a su estado original. Si los cambios funcionan como se esperaba, puede distribuir el archivo .reg que creó en el paso 6 en otros equipos utilizando los métodos de la sección "Distribuir los cambios del Registro" que se explica más adelante.

Eliminar claves y valores del Registro

Para eliminar una clave del Registro con un archivo .reg, ponga un guión (-) delante de *RegistryPath* en el archivo .reg. Por ejemplo, para eliminar la subclave **Test** de la clave del Registro siguiente:

HKEY_LOCAL_MACHINE\Software

ponga un guión delante de la clave del Registro siguiente en el archivo .reg:

HKEY_LOCAL_MACHINE\Software\Test

El ejemplo siguiente tiene un archivo .reg con el que puede realizar esta tarea.

[-HKEY_LOCAL_MACHINE\Software\Test]

Para eliminar un valor del Registro con un archivo .reg, ponga un guión (-) después del signo igual a continuación del *nombreDato* en el archivo .reg. Por ejemplo, para eliminar el valor del Registro **TestValue** de la clave del Registro siguiente:

HKEY_LOCAL_MACHINE\Software\Test

ponga un guión después de "TestValue=" en el archivo .reg. El ejemplo siguiente tiene un archivo .reg con el que puede realizar esta tarea.

HKEY_LOCAL_MACHINE\Software\Test

"TestValue"=-

Para crear el archivo .reg, utilice Regedit.exe para exportar la clave del Registro que desee eliminar y, a continuación, utilice el Bloc de notas para editar el archivo .reg e insertar el guión.

Cambiar el nombre de las claves y valores del Registro

Para cambiar el nombre de una clave o valor, elimine la clave o valor, y, a continuación, cree una nueva clave o valor con el nuevo nombre.

Distribuir los cambios del Registro

Puede enviar un archivo .reg a los usuarios en un mensaje de correo electrónico, poner un archivo .reg en un recurso compartido de red y dirigir a él a los usuarios para que lo ejecuten, o agregar un comando a las secuencias de comandos de inicio de sesión de los usuarios para importar automáticamente el archivo .reg cuando inicien sesión. Cuando los usuarios ejecuten el archivo .reg, reciben los mensajes siguientes:

Editor del Registro

¿Está seguro de que desea agregar la información en *ruta de archivo .reg* al Registro?
Si el usuario hace clic en **Sí**, recibe un mensaje similar al siguiente:
Editor del Registro

La información de la ruta del archivo .reg se ha escrito correctamente en el Registro.
Regedit.exe admite un modificador de la línea de comandos **/s** para no mostrar estos mensajes. Por ejemplo, para ejecutar sin mensajes el archivo .reg (con el modificador **/s**) desde un archivo de lotes de la secuencia de comandos de inicio de sesión, utilice la sintaxis siguiente:
regedit.exe /s *ruta de acceso del archivo .reg*

Nota: ***si los cambios funcionan, puede enviar el archivo de registro a los usuarios adecuados de la red.***

Utilizar Windows Script Host

Windows Script Host le permite ejecutar scripts VBScript y JScript directamente en el sistema operativo. Puede crear archivos VBScript y JScript que utilizan métodos de Windows Script Host para eliminar, leer y escribir claves y valores del Registro.

Utilizar Instrumental de administración de Windows

Instrumental de administración de Windows (WMI) es un componente del sistema operativo Microsoft Windows y es la implementación de Microsoft de Web-Based Enterprise Management (WBEM). WBEM es una iniciativa del sector para desarrollar una tecnología estándar que proporcione acceso a la información de administración en entornos empresariales. Puede utilizar WMI para automatizar las tareas administrativas

(como la modificación del Registro) en un entorno empresarial (figura 10.). Puede utilizar WMI en lenguajes de scripts que tienen un motor en Windows y tratan objetos de Microsoft ActiveX. También puede emplear la utilidad de línea de comandos WMI (Wmic.exe) para modificar el Registro de Windows.

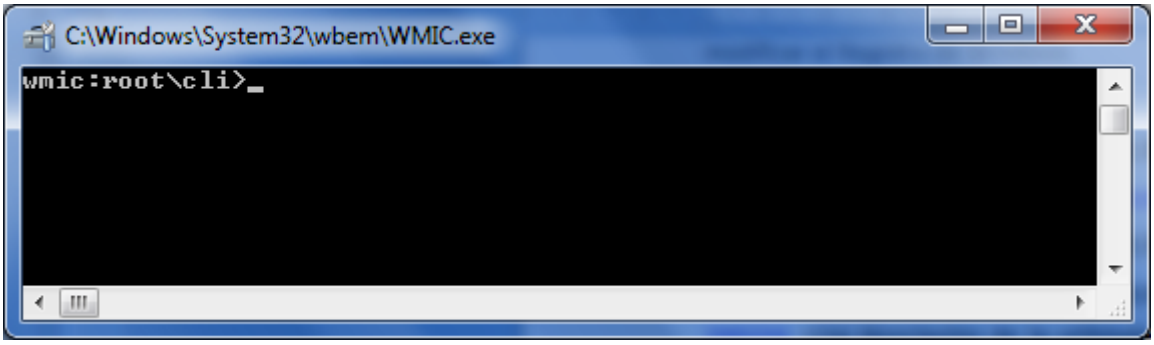
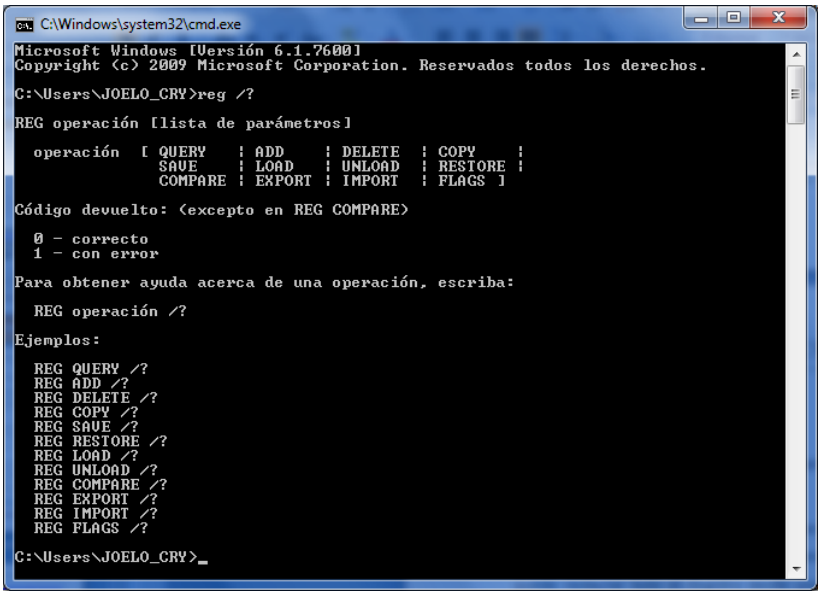


Figura 2.11: Pantalla modo consola para edición de registro.

Utilizar la Herramienta de registro de consola para Windows

Puede utilizar la herramienta de registro de consola para Windows (Reg.exe) con el fin de modificar el Registro. Para obtener ayuda sobre la herramienta Reg.exe, escriba **reg /?** en el símbolo del sistema y haga clic en **Aceptar**.



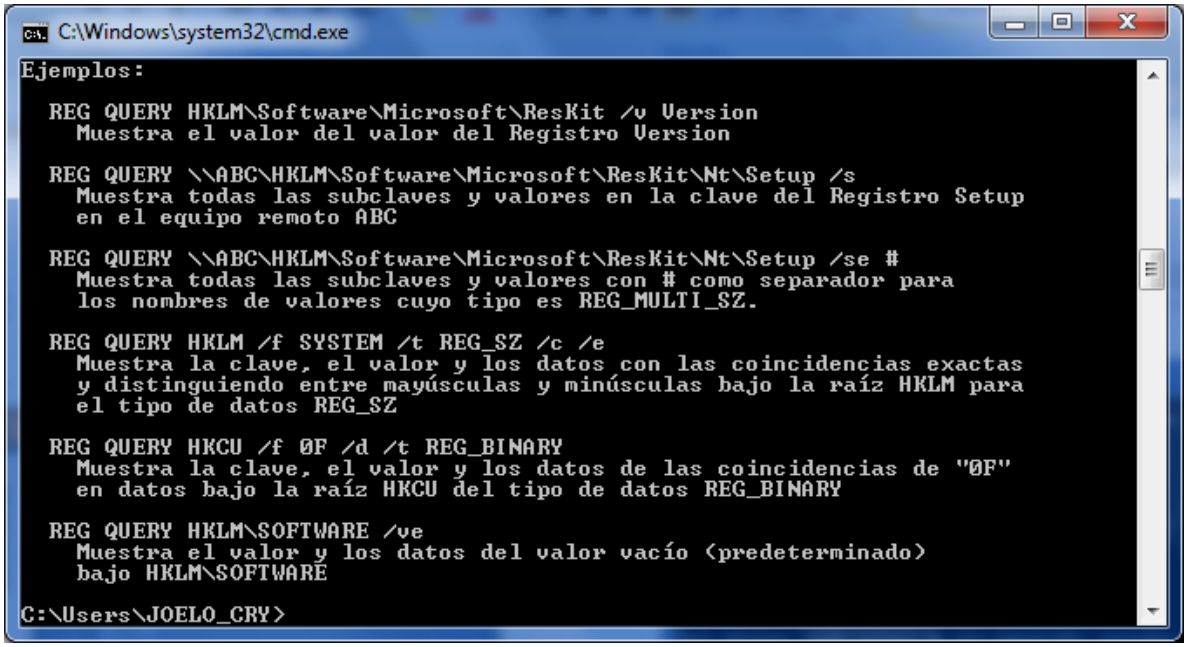


Figura 2.12: Modo consola de Windows

Restaurar el Registro

Para restaurar el Registro, utilice el método apropiado.

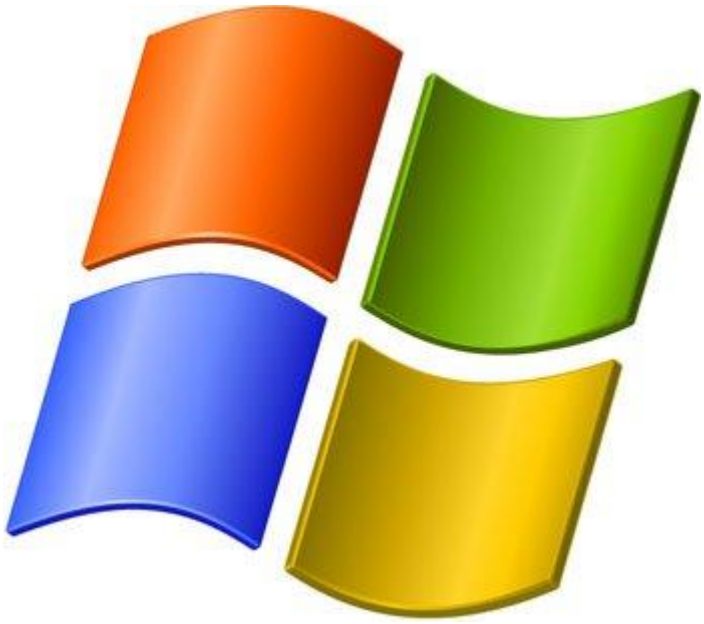
Restaurar las claves del Registro

Para restaurar las subclaves del Registro que exportó, haga doble clic en el archivo de entradas del Registro (.reg) que guardó en la sección Exportar claves del Registro. También puede restaurar todo el Registro desde una copia de seguridad.

Restaurar todo el Registro

Para restaurar todo el Registro, restaure el estado del sistema desde una copia de seguridad.

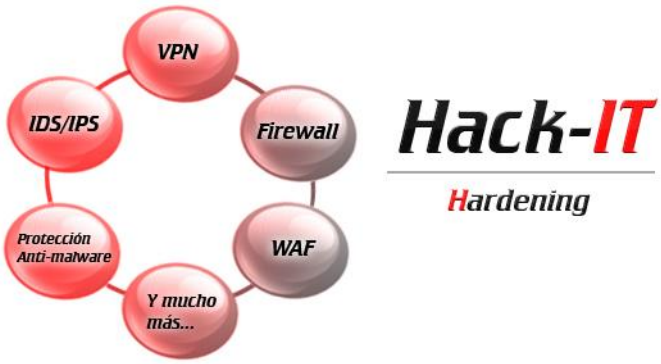
Nota: al hacer una copia de seguridad del estado del sistema también se crean copias actualizadas de los archivos del Registro en la carpeta %SystemRoot%\Repair. Si no puede iniciar Windows XP después de modificar el Registro.



CAPÍTULO III

VULNERABILIDAD

Niveles de seguridad Hardening



Una pregunta que necesita ser considerada al asegurar computadoras es "cómo debemos asegurarlas" a menudo las personas asumen que el nivel más alto de la seguridad es mejor, pero es importante recordar que las vulnerabilidades aparecen cuando se brinda mayor funcionalidad a los usuarios en el uso del computador.

El asegurar la computadora puede ser más importante y de mayor utilidad que defender la vulnerabilidad existente.

En respuesta a esto, se han determinado tres niveles diferentes para la seguridad ya sea por la versión del sistema operativo o de acuerdo al lugar donde se encuentra operando la máquina; de esta manera tenemos:

Home

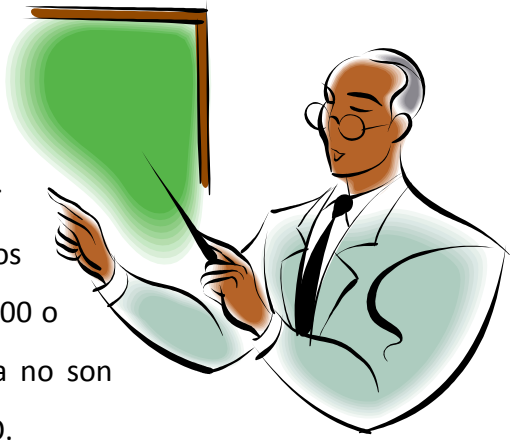
Este nivel es diseñado para los sistemas XP profesional que necesitan operar con los sistemas más viejos tal como Windows NT, o en entornos donde aplicaciones de terceros más viejas. Las colocaciones no afectarán la función o ejecución del sistema operativo o de aplicaciones que están corriendo en el sistema.

Computadora de escritorio en la empresa

En este nivel es diseñado para sistemas XP profesional de funcionamiento en un entorno manejado, donde mantiene una interoperabilidad con los sistemas de herencia. Asume que todos los sistemas operativos dentro de la empresa son Windows 2000 o posterior, por lo tanto es capaz para usar todo lo posible para la seguridad disponible dentro de esos sistemas.

En tales entornos, estas colocaciones de nivel de empresa no son probables para afectar la función o ejecución del SO, sin embargo, uno debe considerar cuidadosamente el impacto posible a las aplicaciones de software al aplicar éstos se recomiendan los controles técnicos que XP profesional proporciona.

Computador portátil en la empresa



Estas colocaciones son casi idénticas a las colocaciones autónomas de empresa, pero con transformaciones apropiadas para los usuarios móviles cuyos sistemas deben hacer funcionar ambos en y lejos de la red corporativa. En los entornos donde todos los sistemas es Windows 2000 o posterior, estas colocaciones de nivel de empresa no son probables para afectar la función o ejecución del SO.

Seguridad especializada - La funcionalidad limitada

Anteriormente conocido como " la seguridad alta" toma forma en este nivel, está diseñado para los sistemas XP profesional en que la seguridad e integridad son las prioridades más altas, aún a expensas de funcionalidad, ejecución, e interoperabilidad. Por lo tanto, cada colocación debe ser considerado cuidadosamente y sólo aplicado por un administrador experimentado que tenga una comprensión completa del impacto potencial de cada poniendo o la acción en un entorno particular.

Una vez determinado los niveles de seguridad que se debe dar una máquina dependiendo de su área, se llega a la conclusión rápida que todo depende del uso que se le dé a la misma, de tal forma, que si el usuario mantiene costumbres de seguridad para con su equipo, las medidas de seguridad prácticamente serían innecesarias, pero no siempre ocurre esto, no solo por manejo del usuario sino por el obligado uso de dispositivos ajenos a nuestro equipo.

Así se determinan configuraciones que son aplicables las veces que sean necesarias o simplemente que se ejecuten como una configuración por defecto en el equipo, las mismas que serán pre-establecidas de acuerdo con la decisión de aplicación del usuario.

Ciclos de vida de Hardening

Mediante la utilización de las fases sobre seguridad el ciclo de vida de Hardening comprende todo el proceso desde la detección de las vulnerabilidades mediante tester o de forma manual, hasta la aplicación de las diferentes medidas de seguridad.

Determinándose así que el ciclo de vida de hardening nunca termina, ya que siempre está en constante evolución y reajuste.

Es así que las fases se pueden ver de esta forma:

Evaluación

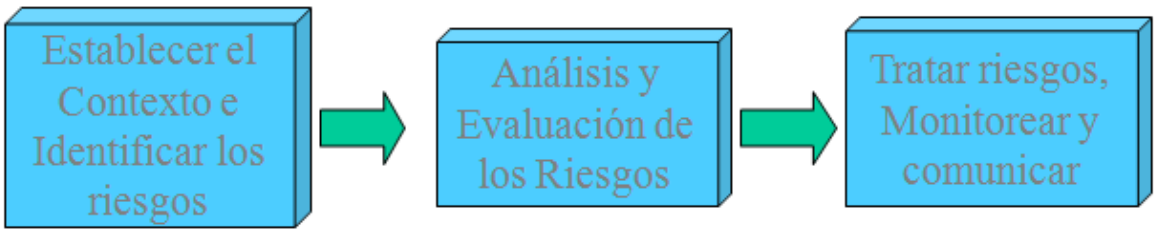


Figura 3.1. Administración de riesgos (basada en el estándar AS/NZ 4360)

Administración de Riesgos:

Método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o procesos para minimizar pérdidas.

Diseño

- Actividades a desarrollar para evitar que sucedan acciones indeseables.
- Configuraciones de Seguridad efectivas basadas en estándares de la industria y organizacionales.

Necesidad de políticas

- Empleados accesando a Internet
- Problemas con el uso de la red o el email
- Empleados utilizando información confidencial o privada
- Acceso remoto a la organización
- Dependencia de los recursos informáticos
- Políticas define que prácticas son o no son aceptadas.
- Como concientizar
    - En persona, por escrito o través de la Intranet.
    - Reuniones por departamento.
    - Publicar artículos, boletines, noticias.
    - Crear un espacio virtual para sugerencias y comentarios.
    - Enviar emails con mensajes de concientización.
    - Pegar letreros en lugares estratégicos.
    - Dar premios a empleados.
    - Exámenes On-line.
    - Crear eventos de Seguridad Informática.
- Firma digital para envío de documentos
- Logs en Firewalls.

- Se requiere Sistemas de detección de Intrusos
- Sistemas de prevención de Intrusos

Implementar

Personal especializado pone en marcha los controles basados en el diseño desarrollado Hardening.

Administración y Soporte

- Observar las actividades normales y reaccionar ante incidentes.
- Monitoreo y alertas.
- Las respuestas se basan en el documento de Políticas de Seguridad definido.
- Forma en que se trata el incidente.
- Encontrar el problema y corregirlo.
- Prácticas forenses.
- Definir la responsabilidad y el causante del problema.

Debe ser continuo con todo el Ciclo de Vida en la medida que se extienda en toda la organización.

Habilidades y experiencia se alcanzan dentro de todo el proceso.

Usos de Services Packs

Service Packs y Hotfixes

Microsoft periódicamente distribuye actualizaciones grandes a sus sistemas operativos en la forma de paquetes de servicio, tan a menudo como una vez cada mes, o menos frecuentemente. Los paquetes de servicio incluyen toda la configuración principal anterior y una nueva configuración de áreas mejoradas la cuales examinada extensamente por Microsoft antes de la liberación.

Considerando el número vasto de las aplicaciones disponibles, es totalmente posible que un insecto (virus) en un Service Pack no se pueda hallar, y pueda escabullirse por este análisis de ingeniería. Los paquetes de servicio deben usarlos en un entorno de prueba antes de ejercer presión en la producción. Si un sistema de prueba no está disponible, espere una semana o dos después de la liberación de un Service Pack, y preste atención al Microsoft Website para los informes de insectos (virus) potenciales.

Es importante tener conciencia del Service Pack y Hotfixes, estos no son pertinentes a los sistemas operativos. Las aplicaciones individuales tienen su propio Service Pack y necesidades de Hotfixes.

Un sistema Windows que es completamente actual en Windows Hotfixes y Service Packs también se necesita mantener actualizado con el Service Pack y Hotfixes para Internet Explorer y Microsoft Office. La seguridad total del sistema requiere atención a ambos sistema operativo y niveles de aplicación.

Análisis de Configuraciones básicas por defecto

Entre las actividades propias de un proceso de Hardening se pueden contar las siguientes:

- **Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina**. Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de

dispositivos ópticos, USB o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.

- **Instalación segura del sistema operativo**. Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (una para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema.

- **Activación y/o configuración adecuada de servicios de actualizaciones automáticas**, para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una corporación, es adecuado instalar un servidor de actualizaciones, que deberá probar en un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción.

- **Instalación, configuración y mantenimiento de programas de seguridad** tales como antivirus, antispyware, y un filtro antispam según las necesidades del sistema.

    - **Configuración de la política local del sistema**, considerando varios puntos relevantes:

- **Política de contraseñas robusta**, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas.

- **Renombramiento y posterior deshabilitación de cuentas estándar del sistema**, como administrador e invitado.

- **Asignación correcta de derechos de usuario**, para reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.

    - **Configuración de opciones de seguridad generales**, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.

    - **Restricciones de software**, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.

    - **Activación de auditorías de sistema**, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.

    - **Configuración de servicios de sistema**. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si el equipo no posee tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.

    - **Configuración de los protocolos de Red**. En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los

mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo.

- **Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema**. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.

- **Configuración de opciones de seguridad de los distintos programas**, como clientes de correo electrónico, navegadores de Internet y en general de cualquier tipo de programa que tenga interacción con la red.

- **Configuración de acceso remoto**. En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.

- **Configuración adecuada de cuentas de usuario**, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la impersonificación de usuarios para realizar labores administrativas en vez de iniciar sesión como administradores.

- **Cifrado de archivos o unidades según las necesidades del sistema**, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.

- **Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema**. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

Requisitos básicos de los sistemas en el campo de la seguridad

Windows introdujo varios realces de seguridad significativos. La mayor parte de los realces significativos de seguridad se detallan en estas diez categorías generales, las cuales permiten identificar los sectores por donde pueden ocurrir infiltraciones, Mediante la alerta del usuario o el bloqueo de las mismas.

Bluetooth

Windows ahora proporciona desde el exterior el apoyo para las conexiones de Bluetooth. Bluetooth se usa más comúnmente para abreviar las comunicaciones de distancia, y sirve como un reemplazo para las conexiones infrarrojas.

Aunque Bluetooth opera en el mismo rango de frecuencia como 802.11 redes inalámbricas, sirve para un propósito muy diferente. Una vez que Bluetooth es configurado para el uso en un puesto de trabajo, se pueden acceder a las opciones de configuración por el tablero de control.

Ciertos ejemplos de las conexiones de Bluetooth incluyen lo siguiente:

- La red en línea para unir su PC a un teléfono móvil con Bluetooth habilitado
- Imprimir a una impresora de Bluetooth habilitado
- Uso de enlace que trasmite por radio los dispositivos tales como ratón o teclado.
- La red personal que crea una conexión de IP entre dos dispositivos Bluetooth habilitados.

Bluetooth obviamente presenta ciertos intereses de seguridad. Sin embargo, en este momento, no existen ningún tipo de opciones de configuración nativas para manejar estas conexiones.

Permisos de DCOM

Las máquinas Windows generalmente alojan a varios DCOM Services. Estos servicios se pueden acceder localmente por el propio puesto de trabajo, o remotamente de otra máquina. Aunque las llamadas locales y remotas son manipuladas de forma diferente, pero ambos terminan pasando por el mismo motor de COM.

Service Pack 2 añade configuraciones de políticas de grupo que controlan permisos para manejar componentes de DCOM. Los permisos son separados en dos categorías distintas: los usuarios que pueden acceder a servicios de DCOM existentes, y usuarios que pueden lanzar o activar servicios. Los derechos son típicamente asignados en dependencia de, sí la solicitud de DCOM vino de la misma máquina (local), o de otra máquina (remoto).

Permisos de RPC

Los servicios de RPC se comportan similares a DCOM Services. Permiten una computadora remota para acceder a un servicio en el puesto de trabajo. Cada servicio por separado requiere un puerto de TCP para ser abierto en el puesto de trabajo. Antes que asignar los puertos específicos a cada servicio, el sistema operativo proporciona un genérico "|portmapper|"el |portmapper| sirve de un libro de dirección, les permite a clientes determinar que el puerto es asignado a un servicio de DCOM específico.

Con Service Pack 2, Microsoft por defecto requiere de todos los clientes para autenticar antes de ser permitido conectar un servicio en el puesto de trabajo. Además, los clientes deben autentificarse antes de ser permitidos para inquirir el |portmapper| para localizar un servicio de DCOM específico.

Permisos de WebDAV

Web (HTTP) basado en gestión de ficheros está llegando a ser cada vez más popular. Usando los estándares protocoliza HTTP, los clientes pueden acceder, modificar y borrar archivos en un servidor remoto. A medida que el protocolo se desarrolló, Microsoft ha empotrado la tecnología más profundamente en el sistema operativo. Dentro de Windows, es capaz de acceder archivos usando WebDAV por el mismo enlace que se acostumbra a acceder a la red se comparte con NetBIOS o SMB.

El protocolo de HTTP usa los métodos de autenticación diferentes de los protocolos de red de Windows tradicionales. Muchos sistemas soportan ciertos modelos de autenticación robustos por HTTP, tales como Kerberos o NTLM. Sin embargo, los clientes y servidores pueden negociar también la autenticación de HTTP "básica", que pasa esencialmente

credenciales a través de la red en el texto claro.

Service Pack 2 introdujeron dos nuevas configuraciones para proteger credenciales enviadas sobre las sesiones de HTTP.

Windows Firewall

El más significativo mejoramiento de seguridad con Windows XP Service Pack 2 es el cortafuego de Windows. Por defecto, el servicio de cortafuego es habilitado, y controlando el tráfico por llegar en todos los enlaces. El servicio proporciona muchas colocaciones muy específicas para el manejo de publicación de puertos de red. Además, el servicio trabaja en combinación con el enlace de RPC para controlar efectivamente el acceso remoto específico a RPC Services, que pueden asignarse con dinamismo a los puertos de llegada.

Wireless proveedor de servicios

La industria de WiFi ha trabajado rápidamente para recobrarse de las vulnerabilidades de seguridad significativas identificadas en la ejecución inicial de 802.11 redes inalámbricas.

Service Pack 2 proporciona acceso a las opciones de seguridad mejoradas por una nueva característica llamada " Wireless proveedor de servicios."

Wireless proveedor de servicios proporciona los controles adicionales para los tres guiones específicos: el proveedor de Hotspot público, un proveedor de servicios de Internet inalámbrico genérico, y la red corporativa. Por usar un Wizard de registro de red inalámbrico y Wizard de disposición, el

cliente puede conectar sin peligro un proveedor de servicios en un canal codificado sin tener que cambiar las contraseñas pesadas.

En este punto, ninguna de las opciones de configuración nativas existe para controlar estas nuevas configuraciones inalámbricas. Por lo tanto, es cuestión del usuario hacer uso de este medio y controlar su seguridad.

Protección de ejecución de datos

La más significativa clase de vulnerabilidades queda en el Buffer Overflow. Con una incorrecta explotación del mismo, un ataque puede cerrar fácilmente los servicios específicos, a veces controlan enteramente sobre una computadora todos los servicios. El problema radical parece extremadamente simple: el ataque ha borrado demasiados datos en la memoria. Los datos extras rebosan en un área de la memoria designada para algo diferente - tal como código ejecutable - y compromete la máquina.

Windows proporciona la protección adicional contra los excesos de OverFlows en dos vías. En primer lugar, el sistema operativo puede trabajar con el hardware para identificar las partes específicas de la memoria como "no ejecutable" - regiones de NX. Sin embargo, esto requiere que el hardware que soporta tal protección. Alternativa, el sistema operativo puede ejecutar un cifrado similar de protección. *No es necesario para mejorar al nuevo hardware beneficiarse de la protección* de ejecución de datos de Windows.

El centro de seguridad

El centro de seguridad continuamente controla los tres pilares de la seguridad en el puesto de trabajo: software contra virus, el cortafuego y los servicios de actualizaciones

de seguridad. Cuando un asunto se levanta con cualquiera de estos tres artículos, el centro de seguridad notifica el usuario. Los artículos individuales pueden ser incapacitados por las llaves de registro.

DTC Control

Las transacciones se pueden coordinarse a través de los procesos múltiples que usa el coordinador (DTC) distribuido de transacción. Todo el proceso es local a una máquina sencilla, o se pudieron extenderse a través de varios dispositivos -- sistemas de archivos, colas y bases de datos de mensaje, por ejemplo.

Puestos de trabajo raramente necesitan estar envueltos en transacciones distribuidas con base en red. A fin de reducir la superficie de ataque del puesto de trabajo, este servicio ha sido inhabilitado por defecto.

La conexión en el viaje de ida de datos con alto tráfico

Service Pack 2 limita el número de intentos de conexión de TCP en el viaje de ida incompleto. Si una aplicación (tal como un scanner portuario) genera un gran número de solicitudes en viaje de ida de conexión, las solicitudes son comprimidas, y son catalogadas como eventos de actividades no normales.

Configuraciones que causan problemáticas

En el transcurso de desarrollar cualquier tipo de norma de seguridad, existe un constante perpetuo: Algo se romperá. Cuando cambia algo en favor de aumentar la seguridad, se "ruptura" un programa vulnerable o explotable potencialmente.

Un defecto lateral desafortunado de inhabilitar los servicios indeseados es la probabilidad que ciertos programas o funciones peligrosas se han usado también para el bien en lugar del mal. La parte desafortunada es esa cuando se inhabilita el código y es arriesgada una operación perfectamente viable porque se inhabilita también otra.

En un esfuerzo para revelar las fuentes probables de problemas, aquí se listan algunas de las configuraciones que son conocidas por causar los problemas, y que tipos de problemas pueden levantarse. Esto es para ayudar a diagnosticar problemas al asegurar sistemas. Ello está sujeto a cambiar como la información se vuelve disponible.

Restricciones adicionales para las conexiones anónimas

"Ningún acceso sin los permisos anónimos explícitos". Muchas aplicaciones más viejas (y ciertas nuevas) usan en realidad las sesiones nulas para comunicarse entre computadoras, o entre procesos en la misma computadora. Si una aplicación no logra trabajar una vez en una computadora la solución es "cerrarla" esto debe ser la primera configuración para "escapar" en vez de tratar de localizar

.

Nivel de LAN Manager Autenticación

“Envié respuesta sólo de NTLMv2".

Esta configuración hará una computadora de Windows XP incapaz para compartir recursos con otras computadoras que son no puestas para usar NTLMv2. Hará la computadora incapaz para compartir recursos con las computadoras de Windows 95/98/Me a menos que instalan la aplicación DSCLIENT.EXE del CD de instalación de Windows 2000.

Restrinja acceso de disco compacto para entrar en el sistema localmente

Un problema ha sido identificado cuando esta configuración se habilita. Cuando los usuarios están instalando software de una unidad de disco compacto, y esos paquetes de instalación usan el instalador de Microsoft (.MSI), el software se instala en realidad por el servicio de instalador de Windows, NO el usuario local. Si esta configuración se habilita, tal instalación de software no será capaz de proceder, debido a esta restricción. La configuración se debe cambiar antes para instalar el software, o el paquete se debe copiaren un directorio local o guía de red para el procedimiento de instalación para tener éxito.

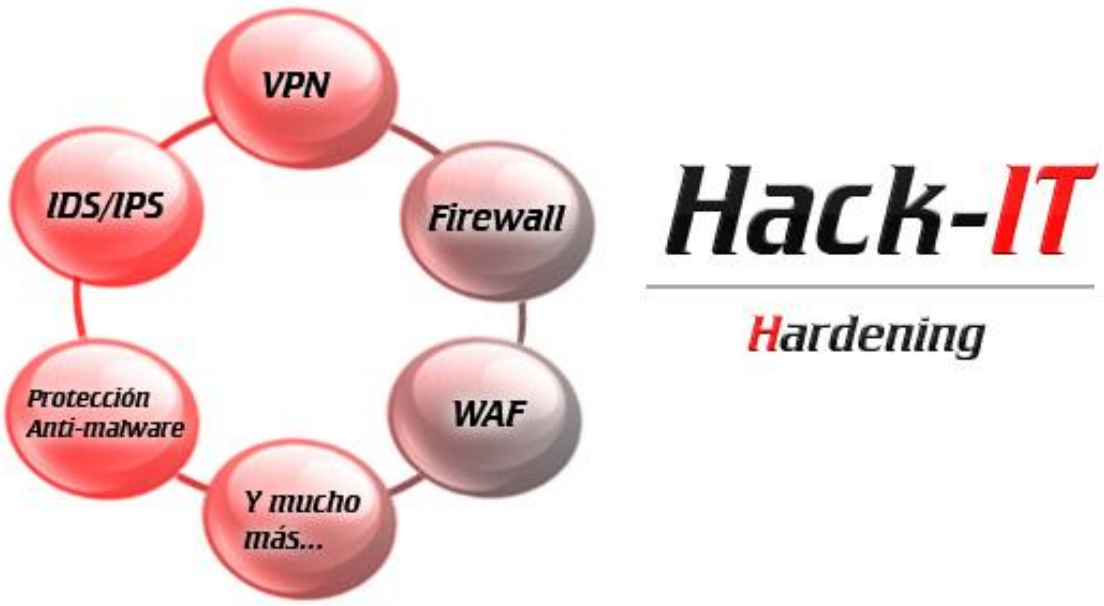
Quite las porciones administrativas en el puesto de trabajo (profesional)

HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\LANMANSERVER\PARAMETERS\AUTO SHAREWKS (EL REG_DWORD) 0.

Quitando las partes administrativas en las computadoras de Windows son totalmente deseables si no están siendo usadas. Esta es probablemente la rotura de ciertas aplicaciones que usan las partes administrativas, la mayor notabilidad de que es suplementario y restauran utilidades.

Los permisos de archivo y de registro

Ello debe ir sin decir que si un usuario o aplicación están intentando acceder un objeto, y recibiendo un " acceso negado " es un error, que cierta atención debe estar sujeta a los permisos que aplicaron a ese objeto.



CAPÍTULO IV

APLICACIÓN HARDENING

Service Packs y actualizaciones de seguridad

Entre **las** liberaciones de los paquetes de servicio, Microsoft distribuye actualizaciones intermedias a sus sistemas operativos en la forma de Hotfixes. Estas actualizaciones son normalmente pequeñas y dirigen un problema sencillo.

Hotfixes se pueden poner en circulación dentro de horas del descubrimiento de cada detalle molestia o vulnerabilidad, porque dirigen un problema sencillo. Después que se sueltan así rápidamente, no pasan la comprobación rigurosa. Deben ser usados con cautela al principio, aún más así que los paquetes de servicio. Cada Hotfix incluye una descripción del asunto que ello se resuelve, si ello es la seguridad, o fija una forma diferente en cierta medida el problema. Éstos deben ser pesados para determinar si el riesgo de instalar el Hotfix vale más que el riesgo de no instalarlo.

Periódicamente, Microsoft soltará un "roll up" de Hotfix que es a ras de tierra entre un Hotfix y un Service Pack. El cuál es o será el más indicado y único a ser instalado hasta que se lance uno nuevo.

Necesidades MAYORES de Service Pack y Hotfix

Valoración del Service Pack instalado

Aunque los Service Packs son generalmente confiables y examinen cuidadosamente la comprobación extensiva, es posible que no sea compatible con cada producto de software en el mercado. Si es posible, pruebe el Service pack en un entorno de prueba, o al menos espere hasta que haya sido lanzado durante un tiempo antes de instalarlo.

Necesidades MENORES de Service Pack y Hotfix

Toda la parte crítica e importante de Hotfixes ha sido instalada hasta la fecha.

Aunque Hotfixes son generalmente confiables y se examinan cuidadosamente, es significativamente posible que un hotfix que dirige un problema sencillo no sea compatible con cada producto de software en el mercado, y pueda causar otros problemas. Si es posible, pruebe Hotfixes en el entorno de prueba, o al menos espere hasta que hayan sido lanzados durante algún un tiempo antes de la instalación.

Auditoría y políticas de cuentas

Una política de contraseña fuerte puede significar una excelente solución al ataque.

- Insista sobre el cambio frecuente de la contraseña.
- Requiera que las contraseñas sean largas compuestas de las combinaciones casuales de superior valor, letras, números, y caracteres especiales en minúsculas.
- No permita las contraseñas en blanco.
- Verificaciones de que las contraseñas aseguradas no sean repetidas.
- Impida el uso de parte del nombre del usuario o ID de usuario para login o Password.
- No permita el uso de las palabras de diccionario comunes.
- Puede proporcionar los controles técnicos que requiere la mayor parte de esta funcionalidad por configurar la política de contraseña del grupo de campo implícito figura 11.

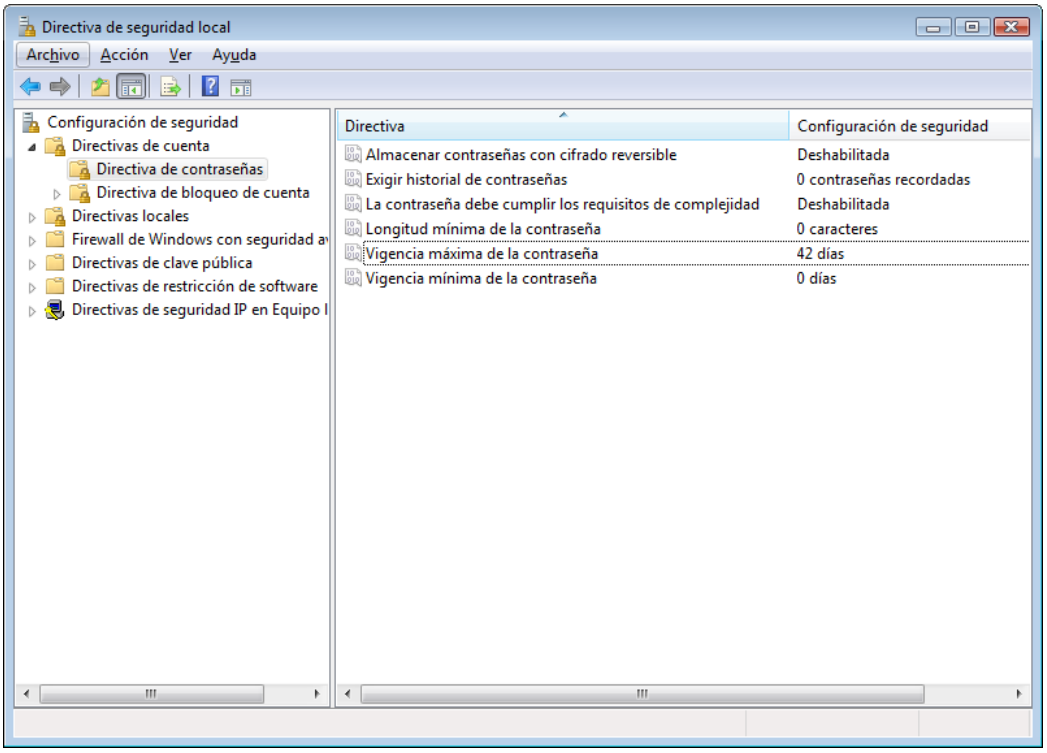


Figura 4.1: Configuración de la política de contraseña en la política implícita de campo.

Otras opciones son los controles temporales que pueden hacer mucho para impedir el uso de cuenta desautorizado. Estas opciones incluyen

- *El usuario debe cambiar la contraseña en la próxima entrada en el sistema.*
- *La cuenta es inhabilitada*
- *La cuenta es sensitiva y no se puede delegar*

Principales características de Auditoría, de políticas de cuenta y Requisitos

Longitud de contraseña

Por lo general, las necesidades de longitud de contraseña y de complejidad de contraseña están acostumbradas a proteger contra los ataques de adivinanza de contraseña. Estos ataques son relativamente no sofisticados: la ruptura es simplemente para hacer las suposiciones repetidas, para ver si la contraseña correcta ha sido escogida. El ataque es

normalmente ejecutado en cierto sentido, para circunvenir las políticas de cierre forzoso de cuenta. Los intentos son típicamente sistemáticos y pueden ser divididos en dos categorías:

- Los ataques de diccionario empiezan con una lista de las palabras comunes que pueden estar acostumbrados a formar contraseñas. Las palabras pueden ser combinadas, por una variedad de los algoritmos de "|morphing|" para mejorar eficacia.
- Los ataques de fuerza bruta repasan a la ligera todas las combinaciones posibles de carácter. El primero " AAAA1 " es probado, entonces " AAAA2 ", entonces " AAAA3 “, y así en una vez todas las cinco contraseñas de caracteres que han sido probadas, la búsqueda empieza de nuevo con seis contraseñas de carácter.

La longitud de contraseña significativamente aumenta resistencia a los ataques de fuerza bruta, un carácter extra sencillo hace la diferencia grande más aún si las contraseñas son el caso insensible y alfanumérico.

Además de la contraseña, ciertos protocolos de Microsoft de herencia padecen de una limitación que haga que una contraseña de ocho caracteres sea particularmente importante. Estos protocolos efectivamente derrumban contraseñas en siete "trozos" de carácter. Esta crea dos vulnerabilidades significativas:

· En primer lugar, contraseñas con siete o menos caracteres se identifican rápidamente.

· En segundo lugar, una contraseña de catorce caracteres o menos es en realidad sólo dos veces tan seguro como una contraseña de siete caracteres.

A fin de proteger contra la vulnerabilidad primera, el consenso general requiere contraseñas para ser ocho caracteres o más.

Protección contra la vulnerabilidad segunda, sin embargo, sólo puede ser suministrada por el uso de los protocolos de autenticación más fuertes.

Edad de una contraseña

Todas las contraseñas se deben cambiar regularmente para asegurar el conocerse sólo por los individuos autorizados para usar la cuenta.

Además de limitar las cuentas de usuario a un usuario sencillo, esto controla también el uso de las cuentas de "papel". Las cuentas de papel típicamente pueden ser divididos entre usuarios para mantenimiento y localizador de problemas, o ellos pueden requerirlo por varios servicios y aplicaciones de sistema, y los privilegios asignados basados en su propósito específico. Con el transcurso del tiempo, las contraseñas de cuenta de papel se vuelven muy conocidas y una buena ruta para acceder recursos.

El administrador local y varias cuentas de servicio son a menudo descuidados, y pueden tener las contraseñas añejas que son bien conocidas por todo el personal.
El requerimiento para cambiar las contraseñas también proporciona una defensa práctica contra los ataques de contraseña de fuerza bruta. Dado la naturaleza del ataque de fuerza bruta, siempre tendrá éxito si existe bastante tiempo para suponer finalmente la contraseña.
En una computadora típica, ello puede tomar semanas o meses para suponer una contraseña alfanumérica larga. Sin embargo, si la contraseña expira y ha sido cambiado desde entonces durante este período, el ataque fracasará.

Menores características de Auditoría, de políticas de cuenta y Requisitos

Políticas de auditoría (mínimos)

Las políticas de auditoría definen los eventos significativos que una computadora debería tener. Las entradas o eventos principales ejecutan dos papeles importantes: proporcionan unos medios para la supervisión casi de tiempo real del sistema, y permiten la investigación de acciones que ocurrieron en el pasado.

Cuando se considera la protección del sistema, la autoría de eventos a menudo identificarán los intentos desautorizados para acceder recursos. Los eventos se pueden generar de las sesiones de usuario interactivas, o de los procesos y servicios de sistema automatizados. La caída de tal evento de seguridad se habilita fácilmente; del menú INICIO de Windows, escoja Panel de control, "herramientas administrativas", escoja "la norma de actuación sobre seguridad local". En las ventanas de consola que aparezca, navegue abajo el árbol a las colocaciones de seguridad | Políticas locales | Política de examen de cuentas. A los cambios hechos, se hace dos veces clic sobre uno de los artículos, escoja las colocaciones apropiadas en la caja de diálogos que aparecen, y escoja "OK". Las Colocaciones tomarán el efecto cuando la ventana seguridad local sea cerrada.

Auditoria en eventos de entrada en las cuentas

Revise los eventos de entrada en el sistema, siguen la pista de todos los intentos para acceder al puesto de trabajo. Éstos pueden venir de una entrada en el sistema interactiva local, una entrada en el sistema de red, un proceso por partida, o aún un servicio. La entrada en el sistema de cuenta suspendida puede mostrar una tendencia para los ataques de contraseña; los eventos de entrada en el sistema exitosos son importantes para identificar que el usuario quiera entrar al puesto de trabajo a un tiempo dado, los

eventos de "entrada en el sistema de cuenta" son generados del uso de las cuentas de campo; esto difiere de los "eventos de entrada en el sistema".

Auditoria de Administrador de cuentas

A fin de seguir la pista de los intentos suspendidos y exitosos para crear nuevos usuarios o grupos, nombran de nuevo usuarios o grupos, habilitan o inhabilitan usuarios, o el cambio las contraseñas de las cuenta, habilite auditoría para los eventos de manejo de cuenta. Los eventos de manejo de cuenta exitosos se generan también cuando una cuenta es cerrar la puerta a, así estos eventos se vuelven importantes al determinar la causa de un cierre forzoso de cuenta.

Control de acceso al directorio de servicios

Ninguna auditoría de acceso de servicio directivo es requerida en Windows XP Profesional porque el directorio atiende al acceso que pueda revisarse sólo en Windows 2000 (o posterior) controladores de campo.

Eventos de entrada en el sistema de cuentas

Similar a eventos de entrada en el sistema identifique que las cuentas están accediendo los recursos en el puesto de trabajo. Estos eventos son generados sólo cuando las credenciales de máquina locales son usadas. Aún si un puesto de trabajo es el miembro de campo, es todavía posible entrar al puesto de trabajo usando una cuenta local.

Control de acceso de objetos

Es posible seguir la pista de cuando los usuarios específicos acceden a los archivos específicos. Esta opción sólo produce eventos cuando unos o más objetos están siendo activamente controlados.

A fin de seguir la pista de acceso de usuario a los archivos o directorios específicos, navegue al archivo o carpeta, edite las propiedades de seguridad para ese objeto, y habilite la auditoría del objeto.

Control de políticas de cambio

Cuando el " revise el cambio político " opción está establecido, cambia a derechos de usuario, revise políticas, o políticas de confianza producirán eventos en el registro de evento de seguridad.

Control de uso de privilegios

El uso de privilegio de auditoría habilita la auditoría para cualquiera operación que requiere una cuenta de usuario, para hacer uso de los privilegios extras que se ha asignado ya. Si esto se habilita, eventos se generarán en el registro de evento de seguridad si unos intentos de usuario o proceso para desviar comprobación transversal, programas de depuración, cree un objeto simbólico, reemplace un proceso nivela simbólico.

El uso de privilegio es usado por todas las cuentas de usuario en una base regular. Si los eventos de éxito y faltas son revisados, habrá gran número eventos en la reflexión del tronco de eventos de tal uso.

Control de rastreo de proceso

Cuando se habilita esta opción, un evento es generado cada vez que una aplicación o unos principios de usuario, hacen alto, o de otra manera cambie un proceso. Esto crea un registro de evento muy grande muy rápidamente, y la información no es normal ni excepcionalmente útil, a menos que está siguiendo la pista de un comportamiento muy

específico. Como tal, es recomendable sólo cuando sea absolutamente necesario.

Control de eventos del sistema

Los eventos de sistema de auditoría son muy importantes. Los eventos de sistema incluyen empezar o cerrar la computadora, el evento completo se dedica a la explotación que tiene impacto a través del sistema entero. Auditoría del éxito y eventos de faltas que se deben habilitar.

Políticas de cuenta

Al aplicar estos valores, es importante considerar exactamente donde estos valores deben ser aplicados para afectar los diferentes tipos de cuenta:

· Si el puesto de trabajo no es un miembro de un campo, estas políticas pueden ser aplicadas localmente y serán firmemente aplicadas a todas las cuentas locales.

· Si el puesto de trabajo pertenece a un campo, cualquier forma que se aplique aquí no impactará las cuentas de campo. En realidad, la política de **cuenta para las cuentas de campo puede sólo ir especificado en la política** implícita de campo. La cuenta usada por el puesto de trabajo para entrar al campo es una cuenta de campo.

