Asegurando los sistemas Windows

Miguel Macías Enguídanos

Universidad Politécnica de Valencia

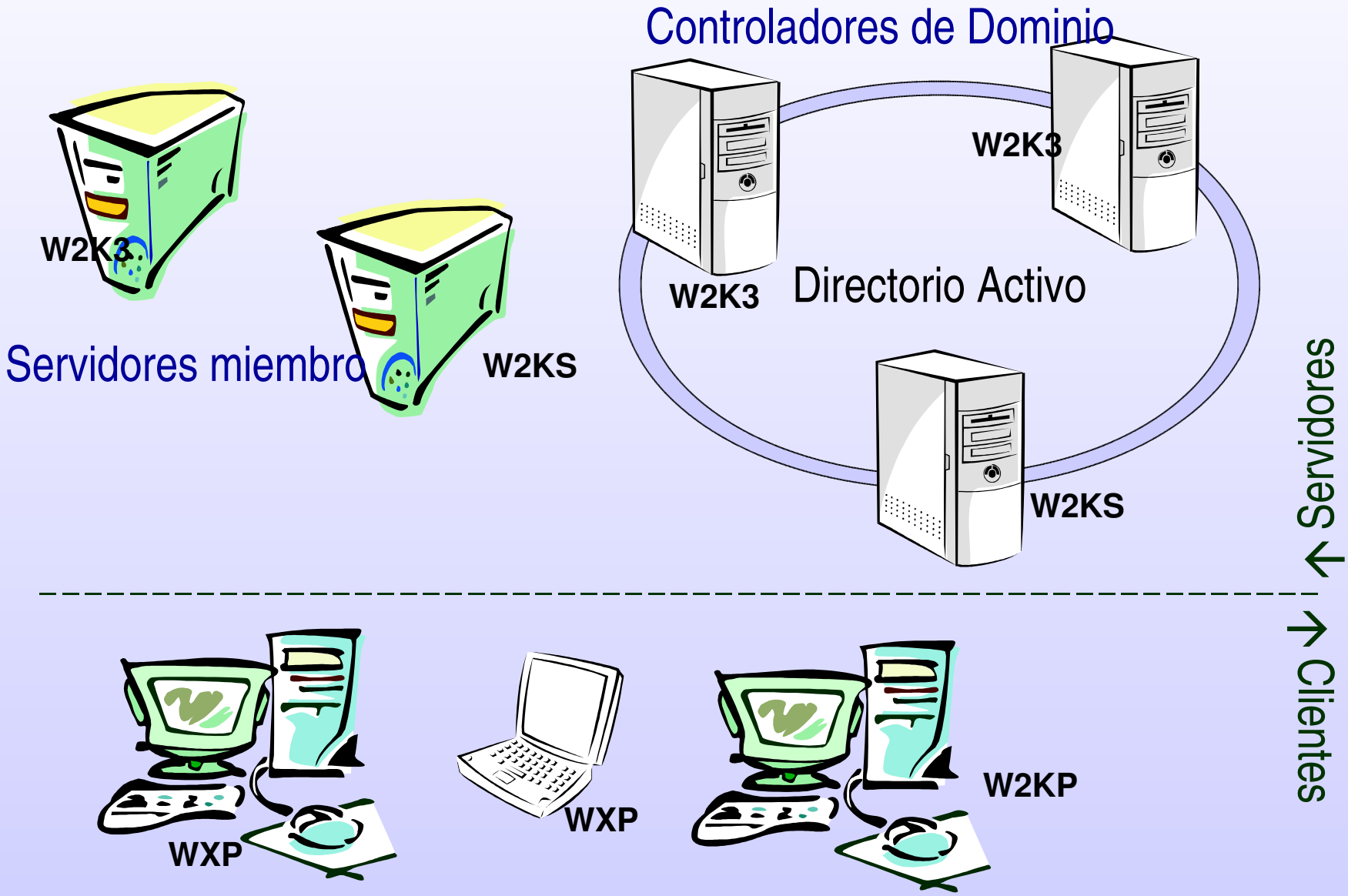
Contenido

- Introducción
- Cuentas de usuario y contraseñas
- Configurando los servicios
- Manteniendo la configuración

Introducción

- La red Windows
- Directivas de grupo
- Plantillas de seguridad

La red Windows



Directivas de grupo

- definen la configuración de equipos y usuarios y son la herramienta fundamental para la gestión centralizada
- los parámetros de configuración se establecen en los objetos de directivas de grupo (GPO) y éstos se enlazan a los contenedores del Directorio Activo
- cada GPO tiene un apartado para la configuración del equipo y un apartado para la configuración del usuario

  Step-by-Step Guide to Understanding the Group Policy Feature Set

  - http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/gpfeat.mspx

Aplicación de las Directivas de grupo

- para determinar qué GPOs se aplican a un objeto (equipo o usuario), se localiza a éste en el Directorio Activo y se recorre la jerarquía de contenedores
- un GPO se aplicará si:
  - no está deshabilitado
  - la cuenta (de equipo o usuario) tiene permisos para leer y aplicar la directiva
  - los parámetros de configuración correspondiente (de equipo o de usuario) no están deshabilitados
- los equipos que no forman parte del Directorio Activo cuentan solo con la Directiva Local

Directivas de grupo: orden de procesamiento

- el orden de aplicación de las directivas de grupo es el siguiente:
  - directiva de grupo Local
  - directivas de grupo del Sitio
  - directivas de grupo del Dominio
  - directivas de grupo de las Unidades Organizativas (desde el nivel más alto en la jerarquía hasta la Unidad Organizativa que contiene al objeto)
- *"El que ríe el último, ríe mejor"*
- si hay varias directivas al mismo nivel, se procesan según la prioridad establecida entre ellas

Directivas de grupo: alterando el orden de procesamiento

- a un contenedor (Sitio, Dominio o Unidad Organizativa) se le puede indicar que bloquee la herencia de directivas
- sin embargo, al vincular un objeto de Directiva de Grupo, se puede marcar como No omitir. Esta configuración tiene preferencia sobre la anterior
- el bucle invertido permite cambiar la lista de directivas que se aplicarán a los usuarios de un equipo. Tendrá prioridad (o reemplazará) la lista de directivas obtenidas para el equipo

