MODULO III
Seguridad en Servidores

PROGRAMA

1. Seguridad física
2. Seguridad en W2K. Infraestructura de seguridad
3. Autenticación en W2K
4. Configuración segura de W2K. Seguridad de recursos
5. Registro de eventos de seguridad en W2K
6. Seguridad de servicios de red en W2K.
7. Seguridad en UNIX
8. Control de acceso y contraseñas. Permisos en directorios
9. Administración de usuarios
10. Aseguramiento de servidores de red en UNIX
11. Análisis de bitácoras

Seguridad Física

Seguridad Física

- La selección e implantación de controles físicos como resultado del análisis de riesgos:
  - Controles de acceso físico
    - Perímetro de seguridad física
    - Acceso sólo a personal autorizado a las áreas protegidas ...

¿Qué pasa si los controles de fallan y un atacante en potencia tiene acceso directamente a los equipos?

Escenario

- Amenaza
  - Competidor

- Actos Amenazantes
  - Un intruso contratado por un competidor logra burlar los controles de acceso a las áreas protegidas. Logra llegar al centro de datos, obteniendo acceso físico a los servidores que soportan el sistema crítico.

Escenario (cont)

- Actos Amenazantes
  - Destrucción o daño físico
    - Apagado de equipos (D)
    - Desconexión de cables eléctricos y de comunicaciones (D)
    - Derribamiento de equipos (D, I)
    - Robo de medios de almacenamiento (C)
    - Robo total (C)

Escenario (cont)

- Actos Amenazantes
  - Acceso a sistema operativo y aplicaciones
    - Instalación de puertas traseras (C, I)
    - Activación de módems (C, I)
    - Robo de bases de datos (C)
    - Alteración de bases de datos (I)
    - Cambio de contraseñas en sistema operativo (C, I, D)
    - Cambio de contraseñas en aplicaciones (C, I, D)

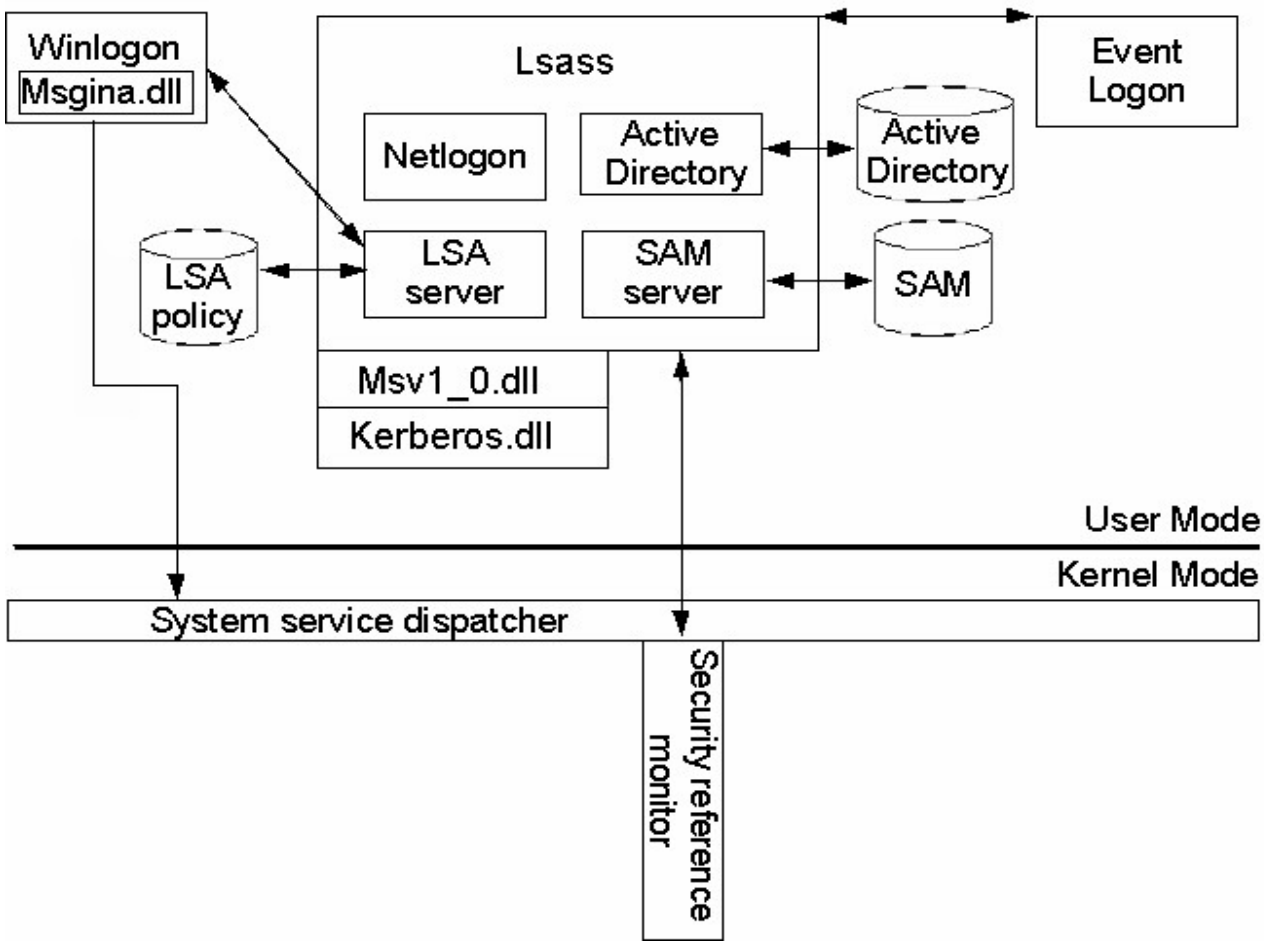
Security-in-depth

- Seguridad en profundidad

  - El establecimiento de controles/salvaguardas de seguridad en diferentes capas, de modo que el compromiso de una de ellas no deje al descubierto los recursos que requieren protección

  - En el caso del compromiso de los controles de acceso físico a las áreas protegidas
    - Establecer una capa de adicional limitando lo que puede hacerse en los equipos

Subsistema de Seguridad de W2K



Acceso físico: Compromiso W2K

SEKUREIT CONSULTORES EN SEGURIDAD INFORMATICA

- Obtención de acceso de *Administrator*
  - Iniciar el servidor desde un medio removible
  - Montar partición NTFS de W2K (read/write)
  - Copiar la SAM (*Security Account Manager)*
  - Modificar contraseña de *Administrator* utilizando herramientas existentes
  - Reiniciar el sistema y hacer login como *Administrator*
  - Restablecer la SAM original

Acceso físico: Compromiso W2K

- *Herramientas útiles*
  - NTFSDOS PRO (www.winternals.com)
    - Montar una partición NTFS desde DOS con capacidades de lectura y escritura
  - System Recovery Console (W2K CDs)
    - Acceso a consola de recuperación limitada con capacidades de lectura y escritura para particiones NTFS.

Acceso físico: Compromiso W2K

- *Herramientas útiles*
  - NTPASSWD (http://home.eunet.no/~pnordahl/ntpasswd/)
    - Utilidad interactiva de modificación de la SAM basada en Linux con capacidad de montar particiones NTFS en modo lectura y escritura
  - Otras distribuciones de Linux con arranque desde floppy o CD con capacidad de montar particiones NTFS en modo de lectura escritura.

Compromiso de Active Directory

SEKUREIT CONSULTORES EN SEGURIDAD INFORMATICA

- Obtención de acceso de *Administrator en AD*

  - Modificar contraseña de *Administrator* utilizando el método demostrado
  - Reiniciar el sistema en modo DSR (*Directory Services Recovery Mode*) (F8).
  - Sustituir en el registro el protector de pantalla (logon.scr) por el *command prompt* (cmd.exe)
  - Reiniciar el equipo normalmente y esperar a que se ejecute el *command prompt*.
  - Ejecutar la aplicación *Administer Users and Computers* y modificar la contraseña del *Administrator*

Vulnerabilidades

- ¿ Qué vulnerabilidades permitieron el éxito de los compromisos demostrados ?