· Si el puesto de trabajo pertenece a un campo, y está situado en una unidad de organización (UO) específica, elabore la política de cuenta que pueda ser situado en esa UO. La política de UO se aplica a todas las cuentas locales en el puesto de trabajo, y haga caso de la norma de actuación sobre seguridad local.

Edad de contraseña (mínima)

La política de contraseña recomendada requiere usuarios para cambiar contraseñas regularmente, y requiera que la contraseña para ser diferente de esos sea con otro contexto a los anteriores. Cuando la edad mínima de contraseña está puesta en 0, un

usuario puede cambiar las contraseñas repetidamente. Entonces con referencia al uso de la contraseña vieja, editar la nueva, esta actividad es impedida por limitar los cambios de contraseña para una vez por día.

Edad de contraseña (máxima)

Las necesidades de edad de contraseña máximas y mínimas se imponen por el proceso de entrada en el sistema. Si una cuenta nunca cierra el sistema por completo, continuará ganando acceso a los recursos hasta los reboots de sistema.

Complejidades de contraseña

La sección 2.1.2 introducida al ataque de contraseña de fuerza bruta. Las contraseñas complejas adelantan y mitigan el riesgo de un ataque de contraseña de fuerza bruta significativamente aumentando el conjunto de todo posible las contraseñas. Esto se hace por requerir contraseñas para incluir una combinación de las letras superiores y en minúsculas, números y símbolos (caracteres especiales) en la contraseña.
Windows XP no proporciona cada granularidad en las necesidades de complejidad de contraseña -- ello es o apagado o encendido. Cuando se exigen las contraseñas complejas, cada contraseña debe contener caracteres de tres de los cuatro conjuntos siguientes de caracteres:

- Letras en mayúsculas
- Letras en minúsculas
- Números
- Los caracteres especiales (símbolos no alfanuméricos)

Habilitar esta colocación proporciona la resistencia pendiente a los ataques de contraseña de fuerza bruta, y se debe poner siempre que sea posible, pero ocasionalmente puede ser

difícil al instrumento. La educación de usuario de fin es una necesidad, como la advertencia envía mensajes para las contraseñas débiles es misterioso y probable para ser de la ayuda pequeña a la mayor parte de los usuarios.

Si no pueda requerir las contraseñas complejas, considere alargar la longitud mínima de contraseña. A menudo un |passphrase| alfabético largo puede ser más resistente a un ataque de fuerza bruta que un |passphrase| complejo corto.

Historial de contraseña

Las contraseñas se deben cambiar en una base regular. Por esa misma regla, los usuarios no deben ser permitidos para usar pocas contraseñas una y otra vez. La colocación de historial de contraseña de Enforce determina cuántas contraseñas previas son guardadas para asegurar que los usuarios no pasan por un ciclo por las contraseñas regulares.

Al determinar su configuración de cuenta completa, considere el efecto combinado de la historia de contraseña y los colocaciones de edad de contraseña máximos, e impiden que los modelos repetitivos. Por ejemplo, si su edad de contraseña es 30 días e historia de contraseña tiene 12 al menos, muchos usuarios pueden adivinar probabilidades de contraseñas establecidas a una variación del mes actual (Enero1, Febrero1 , etc.).

Almacene contraseñas usando la codificación reversible

El modelo de autenticación de Windows permite el almacenamiento de un picadillo de contraseña antes que la contraseña real; un picadillo de contraseña no puede ser descifrado para recobrar la contraseña original. Más bien, para autenticar, la contraseña se debe picar exactamente la misma vía y compare con el picadillo guardado original. Si los valores hacen juego, la contraseña correcta estuvo presente, y el acceso es otorgado.

A fin de soportar ciertas aplicaciones y su autenticación, Microsoft permite la habilidad para almacenar contraseñas usando la codificación reversible. Si a todo posible, esto se debe evitar. Esta opción es incapacitada en defecto, y deba permanecer así. Cada

aplicación que requiere la codificación reversible para contraseñas está poniendo adrede sistemas al riesgo.

Política de cierre forzoso de cuenta

Muchas de las colocaciones sobre proteger contra fuerza bruta y contraseña de diccionario van al ataque. Típicamente estos ataques recogen la información (tales como picadillos de contraseña) y ejecute el |offline| de ataque. Sin embargo, cierta contraseña que supone los ataques todavía ocurre interactiva.

A fin de proteger contra ataques en línea de contraseña, imponga una política de cierre forzoso de cuenta. Tres colocaciones comprenden la política de cierre forzoso de cuenta: duración, umbral y restablezca.

Duración de cierre forzoso de cuenta

Una vez que los criterios para un cierre forzoso son acercados, la cuenta llega a ser cerrada. Sin embargo, la cuenta con referencia a-habilitado de forma automática una vez después de la duración especificada en el " duración de cierre forzoso de cuenta." especifique 0 minutos para tener el cierre forzoso de cuenta hasta que un administrador manualmente restablezca la cuenta.

Umbral de cierre forzoso de cuenta

El usuario tiene varios intentos para entrar en su cuenta, antes del cierre forzoso, este número de intentos es determinado por el Umbral de cierre.

Restablezca el cierre forzoso de cuenta después

Siguiendo una mala entrada en el sistema, el sistema incrementa la cuenta de los intentos

inválidos para esta cuenta. Este contador continúa para incrementar hasta el umbral de cierre forzoso, o el contador es restablecido. El " restablezca el cierre forzoso de cuenta después de " define con qué frecuencia el contador es restablecido.

Configuración de registro de Evento, Aplicación, seguridad y diarios del sistema

Todos los eventos de sistema son reunidos en los diarios de evento. Todos los sistemas Windows XP contienen tres conjuntos de diarios: Aplicación, sistema y seguridad. La aplicación registra entradas típicamente que venga del software instalado; por ejemplo, el software contra virus cortará un evento cuando el virus examina completo, o cuando ello detecta un virus. El registro de sistema reúne los eventos generados por el sistema operativo, tales como reboots de sistema. El registro de seguridad se reúne la seguridad, revisa información como se define por la política de grupo. Todos los tres diarios pueden contener la información útil sobre un incidente de seguridad.

El tamaño implícito de cada registro de evento es 512k. Esto ha sido estándar desde los días de Windows NT 3.5 , cuando los discos duros estaban debajo 2 Gigabytes (GB) en tamaño. Sin embargo, los mejoramientos de capacidad de hardware recientes deberían dejar el espacio de almacenamiento amplio para un registro de evento de 80Mb.
Dos valores adicionales del sistema de control cuando el registro de evento es completo. Esencialmente allí están dos posibilidades:

- Continúe los eventos de entrada como ellos vienen pero arriesgan sobre grabar los eventos importantes.
- Pare los eventos de entrada
- **Sobregrabe eventos como necesite** continúe la entrada de todo evento, sobregrabando el evento más viejo siempre con el requisito.
- **Sobregrabe por el día** permite sobregrabar ciertos eventos, pero no todo. Los eventos

más antiguos que un número específico de días puede ser limpiar. Una vez que todos los eventos más viejos son sobre grabados, ningún nuevo evento es ingresado.

- **No Sobregrabe (aclárese los diarios manualmente)** impida sobregrabar los eventos, y nuevos eventos son perdidos cuando los rellenos de tronco de evento. El registro de evento se debe aclarar manualmente por el administrador de sistema o una aplicación de manejo de tronco automatizada.

Configuración de seguridad

Las colocaciones de seguridad esbozan muchas opciones muy específicas que pueda mejorar una protección del sistema protegiendo contra una amenaza específica.

Para editar los valores de seguridad, figura 10. Escoja INICIO | Panel de Control. Clic dos veces sobre "las herramientas administrativas, " y escoja "Políticas seguridad local". En la ventana que aparezca, expanda las políticas locales, y clic sobre opciones de seguridad. A los cambios hechos, clic dos veces sobre una de las colocaciones en el panel derecho, haga los cambios apropiados, y haga clic sobre OK para salvar las colocaciones.

Si el puesto de trabajo no es un miembro de un dominio, el cambio se volverá efectivo inmediatamente, aunque ello no sacará a luz en el editor local de políticas de seguridad hasta que se cierra. Si el puesto de trabajo pertenece a un dominio, los cambios locales sólo se volverán la política de dominio efectiva, no hace de las colocaciones.

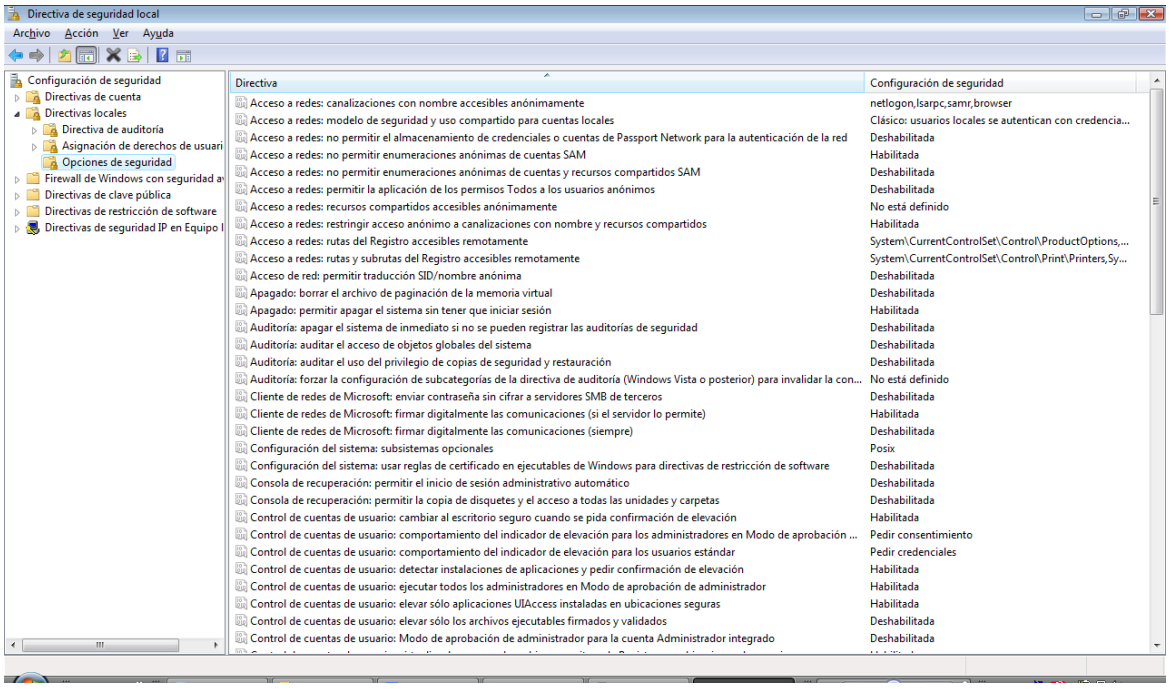


Figura 4.2: Directiva de seguridad local – configuraciones de seguridad

Mayores Configuraciones de seguridad

Los sistemas operativos de Microsoft típicamente soportan una entrada en el sistema de la herencia anónima conocida como una "sesión nula". La sesión nula es en realidad una sesión de entrada en el sistema donde ambos id de usuario y la contraseña son en blanco.

Aunque el sistema operativo pone muchas restricciones en una sesión nula, y ello nunca puede ser usado para una entrada en el sistema interactiva, ello todavía puede ser posible recoger la información significativa por esta cuenta especial anónima.

Las sesiones nulas normalmente pueden estar sin peligro incapacitando desde una característica de herencia. Sin embargo, ciertas aplicaciones de herencia pueden cesar de funcionar correctamente después de inhabilitar las sesiones nulas, así la comprobación es una necesidad. Las colocaciones debajo del contorno disponible controlan dentro de

Windows XP para limitar exactamente lo que la información puede existir por la sesión nula. Note que estas colocaciones afectan las cuentas de puesto de trabajo locales y sólo recursos, pero no cuentas y porciones de campo.

Note que Windows 2000 maneja esta colocación diferentemente, aunque la red efectúa lo mismo. En Windows 2000, estas opciones corresponden a " las restricciones adicionales para las conexiones anónimas. "Además de otras diferencias menores en Windows 2000 y políticas de Windows XP, y herramientas de Windows 2000 no deben ser usadas al poner la política para Windows XP.

Acceso de red: Permitir anónimo SID/traducción de nombre

Cada objeto dentro del directorio activo obtiene un identificador (SID) de seguridad binario único. Los controles de sistema operativo acceden a los recursos por su formato de SID. SID es bien conocido, y cierto SID (administrador local y el huésped local) tienen propiedades que divulgan el propósito real de la cuenta.

Inhabilite esta opción para impedir el usuario nulo de traduciendo los binarios SID en el nombre real de cuenta.

Acceso de red: No permita la enumeración anónima de las cuentas de SAM

Por defecto, la entrada en el sistema de sesión nula puede listar todas las cuentas dentro de su campo. Esto presenta un riesgo de seguridad significativo, particularmente si las contraseñas fuertes no son requeridas. Un ataque es capaz de recoger anónimamente todas las cuentas disponibles, ellos pueden probar entonces la adivinanza básica para localizar rápidamente cuentas con las contraseñas en blanco o muy débiles.

SAM representa el gerente de cuenta de seguridad. La base de datos de SAM tiene toda la

información de cuenta incluyendo contraseñas, derechos de acceso y privilegios especiales. La información de cuenta local resida en la base de datos de SAM local, un archivo en el puesto de trabajo. La información de cuenta de dominio que reside en la base de datos de SAM en el controlador de dominio.

La protección de la sintaxis para esta opción: Los medios habilitados sólo verdaderamente autenticados de entradas en el sistema pueden enumerar otras cuentas; Incapacitado significa que todas las cuentas se pueden reunirse por la sesión nula.

Acceso de red: No permita la enumeración anónima de las cuentas de SAM.

Además de proteger la lista de las cuentas de usuario, ello controla también la lista del archivo de network, establecida en el puesto de trabajo.

La protección de ejecución de datos ((Sólo SP2)

La protección (DEP) de ejecución de datos proporciona protección contra los ataques de exceso de defensas. La protección es puesta en práctica por hardware o software, en dependencia de la configuración de sistema. Por defecto, la protección de ejecución de datos es habilitada para todas las aplicaciones compiladas con las opciones específicas a proteger contra los excesos de defensas.

DEP se puede inhabilitar a todo lo ancho del sistema, o para las aplicaciones específicas. En realidad, Microsoft también ofrece recomendaciones en cómo desplegar DEP. Sin embargo, la más común vía para acceder a las colocaciones de DEP se ha determinado en el panel de control. Escoja el icono de "sistema", y en la pestaña Configuración Avanzada ->. En la ventana que abre, haga clic sobre prevención de ejecución de datos. En esta

ventana, usted puede inhabilitar DEP completamente, o sólo volver en las aplicaciones específicas. Las diferentes opciones son disponibles si su sistema soporta DEP con base en el hardware.

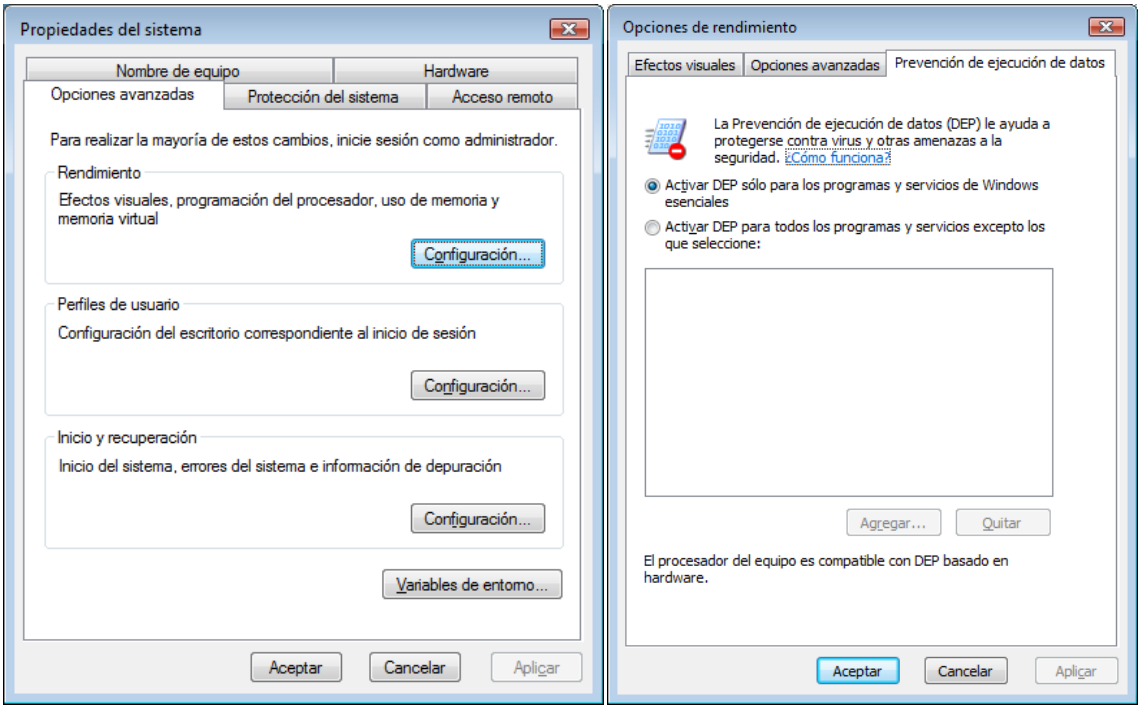


Figura 4.3: Propiedades del Sistema

La Prevención de ejecución de datos (DEP Data ExecutionPrevention) es una característica de seguridad que ayuda a impedir daños en el equipo producidos por virus y otras amenazas a la seguridad. Los programas perjudiciales pueden intentar atacar Windows mediante la ejecución de código desde ubicaciones de la memoria del sistema reservadas para Windows y otros programas autorizados. Estos tipos de ataques pueden dañar los programas y los archivos.

DEP puede ayudar a proteger el equipo mediante la supervisión de los programas para garantizar que utilizan la memoria del sistema de forma segura. Si DEP advierte que un

programa del equipo usa la memoria de forma incorrecta, lo cierra y envía una notificación al usuario.

Debido al significado de las defensas y el desborde de los ataques, y porque las aplicaciones tienen que compilarse específicamente para imponer DEP con base en software, es un requerimiento de seguridad principal para habilitar DEP para todas las aplicaciones.

Menores Configuraciones de seguridad

Cuentas: Estatus de cuenta de administrador

Cada instalación de Windows XP crea una cuenta de "administrador" que da el más alto acceso al sistema. La cuenta da el acceso posible más alto y puede desviar la mayor parte de la seguridad, controla a la máquina local; es comparable a la cuenta "radical" en UNIX. Muchas características de mantenimiento de sistema requieren el uso de la cuenta de administrador. Sin embargo, en algunos los entornos, la existencia de esta cuenta puede presentar un riesgo de seguridad. Por poner el "estatus de cuenta de administrador" para inhabilitar, la cuenta se vuelve indisponible.

Cuentas: Estatus de cuenta de huésped

La cuenta de huésped puede proporcionar cierta regulación a los usuarios no legalizados. Inhabilitar esta cuenta impedirá a los usuarios desconocidos ser autenticados como huéspedes. Esta instalación implícita inhabilita esta cuenta, y debe permanecer incapacitada.

Cuentas: Limitar Cuenta local de contraseñas en blanco solo para entrada.

Windows divide las entradas en el sistema de computadora en dos tipos principales: consola o entradas en el sistema local y entradas en el sistema remotas. En una entrada en el sistema de consola, él se dedica a la explotación del sistema físicamente al dispositivo con el teclado anexo. Las entradas en el sistema remotas son ejecutadas a través de la red usando varios protocolos tal como |telnet|, FTP y escritorio remoto.

Cuando esta colocación se habilita, la computadora rehúsa las entradas en el sistema remotas si los intentos de usuario para usar una contraseña en blanco se ejecutan, aún si la contraseña en blanco es válida para esa cuenta. Las contraseñas nunca deben estar en blanco.

Renombre de nueva cuenta de administrador

A menudo inhabilitar la cuenta de administrador no es común. Sin embargo, simplemente conocer el nombre de una cuenta en una máquina puede ser información valiosa a un ataque. En un intento para ocultar la cuenta, las prácticas mejores recomiendan nombrar de nuevo la cuenta para algo único para su ejecución.

Si se nombra de nuevo la cuenta, el identificador (SID) de seguridad anónimo/nombre la traducción también debe estar deshabilitada. Esto impide que a un ataque localizar la cuenta nombrada de nuevo por su SID.

Renombre de nuevo cuenta de huésped

Similar a la cuenta de administrador, la cuenta de huésped se debe nombrar de nuevo aún si se inhabilita. El sistema operativo pone las salvaguardas adicionales en la cuenta de

huésped y es el menor de un objetivo que la cuenta de administrador.

Revise el acceso del sistema global de objetos

El sistema global se opone típicamente a que proporcione sólo la información de examen de cuentas. Ciertos ejemplos de estos objetos de núcleo, comunican por señales y dispositivos de DOS. La operación de sistema normal no requiere ser revisado a este nivel del detalle.

Revise el uso del soporte y restaure privilegios

Cuando habilite, esta colocación generará una entrada de log para cada archivo que es subida, restaure usando el " soporte o restaure " privilegio. Durante operaciones normales, esto generará una cantidad grande de las entradas de evento, y no se exige.
Varios ataques son de soporte de usar posible o restauran privilegios. Por ejemplo, un ataque puede sostener información sensitiva a una ubicación desautorizada. O, el ataque puede restaurar un archivo inválido - posiblemente un |hacktool| - de un soporte alterado.

Cierre el sistema inmediatamente si es incapaz para registrar las alarmas de seguridad.

Un administrador de sistema puede escoger no, para sobregrabar eventos cuando el registro de evento es completo. Asumiendo que los diarios son encolados apropiadamente, y rutinariamente, esto puede indicar un incidente de seguridad. En el entorno de seguridad especializado, la incapacidad a los eventos de log puede ser la causa justa para parar el servidor.

Si el servidor no puede registrar eventos y esta colocación se habilita, un error de parada ocurre. Para recobrar, el administrador local debe entrar a la computadora y aclare manualmente el evento entre o cambie esta colocación.

DCOM: Restricciones de acceso a la máquina (Sólo SP2)

Con Service Pack 2 para Windows XP, Microsoft introdujo los cambios significativos en el componente distribuido en el modelo (DCOM), el modelo de medidas de seguridad DCOM proporciona los servicios de informática en los puertos de TCP no estándar que puede ser accedido local o remotamente.

Estas nuevas restricciones son importantes al proteger contra DCOM. Desde muchos servicios se pueda publicar completamente el enlace de DCOM, el administrador de máquina retiene un pequeño o ningún control sobre la autenticación. Las nuevas opciones permiten al administrador para poner las restricciones a todo lo ancho del sistema en todo DCOM: Todas las solicitudes de DCOM el primero debe ser autenticado, y entonces las credenciales suministradas son igualadas contra este ACL para determinar si se otorga el acceso. Note que muchas aplicaciones DCOM proporcionarán los controles de seguridad más granulares para un servicio publicado específico.

DCOM: Restricciones de lanzamiento (Sólo SP2)

Las restricciones adicionales pueden ser situadas en que las cuentas son permitidas para activar o lanzar DCOM. Los permisos de lanzamiento son requeridos para que empiece un servidor de COM cuando se activa. La activación es el proceso de conseguir un poder de enlace de COM, y a veces requiera el servidor de COM para lanzarse.

Por defecto, los administradores sólo pueden activar remotamente o lanzan servicio de DCOM. El " todos " grupo es permitido para lanzar o activar sólo de la máquina local.

Permitido para formatear y expulsar los medios desmontables

Esta colocación gobierna el tipo de usuarios que tiene autoridad para quitar NTFS que formatee los medios de la computadora. Las elecciones disponibles (liste de la mayoría para restrictivo menor) son administradores, administradores y usuarios, o administradores de poder y usuarios interactivos.

Los usuarios prevenidos de instalar conductores de impresoras

Usuarios que típicamente necesitan la habilidad para instalar y configurar sus propios impresores. El usuario malicioso pudo optar por instalar un inválido o troyano que imprima como conductor para ganar el control en el sistema.

Los usuarios impedidos de instalar los conductores de impresor pueden llevar a las llamadas de apoyo indeseadas.

Restrinja acceso de CD para entrar en el sistema localmente.

Con privilegios suficientes, los usuarios pueden crear las porciones de red de cualquier carpeta en un puesto de trabajo de Windows. Esto se extiende para dividir una unidad de disco compacto externamente. Esta colocación restringiría el uso de la unidad de disco compacto definida a la entrada en el sistema interactivo local.

Generalmente, usuarios y procesos no deben necesitar acceder remotamente a una unidad de disco compacto desde su puesto de trabajo; sin embargo, habilitar esta colocación pudo causar problemas con ciertos paquetes de instalación de software.

Cuando los usuarios instalan software de una unidad de disco compacto, y el paquete de instalación use el instalador de Microsoft (.el |msi| empaca), el servicio de instalador de Windows en realidad ejecuta la instalación, el install fracasará.

Restrinja acceso Floppy para entrar en el sistema localmente

De nuevo, el usuario no puede recordar que la información en todos los floppy insertados llegue a ser expuesto.

Controlador de dominio: No permite los cambios de contraseña de cuenta de máquina

Si una computadora es un miembro de un DOMINIO, hay una cuenta dentro del dominio. Aunque la cuenta no puede ser usada para entradas en el sistema interactivas, puede estar acostumbrado a autenticar a los recursos de campo. Esta colocación sólo impacta puestos de trabajo que han unido un dominio.

Como cualquiera otra cuenta, en la cuenta de computadora hay nombres y contraseñas. La computadora maneja su propia contraseña y debe cambiar a una contraseña fuerte regularmente. Esta colocación puede impedir que la máquina de manejar su propia contraseña.

Miembro de dominio: Elaborar edad de contraseña de cuenta

Esta colocación determina con qué frecuencia la computadora restablece su contraseña.

Recuerde elaborar los cambios de contraseña ya que no impactan visiblemente el usuario final, y deben ser consistentes con la política corporativa para el manejo de cuenta.

Entrada en el sistema interactivo: No muestre último nombre del usuario

En una computadora puede ver el nombre del último usuario válido que entró al sistema. Esta información puede parecer trivial, pero ello ayuda un ataque a un puesto de trabajo a un individuo particular, o pueda ayudar en un ataque ganar acceso a un dispositivo móvil robado.

Ciertos usuarios no pueden saber su entrada en el sistema, particularmente cuando ello difiere de la dirección de correo electrónico u otras cuentas.

El sistema operativo de Windows trata el CTRL+ALT+DELETE como la llave diferente de entrada. El diseño de sistema operativo impide cada aplicación de interceptar y responder cuando se aplican estas llaves. Cuando usted representa CTRL+ALT+DELETE, es avalado que el proceso de autenticación de sistema operativo manejará la solicitud.

Con el CTRL+ALT+DELETE el requerimiento alzó, el usuario pudo estar representando en realidad su contraseña en una aplicación troyana, antes que el proceso de autenticación de sistema operativo. Recuerde, la aplicación troyana no es capaz de responder.

Texto de mensaje para usuarios intentando entrar

Los usuarios deben acceder a las políticas de uso aceptables, y ser notificado que el sistema se puede controlar. El mensaje es comúnmente mencionado como una "bandera de entrada en el sistema".

Este sistema es sólo para el uso de usuarios autorizados, los no identificados serán controlados.

Título de mensaje para usuarios intentando a ingresar

El título de mensaje actúa como parte de la bandera de entrada en el sistema discutida arriba. El puesto de trabajo pone este texto como el título para la ventana sobresaliente de entrada en el sistema. El texto debe ser neutral o una advertencia. Evite invitar los títulos tal como "bienvenida".

Número de entradas previas en el sistema a Cache

Cuando un puesto de trabajo pertenece a un dominio, los usuarios lo pueden entrar usando las credenciales de dominio. Las credenciales de dominio se pueden ocultar en un archivo oculto en las cuentas de seguridad del puesto de trabajo local, la base de datos de gerente (SAM).

Al establecer la política corporativa para las cuentas ocultadas en un archivo oculto, considere el usuario remoto. Comúnmente entran en el sistema con las credenciales ocultadas en un archivo oculto de un ordenador portátil pequeño. Para acceder recursos corporativos, el usuario establece una conexión de red (VPN) privada virtual a la red corporativa. Desde la entrada en el sistema ocurrir antes del dominio está disponible - el VPN no ha sido establecido - el usuario nunca será impulsado para cambiar la contraseña en la cuenta ocultada en un archivo oculto.

Impulse al usuario a Cambiar Password antes de la expiración

La contraseña de un usuario es cercana a su fecha de expiración, el proceso de entrada en el sistema advierte el usuario y pregunta si querrían cambiar la contraseña. Una vez la

contraseña ha expirado, el usuario será requerido para cambiar la contraseña para completar la entrada en el sistema. Esta colocación gobierna la ventana de la conveniencia entre el tiempo cuando el sistema ofrece el usuario para cambiar la contraseña, y el tiempo cuando son requeridos para cambiar la contraseña.

Requiera autenticación controlador de dominio para abrir puesto de trabajo

Esta colocación resulta de una característica en la autenticación de dominio de Windows; otra comprensión del comportamiento le ayudará a determinar la colocación pertinente a su organización. Esta colocación no afecta los puestos de trabajo autónomos.

La sucesión típica para dejar de abrir unos flujos de puesto de trabajo es usar algo como esto:

1. El usuario repetidamente teclea la contraseña mala.

2. Para cada contraseña intentada, el primer puesto de trabajo compara la contraseña a la contraseña ocultada en un archivo oculto. Si no hacen juego, hace contacto con el controlador de dominio e intentos a la entrada en el sistema.

3. Después de un número predefinido de intentos, el controlador de campo se cierra el exterior la cuenta, y el puesto de trabajo relata el cierre forzoso de cuenta.
En este punto, la mayor parte de los usuarios avisarán el administrador de sistema y tenga el cierre forzoso de cuenta y tal vez la contraseña restablece. Sin embargo, considere el usuario persistente que continúa intentando a la entrada en el sistema.

4. El usuario continúa intentar a la entrada en el sistema. Cada vez que una contraseña mala es ingresada, el puesto de trabajo todavía lo compara al archivo oculto local; cuando

la comparación fracasa, hace contacto con el controlador de campo, que niegue también que el entrada en el sistema.

5. Finalmente, el usuario entra la contraseña correcta. La comparación de puesto de trabajo al archivo oculto local tiene éxito.

Si esta colocación es incapacitada, el usuario entonces con buen resultado abre el puesto de trabajo. Aún con una cuenta cerrado, el usuario puede continuar entonces accediendo recursos de red para conexiones que estaba establecido y autentique antes de la máquina sea sido cerrado - envié por correo servidores y servidores de archivos en particular.

Habilitar esta colocación, sin embargo, añade un adicional retire se cada comparación de puesto de trabajo exitosa con el archivo oculto local

6. El puesto de trabajo presenta las credenciales al controlador de campo. Sólo si la autenticación de controlador de campo tiene éxito puede el puesto de trabajo es abierto.

Habilitar esta colocación para proteger contra los ataques de contraseña de fuerza bruta por el preservador de pantalla. Sin embargo, habilitando lo estorbar el usuario que se cierra e inverne su puesto de trabajo, y entonces intentos para reasumir cuando el controlador de campo es indisponible. Inhabilitar esta colocación (o dejando lo indefinido) minimice tráfico de controlador de campo.

Para mayor información, vea artículos 188700 de base de conocimiento de Microsoft, " el contraseña de Screensaver trabaja aún si la cuenta es cerrar la puerta a " y 281250, " información sobre abriendo un puesto de trabajo "

Comportamiento de remoción de tarjeta con memoria

Cuando los usuarios autentican con tarjetas con memoria, el sistema puede estar puesto en cerradura o salida del sistema el usuario cuando usa la tarjeta de memoria es quitada.

Cada colocación aparte de " ninguna acción " es aceptable.

En un entorno que no usan tarjetas con memoria, esta colocación no tiene ningún efecto.

Acceso de red: No permita el almacenamiento de credenciales o pasaportes de NET para la autenticación de red

Esta colocación controla el comportamiento del " almacenaron nombres del usuario y las contraseñas " característica de Windows XP. esta característica almacenan NTLM, Kerberos, pasaporte y autenticación de SSL; no debe ser confundido con el archivo oculto de autenticación de Internet Explorer, desde entonces es manejado separadamente. Ciertos documentos se refieren a esta colocación como " acceso de red: No permita nombres del usuario guardados y contraseñas a las contraseñas o credenciales seguras para autenticación de campo".

Esté en guardia de la sintaxis para esta opción: Habilitado guardan credenciales fuera del archivo oculto; Incapacitado permite almacenando nombres del usuario y contraseñas.

Fuerce salida del sistema cuando las horas de entrada en el sistema expiran

Esta colocación sólo se aplica a puestos de trabajo una a un campo, como horas de entrada en el sistema no pueden determinado para las cuentas locales. La colocación negocia exclusivamente con conexiones usando el protocolo de SMB, y no con la sesión interactiva de entrada en el sistema.

Habilitar esta característica desconectará todas las conexiones de cliente cuando la entrada en el sistema cronometra límites son alcanzadas. Por defecto, el puesto de trabajo sólo impone las horas de entrada en el sistema durante disposición de sesión, y no después.

Permita que el sistema se cierre sin tener que entrar en el sistema

Ciertos sistemas corren los procesos críticos y sólo debe estar cerrar por los usuarios autorizados. Ocasionalmente, los procesos especiales se pudieron evocar durante arranque de sistema, a veces aún procesan. En entornos donde los reboots de sistema anormales pudieron causar problemas, requiera una entrada en el sistema antes de los reboots.

Objetos de sistema: Fortalezca los permisos implícitos de los objetos de sistema internos

Esta colocación en realidad cava profundo en el comportamiento de sistema operativo y deba estar a la colocación implícita (habilite) a menos que exija explícitamente.
"el sistema interno se opone " son partidos los recursos físicos y lógicos tales como semáforos y nombre de dispositivo de DOS; los objetos todo es creado con listas de control de acceso (ACL). Cuando habilite, el ACL permite otro sistema no administrativo procesar para inquirir los objetos de sistema internos, pero no permite les modificarles.

Configuraciones Adicionales de registro

Los párrafos siguientes describen las colocaciones de seguridad individuales que pueden ser aplicadas en una variedad de vías usando REGEDIT.EXE, REGEDT32.EXE, el grupo de Policy, o Domain de grupo local Policy. Se puede consultar el sitio en Internet de Microsoft TechNet a http://www.microsoft.com/technet. Alguna otra información de registro útil está disponible en http://support.microsoft.com/default.aspx?scid=kb;elene-nos;Q256986yhttp://www.microsoft.com/technet/prodtechnol/winntas/tips/winntmag/inreg.asp.

Suprima Dr. Watson Crash

Dr. Watson es las utilidades de uno de Microsoft que manejan errores en las aplicaciones. Si una aplicación produce un error que Dr. Watson puede manejar, vaciará los contenidos de la memoria para esa aplicación a un archivo para el análisis futuro.

En el proceso de escribir los contenidos de la memoria para grabar en disco, es totalmente posible que información de contraseña pudo ser escrita para grabar en disco además, y más tarde explotado. Ponga este valor al cero para impedir Dr. Watson de escribir los basureros intensivos al disco.

Inhabilite la ejecución automática del instrumento de puesta a punto de sistema

Si una aplicación es ejecutada en memoria no privilegiada, y el instrumento de puesta a punto de sistema es empezado, es posible para esa aplicación para ejecutar código en el espacio de memoria privilegiado. Ponga este valor al cero para impedir el instrumento de puesta a punto de sistema de ejecutar de forma automática.

Inhabilite |autoplay| de cada disco

Aunque es conveniente para aplicaciones para correr de forma automática cuando el explorador de Windows descubra el pecho, ello puede causar también aplicaciones para ejecutarse contra los deseos de un administrativo el usuario, y explotando ese privilegio. Ponga este valor a 255 para impedir que cualquier tipo de drive de forma automática lanzando una aplicación del explorador de Windows.

Inhabilite |autoplay| para el usuario actual

Nota: Debido a la incapacidad para manejar las entradas de registro para cada usuario local por la via de plantillas de seguridad, esta colocación se recomienda, pero requerido o medido.

Inhabilite |autoplay| para nuevos usuarios en defecto

Similar al |autoplay| tome forma sobre, esto impone la política para cualesquiera nuevos perfiles cree en el puesto de trabajo.

Inhabilite la entrada en el sistema automática

Windows también tiene la habilidad para registrar de forma automática un usuario cada vez que la máquina se levanta precipitadamente. Ciertos usuarios pueden preferir que este como una característica. Cierto servidor puede requerir un registro de usuario antes de que pueda ejecutarse, así que requieren chequear esta actividad también.

El problema con esta "característica" para trabajar, es que almacena el |username| y contraseña para ese usuario en el |plaintext| en el registro. Ponga este valor al cero para impedir que cada usuario de forma automática ingrese cuando la computadora se levanta precipitadamente.

Inhabilite los reboots automáticos después de ver una pantalla azul de la muerte

Si alguien ingenie para consiga el control bastante de su computadora que pueden plantar una aplicación allí, el próximo paso es forzar su computadora para comenzar de nuevo para registrar ese |app|. Una fácilmente vía para realizar esta tarea es forzar programática un error que causa la computadora a choque, o "pantalla azul" que reboot la máquina en defecto. Ponga este valor al cero para impedir este comportamiento de sucediendo, y al menos alerta el usuario que algo no tiene razón.

Inhabilite ejecución automática de CD

Si el software malicioso es escrito a un CD, se puede ejecutar por el explorador de Windows sólo por poner el CD en la guía. Ponga este valor al cero para impedir todas las aplicaciones de de forma automática lanzándose de la unidad de disco compacto.

Quite las porciones administrativas en el puesto de trabajo (profesional)

Cada Windows NT/2000 computadora de forma automática tienen las "porciones administrativas" instaladas en defecto. Éstos son limitados para usar por los administradores, pero ellos exponen cada volumen arraigue, y la carpeta de %systemroot% a la red como Admin$, C$, etc. Éstos hacen conveniente remoto de administración, pero presentan también un riesgo si alguien se ingenia para la suposición la contraseña a una cuenta administrativa.

Ayude a proteger contra la fragmentación de paquetes pequeños

Cuando los datos son transbordados a través de una red, los datos están roto abajo en el paquete pequeño. Estos paquetes pequeños no son siempre un tamaño uniforme. Cuando estos paquetes pequeños están rotos abajo en los tamaños más pequeños, tienen por deber para volverse a reunir al otro fin de una ruta de red en la misma orden. Esto siempre no va como planee, y puede usado en ciertos ataques de red.

Ponga este valor a 0 para forzar Windows para usar un 576 paquete pequeño de byte consistente. Más los detalles están disponible en http://support.microsoft.com/?kbid=315669.

Maneje los tiempos de subsistencia viva

El KeepAliveTime determina con qué frecuencia los intentos de |subsystem| de red para verificar que una sesión de TCP es todavía activa. La colocación de 300,000 sale bien a una solicitud cada cinco minutos.

Proteja contra los ataques de liberación de nombre maliciosos

Por defecto, una computadora corriendo NetBIOS soltará su nombre a petición. A fin de proteger contra ataques maliciosos de liberación de nombre, ponga este valor a 1. Microsoft también referencias en al menos un ponga que esto es para Windows 2000 Service Pack 2 o mayor.

Oculte el puesto de trabajo de la inscripción de visor de red

Si el servicio de visor de computadora es incapacitado, o si esta computadora no es la parte de un campo, esta colocación no tiene ningún efecto. De otra manera, impedirá la computadora de anunciarme a los servicios de visor de otras computadoras, y único actúe como un "escuchante" en el campo examina listas.

ADVERTENCIA: Esta colocación quitará su computadora de la lista de las computadoras disponibles en su campo en el entorno de red. Esto debe hacerse para inhabilitar el servicio de visor de computadora, pero esta colocación ejecutará la misma función.

USB bloquea la política de dispositivo de almacenamiento (Sólo SP2)

La mayor parte de los dispositivos de almacenamiento de USB pueden ser unidos a un puesto de trabajo de Windows para proporcionar capacidad de almacenamiento extra, o para mover archivos entre trabajo y casa. Sin embargo, la política corporativa puede prohibir sensitiva móvil salen uno por uno del almacenamiento de red y en un dispositivo

desmontable. La "política de dispositivo de almacenamiento" ayuda a controlar el uso de estos dispositivos.

Cuando habilite, la política de dispositivo de almacenamiento de bloque de USB causa todos los dispositivos de almacenamiento masivo de USB para ser montado sólo para lectura, y archivos no se pueden ahorrar al dispositivo.

NOTA: En el momento de esta escritura, esta funcionalidad era muy limitada, y aplíquese sólo a dispositivos usando el conductor de Microsoft USB estandar. Costumbre conductores de USB no son afectados por esta política.

Protección de Seguridad Adicional

No permita los ordenadores portátiles pequeños para conectar a la LAN

- **Use autenticando interruptores.** Si una computadora desautorizada que se introduzca ya sea por un empleadou otro ajeno a la empresa, o un ataque; los intentos para conectarse a la red, marcaran su acción. Si manejA correctamente la autenticación, puede inhabilitar también las computadoras tomadas de la red, siendo inadvertidamente ATACADO.
- **Use las cuarentenas de red.** Segmente una porción de la red para usarse por los sistemas móviles. Niegue que acceso al resto de la red hasta que se actualice correctamente.

Prohíba las redes inalámbricas que no se encuentran en las necesidades de norma de actuación sobre seguridad de la empresa.

La mejor política es prohibir las redes inalámbricas a menos que ellos encuentran el radio acceda la política de su organización. Imponga esta prohibición incluyendo en la política la declaración que el incumplimiento es causa de terminación de empleo.

Su norma de actuación sobre seguridad inalámbrica debería requerir codificación y autenticación. Esto se puede poner en práctica con nuevas redes inalámbricas por usar EAP protegido (PEAP) y autenticación 802.1x. Las redes inalámbricas más viejas se deben segmentar de la red reforzada por alambre y requieren el uso de las conexiones de VPN a la red reforzada por alambre.

Servicios del sistema

Cada pieza del código que ejecuta en una computadora exista en un proceso. Muchos de estos procesos empiezan como "servicios". Puede mirar una lista de procesos dando un golpe a la tecla secundaria del ratón sobre " mi computadora " , y haga clic sobre "conducción". Expanda "servicios y aplicaciones" y "servicios" de clic. Estos servicios son programados para empezar o a tiempo de bota, como arranque automático o manual normal, o inhabilite para no empezar en modo alguno.

Los servicios listaron debajo de deber ser incapacitado para proteger su computadora contra ciertas vulnerabilidades. Estos servicios pueden restringir también cierta funcionalidad que usted está acostumbrado a, pero nosotros hemos probado para mantener un nivel razonable de la funcionalidad donde posible.

Permisos en servicios listados aquí: **Administradores: Control completo; Sistema: Lea, empiece, haga alto, y la pausa.** Permisos en servicios se deben poner usando la plantilla de seguridad que acompaña la herramienta de raya de CIS Windows.

Más alerta

El servicio más alerta es normalmente acostumbraron a enviar mensajes entre procesos en una computadora que "alertan" el estatus de ciertas funciones para la consola del usuario, incluyendo la ejecución de los trabajos de impresión. Ello trabaja en también conjunción con el servicio de mensajero para enviar estos mismo envian mensajes entre computadoras en una red.
El servicio más alerta es incapacitado en defecto con Windows XP Service Pack 2.

Actualizaciones automáticas

Los servicios de actualizaciones automáticos son sido publicados primero con Windows XP. ello regularmente verifica el microsoft web site en la base, e inicie la descarga de cualesquiera nuevas actualizaciones críticas como se vuelven disponibles. Es diseñado para no usar el ancho de banda de red excesivo. Este servicio no instala algo se, ello haga actualizan listo para instalar.

NOTA: Las actualizaciones automáticas atienden y la transferencia inteligente de base atiende trabajo en conjunto para ayudar mantener las computadoras hasta la fecha con los últimos parches críticos. Las organizaciones que tienen una separata remiendan la estrategia de manejo debería inhabilitar estos servicios para impedir el sistema unmanaged remendando. Otras organizaciones o los usuarios individuales que no tienen otro método de remendando deba dejar estos servicios habilitan y hacen uso de este regalo de Microsoft para mantener arreglan a la fecha.

La transferencia inteligente de la base(a.k.a. LOS BITS)

El servicio de BITS trabaja en conjunción con los servicio de actualizaciones automáticos para descargar las actualizaciones críticas del sitio en Internet de Microsoft, y la marca les disponible por la instalación. El servicio corre en la base, y hace uso del ancho de banda no usado y disponible.

Clipbook

El servicio de Clipbook está acostumbrado a compartir la información de portapapeles entre computadoras en una red. En la mayor parte de los casos, usuarios no quieren compartir que la información con otras computadoras.

Visor de computadora

El visor de computadora (no para ser confundido con Internet browser, tales como Internet Explorer o Netscape) subsistencias están en alineación de las computadoras en una red dentro de un campo. Ello permite usuarios para "examinar" por la vecindad de red para encontrar los recursos divididos necesitan sin conocer el nombre exacto de ese recurso.

Desafortunadamente, ello permite todo el mundo para examinar a esos recursos antes de verificar cualquier en cierta medida autenticación o autorización.

Inhabilitando este servicio requerirá usuarios para saber los recursos que ellos están buscando, de nombre, y pueda resultar en un número aumentado del escritorio de ayuda llama.

Servicio de fax

El servicio de fax es usado para la recepción desatendida de los fax entrantes. No es requerido por la transmisión, o recepción manual de fax. Requiere que una computadora está corriendo todo el tiempo, y tenga el modem ponerse a respuesta de auto.

Hablando en términos generales, con el bajo costo de las máquinas de fax dedicadas, la respuesta a segura la mayor parte del enviando por FAX a las necesidades son tener una máquina de fax dedicada para recibir los fax.

FTP Publishing Service

El servicio de FTP Publishing es parte del departamento de servidor de información de Internet de las aplicaciones Internet. No es instalado en defecto. Es usado para hacer archivos en su disponible local de máquina a otros usuarios en su red o la Internet.

Hablando en términos generales, los puestos de trabajo no comparten archivos con otras computadoras. Este servicio debe ser incapacitado, o apartado. Si ello está instalado, se debe correctamente mantenido, que es un asunto más allá del alcance de esta prueba de características.

IIS Admin Service

También parte del departamento de IIS de servicios, el servicio de IIS Admin maneja los otros servicios de IIS. Si este servicio no está corriendo, otros servicios que son parte del departamento de IIS no funcionará tampoco. Inhabilite este servicio. Si posible, esto debe ser apartado de los puestos de trabajo.

Hacer un índice de servicio

Este servicio hace un índice de archivos en el sistema en un intento para mejorar

ejecución de búsqueda. Sin embargo, el servicio puede ocasionalmente consumir los recursos excesivos cuando comparado con su utilidad.

Mensajero

El servicio de mensajero trabaja en tándem con el servicio más alerta. Permite los servicios más alertas de las computadoras múltiples para enviar alarmas para mutuamente sobre una red. La mayor parte de los usuarios pueden vivir sin el mensajero y los servicios más alertas y todavía realizan las tareas que necesitan hacer en el transcurso de un día normal.

En 15 de octubre de 2003 , Microsoft soltó boletín de seguridad 03-043. Este boletín es un consultor de una vulnerabilidad en el servicio de mensajero que permite un ataque para ejecutar el código de aplicación de su elección. Inhabilite este servicio para impedir que este, o como-sin embargo las vulnerabilidades similares desconocidas de afectar un sistema.

Entrada en el sistema

El servicio de entrada en el sistema establece el canal seguro de NetLogon con un controlador de campo.

Participación de NetMeeting Remote para PC - escritorio

Microsoft ha hecho las herramientas de colaboración una de las mejores que son disponibles en el mercado hoy, pero al mismo tiempo tomaron esa herramienta NetMeeting y probado para hacer ello en una utilidad de control remoto para el personal de escritorio de ayuda para tomar el control de su computadora a tiempo de la necesidad. En un mundo de los ataques de intruso y excesos de parachoques, ello parece quiera sólo una materia del tiempo antes de una proeza es hallada, o se abusa de sólo. Si no tenga un

escritorio de ayuda dedicado, o su escritorio de ayuda no usa participación de buró de NetMeeting remoto inhabilita este servicio. Si su organización requiere este servicio, deba comprender que puede existir un riesgo envolvió.

Gerente de sesión de ayuda para escritorio remoto

Este servicio soporta la funcionalidad remota de asistencia. Inhabilite el servicio para prohibir el uso de la asistencia remota.

Servicio de registro remoto

El registro de Windows es esencialmente una base de datos de colocaciones y opciones de configuración ese sentimiento casi cada función de una computadora de Windows XP. Ello determina cómo toda cosa se comporta a arranque, paro del trabajo, y toda cosa en entre. El propósito de los servicios remotos de registro es exponer que la base de datos al resto de la red por una conexión de NetBIOS.