Directivas de grupo: inicio de sistema

- cuando arranca el equipo se suceden los siguientes eventos:

  se inicia la red y se pone en marcha el servicio RPC

  se obtiene la lista ordenada de GPO aplicables (dependiendo de la ubicación de la cuenta de equipo en el Directorio)

  se aplican los parámetros de configuración correspondientes al equipo (de forma sincrónica)

  se ejecutan las secuencias de comandos de inicio de forma oculta y sincrónica (*timeout* predeterminado: 600 segundos)

  aparece la interfaz de usuario

Directivas de grupo: inicio de sesión

- cuando un usuario inicia sesión se suceden los siguientes eventos:
  - se valida al usuario mediante sus credenciales
  - se obtiene la lista ordenada de GPO aplicables (dependiendo de la ubicación de la cuenta de usuario en el Directorio y de la propiedad de bucle invertido en el equipo)
  - se aplican los parámetros de configuración correspondientes al usuario (de forma sincrónica)
  - se ejecutan las secuencias de comandos de inicio (de forma oculta y sincrónica) y el script de inicio de sesión (visible)
  - aparece la interfaz de usuario

Directivas de grupo: herramientas

- ***gpupdate***: fuerza la aplicación de las directivas apropiadas

  las directivas de grupo se aplican (por defecto) cada 5 minutos en los controladores de dominio y cada 90 minutos en el resto de equipos

  en W2K no existe gpudate y se utiliza un parámetro de secedit:

  - secedit /refreshpolicy {machine_policy | user_policy} /enforce
- ***gpresult***: muestra los GPO que se están aplicando al usuario y el equipo especificados
- ***RSOP.msc***: muestra el conjunto resultante de directivas (*Resultant Set Of Policy*) para un usuario o equipo

Directivas de grupo: herramientas

- ***gpedit.msc***: herramienta gráfica para la gestión de las Directivas de Grupo (si se invoca directamente, carga la Directiva Local)
- ***secpol.msc***: configuración de seguridad local
- ***secedit***: configuración y análisis de la seguridad por comparación con plantillas predefinidas
- ***dcgpofix***: restaura las directivas predeterminadas para el dominio y los controladores de dominio
- ***plantillas administrativas*** *(*.adm)*: son plantillas que definen qué parámetros (con sus claves de registros asociadas) contienen las directivas

Plantillas de seguridad

- son ficheros que contienen parámetros de configuración relativos a la seguridad
- se pueden aplicar directamente a un equipo o a través de Directivas de Grupo
- Microsoft proporciona una serie de plantillas ya definidas que son un buen punto de partida para la configuración de los equipos (*%systemroot%\security\templates*)
- se pueden definir nuevas plantillas de seguridad para cada rol utilizado, pero es conveniente probarlas antes de aplicarlas y prestar atención a su tamaño (si se van a usar mediante Directivas de Grupo)

Plantillas de seguridad: parámetros configurables

- en las plantillas se pueden especificar siete categorías de parámetros relacionados con la configuración del equipo:

  Directivas de cuenta

  - establece la seguridad de las cuentas locales y de dominio
  - contiene: directiva de contraseñas, directiva de bloqueo de cuentas y directiva Kerberos

  Directivas locales

  - determinan la seguridad en el equipo local
  - contiene: directiva de auditoría, asignación de derechos de usuario y opciones de seguridad

Plantillas de seguridad: parámetros configurables

Registro de sucesos

- controla el comportamiento de los registros de sucesos de aplicación, sistema y seguridad

Grupos restringidos

- mantiene la pertenencia a grupos importantes para la seguridad y el anidamiento de estos grupos

Servicios del sistema

- inicio y permisos de los servicios del sistema

Registro

- permisos para las claves del Registro del sistema

Sistema de archivos

- permisos de archivos y carpetas

Plantillas de seguridad: plantillas predefinidas

- seguridad predeterminada (*setup security*)

  configuración predeterminada que se aplica en la instalación

  se usa para la recuperación de desastres

- compatible (*compat**)

  da mayores privilegios a los usuarios para que puedan utilizar aplicaciones no certificadas Windows

  no debería aplicarse a Controladores de Dominio

- segura (*secure**)

  seguridad mejorada con configuraciones de contraseña, bloqueo y auditoría más rigurosas. Deshabilitan LM y NTLM

Plantillas de seguridad: plantillas predefinidas

- de alta seguridad (*hisec**)

  imponen mayores restricciones en los niveles de cifrado y firmado utilizados en la autenticación, en SMB y en los canales protegidos

  limita el uso de datos de inicio de sesión en caché y utiliza grupos restringidos para que no haya Usuarios Avanzados y para controlar el grupo Administradores

- seguridad de la raíz del sistema (*rootsec*)

  define los permisos para la raíz de la unidad del sistema

- SID de usuario que no es de Terminal Server (*Notssid*)

  es mejor utilizar TS en modo de seguridad total

Plantillas de seguridad: herramientas

- ***plantillas de seguridad***: es un complemento MMC que permite crear y modificar plantillas de seguridad
- ***configuración y análisis de seguridad***: complemento MMC que permite analizar y aplicar la configuración de seguridad del equipo local mediante plantillas de seguridad

  el análisis se realiza comparando la seguridad actual con la almacenada en una Base de Datos creada a partir de plantillas (se combinan dando preferencia a la última)
- ***secedit***: permite todas las opciones del complemento anterior y se puede usar de manera automática

Cuentas de usuario y contraseñas

- Opciones de seguridad de cuentas
- Seguridad de las contraseñas
- Transmisión de contraseñas por la red
- Almacenamiento de credenciales
- Permisos
- Derechos

Cuentas de usuario y contraseñas

- desde un punto de vista histórico, las contraseñas son el mayor riesgo de seguridad para las redes
- las opciones de seguridad de cuentas se pueden establecer para las cuentas globales (con un GPO enlazado a nivel de dominio) o para las cuentas locales (con GPO enlazadas a Unidades Organizativas)
- hay que tener presente:

  las opciones de seguridad de cuentas

  la seguridad de las contraseñas

  los permisos y derechos de los usuarios

contraseñas: Opciones de seguridad de cuentas

- se establecen desde la herramienta *Usuarios y Equipos de Active Directory*, en las propiedades del usuario
- o con la utilidad *net user* desde la línea de comandos
- parámetros configurables:

horas de inicio de sesión	estaciones de trabajo
forzar cambio de contraseña	impedir cambio de contraseña
caducidad de la cuenta	deshabilitar la cuenta
impedir la caducidad de la contraseña	delegación de la cuenta
requerir tarjeta inteligente	autenticación Kerberos previa
usar cifrado DES	