  - *Análisis de riesgos incompleto*: La amenaza y acto amenazante no fueron visualizados.
  - *Capacitación deficiente*: Carencia de personal calificado para la administración de servidores
  - *Procedimientos no ejecutados*: Carencia de aseguramiento físico de equipos

El enfoque formal

- *Con base en el ciclo de vida de la Arquitectura de Seguridad Informática: Plan-Do-Check-Act*

  - *Plan*
    - Seleccionar controles
  - *Do*
    - Implantar los controles
    - Desarrollar políticas y procedimientos específicos para el aseguramiento de servidores
  - *Check*
    - Verificar que los controles operan adecuadamente
  - *Act*
    - *Determinar mejoras a la Arquitectura de Seguridad Informática*

Plan: Selección de controles

- *¿Qué controles serían necesarios para mitigar el riesgo?*
  - En cuanto a destrucción o daño físico:
  - En cuanto al acceso a sistemas operativos y aplicaciones:

Do: Políticas y procedimientos

Política de Seguridad de Servidores

- *4 Política*
- *4.1 Instalación de Servidores*
- *1. [...]*
- *2. Todos los servidores propiedad o bajo la responsabilidad de <Compañía>, que estén en modo de producción o pruebas, deberán ser físicamente ubicados en el área protegida del Centro de Datos de la organización.*
- *3. Sólo se podrán utilizar servidores que cumplan las características definidas en la Política de Adquisición de Hardware*
- *4. Todo servidor instalado en el Centro de Datos de la organización será asegurado físicamente como lo señala el Procedimiento de Aseguramiento Físico de Servidores, antes de entrar en operación.*
- *5. [...]*

Do: Políticas y procedimientos

Procedimiento de Aseguramiento Físico de Servidores

3.0 Procedimiento

1. *Instale físicamente el servidor en un rack debidamente empotrado, con paneles frontales, laterales y traseros protegidos con cerraduras.*
2. *Fije el servidor al rack de modo que no pueda ser derribado accidental o deliberadamente.*
3. *En el BIOS, modifique la secuencia de arranque del servidor, de modo que el primer dispositivo de arranque sea el disco duro.*
4. *Modifique la configuración del BIOS para evitar que se muestre la secuencia de teclas para acceder a él durante el proceso de arranque.*
5. *Retire tarjetas de módem, tarjetas de red o cualquier otro dispositivo de comunicación que no será utilizado por el servidor.*
6. *Retire o deshabilite físicamente unidades de floppy, CDROM, o cualquier otra unidad de almacenamiento externa.*
7. *[...]*

Seguridad Física de Servidores

- *Recursos*
  - *CERT, Securing Network Servers*
    www.cert.org/security-improvement/modules/m10.html
  - *Microsoft, Basic Physical Security*
    www.microsoft.com/technet/columns/ security/5min/5min-203.asp
  - *Physical Security*
    www.activsupport.com/network/vpn_security/physical_security.html

Seguridad en Windows 2000

Arquitectura de Windows 2000

- *Grupo de Trabajo*
  - *Un grupo de lógico de computadoras que comparten recursos. Cada una de ellas ve a la otra como un igual*
  - *No existe un mecanismo de control de seguridad para la red*
  - *Cada computadora tiene su base de datos local para controlar el acceso a los recursos*

n máquinas = n bases de datos de seguridad locales

Arquitectura de Windows 2000

- *Dominio*
  - *Un grupo de lógico de computadoras que comparten un servicio de directorio con información sobre:*
    - *Cuentas de usuario, grupos, computadoras...*
    - *Control de acceso*
    - *Recursos compartidos*
    - *Políticas de seguridad*
  - *Windows 2000*
    - *Active Directory es el servicio de directorio compartido*
    - *Remplaza el esquema de dominios de NT 4.0*
    - *No existen PDCs o BDCs, sólo Domain Controllers (Dcs)*

Arquitectura de Windows 2000

- *Active Directory (AD)*
  - *Estrechamente ligado al Sistema de Nombres de Dominio (DNS)*
    - *AD usa DNS para guardar información sobre los DCs en la red (registros SRV)*
    - *Resolución de nombres en la localización de recursos*
    - *Establecer la jerarquía de nombres de AD, en la creación de árboles y bosques*
  - *Componentes de AD*
    - *Sitios*
    - *Dominios*
    - *Unidades Organizativas (UOs)*
    - *Arboles*
    - *Bosques*

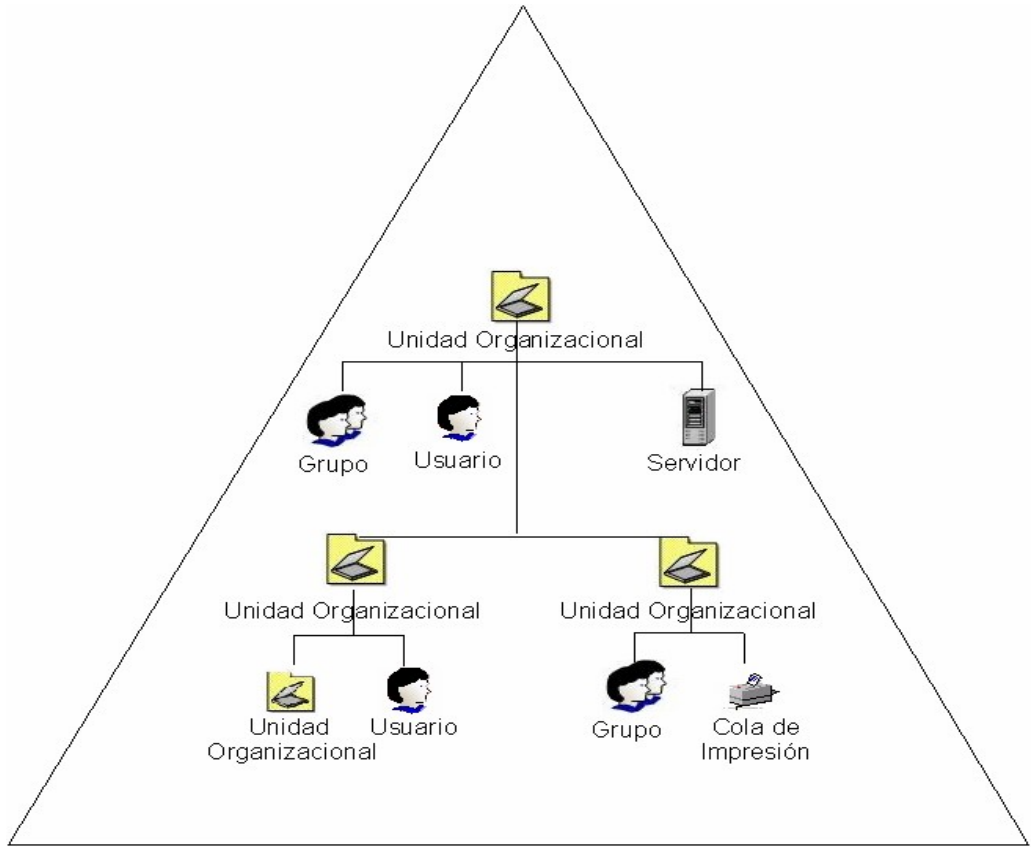
Dominios y UOs

- *Dominios y OU permiten representar la estructura lógica de la organización*

  - *Dominio. Define un entorno limitado en el que pueden establecerse controles de seguridad. Todos los objetos que pertenecen al dominio comparten la misma política de seguridad.*

  - *UO. Un contenedor lógico que permite representar de mejor manera la estructura lógica de la organización. Contiene los objetos terminales de la jerarquía (usuarios, computadoras, directorios compartidos), pero puede contener otras UOs, grupos de usuarios, etc.*

Dominios y UOs



Sitios

- *Un grupo de computadoras en una o varios subredes “bien conectadas”.*
- *“Bien conectadas” significa que las subredes comparten una red de bajo costo y alta velocidad, lo cual normalmente se refiere a subredes ubicadas en una misma ubicación física, conectadas a través de LANs.*
- *Los sitios representan una visión geográfica de la organización.*
- *No existe relación entre sitios y dominios. Es posible tener múltiples dominios en un sitio, o tener múltiples sitios para un dominio.*

Sitios: Propósito

- *Active Directory utiliza Sitios en los procesos de autenticación y replicación, reduciendo tiempos y tráfico WAN*

- ***Autenticación**. Cuando un usuario inicia una sesión en la red desde una estación de trabajo, el sistema autentica al usuario con el controlador de dominio localizado en el mismo sitio, cuando es posible.*

- ***Replicación**. Las actividades de replicación de los controles de dominio que deben ir a sitios remotos deberán cubrir condiciones especiales, por la necesidad de usar conexiones WAN.*