Tan aterrador como eses sonidos, este servicio es habilitado en defecto en cada computadora de Windows desplegado desde el advenimiento de Windows 95. una mayoría de las herramientas de administración remotas ha sido escrito para aprovecharse del servicio remoto de registro para ejecutar funciones que pueden normalmente requerir una porción de su aplicación para ser instalado localmente.

Debido a su distribución extendida, y su propósito inicial, y el hecho que es todavía sólo protegido por un |username| y contraseña, el servicio remoto de registro es responsable para abrir las puertas a los huéspedes no invitado así como las utilidades remotas de manejo que está acostumbrado a soportar. Inhabilite este servicio para impedir el acceso remoto al registro de sistema.

ADVERTENCIA: Por inhabilitar este servicio, usted está cortando cada habilidad para los administradores de personal de apoyo o de campo para manejar remotamente su computadora a menos que existe otra aplicación ya instalada en su computadora para permitir esas funciones. Sea cauteloso que esto puede romper un gran número de aplicaciones a todo lo ancho de la empresa.

Caída y el acceso remoto

La asignación de ruta y el servicio de acceso remoto están usadas o para facilitar servidores son los servidores de acceso remotos, o para permitir computadoras de una red para obrar recíprocamente con computadoras en otro.

RRAS no es enteramente puesto en práctica en profesional de Windows XP guste es en los sistemas operativos de servidor. Usuarios generalmente no necesitan a RRAS en los puestos de trabajo. Si este servicio no pueda ser incapacitado, ello se debe cerrar abajo en lo posible. Más la información está disponible en: http://www.microsoft.com/TechNet/columns/cableguy/cg0601.asp.

Simple Mail Transfer Protocol (SMTP)

Los puestos de trabajo no suelen usarse como SMTP envió por correo servidores. Este servicio es instalado como parte del departamento de IIS de aplicaciones. Debe ser incapacitado o apartado totalmente.

Simple Network Manager Protocol (SNMP)

El protocolo simple de manejo de red (SNMP) ha sido mucho tiempo la norma aceptada para el manejo remoto por todos los dispositivos de red guimbardas, ejes, UNIX, y Windows igualmente. Es sido hallado recientemente que SNMP ha sido proliferar un defecto peligrosamente explotable durante los últimos diez años más o menos. Si no

tenga un sistema activamente usando SNMP para manejo remoto, lo inhabilite o lo quite del sistema.

(SNMP) armado de trampas

Otra parte del protocolo de SNMP es el servicio de trampa de SNMP. Tal como su contraparte, ello debe ser incapacitado y/o apartado.

Programador de tarea

El programador de tarea atiende los apoyos trenzando los programas de lote para la ejecución futura. Esto pudo incluir el virus examina, los soportes, u otras funciones de mantenimiento de sistema. Con Windows XP, la tarea puede correr bajo las credenciales alternas, y necesariamente no tiene que correr bajo la cuenta local de sistema.

Telnet

El servicio de Telnet no es a menudo instalado en puestos de trabajo. Es usado para el manejo remoto de los dispositivos de red, y ofrezca una cáscara de orden basó en la forma del acceso de red a una computadora. Esto es todo santo y bueno, pero el tráfico transferido por Telnet no es protegido o codifique en ninguna vía. Si esto es un requerimiento, tome el tiempo en examinar una solución de manejo remota segura de cáscara (SSH) para cumplir sus necesidades en una manera más segura. Es bien de valor el tiempo y gasto.

Servicios terminales

Los servicios terminales permiten un enlace gráfico remoto al puesto de trabajo. Similar a PcAnywhere o paquetes de software de cliente (VNC) de red virtuales, los servicios

terminales comparten usando el protocolo para buró remoto (RDP). El uso normal del servicio terminal en un puesto de trabajo termina la sesión de entrada en el sistema interactiva existente; sin embargo, si se habilita la asistencia remota, cualquiera sesión existente puede ser dividida entre dos computadoras.

La proposición universal se atora y juegue el dispositivo hospeda

La proposición universal se atora y juega (UPnP) dispositivos puede ser añadido a la red, y emisión su disponibilidad para el manejo. UPnP no debe ser confundido con el enchufe más común y juego (PnP) caracteriza útil para el manejo de hardware. UPnP encuentra dispositivos en la red; PnP encuentra dispositivos físicamente instalados en la computadora. Pocos dispositivos en el mercado corrientemente requieren UPnP, y este servicio deba ser incapacitado a menos que exija explícitamente.

World Wide Web Publishing Service

Los de papaíto grande de todo explotable servicios son el servicio de World Wide Web de Microsoft. Es la mayoría a menudo ataque la plataforma de servidor de red en la Internet hoy. Como consecuencia, ello ha tenido la mayoría insectos encuentre, y la mayoría defectos explotados. Este servidor no es instalado en defecto, pero no deba existir en su puesto de trabajo medio. Si no está yendo para correctamente mantenido por el personal con una educación en la seguridad de IIS, debe ser incapacitado o apartado.

Derechos de usuario

En conjunción con muchos de los grupos privilegiados en Windows XP, existe varios derechos individuales que pueden ser asignados a usuarios o grupos para otorgarles habilidades que puede ser más allá la extensión de los usuarios normales. No todos estos derechos se aplican a Windows XP Professional.

Acceda esta computadora de la red

La habilidad para acceder una computadora de la red es un derecho de usuario que puede otorgarse o revocar en cada máquina como apropie de. Si esta lista se queda vacía, ningunas cuentas de usuario pueden estar acostumbrados a ganar acceso a los recursos de esta computadora de la red.

Actúe como la parte del sistema operativo

El sistema operativo trabaja en un contexto de seguridad especial llamado " LocalSystem". Este contexto de seguridad tiene la habilidad para hacer las cosas que usuarios normales y los usuarios administrativos pueden otorgar este usuario se une a usuarios o grupos dé les la habilidad para exceder privilegio normal, a pesar de su calidad de miembro de grupo.

Añada puestos de trabajo al campo

Este usuario se endereza aplique se sólo a los controladores de campo, y no tenga ningún efecto en profesional de Windows XP.

Ajuste las cuotas de memoria para un proceso

Esta colocación política define las cuentas que puede ajustar la cantidad máxima de la memoria asignó a un proceso.

Permita entrada en el sistema por los servicios terminales

Si los servicios terminales se habilitan, use esta colocación para explícitamente controlar que los usuarios son permitidos para acceder remotamente el puesto de trabajo.

Mantenga archivos y directorios

Este derecho de usuario otorga un usuario o agrupa la habilidad para circunvenir la

seguridad de archivo Windows normal para los propósitos de la ayuda levante se archivos y carpetas. Debe ser limitado cuando sea posible.

Comprobación de travesaño de desviación

El desviando atraviese se la comprobación derecho de usuario permite acceso a archivos o carpetas a pesar de los permisos del usuario a la carpeta matriz. En otros términos, impida que el la herencia de permisos. Desafortunadamente, es necesario otorgar este derecho a usuarios para permitir el operación normal de aplicaciones en un puesto de trabajo.

Cambie el tiempo de sistema

Cambiar el tiempo de sistema en las computadoras de Windows XP es especialmente importante para restringir en un entorno de campo debido al papel esa vez la sincronización juega en la autenticación de Kerberos. Esto no debe ser configurar para todo el mundo exceptúa administradores.

Cree un |pagefile|

A fin de proteger la potencialmente información sensitiva que puede ser guardada en un |pagefile| , la creación de los |pagefiles| debe ser limitada a administradores.

Cree un objeto simbólico

Permita la creación de un símbolo de acceso de seguridad. Este derecho nunca debe ser dado a cada usuario.

Cree permanente parta se opone

El derecho para crear los objetos divididos permanentes debe usarse sólo por aplicaciones

en el núcleo de Windows. El núcleo ya tiene el derecho para creado tal se opone, así ningunos usuarios alguna vez deben ser otorgado este derecho.

Depure programas

Cada usuario puede depurar sus programas, pero este derecho permite un usuario para depurar otros procesos en una máquina. Los usuarios no deben ser otorgado este derecho exceptúe en un entorno de desarrollo aislado donde posible.

Microsoft es pronto para soltar nueva tecnología de aplicación de remendar caliente que requerirá este derecho para aplicar parches. Promete los reboots menos para parches que necesitan ser aplicados. En esto luz, administradores todavía necesitan este derecho para hacer sus trabajos. Esperanzadamente, esto no será un requerimiento permanente, y se puede eliminar en lo sucesivo.

Niegue acceso a esta computadora de la red

El " niegue que acceso " usuario se endereza siempre |supercede| el " permita el acceso " usuario se endereza, de modo que si un usuario es listado bajo ambos derechos de usuario, ese usuario será negar que acceso. Si no existe ningunos usuarios que se deben permitir el acceso una computadora de la red, los todos el grupo debe listado en el " niegue que acceso a esta computadora de la red " usuario se endereza.

Niegue entrada en el sistema como un trabajo de lote

Tal como el otro " niegue..." derechos de usuario, un usuario listado aquí será negar que acceso a la entrada en el sistema como un trabajo de lote, aún si él haya sido explícitamente otorgue ese derecho.

Niegue la entrada en el sistema como un servicio

Tal como el otro " niegue..." derechos de usuario, un usuario listado aquí será negar que acceso a la entrada en el sistema como un servicio, aún si él haya sido explícitamente otorgue ese derecho.

Niegue la entrada en el sistema localmente

Tal como el otro " niegue..." derechos de usuario, un usuario listado aquí será negar acceso a la entrada en el sistema a la consola, aún si él haya sido explícitamente otorgó ese derecho.

Niegue entrada en el sistema por el servicio terminal

Similar al otro " niegue..." los derechos, grupos y cuentas en esta lista no serán capaz de conectar el puesto de trabajo usando los servicios terminales.

Habilite cuentas de computadora y usuario para gozar de confianza para la delegación

Este usuario se endereza sólo aplique se a los controladores de campo. No tiene ningún efecto en profesional de Windows XP.

Fuerce paro del trabajo de un sistema remoto

Esto otorga un usuario el derecho para cerrar una computadora de la red. Debe otorgarse sólo a administradores, y pueda ser limitado a ningunos usuarios o grupos en modo alguno.

Genere los exámenes de cuentas de seguridad

Este derecho de usuario permite un usuario o proceso para generar eventos para ser añadido al registro de evento de seguridad de Windows.

Prioridad de programación de aumento

La prioridad de programación es una de las colocaciones que pueden ser alteradas como se necesita para la afinación de ejecución, pero los usuarios normales no deben tener la habilidad para cambiar la prioridad de otros procesos.

Cargue y descargue conductores de dispositivo

Los conductores de dispositivo ejecutan como las aplicaciones altamente privilegiadas en una computadora de Windows porque interactúan directamente el hardware con el sistema operativo. Estos conductores pueden ser la fuente de las aplicaciones de "caballo de Troya", y deben ser limitados donde posibles. Esta colocación en realidad se aplica a la instalación de enchufe y juega conductores de dispositivo.

Cierre de las páginas en la memoria

El derecho para cerrar páginas en memoria es la habilidad para forzar datos en la memoria física para permanecer en la memoria física, y no folie se para grabar en disco, que pueda degradar seriamente ejecución de sistema. Este derecho de usuario es obsoleto, y debe permanecer vacío.

Entre en el sistema como un trabajo de lote

El derecho a la entrada en el sistema como un trabajo de lote significa que el usuario ha listado la habilidad a la entrada en el sistema usando la facilidad de cola de lote. Por

defecto, los administradores tienen este derecho, pero muy raramente usa lo. Quite todos los usuarios y grupos de este derecho.

Entre en el sistema como un servicio

La mayor parte de las aplicaciones ése no obra recíprocamente directamente con el usuario de entrada en el sistema (y muchos ese haga) opere en realidad como un servicio. Estos servicios casi siempre ejecutan bajo las credenciales de seguridad de LocalSystem. Si un servicio se necesita ejecutar en un contexto de usuario, que usuario tendría que ser listado aquí.

Entrada en el sistema localmente

Todo el mundo que diarios en localmente a una computadora deben ser listados aquí, o por nombres del usuario individuales, o por los "usuarios" agrupe se.

Auditoría de conducción y registro de seguridad

La habilidad para manejar el registro de evento de seguridad es el equivalente a la habilidad para un intruso para cubrir su están en alineación y destruya la evidencia lo que ha sido hecha a un sistema de computadora. Este derecho de usuario debe ser altamente limitado, posiblemente aún a sólo un subconjunto de los administradores de sistema.

Modifique los valores de entorno necrológicas

Los usuarios individuales han la habilidad para cambiar sus propias variables de entorno, pero los administradores y cuentas sólo que tienen este derecho puede cambiar las variables de entorno de otros usuarios en un sistema.

Ejecute las tareas de mantenimiento de volumen

Las más común tarea de mantenimiento de volumen son "|defrag|" y "|chkdsk|". Además del impacto de ejecución potencial, este derecho pudo permitir también el acceso de bajo nivel a archivos desviando las limitaciones de permiso estandares.

Perfile el proceso sencillo

Este derecho de usuario otorga la habilidad para un usuario para controlar la ejecución de otro usuario o proceso de no-sistema.

Ejecución de sistema Profile

El derecho de usuario de ejecución de sistema Profile permite un usuario o grupo de usuarios para controlar ejecución de sistema, incluyendo los procesos de sistema.

Quite computadora de atracar estación

Este derecho de usuario es sólo lo que usted tener espere se.

Reemplace un símbolo de nivel de proceso

La habilidad para reemplazar un proceso nivela el símbolo esencialmente significa que un proceso puede cambiar la autoridad de autenticación de sus propios procesos de niño.

Restaura archivos y directorios

En conjunción con el usuario de "archivos y directorios suplementarios" enderece se, esto puede ser muy peligroso si un usuario sostiene cierta seguridad relacione información, lo altere, y lo restaure de vuelta al mismo lugar. Debe ser limitado a administradores.

Cierre el sistema

Usuarios otorgaron este derecho tenga la habilidad para cerrar la computadora. Esto surte efecto sólo si usuarios son requeridos para entrar a cierre un sistema.

Sincronice el directorio atiende datos

Este derecho de usuario no tiene ningún efecto en profesional de Windows XP.

Tome la propiedad de archivo u otros objetos

Un usuario que " posee " un archivo tiene mayor autoridad sobre ese archivo que aún los permisos sugerirían. El derecho para tomar la propiedad de un archivo es equivalente a la habilidad para comprometer un sistema de archivos entero.

Otros Requisitos del sistema

Asegure grabe en disco todo volúmenes están usando el sistema de archivos de NTFS

Advertencia: No haga este si su sistema es un sistema de bota dual con Windows 95/98/Me. el sistema operativo alterno cese funcionando, y no pueda recobrarse.

Desde los primeros días de dos, archivos han sido almacenados en los discos flexibles. Estos discos dividen datos en bloques, y esos bloques son escritos a los bloques similares en un disco físico. El "mapa" describiendo que los bloques están teniendo que los archivos son guardados en la parte del disco llame el " archive la distribución tabula " o FAT.

Cuando DOS mover a hard disk, el mismo estilo de FAT de distribución de disco es sido usado. los |filesystems| de FAT han cierto los puntos buenos sobre todo, es bastante

simple. Cada sistema pudo leer los discos, y si existía un problema, los datos pudieron haber sido restaurado. Cuando los discos empezaron para criar más allá del tamaño de las capacidades de FAT, era expandido a FAT32 , tener en cuenta los discos más grandes. Sin embargo, FAT y FAT32 no ofrecen cada seguridad.

La interoperabilidad de NTFS ha venido un buen trecho desde su introducción inicial. Se puede desviar si el sistema se puede rebooted, pero es la vía de ONLY que cualquiera seguridad de archivo a nivel se puede imponer mientras que sistema está operando.

Para determinar si un volumen de disco es NTFS, haga clic dos veces sobre " mi computadora " en el buró. Dé un golpe a la tecla secundaria del ratón sobre la unidad C (la c:) y haga clic sobre propiedades. Las hoja de vidrio de propiedades para ese disco describirán el "sistema de archivos" como FAT o NTFS.

Figura 4.4. Propiedades de la unidad de disco

A fin de hacer un disco de FAT en un disco de NTFS, abra un aviso de comandos (haga clic sobre principio-> programan-> los accesorios->aviso de comandos) y teclee " convierta c: /fs:ntfs ". El sistema probablemente sea requerido para comenzar de nuevo para ejecutar esta tarea. Tome la misma acción con la d: maneje y cualquier otros que sacan a luz como discos de FAT.

Una vez que los discos han sido convertidos a la seguridad implícita de sistema de archivos

de NTFS deba ser aplicado a la guía de bota (la c:). Abra un aviso de comandos (haga clic sobre principio, los programas, accesorios, y el aviso de comandos) y represente la orden siguiente para los puestos de trabajo:

"secedit /configure /dbdefault.sdb /cfg %windir%\inf\defltwk.inf /areas filestore"
o la orden siguiente para los servidores:
"secedit /configure /dbdefault.sdb /cfg %windir%\inf\defltsv.inf /areas filestore"
y la prensa entra. El parámetro de /db es requerido, aunque la base de datos no existe hasta después de la orden corra se. ¿Teclee " |secedit|/?"para más información en esta orden.

Otras aplicaciones habrán la habilidad para usar estas características de seguridad. La mayor parte de los usuarios nunca necesitan actualizar estos permisos de archivo, mientras que administradores de sistema de todos los niveles necesitarán hacer así de vez en cuando. En realidad, es posible lisiar un sistema incorrectamente modificando esa seguridad. Es importante tener presente que esto es todavía un step up de un |filesystem| de FAT sin la seguridad.

NetBIOS en todos los dispositivos de red

Por defecto, el puesto de trabajo de XP usará ambos NetBIOS y DNS transportan en intentar para localizar los recursos divididos tales como archivos e impresores. Sin embargo, Windows 2000 introdujo la habilidad para eliminar NetBIOS y WINS para localizar recursos, en favor de una conexión de TCP directa por DNS.

Inhabilitar NetBIOS reduce los servicios corriendo en el puesto de trabajo. El servicio de nombre de NetBIOS corre sobre TCP y UDP puerto 137, el servicio de datagrama escucha en puerto de UDP 138 y el servicio de sesión escucha en puerto de TCP 139. Todo el

recurso de SMB que divide las aplicaciones usará puerto de TCP y UDP 445 , y puertos 137,138 y 139 se pueda cortafuego.

NetBIOS se puede inhabilitarse sólo efectivamente si recursos todo partidos en la red de cliente corren sobre a Windows 2000 o posterior.
Vea artículo 299977 de base de conocimiento de Microsoft para los artículos adicionales para considerar al inhabilitar NetBIOS. También vea artículo 315267 de base de conocimiento para la información sobre cómo inhabilitar NetBIOS en Windows XP.

Warning: Inhabilitar NetBIOS no es sustentado por Microsoft y pueda resultar en la pérdida de la funcionalidad y el comportamiento de sistema inestable/impredecible. El comprobación apropiado debe ser conducido en los sistemas de no-producción para determinar el impacto de inhabilitar NetBIOS en sus sistemas/redes.

Habilite el cortafuego de Windows en todos los dispositivos de red.

Por lo general, el cortafuego de Windows es disponible sólo cuando es unido directamente a la Internet, pero no para las conexiones de red de área local (LAN). El cortafuego se habilita también en conexión en Internet en línea y conexión en Internet divididas.

Cuando habilite, el cortafuego de Windows bloquea el tráfico por llegar a su puesto de trabajo a menos que un puerto se abre explícitamente. El cortafuego de Windows típicamente no es necesario en las redes internas donde un cortafuego ya existe entre el cliente y la red untrusted. El cortafuego de Windows también soporta tala de actividad.

Para más información sobre el cortafuego de Windows en Windows XP, vea artículo 320855 de base de conocimiento de Microsoft.

Grupos limitados

Con los grupos limitados habilite, el sistema operativo evaluará la calidad de miembro de grupo local en la bota y cuando agrupe la política se refresca. Miembros en la política de "grupos limitados" son comparados contra la corriente real agrupe calidad de miembro. Si las cuentas listadas en la política no están en el grupo, se suman. Viceversa, si una cuenta está en el grupo pero no en la política, se quita.

Usuarios para escritorio remotos

Use esta política para explícitamente controlar que los usuarios son permitidos para usar el servicio para buró remoto (servicios terminales).

Permisos de archivos y entradas del Registro

Una vez que un volumen ha sido convierta a NTFS, y una vez las colocaciones básicas de seguridad de archivo han sido aplicadas, adicional colocaciones se deben aplicarse. La mayor parte del conozca sistema operativo y proezas de aplicación existen debido a los factores múltiples. En primer lugar, allí está una aplicación que tiene un defecto que abre una puerta privilegiada baja en un sistema operativo. Y secundar, que libre acceso permite un intruso inteligente para elevar su privilegio y hacerse cargo del sistema. Los permisos listaron debajo de ayudar para hacer un sistema operativo "resistente" para privilegiar la elevación, aún a las vulnerabilidades de software potenciales que han todavía no sido hallado.

ADVERTENCIA: Es posible que los permisos aplicados aquí pueden quitar cierto en cierta medida la funcionalidad de aplicación que está acostumbrado a. Si que suceda y usted necesita retroceder fuera para un estado previamente conocido, usan las mismas instrucciones que estuvieron acostumbrado a aplicar los permisos básicos para un sistema de archivos de NTFS frescamente convertido para "desatar" la mayor parte de las colocaciones que usted ve abajo.

Plantillas administrativas

Sistema

Llamada de procedimiento remoto

El modelo de medidas de seguridad de llamada de procedimiento remoto (RPC) ha sido mejorado para Windows XP atienda paquete 2. RPC está acostumbrado a publicar servicios en los puertos de TCP no estándar. un cliente localiza servicios uniendo al |mapper| de |endpoint| de RPC (que corra sobre un puerto estándar) e inquiriendo el servidor para un servicio específico.

Service Pack 2 permite al administrador para requerir autenticación para conectar el |mapper| de |endpoint|. Adicionalmente, el administrador puede especificar las necesidades de autenticación globales que deben ser acercadas antes de unirse a cada servicio de RPC.

Importante: El enlace de herencia de NetSchedule usa RPC para comunicarse con el servicio de programador este enlace se usa más comúnmente por AT.EXE u otra herencia fijando la hora de aplicaciones, y no soporte autenticación. *AT.EXE no trabaje cuando la autenticación de RPC es requerida completamente político.*

La autenticación de RPC EnpointMapperClient(Sólo SP2)

En defecto en Service Pack 2 , el |mapper| de |endpoint| de RPC no puede accederse por los clientes anónimos. Ello puede necesario poner que esto para "incapacitado" para las aplicaciones RPC que no soporta autenticación.

Restricciones para los clientes de RPC no legalizado (Sólo SP2)

En defecto en Service Pack 2 , todos los servicios de RPC requieren autenticación a fin de unir, y todo anónimo llamadas se rechazan. La autenticación puede ser incapacitada por político.

Ciertas aplicaciones pudieron ser escritas para invocar explícitamente los |callbacks| de RPC sin autenticación, y desvían estas nuevas restricciones (el RPC_SI_PERMITA_CALLBACKS_CON_NINGÚN_AUTH).

Esta es una nueva opción, y no se aplica a las aplicaciones de herencia. En defecto, aplicaciones registrado desvie por este camino la autenticación aún cuando las "restricciones para los clientes de RPC no legalizado" son habilitadas. Sin embargo el administrador puede optar por requerir que uniforme estos servicios para autenticarse usando la colocación " autentique sin excepciones."

Red

Windows Firewall

Windows XP Service Pack 2 contiene los mejoramientos significativos al cortafuego de Windows. El cortafuego soporta manejo remoto, y un conjunto ancho de las opciones de configuración por la política de grupo.

El cortafuego de Windows bloquea el tráfico por llegar sólo. Si no fuera por ICMP trafique, ninguna configuración u opciones de filtro es suministrado para los paquete pequeño en viaje de ida predominantes.

El apoyo de IPv6 es incluido en el cortafuego de Windows en defecto.

Note que el cortafuego de Windows puede derrotar la operación remota de muchos manejo de Microsoft consuele (MMC) mordisque sin hacer presa-en, incluyendo manejo de computadora, manejo de disco, espectador de evento, el conjunto resultante de la política, atienden, y muchos otros. Para mayor información, vea artículo 840634 de Microsoft Knowledgebase, http://support.microsoft.com/default.aspx?scid=kb;el ene-nos;840634.

ADVERTENCIA: Colocaciones de cortafuego, aún más de la mayor parte de otras colocaciones de seguridad en esta guía, deba ser hecho a la medida a su sitio. El comprobación es crítico antes de desplegar una configuración de cortafuego para su sitio. Las colocaciones de cortafuego impropias pudieron bloquear las aplicaciones críticas tales como agentes de manejo contra virus o para buró. En ciertos casos, las colocaciones de cortafuego impropias pudieron aún bloquear directorio activo y el manejo político del grupo de la máquina, dejando ninguna vía con facilidad hacer cambios.

Perfil de Dominio

El cortafuego soporta dos perfiles separados. El perfil de campo se aplica sólo a computadoras que se une a un campo, y no tenga ningún efecto en las máquinas de trabajo en grupo. Cuando una computadora de campo es unida a la red corporativa, típicamente una política menos estricta se puede aplicarse.

Protege todas las conexiones de red (Sólo SP2)

En defecto, todos los enlaces de red son protegidos por el servicio de cortafuego de Windows. Si esta colocación está incapacitada, la colocación especificó en la plantilla administrativa Network\Network uso Connections\Prohibit de cortafuego de conexión en Internet " surta efecto.

No permite excepciones (Sólo SP2)

La política de cortafuego da al administrador control muy bien áspero sobre permitir y prohibir tráfico de red. Sin embargo, cuando " no permita las excepciones " habilite se, el cortafuego bloquea trafique todo, e ignoran las excepciones definidas abajo.

Permite las excepciones de programa locales

Cuando un programa es definido como una excepción, puede recibir el tráfico de red no solicitado en cualquier puerto pide el cortafuego para abrir. Windows soporta dos programe las listas de excepción: un defina en política de grupo, y otro defina localmente por el tablero de control de la máquina.

Habilitar esta colocación permite que el administrador de sistema especifique programas que pueden recibir tráfico de red entrante, y desvian las restricciones de cortafuego de Windows.

Permite la excepción de administración remota

En un entorno corporativo, varios sistemas pueden estar acostumbrado a inquirir y manejar puestos de trabajo. Estos sistemas podrían conectar remotamente el registro a parche leído información, conecta el sistema de archivos para recuperar diarios, o usar la instrumentación (WMI) de manejo de Windows para leer varios parámetros de sistema.
Cuando la administración remota es habilitado, el servicio de cortafuego de Windows abre puertos de TCP 135 y 445. Ello permite también SVCHOST.EXE y LSASS.EXE para recibir el tráfico entrante en los puertos dinámicos.

Esta colocación puede ser abierta a todos los anfitriones, al subred de comunicación local, o a un IP específico dirija rango.

Permite archivo y el impresor que divide la excepción (Sólo SP2)

Para un puesto de trabajo para compartir archivos o localmente unir impresores, esta colocación se debe habilitar. Esto no necesita habilitarse para el cliente para conectar archivos en otra máquina, o para acceder un impresor remoto.

Cuando habilite, esta colocación permite el tráfico por llegar en puertos de UDP 137 y 138 , y puertos de TCP 139 y 445.

Permite las excepciones de ICMP (Sólo SP2)

Protocolo de Internet Control Message (ICMP) el tráfico está acostumbrado a responder a los problemas de red no pasajeros. el tráfico de ICMP difiere de TCP y UDP trafique, y está usado primariamente para maneje la red mismo, y no para enviar datos de aplicación. Sin embargo, las aplicaciones maliciosas han sido conocidas para usar ICMP trafique como un canal de datos.

Los cortafuego de ventanas proporcionan el control granular sobre exactamente que los mensajes ICMP se aceptan y envian. Para más información en mensajes ICMP específicos, refiera a RFC 792, " protocolo de mensaje de control de Internet."

Permite la excepción remota para buró (Sólo SP2)

El protocolo para buró remoto da a un acceso completo remoto de administrador al enlace gráfico del puesto de trabajo. Puede haber terminado una sesión separada, o pueden compartir la sesión con un usuario de entrada en el sistema. Esta característica es a menudo útil para localizar, y se usa por el servicio remoto de asistencia.

Cuando el buró remoto es permitido, el cortafuego de Windows permite las conexiones por llegar en puerto 3389. Como otras colocaciones de red, esto se puede otorgar todos los usuarios, al subred de comunicación local, o a un subred de comunicación de IP específico.

Permite la excepción de marco de UPnP(Sólo SP2)

Cuando se habilita el juego (UPnP) de n de enchufe universal, la computadora puede recibir PnP no solicitado envian mensajes. Por habilitar esta política, usted abre puerto de TCP 2869 y puerto de UDP 1900 en el cortafuego de Windows.

Prohibe notificaciones

Típicamente, cuando unos intentos de aplicación para hacer accesible un puerto de red para estar atento a tráfico no solicitado, el usuario se notifica, y da la opción de sea permitir este comportamiento o no. Si esta opción es incapacitada por política, la exhibición es prohibida y la conexión es bloqueada.

Si esta política no es configurada, un administrador puede acceder el cortafuego de Windows por el tablero de control y habilite esta notificación.

Registre paquetes pequeños caídos o perdidos ((Sólo SP2)

Cuando se habilita la tala, el cortafuego de Windows escribe la información sobre el conexión de red a un archivo de tronco. El tamaño del archivo es controlado por político. A la opción de la tala toda información de conexión, o información justa sobre las conexiones caídas.

Prohíbe respuesta de |unicast| a |multicast| o emisión (Sólo SP2)

A menudo el tráfico se puede enviar a una dirección difundida. Los anfitriones pueden optar por responder a tráfico difundido; si es así, una emisión entrante sencilla paquete pequeño puede generar un gran número de paquete pequeño de réplica de |unicast| al remitente. Esto puede resultar en un ataque de negación de servicio.
Configure esta colocación para inhabilitar respuestas a |multicast| o los paquete pequeño difundidos.

Si la red de |muticast| es soportada en su entorno, esta colocación se debe habilitar.

Define las excepciones portuarias (Sólo SP2)

Puede optar por abrir los puertos específicos para su entorno de campo entero. Por ejemplo, su contra virus o remiende los agentes de manejo pueden estar atento a las conexiones entrantes en un puerto específico. Si es así, puede configurar todos los clientes para dejar este puerto abra por la política de grupo definiendo lo como una excepción portuaria.

Permite las excepciones de puerto locales (Sólo SP2)

Las excepciones portuarias pueden hacerse también en una base por máquina. Si esta colocación se habilita, un administrador puede abrir los puertos específicos (e.g., HTTP en portuario 80) para las máquinas específicas individuales por el cortafuego de Windows tome forma en el tablero de control.

Perfil estándar

El cortafuego de Windows también usa un perfil de "norma" , que ofrece mismas colocaciones como el perfil de campo. Sin embargo, el perfil estandar es aplicado a los puestos de trabajo de campo cuando un controlador de campo no es disponible. Esto se vuelve particularmente útil para los ordenadores portátiles pequeños corporativos, y permita que el administrador imponga una norma de actuación sobre seguridad de stricte cuando el dispositivo es unido a una red no asegurada.

Las computadoras que son miembros de un trabajo en grupo (no una a un campo) siempre use el perfil estándar.

Advertencia: El cortafuego de "perfil estandar" toma forma defina en esta guía asuma que la computadora pertenece a un campo. **Estas colocaciones son probablemente no aproprie de para una oficina pequeña, las casa matriz o máquina de trabajo en grupo. También no pueden ser apropiados para las corporaciones grandes con máquinas que se mueven regularmente entre los campos**. Más bien, son diseñados para proteger un dispositivo tal como un ordenador portátil pequeño móvil que se va la red corporativa fiable y en una red pública untrusted. El perfil estandar esbozado en esta política protegerá la computadora cuando está en la red untrusted.

Componentes de Windows

Centro de seguridad

Encienda la seguridad central (Sólo PC de dominio)(Sólo SP2)

El centro de seguridad es útil para mostrar el alarmas significativas al usuario. En defecto, el centro de seguridad es habilitado, y altere el usuario cuando la computadora tiene un degradado la seguridad pose. La seguridad centra los monitores tres artículos críticos:

- El software contra virus está corriendo, y firmas son al día. Esta característica se puede inhabilitar por poner el registro teclee HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusDisableNotify a 1.
- Los cortafuego de ventanas están corriendo. Esta característica se puede inhabilitar por poner el registro teclee HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify a 1.
- El servicio de actualización de Windows está corriendo, y todo las actualizaciones han sido aplicadas.

Esta característica se puede inhabilitar por poner el registro teclee HKLM\SOFTWARE\Microsoft\Security Center\UpdatesDisableNotify a 1.

CAPÍTULO V

RESULTADOS

Los resultados que se esperan con la implementación de este proyecto de investigación son las siguientes:

Resolver los problemas de seguridad en los sistemas operativos Microsoft, mediante la utilización de Hardening en el Ministerio de Trasporte y Obras Públicas del Ecuador o en otra entidad. Los usuarios tenían intrusiones en sus maquinas de hasta un 70% al año de tipo interna Figura 6. Ahora se considera una intrusión sólo cuando es de tipo virus Figura 7.

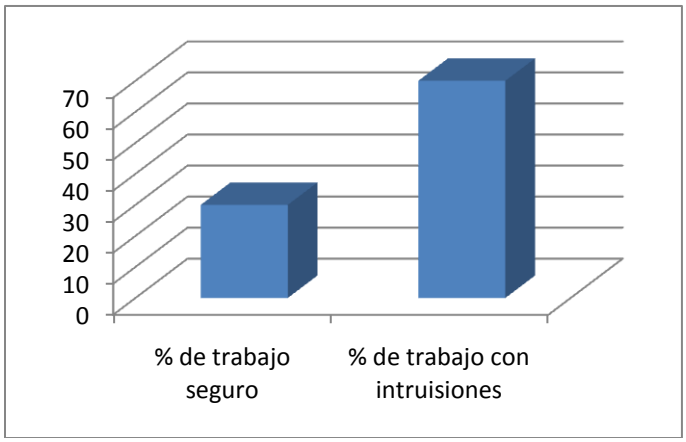


Figura 5.1: "Porcentaje de trabajo sin medidas de seguridad"

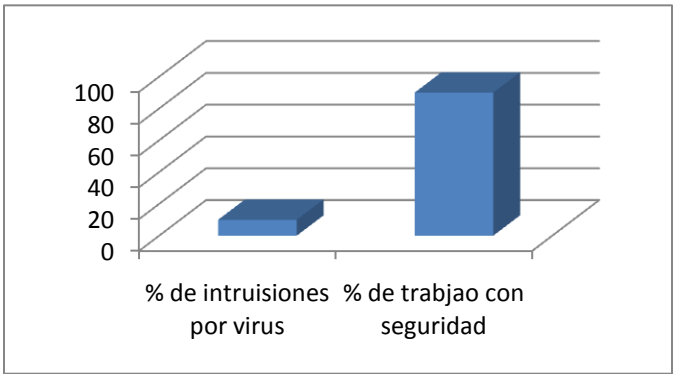


Figura 5.2: "Porcentaje de trabajo con medidas de seguridad Hardening"

Realizar pruebas sobre sistemas operativos Microsoft para determinar sus vulnerabilidades, a través del uso de herramientas (software) de testeo. Los administradores de los sistemas y redes hacían un escaneo de los mismos sólo en un 10% Figura 8. Las áreas de vulnerabilidad de los sistemas con sus respectivas acciones y afectaciones los mismos que los administradores del sistema no protegían sus sistemas en el área de software.

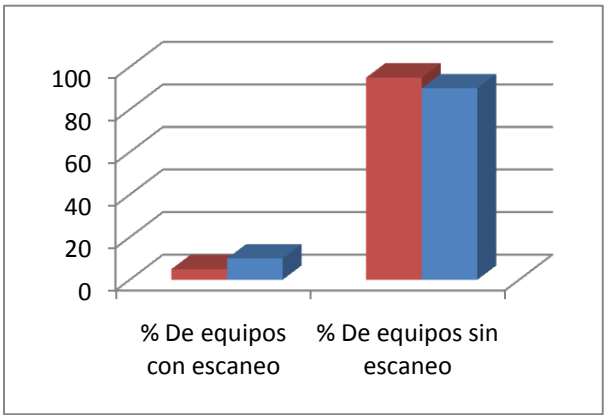


Figura 5.3: "Porcentaje de escaneo de vulnerabilidades"

Elaborar un manual de Hardening que permita al usuario configurar su sistema operativo, para contrarrestar las áreas e vulnerabilidad ha hecho que los administradores de red ahorren hasta un 90% de tiempo en la protección de cada uno de los equipos figura 9.

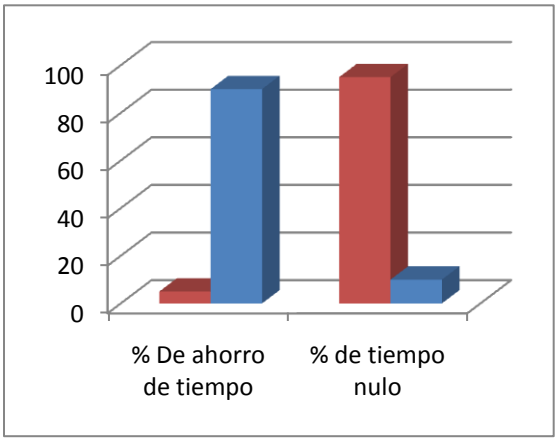


Figura 5.4: "Porcentaje de ahorro de tiempo en la protección de equipos informáticos"

Elaborar e implementar archivos de tipo registro estándar con configuración de Hardening, para uso en equipos de similares características con sistemas operativos iguales ha logrado que el 95% de los equipos adopten esta medida de seguridad (figura 11) para protección de su información.

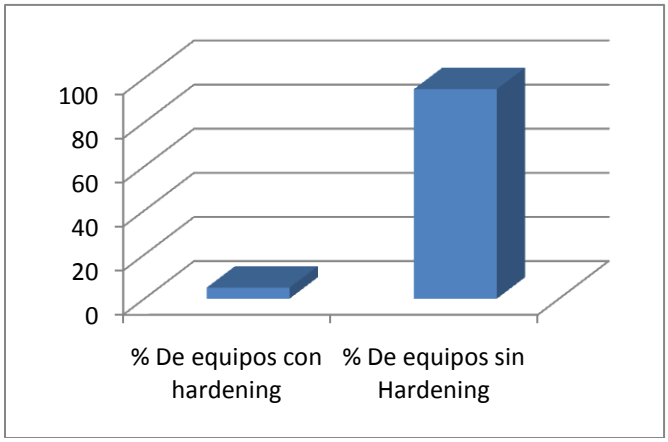


Figura 5.5: "Porcentaje de trabajo sin medidas de seguridad"

Manual de Aplicación Hardening

Tareas a realizar:

1. Aplicación de la herramienta Tester
2. Escaneo de vulnerabilidades mediante la herramienta NG
3. Obtención de resultados
4. Corrección de vulnerabilidades
    a. Aplicación Hardening
        i. Aplicación por código
        ii. Aplicación Manual
        iii. Aplicación por actualización
5. Resultados

1. Aplicación de la herramienta Tester

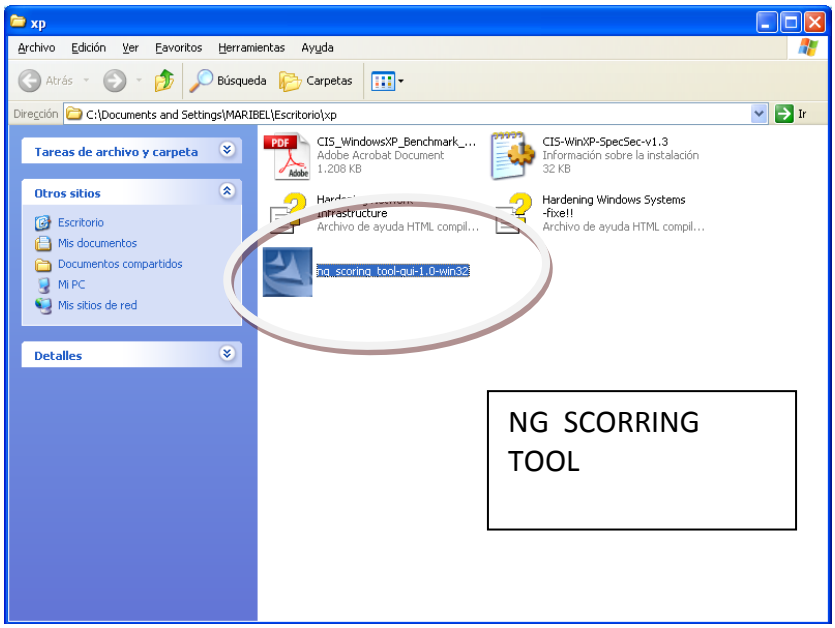


Figura 5.6: Aplicación de la herramienta Tester

La ejecución de la herramienta tester que parte desde el proceso de la instalación, hasta el proceso de ejecución del mismo en el sistema del Computador para el cual se va a evaluar su seguridad, lo cual dependerá del tipo de sistema que usa para la selección de la herramienta, la ayuda de instalación se puede encontrar en ANEXO A.

2. Escaneo de vulnerabilidades mediante la herramienta NG

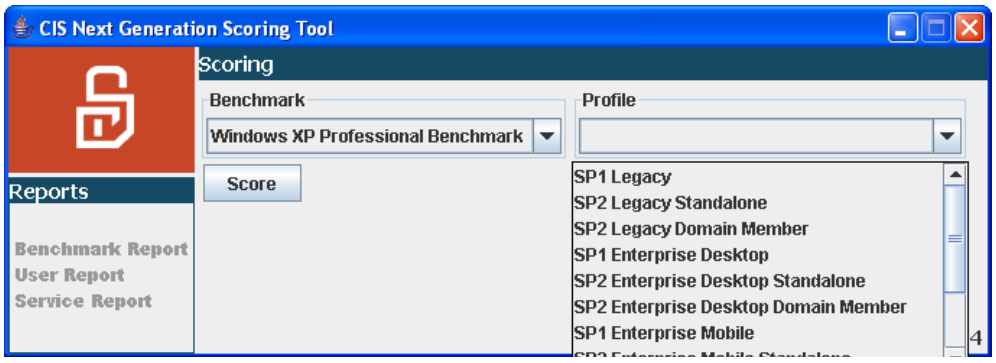


Figura 5.7: Escaneo de vulnerabilidades mediante la herramienta NG

Dependiendo del Sistema operativo en el cual se instala y se va a evaluar posteriormente se selecciona las características del mismo según indica la herramienta para lo cual se determinan las características de acuerdo a la siguiente tabla (fig. a).

La selección debe ser necesariamente aplicada a una de las que ofrece la herramienta ya que sin esto no se puede continuar con el análisis y podría mostrarle errores que impiden la continuación del escaneo (fig. b).

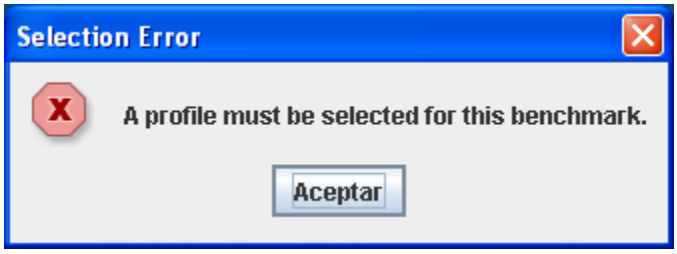


Figura 5.8: Selección del Sistema Operativo y el tipo de Equipo es necesario.

En caso de no contar con la información requerida sobre sistema operativo puede recurrir a esta información con las siguientes instrucciones:

Seleccionamos:

→ INICIO

→ EJECUTAR y escribimos el comando

→ DXDIAG(fig c.)

→ ENTER.

El cual sirve no sólo para ver estas caracteristicas sino tambien, los controladores de Windows, Memoria y en si todos los dispositivos instalados (fig. d).

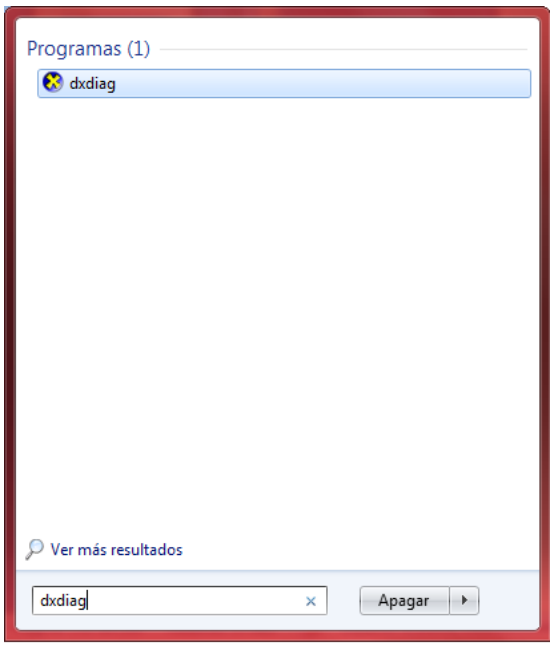


Figura 5.9: Comando que muestra información del sistema

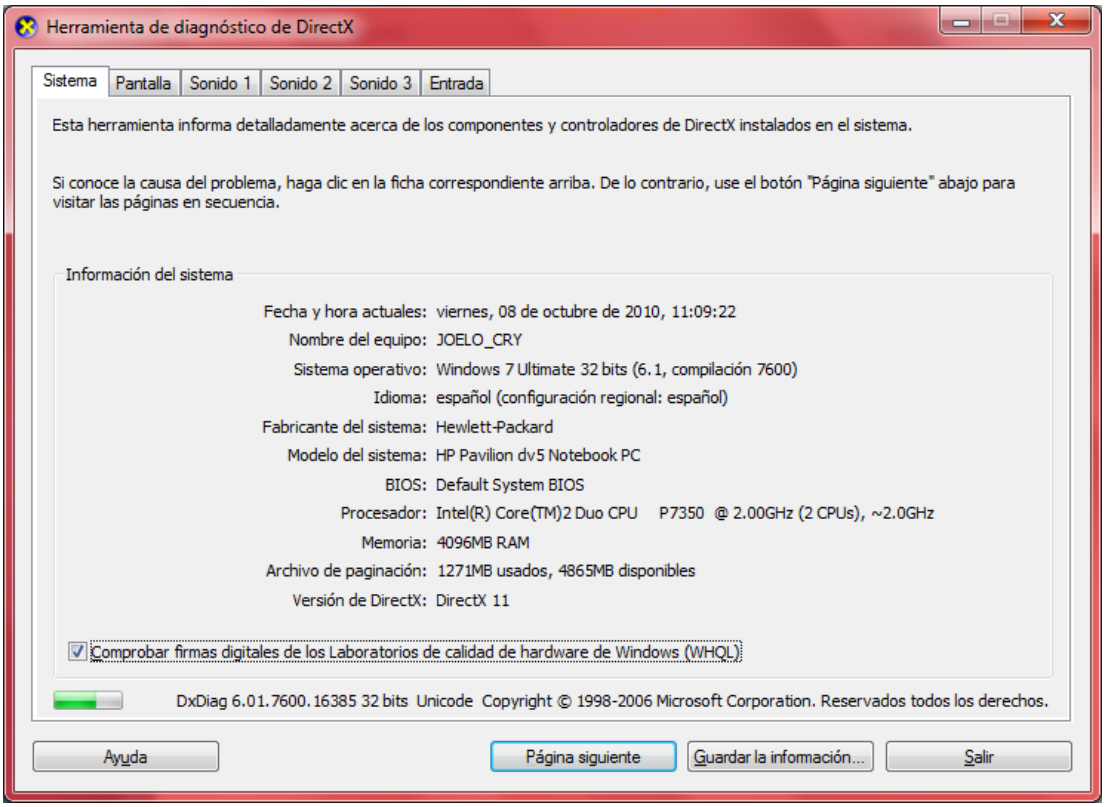


Figura 5.10. Información del Sistema y Equipo

Tabla 5.1: Selección del Sistema según su trabajo y ubicación. De acuerdo a los Niveles de Seguridad de Hardening Capitulo II Vulnerabilidad.

TIPO DE SELECCIÓN SEGUN LA UBICACIÓN DE LA MÁQUINA O TRABAJO QUE REALIZA	
LEGACY	Home
ENTERPRISE DESKTOP	Computadora de escritorio en la empresa
ENTERPRISE MOBILE	Computador portátil en la empresa
SPECIALIZED SECURITY LIMITED FUNCIONALITY	Seguridad especializada - La funcionalidad limitada

Otra manera de ver la información que necesitamos es a través de MI PC haciendo clic derecho sobre el mismo y luego en →PROPIEDADES, lo cual le desplegara este tipo de información (fig. e).