Cuentas de usuario y contraseñas: Seguridad de las contraseñas

- Mediande directivas de grupo se pueden establecer los parámetros de seguridad aplicables a las contraseñas:

directivas de contraseñas

Directiva	Configuración de seguridad
Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio	Deshabilitada
Forzar el historial de contraseñas	0 contraseñas recordadas
Las contraseñas deben cumplir los requerimientos de complejidad	Deshabilitada
Longitud mínima de la contraseña	0 caracteres
Vigencia máxima de la contraseña	0
Vigencia mínima de la contraseña	0 días

directiva de bloqueo de cuentas

Directiva	Configuración de seguridad
Duración del bloqueo de cuenta	No aplicable
Restablecer la cuenta de bloqueos después de	No aplicable
Umbral de bloqueos de la cuenta	0 intentos de inicio de sesión incorrectos

Cuentas de usuario y contraseñas: Seguridad de las contraseñas

- los requerimientos de complejidad para las contraseñas obligan a que éstas tengan como mínimo 8 caracteres e incluyan caracteres de 3 de estas 4 categorías:
  - letras mayúsculas (alfabeto inglés)
  - letras minúsculas
  - números
  - caracteres no alfanuméricos (~!@#$%^&*_-+=|\{}[]:;'<>,.?/)
- Por defecto se usa *passfilt.dll*, pero se puede cambiar:

  How To Password Change Filtering & Notification in Windows NT
  - http://support.microsoft.com/default.aspx?scid=kb;en-us;151082

contraseñas: Transmisión de contraseñas por la red

- El protocolo de autenticación utilizado determina cómo se transmiten las credenciales a través de la red y cómo se almacenan

  LM (*LAN Manager*)

  - muy vulnerable a los ataques de diccionario y fuerza bruta
  - para eliminar los *hash* de las contraseñas en la SAM y el AD:
    - establecer la directiva asociada en un GPO o
    - HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash= 1 (DWORD)

  NTLM (*NT LAN Manager*)

  - tampoco almacena las contraseñas en claro, pero es mucho más robusto que LM

contraseñas: Transmisión de contraseñas por la red

NTLMv2

- varía, sobre todo, el proceso de autenticación
- requiere la sincronización de los relojes de clientes y servidores
- la directiva nivel de autenticación de LAN Manager permite habilitar este tipo de autenticación e impedir el uso de LM

Kerberos

- es el protocolo de autenticación predeterminado desde W2K
- se puede configurar desde las Directivas de Grupo (para cuentas de dominio, no existe a nivel local)
  - forzar restricciones de inicio de sesión de usuario
  - vigencia máxima del vale de servicio / usuario
  - vigencia máxima de renovación de vales de usuario
  - tolerancia máxima para la sincronización de los relojes de los equipos

contraseñas: Almacenamiento de credenciales

- Además de las contraseñas presentes en la SAM y el DA, Windows almacena otras credenciales por distintos motivos:
  - la autoridad de seguridad local (LSA) almacena información conocida como secretos LSA (nombres de usuarios, contraseñas y nombres de cuentas, contraseñas para servicios, …)
  - las cuentas de dominio utilizadas para iniciar sesión se almacenan en una caché (cifrado de manera irreversible)
  - XP introduce un nuevo método de administrar credenciales para los recursos disponibles (*cmdkey*)
- con la utilidad *Windows System Key Protection* (*Syskey*) se puede incrementar la seguridad de los secretos almacenados
  - establece la “clave maestra” utilizada para proteger la clave de cifrado de contraseñas y puede eliminarse del sistema

Cuentas de usuario y contraseñas: Permisos y derechos

- los permisos definen los recursos a los que las cuentas tienen acceso y el nivel permitido
- son válidos para los objetos del Directorio Activo, del Sistema de Archivos y las claves del Registro
- los derechos son acciones u operaciones que una cuenta puede o no realizar
- se dividen en privilegios y derechos de inicio de sesión
- si existe conflicto, los derechos (los privilegios) tienen prioridad sobre los permisos

Cuentas de usuario y contraseñas: Permisos

- cada objeto tiene una lista de control de acceso con permisos heredados y explícitos
  - en el Sistema de Archivos sólo NTFS permite esta seguridad
- el orden de aplicación es:
  - denegar explícito (tiene prioridad sobre todos los demás)
  - otorgar explícito (prioridad sobre la denegación heredada)
  - denegar heredado (prioridad sobre los otorgados por herencia)
  - otorgar heredado
- los permisos se van acumulando y la cuenta recibe todos los permisos que le son aplicables

Cuentas de usuario y contraseñas: Permisos sobre Ficheros

- cuando se accede a través de la red se tiene en cuenta, también, la lista de control de acceso asociada al recurso compartido

  se obtienen dos conjuntos de permisos acumulando los equivalentes a *Compartir* y a *NTFS*. Al final se asigna el conjunto más restrictivo de ambos

- al crear o copiar un objeto, éste hereda los permisos establecidos en su nuevo contenedor
- cuando se mueve un objeto dentro de la misma partición mantendrá la herencia, pero del nuevo contenedor
- se puede bloquear la herencia de permisos

Cuentas de usuario y contraseñas: Asignación de Permisos

- la asignación de permisos se basa en los grupos de seguridad, siguiendo la estrategia: A – G – U – DL

  las cuentas de Usuario se agrupan en grupos Globales. Estos grupos se introducen en grupos Universales, con los que se rellenan los grupos de Dominio Local