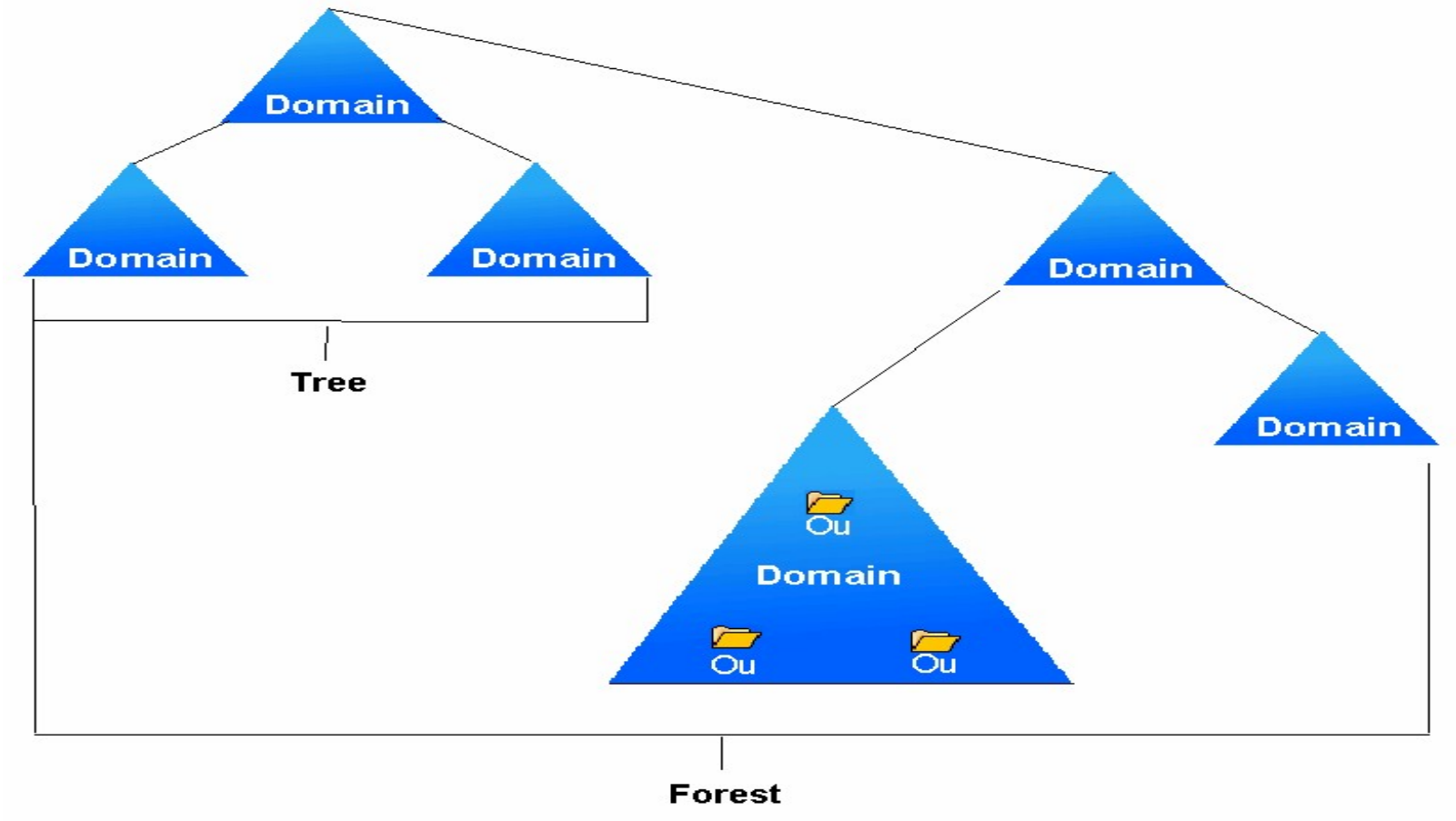
Arboles

- *Arbol*
  - *Un conjunto jerárquico de dominios que comparten un namespace contiguo, en el cual cada nombre en el namespace desciende directamente de un nombre raíz.*
  - *Apropiado para organizaciones centralizadas que comparten un nombre único*

Bosques

- *Bosque*
  - *Un conjunto de árboles de dominio completamente independientes.*
  - *Apropiado para una organización con múltiples líneas de negocios con nombres independientes.*
  - *No existe un grupo central de TI que administre la organización. Cada una de las divisiones tiene una infraestructura independiente*

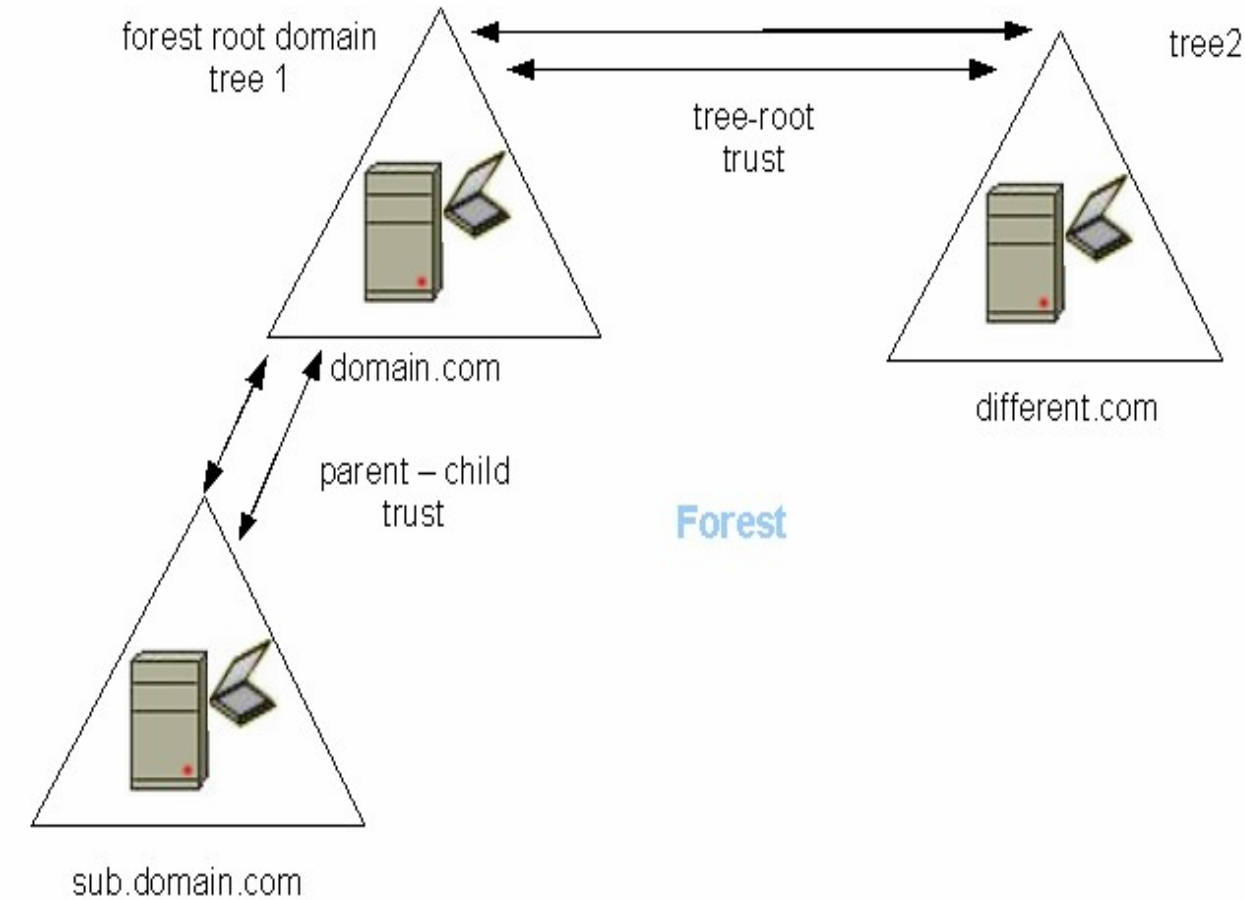
Arboles y Bosques



Relaciones de Confianza

- *Relaciones de confianza transitivas de dos vías.*
- *Relación transitiva: Si un dominio A confía en un dominio B, y el dominio B confía en un dominio C, entonces el dominio A también confía en el dominio C.*
  - *Esto permite que los usuarios o computadoras puedan autenticarse en cualquier dominio del árbol o del bosque*
  - *Las relaciones de confianza se crean automáticamente cuando se añade un nuevo dominio al árbol.*
  - *Protocolo de autenticación Kerberos V5*

Relaciones de Confianza



Grupos en *Active Directory*

- ***En AD existen 2 tipos de grupos:***

- ***Grupos de Distribución***
  - ***Utilizados exclusivamente para aplicaciones de correo electrónico (Exchange), no proveen características de seguridad***

- ***Grupos de Seguridad***
  - ***Utilizados para control de acceso. Estos grupos son listados en los DACLs que definen los permisos sobre los objetos***

Ambito de grupos de seguridad

- ***El ámbito (scope) define como son asignados los permisos a los miembros del grupo.***
  - ***Global***
    - ***Pueden asignarse permisos a recursos localizados en cualquier dominio***
    - ***Los miembros sólo pueden provenir del dominioen que se creó el grupo***
    - ***Sus miembros: Otros grupos globales, cuentas individuales***
  - ***Domain Local***
    - ***Pueden asignarse permisos sólo a recursos que pertenezcan al dominio en que se creó el grupo***
    - ***Los miembros del grupo pueden provenir de cualquier dominio***
    - ***Sus miembros: otros domain local groups en el mismo dominio, grupos globales y universales de cualquier dominio, y cuentas individuales de cualquier dominio***

Ambito de grupos de seguridad

- ***El ámbito (scope) define como son asignados los permisos a los miembros del grupo.***

  - ***Universal***
    - ***Pueden asignarse permisos a recursos localizados en cualquier dominio***
    - ***Los miembros pueden provenir de cualquier dominio***
    - ***Sólo opera en modo nativo***
    - ***Apropiados para consolidar grupos distribuidos en múltiples dominios***
    - ***Sus miembros: otros grupos universales, grupos globales, cuentas individuales***