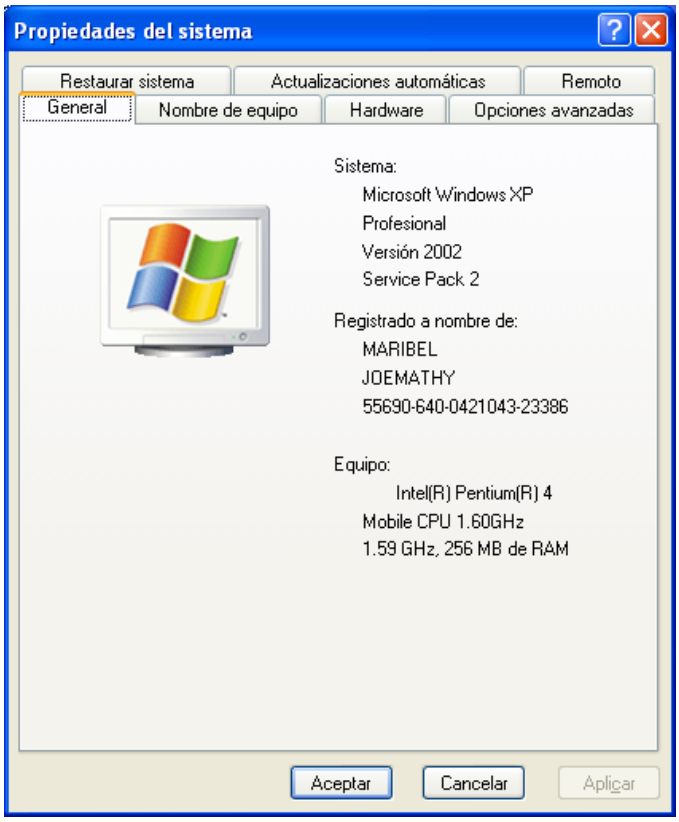
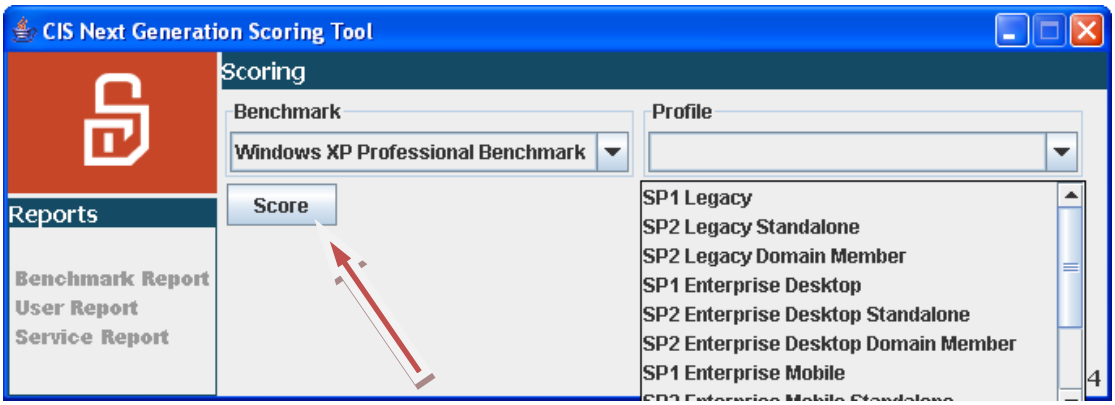


Figura 5.11: Propiedades del Sistema - Visualización de características de Sistema Operativo y Service Pack instalado.

Después de completar esta información requerida, hacemos clic en → SCORE



Después esto y haber seleccionado todo lo solicitado nos presentara una tabla en la cual se deberá necesariamente llenar la información (fig. f). Para lo cual nos da tres tipos de opciones Si – No – Desconoce.

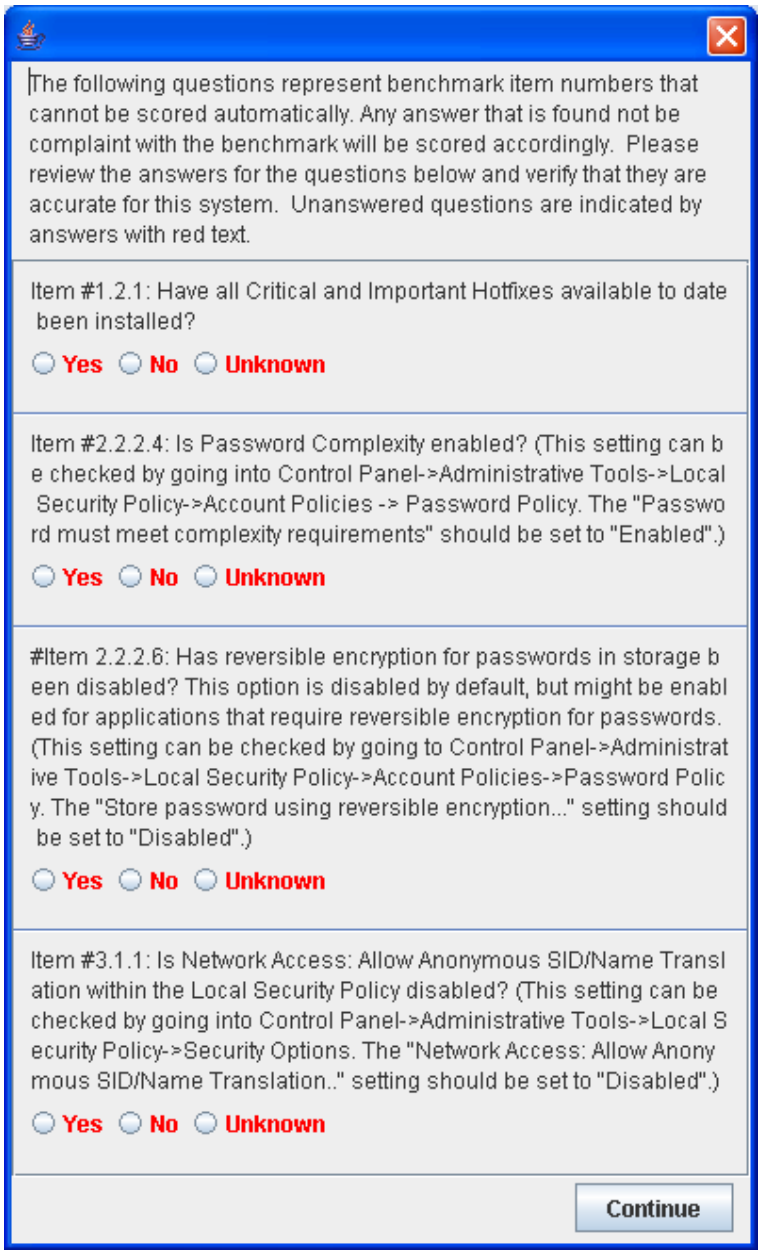


Figura 5.12: Análisis de estado del equipo a través de la herramienta de escaneo mediante encuesta de situaciones.

La Efectividad de esta encuesta dependerá de repuestas Asertivas, es decir, Si es afirmativo o negativo pero no desconocido.

La repuestas afirmativas deben ser 100% positivas, es decir que, si algún detalle de la pregunta no cumple con su sistema y sus características simplemente es NO.

Para el control de no poner desconocido a continuación se aclaran las preguntas y su forma de localizar en su sistema dicha información:

PREGUNTAS

Las siguientes preguntas representan un punto de referencia, estos ítems no pueden ser calificados por el software automáticamente ya que algunas de estas respuestas no se encuentran con el software y no pueden ser calificadas correctamente, Para lo cual se pide de favor revisar las respuestas para las preguntas de abajo y verificar que su respuesta sea precisa para el sistema en uso. No deje sin responder las preguntas con texto en rojo.

Pregunta #1.2.1: Tiene todos los Hotfixes Críticos e Importantes disponibles e instalados a la fecha en su Computador.

La forma de visualizar dicha información es ingresando de la siguiente forma:

→ INICIO

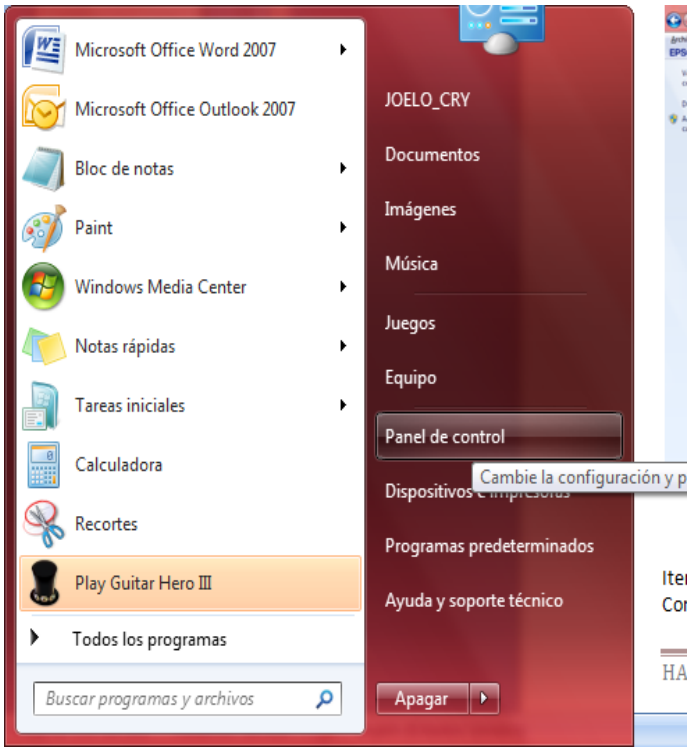
→ PANEL DE CONTROL

→ SISTEMA Y SEGURIDAD (fig. g).

→ WINDOWS UPDATES (fig. h)

→ ULTIMAS ACTUALIZACIONES (fig i).

Ahí encontrara todas las actualizaciones hasta la última que deberá ser la lanzada por Microsoft a la fecha.



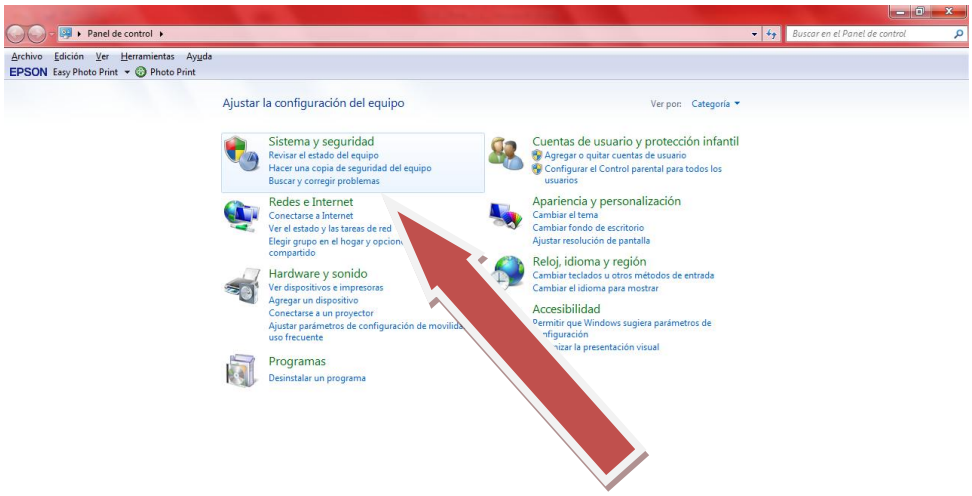


Figura 5.13: Sistema y seguridad

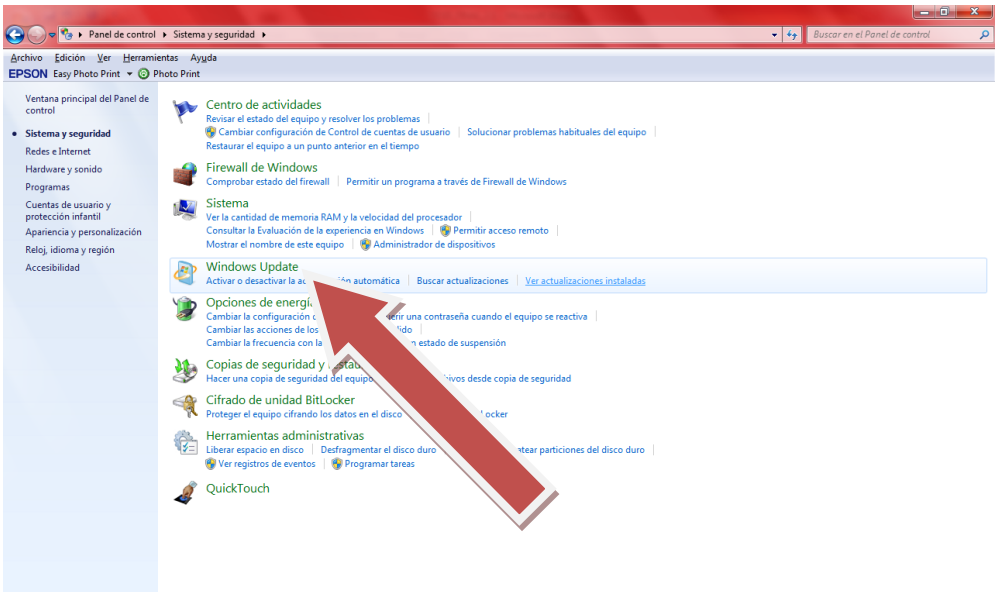


Figura 5.14: Windows updates.

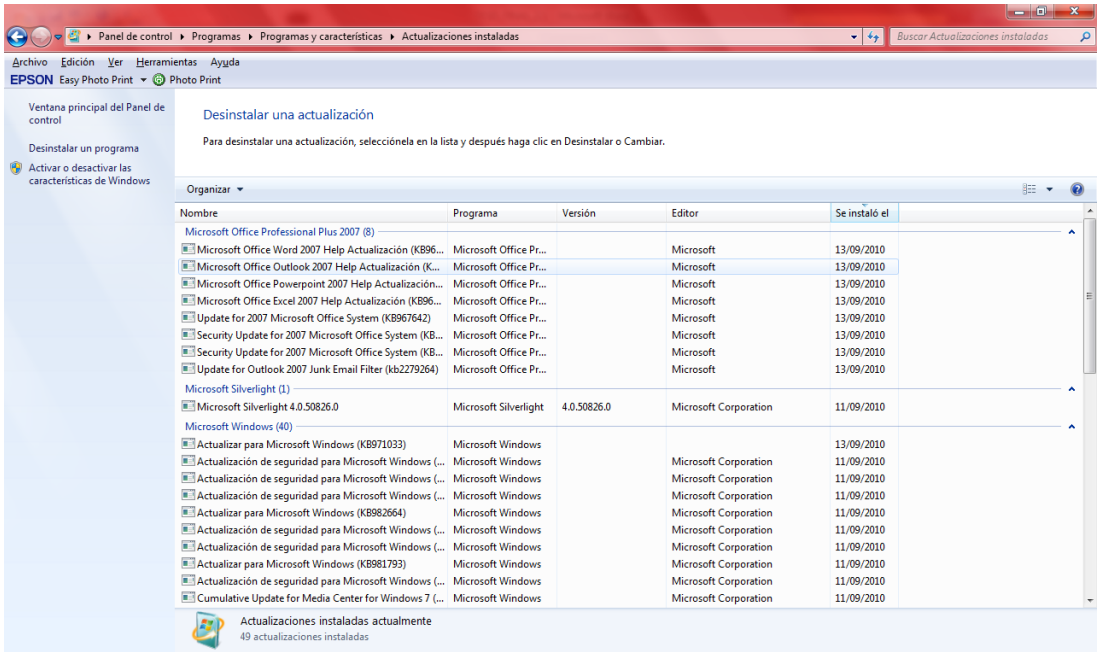


Figura 5.15: Listado de actualizaciones y Hotfix de Windows

Pregunta #2.2.2.4: La complejidad de Password está habilitada.

Esta configuración puede ser revisada por:

→ PANEL DE CONTROL

→ HERRAMIENTAS ADMINISTRATIVAS

→ POLITICAS DE SEGURIDAD LOCAL

→ POLITICAS DE CUENTA

→ DIRECTIVA DE CONTRASEÑÁS – CONTRASEÑAS

La complejidad de contaseñas debe estar en posición de habilitado (fig. j).

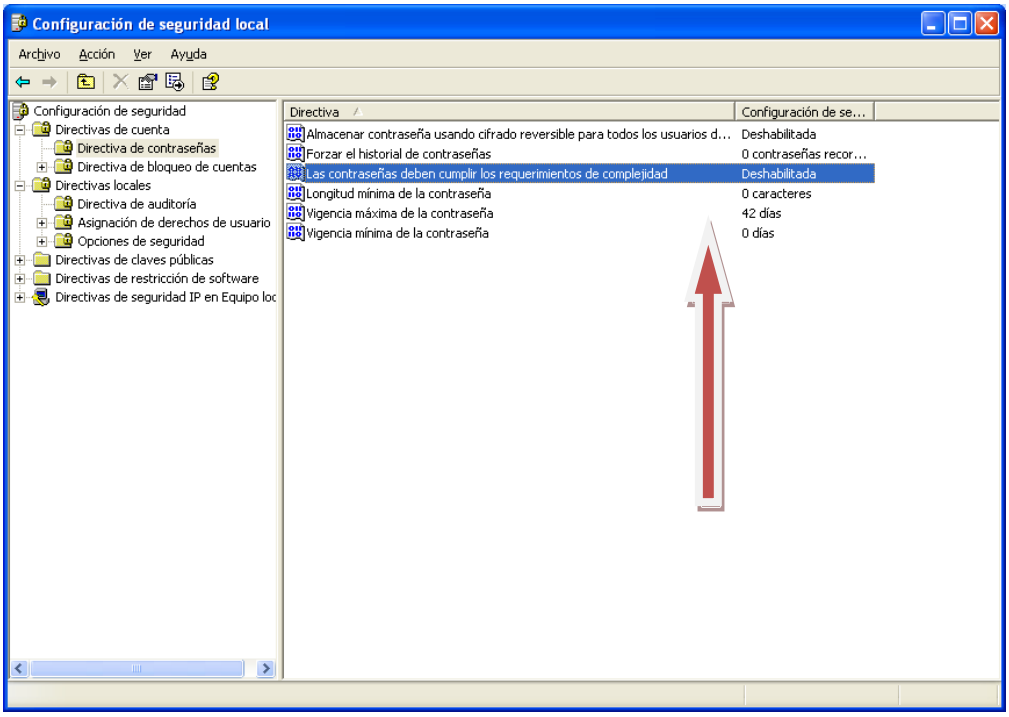


Figura 5.16: Configuración de seguridad local - Complejidad de contraseñas

Pregunta #2.2.2.6: ¿Tiene la opción almacenar contraseñas con cifrado reversible deshabilitada? Esta opción esta deshabilitada por defecto, pero podría ser habilitada por aplicaciones que requieren cifrado reversible de contraseñas.

Esta configuración puede ser revisada por:

→ PANEL DE CONTROL

→ HERRAMIENTAS ADMINISTRATIVAS

→ POLITICAS DE SEGURIDAD LOCAL

→ POLITICAS DE CUENTA

→ DIRECTIVA DE CONTRASEÑAS → almacenar contraseñas con cifrado reversible (fig. k).

Esta opción debería estar configurada en “Deshabilitada”.

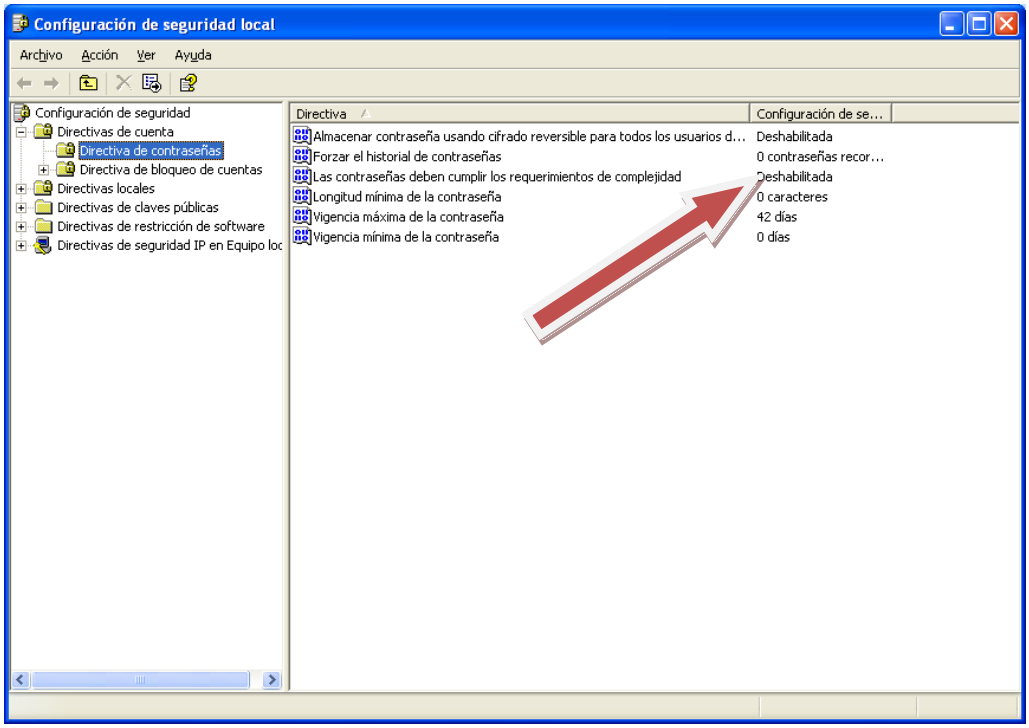


Figura 5.17: Contraseña con cifrado reversible.

Pregunta #3.1.1: ¿Acceso a redes: Permitir Traducción de SID/NOMBRE anónima está como deshabilitado?

Esta configuración puede ser revisada por:

→ PANEL DE CONTROL

→ HERRAMIENTAS ADMINISTRATIVAS

→ POLITICAS DE SEGURIDAD LOCAL

→ DIRECTIVAS LOCALES

→ OPCIONES DE SEGURIDAD → Acceso a redes: Permitir Traducción de SID/NOMBRE anónima (fig. L).

Esta opción debería estar configurada en “Deshabilitada”.

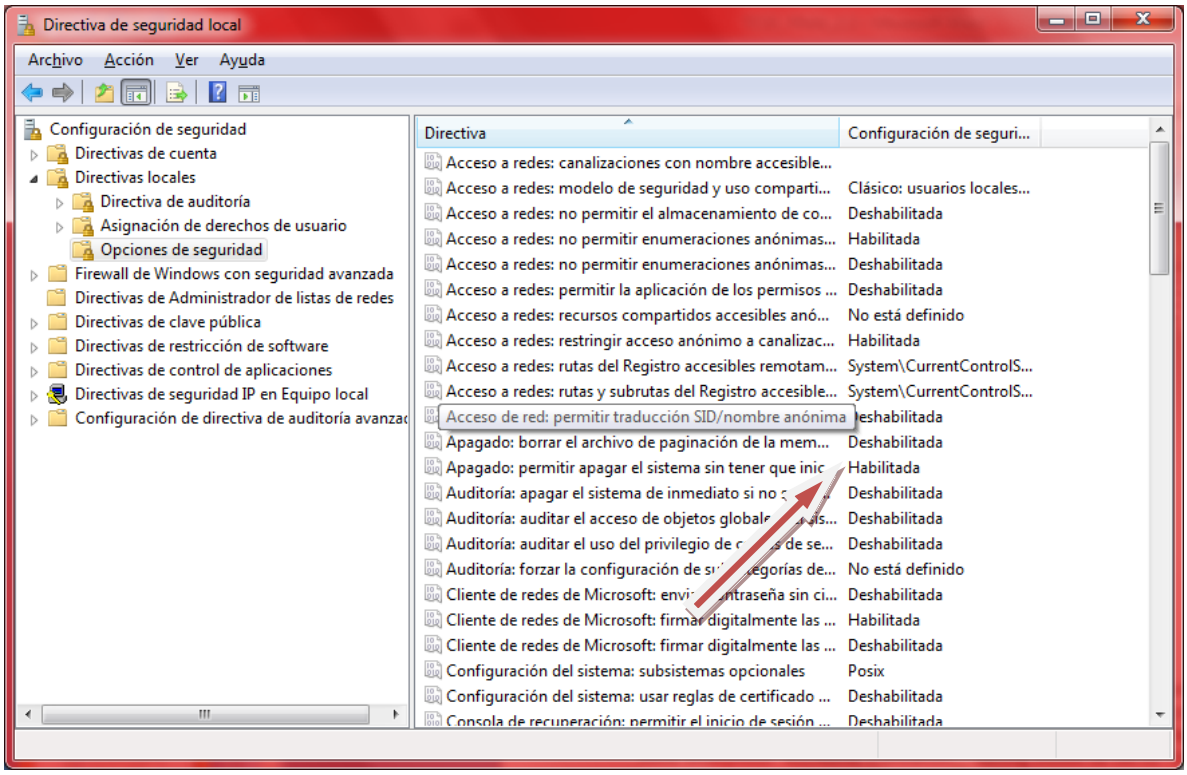


Figura 5.18: Directivas de seguridad local – Acceso a redes

Una vez que se ha terminado de llenar dicho cuestionario el software de Testeo le presentara un mensaje (fig. m) de finalización de tarea.

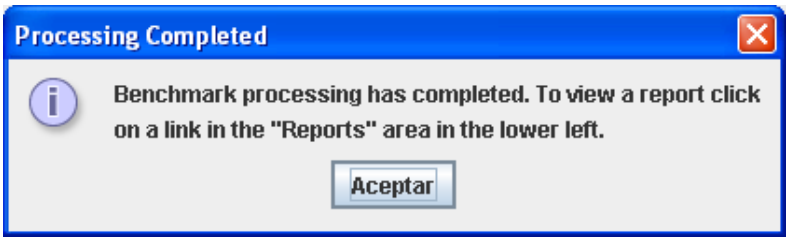
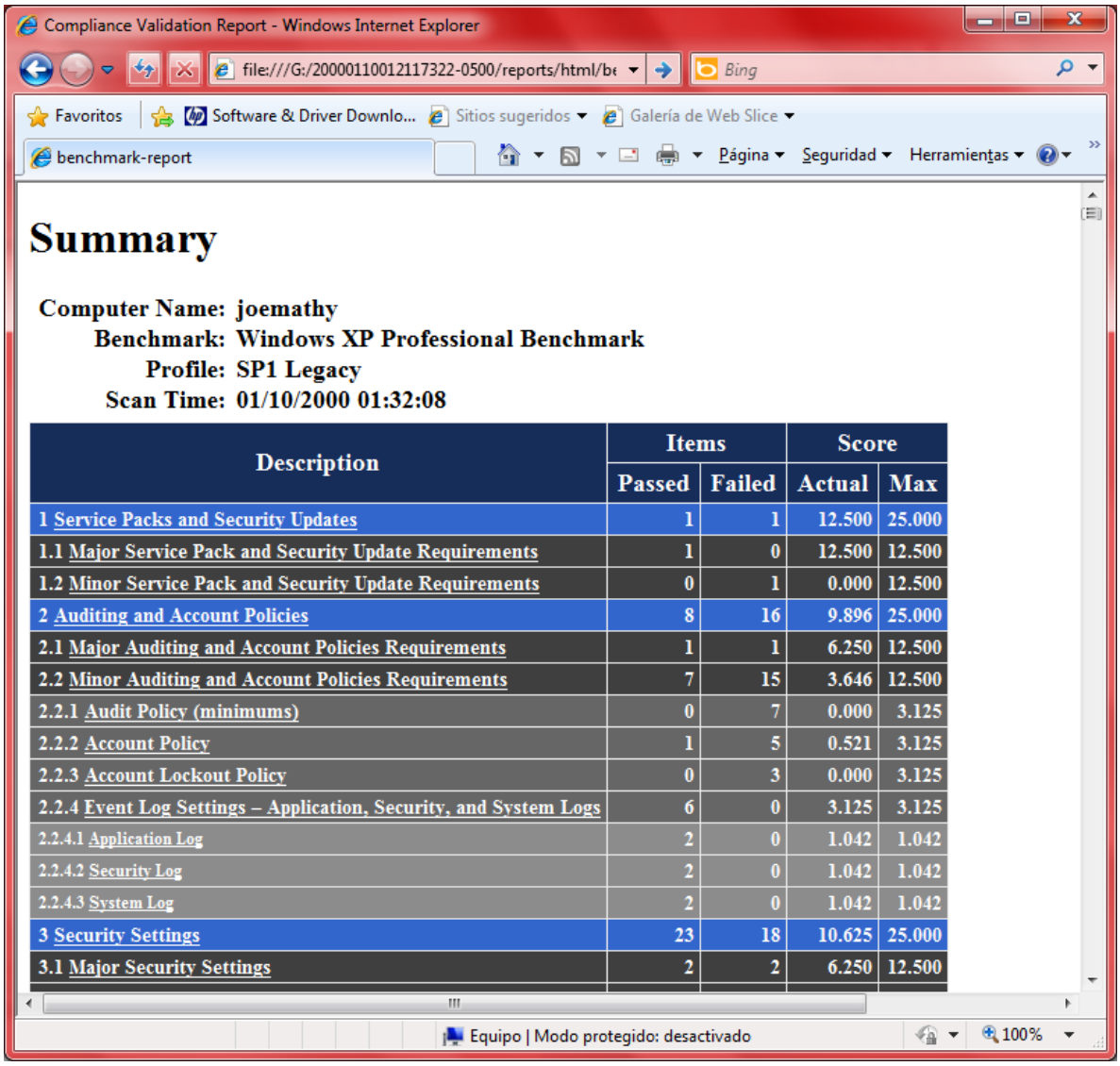


Figura 5.19: Finalización de tarea de escaneo de vulnerabilidades.

Los resultados obtenidos serán analizados a través de una tabla (fig. n) donde se muestran las deficiencias sobre seguridad determinando así las áreas de vulnerabilidad.

Dicho reporte se presenta en un formato que puede ser visualizado mediante el browser.



Description	Items		Score	
	Passed	Failed	Actual	Max
1 Service Packs and Security Updates	1	1	12.500	25.000
1.1 Major Service Pack and Security Update Requirements	1	0	12.500	12.500
1.2 Minor Service Pack and Security Update Requirements	0	1	0.000	12.500
2 Auditing and Account Policies	8	16	9.896	25.000
2.1 Major Auditing and Account Policies Requirements	1	1	6.250	12.500
2.2 Minor Auditing and Account Policies Requirements	7	15	3.646	12.500
2.2.1 Audit Policy (minimums)	0	7	0.000	3.125
2.2.2 Account Policy	1	5	0.521	3.125
2.2.3 Account Lockout Policy	0	3	0.000	3.125
2.2.4 Event Log Settings – Application, Security, and System Logs	6	0	3.125	3.125
2.2.4.1 Application Log	2	0	1.042	1.042
2.2.4.2 Security Log	2	0	1.042	1.042
2.2.4.3 System Log	2	0	1.042	1.042
3 Security Settings	23	18	10.625	25.000
3.1 Major Security Settings	2	2	6.250	12.500

Figura 5.20: Tabla – Reporte de resultados de escaneo.

El Reporte de vulnerabilidades muestra sus deficiencias y fortalezas y al hacer clic sobre alguna muestra en forma directa cual es la falla (fig. o). Y ya con esto sólo dependerá del usuario para realizar su configuración para su mejora.

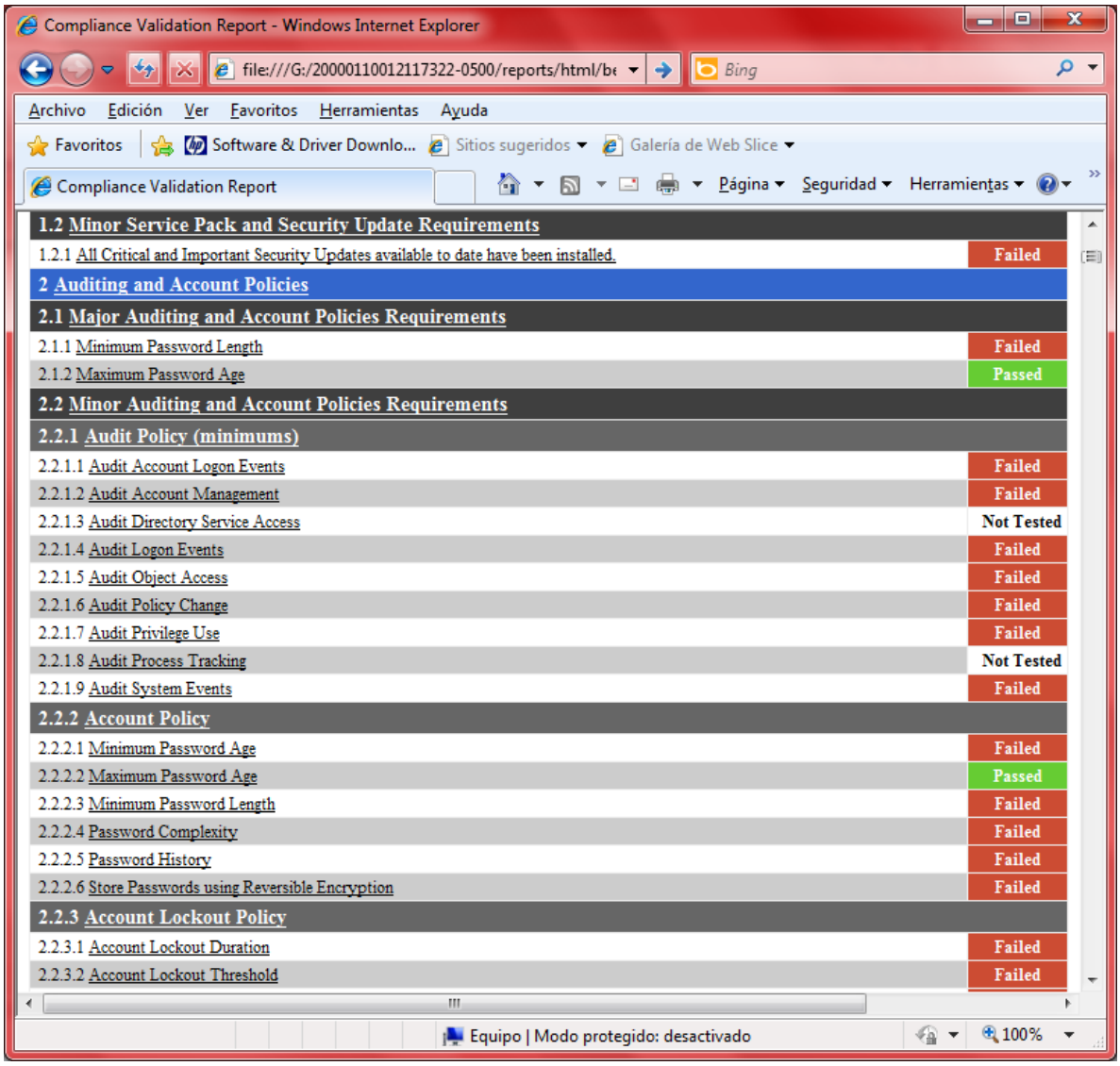
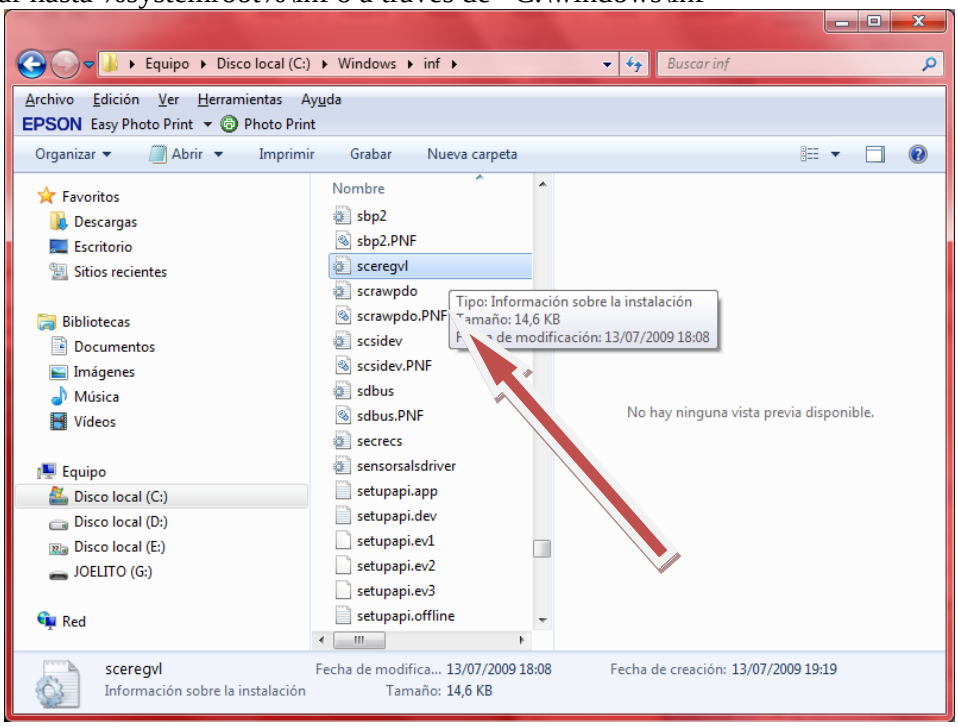


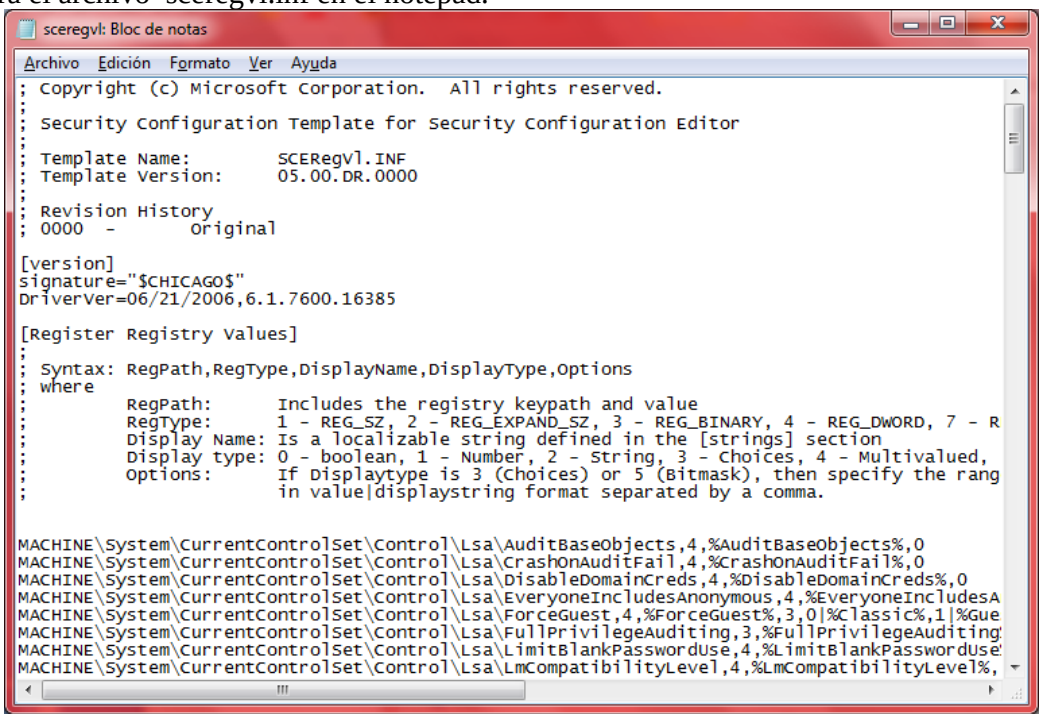
Figura 5.21: Tabla Reporte Expandida.

Modificar el archivo sceregvl.inf para cambio de código y aumento de seguridad.

1. Navegar hasta %systemroot%\inf o a través de C:\windows\inf



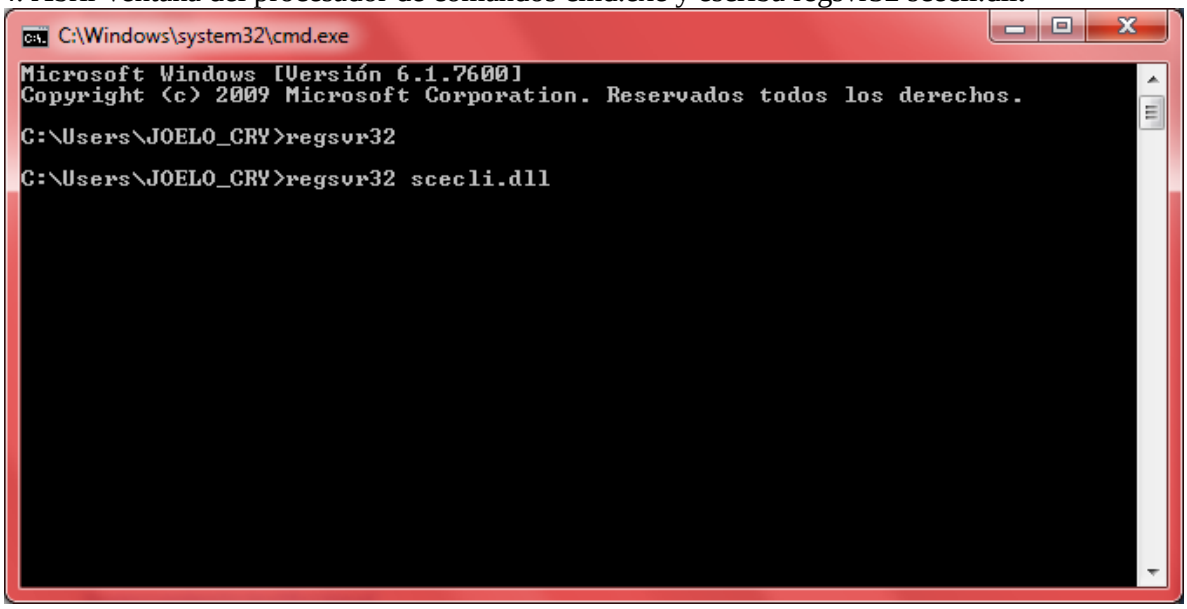
2. Abra el archivo sceregvl.inf en el notepad.



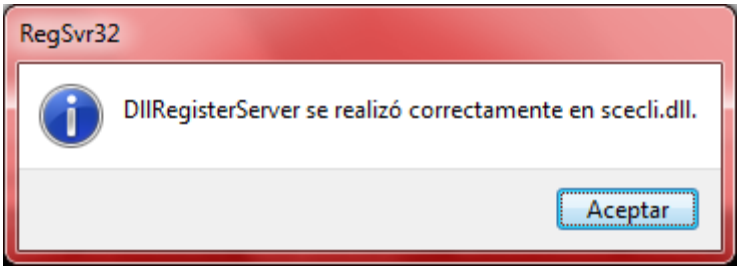
3. Reemplace sceregvl.inf con el archivo de configuración según el sistema que use.

Ver: ANEXO B – ANEXO C.

4. Abrir ventana del procesador de comandos cmd.exe y escriba regsvr32 scecli.dll.



5. Asegúrese que regsvr32 se registre satisfactoriamente.



Resultados

Una vez realizados los cambios se notará claramente en la realización de las tareas como el ingreso con contraseñas (fig. p), la mismas que ofrecerán correcciones para la seguridad el momento de manipularlas. Todo dependerá del sistema que se use y el tipo de seguridad que se le haya dado.

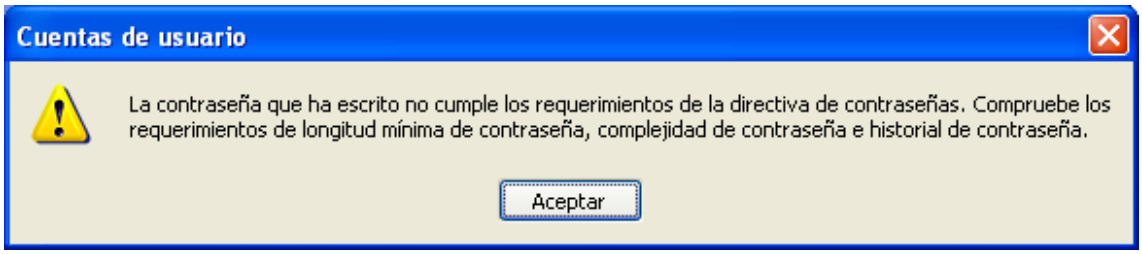


Figura 5.22: Ejemplo sobre cambios en la seguridad – Longitud de la contraseña.

Elaboración de manual de configuraciones especiales

Objetivo

Implementar esquemas de Seguridad Informática basados en Metodologías y estándares de la Industria.

Aseguramiento Institucional

Desarrollar diagnóstico de seguridad informática en las instituciones.

- Ejecutado por los técnicos de informática designados para el desarrollo del diagnóstico, según guía proporcionada para tal fin.
- Desarrollar el diagnóstico en cada institución.
- Crear una matriz regional con los hallazgos.
- Presentar hallazgos, conclusiones y recomendaciones en reuniones de informáticos.

Elaborar prototipo de Seguridad Informática y presentación en las reuniones para su aprobación

- Revisar documento desarrollado por técnicos en Seguridad Informática
- Tomando como base diagnóstico realizado, se tomarán todas aquellas acciones y recomendaciones que consideren más adecuadas a fin de implementarlas en cada institución.

Elaborar planes de Trabajo institucionales de implementación de dichas recomendaciones

- Producto de las Políticas y estándares anteriores, cada institución deberá implementar las medidas preventivas y correctivas del caso con el objetivo de nivelar los esquemas de seguridad informática

Implementar y dar seguimiento al Plan de Trabajo, propio de cada Institución

Manejo se software

Aplicación Syspred

Microsoft dispone de herramientas propias que pueden facilitarnos la vida para conseguir tener múltiples equipos en nuestra red con el sistema operativo Windows XP, configurado de la misma manera. Así, podemos realizar la instalación de un solo equipo y después usando la herramienta sysprep.exe, clonar todos los equipos ahorrando así mucho tiempo y dinero.

Según se puede leer en la página de ayuda de Microsoft "Sysprep es una herramienta diseñada para los administradores de sistemas, Fabricantes de equipos originales (OEM) y otras personas que deben implementar automáticamente el sistema operativo Windows XP en varios equipos. Después de realizar los pasos de instalación iniciales en un único equipo, puede ejecutar la herramienta Sysprep con el fin de preparar el equipo de ejemplo para la clonación."

Sin embargo antes de proceder a realizar todo el proceso, necesitamos tener claras algunas características de hardware del sistema. Entre ellas debemos tener en cuenta las siguientes:

- Los equipos de referencia y de destino deben tener HAL compatibles. Por ejemplo, los MPS (sistemas multiprocesador) basados en Controladora programable avanzada de interrupciones (APIC) deben utilizar la misma HAL APIC. Un sistema basado en una HAL estándar Controladora programable de interrupciones (PIC) no es compatible con la HAL APIC ni con la HAL MPS.
- Los equipos de destino y de referencia deben tener la misma compatibilidad con Interfaz avanzada de configuración y energía (ACPI).
- Los dispositivos Plug and Play de los equipos de referencia y de destino (como módems, tarjetas de sonido, adaptadores de red y tarjetas de vídeo) no tienen por qué ser del mismo fabricante. Sin embargo, los controladores para estos dispositivos deben estar disponibles.
- Se requiere software de creación de imágenes de disco o dispositivos de hardware de duplicación de discos de terceros. Estos productos crean imágenes binarias del disco duro de un equipo y duplican la imagen en otro disco duro o almacenan la imagen en un archivo en un disco independiente.

- El tamaño del disco duro del equipo de destino debe ser al menos igual que el del equipo de referencia. Si el equipo de destino tiene un disco duro mayor, la diferencia no se incluirá en la partición primaria. Sin embargo, puede utilizar la clave ExtendOemPartition del archivo Sysprep.inf para extender la partición primaria si se formateó utilizando el sistema de archivos NTFS.

Existen unos pasos muy concretos para realizar con éxito el duplicado del sistema en los equipos que necesitemos. Se detallan a continuación:

1. En un equipo de referencia, instale el sistema operativo y todos los programas que desee instalar en los equipos de destino.
2. Haga clic en Inicio y en Ejecutar, escriba cmd y haga clic en Aceptar.
3. En el símbolo del sistema, cambie a la carpeta raíz de la unidad C y escriba md Sysprep.

4. Inserte el CD del sistema operativo Windows XP en la unidad de CD-ROM o de DVD-ROM adecuada y abra el archivo Deploy.cab de la carpeta \Support\Tools.