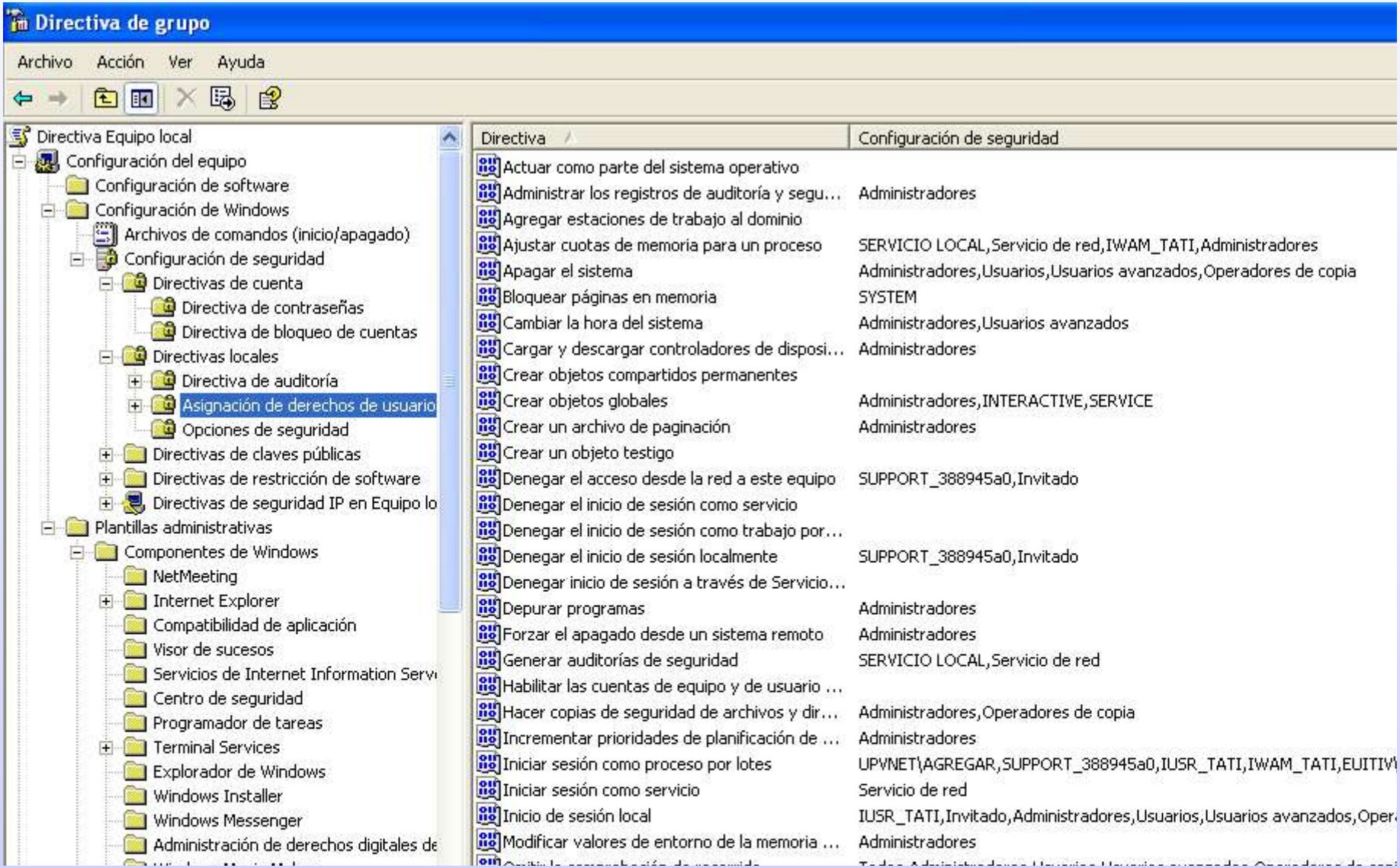
  se admiten las variaciones: A – G – DL, A – G – U, A – U

- se pueden forzar los permisos de los recursos con GPO
- el propietario de un objeto siempre tiene la potestad de cambiar sus permisos
- el grupo *Administradores* tiene concedido el derecho a tomar posesión de los objetos

Cuentas de usuario y contraseñas: Herramientas para Permisos

- ***cacls***: permite la gestión básica de permisos sobre ficheros y carpetas
- ***xcacls***: ofrece mayor control sobre los permisos especiales y puede formar parte de procesos por lotes
- ***subinacl***: opera sobre varios tipos de objetos (ficheros, carpetas, registro, servicios, …) a bajo nivel. Permite *regalar* la propiedad de un objeto
- ***dsacls***: gestiona permisos de los objetos del DA
- ***robocopy***: útil para replicar estructuras de carpetas
- ***whoami***: muestra los SID asociados a una cuenta

Cuentas de usuario y contraseñas: Derechos



Configurando los servicios

- Seguridad en TCP/IP
- Servicios
- Servicio DNS
- Servicios de Terminal Server
- Servicio DHCP
- Servicio WINS
- Enrutamiento y Acceso Remoto
- Servicios de Certificate Server
- Internet Information Server (IIS)

Seguridad en TCP/IP

- para prevenir los ataques de DoS se puede endurecer la pila de protocolos TCP/IP a través de los siguientes parámetros del registro:

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

EnableICMPRedirect	0	SynAttackProtect	2
TCPMaxConnectResponseRetransmissions	2	TCPMaxHalfOpen	500
TCPMaxHalfOpenRetired	400	TCPMaxPortsExhausted	5
TCPMaxDataRetransmissions	3	EnableDeadGWDetect	0
EnablePMTUDiscovery	0	DisableIPSourceRouting	2
NoNameReleaseOnDemand*	1	PerformRouterDiscovery	0

* en …\Services\Netbt\Parameters

estos valores se pueden introducir en una directiva de grupo para aplicarlos a varios equipos

Seguridad en TCP/IP

- el servicio *Compartir impresoras y archivos para redes Microsoft* permite a otros equipos acceder a nuestros recursos.

  ha sido fuente de numerosos problemas y no es necesario para conectarse a recursos de otros equipos

  si se elimina de una interfaz de red, el equipo dejará de esperar conexiones SMB en los puertos 139 o 445

- el protocolo SMB puede implementarse directamente sobre TCP/IP, por lo que ya no es necesario *NetBIOS sobre TCP/IP*

  los sistemas W9x y algunas aplicaciones necesitan NetBT

Seguridad en TCP/IP

- si están activos *NetBT* y *SMB directo*, se prueban ambos métodos al mismo tiempo y se usa el primero que responda

  NetBT usa los puertos 137 (TCP y UDP) para el servicio de nombres, 138 (UDP) para el servicio de datagramas y 139 (TCP) para el servicio de sesión