Anidamiento de grupos

- ***Estrategia de anidamiento (Microsoft)***
  - ***Ubicar a los usuarios del dominio en Grupos Globales***
  - ***Anidar Grupos Globales como sea necesario, para permitir flexibilidad en caso de cambios en la organización o en el diseño de la red***
  - ***Anidar Grupos Globales en Grupos Universales para consolidar grupos distribuidos en múltiples dominios***
  - ***Anidar Grupos Globales y Universales en Domain Local Groups en la ubicación en que serán administrados***
  - ***Asignar permisos de acceso a los recursos a los Domain Local Groups***

Autenticación en W2K

- ***Existen sólo dos protocolos de autenticación en dominios de Windows 2000***

- ***Windows NT Lan Manager v2 (NTLM v2)***
  - ***Protocolo de autenticación oficial de Windows NT 4.0.***
  - ***Compatibilidad con sistemas NT 4.0 y clientes Windows 9x***
  - ***Basado en Reto-Respuesta, usando tres tipos de mensaje***

- ***Kerberos versión 5***
  - ***Protocolo de autenticación por omisión en equipos con Windows 2000 y Windows XP Professional***

Kerberos 5 (Windows 2000)

- ***Componentes***
  - ***Base de datos de cuentas: AD***
  - ***Kerberos Policy***
  - ***Kerberos Security Support Provider (SSP)***
  - ***Caché de credenciales***
  - ***KDC***
    - ***Authentication Service (AS)***
    - ***Ticket Granting Service (TGS)***

Logon Interactivo

- ***Un usuario Alice, se firma en un dominio Domain, desde una estación de trabajo Wkst.***

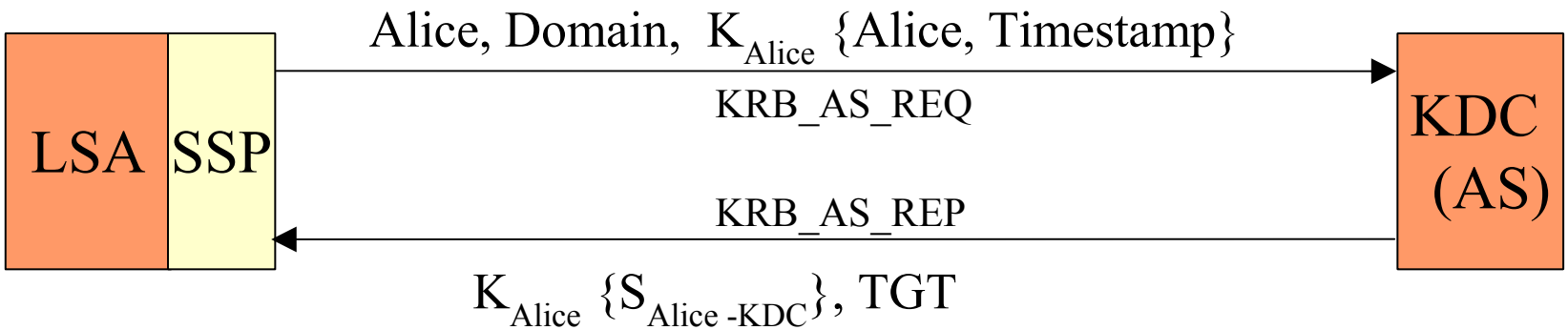
1. ***A través de Winlogon Alice inserta sus credenciales (usuario, contraseña y dominio)***

2. ***Winlogon entrega la información a la Autoridad de Seguridad Local (LSA) para validarla***

3. ***A partir de la contraseña de Alicia, la LSA calcula su long-term key (K_{Alice}) utilizando una función de hash.***

Logon Interactivo (cont.)

4. LSA solicita un TGT para Alice al KDC a través de Kerberos SSP



$$TGT = K_{KDC} \{ S_{Alice\ -KDC} , \text{Datos de Autorización para Alice} \}$$

Logon Interactivo (cont.)

5. LSA solicita un ticket de sesión para la computadora local

$$TGT = K_{KDC} \{ S_{Alice\text{-}KDC}, \text{Datos de Autorización para Alice} \}$$

$$Ticket = K_{Wkst} \{ S_{Alice\text{-}Wkst}, \text{Datos de Autorización para Alice} \}$$

Logon Interactivo (cont.)

6. ***LSA recibe el ticket, lo descifra y extrae los Datos de Autorización para Alice***

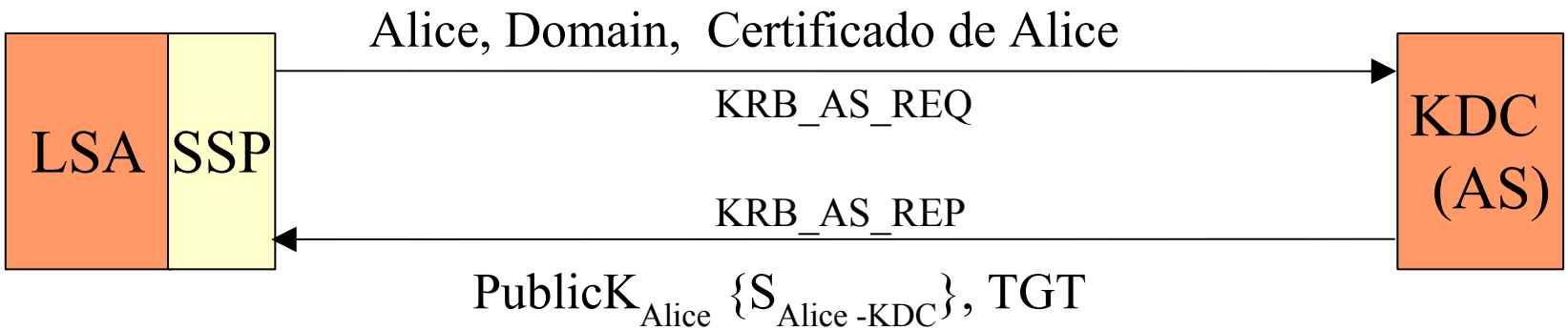
7. ***LSA construye un token de acceso, conteniendo***
   - ***SID de Alice***
   - ***SID de los grupos de seguridad a que pertenece Alice***
   - ***Derechos de usuario de Alice***

8. ***LSA devuelve el token de acceso a Winlogon, junto con un identificador de sesión y la confirmación de que el proceso de firma fue exitoso.***

9. ***Winlogon crea un contexto de seguridad para Alice***

Uso de tarjetas inteligentes

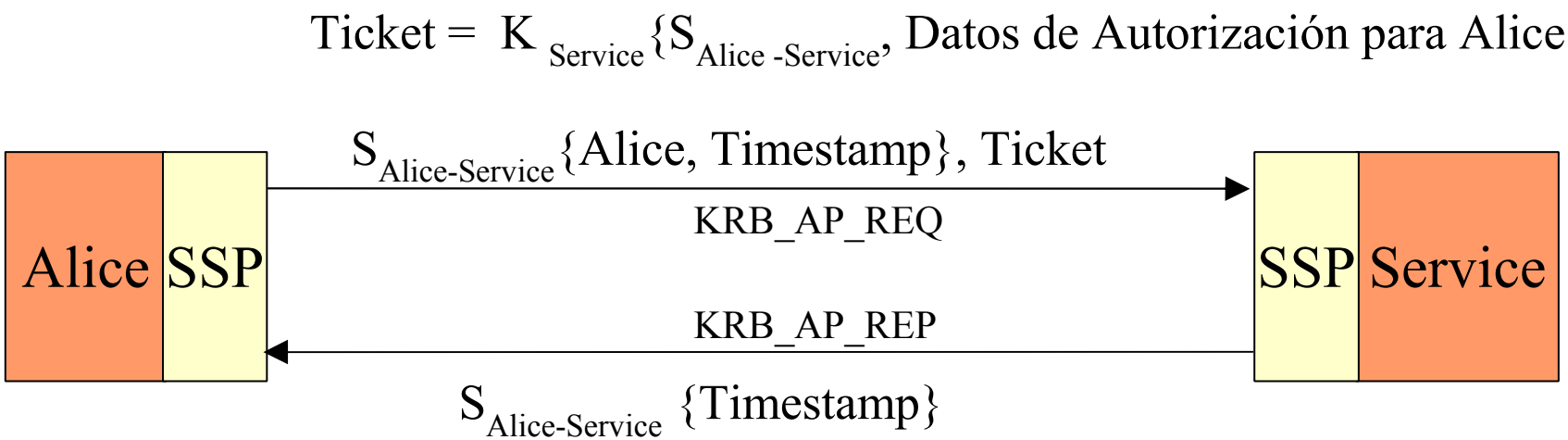
- **No se utiliza una clave simétrica compartida**
- **En su lugar, se utiliza un par de claves almacenado en la tarjeta inteligente, como un certificado X.509 v3**



$$TGT = K_{KDC} \{ S_{Alice\text{-}KDC} , \text{Datos de Autorización para Alice} \}$$