Nota: para asegurarse de que está utilizando la versión correcta del archivo Deploy.cab para su Service Pack, utilice el archivo Deploy.cab que se distribuye con ese Service Pack. Visite el siguiente sitio web de Microsoft para descargar la versión correcta para su Service Pack:

http://www.microsoft.com/spain/windowsxp/downloads/default.mspx
(http://www.microsoft.com/spain/windowsxp/downloads/default.mspx)

5. Copie los archivos Sysprep.exe y Setupcl.exe a la carpeta Sysprep.
Nota: si utiliza el archivo Sysprep.inf, copie también este archivo a la carpeta Sysprep. Para que la herramienta Sysprep funcione correctamente, los archivos Sysprep.exe, Setupcl.exe y Sysprep.inf deben estar todos en la misma carpeta.
6. Quite el CD del sistema operativo Windows XP.
7. En el símbolo del sistema, escriba cd Sysprep para cambiar a la carpeta Sysprep.
8. Para ejecutar la herramienta Sysprep, escriba el comando siguiente en el símbolo del sistema:

Sysprep /parámetro opcional

Nota: para obtener una lista de parámetros, consulte la sección “Parámetros de Sysprep”.
Si ejecuta el archivo Sysprep.exe desde la carpeta %systemdrive%\Sysprep, el archivo Sysprep.exe quitará toda la carpeta y su contenido después de finalizar su ejecución.

9. Microsoft recomienda que después de ejecutar el archivo Sysprep.exe en un equipo de referencia aísle el equipo de referencia de la red local donde se implementará la imagen

para evitar posibles conflictos de NetBIOS. Esto permite a la herramienta Sysprep completar el programa de instalación, unirse al dominio especificado y utilizar el nuevo nombre de equipo que se indica en el archivo de respuesta Sysprep.inf.

Archivo de configuración de Sysprep

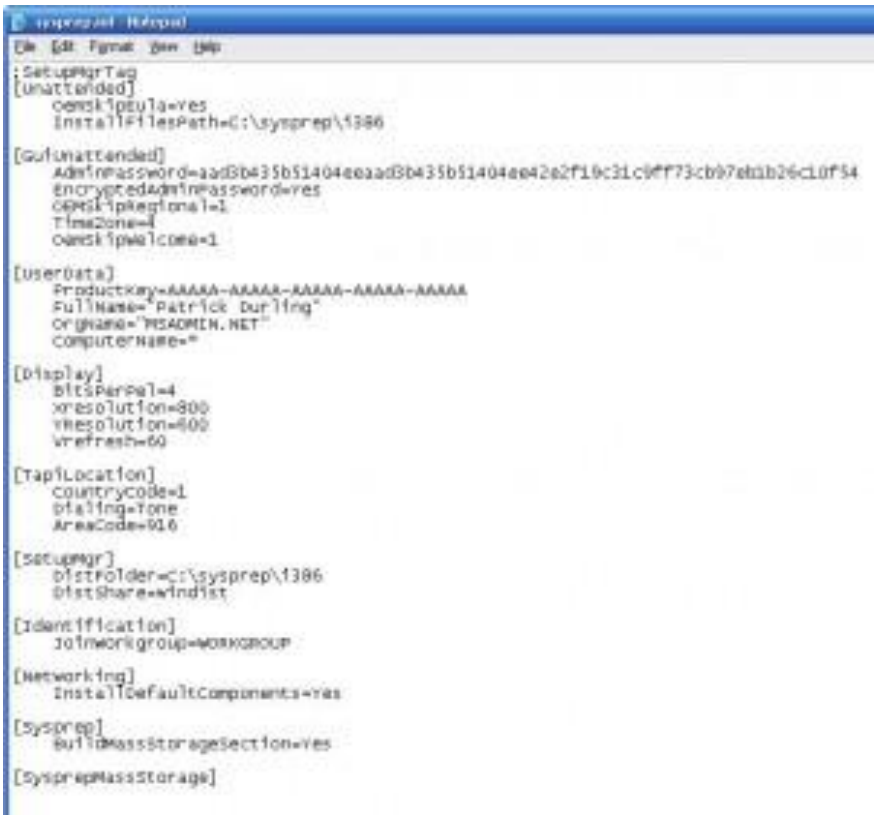


Figura 5.23: Archivo de configuración de Sysprep

CONCLUCIONES

- Entre sus ventajas, se puede contar con la disminución de efectividad de los sistemas por incidentes de seguridad

- Mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, a través de pruebas.

- Una administración más simple y mayor rapidez en la identificación de problemas con el uso de manuales de configuración.

- La posibilidad de poder hacer un seguimiento de los incidentes y en algunos casos identificar el origen de los mismos, ya que existe un similitud entre S.O.

Es un trabajo que no es trivial, y que bien vale la pena hacerlo.

El Hardening es una ayuda indispensable para ahorrarse bastantes dolores de cabeza por parte de los administradores de sistemas. Entre sus ventajas, se puede contar con la disminución de efectividad de los sistemas por incidentes de seguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas, ya que muchas de las posibles causas de ellos quedarán descartadas en virtud de las medidas tomadas, y finalmente la posibilidad de poder hacer un seguimiento de los incidentes y en algunos casos identificar el origen de los mismos. Es un trabajo que no es trivial, y que bien vale la pena hacerlo.

RECOMENDACIONES

Las recomendaciones contenidas en la presente son resultantes de un proceso de análisis y evaluaciones que cada usuario ha experimentado en el uso de los sistemas operativos.

Son propuestas proporcionando la información útil a organizaciones intentando para evaluar o mejorar la seguridad de sus redes, sistemas, y dispositivos.

El uso apropiado de las recomendaciones requiere análisis cuidadoso y adaptación a las necesidades de usuario específicas.

Ninguna red, sistema, dispositivo, hardware, software, o componente se puede hacer enteramente seguro; Estamos usando los productos y las recomendaciones solamente a nuestro propio riesgo; Nosotros tenemos la responsabilidad única para evaluar los riesgos y beneficios de los productos.
Primero habrá que evaluar la aplicación para luego hacerla efectiva.
Todas las aplicaciones funcionan correctamente pero hay que ver qué es lo realmente se necesita.

BIBLIOGRAFÍA

[1] El centro para la seguridad de Internet [ONLINE] http://www.cisecurity.org

[2] El instituto de SANS [ONLINE] http://www.sans.org

[3] [ONLINE] http://www.nsa.gov/ia

[4] Departamento de las recomendaciones de defensa no corrientemente disponible en línea.

Microsoft Windows Security [ONLINE] http://www.microsoft.com/security

[5] [ONLINE] http://tipsdeseguridad.spaces.live.com/blog/cns!779AF69CE6408BD1!2273.trak

[6] [ONLINE] http://labs.dragonjar.org/xmlrpc.php?rsd

[7] [ONLINE] http://geeks.ms/blogs/vista-tecnica/archive/2007/12/24/sistemas-de-integridad-en-win

[8] [ONLINE] http://www.fistconference.org/data/presentaciones/hardeningaltaseguridadbajow32.pdf

[9] [ONLINE] http://www.aibarra.org/investig/tema0.htm#INVESTIGACI%D3N

[10] Akelos, Web Services. [ONLINE] www.akelos.org/docs/tutorials/booklink-es.2009.

[11] Piattini Mario, Modelo Vista Controlador. [ONLINE] http://images.google.com.ec/imagen

[12] D. Gamma, Propuesta_de_un_modelo_navegacional.pdf

[13] Davis A, Principles of Software Development, 1ª ed. McGraw-Hill, 1995.

[14] Bonus, Web con un amplio glosario de términos de Ingeniería del software. [ONLINE] http://www.qxtecno.com/documentos/Fundamentos.pdf 2006

El centro para la seguridad de Internethttp://www.cisecurity.org

El instituto de SANShttp://www.sans.org

La recomendación de seguridad de agencia de seguridad nacional guia-http://www.nsa.gov/ia

Departamento de las recomendaciones de defensa no corrientemente disponible en línea.

Microsoft Windows Securityhttp://www.microsoft.com/security

Windows XP Security Guide¿http://go.microsoft.com/fwlink/?guía de seguridad de LinkId=14839 Server 2003¿http://go.microsoft.com/fwlink/?amenazas de LinkId=14845 y medida preventiva guian¿http://go.microsoft.com/fwlink/?LinkId=15159

Microsoft Directory atiende el cliente para Windows 9x/me-¿http://www.microsoft.com/TechNet/prodtechnol/ntwrkstn/downloads/utils/dsclient.asp?frame=true

Artículo de Windows NT Magazine con respecto a editando el registro-¿http://www.microsoft.com/technet/treeview/default.asp?magneto de url=/technet/prodtechnol/winntas/tips/winnt/inreg.asp

orientaciones de NIST Windows 2000 Security -http://csrc.nist.gov/itsec/guidance_W2Kpro.html

ANEXOS

ANEXO A. MANUAL DE USUARIO NG SORING TOOL

NG SCORING TOOL

Introducción a la herramienta de marcado de NG

Las herramientas de CIS Scoring habilitan a usuarios finales para verificar que la configuración de seguridad de sistemas antes del despliegue de red, sistemas de monitor y dispositivos de red para la conformidad progresiva con las pruebas de características, y demostrar a auditores y socios de negocio su misión con las normas internacionalmente aceptadas para la configuración de seguridad. Las herramientas de marcado de CIS son basados en el anfitrión (HOST) y producen los informes qu radores de sistema para asegurar ambas nuevas instalaciones y sistemas de producción.

La próxima herramienta de **NG** estará escrita en JAVA. Es diseñada para ser la plataforma independiente, permitiendo correr en casi cualquier entorno y para marcar sus sistemas comparados con todas las pruebas de características de CIS. Versiones de la herramienta de NG son disponibles con o sin una máquina virtual (JVM) de JAVA que consta en el NG directorio de instalación de la herramienta. La versión sin el JVM es diseñada para sistemas con Java 1.5 de SUN o el posterior ya está instalado.

La herramienta de NG lee el archivo Benchmark y la configuración verifica los archivos. Ambos archivos están en el formato de XML. Los archivos Benchmark expresan las recomendaciones de configuración de consenso. Ellos instruyen la herramienta de NG para verificar la seguridad técnica de un sistema controles e informe en la sumisión de esos controles con las recomendaciones de prueba de características.

La configuración verifica los archivos que expresan el método que la herramienta de NG usa para verificar el sistema para los controles recomendados técnicos. Ellos Instruyen en cómo ejecutar la configuración.

Habilitan a los usuarios para comparar la configuración de sus sistemas con las recomendaciones de prueba. Para las configuraciones de sistema que es de acuerdo con las recomendaciones de prueba de características, la herramienta de NG relata esos artículos de prueba de características como PASS "pase". Para las configuraciones de sistema, NO de acuerdo con las recomendaciones de prueba de características, la herramienta de NG relata esos artículos de prueba de características como FAILED "fracaso" Los informes también guían a los usuarios en cómo poner los controles recomendados en "suspender", con eso mejorando la configuración de seguridad del sistema examinado.

Comparaciones lógicas avanzadas

La herramienta de NG soporta comparaciones lógicas tal como: *menos de o igual a* y *mayor que o igual a las* comparaciones. Esto lo habilita para reconocer "pase" una configuración de sistema que proporciona mayor seguridad que la recomendación asociada de prueba de características.

Formatos de presentación de informes adicionales

La versión inicial de la herramienta de NG producirá informes en HTML, que se puede mirar por todos los visores populares incluyendo Internet Explorer, Mozilla, ópera, y safari. El informe adicional posee opciones que se suman con el transcurso del tiempo, incluyendo XML, PDF, CSV y texto de ASCII.

Interfaz de usuario (GUI) gráfica La interfaz de usuario para la versión pública de la herramienta de NG es altamente interactivo GUI. Este enlace da al usuario un nivel avanzado del control sobre el NG y las funciones de herramienta.

La herramienta de NG no verifica de forma automática para el estatus de parche en los sistemas en que es corrido. Cuando usted corre la herramienta de NG confirmará manualmente el estatus de parche respondiendo exactamente a una pregunta cuando impulsado por la herramienta de NG.

Además, existen unas cuantas pruebas de características específicas donde toma forma en algunas de las pruebas de características que la herramienta de NG no puede acceder de forma automática. Como consecuencia, información sobre el estatus de estas colocaciones es pedida al usuario de la herramienta de NG en la forma de respuestas a las preguntas preguntado por la herramienta de NG cuando es corrido.

Manualmente responder estas preguntas, así como la pregunta de estatus de parche, es requerida por la herramienta de NG para producir una cuenta exacta y una pintura clara del estado de configuración del sistema.

Los archivo de Configuración

Para una herramienta para verificar el estatus de configuración de muchos sistemas, aplicaciones y dispositivos de red, debe ser capaz de ver las verificaciones lectoras y ejecutadas expresadas en un formato de datos consistente. La herramienta de NG lee y ejecuta las expresiones de verificación basadas en el modelo de datos y representación de XML conocidos como OVAL Vulnerabilidad abierta e idioma de evaluación.

El esquema de definición de OVAL especifica cómo referirse a los parámetros de

configuración en las definiciones. Define lo que los datos de sistema para reunirse y cómo reunirlo.

Las características de sistema OVAL, el esquema define un formato de XML estándar para almacenar información de configuración de sistema. Esta información de configuración incluye los parámetros de sistema operativo, y otros valores de configuración pertinentes de la seguridad. El propósito de este esquema es proporcionar una "base de datos" de las características de sistema contra que las definiciones de OVAL pueden ser comparadas con evaluar una configuración de sistema.

El OVAL resulta el esquema definido en un formato de XML estándar para almacenar los resultados de una evaluación de configuración de sistema. Los datos de resultados contienen el estado actual de la configuración de un sistema como comparado con un conjunto de las definiciones de OVAL. Los esquemas de resultados permiten la herramienta de NG para consumir estos datos, lo interpreta, y presenta el informe de ello.

Descargar e instalar la herramienta de marcado de NG

El primer paso al instalar la herramienta de NG es determinar exactamente lo que la versión de la herramienta de NG conviene sus necesidades. Si es el miembro de cis, usted tendrá acceso a versiones de la herramienta de NG que ha mejorado características. Las versiones de miembro se pueden descargar de http://members.cisecurity.org.

No Los miembro tienen acceso gratuito a la herramienta de NG del sitio Web público a http://www.cisecurity.org. Simplemente escoja la plataforma que desea probar (Windows, Solaris, etc...) y clic en el apropiado vincula la página principal.

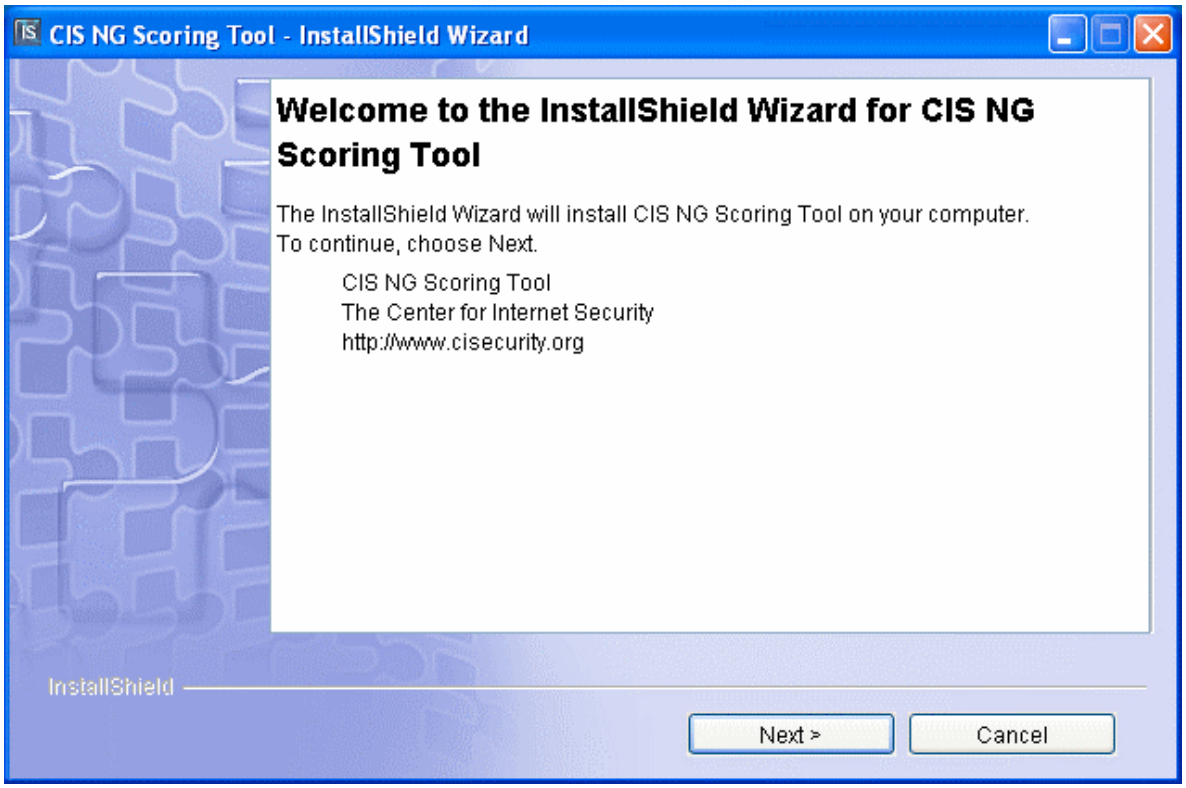
Esto le tomará para una página de la plataforma específica que contenga información sobre la herramienta de NG y la prueba de características asociada o pruebas de características. Por favor, tome tiempo para repasar esta página como ello contiene la información importante que puede impactar el NG la funcionalidad de herramienta en su sistema.

La herramienta de NG es escrita en el lenguaje de programación de Java popular. A fin de asegurar que todos pueden hacer uso de la herramienta de NG, CIS haya preparado un instalador empaquetado que incluya una máquina virtual de JAVA (JVM.) Esto JVM es requerido por la herramienta de NG para correr. Sin embargo, ciertos usuarios tendrán ya un JVM en su sistema. Si usted es cierto que ya tiene el sol JAVA 1.5 o posterior instalado, puede reducir tiempo de descarga y uso de espacio en disco por escoger el paquete de herramienta de NG que no incluye el JVM. esto se marca claramente en la página de descarga. El instalador de herramienta de NG verificará que usted tiene el JVM instalado y

le notifique si no puede encontrar ello.

Instalar la herramienta de marcado de NG en Microsoft Windows

Una vez que la herramienta de NG ha sido descargada a su sistema, clic dos veces la tecla del Ratón sobre simplemente el icono de instalador para comenzar al proceso de instalación. Este icono se puede encontrar dondequiera que le escoger para descargar el paquete para. Tipicamente esto es el buró, pero pueda en otra parte basado en sus preferencias de sistema. La primera pantalla que usted ve debe parecerse a este:



Haga clic " después > " para continuar.

Usted debe acceder a los términos de CIS del uso escogiendo " acepto che los términos del acuerdo de licencia " y escogiendo " después >".

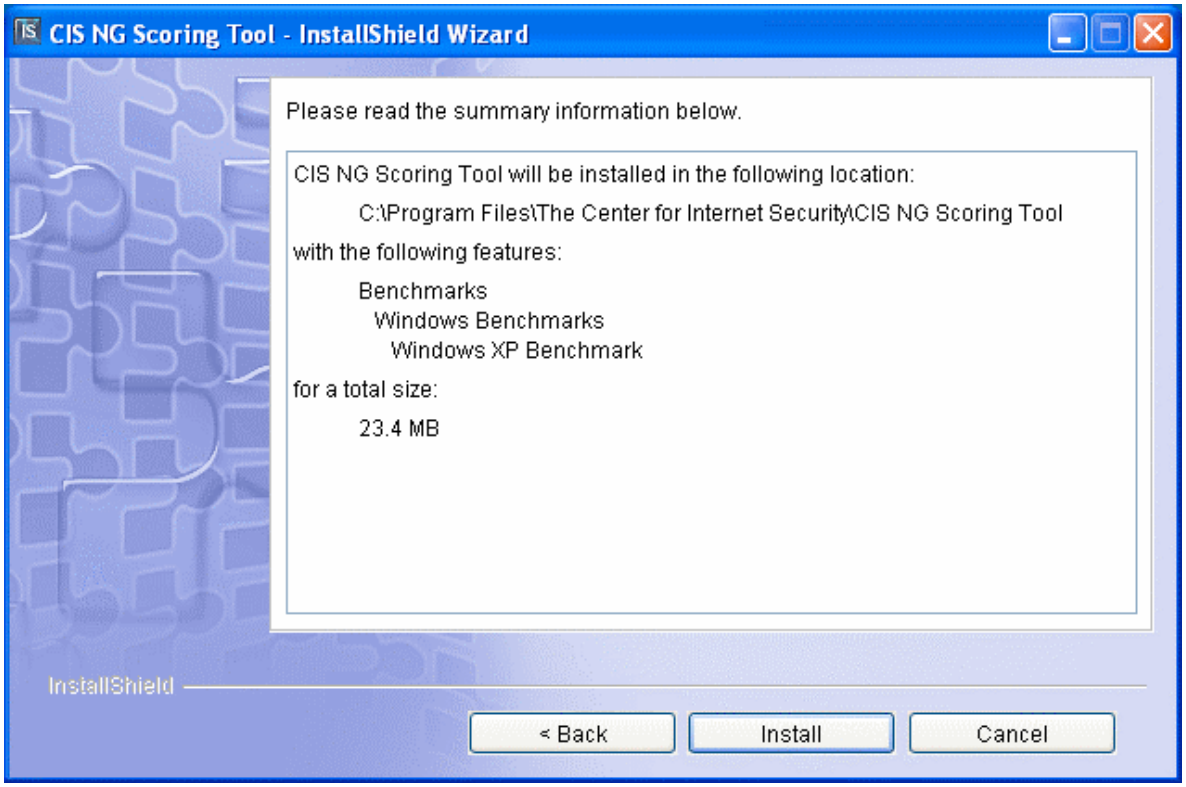
El instalador escoge una ubicación implícita para instalar la herramienta de NG, pero puede hacer caso de este para instalarlo dondequiera que prefiere. El instalador creará todos los directorios ése no existe ya.

Después, escoja la instalación "típica" o "a la medida". CIS recomienda que todos los usuarios escogen "típicos" para asegurar que todos los componentes necesitados se

instalen.

Cuando escoge "típico", la herramienta de NG detectará de forma automática el tipo del sistema y ofrecerán varias elecciones de instalación basadas en eso. Por ejemplo, al correr en un sistema Windows XP, la herramienta de NG ofrecerá sólo lo pertinente a Windows XP.

Lo siguiente secciones de este manual usarán la prueba de características de profesional de Windows XP y versión de GUI de la herramienta de NG como nuestro ejemplo.



Si desee instalar otros archivos, escoja " costumbre instala " y escogen los archivos que desea. Por favor, esté seguro de escoger los archivos para el sistema que está corriendo la herramienta de NG en, o no trabajará.

Clic en "instalar" para terminar el proceso, una barra de estatus progresará para mostrar el progreso de la instalación. Por lo general, la instalación debe tomar sólo 1-2 minutos.

Cuando el proceso de instalación de herramienta de NG es completado, haga clic en el botón de "fin".

Correr la herramienta de marcado de NG en Windows

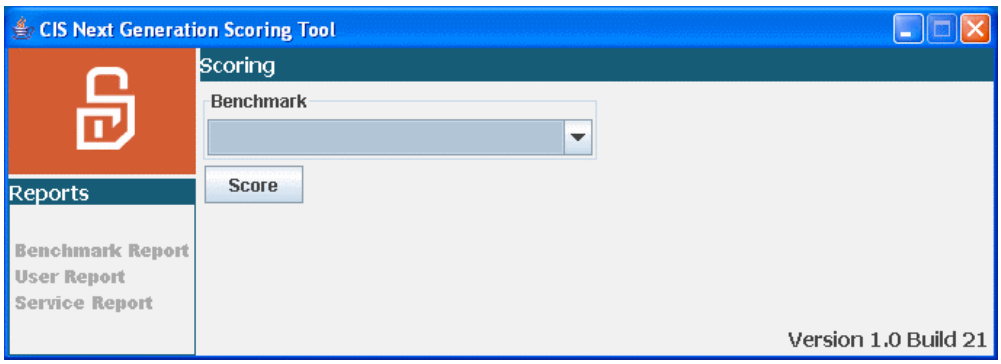
Para empezar la herramienta de NG, haga clic en Start- > todo Programs- >el centro para Internet Security-> marcado de CIS NG Tool- > GUI de herramienta de marcado de NG.

Desde aquí puede abrir también el documento de prueba de características, el README para la herramienta de NG, y accede los "resultados" el directorio. Por favor, esté seguro de leer el archivo README antes de la corrida la herramienta de NG como ello contiene la información importante, incluyendo detalles con respecto a los asuntos conocidos con respecto a la herramienta de NG y corriendo lo en sus sistemas.

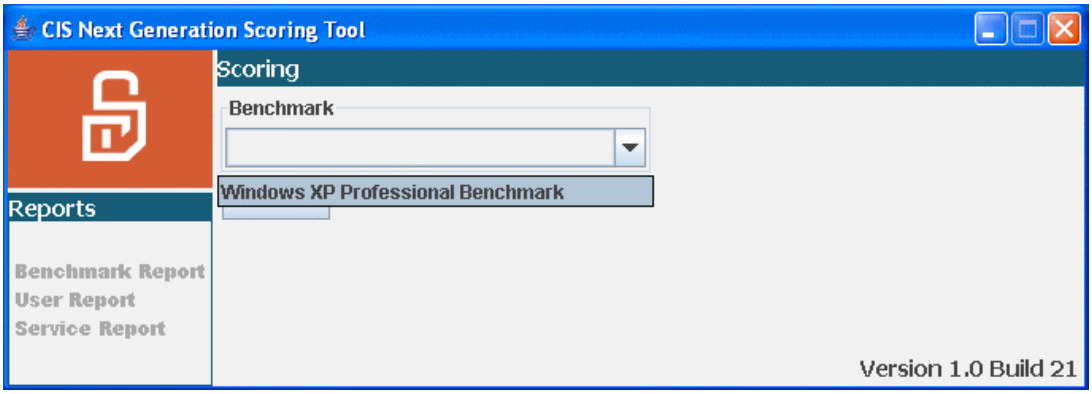
También, note que los "resultados" el directorio serán vacíos hasta que ha corrido la herramienta de NG a terminación exitosa al menos un tiempo.

La cantidad del tiempo que toma la herramienta de NG para empezar variar en dependencia de las especificaciones del sistema que está corriendo en. En promedio, el tiempo de arranque debe tener alrededor de 10-20 segundos.

Una vez que la herramienta de NG ha empezado, usted verá la siguiente la pantalla:



Note que tiene que hacer elecciones en la caja de abajo de modo que la herramienta de NG sabe cómo quiere que su sistema se pruebe. En la caja primera, escoja el documento de prueba de características. En este ejemplo, nosotros escogeremos prueba de características de Windows XP profesional.



Después, escoja que perfile que usted quiere usar en la mano derecha caiga boxee abajo. Los perfiles diferentes representan los niveles diferentes de la seguridad en la prueba de características. Para la prueba de características de profesional de Windows XP estos niveles son:

Herencia - colocaciones en este nivel son diseñadas para los sistemas XP profesional que necesitan operar con los sistemas más viejos tal como Windows NT, o en entornos donde aplicaciones de terceros más viejas exija se. Las colocaciones no son probables para afectar la función o ejecución del sistema operativo o de aplicaciones que son corriendo en el sistema.

Buró de empresa - colocaciones en este nivel son diseñadas para sistemas XP profesional de funcionamiento en un entorno manejado donde interoperabilidad con los sistemas de herencia no exija. Asume que todos los sistemas operativos dentro de la empresa son Windows 2000 o posterior, y por lo tanto capaz para usar todo posible seguridad caracteriza disponible dentro de esos sistemas. En tales entornos, estas colocaciones de nivel de empresa no son probables para afectar la función o ejecución del OS. sin embargo, uno debe considerar cuidadosamente el impacto posible en las aplicaciones de software al aplicar éstos recomiendan los controles técnicos que XP profesional.

La empresa móvil - estas colocaciones son casi idénticas a las colocaciones autónomas de empresa, pero con transformaciones apropiadas para los usuarios móviles cuyos sistemas deben hacer funcionar ambos en y lejos de la red corporativa. En los entornos donde todos los sistemas es Windows 2000 o posterior, estas colocaciones de nivel de empresa no son probables para afectar la función o ejecución del OS.

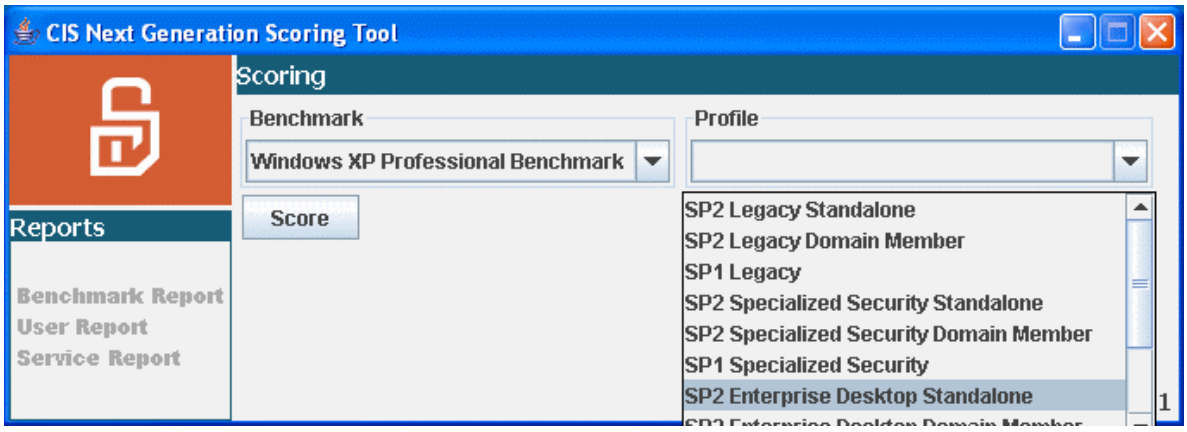
Sin embargo, uno debe considerar cuidadosamente el impacto posible en las aplicaciones de software al aplicar éstos recomiendan los controles técnicos que XP profesional.

Seguridad especializada La funcionalidad limitada Anteriormente conocido como " la

seguridad alta, " tome forma en este nivel está diseñado para los sistemas XP profesional en que seguridad e integridad son las prioridades más altas, aún a expensas de funcionalidad, ejecución, e interoperabilidad. Por lo tanto, cada colocación debe ser considerado cuidadosamente y sólo aplicado por un administrador experimentado que tiene A

la comprensión completa del impacto potencial de cada poniendo o la acción en un entorno particular.

Es importante escoger el nivel correcto para su sistema. Por regla general, escoger el nivel de empresa es un compromiso bueno entre seguridad sólida y funcionalidad. Aquí nosotros usaremos " empresa de SP2 autónomo para buró ".



Una vez que ambas selecciones han sido hechas, haga clic en la "cuenta". Para ejecución óptima, usted debe correr sólo la herramienta de NG mientras que ningún otras aplicaciones están corriendo.

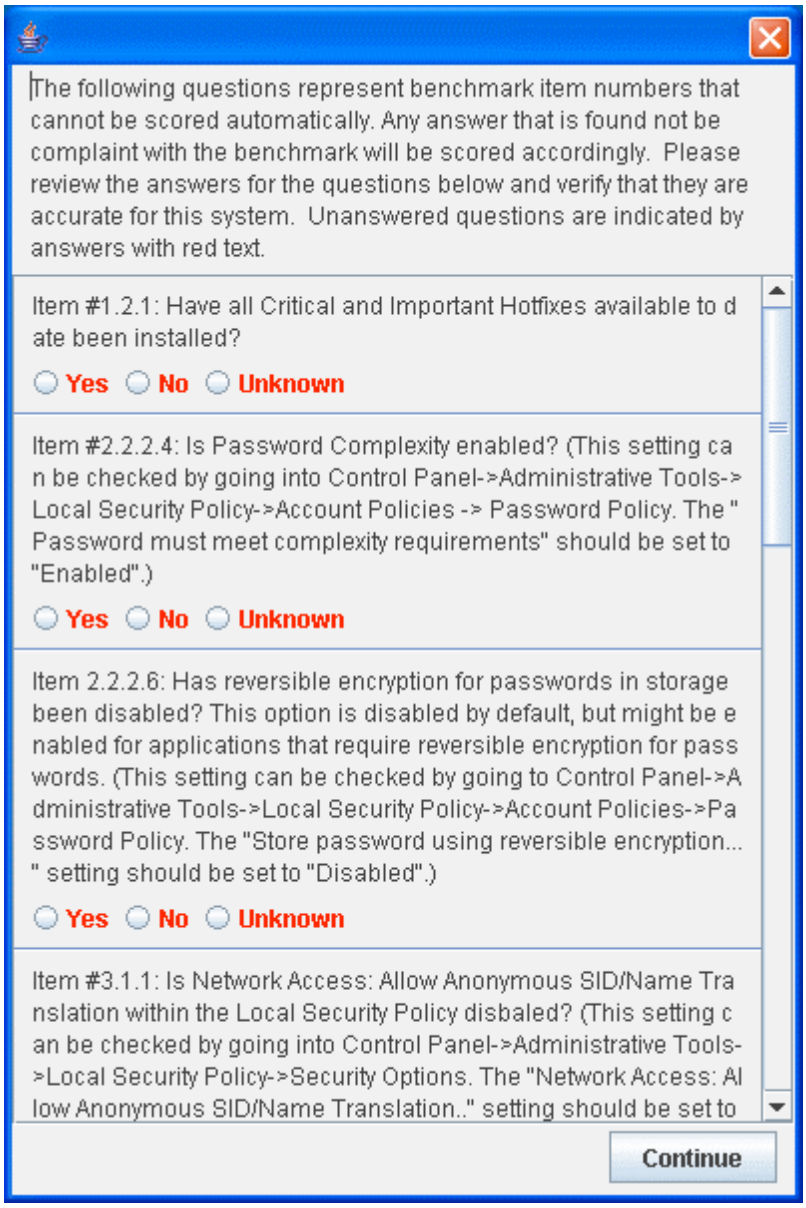
En este punto, la herramienta de NG comenzará a varias fases en su análisis del sistema.

La primera fase es verificar la presencia e integridad de los archivo Java necesarios.

Si reciba un error durante esta fase, por favor avise CIS a:

ngtool-feedback@lists.cisecurity.org.

Después, la herramienta de NG presenta un cuestionario que requiere la entrada de usuario (vea el tiro de pantalla en lo siguiente folia).



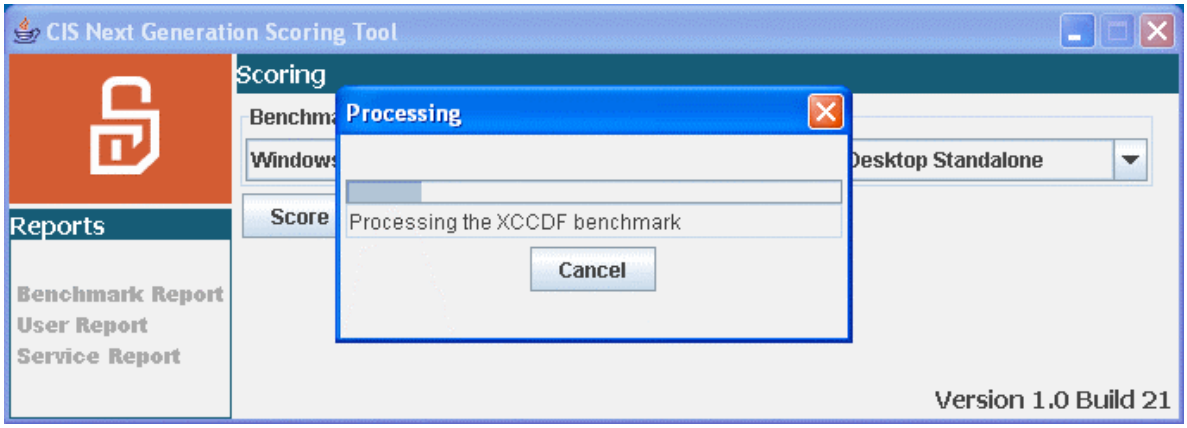
Existe unas cuantas colocaciones que la herramienta de NG no puede verificar corrientemente de forma automática.

Para mayor información, por favor vea el archivo README. Es importante que el usuario correctamente responde estas preguntas de modo que la herramienta de NG pueda retornar una cuenta exacta. Por favor, tome el tiempo en verificar su sistema y escoger la respuesta correcta.

Cada pregunta incluye una descripción de cómo verificar la colocación en su sistema.

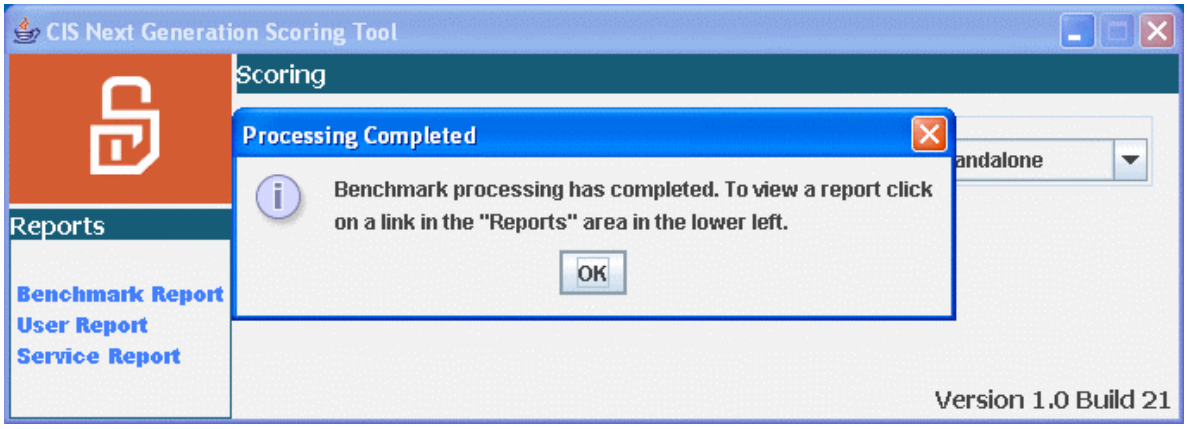
La herramienta de NG no procederá hasta una respuesta haya sido provea para cada pregunta.

Después que ha respondido todas las preguntas, haga clic "continúe" y la herramienta de NG comenzará a su proceso de comprobación automatizado. Durante este tiempo, varias cajas de estatus parecerán mantenerle informe en lo que la herramienta de NG está haciendo.



La cantidad del tiempo necesaria para la herramienta de NG para completar un examine enteramente varie grandemente basado en las especificaciones de su sistema. Por regla general, sin embargo, la herramienta de NG debería completar dentro de unos cuantos minutos.

Cuando está terminado, el " procesando complete " caja aparezca y usted puede el anuncio que el color del tres informe vincula el lado izquierdo de la ventana de herramienta de NG es ahora azul.



Esto indica que la herramienta de NG ha creado con buen resultado estos tres informes

Informe de informe/servicio de informe/usuario de prueba de características - y puede mirarles ahora.

Clic en la "aprobación" para cerrar la caja.

Correr la herramienta de marcado de NG en Solaris 10

Cambio al directorio donde la herramienta era instalada. En rebeldía este /opt/CISngtool. Por favor, asegure de que el ng.sh en este archivo directivo haya el ejecución mordido conjunto.

Para mirar las opciones de línea de orden disponibles: ./ng.shh

Para correr la herramienta de marcado:

./ng.sh opciones

Inicialmente la herramienta pedirá entrada de usuario en la forma de un cuestionario interactivo.

Responder estas preguntas tan exactamente como posible altamente recomendado.

Una vez que el cuestionario ha sido completado, la herramienta comenzará a es la marcado automática corra, que tipicamente último un promedio de 30 segundos, pero varie basado en las especificaciones de sistema de objetivo y la carga media.

Para mirar el HTML anuncie una vez la herramienta ha completado su operaciones, usa su visor de Web para abrir los archivos localizados en

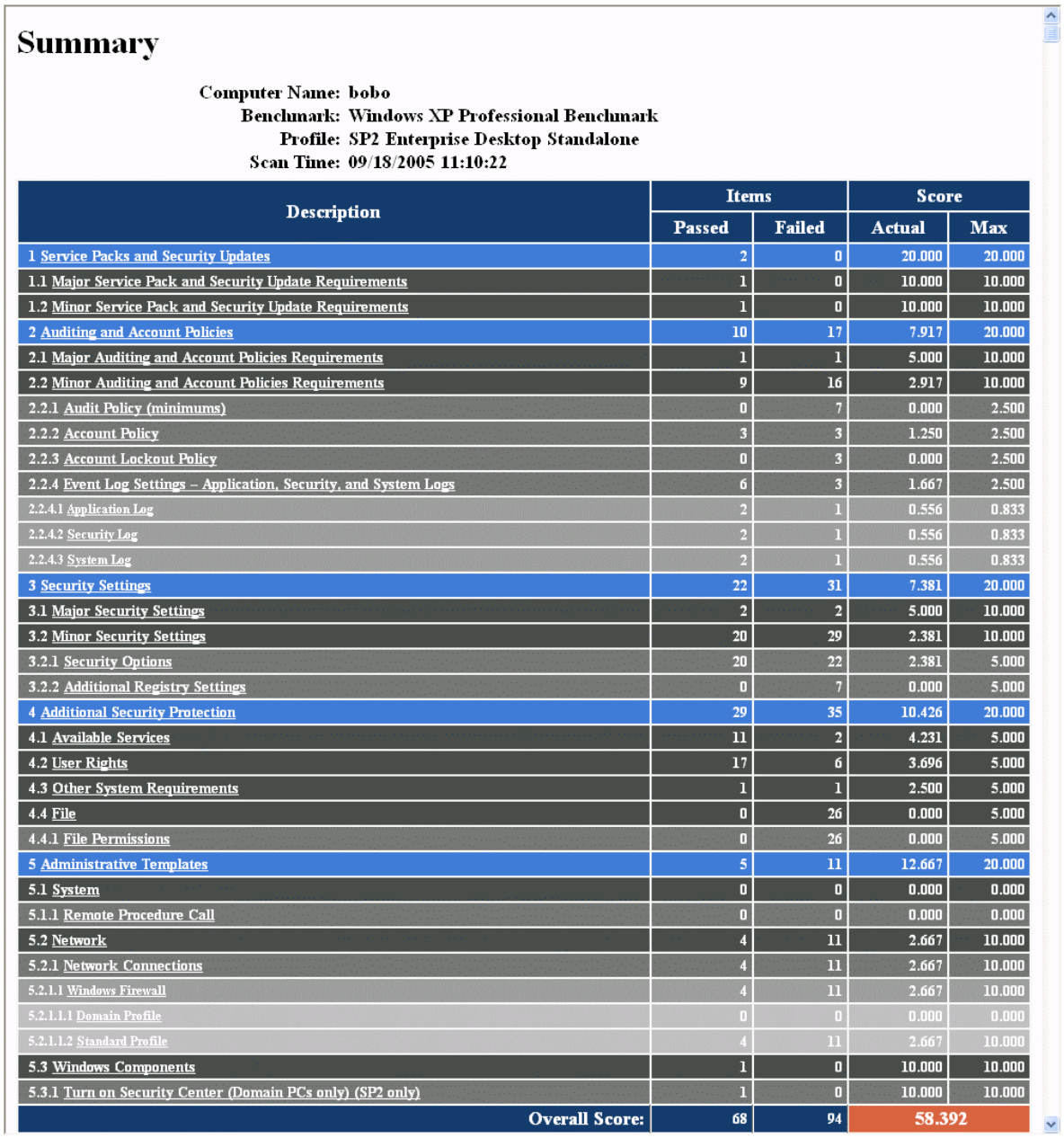
<la directorio installation
>/results//results//results//results//results//results//results//results//results//results//r
esults//results//results//results//results//results//results//results//results//results//resul
ts//results//results//results//results//results//results//results//results//results//results//
results//results//results//results//results//results//results//results//results//results//res
ults//results//results//results//results//results//results//results//results//results//results
//results//results//results//results//results//results//results//results//results//results//re
sults//results/< el TIMESTAMP > /reports/html.

Donde TIMESTAMP es el último |timestamp| para cuando la herramienta corrió.

Sección 7: Los informes de herramienta de marcado de NG

Hacer clic en uno de los enlaces de informe lanzará su visor de Web y exhibición el informe escogido. Lo siguiente los visores son conocidos para de trabajo con los informes de herramienta de NG: Internet Explorer, Mozilla/Firefox, ópera, y safari.

Empezamos con el informe de prueba de características, que contienen tres secciones relacionadas.



Summary

Computer Name: bobo
Benchmark: Windows XP Professional Benchmark
Profile: SP2 Enterprise Desktop Standalone
Scan Time: 09/18/2005 11:10:22

Description	Items		Score	
	Passed	Failed	Actual	Max
1 Service Packs and Security Updates	2	0	20.000	20.000
1.1 Major Service Pack and Security Update Requirements	1	0	10.000	10.000
1.2 Minor Service Pack and Security Update Requirements	1	0	10.000	10.000
2 Auditing and Account Policies	10	17	7.917	20.000
2.1 Major Auditing and Account Policies Requirements	1	1	5.000	10.000
2.2 Minor Auditing and Account Policies Requirements	9	16	2.917	10.000
2.2.1 Audit Policy (minimums)	0	7	0.000	2.500
2.2.2 Account Policy	3	3	1.250	2.500
2.2.3 Account Lockout Policy	0	3	0.000	2.500
2.2.4 Event Log Settings – Application, Security, and System Logs	6	3	1.667	2.500
2.2.4.1 Application Log	2	1	0.556	0.833
2.2.4.2 Security Log	2	1	0.556	0.833
2.2.4.3 System Log	2	1	0.556	0.833
3 Security Settings	22	31	7.381	20.000
3.1 Major Security Settings	2	2	5.000	10.000
3.2 Minor Security Settings	20	29	2.381	10.000
3.2.1 Security Options	20	22	2.381	5.000
3.2.2 Additional Registry Settings	0	7	0.000	5.000
4 Additional Security Protection	29	35	10.426	20.000
4.1 Available Services	11	2	4.231	5.000
4.2 User Rights	17	6	3.696	5.000
4.3 Other System Requirements	1	1	2.500	5.000
4.4 File	0	26	0.000	5.000
4.4.1 File Permissions	0	26	0.000	5.000
5 Administrative Templates	5	11	12.667	20.000
5.1 System	0	0	0.000	0.000
5.1.1 Remote Procedure Call	0	0	0.000	0.000
5.2 Network	4	11	2.667	10.000
5.2.1 Network Connections	4	11	2.667	10.000
5.2.1.1 Windows Firewall	4	11	2.667	10.000
5.2.1.1.1 Domain Profile	0	0	0.000	0.000
5.2.1.1.2 Standard Profile	4	11	2.667	10.000
5.3 Windows Components	1	0	10.000	10.000
5.3.1 Turn on Security Center (Domain PCs only) (SP2 only)	1	0	10.000	10.000
Overall Score:	68	94	58.392	

El informe de prueba de características es los más grandes de los tres informes y

contenga la más útil información. En la parte superior del informe es el "resumen" de título y el nombre de la computadora examinado, la fecha y hora de la corrida de marcado, y la prueba de características y nombre de perfil.

Esta vista sumaria del informe de prueba de características ha tres columnas. La columna de descripción contiene el número y nombre de cada sección de prueba de características, ítem y sub el artículo.

Las columna de artículos son abiertas en dos sub columnas que indique el paso/suspenda el estatus de cada prueba de características ítem y sub el artículo. La herramienta relata un artículo o sub el artículo como pase si la configuración real del sistema examinado es el mismo o más seguro que la recomendación correspondiente de prueba de características. Relata un artículo o sub el artículo como suspenda si la configuración real del sistema examinado es diferente o menos segura de la recomendación de prueba de características correspondiente.

La columna de cuenta identifica la cuenta real y posible máxima del sistema para cada sección de prueba de características y sus artículos descendientes y sub artículos con respecto a las recomendaciones de configuración de la prueba de características.

La marcado de herramienta de NG algoritmo refleja la organización de la prueba de características de sus recomendaciones de configuración.

Para ilustrar este punto, las pruebas de características son organizadas en secciones y los artículos descendientes y sub los artículos. Las secciones de prueba de características contienen los niveles variantes de los artículos descendientes y sub los artículos. Cada artículo es o una recomendación de configuración específica o una compilación de las recomendaciones, que se identifica en el plan de numeración como sub los artículos.