  SMB directo usa el puerto 445 (TCP y UDP)

- Windows intenta actualizar el *registro DNS* correspondiente para cada adaptador

  esta opción se puede deshabilitar si no es conveniente

Seguridad en TCP/IP: filtros y cortafuegos

- se pueden establecer filtros TCP/IP comunes para todas las interfaces de red
  - los filtros están basados en puertos TCP, UDP y protocolos IP
  - pueden configurarse directamente en el registro, en HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- el cortafuegos está disponible para cada adaptador de red independientemente (no existe en W2K)
  - monitoriza el estado de las conexiones y permite definir las reglas basándose en los puertos, las direcciones, los mensajes ICMP, …
  - mantiene un registro de seguridad (en %windir%\pfirewall.log)

Seguridad en TCP/IP: IPSec

- IPSec ofrece autenticación y cifrado a bajo nivel
  - es transparente para las aplicaciones
- puede ponerse en marcha mediante Directivas que establezcan:
  - protocolo (AH, ESP o ambos)
  - modo (transporte o túnel)
  - métodos de autenticación (Kerberos, certificados o secreto)
  - políticas (predefinidas: cliente, servidor o servidor seguro)
- se puede monitorizar IPSec con la herramienta IPSecMon, con el complemento MMC o con el log

Seguridad en TCP/IP: herramientas

- ***netstat***: muestra la actividad y el estado de los puertos

  desde XP permite ver el proceso asociado a un puerto con -o
- ***tasklist***: muestra los procesos que se están ejecutando
- ***portqry***: realiza un escaneo y análisis de puertos
- ***ipconfig***: muestra la configuración TCP/IP
- ***nbtstat***: gestión de NetBIOS sobre TCP/IP
- ***netsh***: gestión de la configuración TCP/IP
- ***netdiag***: diagnósticos de conectividad

Servicios

- son las aplicaciones que se ejecutan independientemente de los usuarios

  srvany permite ejecutar cualquier aplicación como servicio

- la configuración de los servicios se almacena en el registro y éstos son controlados por el *Service Control Manager* (*services.exe*)
- los permisos sobre el SCM son fijos, pero se pueden modificar los permisos sobre los servicios
- para configurar los servicios está la consola ***services.msc***, aunque algunos valores solo se pueden establecer en el registro directamente

Servicios: seguridad

- Windows instala más de 100 servicios por defecto
- hay que dejar en marcha solo los imprescindibles para el funcionamiento del sistema

  Services That Are Turned Off by Default in Windows Server 2003

  - http://support.microsoft.com/default.aspx?scid=kb;en-us;812519
- las opciones a tener en cuenta son:

  el tipo de inicio (automático, manual, deshabilitado, sistema)

  el contexto de seguridad (la cuenta del sistema local tiene control total sobre todos los recursos y *pertenece* al grupo Administradores)

Servicios: herramientas

- ***net {start | stop}***: inicia o para un servicio
- ***net {pause | continue}***: detiene o reanuda un servicio
- ***subinacl***: gestiona los permisos del servicio
- ***services.msc***: herramienta gráfica para gestionar (excepto las listas de control de acceso) los permisos
- ***directivas de grupo***: permiten establecer la seguridad de los servicios (quién puede iniciar, pausar, …)
- ***sc***: gestiona los servicios y permite determinar cuáles no son necesarios para iniciar el sistema

Servicio DNS

- es necesario evitar los ataques contra los servidores y los clientes DNS utilizando las siguientes medidas:

  implementación de zonas integradas de Active Directory

  - permite almacenar los registros DNS en el Directorio, en lugar de en ficheros de texto
  - cada registro es un objeto del Directorio y, por tanto, puede tener su propia DACL individual

  servidores DNS internos y externos independientes

  - los servicios del Directorio se anuncian mediante registros de recursos SRV. Estos registros no deben ser accesibles desde el exterior de la red
  - aunque se tenga el mismo espacio de nombres en la red pública y en la privada es conveniente crear zonas independientes

Servicio DNS

restricción de transferencias de zona

- se pueden restringir las transferencias a direcciones IP o a los servidores enumerados en las propiedades DNS

implementación de IPSec entre servidores y clientes

- evita las consultas de clientes no autorizados al servidor interno

restricción del tráfico DNS en el cortafuegos

- habitualmente se impide que los clientes internos consulten servidores en Internet y que los clientes externos consulten nuestros servidores DNS

restringir la administración del servicio

- el grupo DNSAdmins permite la administración del DNS sin ofrecer permisos excesivos para otros servicios

protección de la caché DNS

Servicios de Terminal Server

- modo de funcionamiento

  solo habría que utilizar el modo de Servidor de Aplicaciones en servidores miembro y cuando sea estrictamente necesario

  el modo de Administración Remota permite una gestión bastante segura para administrar los CD

- restringir los usuarios y grupos que tienen el derecho a iniciar sesión localmente

  idealmente todos los Terminal Server estarán en una Unidad Organizativa y se les podrá aplicar el mismo GPO

- restringir las aplicaciones que se pueden ejecutar

  se puede cambiar el *shell* del usuario o utilizar ***Appsec***

Servicios de Terminal Server

- implementación de la forma más segura de cifrado

  bajo: se cifra solo desde el cliente al servidor con RC4 y claves de 40 o 56 bits (dependiendo de la versión de RDP)

  medio: se cifra en ambas direcciones con el algoritmo anterior

  alto: cifrado en ambas direcciones con claves de 128 bits (se necesita el *High Encryption Pack*)

- fortalecer la configuración de seguridad

  al instalar el servicio se puede activar la opción *Seguridad total*, con lo que no se utilizará un usuario específico para los servicios de Terminal Server (en caso contrario, aplicar la plantilla de seguridad *NoTSSID.inf*)

Servicio DHCP

- conservar el comportamiento predeterminado de registro de nombres
  - el servidor registra el recurso PTR y el cliente el recurso A
  - los clientes con IP estática registran los recursos A y PTR
- utilización del grupo DNSUpdateProxy
  - los servidores DHCP que pertenezcan a este grupo no tomarán posesión de los registros que inserten en el DNS
  - útil si se van a actualizar clientes a WXP (o W2K) o si hay varios servidores DHCP que registran información DNS para los mismos clientes