Logon Remoto

- ***Alice* intenta abrir un archivo en un folder compartido remoto**



Seguridad de Active Directory

- *Componentes de seguridad de Active Directory*
  - *Security Principals: Usuario, Grupo de Seguridad, Servicio y Computadora.*
  - *Security Identifiers: Identificadores únicos, nunca reutilizados, de los Security Principals.*
    S-R-X-Y-Y-Y-Y-RID
  - *Security Descriptors: Información de seguridad asociada con un objeto (Discretionary ACL y System ACL)*

Control de acceso a objetos

- *La seguridad de AD está basada en listas de control de acceso (ACLs), que protegen a los objetos*

- *Cada objeto tiene asociado un security descriptor*
- *Cada security descriptor tiene asociado una DACL y una SACL*

- ***DACL***
- *Un conjunto de registros de control de acceso (ACE)*
- *Un ACE especifica que accesos sobre un objeto son permitidos para un security principal.*
- *Un ACE contiene un SID y un conjunto de permisos*

Control de acceso a objetos

- ***SACL***
- *Un conjunto de registros de control de acceso (ACE)*
- *Un ACE controla como el subsistema de seguridad audita intentos de acceso a los objetos*
- *Un ACE contiene un SID y un conjunto de permisos, indicando que accesos serán auditados*

Herencia

- ***A través de la herencia, los ACEs de un objeto padre (un contenedor) pueden ser propagados a todos sus hijos.***

- ***El proceso de herencia ocurre cuando se crea un nuevo objeto hijo, o cuando se modifican la DACL o SACL del padre.***

- ***El proceso de herencia puede bloquearse***

Sistemas de Archivos en W2K

- ***NTFS***
  - ***Los archivos y directorios son objetos asegurables***
  - ***Permite cifrado de archivos individuales o directorios completos (EFS, Encryption File System)***
  - ***Permite manejo de cuotas***
  - ***Permite compresión de archivos y directorios***
  - ***Es posible establecer auditoría de accesos a los archivos y directorios***

Permisos NTFS

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder / Execute File	X	X	X	X		
Lis Folder / Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create Files / Write Data	X	X				X
Create Folders / Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					

Permisos NTFS

- ***Qué ocurre con los permisos cuando un archivo es movido a otra carpeta?***
  - ***Si el archivo es movido a otra carpeta dentro de la misma partición NTFS, conservará los permisos.***
  - ***Si el archivo es movido a otra partición NTFS, heredará los permisos de la carpeta destino.***
  - ***Si el archivo es movido a cualquier otra ubicación, heredará los permisos del folder o partición destino.***

Carpetas compartidas

- ***En un dominio, sólo Administradores y Power Users pueden establecer carpetas compartidas***

- ***Tres permisos posibles***
  - ***Full Control***
  - ***Change***
  - ***Read***

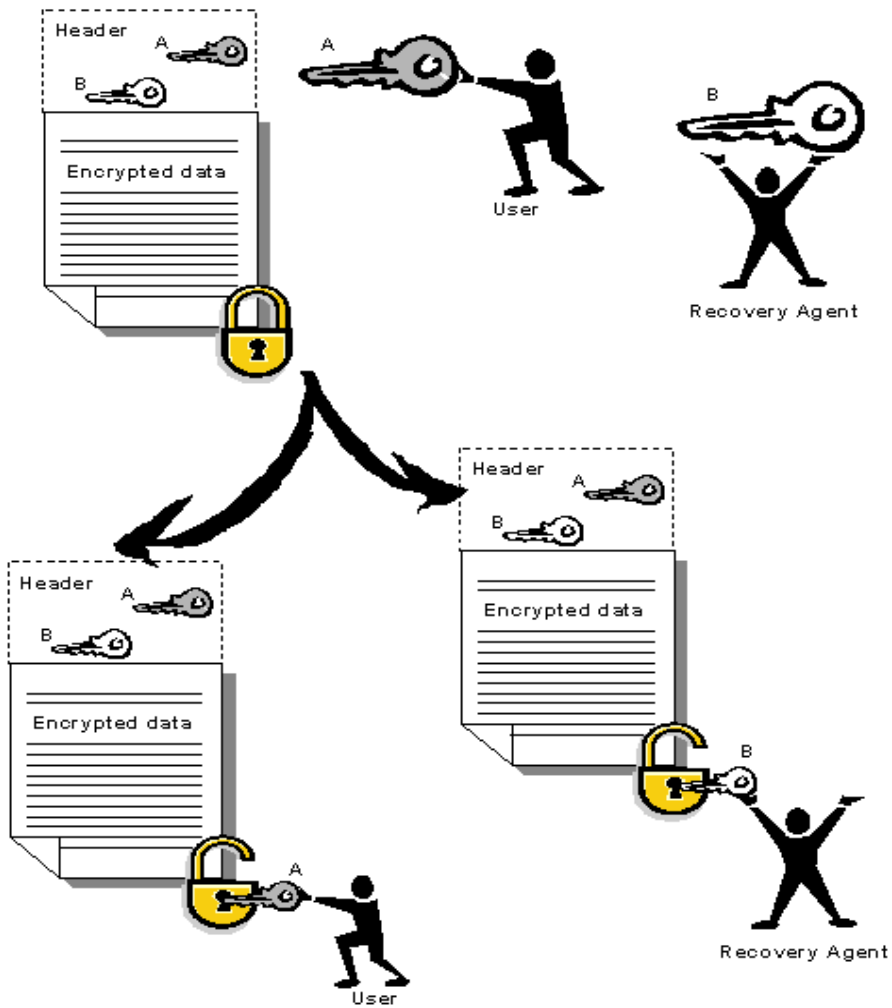
- ***Los permisos efectivos de un usuario consisten de sus permisos de carpeta compartida más restrictivos, intersectados con sus permisos NTFS menos restrictivos.***

Encryption File System (EFS)

- ***Un par de llaves asimétricas por usuario***
- ***Una llave simétrica de cifrado por archivo (File Encryption Key, FEK)***
- ***Cifrado DES (3DES opcional)***

- ***Procedimiento para cifrar un archivo***
  - ***EFS genera la FEK***
  - ***EFS cifra el archivo con la FEK***
  - ***EFS cifra la FEK con la llave pública del usuario y guarda el resultado junto con el archivo cifrado***

Agentes de Recuperación de Datos



Distributed File System (DFS)

- ***Una estructura de carpetas virtual, para que los usuarios perciban una estructura contigua única, aún cuando en realidad se trate carpetas alojadas en diferentes servidores a lo largo de la organización.***

  - ***Facilitar la búsqueda de Carpetas Compartidas en un ambiente de red***
  - **Tolerancia a fallas a través de replicación**
  - ***Balanceo de cargas***

Distributed File System (cont)

- ***Componentes del DFS***
  - ***DFS Root***
    - ***La carpeta compartida que sirve como raíz a un árbol DFS***
  - ***Host Server***
    - ***El servidor que almacena la raíz DFS***
  - ***DFS Links***
    - ***Carpetas compartidas que aparecen como subcarpetas de la Raíz DFS***
  - ***Réplicas***
    - ***Carpetas compartidas idénticas a un DFS link***
    - ***Hasta 32 réplicas por DFS link***

Registro de Eventos de Seguridad

- ***Categorías de Auditoría***

  - ***Account Logon Events***
    - ***Un DC recibe solicitudes de inicio de sesión en la red***
  - ***Account Management***
    - ***Una cuenta de usuario o grupo es creada o modificada***
  - ***Directory Service Access***
    - ***Se accede a un objeto de AD***
  - ***Logon Events***
    - **Un usuario intenta iniciar o cerrar la sesión en una estación de trabajo interactivamente**

Registro de Eventos de Seguridad

- ***Object Access***
  - ***Un usuario intenta acceder a un archivo, carpeta, impresora o llave del registro.***
- ***Policy Change***
  - ***Se realiza un cambio en las directivas de asignación de derechos de usuario, directivas de auditoría o directivas de contraseñas***
- ***Privilege Use***
  - ***Un usuario intenta ejercitar un derecho tal como, apagar el sistema, realizar respaldo, tomar posesión de objetos, etc.***

Registro de Eventos de Seguridad

- ***Process Tracking***
  - ***Creación y eliminación de procesos, activación de programas.***
- ***System Events***
  - ***Se realiza un cambio en las directivas de asignación de derechos de usuario, directivas de auditoría o directivas de contraseñas***

Políticas de Grupo

- *Un mecanismo usado en Active Directory para controlar el entorno de trabajo de usuarios y computadoras en un dominio de Windows 2000*
- *Son aplicadas a sites, dominios o UOs afectando a los objetos del contenedor.*

- *Computer Configuration. Permite establecer directivas que serán aplicadas a todas las computadoras dentro del ámbito de la Política de Grupo, sin importar quién inicie sesión.*
- *User Configuration. Permite establecer directivas que serán aplicadas a todos los usuarios dentro del ámbito de la política de grupo, sin importar en qué computadora inicien sesión.*

Políticas de Grupo: Herencia

- *La definición de políticas de grupo es almacenada en un Objeto de Políticas de Grupo (GPO).*

- *Por naturaleza las políticas de grupo son heredadas jerárquicamente*

Políticas de Grupo: Posibilidades

¿Qué se puede controlar con las políticas de grupo?