Por ejemplo, en la prueba de características para Windows XP (vea el informe sobre), sección 2 está revisando y las políticas de cuenta. Esa sección es comprendida de dos artículos de prueba de características:

2.1 se especializan auditoría y necesidades de políticas de cuenta

2.2 menor revisando y necesidades de políticas de cuenta

Además, prueba de características ítem 2.2 comprenda se de cuatro sub los artículos:

2.2.1 revise político (mínimos)

2.2.2 política de cuenta

2.2.3 política de cierre forzoso de cuenta

2.2.4 el evento entra colocaciones Aplicación, seguridad, y diarios de sistema

Y sub artículo 2.2.4 comprenda se de otra capa de tres adicional sub los artículos:

2.2.4.1 registro de aplicación

2.2.4.2 registro de seguridad

2.2.4.3 registro de sistema

Cómo la herramienta de NG calcula los grandes números posibles máximos

La cuenta posible máxima para la prueba de características es 100 puntos. Para calcular la cuenta posible máxima para cada nivel de la prueba de características, el NG el algoritmo de marcado de herramienta para la prueba de características de Windows XP divide la cuenta posible máxima total de cada nivele por el número de los descendiente inmediatos de ese nivel. Lo siguiente los ejemplos ilustran cómo el los trabajos de algoritmo de marcado de la herramienta NG relativos al cálculo de granes números posibles máximos:

(1) para calcular la cuenta disponible para la sección 2 de la prueba de características, divida la cuenta posible máxima para la prueba de características (100 puntos) por el número de secciones dentro de la prueba de características (5). Por lo tanto, la cuenta posible máxima para sección 2 es 20 puntos.

(2) para calcular la cuenta posible máxima para artículo 2.2, divida la cuenta posible máxima para la sección 2 (20 puntos) por el número de sub artículos dentro de la sección 2 (2). Por lo tanto, la cuenta posible máxima para sección 2.2 es 10 puntos.

(3) para calcular la cuenta posible máxima para sub artículo 2.2.4, divida la cuenta posible máxima para ítem 2.2 (10 puntos) por el número del descendiente de 2.2's de artículo sub artículos (4). Por lo tanto, la cuenta posible máxima para sub artículo 2.2.4 es 2.5 puntos.

(4) para calcular la cuenta posible máxima para sub artículo 2.2.4.1, divida la cuenta posible máxima para sub ítem 2.2.4 (2.5 puntos) por el número de sub 2.2.4's de artículo sub artículos (3). Por lo tanto, la cuenta posible máxima para sub artículo 2.2.4.1 es 0.833 puntos.

Los granes números disponibles para los niveles profundos siguen el mismo modelo de lógica como se esboza arriba.

Cómo la herramienta de NG calcula los tantear reales de un sistema

Para calcular la cuenta real de un sistema como comparado con cada nivel de una prueba de características, el NG el algoritmo de marcado de herramienta toma la suma de todos los granes números reales de cada uno de un particular los niveles descendientes inmediatos de nivel. Lo siguiente ejemplos del informe sumario anterior ilustran cómo el NG el algoritmo de marcado de herramienta calcula la cuenta real de un nivel.

(1) para calcular la cuenta completa real de la prueba de características, sume la cuenta real de cada sección del informe: La sección 1 la cuenta real (20 puntos) + La sección 2 la cuenta real (7.917 puntos) + La sección 3 la cuenta real (7.381 puntos) + La sección 4 la cuenta real (10.426 puntos) + La sección 5 la cuenta real (12.667 puntos) = 58.392 puntos para la cuenta completa real de la prueba sistema sumisión con todas las recomendaciones de configuración encontradas dentro de la prueba de características.

(2) para calcular la cuenta real de la sección 2, sume la cuenta real de cada uno de la sección 2 artículos: Ítem la cuenta de 2.1's real (5 puntos) + Ítem la cuenta de 2.2's real (2.917 puntos) = 7.917 puntos para la cuenta real de la sumisión del sistema de prueba con todas las recomendaciones de configuración encuentre dentro de la sección 2 de la prueba de características.

Los granes números reales de la sumisión del sistema de prueba con todas las recomendaciones de configuración encontradas dentro de los niveles profundos de la prueba de características se calculan esté usando el mismo modelo de lógica como se esboza arriba.

La cuenta a nivel más alto relatada por la herramienta de NG es la cuenta completa (en el color rojo en la vista sumaria del informe de prueba de características). En el informe de muestra sobre la cuenta completa son 58.392 fuera de un posible máximo de 100 puntos.

Cómo usar el informe de prueba de características para identificar los pasos de acción posibles

De la vista sumaria del informe de prueba de características es fácil de identificar acciones que pueden ser tomadas en mejorar la configuración de seguridad de su sistema.

Escoja " 3.2 seguridad menor tome forma ".

Escoger este enlace le toma adelantar abajo la página a un mayor estado detallado del " la seguridad menor tome forma " resultados. Usted puede ver ahora específicamente que los artículos y sub los artículos pasado y que fracase. Usted puede el anuncio que existe tres valores posibles aquí:

En espera de una vacante para ascender: Esto significa que la herramienta de NG verificó el artículo y encuentre que es consistente con la recomendación de prueba de características. La herramienta de NG comprende los conceptos de " igual a ", " mayor que " , y " menos de" esto significa que un artículo, sub el artículo pase si ello sirve para o más seguro que la recomendación.

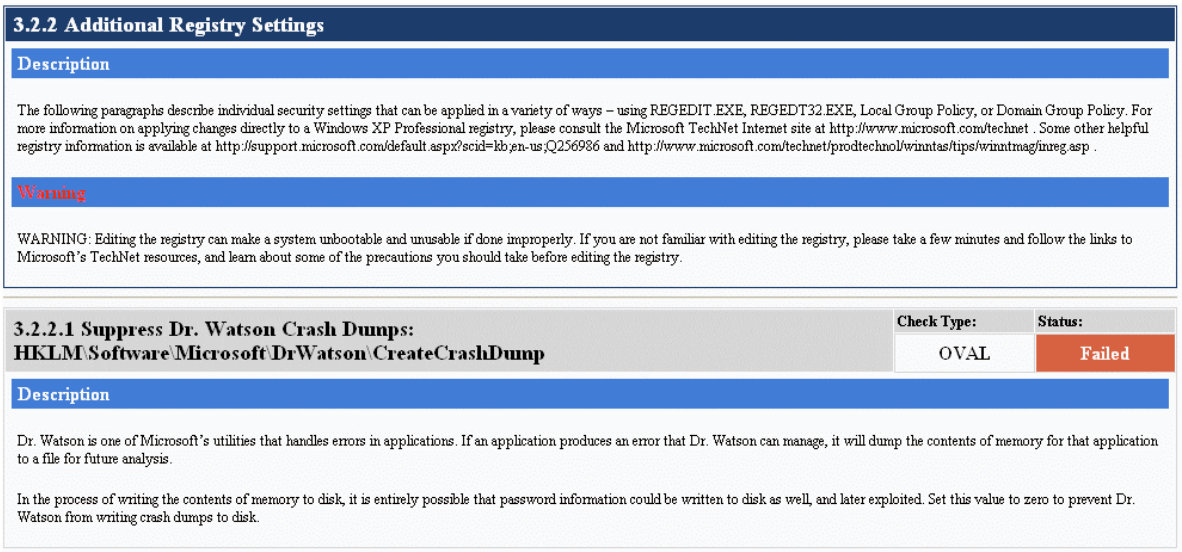
Suspendido: Esto significa que la herramienta de NG verificó el artículo o sub ítem y encuentre que no es dócil con la recomendación de prueba de características. Específicamente, ello no era igual a o es menos seguro.

No examine: Dentro de cada nivel de la prueba de características, existe varias colocaciones que tienen un valor recomendado de " no defina ". Esto ocurre más frecuentemente cuando el valor implícito del sistema operativo es considerado para ser seguro, o si el artículo o sub el artículo es simplemente demasiado complejo o subjetivo para recomendar un valor. En estos casos, la herramienta de NG no probará la colocación y anuncie " no examine."

3.2 Minor Security Settings	
3.2.1 Security Options	
3.2.1.1 Accounts: Administrator Account Status	Not Tested
3.2.1.2 Accounts: Guest Account Status	Passed
3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only	Passed
3.2.1.4 Accounts: Rename Administrator Account	Failed
3.2.1.5 Accounts: Rename Guest Account	Failed
3.2.1.6 Audit: Audit the access of global system objects	Not Tested
3.2.1.7 Audit: Audit the use of backup and restore privilege	Not Tested
3.2.1.8 Audit: Shut Down system immediately if unable to log security alerts	Not Tested
3.2.1.9 DCOM: Machine Access Restrictions	Not Tested
3.2.1.10 DCOM: Machine Launch Restrictions	Not Tested
3.2.1.11 Devices: Allow undock without having to log on	Not Tested
3.2.1.12 Devices: Allowed to format and eject removable media	Passed
3.2.1.13 Devices: Prevent users from installing printer drivers	Failed
3.2.1.14 Devices: Restrict CD-ROM Access to Locally Logged-On User Only	Not Tested
3.2.1.15 Devices: Restrict Floppy Access to Locally Logged-On User Only	Not Tested
3.2.1.16 Devices: Unsigned Driver Installation Behavior	Passed
3.2.1.17 Domain Controller: Allow Server Operators to Schedule Tasks	Not Tested
3.2.1.18 Domain Controller: LDAP Server Signing Requirements	Not Tested
3.2.1.19 Domain Controller: Refuse machine account password changes	Not Tested
3.2.1.20 Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	Passed
3.2.1.21 Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Passed
3.2.1.22 Domain Member: Digitally Sign Secure Channel Data (When Possible)	Passed
3.2.1.23 Domain Member: Disable Machine Account Password Changes	Passed
3.2.1.24 Domain Member: Maximum Machine Account Password Age	Passed
3.2.1.25 Domain Member: Require Strong (Windows 2000 or later) Session Key	Failed
3.2.1.26 Interactive Logon: Do Not Display Last User Name	Failed
3.2.1.27 Interactive Logon: Do not require CTRL+ALT+DEL	Passed
3.2.1.28 Interactive Logon: Message Text for Users Attempting to Log On	Failed
3.2.1.29 Interactive Logon: Message Title for Users Attempting to Log On	Failed
3.2.1.30 Interactive Logon: Number of Previous Logons to Cache	Failed
3.2.1.31 Interactive Logon: Prompt User to Change Password Before Expiration	Passed
3.2.1.32 Interactive Logon: Require Domain Controller authentication to unlock workstation	Failed
3.2.1.33 Interactive Logon: Smart Card Removal Behavior	Failed
3.2.1.34 Microsoft Network Client: Digitally sign communications (always)	Failed
3.2.1.35 Microsoft Network Client: Digitally sign communications (if server agrees)	Passed
3.2.1.36 Microsoft Network Client: Send Unencrypted Password to Connect to Third-Part SMB Server	Passed
3.2.1.37 Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session	Passed
3.2.1.38 Microsoft Network Server: Digitally sign communications (always)	Failed
3.2.1.39 Microsoft Network Server: Digitally sign communications (if client agrees)	Failed
3.2.1.40 Microsoft Network Server: Disconnect clients when logon hours expire	Passed

Escoger un artículo individual tomará le a otra sección del informe que proporciona el detalle sobre ese específico ítem, incluyendo texto del documento real de prueba de

características. Este texto discute la pertinencia de seguridad de ese ítem y pueda proporcionar cierta guía en porque deba poner ello al valor recomendado. Por ejemplo, desplace abajo y haga clic en ítem " 3.2.2.1: Suprima Dr. Watson Crash Dumps".



3.2.2 Additional Registry Settings

Description

The following paragraphs describe individual security settings that can be applied in a variety of ways – using REGEDIT.EXE, REGEDT32.EXE, Local Group Policy, or Domain Group Policy. For more information on applying changes directly to a Windows XP Professional registry, please consult the Microsoft TechNet Internet site at http://www.microsoft.com/technet . Some other helpful registry information is available at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q256986 and http://www.microsoft.com/technet/prodtechnol/winntas/tips/winntmag/inreg.asp .

Warning

WARNING: Editing the registry can make a system unbootable and unusable if done improperly. If you are not familiar with editing the registry, please take a few minutes and follow the links to Microsoft's TechNet resources, and learn about some of the precautions you should take before editing the registry.

3.2.2.1 Suppress Dr. Watson Crash Dumps:
HKLM\Software\Microsoft\DrWatson\CreateCrashDump

Check Type:	Status:
OVAL	Failed

Description

Dr. Watson is one of Microsoft's utilities that handles errors in applications. If an application produces an error that Dr. Watson can manage, it will dump the contents of memory for that application to a file for future analysis.

In the process of writing the contents of memory to disk, it is entirely possible that password information could be written to disk as well, and later exploited. Set this value to zero to prevent Dr. Watson from writing crash dumps to disk.

El anuncio que en el texto de encabezamiento de sección existe una "advertencia" mostró. Esto indica la información importante ése se debe escuchar por el lector. Esto misma información está en la prueba de características se documenta.

Para cada artículo o sub artículo, usted verá un nombre, descripción, y pase/suspenda estatus. Verá también un campo de "tipo de verificación". Allí están tres valores posibles para esto: OVAL, cuestionario, y ninguno.

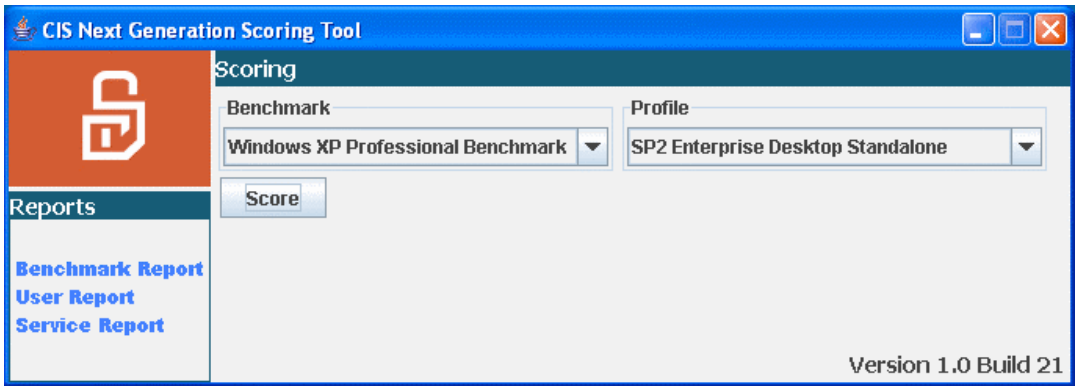
ÓVALO: Esto significa que la herramienta de NG tiene la información necesaria para ejecutado una verificación de esta colocación de forma automática.

Cuestionario: Esto significa que la herramienta de NG es la verificación incapaz el valor de forma automática, así estatus del artículo o sub el artículo es pedido en tiempo de ejecución de herramienta por la via de una respuesta de usuario a una pregunta de cuestionario.

Ninguno: Esto significa que la herramienta de NG no está verificando el artículo o sub ítem y el campo correspondiente de "estatus" lea " no examine ". Como mencione sobre, esto significa más comúnmente que el artículo o sub el artículo es " no defina ".

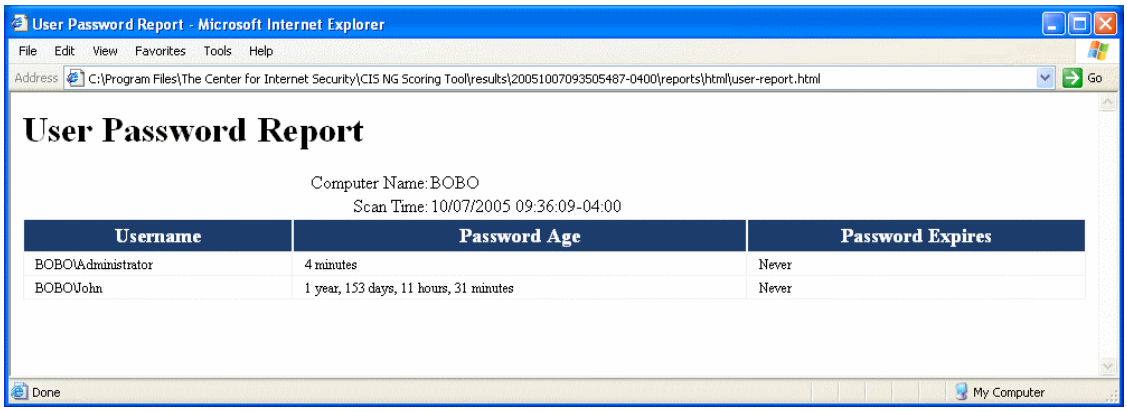
Esté repasando esta información, usted puede aprender sobre los aspectos importantes de su configuración de protección del sistema y cómo mejorarlo.

Permítanos volver y echar una mirada a los otros dos informes. Vuelva a las ventana de herramienta de NG y clic principales en "informe de usuario", localizado sólo debajo del "informe de prueba de características" en la esquina izquierda inferior de la ventana.



Una parte importante de tener un sistema seguro está haciendo seguro eses usuarios sólo autorizados tienen acceso al sistema, así como hacer ciertos eses esos usuarios sigue el bien se adiestra al poner y renovar sus contraseñas.

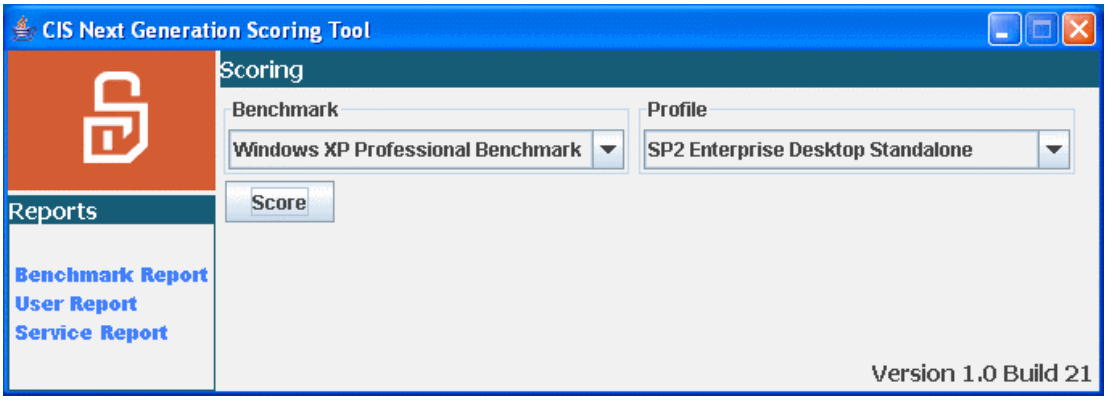
Este informe mostrará usted cada cuenta de usuario en su sistema así como cuánto tiempo ha sido después que cambiaron su contraseña.



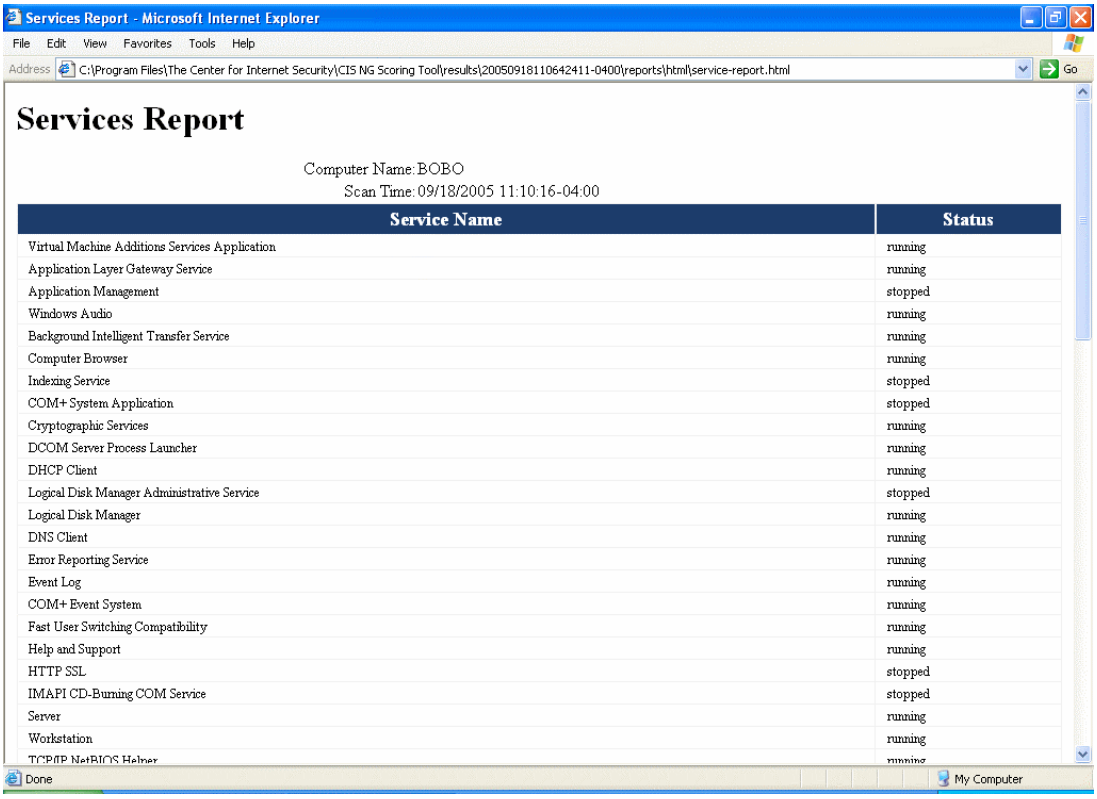
Usted notará en el ejemplo anterior que existe dos cuentas en este sistema.

La contraseña de la cuenta de administrador ha sido cambiada recientemente, que es bueno. Sin embargo, la cuenta de John ha tenido la misma contraseña para bien sobre los 1 años. Esta es la seguridad mala adiestre se. Vea la sección 2.1 de la prueba de características de Windows XP para más información.

Parte posterior en la ventana de herramienta de NG principal, hace clic en " servicios anuncie ".



Muchas vulnerabilidades de seguridad se pueden atribuir a servicios que corren sobre los sistemas de computadora. Estos servicios pudieron ser de alguna importancia como un servidor Web, participación de archivo, o aún un servicio que hacen un índice de sus archivos para rápidamente penetrante. La práctica de seguridad buena requiere que usted inhabilita todos los servicios que no es absolutamente necesario para esa la operación diaria de sistema.



Este informe es diseñado para la exhibición lo que atienden está instalado en su sistema, y si o no se habilitan o inhabilitan. La prueba de características proporciona guía en lo que

los servicios deben ser incapacitados a fin de mejorar seguridad. Esta guía se puede proporcionar en la sección 4.1 de la prueba de características.

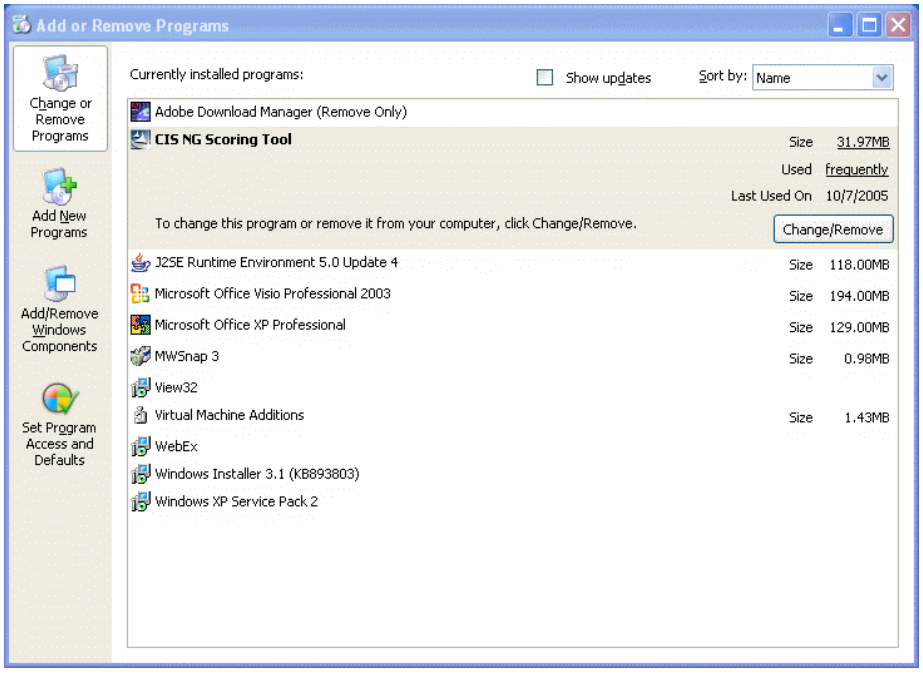
Los informe de servicios muestran que usted el estado de todos los servicios instalado en su sistema. Esto es útil al determinar si no-necesidad fundamental o los servicios inesperados son instaladas y/o corredoras en su sistema.

Cada vez corre la herramienta de NG, un nuevo directorio de tiempo sellado es creado en los "resultados" el directorio. Esto le permite para seguir la pista de manualmente el estatus de su sistema con el transcurso del tiempo. Los beneficios de la calidad de miembro de CIS incluyen el derecho para recibir un tablero de instrumentos añadido eses agregados tantean de anfitriones múltiples, relatan tendencias con el transcurso del tiempo, y crean los informes comprensivos para la organización entera del miembro.

Desinstalar la herramienta de marcado de NG en Windows

Para quitar la herramienta de NG, use simplemente la omisión Windows añadir / quitar programe funcionalidad.

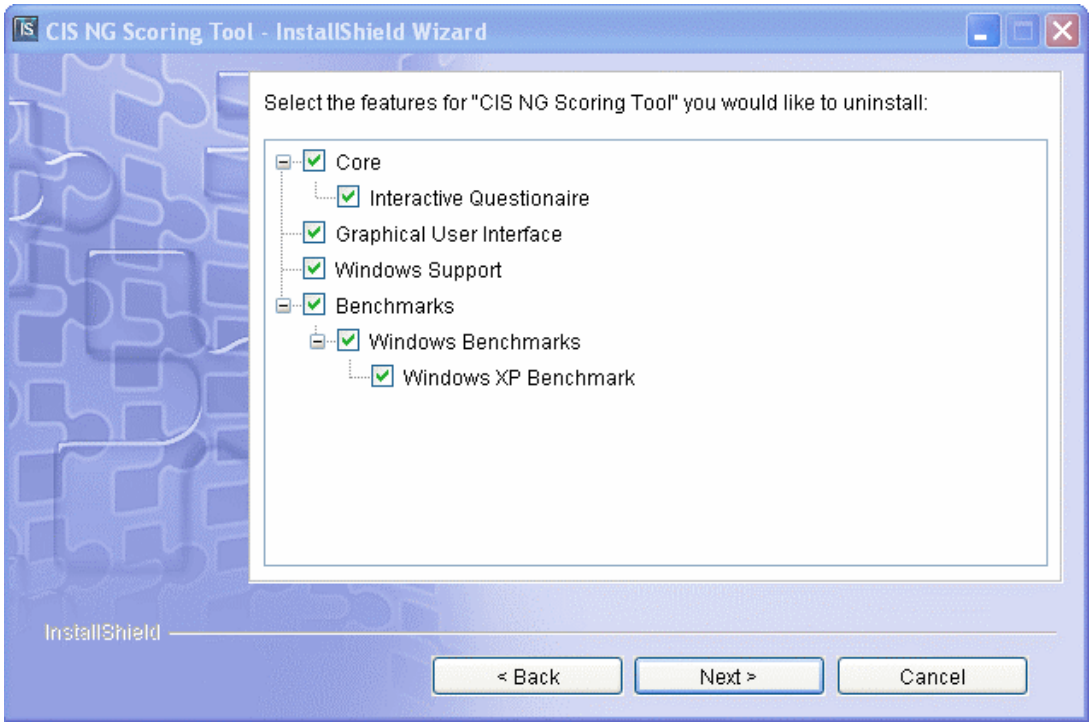
Clic en Start- > Panel de Control y entonces golpee dos veces la tecla del Ratón sobre en el " añadir / quitar los programas " icono. Esta lanzará una ventana similar a éste:



Por favor, note que la lista de le programan ver en esta ventana diferencie de un sistema al próximo. En cada caso, localice la línea de "herramienta de marcado de CIS NG", realce

sobre, y haga clic en " cambie/quite ".

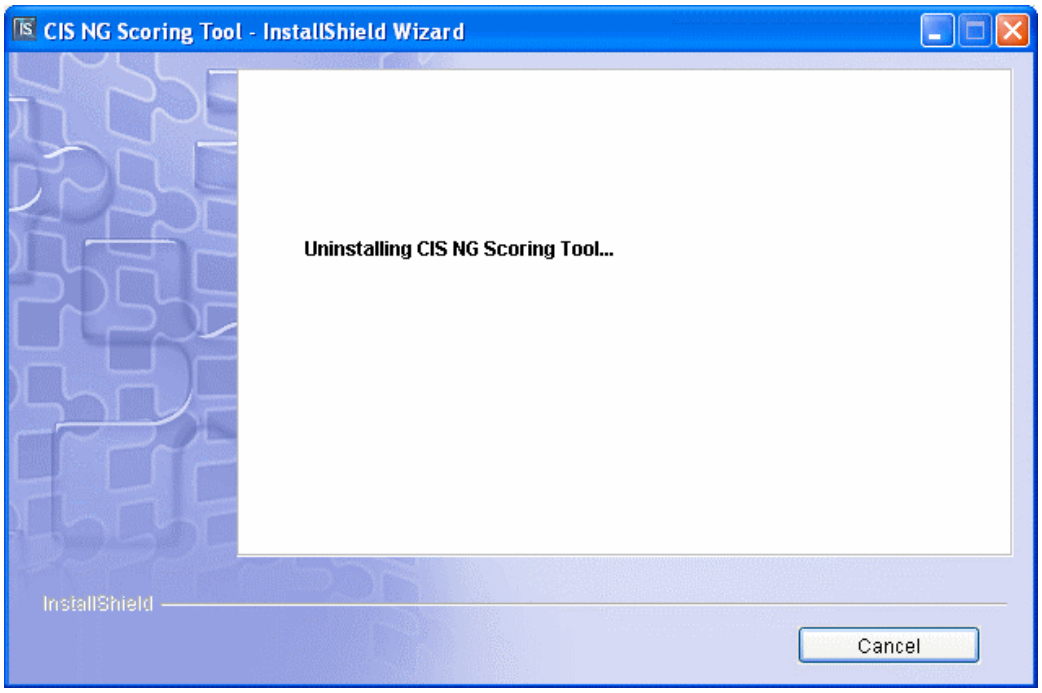
Esto lanzará el mismo programa de instalador acostumbró a instalar la herramienta de NG. En la pantalla primera, haga clic sobre "próximo". Verá ahora una lista de componentes que puede ser quitada:



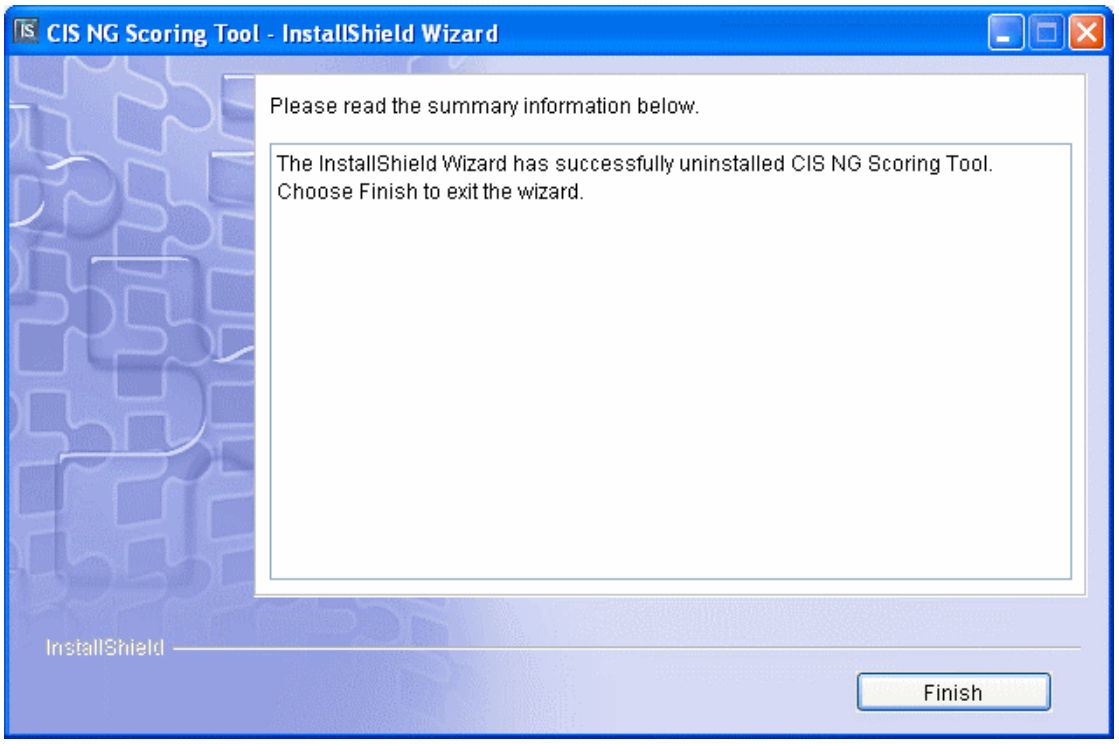
Verifique que cada componente es verificado y haga clic sobre "próximo". Por favor, note que puede uncheck ciertos componentes, con eso dejando detrás de ciertas partes de la herramienta de NG. Sin embargo, no existe ninguna razón hacer así en este momento y nosotros recomendamos quitar la herramienta de NG entera.

La pantalla próxima simplemente resume lo que quite se. Clic en "desinstalar" para quitar la herramienta de NG.

El desintalador mostrará lo siguiente pantalla:



Cuando la instalación ha terminado, haga clic en el botón "terminado":



Corrientemente, el programa de uninstall no quita los reales directamente donde la

herramienta de NG era instalada. Específicamente, sale detrás del "resultado" directamente y un archivo de tronco. Si usted es cierto le ya no necesitar la herramienta de NG anuncia en este sistema, puede quitar el directorio arrastrando lo en la arca de Recycle " o borrando lo.

En rebeldía, la herramienta de NG es situada en " c:\Programe centro Files\The para seguridad de Internet ".

Está a salvo para dejar este directorio en su sistema y requiere che muy poco espacio en disco.

Cómo ver el Registro del sistema en las versiones de 64 bits de Windows

El Registro en las versiones de 64 bits de Windows se divide en claves de 32 bits y de 64 bits. Muchas de las claves de 32 bits tienen los mismos nombres que sus homólogas de 64 bits y viceversa.

La versión de 64 bits predeterminada del Editor del Registro (Regedit.exe) que se incluye con las versiones de 64 bits de Windows muestra las claves de 64 bits y de 32 bits. El redirector del Registro de WOW64 presenta a los programas de 32 bits claves diferentes para las entradas del Registro correspondientes a programas de 32 bits. En la versión de 64 bits del Editor del Registro, las claves de 32 bits se muestran bajo la clave del Registro siguiente:

HKEY_LOCAL_MACHINE\Software\WOW6432Node

Puede ver o editar las claves y valores del Registro de 64 y de 32 bits utilizando la versión de 64 bits predeterminada del Editor del Registro. Para ver o editar las claves de 64 bits, debe utilizar la versión de 64 bits del Editor del Registro (Regedit.exe). También puede ver o editar las claves y valores de 32 bits utilizando la versión de 32 bits del Editor del Registro en la carpeta %systemroot%\Syswow64. No hay ninguna diferencia en la manera en que se realizan las tareas en las versiones de 32 y de 64 bits del Editor del Registro. Para abrir la versión de 32 bits de Editor del Registro, siga estos pasos:

1. Haga clic en **Inicio** y, a continuación, en **Ejecutar**.
2. En el cuadro **Abrir**, escriba **%systemroot%\syswow64\regedit** y haga clic en **Aceptar**.

   Nota:

   Debe cerrar la versión de 64 bits del Editor del Registro para poder abrir la de 32 bits (y viceversa) a menos que inicie la segunda sesión del Editor del Registro con el modificador **-m**. Por ejemplo, si la versión de 64 bits del Editor del Registro ya se está ejecutando, escriba **%systemroot%\syswow64\regedit -m** en el paso 2 para iniciar la versión de 32 bits del Editor del Registro.

Para permitir la coexistencia del registro COM de 32 y de 64 bits, y los estados de los programas, WOW64 presenta a los programas de 32 bits una vista alternativa del Registro. Los programas de 32 bits ven un árbol **HKEY_LOCAL_MACHINE\Software** de 32 bits (**HKEY_LOCAL_MACHINE\Software\WOW6432Node**) que es completamente diferente del verdadero árbol **HKEY_LOCAL_MACHINE\Software** de 64 bits. De esta forma se aísla a **HKEY_CLASSES_ROOT**, porque la parte correspondiente a cada equipo de este árbol reside dentro de la clave del Registro siguiente:

HKEY_LOCAL_MACHINE\Software

Para habilitar la interoperabilidad de los programas de 64 y 32 bits a través de COM y otros mecanismos, WOW64 utiliza un "reflector del Registro" que refleja ciertas claves y valores del Registro entre las vistas del Registro de 64 y de 32 bits. El reflector es "inteligente" ya que sólo refleja los datos de activación de COM.

Claves reflejadas

El reflector del Registro de WOW64 puede modificar el contenido de las claves y valores durante el proceso de reflexión para ajustar los nombres de rutas de acceso, etcétera.

Debido a esto, el contenido de 32 bits y de 64 bits puede diferir. Se reflejan las claves siguientes:

- **HKEY_LOCAL_MACHINE\Software\Classes**
- **HKEY_LOCAL_MACHINE\Software\COM3**
- **HKEY_LOCAL_MACHINE\Software\Ole**
- **HKEY_LOCAL_MACHINE\Software\EventSystem**
- **HKEY_LOCAL_MACHINE\Software\RPC**

La información de este artículo se refiere a:

- Microsoft Windows Server 2003, 64-Bit Datacenter Edition
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Advanced Server, Limited Edition

ANEXO B. ARCHIVOS PARA CORRECIÓN DE VULNERABILIDADES EN REGEDIT

i. ARCHIVO PARA CORRECCIÓN POR CÓDIGO WINDOWS XP

COMPUTADOR TIPO

Home

```
[Profile Description]
Description=NIST Windows XP Professional Legacy Security Settings
[Version]
signature="$CHICAGO$"
Revision=1
[Unicode]
Unicode=yes
[System Access]
; 1.1 - Enforce password history  (Apply at the domain level)
PasswordHistorySize = 24
; 1.2 - Maximum password age (Apply at the domain level)
MaximumPasswordAge = 90
; 1.3 - Minimum password age (Apply at the domain level)
MinimumPasswordAge = 1
; 1.4 - Minimum password length (Apply at the domain level)
MinimumPasswordLength = 8
; 1.5 - Passwords must meet complexity requirements (Apply at the domain level)
PasswordComplexity = 1
; 1.6 - Store password using reversible encryption for all users in the domain (Apply at the domain level)
ClearTextPassword = 0
; 2.1 - Account lockout duration (Apply at the domain level)
LockoutDuration = 15
; 2.2 - Account lockout threshold (Apply at the domain level)
LockoutBadCount = 50
; 2.3 - Reset account lockout counter after (Apply at the domain level)
ResetLockoutCount = 15
; 5.1 - Accounts: Administrator account status
EnableAdminAccount = 1
; 5.2 - Accounts: Guest account status (Security Options)
EnableGuestAccount = 0
; 5.43 - Network access: Allow anonymous SID/Name translation  (Apply at the domain level)
LSAAnonymousNameLookup = 0
; 5.54 - Network security: Force logoff when logon hours expire (Apply at the domain level)
ForceLogoffWhenHourExpire = 1
[System Log]
; 6.3 - Maximum system log size
MaximumLogSize = 16384
; 6.6 - Prevent local guests group from accessing system log
RestrictGuestAccess = 1
; 6.12 - Retention method for system log
AuditLogRetentionPeriod = 0
[Security Log]
; 6.2 - Maximum security log size
MaximumLogSize = 81920
; 6.5 - Prevent local guests group from accessing security log
RestrictGuestAccess = 1
; 6.11 - Retention method for security log
AuditLogRetentionPeriod = 0
[Application Log]
; 6.1 - Maximum application log size
MaximumLogSize = 16384
; 6.4 - Prevent local guests group from accessing application log
RestrictGuestAccess = 1
; 6.10 - Retention method for application log
AuditLogRetentionPeriod = 0
[Event Audit]
; 3.1 - Audit account logon events
AuditLogonEvents = 1
; 3.2 - Audit account management
AuditAccountManage = 1
; 3.4 - Audit logon events
AuditAccountLogon = 1
; 3.5 - Audit object access
AuditObjectAccess = 0
; 3.6 - Audit policy change
```

```
AuditPolicyChange = 1
; 3.7 - Audit privilege use
AuditPrivilegeUse = 0
; 3.8 - Audit process tracking
AuditProcessTracking = 0
; 3.9 - Audit system events
AuditSystemEvents = 1
;-----------------------------------------------------------------
;Valores de Registro
;-----------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                ( 1 )
; REG_EXPAND_SZ         ( 2 )  // with environment variables to expand
; REG_BINARY            ( 3 )
; REG_DWORD             ( 4 )
; REG_MULTI_SZ          ( 7 )
[Registry Values]
; 5.3 - Accounts: Limit local account use of blank passwords to console logon only
MACHINE\System\Currentcontrolset\Control\Lsa\Limitblankpasswordуse=4,1
; 5.12 - Devices: Allowed to format and eject removable media
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"2"
; 5.13 - Devices: Prevent users from installing printer drivers
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1
; 5.16 - Devices: Unsigned driver installation behavior
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
; 5.20 - Domain Member: Digitally encrypt or sign secure channel data (always)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
; 5.21 - Domain Member: Digitally encrypt secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
; 5.22 - Domain Member: Digitally sign secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
; 5.23 - Domain Member: Disable machine account password changes
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
; 5.24 - Domain Member: Maximum machine account password age
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,30
; 5.25 - Domain Member:  Require Strong (Windows 2000 or later) Session Key
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,0
; 5.27 - Interactive logon: Do not display last user name
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
; 5.28 - Interactive logon: Do not require CTRL+ALT+DEL
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
; 5.29 - Interactive logon: Message text for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,This system is for the use of authorized users only. Individuals using this computer system without authority"," or in excess of their authority"," are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity"," system personal may provide the evidence of such monitoring to law enforcement officials.
; 5.30 - Interactive logon: Message title for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"-- WARNING --"
; 5.31 - Interactive logon: Number of previous logons to cache (in case domain controller is not available)
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"2"
; 5.32 - Interactive logon: Prompt user to change password before expiration
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
; 5.33 - Interactive logon: Require Domain Controller authentication to unlock workstation
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=4,1
; 5.35 - Interactive logon: Smart card removal behavior
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"
; 5.36 - Microsoft network client: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,0
; 5.37 - Microsoft network client: Digitally sign communications (if server agrees)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
; 5.38 - Microsoft network client: Send unencrypted password to third-party SMB servers
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
; 5.39 - Microsoft network server: Amount of idle time required before suspending session
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
```

```
; 5.40 - Microsoft network server: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
; 5.41 - Microsoft network server: Digitally sign  communication (if client agrees)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
; 5.42 - Microsoft network server: Disconnect clients when logon hours expire (Apply at the domain level)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
; 5.44 - Network access: Do not allow anonymous enumeration of SAM accounts
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
; 5.45 - Network access: Do not allow anonymous enumeration of SAM accounts and shares
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
; 5.46 - Network access: Do not allow storage of credentials or .NET Passports for network authentication
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
; 5.47 Network access: Let Everyone permissions apply to anonymous users
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
; 5.52 - Network access: Sharing and security model for local accounts
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0
; 5.53 - Network security: Do not store LAN Manager hash value on next password change
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
; 5.55 - Network security: LAN Manager Authentication Level
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4
; 5.56 - Network security: LDAP client signing requirements
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1
; 5.57 - Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248
; 5.58 - Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248
; 5.59 - Recovery Console: Allow automatic administrative logon
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
; 5.62 - Shutdown: Clear virtual memory pagefile
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
; 5.64 - System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1
; 5.65 - System objects: Default owner for objects created by members of the Administrators group
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
; 5.67 - System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
;
; The remaining registry values will not appear in the Security Templates MMC snap-in
;
; 5.79 - MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)
MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt=4,1
; 5.80 - MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
; 5.82 - MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
; 5.84 - MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode=4,1
; 5.85 - MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)
MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=4,0
[Privilege Rights]
; 4.2 - Act as part of the operating system
SeTcbPrivilege =
; 4.3 - Add workstations to domain (Apply at the domain level)
SeMachineAccountPrivilege = Administrators
; 4.5 - Allow log on locally
SeInteractiveLogonRight = Users,Administrators
; 4.9 - Change the system time
SeSystemtimePrivilege = Administrators
; 4.10 - Create a pagefile
SeCreatePagefilePrivilege = Administrators
; 4.14 - Debug programs (require by some MS installer programs use to install MS hotfixes)
SeDebugPrivilege = Administrators
; 4.15 - Deny access to this computer from the network
SeDenyNetworkLogonRight = Guests,Support_388945a0
; 4.21 - Force shutdown from a remote system
```

```
SeRemoteShutdownPrivilege = Administrators
; 4.22 - Generate security audits
SeAuditPrivilege = *S-1-5-19,*S-1-5-20
; 4.24 - Increase scheduling priority
SeIncreaseBasePriorityPrivilege = Administrators
; 4.25 - Load and unload device drivers
SeLoadDriverPrivilege = Administrators
; 4.26 - Lock pages in memory
SeLockMemoryPrivilege =
; 4.29 - Manage auditing and security log
SeSecurityPrivilege = Administrators
; 4.30 - Modify firmware environment values
SeSystemEnvironmentPrivilege = Administrators
; 4.31 - Perform Volume Maintenance Task
SeManageVolumePrivilege = Administrators
; 4.33 - Profile system performance
SeSystemProfilePrivilege = Administrators
; 4.34 - Remove computer from docking station
SeUndockPrivilege = Administrators,Users
; 4.35 - Replace a process level token
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
; 4.37 - Shut down the system
SeShutdownPrivilege = Administrators,Users
; 4.39 - Take ownership of files or other objects
SeTakeOwnershipPrivilege = Administrators
[Group Membership]
; 7.1 - Backup Operators
Backup Operators__Memberof =
Backup Operators__Members =
; 7.2 - Power Users
Power Users__Memberof =
Power Users__Members =
[File Security]
; 9.1 - arp.exe
"%SystemRoot%\System32\arp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.2 - at.exe
"%SystemRoot%\System32\at.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.3 - attrib.exe
"%SystemRoot%\System32\attrib.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.4 - cacls.exe
"%SystemRoot%\System32\cacls.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.5 - debug.exe
"%SystemRoot%\System32\debug.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.6 - edlin.exe
"%SystemRoot%\System32\edlin.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.7 - eventcreate.exe
"%SystemRoot%\System32\eventcreate.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.8 - eventtriggers.exe
"%SystemRoot%\System32\eventtriggers.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.9 - ftp.exe
"%SystemRoot%\system32\ftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.10 - nbtstat.exe
"%SystemRoot%\System32\nbtstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.11 - net.exe
"%SystemRoot%\system32\net.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.12 - net1.exe
"%SystemRoot%\system32\net1.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.13 - netsh.exe
"%SystemRoot%\system32\netsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.14 - netstat.exe
"%systemRoot%\System32\netstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.15 - nslookup.exe
"%SystemRoot%\System32\nslookup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.16 - ntbackup.exe
"%SystemRoot%\System32\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
```

```
; 9.17 - rcp.exe
"%SystemRoot%\system32\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.18 - reg.exe
"%SystemRoot%\system32\reg.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.19 - regedit.exe
"%SystemRoot%\system32\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.20 - regedt32.exe
"%SystemRoot%\system32\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.21 - regini.exe
"%SystemRoot%\System32\regini.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.22 - regsvr32.exe
"%SystemRoot%\system32\regsvr32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.23 - rexec.exe
"%SystemRoot%\system32\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.24 - route.exe
"%SystemRoot%\system32\route.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.25 - rsh.exe
"%SystemRoot%\system32\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.26 - sc.exe
"%SystemRoot%\system32\sc.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.27 - secedit.exe
"%SystemRoot%\System32\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.28 - subst.exe
"%SystemRoot%\system32\subst.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.29 - systeminfo.exe
"%SystemRoot%\System32\systeminfo.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.30 - telnet.exe
"%SystemRoot%\system32\telnet.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.31 - tftp.exe
"%SystemRoot%\system32\tftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.32 - tlntsvr.exe
"%SystemRoot%\system32\tlntsvr.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
[Service General Setting]
; 8.1 - Alerter
Alerter,4,""
; 8.6 - ClipBook
ClipSrv,4,""
; 8.19 - FTP Publishing Service
MSFtpsvc,4,""
; 8.22 - IIS Admin Service
IISADMIN,4,""
; 8.30 - Messenger
Messenger,4,""
; 8.33 - NetMeeting Remote Desktop Sharing
mnmsrvc,4,""
; 8.52 - Routing and Remote Access
RemoteAccess,4,""
; 8.59 - SMTPSVC (Simple Mail Transfer Protocol)
SMTPSVC,4,""
; 8.60 - SNMP
SNMP,4,""
; 8.61 - SNMPTRAP
SNMPTRAP,4,""
; 8.62 - SSDP Discovery Service
SSDPSRV,4,""
; 8.68 - Telnet
TlntSvr,4,""
; 8.85 - World Wide Web Publising Services
W3SVC,4,""
```