Servicio DHCP

- evitar el servicio DHCP en los Controladores de Dominio

  el CD ha de tener la posesión de sus registros A y SRV (problemático cuando se utiliza DNSUpdateProxy)

  para evitar que los registros DNS se realicen en el contexto de seguridad del CD se puede utilizar ***netsh*** para designar la cuenta de usuario que se utilizará

- revisar la Base de Datos y buscar *BAD_ADDRESS*

  indican direcciones IP duplicadas y pueden ser debidas a un ataque en curso

- controlar la pertenencia a *Administradores DHCP*
- habilitar la auditoría DHCP (*%windir%\system32\dhcp*)

Servicio WINS

- supervisar el grupo *Administradores de WINS*

  los miembros de este grupo pueden modificar la configuración del servidor, incluyendo la replicación y la inclusión de registros estáticos

- validar la configuración de replicación WINS

  si se elimina un servidor WINS de la red se pueden crear registros duplicados y falsos en la Base de Datos

- eliminar y decomisar aplicaciones NetBIOS

  se puede determinar si NetBIOS es necesario revisando, en cada servidor WINS, los contadores de *Monitor de Sistema*: cantidad total de registros, consultas y consultas correctas

Enrutamiento y Acceso Remoto: servidores

- implementación de la autenticación y cuentas RADIUS

  el servidor RADIUS es un servidor que ejecuta IAS (*Internet Authentication Service*) y puede colocarse detrás de un cortafuegos (es transparente a NAT)

  se conecta directamente a un Controlador de Dominio para validar las credenciales y ofrece directivas de acceso remoto centralizadas

- asegurar el tráfico entre los servidores de acceso remoto y el servidor RADIUS

  para evitar los ataques de inspección y fuerza bruta se puede emplear una directiva IPSec que requiera cifrado ESP

Enrutamiento y Acceso Remoto: servidores

- configuración de las directivas de acceso remoto

  las conexiones remotas se aseguran configurando las condiciones (restricciones de día y hora, identificación de la estación, nombre del cliente RADIUS, protocolo de entramado, tipo de tunel, …) y perfiles (restricciones de marcado, restricciones de IP, autenticación, cifrado, …) de cada directiva

- implantación de certificados para L2TP/IPSec

  los certificados de equipo son necesarios para IPSec y los de usuario para la autenticación EAP-TLS

  no es seguro el uso de secretos para IPSec. Hay que utilizar certificados

Enrutamiento y Acceso Remoto: servidores

- restringir los servidores que puedan ejecutar RRAS

  mediante Directivas de Grupo se puede garantizar que sólo los servidores autorizados puedan iniciar el RRAS

- bloqueo de cuentas de acceso remoto

  para evitar los ataques de diccionario en línea se pueden bloquear las cuentas de acceso remoto (sin afectar a la red local) agregando al registro las claves *MaxDenials* y *ResetTime*

- establecer un control de cuarentena

  característica nueva de W2K3 que impide la conexión remota de un equipo hasta que se comprueba su configuración

Enrutamiento y Acceso Remoto: clientes

- configuración de paquetes CMAK

  los paquetes de *Connection Manager* permiten configurar las opciones de seguridad (tipo de autenticación, cifrado, evitar guardar la contraseña, …)

- implementación de autenticación segura

  solo son recomendables MS-CHAPv2 (contraseñas) y EAP-TLS (certificados)

- implantación de certificados necesarios

  tanto para EAP-TLS como para L2TP/IPSec son necesarios certificados (que deberían emplearse con tarjetas inteligentes)

Servicios de Certificate Server

- implementar medidas de seguridad físicas
  - se puede crear una jerarquía de tres capas con la CA raíz y las de segundo nivel fuera de la red
- implementar medidas de seguridad lógicas
  - restringir la pertenencia al grupo Administradores de la CA
  - revisar los permisos de las carpetas *Certsrv* y *Certlog* (en *%systemroot%\system32*)
  - asignar permisos si se especifica una ubicación de carpeta compartida en la configuración del recurso *CertEnroll*
  - supervisar la pertenencia del grupo global *Publicadores de Certificados*

Servicios de Certificate Server

- modificar los puntos de publicación CRL y de certificados de CA

  han de publicarse en ubicaciones a las que todos los usuarios tengan acceso

- habilitar la comprobación CRL en todas las aplicaciones

  si una aplicación no realiza la comprobación CRL, los atacantes podrán utilizar un certificado revocado

- administrar permisos de plantillas de certificados

  se puede otorgar el permiso de *Leer* e *Inscribir* solo a grupos determinados

Internet Information Server (IIS)

- ha sido objeto de numerosos ataques y tiene una fama nefasta, pero las últimas versiones han mejorado considerablemente
- hay que garantizar que el servidor que albergará IIS sea seguro:

  minimizando los servicios que se ejecutan

  definiendo las cuentas de usuario para el acceso anónimo

  asegurando el sistema de archivos

  aplicando opciones de configuración para evitar los ataques de Denegación de Servicio

Internet Information Server (IIS)

- la configuración de seguridad para IIS se basa en:

  la autenticación de usuarios

  - anónima (usará una cuenta local para representar al usuario)
  - básica (las credenciales viajan en claro por la red)
  - de síntesis (se envía un resumen de la contraseña, pero se necesita este resumen en el Directorio Activo)
  - de Windows integrada (utiliza NTLM o Kerberos)
  - basada en certificados (es la opción más segura y menos flexible)

  los permisos del sitio Web

  - diferentes a los permisos NTFS y se aplican los más restrictivos

  canales de comunicación

  - implementando el cifrado SSL con claves de 128 bits

Internet Information Server (IIS): herramientas

- ***IIS Lockdown***: asegura IIS a todos los niveles

  la configuración se determina con plantillas

  el archivo *IISlockd.ini* contiene plantillas predefinidas y permite crear nuevas plantillas personalizadas

- ***URLScan***: es un filtro que analiza las solicitudes HTTP

  puede trabajar con IIS Lockdown o de manera independiente

  las solicitudes HTTP se analizan a partir del fichero de configuración *URLScan.ini* (en la carpeta *%systemroot%\system32\Inetsrv\URLScan*) y si deniega la petición, el servidor devuelve el error *Objeto no encontrado*, sin dar mayores explicaciones al cliente