- ***Plantillas Administrativas:***
  - ***Establecer parámetros de registro para controlar la apariencia del escritorio y el comportamiento del SO y aplicaciones.***
- ***Security Settings:***
  - ***Establecer parámetros de seguridad aplicables a computadoras y usuarios dentro del ámbito del GPO.***
- ***Instalación de Software:***
  - ***Administrar de forma centralizada el software de la organización.***

Políticas de Grupo: Posibilidades

- ***Scripts:***
  - ***Aplicar scripts para automatizar el inicio y apagado del equipo, así como el inicio y término de sesión de un usuario***
- ***Servicios de Instalación Remota (RIS)***
  - ***Instalar Windows a través de la red con mínima intervención del usuario***
- ***Mantenimiento de Internet Explorer:***
  - ***Administrar y personalizar el Internet Explorer en computadoras con Windows 2000***
- ***Redirección de Carpetas:***
  - ***Redirigir las carpetas especiales del perfil del usuario (My Documents, Application Data, Desktop, Start Menu) a un lugar específico dentro de la red.***

Políticas de Grupo: Procesamiento

- **Las GPOs son acumulativas, y siguen el siguiente orden de procesamiento**

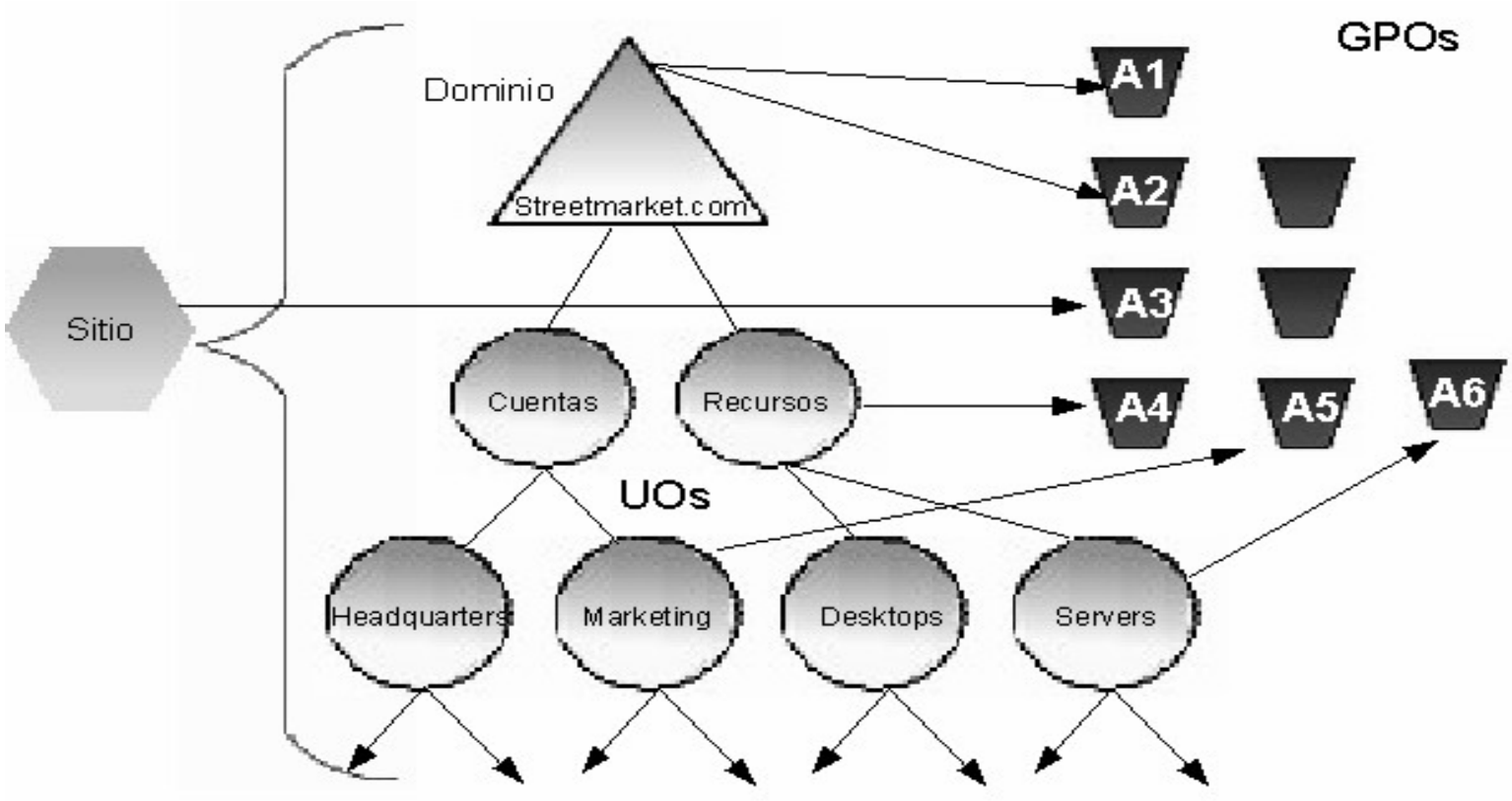
  1. ***Política de Grupo Local (la que existe en cada cliente)***
  2. ***Política de Grupo de Sitio***
  3. ***Política de Grupo de Dominio***
  4. ***Política de Grupo de UO***
  5. ***Política de Grupo de UO hija***

- ***El orden de procesamiento es crítico: Si dos políticas establecen un comportamiento distinto para un mismo parámetro, prevalecerá el definido por la última política procesada.***

Políticas de Grupo: Procesamiento

- **La aplicación de políticas se puede modificar a través de dos métodos:**
  - ***Block Inheritance. Bloquear la aplicación de GPOs establecidas en contenedores padres. Sólo los parámetros de la GPO actual serán aplicados.***
  - ***No override. Garantizar que ninguna política procesada posteriormente podrá remplazar los parámetros de la actual.***
  - ***"No override" tiene precedencia sobre "Block Inheritance"***

Políticas de Grupo: Procesamiento



Plantillas de Seguridad

- **Un archivo de configuración (.inf) que consolidad parámetros de la sección *Security Settings*, que son aplicables a las políticas de grupo, permitiendo la estandarización de la seguridad a través de un dominio.**
  - **Areas configurables:**
    - ***Account policies***
    - ***Local policies***
    - ***Event log***
    - ***Restricted groups***
    - ***System services***
    - ***Registry***
    - ***File system***

Plantillas de Seguridad: NSA

- **La *National Security Agency* (NSA) provee un conjunto de plantillas que cumplen con sus *Windows 2000 Security Recommendation Guides.***
  - ***W2KDC.inf***
    - ***Aplicable a Windows 2000 Server / Advanced Server configurado como controlador de dominio.***
  - ***W2_Server.inf***
    - ***Aplicable a Windows 2000 Server / Avanced Server configurado como miembro del dominio.***
  - ***W2K_Workstation.inf***
    - ***Aplicable a estaciones de trabajo Windows 2000 proffesional***
  - ***W2K_Domain_Policy.inf***
    - ***Aplicable a nivel de dominio, a través de una GPO***

CIS Security Benchmarks

- ***Center for Internet Security (CIS)***
- ***Basados en las mejores prácticas de la NSA, Sans Institute, Departamento de Defensa***
  - ***Nivel 1***
    - ***Mejorar el nivel de seguridad de un sistema operativo "out of the box".***
    - ***Representa el nivel mínimo de seguridad recomendado para un sistema operativo***
  - ***Nivel 2***
    - ***Medidas de seguridad más detalladas y especializadas***

Seguridad en Windows 2000

- *National Security Agency's (www.nsa.gov)*
  - *Windows 2000 Security Recommendation Guides*
- *Center for Internet Security (www.cisecurity.org)*
  - *CIS Benchmarks and Security Tools*

Seguridad en Windows 2000

- *Recursos*
  - *Step-by-step guide to understanding the Group Policy Feature Set*

    www.microsoft.com/windows2000/techinfo/ planning/ management/groupsteps.asp
  - *Windows 2000 Server Baseline Security Checklist*

    www.microsoft.com/technet/security/ tools/chklist/w2ksvrcl.asp
  - *Improve Windows Servers Security*

    www.microsoft.com/technet/security/tools/chklist/wsrvsec.asp
  - *IIS Baseline Security Checklist*

    www.microsoft.com/technet/security/ tools/chklist/iis50cl.asp

Domain Name System (DNS)

- *Recomendaciones*

  - *Usar Active Directory Integrated Zones*
    - *Establecer quién puede actualizar un DNS*
    - *Establecer ACLs para controlar qué usuarios pueden hacer cambios en los registros de zona y de recursos.*

  - *Crear un grupo especial para administradores de DNSs*
  - *Asignar el grupo de administradores de DNS a una UO y aplicar una política de grupo*

Seguridad en UNIX

Principales fallas de seguridad

- *SANS/FBI Top 20 list*
  - *Remote procedure calls*
    Buffer overflows en procedimientos ejecutados con privilegios de root
  - *Servidor web Apache*
    Scripts CGI
  - *Secure Shell (SSH)*
    Vulnerabilidades de SSH y OpenSSL
    Versión trojanizada
  - *Simple Network Management Protocol (SNMP)*
    Comunidades default: public y private
    Carencia de cifrado

Principales fallas de seguridad

- *Sendmail*
  - *Buffer overflows*
  - *Open relay*
- *BIND, DNS*
  - *Buffer overflows*
  - *Denegación de servicio*
  - *Cache poisoining*
- *FTP, r-services*
- *Line Printer Daemon (LPD)*
- *Cuentas con contraseñas débiles / sin contraseña*

Contraseñas / Archivo shadow

- */etc/passwd*

acount-name:password:UID:GID:Description:Directory:Program

- */etc/shadow*

acount-name:password:Lastchg:Min:Max:Warning:Inactive:Expire:Flag

Lastchg = Número de días desde 01/01/1970 a la fecha en que la contraseña fue modificada por última vez.