Computadora de escritorio en la empresa

```
[Profile Description]
Description=NIST Windows XP Professional Enterprise Security Settings
[Version]
signature="$CHICAGO$"
Revision=1
 [Unicode]
Unicode=yes
[System Access]
; 1.1 - Enforce password history (Apply at the domain level)
PasswordHistorySize = 24
; 1.2 - Maximum password age (Apply at the domain level)
MaximumPasswordAge = 90
; 1.3 - Minimum password age (Apply at the domain level)
MinimumPasswordAge = 1
; 1.4 - Minimum password length (Apply at the domain level)
MinimumPasswordLength = 8
; 1.5 - Passwords must meet complexity requirements (Apply at the domain level)
PasswordComplexity = 1
; 1.6 - Store password using reversible encryption for all users in the domain (Apply at the domain level)
ClearTextPassword = 0
; 2.1 - Account lockout duration (Apply at the domain level)
LockoutDuration = 15
; 2.2 - Account lockout threshold (Apply at the domain level)
LockoutBadCount = 50
; 2.3 - Reset account lockout counter after (Apply at the domain level)
ResetLockoutCount = 15
; 5.2 - Accounts: Guest account status (Security Options)
EnableGuestAccount = 0
; 5.43 - Network access: Allow anonymous SID/Name translation (Apply at the domain level)
LSAAnonymousNameLookup = 0
; 5.54 - Network security: Force logoff when logon hours expire (Apply at the domain level)
ForceLogoffWhenHourExpire = 1
[System Log]
; 6.3 - Maximum system log size
MaximumLogSize = 16384
; 6.6 - Prevent local guests group from accessing system log
RestrictGuestAccess = 1
; 6.12 - Retention method for system log
AuditLogRetentionPeriod = 0
[Security Log]
; 6.2 - Maximum security log size
MaximumLogSize = 81920
; 6.5 - Prevent local guests group from accessing security log
RestrictGuestAccess = 1
; 6.11 - Retention method for security log
AuditLogRetentionPeriod = 0
[Application Log]
; 6.1 - Maximum application log size
MaximumLogSize = 16384
; 6.4 - Prevent local guests group from accessing application log
RestrictGuestAccess = 1
```

```
; 6.10 - Retention method for application log
AuditLogRetentionPeriod = 0
[Event Audit]
; 3.1 - Audit account logon events
AuditLogonEvents = 1
; 3.2 - Audit account management
AuditAccountManage = 1
; 3.4 - Audit logon events
AuditAccountLogon = 1
; 3.5 - Audit object access
AuditObjectAccess = 0
; 3.6 - Audit policy change
AuditPolicyChange = 1
; 3.7 - Audit privilege use
AuditPrivilegeUse = 0
; 3.8 - Audit process tracking
AuditProcessTracking = 0
; 3.9 - Audit system events
AuditSystemEvents = 1
;-----------------------------------------------------------------------
;Valores de Registro
; Registry value name in full path = Type, Value
; REG_SZ                ( 1 )
; REG_EXPAND_SZ         ( 2 )  // with environment variables to expand
; REG_BINARY            ( 3 )
; REG_DWORD             ( 4 )
; REG_MULTI_SZ          ( 7 )
[Registry Values]
; 5.3 - Accounts: Limit local account use of blank passwords to console logon only
MACHINE\System\Currentcontrolset\Control\Lsa\Limitblankpassworduse=4,1
; 5.12 - Devices: Allowed to format and eject removable media
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"2"
; 5.13 - Devices: Prevent users from installing printer drivers
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1
; 5.16 - Devices: Unsigned driver installation behavior
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
; 5.20 - Domain Member: Digitally encrypt or sign secure channel data (always)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
; 5.21 - Domain Member: Digitally encrypt secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
; 5.22 - Domain Member: Digitally sign secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
; 5.23 - Domain Member: Disable machine account password changes
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
; 5.24 - Domain Member: Maximum machine account password age
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,30
; 5.25 - Domain Member:  Require Strong (Windows 2000 or later) Session Key
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
; 5.27 - Interactive logon: Do not display last user name
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
; 5.28 - Interactive logon: Do not require CTRL+ALT+DEL
```

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
; 5.29 - Interactive logon: Message text for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,This system is for the use of authorized users only. Individuals using this computer system without authority"," or in excess of their authority"," are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity"," system personal may provide the evidence of such monitoring to law enforcement officials.
; 5.30 - Interactive logon: Message title for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"-- WARNING --"
; 5.31 - Interactive logon: Number of previous logons to cache (in case domain controller is not available)
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"2"
; 5.32 - Interactive logon: Prompt user to change password before expiration
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
; 5.33 - Interactive logon: Require Domain Controller authentication to unlock workstation
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=4,1
; 5.35 - Interactive logon: Smart card removal behavior
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"
; 5.36 - Microsoft network client: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,1
; 5.37 - Microsoft network client: Digitally sign communications (if server agrees)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
; 5.38 - Microsoft network client: Send unencrypted password to third-party SMB servers
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
; 5.39 - Microsoft network server: Amount of idle time required before suspending session
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
; 5.40 - Microsoft network server: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
; 5.41 - Microsoft network server: Digitally sign communication (if client agrees)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
; 5.42 - Microsoft network server: Disconnect clients when logon hours expire (Apply at the domain level)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
; 5.44 - Network access: Do not allow anonymous enumeration of SAM accounts
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
; 5.45 - Network access: Do not allow anonymous enumeration of SAM accounts and shares
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
; 5.46 - Network access: Do not allow storage of credentials or .NET Passports for network authentication
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
; 5.47 Network access: Let Everyone permissions apply to anonymous users
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
; 5.52 - Network access: Sharing and security model for local accounts
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0
; 5.53 - Network security: Do not store LAN Manager hash value on next password change
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
; 5.55 - Network security: LAN Manager Authentication Level
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4
; 5.56 - Network security: LDAP client signing requirements
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1
; 5.57 - Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248
; 5.58 - Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248

```
; 5.59 - Recovery Console: Allow automatic administrative logon
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
; 5.62 - Shutdown: Clear virtual memory pagefile
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
; 5.64 - System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1
; 5.65 - System objects: Default owner for objects created by members of the Administrators group
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
; 5.67 - System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
; 5.79 - MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)
MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt=4,1
; 5.80 - MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
; 5.84 - MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode=4,1
; 5.85 - MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)
MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=4,0
[Privilege Rights]
; 4.2 - Act as part of the operating system
SeTcbPrivilege =
; 4.3 - Add workstations to domain (Apply at the domain level)
SeMachineAccountPrivilege = Administrators
; 4.5 - Allow log on locally
SeInteractiveLogonRight = Users,Administrators
; 4.9 - Change the system time
SeSystemtimePrivilege = Administrators
; 4.10 - Create a pagefile
SeCreatePagefilePrivilege = Administrators
; 4.14 - Debug programs
SeDebugPrivilege = Administrators
; 4.15 - Deny access to this computer from the network
SeDenyNetworkLogonRight = Guests,Support_388945a0
; 4.21 - Force shutdown from a remote system
SeRemoteShutdownPrivilege = Administrators
; 4.22 - Generate security audits
SeAuditPrivilege = *S-1-5-19,*S-1-5-20
; 4.24 - Increase scheduling priority
SeIncreaseBasePriorityPrivilege = Administrators
; 4.25 - Load and unload device drivers
SeLoadDriverPrivilege = Administrators
; 4.26 - Lock pages in memory
SeLockMemoryPrivilege =
; 4.29 - Manage auditing and security log
SeSecurityPrivilege = Administrators
; 4.30 - Modify firmware environment values
SeSystemEnvironmentPrivilege = Administrators
; 4.31 - Perform volume maintenance tasks
SeManageVolumePrivilege = Administrators
; 4.33 - Profile system performance
SeSystemProfilePrivilege = Administrators
```

```
; 4.34 - Remove computer from docking station
SeUndockPrivilege = Administrators,Users
; 4.35 - Replace a process level token
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
; 4.37 - Shut down the system
SeShutdownPrivilege = Administrators,Users
; 4.39 - Take ownership of files or other objects
SeTakeOwnershipPrivilege = Administrators
[Group Membership]
; 7.1 - Backup Operators
Backup Operators__Memberof =
Backup Operators__Members =
; 7.2 - Power Users
Power Users__Memberof =
Power Users__Members =
[File Security]
; 9.1 - arp.exe
"%SystemRoot%\System32\arp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.2 - at.exe
"%SystemRoot%\System32\at.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.3 - attrib.exe
"%SystemRoot%\System32\attrib.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.4 - cacls.exe
"%SystemRoot%\System32\cacls.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.5 - debug.exe
"%SystemRoot%\System32\debug.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.6 - edlin.exe
"%SystemRoot%\System32\edlin.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.7 - eventcreate.exe
"%SystemRoot%\System32\eventcreate.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.8 - eventtriggers.exe
"%SystemRoot%\System32\eventtriggers.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.9 - ftp.exe
"%SystemRoot%\system32\ftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.10 - nbtstat.exe
"%SystemRoot%\System32\nbtstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.11 - net.exe
"%SystemRoot%\system32\net.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.12 - net1.exe
"%SystemRoot%\system32\net1.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.13 - netsh.exe
"%SystemRoot%\system32\netsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.14 - netstat.exe
"%systemRoot%\System32\netstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.15 - nslookup.exe
"%SystemRoot%\System32\nslookup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.16 - ntbackup.exe
"%SystemRoot%\System32\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.17 - rcp.exe
"%SystemRoot%\system32\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.18 - reg.exe
```

```
"%SystemRoot%\system32\reg.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.19 - regedit.exe
"%SystemRoot%\system32\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.20 - regedt32.exe
"%SystemRoot%\system32\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.21 - regini.exe
"%SystemRoot%\System32\regini.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.22 - regsvr32.exe
"%SystemRoot%\system32\regsvr32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.23 - rexec.exe
"%SystemRoot%\system32\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.24 - route.exe
"%SystemRoot%\system32\route.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.25 - rsh.exe
"%SystemRoot%\system32\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.26 - sc.exe
"%SystemRoot%\system32\sc.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\subst.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\systeminfo.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\telnet.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\tftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.32 - tlntsvr.exe
"%SystemRoot%\system32\tlntsvr.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
[Service General Setting]
; 8.1 - Alerter
Alerter,4,""
; 8.6 - ClipBook
ClipSrv,4,""
; 8.19 - FTP Publishing Service
MSFtpsvc,4,""
; 8.22 - IIS Admin Service
IISADMIN,4,""
; 8.30 - Messenger
Messenger,4,""
; 8.33 - NetMeeting Remote Desktop Sharing
mnmsrvc,4,""
; 8.52 - Routing and Remote Access
RemoteAccess,4,""
; 8.59 - SMTPSVC (Simple Mail Transfer Protocol)
SMTPSVC,4,""
; 8.60 - SNMP
SNMP,4,""
; 8.61 - SNMPTRAP
SNMPTRAP,4,""
; 8.62 - SSDP Discovery Service
SSDPSRV,4,""
; 8.68 - Telnet
TlntSvr,4,""
; 8.85 - World Wide Web Publising Services
W3SVC,4,""
```

Computador portátil en la empresa

```
[Profile Description]
Description=NIST Windows XP Professional SOHO Security Settings
[Version]
signature="$CHICAGO$"
Revision=1
[Unicode]
Unicode=yes
[System Access]
; 1.1 - Enforce password history (Apply at the domain level)
PasswordHistorySize = 24
; 1.2 - Maximum password age (Apply at the domain level)
MaximumPasswordAge = 90
; 1.3 - Minimum password age (Apply at the domain level)
MinimumPasswordAge = 1
; 1.4 - Minimum password length (Apply at the domain level)
MinimumPasswordLength = 8
; 1.5 - Passwords must meet complexity requirements (Apply at the domain level)
PasswordComplexity = 1
; 1.6 - Store password using reversible encryption for all users in the domain (Apply at the domain level)
ClearTextPassword = 0
; 2.1 - Account lockout duration (Apply at the domain level)
LockoutDuration = 15
; 2.2 - Account lockout threshold (Apply at the domain level)
LockoutBadCount = 50
; 2.3 - Reset account lockout counter after (Apply at the domain level)
ResetLockoutCount = 15
; 5.2 - Accounts: Guest account status (Security Options)
EnableGuestAccount = 0
; 5.43 - Network access: Allow anonymous SID/Name translation (Apply at the domain level)
LSAAnonymousNameLookup = 0
; 5.54 - Network security: Force logoff when logon hours expire (Apply at the domain level)
ForceLogoffWhenHourExpire = 1
[System Log]
; 6.3 - Maximum system log size
MaximumLogSize = 16384
; 6.6 - Prevent local guests group from accessing system log
RestrictGuestAccess = 1
; 6.12 - Retention method for system log
AuditLogRetentionPeriod = 0
[Security Log]
; 6.2 - Maximum security log size
MaximumLogSize = 81920
; 6.5 - Prevent local guests group from accessing security log
RestrictGuestAccess = 1
; 6.11 - Retention method for security log
AuditLogRetentionPeriod = 0
[Application Log]
; 6.1 - Maximum application log size
MaximumLogSize = 16384
; 6.4 - Prevent local guests group from accessing application log
RestrictGuestAccess = 1
; 6.10 - Retention method for application log
AuditLogRetentionPeriod = 0
[Event Audit]
; 3.1 - Audit account logon events
AuditLogonEvents = 1
; 3.2 - Audit account management
AuditAccountManage = 1
; 3.4 - Audit logon events
AuditAccountLogon = 1
; 3.5 - Audit object access
AuditObjectAccess = 0
```

```
; 3.6 - Audit policy change
AuditPolicyChange = 1
; 3.7 - Audit privilege use
AuditPrivilegeUse = 0
; 3.8 - Audit process tracking
AuditProcessTracking = 0
; 3.9 - Audit system events
AuditSystemEvents = 1
;-----------------Valores de registro
; REG_SZ                ( 1 )
; REG_EXPAND_SZ         ( 2 )  // with environment variables to expand
; REG_BINARY            ( 3 )
; REG_DWORD             ( 4 )
; REG_MULTI_SZ          ( 7 )
[Registry Values]
; 5.3 - Accounts: Limit local account use of blank passwords to console logon only
MACHINE\System\Currentcontrolset\Control\Lsa\Limitblankpasswordуse=4,1
; 5.12 - Devices: Allowed to format and eject removable media
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"2"
; 5.13 - Devices: Prevent users from installing printer drivers
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,0
; 5.16 - Devices: Unsigned driver installation behavior
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
; 5.20 - Domain Member: Digitally encrypt or sign secure channel data (always)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
; 5.21 - Domain Member: Digitally encrypt secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
; 5.22 - Domain Member: Digitally sign secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
; 5.23 - Domain Member: Disable machine account password changes
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
; 5.24 - Domain Member: Maximum machine account password age
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,30
; 5.25 - Domain Member:  Require Strong (Windows 2000 or later) Session Key
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
; 5.27 - Interactive logon: Do not display last user name
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
; 5.28 - Interactive logon: Do not require CTRL+ALT+DEL
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
; 5.29 - Interactive logon: Message text for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,This system is for the use of authorized
users only. Individuals using this computer system without authority"," or in excess of their authority"," are subject to having all their
activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring
and is advised that if such monitoring reveals possible evidence of criminal activity"," system personal may provide the evidence of such
monitoring to law enforcement officials.
; 5.30 - Interactive logon: Message title for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"-- WARNING --"
; 5.31 - Interactive logon: Number of previous logons to cache (in case domain controller is not available)
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"2"
; 5.32 - Interactive logon: Prompt user to change password before expiration
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
; 5.33 - Interactive logon: Require Domain Controller authentication to unlock workstation
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=4,0
; 5.35 - Interactive logon: Smart card removal behavior
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"
; 5.36 - Microsoft network client: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,1
; 5.37 - Microsoft network client: Digitally sign communications (if server agrees)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
; 5.38 - Microsoft network client: Send unencrypted password to third-party SMB servers
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
; 5.39 - Microsoft network server: Amount of idle time required before suspending session
```

```
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
; 5.40 - Microsoft network server: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
; 5.41 - Microsoft network server: Digitally sign  communication (if client agrees)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
; 5.42 - Microsoft network server: Disconnect clients when logon hours expire (Apply at the domain level)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
; 5.44 - Network access: Do not allow anonymous enumeration of SAM accounts
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
; 5.45 - Network access: Do not allow anonymous enumeration of SAM accounts and shares
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
; 5.46 - Network access: Do not allow storage of credentials or .NET Passports for network authentication
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
; 5.47 Network access: Let Everyone permissions apply to anonymous users
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
; 5.52 - Network access: Sharing and security model for local accounts
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0
; 5.53 - Network security: Do not store LAN Manager hash value on next password change
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
; 5.55 - Network security: LAN Manager Authentication Level
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4
; 5.56 - Network security: LDAP client signing requirements
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1
; 5.57 - Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248
; 5.58 - Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248
; 5.59 - Recovery Console: Allow automatic administrative logon
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
; 5.62 - Shutdown: Clear virtual memory pagefile
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
; 5.64 - System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1
; 5.65 - System objects: Default owner for objects created by members of the Administrators group
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
; 5.67 - System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
; 5.79 - MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)
MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt=4,1
; 5.80 - MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
; 5.84 - MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode=4,1
; 5.85 - MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)
MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=4,0
[Privilege Rights]
; 4.2 - Act as part of the operating system
SeTcbPrivilege =
; 4.3 - Add workstations to domain (Apply at the domain level)
SeMachineAccountPrivilege = Administrators
; 4.5 - Allow log on locally
SeInteractiveLogonRight = Users,Administrators
; 4.9 - Change the system time
SeSystemtimePrivilege = Administrators
; 4.10 - Create a pagefile
SeCreatePagefilePrivilege = Administrators
; 4.14 - Debug programs
SeDebugPrivilege = Administrators
; 4.15 - Deny access to this computer from the network
SeDenyNetworkLogonRight = Guests,Support_388945a0
; 4.21 - Force shutdown from a remote system
SeRemoteShutdownPrivilege = Administrators
```

```
; 4.22 - Generate security audits
SeAuditPrivilege = *S-1-5-19,*S-1-5-20
; 4.24 - Increase scheduling priority
SeIncreaseBasePriorityPrivilege = Administrators
; 4.25 - Load and unload device drivers
SeLoadDriverPrivilege = Administrators
; 4.26 - Lock pages in memory
SeLockMemoryPrivilege =
; 4.29 - Manage auditing and security log
SeSecurityPrivilege = Administrators
; 4.30 - Modify firmware environment values
SeSystemEnvironmentPrivilege = Administrators
; 4.31 - Perform volume maintenance tasks
SeManageVolumePrivilege = Administrators
; 4.33 - Profile system performance
SeSystemProfilePrivilege = Administrators
; 4.34 - Remove computer from docking station
SeUndockPrivilege = Administrators,Users
; 4.35 - Replace a process level token
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
; 4.37 - Shut down the system
SeShutdownPrivilege = Administrators,Users
; 4.39 - Take ownership of files or other objects
SeTakeOwnershipPrivilege = Administrators
[Group Membership]
; 7.1 - Backup Operators
Backup Operators__Memberof =
Backup Operators__Members =
; 7.2 - Power Users
Power Users__Memberof =
Power Users__Members =
[File Security]
; 9.1 - arp.exe
"%SystemRoot%\System32\arp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.2 - at.exe
"%SystemRoot%\System32\at.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.3 - attrib.exe
"%SystemRoot%\System32\attrib.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.4 - cacls.exe
"%SystemRoot%\System32\cacls.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.5 - debug.exe
"%SystemRoot%\System32\debug.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.6 - edlin.exe
"%SystemRoot%\System32\edlin.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.7 - eventcreate.exe
"%SystemRoot%\System32\eventcreate.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.8 - eventtriggers.exe
"%SystemRoot%\System32\eventtriggers.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.9 - ftp.exe
"%SystemRoot%\system32\ftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.10 - nbtstat.exe
"%SystemRoot%\System32\nbtstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.11 - net.exe
"%SystemRoot%\system32\net.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.12 - net1.exe
"%SystemRoot%\system32\net1.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.13 - netsh.exe
"%SystemRoot%\system32\netsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.14 - netstat.exe
"%systemRoot%\System32\netstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.15 - nslookup.exe
"%SystemRoot%\System32\nslookup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
```

```
; 9.16 - ntbackup.exe
"%SystemRoot%\System32\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.17 - rcp.exe
"%SystemRoot%\system32\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.18 - reg.exe
"%SystemRoot%\system32\reg.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.19 - regedit.exe
"%SystemRoot%\system32\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.20 - regedt32.exe
"%SystemRoot%\system32\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.21 - regini.exe
"%SystemRoot%\System32\regini.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.22 - regsvr32.exe
"%SystemRoot%\system32\regsvr32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.23 - rexec.exe
"%SystemRoot%\system32\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.24 - route.exe
"%SystemRoot%\system32\route.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.25 - rsh.exe
"%SystemRoot%\system32\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
; 9.26 - sc.exe
"%SystemRoot%\system32\sc.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\subst.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\systeminfo.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\telnet.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\tftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\tlntsvr.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
[Service General Setting]
; 8.1 - Alerter
Alerter,4,""
; 8.6 - ClipBook
ClipSrv,4,""
; 8.19 - FTP Publishing Service
MSFtpsvc,4,""
; 8.22 - IIS Admin Service
IISADMIN,4,""
; 8.30 - Messenger
Messenger,4,""
; 8.33 - NetMeeting Remote Desktop Sharing
mnmsrvc,4,""
; 8.52 - Routing and Remote Access
RemoteAccess,4,""
; 8.59 - SMTPSVC (Simple Mail Transfer Protocol)
SMTPSVC,4,""
; 8.60 - SNMP
SNMP,4,""
; 8.61 - SNMPTRAP
SNMPTRAP,4,""
; 8.62 - SSDP Discovery Service
SSDPSRV,4,""
; 8.68 - Telnet
TlntSvr,4,""
; 8.85 - World Wide Web Publising Services
W3SVC,4,""
```

Seguridad especializada - La funcionalidad limitada

```
[Profile Description]
Description=NIST Windows XP Professional Specialized Security Limited Functionality Security Settings
[Version]
signature="$CHICAGO$"
Revision=1
[Unicode]
Unicode=yes
 [System Access]
; 1.1 - Enforce password history (Apply at the domain level)
PasswordHistorySize = 24
; 1.2 - Maximum password age (Apply at the domain level)
MaximumPasswordAge = 90
; 1.3 - Minimum password age (Apply at the domain level)
MinimumPasswordAge = 1
; 1.4 - Minimum password length (Apply at the domain level)
MinimumPasswordLength = 12
; 1.5 - Passwords must meet complexity requirements (Apply at the domain level)
PasswordComplexity = 1
; 1.6 - Store password using reversible encryption for all users in the domain (Apply at the domain level)
ClearTextPassword = 0
; 2.1 - Account lockout duration (Apply at the domain level)
LockoutDuration = 15
; 2.2 - Account lockout threshold (Apply at the domain level)
LockoutBadCount = 10
; 2.3 - Reset account lockout counter after (Apply at the domain level)
ResetLockoutCount = 15
; 5.1 - Accounts: Administrator account status
EnableAdminAccount = 1
; 5.2 - Accounts: Guest account status (Security Options)
EnableGuestAccount = 0
; 5.43 - Network access: Allow anonymous SID/Name translation (Apply at the domain level)
LSAAnonymousNameLookup = 0
; 5.54 - Network security: Force logoff when logon hours expire (Apply at the domain level)
ForceLogoffWhenHourExpire = 1
[System Log]
; 6.3 - Maximum system log size
MaximumLogSize = 16384
; 6.6 - Prevent local guests group from accessing system log
RestrictGuestAccess = 1
; 6.12 - Retention method for system log
AuditLogRetentionPeriod = 0
[Security Log]
; 6.2 - Maximum security log size
MaximumLogSize = 81920
; 6.5 - Prevent local guests group from accessing security log
RestrictGuestAccess = 1
; 6.11 - Retention method for security log
AuditLogRetentionPeriod = 0
[Application Log]
; 6.1 - Maximum application log size
MaximumLogSize = 16384
; 6.4 - Prevent local guests group from accessing application log
RestrictGuestAccess = 1
; 6.10 - Retention method for application log
AuditLogRetentionPeriod = 0
[Event Audit]
; 3.1 - Audit account logon events
AuditLogonEvents = 3
; 3.2 - Audit account management
AuditAccountManage = 3
; 3.4 - Audit logon events
AuditAccountLogon = 3
; 3.5 - Audit object access
AuditObjectAccess = 2
; 3.6 - Audit policy change
```

```
AuditPolicyChange = 1
; 3.7 - Audit privilege use
AuditPrivilegeUse = 2
; 3.8 - Audit process tracking
AuditProcessTracking = 0
; 3.9 - Audit system events
AuditSystemEvents = 1
;-Valores de Registro---------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                ( 1 )
; REG_EXPAND_SZ         ( 2 )  // with environment variables to expand
; REG_BINARY            ( 3 )
; REG_DWORD             ( 4 )
; REG_MULTI_SZ          ( 7 )
[Registry Values]
; 5.3 - Accounts: Limit local account use of blank passwords to console logon only
MACHINE\System\Currentcontrolset\Control\Lsa\Limitblankpasswordуse=4,1
; 5.6 - Audit: Audit the access of global system objects
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
; 5.7 - Audit: Audit the use of Backup and Restore privilege
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
; 5.11 - Devices: Allow undock without having to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UndockWithoutLogon=4,0
; 5.12 - Devices: Allowed to format and eject removable media
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"0"
; 5.13 - Devices: Prevent users from installing printer drivers
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers=4,1
; 5.14 - Devices: Restrict CD-ROM access to locally logged-on user only
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,"0"
; 5.15 - Devices: Restrict floppy access to locally logged-on user only
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,"0"
; 5.16 - Devices: Unsigned driver installation behavior
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
; 5.20 - Domain Member: Digitally encrypt or sign secure channel data (always)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
; 5.21 - Domain Member: Digitally encrypt secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
; 5.22 - Domain Member: Digitally sign secure channel data (when possible)
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
; 5.23 - Domain Member: Disable machine account password changes
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
; 5.24 - Domain Member: Maximum machine account password age
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,30
; 5.25 - Domain Member:  Require Strong (Windows 2000 or later) Session Key
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
; 5.27 - Interactive logon: Do not display last user name
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
; 5.28 - Interactive logon: Do not require CTRL+ALT+DEL
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
; 5.29 - Interactive logon: Message text for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,This system is for the use
of authorized users only. Individuals using this computer system without authority"," or in excess of their authority","
are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this
system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of
criminal activity"," system personal may provide the evidence of such monitoring to law enforcement officials.
; 5.30 - Interactive logon: Message title for users attempting to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"-- WARNING --"
; 5.31 - Interactive logon: Number of previous logons to cache (in case domain controller is not available)
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"0"
; 5.32 - Interactive logon: Prompt user to change password before expiration
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
; 5.33 - Interactive logon: Require Domain Controller authentication to unlock workstation
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=4,1
; 5.35 - Interactive logon: Smart card removal behavior
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"
```

```
; 5.36 - Microsoft network client: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,1
; 5.37 - Microsoft network client: Digitally sign communications (if server agrees)
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
; 5.38 - Microsoft network client: Send unencrypted password to third-party SMB servers
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
; 5.39 - Microsoft network server: Amount of idle time required before suspending session
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
; 5.40 - Microsoft network server: Digitally sign communications (always)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
; 5.41 - Microsoft network server: Digitally sign  communication (if client agrees)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
; 5.42 - Microsoft network server: Disconnect clients when logon hours expire (Apply at the domain level)
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
; 5.44 - Network access: Do not allow anonymous enumeration of SAM accounts
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
; 5.45 - Network access: Do not allow anonymous enumeration of SAM accounts and shares
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
; 5.46 - Network access: Do not allow storage of credentials or .NET Passports for network authentication
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
; 5.47 Network access: Let Everyone permissions apply to anonymous users
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
; 5.48 - Network access: Named Pipes that can be accessed anonymously
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,COMNAP,COMNODE,SQ
L\QUERY,SPOOLSS,LLSRPC,browser
; 5.49 - Network access: Remotely accessible registry paths
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine=7,System\CurrentC
ontrolSet\Control\ProductOptions,System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Contr
ol\Server                    Applications,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP
Server,Software\Microsoft\Windows
NT\CurrentVersion,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal
Server,System\CurrentControlSet\Control\Terminal    Server\UserConfig,System\CurrentControlSet\Control\Terminal
Server\DefaultUserConfiguration
; 5.51 - Network access: Shares that can be accessed anonymously
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,COMCFG,DFS$
; 5.52 - Network access: Sharing and security model for local accounts
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0
; 5.53 - Network security: Do not store LAN Manager hash value on next password change
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
; 5.55 - Network security: LAN Manager Authentication Level
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
; 5.56 - Network security: LDAP client signing requirements
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1
; 5.57 - Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248
; 5.58 - Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248
; 5.59 - Recovery Console: Allow automatic administrative logon
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
; 5.60 - Recovery console: Allow floppy copy and access to all drives and all folders
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
; 5.61 - Shutdown: Allow system to be shut down without having to log on
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
; 5.62 - Shutdown: Clear virtual memory pagefile
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
; 5.64 - System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1
; 5.65 - System objects: Default owner for objects created by members of the Administrators group
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
; 5.66 - System objects: Require case insensitivity for non-Windows subsystems
MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=4,1
; 5.67 - System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
; 5.70 - MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=1,"0"
```

```
; 5.73 - MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
; 5.75 - MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
; 5.76 - MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
; 5.77 - MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)
MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden=4,1
; 5.78 - MSS: (KeepAliveTime)How often keep-alive packets are sent in milliseconds
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
; 5.79 - MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)
MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt=4,1
; 5.80 - MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
; 5.81 - MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from
WINS servers
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand=4,1
; 5.82 - MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames
(recommended)
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
; 5.83 - MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to
DoS)
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
; 5.84 - MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode=4,1
; 5.85 - MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0
recommended)
MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=4,0
; 5.86 - MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1
; 5.87 - MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not
acknowledged
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
; 5.88 - MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5
is default)
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
; 5.89 - MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90
[Privilege Rights]
; 4.1 - Access this computer from the network
SeNetworkLogonRight = Administrators
; 4.2 - Act as part of the operating system
SeTcbPrivilege =
; 4.3 - Add workstations to domain (Apply at the domain level)
SeMachineAccountPrivilege = Administrators
; 4.4 - Adjust memory quotas for a process
SeIncreaseQuotaPrivilege = Administrators,*S-1-5-19,*S-1-5-20
; 4.5 - Allow log on locally
SeInteractiveLogonRight = Users,Administrators
; 4.6 - Allow logon through Terminal Service
SeRemoteInteractiveLogonRight =
; 4.7 - Back up files and directories
SeBackupPrivilege = Administrators
; 4.8 - Bypass traverse checking
SeChangeNotifyPrivilege = Administrators,Users
; 4.9 - Change the system time
SeSystemtimePrivilege = Administrators
; 4.10 - Create a pagefile
SeCreatePagefilePrivilege = Administrators
; 4.11 - Create a token object
SeCreateTokenPrivilege =
; 4.13 - Create permanent shared objects
SeCreatePermanentPrivilege =
; 4.14 - Debug programs (require by some MS installer programs use to install MS hotfixes)
SeDebugPrivilege =
```

```
; 4.15 - Deny access to this computer from the network
SeDenyNetworkLogonRight = Guests,Support_388945a0
; 4.16 - Deny log on as a batch job
SeDenyBatchLogonRight = Guests,Support_388945a0
; 4.18 - Deny log on locally
SeDenyInteractiveLogonRight = Support_388945a0,Guests
; 4.19 - Deny log on through Terminal Services
SeDenyRemoteInteractiveLogonRight = *S-1-1-0
; 4.20 - Enable computer and user accounts to be trusted for delegation (not applicable)
SeEnableDelegationPrivilege =
; 4.21 - Force shutdown from a remote system
SeRemoteShutdownPrivilege = Administrators
; 4.20 - Generate security audits
SeAuditPrivilege = *S-1-5-19,*S-1-5-20
; 4.24 - Increase scheduling priority
SeIncreaseBasePriorityPrivilege = Administrators
; 4.25 - Load and unload device drivers
SeLoadDriverPrivilege = Administrators
; 4.26 - Lock pages in memory
SeLockMemoryPrivilege =
; 4.27 - Log on as a batch job
SeBatchLogonRight =
; 4.28 - Log on as a service
SeServiceLogonRight = *S-1-5-19,*S-1-5-20
; 4.29 - Manage auditing and security log
SeSecurityPrivilege = Administrators
; 4.30 - Modify firmware environment values
SeSystemEnvironmentPrivilege = Administrators
; 4.31 - Perform Volume Maintenance Task
SeManageVolumePrivilege = Administrators
; 4.32 - Profile single process
SeProfileSingleProcessPrivilege = Administrators
; 4.33 - Profile system performance
SeSystemProfilePrivilege = Administrators
; 4.34 - Remove computer from docking station
SeUndockPrivilege = Administrators,Users
; 4.35 - Replace a process level token
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
; 4.36 - Restore files and directories
SeRestorePrivilege = Administrators
; 4.37 - Shut down the system
SeShutdownPrivilege = Administrators,Users
; 4.39 - Take ownership of files or other objects
SeTakeOwnershipPrivilege = Administrators
[Group Membership]
; 7.1 - Backup Operators
Backup Operators__Memberof =
Backup Operators__Members =
; 7.2 - Power Users
Power Users__Memberof =
Power Users__Members =
; 7.3 - Remote Desktop Users
Remote Desktop Users__Memberof =
Remote Desktop Users__Members =
[File Security]
"%SystemRoot%\System32\arp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\at.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\attrib.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\cacls.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\debug.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\edlin.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\eventcreate.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\eventtriggers.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\ftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\nbtstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
```

```
"%SystemRoot%\system32\net.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\net1.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\netsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%systemRoot%\System32\netstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\nslookup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\reg.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\regini.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\regsvr32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\route.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\sc.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\subst.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\System32\systeminfo.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\telnet.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\tftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\system32\tlntsvr.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
[Service General Setting]
; 8.1 - Alerter
Alerter,4,""
; 8.6 - ClipBook
ClipSrv,4,""
; 8.9 - Computer Browser
Browser,4,""
; 8.18 - Fax
Fax,4,""
; 8.19 - FTP Publishing Service
MSFtpsvc,4,""
; 8.22 - IIS Admin Service
IISADMIN,4,""
; 8.24 - Indexing Service
CiSvc,4,""
; 8.30 - Messenger
Messenger,4,""
; 8.33 - NetMeeting Remote Desktop Sharing
mnmsrvc,4,""
; 8.47 - Remote Desktop Help Session Manage
RDSessMgr,4,""
; 8.52 - Routing and Remote Access
RemoteAccess,4,""
; 8.59 - SMTPSVC (Simple Mail Transfer Protocol)
SMTPSVC,4,""
; 8.60 - SNMP
SNMP,4,""
; 8.61 - SNMPTRAP
SNMPTRAP,4,""
; 8.62 - SSDP Discovery Service
SSDPSRV,4,""
; 8.65 - Task Scheduler
Schedule,4,""
; 8.68 - Telnet
TlntSvr,4,""
; 8.69 - Terminal Services
TermService,4,""
; 8.73 - Universal Plug and Play Device Host
upnphost,4,""
; 8.85 - World Wide Web Publising Services
W3SVC,4,""
```

ii. ARCHIVO PARA CORRECCIÓN POR CÓDIGO WINDOWS SERVER

WINDOWS SERVER CONTROLADORES DE DOMINIO

```
[version]
signature="$CHICAGO$"
DriverVer=10/01/2002,5.2.3790.0
[Register Registry Values] ; ; Syntax: RegPath,RegType,DisplayName,DisplayType,Options ; where ; RegPath: Includes the registry keypath and value ; RegType: 1 - REG_SZ, 2 - REG_EXPAND_SZ, 3 - REG_BINARY, 4 - REG_DWORD, 7 - REG_MULTI_SZ ; Display Name: Is a localizable string defined in the [strings] section ; Display type: 0 - boolean, 1 - Number, 2 - String, 3 - Choices, 4 - Multivalued, 5 - Bitmask ; Options: If Displaytype is 3 (Choices) or 5 (Bitmask), then specify the range of values and corresponding display strings ; in value|displaystring format separated by a comma.
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects,4,%AuditBaseObjects%,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail,4,%CrashOnAuditFail%,0
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds,4,%DisableDomainCreds%,0
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous,4,%EveryoneIncludesAnonymous%,0
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest,4,%ForceGuest%,3,0|%Classic%,1|%GuestBased%
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing,3,%FullPrivilegeAuditing%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse,4,%LimitBlankPasswordUse%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel,4,%LmCompatibilityLevel%,3,0|%LMCLevel0%,1|%LMCLevel1%,2|%LMCLevel2%,3|%LMCLevel3%,4|%LMCLevel4%,5|%LMCLevel5%
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec,4,%NTLMMinClientSec%,5,16|%NTLMIntegrity%,32|%NTLMConfidentiality%,524288|%NTLMv2Session%,536870912|%NTLM128%
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec,4,%NTLMMinServerSec%,5,16|%NTLMIntegrity%,32|%NTLMConfidentiality%,524288|%NTLMv2Session%,536870912|%NTLM128%
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash,4,%NoLMHash%,0
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner,4,%NoDefaultAdminOwner%,3,0|%DefaultOwner0%,1|%DefaultOwner1% MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous,4,%RestrictAnonymous%,0
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM,4,%RestrictAnonymousSAM%,0
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl,4,%SubmitControl%,0
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy,4,%FIPS%,0
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers,4,%AddPrintDrivers%,0
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine,7,%AllowedPaths%,4
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine,7,%AllowedExactPaths%,4
MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive,4,%ObCaseInsensitive%,0
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown,4,%ClearPageFileAtShutdown%,0 MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode,4,%ProtectionMode%,0 MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional,7,%OptionalSubSystems%,4
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature,4,%EnableSMBSignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature,4,%RequireSMBSignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff,4,%EnableForcedLogoff%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect,4,%AutoDisconnect%,1,%Unit-Minutes%
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess,4,%RestrictNullSessAccess%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes,7,%NullPipes%,4
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares,7,%NullShares%,4
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature,4,%EnableSMBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature,4,%RequireSMBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword,4,%EnablePlainTextPassword%,0
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity,4,%LDAPClientIntegrity%,3,0|%LDAPClient0%,1|%LDAPClient1%,2|%LDAPClient2%
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange,4,%DisablePWChange%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge,4,%MaximumPWAge%,1,%Unit-Days%
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange,4,%RefusePWChange%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel,4,%SignSecureChannel%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel,4,%SealSecureChannel%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal,4,%SignOrSeal%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey,4,%StrongKey%,0
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity,4,%LDAPServerIntegrity%,3,1|%LDAPServer1%,2|%LDAPServer2% MACHINE\Software\Microsoft\Driver Signing\Policy,3,%DriverSigning%,3,0|%DriverSigning0%,1|%DriverSigning1%,2|%DriverSigning2%
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD,4,%DisableCAD%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName,4,%DontDisplayLastUserName%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption,1,%LegalNoticeCaption%,2
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText,7,%LegalNoticeText%,4
```

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ScForceOption,4,%ScForceOption%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon,4,%ShutdownWithoutLogon%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UndockWithoutLogon,4,%UndockWithoutLogon%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel,4,%RCAdmin%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand,4,%RCSet%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms,1,%AllocateCDRoms%,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateDASD,1,%AllocateDASD%,3,0|%AllocateDASD0%,1|%AllocateDASD1%,2|%AllocateDASD2%
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies,1,%AllocateFloppies%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount,1,%CachedLogonsCount%,1,%Unit-
Logons% MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon,4,%ForceUnlockLogon%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning,4,%PasswordExpiryWarning%,1,%Unit-
Days% MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScRemoveOption,1,%ScRemove%,3,0|%ScRemove0%,1|%ScRemove1%,2|%ScRemove2%
MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection,4,%ForceHighProtection%,3,0|%CryptAllowNoUI%,1|%Crypt
AllowNoPass%,2|%CryptUsePass%
MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\AuthenticodeEnabled,4,%AuthenticodeEnabled%,0 ; delete
these values from the UI - Rdr in case NT4 w SCE MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DisableCAD
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\LegalNoticeText MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ShutdownWithoutLogon MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\CmdConsSecurityLevel MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\AddPrintDrivers MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\EnableSecuritySignature
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\RequireSecuritySignature
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\EnablePlainTextPassword
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnableSecuritySignature
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecuritySignature
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword
MACHINE\Software\Microsoft\Windows\CurrentVersion\NetCache\EncryptEntireCache MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\EFS\AlgorithmID MACHINE\Software\Microsoft\Non-Driver Signing\Policy
MACHINE\Software\Policies\Microsoft\Cryptography\ForceHighProtection ;============================== MSS Values
==============================
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect,4,%EnableICMPRedirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%SynAttackProtect%,3,0|%SynAttackProtect0%,1
|%SynAttackProtect1%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect,4,%EnableDeadGWDetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery,4,%EnablePMTUDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime,4,%KeepAliveTime%,3,150000|%KeepAliveTime0%,30
0000|%KeepAliveTime1%,600000|%KeepAliveTime2%,1200000|%KeepAliveTime3%,2400000|%KeepAliveTime4%,3600000|%KeepAliv
eTime5%,7200000|%KeepAliveTime6%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%DisableIPSourceRouting%,3,0|%DisableIP
SourceRouting0%,1|%DisableIPSourceRouting1%,2|%DisableIPSourceRouting2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions,4,%TcpMaxConnectRespon
seRetransmissions%,3,0|%TcpMaxConnectResponseRetransmissions0%,1|%TcpMaxConnectResponseRetransmissions1%,2|%TcpMaxC
onnectResponseRetransmissions2%,3|%TcpMaxConnectResponseRetransmissions3%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions,4,%TcpMaxDataRetransmissions%,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery,4,%PerformRouterDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted,4,%TCPMaxPortsExhausted%,1
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand,4,%NoNameReleaseOnDemand%,0
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation,4,%NtfsDisable8dot3NameCreation%,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun,4,%NoDriveTypeAutoRun%,3,0|%N
oDriveTypeAutoRun0%,255|%NoDriveTypeAutoRun1%
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel,4,%WarningLevel%,3,50|%WarningLevel0%,60|%War
ningLevel1%,70|%WarningLevel2%,80|%WarningLevel3%,90|%WarningLevel4% MACHINE\SYSTEM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod,4,%ScreenSaverGracePeriod%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta,4,%DynamicBacklogGrowthDelta%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog,4,%EnableDynamicBacklog%,0
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog,4,%MinimumDynamicBacklog%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog,4,%MaximumDynamicBacklog%,3,10000|%
MaximumDynamicBacklog0%,15000|%MaximumDynamicBacklog1%,20000|%MaximumDynamicBacklog2%,40000|%MaximumDynami
cBacklog3%,80000|%MaximumDynamicBacklog4%,160000|%MaximumDynamicBacklog5%

MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode,4,%SafeDllSearchMode%,0 [Strings] ;============================== Accounts ========== ;Specified in UI code - Accounts: Administrator account status ;Specified in UI code - Accounts: Guest account status ;Specified in UI code - Accounts: Rename administrator account ;Specified in UI code - Accounts: Rename guest account LimitBlankPasswordUse = "Accounts: Limit local account use of blank passwords to console logon only" ;============================== Audit ========== AuditBaseObjects="Audit: Audit the access of global system objects" FullPrivilegeAuditing="Audit: Audit the use of Backup and Restore privilege" CrashOnAuditFail="Audit: Shut down system immediately if unable to log security audits" ;============================== Devices ========== AllocateDASD="Devices: Allowed to format and eject removable media" AllocateDASD0="Administrators" AllocateDASD1="Administrators and Power Users" AllocateDASD2="Administrators and Interactive Users" AddPrintDrivers="Devices: Prevent users from installing printer drivers" AllocateCDRoms="Devices: Restrict CD-ROM access to locally logged-on user only" AllocateFloppies="Devices: Restrict floppy access to locally logged-on user only" DriverSigning="Devices: Unsigned driver installation behavior" DriverSigning0="Silently succeed " DriverSigning1="Warn but allow installation" DriverSigning2="Do not allow installation" UndockWithoutLogon="Devices: Allow undock without having to log on" ;============================== Domain controller ========== SubmitControl="Domain controller: Allow server operators to schedule tasks" RefusePWChange="Domain controller: Refuse machine account password changes" LDAPServerIntegrity = "Domain controller: LDAP server signing requirements" LDAPServer1 = "None" LDAPServer2 = "Require signing" ;============================== Domain member ========== DisablePWChange="Domain member: Disable machine account password changes" MaximumPWAge="Domain member: Maximum machine account password age" SignOrSeal="Domain member: Digitally encrypt or sign secure channel data (always)" SealSecureChannel="Domain member: Digitally encrypt secure channel data (when possible)" SignSecureChannel="Domain member: Digitally sign secure channel data (when possible)" StrongKey="Domain member: Require strong (Windows 2000 or later) session key" ;============================== Interactive logon ========== DisableCAD = "Interactive logon: Do not require CTRL+ALT+DEL" DontDisplayLastUserName = "Interactive logon: Do not display last user name" LegalNoticeText = "Interactive logon: Message text for users attempting to log on" LegalNoticeCaption = "Interactive logon: Message title for users attempting to log on" CachedLogonsCount = "Interactive logon: Number of previous logons to cache (in case domain controller is not available)"PasswordExpiryWarning = "Interactive logon: Prompt user to change password before expiration" ForceUnlockLogon = "Interactive logon: Require Domain Controller authentication to unlock workstation" ScForceOption = "Interactive logon: Require smart card" ScRemove = "Interactive logon: Smart card removal behavior" ScRemove0 = "No Action" ScRemove1 = "Lock Workstation" ScRemove2 = "Force Logoff" ;============================== Microsoft network client ========== RequireSMBSignRdr="Microsoft network client: Digitally sign communications (always)" EnableSMBSignRdr="Microsoft network client: Digitally sign communications (if server agrees)" EnablePlainTextPassword="Microsoft network client: Send unencrypted password to third-party SMB servers" ;============================== Microsoft network server ========== AutoDisconnect="Microsoft network server: Amount of idle time required before suspending session" RequireSMBSignServer="Microsoft network server: Digitally sign communications (always)" EnableSMBSignServer="Microsoft network server: Digitally sign communications (if client agrees)" EnableForcedLogoff="Microsoft network server: Disconnect clients when logon hours expire" ;============================== Network access ========== ;Specified in UI code - Network access: Allow anonymous SID/Name translation DisableDomainCreds = "Network access: Do not allow storage of credentials or .NET Passports for network authentication" RestrictAnonymousSAM = "Network access: Do not allow anonymous enumeration of SAM accounts" RestrictAnonymous = "Network access: Do not allow anonymous enumeration of SAM accounts and shares" EveryoneIncludesAnonymous = "Network access: Let Everyone permissions apply to anonymous users" RestrictNullSessAccess = "Network access: Restrict anonymous access to Named Pipes and Shares" NullPipes = "Network access: Named Pipes that can be accessed anonymously" NullShares = "Network access: Shares that can be accessed anonymously" AllowedPaths = "Network access: Remotely accessible registry paths and sub-paths" AllowedExactPaths = "Network access: Remotely accessible registry paths" ForceGuest = "Network access: Sharing and security model for local accounts" Classic = "Classic - local users authenticate as themselves" GuestBased = "Guest only - local users authenticate as Guest";============================== Network security ========== ;Specified in UI code - Network security: Enforce logon hour restrictions NoLMHash = "Network security: Do not store LAN Manager hash value on next password change" LmCompatibilityLevel = "Network security: LAN Manager authentication level" LMCLevel0 = "Send LM & NTLM responses" LMCLevel1 = "Send LM & NTLM - use NTLMv2 session security if negotiated" LMCLevel2 = "Send NTLM response only" LMCLevel3 = "Send NTLMv2 response only" LMCLevel4 = "Send NTLMv2 response only\refuse LM" LMCLevel5 = "Send NTLMv2 response only\refuse LM & NTLM" NTLMMinClientSec = "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" NTLMMinServerSec = "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" NTLMIntegrity = "Require message integrity" NTLMConfidentiality = "Require message confidentiality" NTLMv2Session = "Require NTLMv2 session security" NTLM128 = "Require 128-bit encryption" LDAPClientIntegrity = "Network security: LDAP client signing requirements" LDAPClient0 = "None" LDAPClient1 = "Negotiate signing" LDAPClient2 = "Require signing" ;============================== Recovery console ========== RCAdmin="Recovery console:

Allow automatic administrative logon" RCSet="Recovery console: Allow floppy copy and access to all drives and all folders" ;============================== Shutdown == ShutdownWithoutLogon="Shutdown: Allow system to be shut down without having to log on" ClearPageFileAtShutdown="Shutdown: Clear virtual memory pagefile" ProtectionMode = "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" NoDefaultAdminOwner = "System objects: Default owner for objects created by members of the Administrators group" DefaultOwner0 = "Administrators group" DefaultOwner1 = "Object creator" ObCaseInsensitive = "System objects: Require case insensitivity for non-Windows subsystems" ;============================== System cryptography == FIPS="System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing"ForceHighProtection="System cryptography: Force strong key protection for user keys stored on the computer" CryptAllowNoUI="User input is not required when new keys are stored and used" CryptAllowNoPass="User is prompted when the key is first used" CryptUsePass="User must enter a password each time they use a key" ;============================== System Settings == AuthenticodeEnabled = "System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies" OptionalSubSystems = "System settings: Optional subsystems" Unit-Logons="logons" Unit-Days="days" Unit-Minutes="minutes" Unit-Seconds="seconds" ;============================== MSS Settings ============================== EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)" SynAttackProtect0 = "No additional protection, use default settings" SynAttackProtect1 = "Connections time out sooner if a SYN attack is detected" EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)" EnablePMTUDiscovery = "MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)" KeepAliveTime = "MSS: How often keep-alive packets are sent in milliseconds" KeepAliveTime0 ="150000 or 2.5 minutes" KeepAliveTime1 ="300000 or 5 minutes (recommended)" KeepAliveTime2 ="600000 or 10 minutes" KeepAliveTime3 ="1200000 or 20 minutes" KeepAliveTime4 ="2400000 or 40 minutes" KeepAliveTime5 ="3600000 or 1 hour" KeepAliveTime6 ="7200000 or 2 hours (default value)" DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" DisableIPSourceRouting0 = "No additional protection, source routed packets are allowed" DisableIPSourceRouting1 = "Medium, source routed packets ignored when IP forwarding is enabled" DisableIPSourceRouting2 = "Highest protection, source routing is completely disabled" TcpMaxConnectResponseRetransmissions = "MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged" TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open connections dropped after 3 seconds"TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open connections dropped after 9 seconds" TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open connections dropped after 21 seconds" TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open connections dropped after 45 seconds" TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)" PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" TCPMaxPortsExhausted = "MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection (5 is recommended)" NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" NtfsDisable8dot3NameCreation = "MSS: Enable the computer to stop generating 8.3 style filenames" NoDriveTypeAutoRun = "MSS: Disable Autorun for all drives" NoDriveTypeAutoRun0 = "Null, allow Autorun" NoDriveTypeAutoRun1 = "255, disable Autorun for all drives" WarningLevel = "MSS: Percentage threshold for the security event log at which the system will generate a warning" WarningLevel0 = "50%" WarningLevel1 = "60%" WarningLevel2 = "70%" WarningLevel3 = "80%" WarningLevel4 = "90%" ScreenSaverGracePeriod = "MSS: The time in seconds before the screen saver grace period expires (0 recommended)" DynamicBacklogGrowthDelta = "MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)" EnableDynamicBacklog = "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications (recommended)" MinimumDynamicBacklog = "MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)" MaximumDynamicBacklog = "MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications" MaximumDynamicBacklog0 = "10000" MaximumDynamicBacklog1 = "15000" MaximumDynamicBacklog2 = "20000 (recommended)" MaximumDynamicBacklog3 = "40000" MaximumDynamicBacklog4 = "80000" MaximumDynamicBacklog5 = "160000" SafeDllSearchMode = "MSS: Enable Safe DLL search mode (recommended)"

WINDOWS SERVER SERVIDORES MIEMBROS DE DOMINIO

```
[version]
signature="$CHICAGO$"
DriverVer=10/01/2002,5.2.3790.0
[Register Registry Values] ; ; Syntax: RegPath,RegType,DisplayName,DisplayType,Options ; where ; RegPath: Includes the registry keypath and value ; RegType: 1 - REG_SZ, 2 - REG_EXPAND_SZ, 3 - REG_BINARY, 4 - REG_DWORD, 7 - REG_MULTI_SZ ; Display Name: Is a localizable string defined in the [strings] section ; Display type: 0 - boolean, 1 - Number, 2 - String, 3 - Choices, 4 - Multivalued, 5 - Bitmask ; Options: If Displaytype is 3 (Choices) or 5 (Bitmask), then specify the range of values and corresponding display strings ; in value|displaystring format separated by a comma.
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects,4,%AuditBaseObjects%,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail,4,%CrashOnAuditFail%,0
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds,4,%DisableDomainCreds%,0
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous,4,%EveryoneIncludesAnonymous%,0
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest,4,%ForceGuest%,3,0|%Classic%,1|%GuestBased%
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing,3,%FullPrivilegeAuditing%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse,4,%LimitBlankPasswordUse%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel,4,%LmCompatibilityLevel%,3,0|%LMCLevel0%,1|%LMCLevel1%,2|%LMCLevel2%,3|%LMCLevel3%,4|%LMCLevel4%,5|%LMCLevel5%
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec,4,%NTLMMinClientSec%,5,16|%NTLMIntegrity%,32|%NTLMConfidentiality%,524288|%NTLMv2Session%,536870912|%NTLM128%
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec,4,%NTLMMinServerSec%,5,16|%NTLMIntegrity%,32|%NTLMConfidentiality%,524288|%NTLMv2Session%,536870912|%NTLM128%
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash,4,%NoLMHash%,0
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner,4,%NoDefaultAdminOwner%,3,0|%DefaultOwner0%,1|%DefaultOwner1% MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous,4,%RestrictAnonymous%,0
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM,4,%RestrictAnonymousSAM%,0
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl,4,%SubmitControl%,0
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy,4,%FIPS%,0
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrinterDrivers,4,%AddPrintDrivers%,0
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine,7,%AllowedPaths%,4
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine,7,%AllowedExactPaths%,4
MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive,4,%ObCaseInsensitive%,0
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown,4,%ClearPageFileAtShutdown%,0 MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode,4,%ProtectionMode%,0 MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional,7,%OptionalSubSystems%,4
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature,4,%EnableSMBSignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature,4,%RequireSMBSignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff,4,%EnableForcedLogoff%,
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect,4,%AutoDisconnect%,1,%Unit-Minutes%
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess,4,%RestrictNullSessAccess%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes,7,%NullPipes%,4
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares,7,%NullShares%,4
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature,4,%EnableSMBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature,4,%RequireSMBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword,4,%EnablePlainTextPassword%,0
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity,4,%LDAPClientIntegrity%,3,0|%LDAPClient0%,1|%LDAPClient1%,2|%LDAPClient2%
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange,4,%DisablePWChange%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge,4,%MaximumPWAge%,1,%Unit-Days%
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange,4,%RefusePWChange%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel,4,%SignSecureChannel%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel,4,%SealSecureChannel%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal,4,%SignOrSeal%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey,4,%StrongKey%,0
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity,4,%LDAPServerIntegrity%,3,1|%LDAPServer1%,2|%LDAPServer2% MACHINE\Software\Microsoft\Driver Signing\Policy,3,%DriverSigning%,3,0|%DriverSigning0%,1|%DriverSigning1%,2|%DriverSigning2%
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD,4,%DisableCAD%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName,4,%DontDisplayLastUserName%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption,1,%LegalNoticeCaption%,2
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText,7,%LegalNoticeText%,4
```

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ScForceOption,4,%ScForceOption%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon,4,%ShutdownWithoutLogon%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UndockWithoutLogon,4,%UndockWithoutLogon%,MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel,4,%RCAdmin%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand,4,%RCSet%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms,1,%AllocateCDRoms%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD,1,%AllocateDASD%,3,0|%AllocateDASD0%,1|%AllocateDASD1%,2|%AllocateDASD2%
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies,1,%AllocateFloppies%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount,1,%CachedLogonsCount%,1,%Unit-Logons% MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon,4,%ForceUnlockLogon%,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning,4,%PasswordExpiryWarning%,1,%Unit-Days% MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption,1,%ScRemove%,3,0|%ScRemove0%,1|%ScRemove1%,2|%ScRemove2%
MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection,4,%ForceHighProtection%,3,0|%CryptAllowNoUI%,1|%CryptAllowNoPass%,2|%CryptUsePass%
MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\AuthenticodeEnabled,4,%AuthenticodeEnabled%,0 ; delete these values from the UI - Rdr in case NT4 w SCE MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DisableCAD
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CmdConsSecurityLevel MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\AddPrintDrivers MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\EnableSecuritySignature
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\RequireSecuritySignature
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\EnablePlainTextPassword
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnableSecuritySignature
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecuritySignature
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword
MACHINE\Software\Microsoft\Windows\CurrentVersion\NetCache\EncryptEntireCache MACHINE\Software\Microsoft\Windows NT\CurrentVersion\EFS\AlgorithmID MACHINE\Software\Microsoft\Non-Driver Signing\Policy
MACHINE\Software\Policies\Microsoft\Cryptography\ForceHighProtection ;============================== MSS Values ==============================
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect,4,%EnableICMPRedirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%SynAttackProtect%,3,0|%SynAttackProtect0%,1|%SynAttackProtect1%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect,4,%EnableDeadGWDetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery,4,%EnablePMTUDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime,4,%KeepAliveTime%,3,150000|%KeepAliveTime0%,300000|%KeepAliveTime1%,600000|%KeepAliveTime2%,1200000|%KeepAliveTime3%,2400000|%KeepAliveTime4%,3600000|%KeepAliveTime5%,7200000|%KeepAliveTime6%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%DisableIPSourceRouting%,3,0|%DisableIPSourceRouting0%,1|%DisableIPSourceRouting1%,2|%DisableIPSourceRouting2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions,4,%TcpMaxConnectResponseRetransmissions%,3,0|%TcpMaxConnectResponseRetransmissions0%,1|%TcpMaxConnectResponseRetransmissions1%,2|%TcpMaxConnectResponseRetransmissions2%,3|%TcpMaxConnectResponseRetransmissions3%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions,4,%TcpMaxDataRetransmissions%,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery,4,%PerformRouterDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted,4,%TCPMaxPortsExhausted%,1
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand,4,%NoNameReleaseOnDemand%,0
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation,4,%NtfsDisable8dot3NameCreation%,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun,4,%NoDriveTypeAutoRun%,3,0|%NoDriveTypeAutoRun0%,255|%NoDriveTypeAutoRun1%
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel,4,%WarningLevel%,3,50|%WarningLevel0%,60|%WarningLevel1%,70|%WarningLevel2%,80|%WarningLevel3%,90|%WarningLevel4% MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod,4,%ScreenSaverGracePeriod%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta,4,%DynamicBacklogGrowthDelta%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog,4,%EnableDynamicBacklog%,0
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog,4,%MinimumDynamicBacklog%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog,4,%MaximumDynamicBacklog%,3,10000|%MaximumDynamicBacklog0%,15000|%MaximumDynamicBacklog1%,20000|%MaximumDynamicBacklog2%,40000|%MaximumDynamicBacklog3%,80000|%MaximumDynamicBacklog4%,160000|%MaximumDynamicBacklog5%

MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode,4,%SafeDllSearchMode%,0 [Strings] ;============================== Accounts ========== ;Specified in UI code - Accounts: Administrator account status ;Specified in UI code - Accounts: Guest account status ;Specified in UI code - Accounts: Rename administrator account ;Specified in UI code - Accounts: Rename guest account LimitBlankPasswordUse = "Accounts: Limit local account use of blank passwords to console logon only" ;============================== Audit ========== AuditBaseObjects="Audit: Audit the access of global system objects" FullPrivilegeAuditing="Audit: Audit the use of Backup and Restore privilege" CrashOnAuditFail="Audit: Shut down system immediately if unable to log security audits";============================== Devices ========== AllocateDASD="Devices: Allowed to format and eject removable media" AllocateDASD0="Administrators" AllocateDASD1="Administrators and Power Users" AllocateDASD2="Administrators and Interactive Users" AddPrintDrivers="Devices: Prevent users from installing printer drivers" AllocateCDRoms="Devices: Restrict CD-ROM access to locally logged-on user only" AllocateFloppies="Devices: Restrict floppy access to locally logged-on user only" DriverSigning="Devices: Unsigned driver installation behavior" DriverSigning0="Silently succeed " DriverSigning1="Warn but allow installation" DriverSigning2="Do not allow installation" UndockWithoutLogon="Devices: Allow undock without having to log on" ;============================== Domain controller ========== SubmitControl="Domain controller: Allow server operators to schedule tasks" RefusePWChange="Domain controller: Refuse machine account password changes" LDAPServerIntegrity = "Domain controller: LDAP server signing requirements" LDAPServer1 = "None" LDAPServer2 = "Require signing" ;============================== Domain member ========== DisablePWChange="Domain member: Disable machine account password changes" MaximumPWAge="Domain member: Maximum machine account password age" SignOrSeal="Domain member: Digitally encrypt or sign secure channel data (always)" SealSecureChannel="Domain member: Digitally encrypt secure channel data (when possible)" SignSecureChannel="Domain member: Digitally sign secure channel data (when possible)" StrongKey="Domain member: Require strong (Windows 2000 or later) session key" ;============================== Interactive logon ========== DisableCAD = "Interactive logon: Do not require CTRL+ALT+DEL" DontDisplayLastUserName = "Interactive logon: Do not display last user name" LegalNoticeText = "Interactive logon: Message text for users attempting to log on" LegalNoticeCaption = "Interactive logon: Message title for users attempting to log on" CachedLogonsCount = "Interactive logon: Number of previous logons to cache (in case domain controller is not available)"PasswordExpiryWarning = "Interactive logon: Prompt user to change password before expiration" ForceUnlockLogon = "Interactive logon: Require Domain Controller authentication to unlock workstation" ScForceOption = "Interactive logon: Require smart card" ScRemove = "Interactive logon: Smart card removal behavior" ScRemove0 = "No Action" ScRemove1 = "Lock Workstation" ScRemove2 = "Force Logoff" ;============================== Microsoft network client ========== RequireSMBSignRdr="Microsoft network client: Digitally sign communications (always)" EnableSMBSignRdr="Microsoft network client: Digitally sign communications (if server agrees)" EnablePlainTextPassword="Microsoft network client: Send unencrypted password to third-party SMB servers" ;============================== Microsoft network server ========== AutoDisconnect="Microsoft network server: Amount of idle time required before suspending session" RequireSMBSignServer="Microsoft network server: Digitally sign communications (always)" EnableSMBSignServer="Microsoft network server: Digitally sign communications (if client agrees)" EnableForcedLogoff="Microsoft network server: Disconnect clients when logon hours expire" ;============================== Network access ========== ;Specified in UI code - Network access: Allow anonymous SID/Name translation DisableDomainCreds = "Network access: Do not allow storage of credentials or .NET Passports for network authentication" RestrictAnonymousSAM = "Network access: Do not allow anonymous enumeration of SAM accounts" RestrictAnonymous = "Network access: Do not allow anonymous enumeration of SAM accounts and shares" EveryoneIncludesAnonymous = "Network access: Let Everyone permissions apply to anonymous users" RestrictNullSessAccess = "Network access: Restrict anonymous access to Named Pipes and Shares" NullPipes = "Network access: Named Pipes that can be accessed anonymously" NullShares = "Network access: Shares that can be accessed anonymously" AllowedPaths = "Network access: Remotely accessible registry paths and sub-paths" AllowedExactPaths = "Network access: Remotely accessible registry paths" ForceGuest = "Network access: Sharing and security model for local accounts" Classic = "Classic - local users authenticate as themselves" GuestBased = "Guest only - local users authenticate as Guest";============================== Network security ========== ;Specified in UI code - Network security: Enforce logon hour restrictions NoLMHash = "Network security: Do not store LAN Manager hash value on next password change" LmCompatibilityLevel = "Network security: LAN Manager authentication level" LMCLevel0 = "Send LM & NTLM responses" LMCLevel1 = "Send LM & NTLM - use NTLMv2 session security if negotiated" LMCLevel2 = "Send NTLM response only" LMCLevel3 = "Send NTLMv2 response only" LMCLevel4 = "Send NTLMv2 response only\refuse LM" LMCLevel5 = "Send NTLMv2 response only\refuse LM & NTLM" NTLMMinClientSec = "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" NTLMMinServerSec = "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" NTLMIntegrity = "Require message integrity" NTLMConfidentiality = "Require message confidentiality" NTLMv2Session = "Require NTLMv2 session security" NTLM128 = "Require 128-bit encryption" LDAPClientIntegrity = "Network security: LDAP client signing requirements" LDAPClient0 = "None" LDAPClient1 = "Negotiate signing" LDAPClient2 = "Require signing" ;============================== Recovery console ========== RCAdmin="Recovery console:

Allow automatic administrative logon" RCSet="Recovery console: Allow floppy copy and access to all drives and all folders" ;============================== Shutdown == ShutdownWithoutLogon="Shutdown: Allow system to be shut down without having to log on" ClearPageFileAtShutdown="Shutdown: Clear virtual memory pagefile" ProtectionMode = "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)" NoDefaultAdminOwner = "System objects: Default owner for objects created by members of the Administrators group" DefaultOwner0 = "Administrators group" DefaultOwner1 = "Object creator" ObCaseInsensitive = "System objects: Require case insensitivity for non-Windows subsystems" ;============================== System cryptography == FIPS="System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing"ForceHighProtection="System cryptography: Force strong key protection for user keys stored on the computer" CryptAllowNoUI="User input is not required when new keys are stored and used" CryptAllowNoPass="User is prompted when the key is first used" CryptUsePass="User must enter a password each time they use a key" ;============================== System Settings == AuthenticodeEnabled = "System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies" OptionalSubSystems = "System settings: Optional subsystems" Unit-Logons="logons" Unit-Days="days" Unit-Minutes="minutes" Unit-Seconds="seconds" ;============================== MSS Settings ============================== EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes" SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)" SynAttackProtect0 = "No additional protection, use default settings" SynAttackProtect1 = "Connections time out sooner if a SYN attack is detected" EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)" EnablePMTUDiscovery = "MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)" KeepAliveTime = "MSS: How often keep-alive packets are sent in milliseconds" KeepAliveTime0 ="150000 or 2.5 minutes" KeepAliveTime1 ="300000 or 5 minutes (recommended)" KeepAliveTime2 ="600000 or 10 minutes" KeepAliveTime3 ="1200000 or 20 minutes" KeepAliveTime4 ="2400000 or 40 minutes" KeepAliveTime5 ="3600000 or 1 hour" KeepAliveTime6 ="7200000 or 2 hours (default value)" DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)" DisableIPSourceRouting0 = "No additional protection, source routed packets are allowed" DisableIPSourceRouting1 = "Medium, source routed packets ignored when IP forwarding is enabled" DisableIPSourceRouting2 = "Highest protection, source routing is completely disabled" TcpMaxConnectResponseRetransmissions = "MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged" TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open connections dropped after 3 seconds" TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open connections dropped after 9 seconds" TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open connections dropped after 21 seconds" TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open connections dropped after 45 seconds" TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)" PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)" TCPMaxPortsExhausted = "MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection (5 is recommended)" NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" NtfsDisable8dot3NameCreation = "MSS: Enable the computer to stop generating 8.3 style filenames" NoDriveTypeAutoRun = "MSS: Disable Autorun for all drives" NoDriveTypeAutoRun0 = "Null, allow Autorun" NoDriveTypeAutoRun1 = "255, disable Autorun for all drives" WarningLevel = "MSS: Percentage threshold for the security event log at which the system will generate a warning" WarningLevel0 = "50%" WarningLevel1 = "60%" WarningLevel2 = "70%" WarningLevel3 = "80%" WarningLevel4 = "90%" ScreenSaverGracePeriod = "MSS: The time in seconds before the screen saver grace period expires (0 recommended)" DynamicBacklogGrowthDelta = "MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)" EnableDynamicBacklog = "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications (recommended)" MinimumDynamicBacklog = "MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)" MaximumDynamicBacklog = "MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications" MaximumDynamicBacklog0 = "10000" MaximumDynamicBacklog1 = "15000" MaximumDynamicBacklog2 = "20000 (recommended)" MaximumDynamicBacklog3 = "40000" MaximumDynamicBacklog4 = "80000" MaximumDynamicBacklog5 = "160000" SafeDllSearchMode = "MSS: Enable Safe DLL search mode (recommended)"

ANEXO C.
CHECKLISTS

ITEM	CONFIGURACIÓN	HOME	COMPUTADOR EN LA EMPRESA		SEGURIDAD ESPECIALIZADA
			ESCRITORIO	PORTATIL	FUNCIONALIDAD LIMITADA
1	**SERVICE PACK Y ACTUALIZACIONES DE SEGURIDAD**				
1,1	Mayores requerimientos de ServicePack y actualizaciones				
1,1,1	Valoración de ServicePack instalado	Service Pack 3 a partir de la última actualización			
1,2	Menores requerimientos de ServicePack y actualizaciones				
1,2,1	Las actualizaciones de seguridad son referidas por Microsoft Security Bulletins	Todas las actualizaciones críticas e importantes de seguridad			
2	**AUDITORIA Y POLITICAS DE CUENTA**				
2,1	Mayores requerimientos de auditoría y políticas de cuenta				
2,1,1	Longitud mínima de contraseña	8 caracteres			12 caracteres
2,1,2	Edad máxima de contraseña	90 días			
2,2	Menores requerimientos de auditoría y políticas de cuentas				
2,2,1	Políticas de cuenta (mínimos)				
2,2,1,1	Auditoria en eventos de entrada en las cuentas	Éxito y Fallo			
2,2,1,2	Auditoria de Administrador de cuentas	Éxito y Fallo			
2,2,1,3	Control de acceso al directorio de servicios	(No definido)			
2,2,1,4	Eventos de entrada en el sistema de cuentas	Éxito y Falla			
2,2,1,5	Control de acceso de objetos	Fallo (mínima)			Éxito y Falla
2,2,1,6	Control de políticas de cambio	Éxito (mínimo)			
2,2,1,7	Control de uso de privilegios	Fallo (mínima)			
2,2,1,8	Control de rastreo de proceso	(No definido)			
2,2,1,9	Control de eventos del sistema	Éxito (mínimo)			
2,2,2	Póliticas de Cuenta				
2,2,2,1	Edad mínima de contraseña	1 día			
2,2,2,2	Edad máxima de contraseña	90 días			

2,2,2,3	Longitud mínima de contraseña	8 caracteres	12 caracteres
2,2,2,4	Complejidad de contraseña	Habilitado	
2,2,2,5	Historial de contraseña	24 contraseñas recordadas	
2,2,2,6	Almacenaje de contraseñas usando encriptación reversible	Inhabilitado	
2,2,3	Política de cierre forzoso de cuenta		
2,2,3,1	Duración de cierres forzoso de cuenta	15 minutos	15 minutos
2,2,3,2	Umbral de cierre forzoso de cuenta	50 intentos	10 intentos
2,2,3,3	Restablezca el cierre forzoso de cuenta después	15 minutos	15 minutos
2,2,4	Configuración Registro Evento, Aplicación, seguridad y diarios del sistema		
2,2,4,1	Aplicación de Registro		
2,2,4,1,1	Tamaño máximo de registro de eventos	16 MB	
2,2,4,1,2	Restringir acceso a invitado	Habilitado	
2,2,4,1,3	Método de retención de registro	Según sea necesario	
2,2,4,1,4	Retención de registro	(No definido)	
2.2.4.2	Seguridad de registro		
2,2,4,2,1	Tamaño máximo de registro de evento	80 MB	
3	**CONFIGURACIONES DE SEGURIDAD**		
3,1	Mayores configuraciones de Seguridad		
3,1,1	Acceso de red: permitir anónimo SID/traducción de nombre	Inhabilitado	
3,1,2	Acceso de red: No permita enumeraciones anónimas de cuentas SAM.	Habilitado	
3,1,3	No permita enumeraciones anónimas de cuentas SAM y compartidas.	Habilitado	
3,1,4	Protección de ejecución de datos	Habilitado	

3,2	Menores configuraciones de Seguridad				
3,2,1	Opciones de seguridad				
3,2,1,1	Cuentas: Administrador de estado de cuentas	(No definido)	(No definido)		(No definido)
3,2,1,2	Cuentas: Estado de cuenta invitado	Inhabilitado			
3,2,1,3	Cuentas: Limitar Cuenta local de contraseñas en blanco solo para entrada	Habilitado			
3,2,1,4	Cuentas: Renombrar cuenta de administrador	(Usuario define valor)			
3,2,1,5	Cuentas: Renombrar cuenta de invitado	(Usuario define valor)			
3,2,1,6	Auditoria: Controle el acceso del sistema global de objetos	(No definido)			Inhabilitado
3,2,1,7	Auditoria: Controle el uso de privilegios de backup y restauración	(No definido)			Inhabilitado
3,2,1,8	Apague el sistema de inmediato si es incapaz de registrar alertas de seguridad	(No definido)			
3,2,1,9	DCOM: Restricciones de acceso a la máquina	(No definido)			
3,2,1,10	DOCM: Restricciones de lanzamiento (SP2)	(No definido)			
3,2,1,11	Dispositivos: Permitir formatear y expulsar dispositivos removibles	Administradores, Usuarios interactivos			Administradores
3,2,1,12	Dispositivos: Usuarios prevenidos de instalar drivers de impresoras	(No definido)	Habilitado	(No definido)	Habilitado
3,2,1,13	Dispositivos: Restrinja acceso CD para entrar en el sistema localmente	(No definido)			Inhabilitado
3,2,1,14	Dispositivos: Restrinja acceso Floppy para entrar en el sistema localmente	(No definido)			Inhabilitado
3,2,1,15	Controlador de dominio: No Permite cambios de contraseña	(No aplicable)			
3,2,1,16	Miembro de dominio: Elaborar edad de contraseña de cuenta	30 días			
3,2,1,17	Entrada interactiva: No muestre último nombre del usuario	Habilitado			
3,2,1,18	Texto de mensaje para usuarios intentando ingresar	Tradicional, O aprobado			
3,2,1,19	Título de mensaje para usuarios intentando a ingresar	Tradicional, O aprobado			

3,2,1,20	Número de entradas previas en el sistema a Cache	2	1	2	0
3,2,1,21	Impulse al usuario a Cambiar Password antes de la expiración	14 días			
3,2,1,22	Requiera autenticación controlador de dominio para abrir puesto de trabajo	(No definido)	Habilitado	Inhabilitado	(No definido)
3,2,1,23	Comportamiento de remoción de tarjeta con memoria	Bloquear Estación de trabajo			
3,2,1,24	Acceso de red: No permita el almacenamiento de credenciales o pasaportes de NET para la autenticación de red	(No definido)	Habilitado		
3,2,1,25	Fuerce salida del sistema cuando las horas de entrada en el sistema expiran	(No definido)	Habilitado	(No definido)	Habilitado
3,2,1,26	Permita que el sistema se cierre sin tener que entrar en el sistema	Inhabilitado			
3,2,1,27	Objetos de sistema: Fortalezca permisos implícitos de objetos internos	(No definido)	Habilitado		
3.2.2	Configuraciones Adicionales de registro				
3.2.2.1	Inhabilite ejecución automática del instrumento puesta a punto de sistema HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\AutoWindows NT\CurrentVersion\ AEDebug\Auto	(No definido)			
3.2.2.2	Inhabilite |autoplay| de cada disco HKLM\Software\Microsoft\Policies\Explorer\NoDriveTypeAutoRun Windows\CurrentVersion\	(REG_DWORD) 255			

3.2.2.3	Inhabilite |autoplay| para el usuario actual HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\ NoDriveTypeAutoRun	(REG_DWORD) 255	
3.2.2.4	Inhabilite la entrada en el sistema automática HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoDriveTypeAutoRun	(No definido)	
3.2.2.5	Inhabilite los reboots automáticos después de ver una pantalla azul de la muerte: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\AutoAdminLogon	(No definido)	(REG_DWORD) 0
3.2.2.6	Inhabilite ejecución automática de CD: HKLM\System\CurrentControlSet\ Services\CDrom\Autorun (REG_DWORD)	(REG_DWORD) 0	
3.2.2.7	Quite las porciones administrativas en el puesto de trabajo (profesional) HKLM\System\CurrentControlSet\Services\LanmanServer\ Parameters\AutoShareWks	(No definido)	0
3.2.2.8	Ayude a proteger contra la fragmentación de paquetes pequeños: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ EnablePMTUDiscovery	(No definido)	
3.2.2.9	Maneje los tiempos de subsistencia viva HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ KeepAliveTime	(No definido)	(REG_DWORD) 300000

3.2.2.10	Proteja contra los ataques de liberación de nombre maliciosos: HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand	(No definido)	(No definido)	(REG_DWORD) 1
3.2.2.11	Oculte el puesto de trabajo de la inscripción de visor de red: HKLM\System\CurrentControlSet\Services\ Lanmanserver\Parameters\HiddenSettings\DisableBasicOverClearChannel	(No definido)		(REG_DWORD) 1
3.2.2.12	USB bloquea la política de dispositivo de almacenamiento (sólo SP2): HKLM\System\CurrentControlSet \Control\StorageDevicePolicies	(No definido)		(REG_DWORD) 1
4	**PROTECCION DE SEGURIDAD ADICIONAL**			
4.1	Los servicios disponibles (permisos sobre servicios listados aquí: Administradores: Control completo; Sistema: Lea, empiece, haga alto, y pause)			
4.1.1	Alertador	Inhabilitado		
4.1.2	Actualizaciones automáticas	(No definido)		
4.1.3	Base inteligente de transferencia de servicios.	(No definido)		
4.1.4	Clipbook	Inhabilitado		
4.1.5	Visor de computadora	(No definido)	Inhabilitado	
4.1.6	Servicio de Fax	(No definido)		Inhabilitado
4.1.7	Servicio de publicación FTP	Inhabilitado		
4.1.8	Servicio Administrador IIS	Inhabilitado		
4.1.9	Servicio de Indexación	(No definido)		Inhabilitado
4.1.10	Messenger	Inhabilitado		
4.1.11	Ingreso de Red	(No definido)		
4.1.12	Repartición de Escritorio Remoto NetMeeting	Inhabilitado		
4.1.13	Manejador de Ayuda de Sesión de Escritorio Remoto	(No definido)	(No definido)	Inhabilitado
4.1.14	Servicio de Registro Remoto	(No definido)		

4.1.15	Ruteado y Acceso Remoto	Inhabilitado		
4.1.16	Protocolo de Transferencia Simple de Correo (SMTP)	Inhabilitado		
4.1.17	Protocolo de Manejo Simple de Red (SNMP) Servicio	Inhabilitado		
4.1.18	Protocolo de Manejo Simple de Red (SNMP) Trampa	Inhabilitado		
4.1.19	Calendario de Tareas	(No definido)		Inhabilitado
4.1.20	Telnet	Inhabilitado		
4.1.21	Servicio de Terminal	(No definido)		Inhabilitado
4.1.22	Dispositivo Host Universal Plug and Play	(No definido)	Inhabilitado	
4.2.1	Acceso a la PC de la Red	(No definido)	(No definido)	
4.2.2	Actuar como parte de la operación del sistema	Ninguna		
4.2.3	Añadir estaciones de trabajo al Dominio	(No aplicable)		
4.2.4	Ajustar cuotas de memoria para un proceso	(No definido)		
4.2.5	Permita ingresar completamente a la Terminal de Servicios	(No definido)		Ninguna
4.2.6	Conserve Archivos y directorios	(No definido)		
4.2.7	Comprobación de ruta de desviación	(No definido)		
4.2.8	Cambio de tiempo del sistema	Administradores		
4.2.9	Crear una página de archivo	Administradores		
4.2.10	Crear un objeto simbólico	Ninguna		
4.2.11	Crear permanentemente partes de objetos	Ninguna		
4.2.12	Depuración de programas	Administradores	Administradores	Ninguna

4.2.13	Niegue acceso esta computadora de la Red	Invitado, soporta 388945 a 0
4.2.14	Niegue ingreso como un grupo de trabajo	(No definido)
4.2.15	Niegue ingreso como un servicio	(No definido)
4.2.16	Niegue ingreso localmente	(No definido)
4.2.17	Niegue ingreso completamente de Terminal de Servicio	(No definido)
4.2.18	Habilite PC y cuentas de usuario para ser confiables según sean delegados	(No aplicable)
4.2.19	Forcé el apagado del sistema de un sistema remoto	Administradores
4.2.20	Genere auditorias de seguridad	Servicio Local, Servicio de Red
4.2.21	Incremente prioridad de horario	Administradores
4.2.22	Cargue y descargue drivers de dispositivos	Administradores
4.2.23	Asegure páginas en la memoria	Ninguna
4.2.24	Ingreso como grupo de trabajo	(No definido)
4.2.25	Ingreso como un servicio	(No definido)
4.2.26	Ingreso localmente	Usuarios, Administradores
4.2.27	Manejo de auditoría e ingreso de seguridad	Administradores
4.2.28	Modifique los valores del entorno de firmware	Administradores
4.2.29	Ejecute las tareas de mantenimiento de volumen	Administradores
4.2.30	Proceso de perfil sencillo	Administradores
4.2.31	Ejecute el sistema de perfiles	Administradores
4.2.32	Remueva el PC de la estación de acoplamiento	Usuarios, Administradores

4.2.33	Reemplace un símbolo de nivel de proceso	Servicio Local, Servicio de Red	
4.2.34	Restaure archivos y directorios	Administradores	
4.2.35	Apague el sistema	Usuarios, Administradores	
4.2.36	Sincronice el directorio de servicio de datos	(No aplicable)	
4.2.37	Tome propiedad de archivo o de otro objeto	Administradores	
4.3	Otros Requerimientos del Sistema		
4.3.1	Asegure volúmenes que usan archivos del sistema NTFS	Todos los volumenes	
4.3.2	Inhabilite el NetBIOS	(No definido)	(No definido)
4.3.3	Habilite el Firewall de la conexión de Internet	(No definido) pero fuertemente recomendado	
4.3.4	Restrinja Grupos	Usuarios de escritorio remoto: (Ninguna)	
4.4	Archivo		
4.4.1	Permisos de archivos		
4.4.1.1	%SystemRoot%\system32\at.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.2	%SystemRoot%\system32\attrib.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.3	%SystemRoot%\system32\cacls.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.4	%SystemRoot%\system32\debug.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.5	%SystemRoot%\system32\drwatson.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.6	%SystemRoot%\system32\drwtsn32.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.7	%SystemRoot%\system32\edlin.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	
4.4.1.8	%SystemRoot%\system32\eventcreate.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.9	%SystemRoot%\system32\eventtriggers.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.10	%SystemRoot%\system32\ftp.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	Admnistradores: Lleno - Sistema: Lleno
4.4.1.11	%SystemRoot%\system32\net.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	Admnistradores: Lleno - Sistema: Lleno
4.4.1.12	%SystemRoot%\system32\net1.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	Admnistradores: Lleno - Sistema: Lleno

4.4.1.13	%SystemRoot%\system32\netsh.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.14	%SystemRoot%\system32\rcp.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.15	%SystemRoot%\system32\reg.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.16	%SystemRoot%\regedit.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.17	%SystemRoot%\system32\regedt32.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.18	%SystemRoot%\system32\regsvr32.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.19	%SystemRoot%\system32\rexec.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.20	%SystemRoot%\system32\rsh.exe	Administradores: Lleno -Sistema: Lleno	
4.4.1.21	%SystemRoot%\system32\runas.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	Admnistradores: Lleno - Sistema: Lleno
4.4.1.22	%SystemRoot%\system32\sc.exe	Administrador: Lleno - Sistema: Lleno	
4.4.1.23	%SystemRoot%\system32\ subst.exe	Administrador: Lleno - Sistema: Lleno	
4.4.1.24	%SystemRoot%\system32\telnet.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	Admnistradores: Lleno - Sistema: Lleno
4.4.1.25	%SystemRoot%\system32\tftp.exe	Administradores: Lleno -Sistema: Lleno - Interactivo: Lleno	Admnistradores: Lleno - Sistema: Lleno
4.4.1.26	%SystemRoot%\system32\tlntsvr.exe	Administrador: Lleno - Sistema: Lleno	
5	**PLANTILLAS ADMINISTRATIVAS**		
5.1	Sistema		
5.1.1	Llamada a proceso remoto		
5.1.1.1	La autenticación de RPC Enpoint Mapper Client (sólo SP2)	(No definido)	Habilitado

5.1.1.2	Restricciones para los clientes de RPC no legalizado (sólo SP2)		
5.2	Red		
5.2.1	Conexiones de Red		
5.2.1.1	Firewall de Windows		
5.2.1.1.1	Perfil de Dominio		
5.2.1.1.1.1	Protege todas las conexiones de red (sólo SP2)	Habilitado	Habilitado
5.2.1.1.1.2	No permite excepciones (sólo SP2)	Inhabilitado	Habilitado
5.2.1.1.1.3	Permite las excepciones de programa locales	Habilitado	Inhabilitado
5.2.1.1.1.4	Permite la excepción de administración remota	Habilitado; defina subred(s) usadas sólo para soporte interno	Inhabilitado
5.2.1.1.1.5	Permite archivo y el impresor que divide la excepción (sólo SP2)	Habilitado	Inhabilitado
5.2.1.1.1.6	Permita excepciones ICMP (sólo SP2)	(No definido)	Inhabilitado
5.2.1.1.1.7	Permita excepciones de escritorio remoto (sólo SP2)	Habilitado; defina subred(s) usadas sólo para soporte interno	Inhabilitado
5.2.1.1.1.8	Permita excepciones UPnP framework (sólo SP2)	Habilitado; defina subred(s) usadas sólo para soporte interno	Inhabilitado
5.2.1.1.1.9	Prohíba notificaciones	Inhabilitado	Habilitado
5.2.1.1.1.10	Registrar paquetes caídos (sólo SP2)	Registre paquetes pequeños caídos	Registre paquetes pequeños caídos, perdidos.
5.2.1.1.1.11	Registre ruta de archivo y nombre (sólo SP2)	Registre la ruta del archivo y el nombre:	Registre la ruta del archivo y el nombre:

		%SystemRoot%\firewall_domain.log	%SystemRoot%\firewall_domain.log
5.2.1.1.1.12	Registre el límite de tamaño del archivo (sólo SP2)	Tamaño limite (KB): 4096	Tamaño limite (KB): 4096
5.2.1.1.1.13	Registre éxito de conexión (sólo SP2)	(No definido)	Registro conexión exitosa
5.2.1.1.1.14	Prohíba respuesta de unicast a multicast o broadcast (sólo SP2)	Habilitado	Habilitado
5.2.1.1.1.15	Defina excepciones de puertos (sólo SP2)	(No configurado)	(No configurado)
5.2.1.1.1.16	Permita excepciones de puertos locales (sólo SP2)	Habilitado	Inhabilitado

5.2.1.1.2	Perfil Estándar		
5.2.1.1.2.1	Proteja todas las conexiones de red (Sólo SP2)	Habilitado	Habilitado
5.2.1.1.2.2	No permita excepciones (Sólo SP2)	Habilitado	Habilitado
5.2.1.1.2.3	Permita excepciones de programas locales (Sólo SP2)	Inhabilitado	Inhabilitado
5.2.1.1.2.4	Permita excepciones de administración remota (Sólo SP2)	Inhabilitado	Inhabilitado
5.2.1.1.2.5	Permita excepciones de archivos e impresoras compartidas (Sólo SP2)	Inhabilitado	Inhabilitado
5.2.1.1.2.6	Permita excepciones ICMP (sólo SP2)	Habilitado; Permita apagar la salida de ruta del recurso, Permita la solicitud repetida de entrada en ruta, Permita paquetes muy grandres en salida de ruta.	Inhabilitado
5.2.1.	Permita excepciones de escritorio remoto (sólo SP2)	Inhabilitado	Inhabilitado

1.2.7			
5.2.1.1.2.8	Permita excepciones UPnP framework (sólo SP2)	Inhabilitado	Inhabilitado
5.2.1.1.2.9	Prohíba notificaciones (sólo SP2)	Inhabilitado	Habilitado
5.2.1.1.2.10	Registre paquetes pequeños caídos o perdidos (Sólo SP2)	Registre paquetes pequeños caídos	Registre paquetes pequeños caídos, perdidos.
5.2.1.1.2.11	Registre ruta de archivo y nombre (sólo SP2)	Registre archivo y nombre: %SystemRoot%\firewall_standard.log	Registre archivo y nombre: %SystemRoot%\firewall_standard.log
5.2.1.1.2.12	Registre limite de tamaño del archivo (sólo SP2)	Tamaño limite (KB): 4096	Tamaño limite (KB): 4096
5.2.1.1.2.13	Registre Conexión exitosa (Sólo SP2)	(No definido)	Registro conexión exitosa
5.2.1.1.2.14	Prohíbe respuesta de unicast a multicast o Broadcast (Sólo SP2)	Habilitado	Habilitado
5.2.1.1.2.15	Defina excepciones de puertos (sólo SP2)	(No configurado)	(No configurado)
5.2.1.1.2.16	Permita excepciones de puertos locales (sólo SP2)	Inhabilitado	Inhabilitado
5.3	Componentes de Windows		
5.3.1	Centro de Seguridad		
5.3.1.1	Vaya al Centro de seguridad (Sólo PCs de Dominio) (Sólo SP2)	Habilitado	Habilitado

BIOGRAFÍA

José Luis Cruz, nacido el 1 de febrero de 1983 en la ciudad de Puyo provincia de Pastaza, hijo de Gonzalo Cruz y Fanny Montero, vivió su niñez en diferentes ciudades debido al trabajo de su padre de profesión Militar; su educación primaria la realizo en la escuela COMIL No.10, su bachillerato lo consiguió en el Colegio Particular “Jesús de Nazareth” de la ciudad de Quito, egresado como Bachiller en Ciencias de la Computación, siguiendo con sus estudios ingresa a la universidad Escuela Politécnica del Ejército, ahí dedica 5 años de su vida a la formación de su profesión en la carrera de Ingeniería en Sistemas e Informática.

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR

JOSÉ LUIS CRUZ MONTERO

_____

José Luis Cruz Montero

COORDINADOR DE CARRERA

INGENIERO DANILO MARTÍNEZ

_____

Ing. Danilo Martínez

Sangolquí, 21 de Octubre del 2010

Contenido

RESUMEN 1

CAPÍTULO I 2

PLAN DE TESIS 2

Introducción 3

Justificación e Importancia 4

Objetivos 5

Objetivo General 5

Objetivos Específicos 5

Situación Actual 6

Alcance 7

Limitaciones 9

Metodología de aplicación 9

La investigación 9

Herramientas de Desarrollo 10

HERRAMIENTAS DE DETECCIÓN DE VULNERABILIDADES 10

Investigación de Aplicación del Hardening 11

Factibilidad 14

Factibilidad técnica 14

Factibilidad económica 15

Factibilidad operativa 15

Presupuesto y Cronograma de Trabajo 16
PRESUPUESTO 16
CRONOGRAMA 17
Bibliografía utilizada en Plan de Tesis 18
CAPÍTULO II 19
Marco Teórico 19
Hardening de MICROSOFT Windows 20
Introducción 20
Hardening 22
¿Qué es la seguridad? 23
El dilema de la seguridad 24
Enemigos de la seguridad 27
Lo que a Windows le hace falta 28
¿Qué podemos conseguir realmente? 30
Características generales de HARDENING 32
Endurecimiento de sistemas Microsoft Windows 35
Consideraciones de software 36
Consideraciones de hardware y red 38
Recolección de la información sobre seguridad aplicada en los sistemas de operativos Microsoft 40
Aplicación de Testers para análisis de riesgos 41
Comprobación del sistema 43

Prueba de gestión de sesiones 44

Evaluación (Assess): 44

Manejo de herramientas 45

Microsoft Baseline Security Analyzer 46

NG ScoringTool 47

Análisis de vulnerabilidades - Sectores de Acción y afectación 50

Manejo del Editor de Registros de Windows 52

Introducción al registro de Windows 52

HKEY_CLASSES_ROOT 59

HKEY_CURRENT_USER 60

HKEY_LOCAL_MACHINE 60

HKEY_USERS 60

HKEY_CURRENT_CONFIG 60

HKEY_DIN_DATA 60

Realizar una copia de seguridad del Registro 61

- Utilizar un archivo de entradas del Registro (.reg) 63

Cómo agregar, modificar o eliminar subclaves y valores del Registro mediante un archivo de entradas de registro (.reg) 64

Utilizar Instrumental de administración de Windows 69

CAPÍTULO III 72

VULNERABILIDAD 72

Niveles de seguridad Hardening 73

Ciclos de vida de Hardening 76
Evaluación 76
Diseño 77
Implementar 78
Administración y Soporte 78
Usos de Services Packs 78
Service Packs y Hotfixes 78
Análisis de Configuraciones básicas por defecto 79
Requisitos básicos de los sistemas en el campo de la seguridad 83
Bluetooth 83
Permisos de DCOM 84
Permisos de RPC 85
Permisos de WebDAV 85
Windows Firewall 86
Wireless proveedor de servicios 86
Protección de ejecución de datos 87
El centro de seguridad 87
DTC Control 88
La conexión en el viaje de ida de datos con alto tráfico 88
Configuraciones que causan problemáticas 88
Restricciones adicionales para las conexiones anónimas 89

Restrinja acceso de disco compacto para entrar en el sistema localmente 90
Quite las porciones administrativas en el puesto de trabajo (profesional) 90
Los permisos de archivo y de registro 90
CAPÍTULO IV 91
APLICACIÓN HARDENING 91
Service Packs y actualizaciones de seguridad 92
Necesidades MAYORES de Service Pack y Hotfix 92
Necesidades MENORES de Service Pack y Hotfix 93
Auditoría y políticas de cuentas 93
Principales características de Auditoría, de políticas de cuenta y Requisitos 94
Menores características de Auditoría, de políticas de cuenta y Requisitos 97
Configuración de seguridad 105
Mayores Configuraciones de seguridad 106
Menores Configuraciones de seguridad 110
Protección de Seguridad Adicional 126
Servicios del sistema 127
Más alerta 128
Actualizaciones automáticas 128
Derechos de usuario 135
Otros Requisitos del sistema 143
Permisos de archivos y entradas del Registro 147

Plantillas administrativas 148
Sistema 148
Red 149
Componentes de Windows 156
CAPÍTULO V 157
RESULTADOS 157
Manual de Aplicación Hardening 160
Tareas a realizar: 160
Modificar el archivo sceregvl.inf para cambio de código y aumento de seguridad. 174
Resultados 175
Elaboración de manual de configuraciones especiales 176
Objetivo 176
Aseguramiento Institucional 176
Manejo se software 177
Aplicación Syspred 177
Archivo de configuración de Sysprep 180
CONCLUCIONES 181
RECOMENDACIONES 182
BIBLIOGRAFÍA 183
ANEXOS 185
ANEXO A. MANUAL DE USUARIO NG SORING TOOL 186

NG Scoring Tool 186

Introducción a la herramienta de marcado de NG 186

Comparaciones lógicas avanzadas 187

Formatos de presentación de informes adicionales 187

Los archivo de Configuración 187

Descargar e instalar la herramienta de marcado de NG 188

Cómo ver el Registro del sistema en las versiones de 64 bits de Windows 208

ANEXO B. ARCHIVOS PARA CORRECIÓN DE VULNERABILIDADES EN REGEDIT 211

i. ARCHIVO PARA CORRECCIÓN POR CÓDIGO WINDOWS XP 212

COMPUTADOR TIPO 213

ii. ARCHIVO PARA CORRECCIÓN POR CÓDIGO WINDOWS SERVER 239

WINDOWS SERVER CONTROLADORES DE DOMINIO 240

WINDOWS SERVER SERVIDORES MIEMBROS DE DOMINIO 245

ANEXO C. CHECKLISTS 250

BIOGRAFÍA 264

HOJA DE LEGALIZACIÓN DE FIRMAS 265