Manteniendo la configuración

- Actualizaciones
- Auditoría
- Evaluación de la seguridad

Actualizaciones

- la mayoría de ataques pueden evitarse garantizando que los equipos tienen instaladas las últimas revisiones del Sistema Operativo
- Microsoft dispone de 3 tipos de actualizaciones:

  revisiones (*hotfixes*): solucionan un único problema y se desarrollan de manera rápida sin pruebas exhaustivas

  soluciones acumulativas (*roll-ups*): combinan varias revisiones y se prueban con mayor intensidad

  service packs: son colecciones con todas las revisiones distribuidas desde el lanzamiento inicial del Sistema. Pasan un período de prueba intenso (con versiones beta)

Actualizaciones

- cuando se lanza un parche, Microsoft distribuye un boletín de seguridad y se le aplica una clasificación:

  crítica: la vulnerabilidad tiene un gran riesgo (gusanos, …) y es necesario aplicar el parche inmediatamente

  importante: podría comprometerse la confidencialidad, integridad o disponibilidad de los datos. Debe aplicarse

  moderada: vulnerabilidad difícil de explotar o mitigable con medidas de seguridad. Evaluar si ha de aplicarse

  baja: vulnerabilidad con muy poco riesgo o con un impacto mínimo. Hay que estudiar si es necesario antes de probar y aplicar

Actualizaciones: gestión de revisiones

- notificación

  para saber cuándo se distribuye un nuevo parche se puede suscribir a las alertas por correo que distribuye Microsoft:

  - http://www.microsoft.com/security/bulletins/alerts.mspx

  también el CERT es una buena fuente de información:

  - http://www.cert.org

- evaluación

  es necesario determinar si el parche es necesario y en qué equipos hay que instalarlo

  el agrupamiento de equipos en Unidades Organizativas ayuda bastante en la implantación de los parches

Actualizaciones: gestión de revisiones

- obtención

  el Catálogo de *Windows Update* es la opción más cómoda para descargar los parches correspondientes a todos los Windows

- prueba

  para evitar efectos colaterales es conveniente instalar los parches en una red de prueba o lanzar un proyecto piloto

- implantación

  se pueden instalar los parches equipo por equipo, mediante Directivas de Grupo o con alguna herramienta de gestión

- validación

  mediante el Sistema de Archivos, el Registro o herramientas

Actualizaciones: herramientas

- todas las herramientas utilizan el catálogo de boletines de parches de seguridad (*MSSecure.xml*) para determinar las actualizaciones necesarias

  http://www.microsoft.com/technet/security/search/mssecure.cab

- ***Windows Update***: aplicación basada en Web válida para usuarios individuales (requiere *Internet Explorer*)
- ***Actualizaciones automáticas***: gestiona el proceso de las actualizaciones de forma más o menos desatendida

  se puede establecer una configuración uniforme de esta característica mediante Directivas de Grupo

Actualizaciones: herramientas

- ***SUS*** *(Software Update Services)*: permite mantener las actualizaciones en un servidor propio, pudiendo aprobar solo las requeridas

  se puede descargar gratuitamente desde

  - http://www.microsoft.com/windowsserversystem/sus

  permite una gestión completa utilizando GPO para establecer la configuración de las Actualizaciones automáticas

  si no se dispone del Directorio Activo se puede configurar el cliente SUS mediante el registro:

  - HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

- ***SMS***: incluye el *Software Update Services Feature Pack*

Auditoría

- antes de iniciar la auditoría hay que establecer qué sucesos se quieren registrar y cuándo (éxito o fallo)
- además, hay que establecer las opciones de configuración de los ficheros de *log*
- se puede indicar que el sistema pare si no puede registrar nuevos eventos (registro lleno)

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail= 1

  solo podrá iniciar sesión un administrador y el sistema no se recuperará hasta que no pueda registrar los sucesos

Auditoría: categorías

- acceso a objetos
  - registran los accesos a ficheros, impresoras y el registro
  - hay que configurar la lista de control de acceso del sistema (SACL) para cada objeto que se quiera auditar
  - pueden generar una gran cantidad de información y afectar el rendimiento de los sistemas
- acceso del servicio de directorio
  - hay que activarlo en todos los controladores de dominio (a través de un GPO) y especificar las SACL en los objetos que se quieran auditar
  - los sucesos correctos incluyen la replicación e incrementan considerablemente el tamaño de los registros

Auditoría: categorías

- cambio de directivas

  incluye los cambios en la asignación de derechos de usuario, las políticas de auditoría y las relaciones de confianza entre dominios

- seguimiento de procesos

  permite tener un registro detallado de la ejecución de procesos, incluyendo la activación del programa, su finalización, el acceso indirecto a objetos, …

  es muy útil para depurar aplicaciones y ver cómo funcionan, pero no se suele utilizar en un entorno de producción

Auditoría: categorías

- uso de privilegios

  detecta sucesos asociados con ataques comunes: apagado local o remoto de un equipo, carga y descarga de drivers, visionado del registro de seguridad, apropiamiento de objetos, actuar como parte del Sistema Operativo

  hay algunos derechos de usuario que no son auditados: depurar programas, omitir la comprobación de recorrido, crear un objeto testigo, reemplazar un testigo a nivel de proceso, generar auditorías de seguridad

  para registrar la *copia y restauración de ficheros y carpetas* hay que especificarlo en una directiva explícita

Auditoría: categorías

- administración de cuentas

  registra los cambios en las cuentas de usuario, grupos, cambios de contraseña y modificaciones de la política de seguridad de un equipo

  es conveniente registrar los sucesos correctos (permiten rastrear en caso de ataque) y erróneos (suelen corresponder a un administrador intentando elevar sus privilegios)

- sucesos de inicio de sesión

  registran la conexión y desconexión a/de un equipo

  es conveniente registrar los sucesos correctos (permiten comprobar el comportamiento y facilitar las investigaciones) y erróneos (permiten prevenir y responder ataques)

Auditoría: categorías

- sucesos de inicio de sesión de cuenta

  se registran en el controlador de dominio que valida las credenciales o en el equipo local

  el registro se realiza en el equipo donde se autentica la cuenta, a diferencia de los anteriores, que se crean en el equipo donde se utiliza la cuenta

  es conveniente registrar los sucesos correctos (permiten comprobar el comportamiento) y erróneos (indicios de ataque)