Min = Mínimo número de días requerido para permitir cambio de contraseña

Max = Máximo número de días que la contraseña es válida

Warning = Número de días previos a la expiración de la contraseña

Inactive = Número de días de inactividad permitidos

Expire = Fecha absoluta en que no será permitido hacer login en el futuro

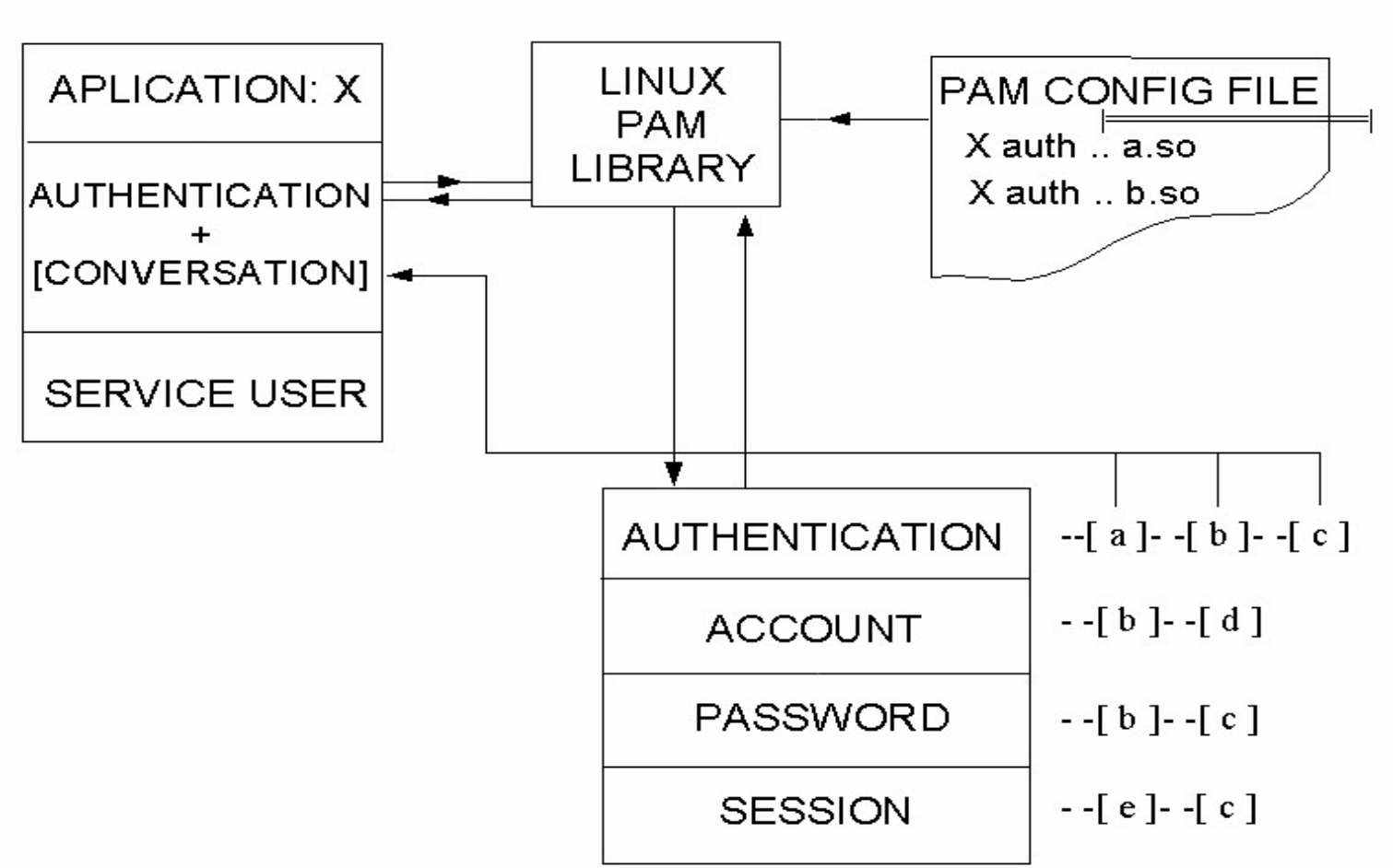
Pluggable Authentication Modules (PAM)

- *Una suite de librerías que permiten al administrador del sistema indicar cómo las aplicaciones autenticarán a los usuarios*

- *Los módulos PAM pueden como pilas (stacks) de cuatro tipos de módulos diferentes a ser procesados*

  - *Authentication Management*
  - *Account Management*
  - *Session Management*
  - *Password Management*

Pluggable Authentication Modules (PAM)



Módulos comunes

- *Pam_deny.so*
  - *Usado para denegar acceso. Indica a la aplicación la ocurrencia de una falla.*
- *Pam_permit.so*
  - *Usado para permitir el acceso, indicando el éxito del módulo.*
- *Pam_unix.so*
  - *Modulo de autenticación de UNIX. Hace llamadas estándar al sistema para realizar la autenticación*
- *Pam_securetty.so*
  - *Si es root quien está siendo autenticado, verifica que la terminal desde la que se conecta exista en /etc/securetty.*
- *Pam_rootok.so*
  - *Este módulo autentica exitosamente al usuario si su UID es cero*

Módulos comunes

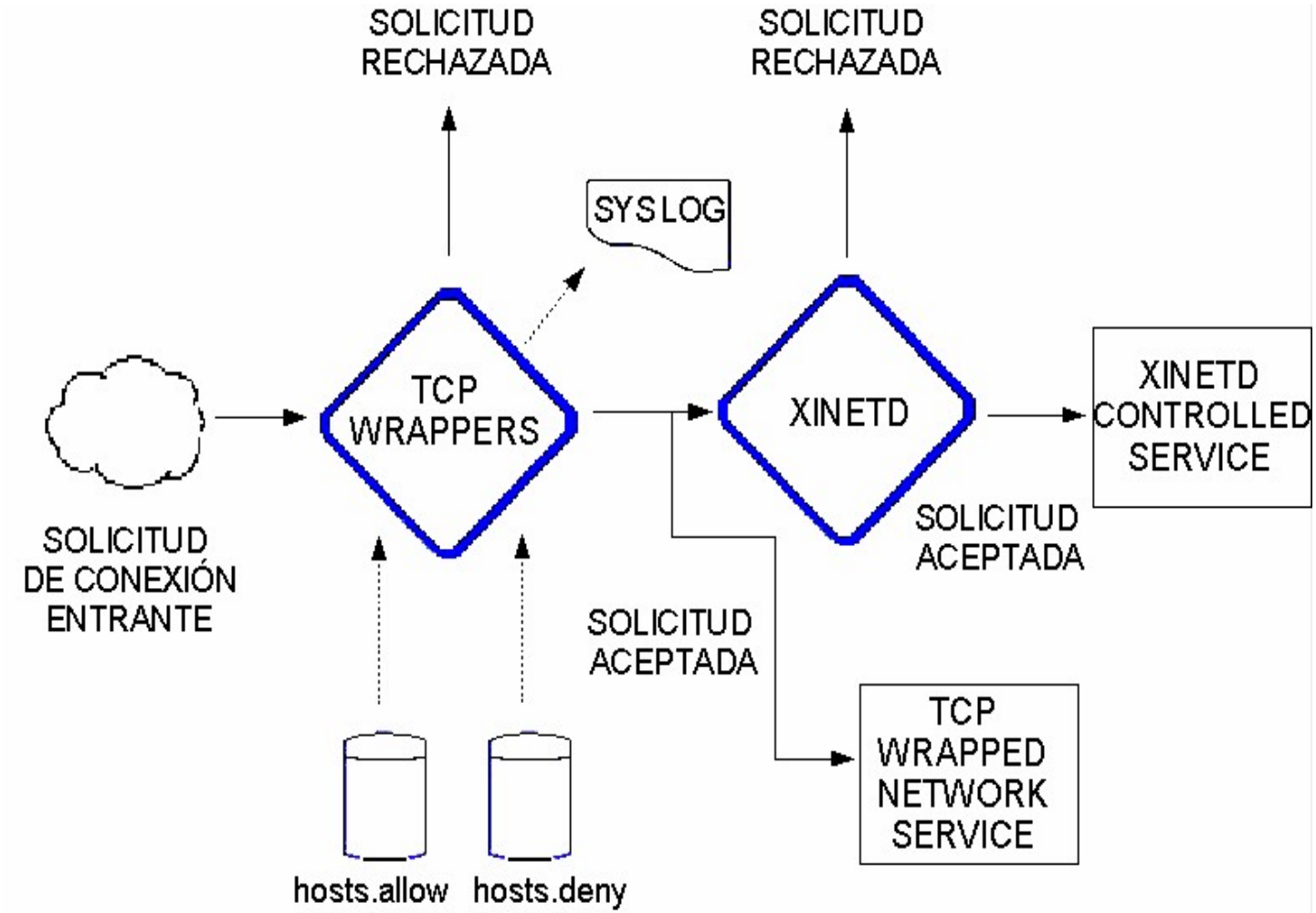
- *Pam_nologin.so*
  - *Valida la existencia del archivo /etc/nologin. Si dicho archivo existe, sólo root está autorizado para establecer una conexión*
- *Pam_wheel.so*
  - *Sólo permite acceso como root a los miembros del grupo wheel.*
- *Pam_env.so*
  - *Establece las variables de entorno definidas en /etc/security/pam_env.conf*
- *Pam_stack.so*
  - *Este módulo invoca recursivamente la pila definida en otro archivo de configuración. Si la pila invocada es ejecutada satisfactoriamente, pam_stack.so indica el éxito del módulo*