- sucesos del sistema

  borrado de los registros de sucesos, apagado del equipo, …

Auditoría: monitorización de los registros

- el Visor de sucesos (*eventvwr.msc*) permite ver los detalles, buscar, filtrar, ordenar y exportar
- ***dumpel*** (*Dump Event Log*) permite exportar y filtrar los registros de varios equipos
- *Event Comb* (*Eventcombmt.exe*) permite consolidar los registros de varios equipos y hacer búsquedas sobre el resultado final

  para relacionar sucesos que ocurren en distintos equipos hay que asegurar que tengan sincronizados los relojes
- es habitual escribir scripts que indaguen en los registros buscando comportamientos sospechosos

Evaluación: herramientas

- para comprobar que las Directivas de Grupo se están aplicando como se pensaba:

  gpresult: muestra los GPO que se están aplicando al usuario y el equipo especificados

  RSOP.msc: muestra el conjunto resultante de directivas una vez aplicadas todos los GPO

  secedit: configuración y análisis de la seguridad por comparación con plantillas predefinidas

  - existe el complemento MMC Configuración y análisis de seguridad con la misma funcionalidad

  gpupdate: fuerza la aplicación de las directivas apropiadas

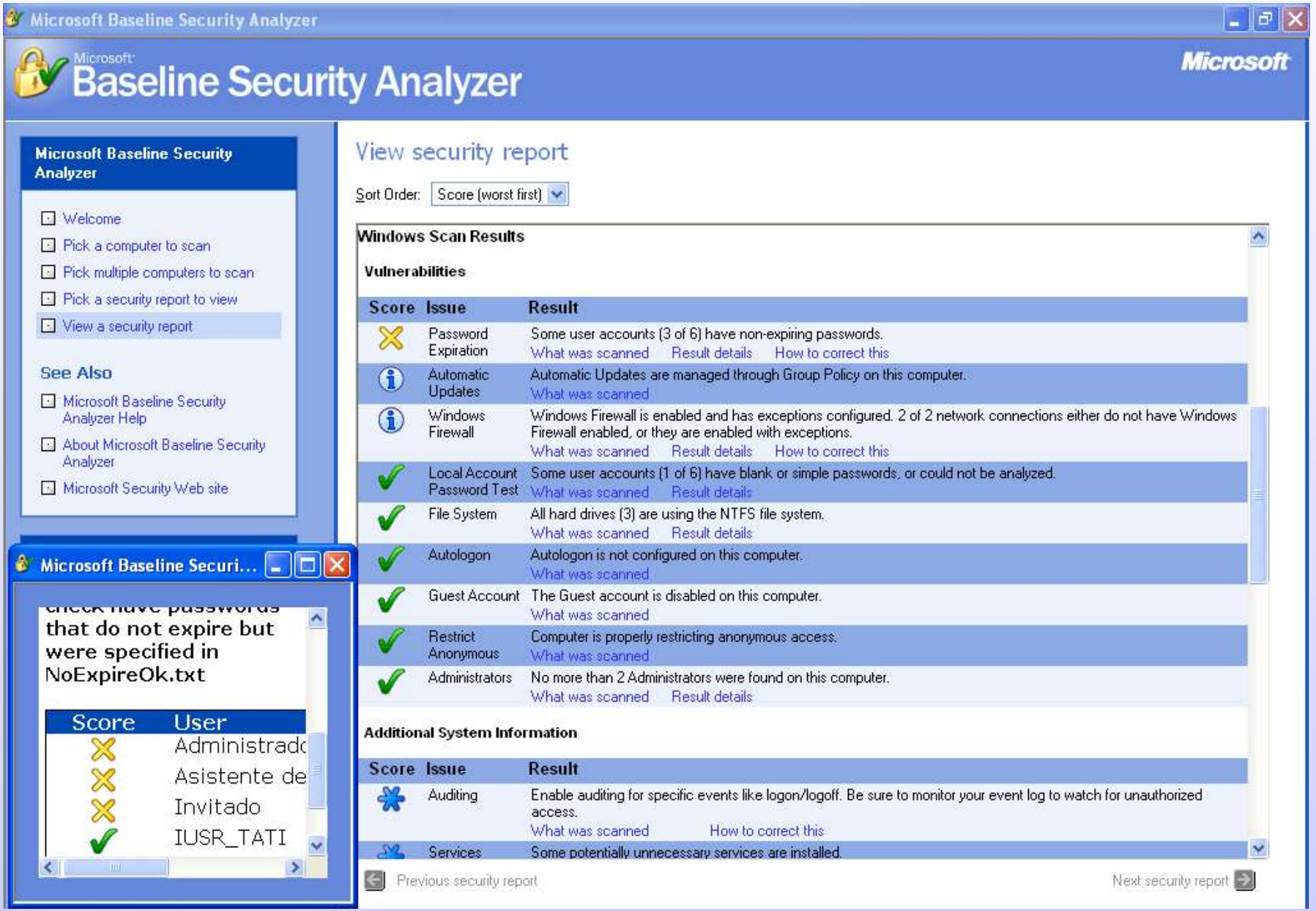
Evaluación: herramientas

- para comprobar que los parches están instalados y efectuar un repaso global de la configuración de seguridad en los equipos:

  MBSA (Microsoft Baseline Security Analyzer): analiza las opciones de seguridad erróneas comunes

  - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
  - se puede utilizar en modo gráfico o desde procesos automáticos
  - comprueba los parches instalados, la configuración de seguridad del Sistema Operativo (servicios innecesarios, grupo Administradores, contraseñas, …), el servicio IIS (directorios virtuales, aplicaciones de ejemplo, …), SQL Server (sysadmin, contraseñas, permisos, …) y las aplicaciones de escritorio (Internet Explorer, Office, …)

Evaluación: herramientas



Evaluación: herramientas

- para comprobar los puertos abiertos y los procesos que los utilizan:

  netstat: muestra la actividad y el estado de los puertos, así como el PID de los procesos correspondientes

  tasklist: muestra los procesos que se están ejecutando

  portqry: realiza un escaneo y análisis de puertos, con soporte para LDAP, RPC, DNS, NetBIOS, SNMP, TFTP, L2TP, …

  netsh: permite mostrar y modificar la configuración TCP/IP de un equipo local o remoto. Puede automatizarse completamente