TCP Wrappers

- *Control de acceso a servicios de red por nombre de host y dirección IP*

- *El concepto de operación es la inclusión de un intermediario entre el servicio y el cliente, el cual verifica reglas de control de acceso para permitir o rechazar el establecimiento de la conexión*

TCP Wrappers



TCP Wrappers

- *El control de acceso se realiza a través de dos archivos de configuración /etc/hosts.allow y /etc/hosts.deny.*

1. *Se verifican secuencialmente las reglas del archivo hosts.allow. Si se encuentra una coincidencia, se permite la conexión, y TCP Wrappers cede el control al servicio.*

2. *En caso contrario, se verifican secuencialmente las reglas del archivo hosts.deny. Si se encuentra una coincidencia la conexión es rechazada.*

3. *Si no existe una coincidencia en cualquiera de los dos archivos, la conexión es permitida.*

TCP Wrappers

- *Formato de archivos de configuración:*

<daemon_list> : <client_list> [: <option> [: <option>]]

Ejemplos:
*ALL : *.mydomain.com*
ALL : 192.168.
in.telnetd : /etc/telnetd.hosts
sshd : LOCAL
ALL : 192.168.0. EXCEPT 192.168.0.25
sshd : .prohibido.com : twist /bin/echo 421 Error %a
ALL EXCEPT in.ftpd : host.mydomain.com : severity emerg

Xinetd

- *Un súper-servicio que controla el acceso a un conjunto de servicios de red, tales como FTP, POP y TELNET*

- *Además de las reglas de TCP Wrappers, xinetd tiene sus propias reglas de acceso:*

  - *only-from: Permite el uso del servicio, sólo a los hosts especificados*

  - *no-access: Bloquea el acceso al servicio a los hosts especificados*

  - *access-times: Especifica el rango de tiempo en que un servicio en particular puede ser utilizado*

Xinetd

- *Ejemplos:*

only-from = 10.1.1.0/24
only-from = administración.sekureit.com

no-access = 200.77.33.22

access-times = 09:28-23:15

Xinetd

- *Adicionalmente, xinetd posee opciones de administración de recursos:*
  - *per-source: Define el número máximo de instancias de un servicio con una IP específica*
  - *cps: Define el número máximo de conexiones permitidas a un servicio por segundo*
  - *max-load: Define el límite máximo de uso de CPU para un servicio específico*

Permisos en Archivos y Directorios

Permisos por omisión en la creación de

- *Archivos: rw-rw-rw (666)*
- *Directorios: rwxrwxrwx (777)*

umask

- *Muestra o establece los modos de acceso que el sistema debe deshabilitar por omisión al crear un nuevo objeto.*

- *Por ejemplo, al crear un nuevo archivo con*

umask 002	*--- --- -w-*	*umask 022*	*--- -w- -w-*
Complemento a 1 de 002	*rwx rwx r-x*		*rwx r-x r-x*
	and		*and*
Permisos por omisión 666	*rw- rw- rw-*		*rw- rw- rw-*
Permisos resultantes:	***rw- rw- r-- (664)***		***rw- r-- r-- (644)***

Bit Set UID (SUID)

- *El bit número 12 en la representación de permisos de archivos y directorios (izquierda a derecha)*
- *Si el bit SUID está encendido para un archivo ejecutable, cualquier proceso que ejecute el archivo tendrá los permisos asociados al propietario del archivo, en lugar de los asociados al usuario que creo el proceso.*
- *Establecer el bit SUID: chmod u+s filename*
- *Por ejemplo:*

  rws r-x r-x (4755)

Bit Set GID (SGID)

- *El bit número 11 en la representación de permisos de archivos y directorios (izquierda a derecha)*

- *Si el bit SGID está encendido para un archivo ejecutable, el GID del proceso es cambiado por el GID del propietario del archivo. El acceso a los recursos estará condicionado por los permisos asociados al grupo propietario en lugar de los asociados a los del grupo del usuario que creo el proceso.*

- *Establecer el bit SGID: chmod g+s filename*

- *Por ejemplo:*

rwx r-s r-x (2755)

Uso del Sticky Bit

- *El bit número 10 en la representación de permisos de archivos y directorios (izquierda a derecha)*
- *Util en la protección de directorios compartidos*
- Una vez aplicado a un directorio, un archivo contenido en dicho directorio sólo podrá ser eliminado por
  - root
  - El propietario del archivo
  - El propietario del directorio
- *Establecer el sticky bit para un directorio:*

  chmod +t dirname

ACLs y atributos extendidos

- *Los atributos extendidos son pares nombre,valor arbitrarios que están asociados a archivos y directorios*
- *Pueden ser utilizados para almacenar objetos de sistema, tales como listas de control de acceso (ACLs).*
- *Una ACL permite una definición de permisos más fina, de modo que es posible otorgar permisos sobre los archivos y directorios a usuarios o grupos específicos*

ACLs y atributos extendidos

- *Mostrar los permisos para un archivo o directorio*

  getfacl filename

- *Otorgar permisos de lectura y ejecución a un grupo específico sobre un archivo o directorio*

  setfacl -m g:groupname:rx filename

- *Otorgar permisos de lectura y escritura a un usuario específico sobre un archivo o directorio*

  setfacl -m u:username:rw filename

Syslog

- *El sistema general de registro de mensajes de los sistemas UNIX*
- *Escucha por mensajes escritos dos puntos:*
  - */dev/log* *Mensajes generados por los procesos del sistema*
  - *514/UDP* *Mensajes procedentes de otros sistemas en la red*
- *Otro demonio klog, escucha mensajes del kernel y los pasa a syslog como lo haría un proceso más.*
  - */dev/klog* *Mensajes generados por el kernel*

Syslog

- *El sistema general de registro de mensajes de los sistemas UNIX*
- *Escucha por mensajes escritos dos puntos:*
  - */dev/log* *Mensajes generados por los procesos del sistema*
  - *514/UDP* *Mensajes procedentes de otros sistemas en la red*
- *Otro demonio klog, escucha mensajes del kernel y los pasa a syslog como lo haría un proceso más.*
  - */dev/klog* *Mensajes generados por el kernel*

Syslog Facilities

- *Hacen referencia a las áreas que originan los mensajes*

- *auth* *Relativos al sistema de autenticación (login, su)*
- *authpriv* *Mensajes auth, que incluyen información sensible*
- *cron* *Relativos al demonio cron*
- *daemon* *Otros demonios del sistema, tales como sshd, xinetd*
- *kern* *Mensajes generados por el kernel*
- *lpr* *Relativos al line printer subsystem (lpd, lpdsched)*
- *Mail* *Mensajes generados por el susbsistema de correo*

Syslog Levels

- *Indican el nivel de seguridad de un mensaje*

0	*emerg*	*El sistema es inutilizable*
1	*alert*	*Debe tomarse una acción inmediata*
2	*crit*	*Condiciones críticas*
3	*err*	*Condiciones de error*
4	*warn*	*Condiciones de alerta*
5	*notice*	*Condiciones normales, pero significativas*
6	*info*	*Mensaje informativo*
7	*debug*	*Mensajes de nivel de depuración*

Configuración de Syslog

Los mensajes recabados por syslog pueden ser:

- *Agregados a un archivo determinado*
- *Enviados a un servidor syslog remoto*
- *Entregados en la terminal de una lista de usuarios que estén conectados*
- *Entregados en la terminal de todos los usuarios conectados*
- *Enviados a alguna terminal en particular*
- *Entregados a otros progrmas para su procesamiento a través de un pipe*

Gracias por su atención

http://www.sekureit.com