Hardening de Windows

Autor: Diego Bruno

Edición y Corrección: Lic. Cristian Borghello, MVP - CISSP

Fecha Publicación: 22 de enero de 2010

Publicado en Segu-Info

INTRODUCCIÓN

Hace muy poco tiempo leí un artículo muy interesante de Derek Malber, reconocido escritor y revisor técnico de muchísimos artículos del sitio Windowsecurity.com, que en un curso de seguridad que brindó, le pidió a la audiencia, la mayoría de todos ellos administradores, que rankearan sus conocimientos sobre la arquitectura de seguridad de Windows en general y sus conocimientos sobre los permisos NTFS y su uso. El ranking debía ser del 1 al 10, en dónde el 10 era la nota máxima, lo mismo a ser un súper experto.

La mayoría de los asistentes se puso como nota entre un 7 y 8.

El autor comenta que la realidad, una vez dada su charla y preguntándoles a los asistentes a medida que la misma transcurría, era que el nivel en realidad era de entre un 2 y un 4.

La realidad es que no se puede culpar por esto a los administradores ya que la mayoría de ellos están sobrecargados de tareas administrativas y no siempre tienen el tiempo de empaparse de las funcionalidades de NTFS, pero por sobre todas las cosas lo más importante es la mala información que hay sobre NTFS y de la seguridad del sistema operativo en sí, incluso muchas veces por la misma gente de Microsoft.

Pero sin embargo comprender la arquitectura en forma profunda de la arquitectura de seguridad cómo del sistema operativo junto a los permisos NTFS y el saber aplicarlos es un componente fundamental para prevenir exploits maliciosos y un hardening bien granular del sistema. En esta parte vamos a ver como la seguridad de Windows realmente trabaja, que son los SIDs y los RIDs, revelar todos los usuarios y grupos built-in del sistema, discutir la diferencia entre los permisos que se setean en un fileshare y los NTFS y algunas recomendaciones extras.

Una vez entendido todos los conceptos que pasamos a explicar ahora, estaremos entonces en condiciones de meternos en la parte dura del hardening a través de la protección de los archivos de alto riesgo y de las entradas de registry de alto riesgo.

La finalidad de este capítulo es la de que el usuario aprenda los conceptos mínimos de la estructura de seguridad de Windows y de cómo funciona y que se adapte a la jerga técnica de dichos conceptos para así poder realmente entenderlos. Una vez entendido esto podemos pasar al siguiente punto de la capacitación la cual es el uso de los permisos NTFS.

SEGU-INFO.COM.AR

ALGUNOS DE LOS CONCEPTOS ERRÓNEOS DE NTFS QUE VEREMOS SON:

- El grupo everyone tiene full control en la mayoría de los recursos de Windows por default.
- Los permisos que deniegan siempre sobrescriben a los que permiten.
- Los permisos efectivos se dan como resultado de la interacción de los permisos NTFS y de los permisos de ShareFolders.
- Cuando tanto los permisos NTFS como los de FileShare se ven envueltos, el permiso efectivo resultánte es siempre el menos permisivo.
- El permiso de Read solo habilita a un usuario a ver un recurso.
- Los permisos de Read y Execute son necesarios para ejecutar un programa.

CÓMO TRABAJA LA SEGURIDAD EN WINDOWS

Para comprender como los permisos NTFS controlan el acceso a los recursos, se debe entender los mecanismos que envuelven a la seguridad de Windows.

Cuando un security principal (Como ser por ejemplo un usuario, un grupo, una computadora o una cuenta de servicio) intenta acceder a un recurso de Windows protegido como ser un archivo, una carpeta, una carpeta compartida, una impresora o cualquier otro recurso, debe probarle a Windows que tiene los permisos necesarios para acceder a dicho recurso.

LAS FASES DEL CONTROL DE ACCESO

El proceso que ocurre cuando un security principal intenta acceder a un objeto protegido del sistema operativo (Sin importar su versión) se llama control de acceso (Access control) el cual responde al modelo de acceso discrecional. Este proceso está compuesto de 4 etapas, las cuales son:

- Identification (Identificación)
- Authentication (Autenticación)
- Authorization (Autorización)
- Accounting/Auditing (Auditoría)

Identification (Identificación)

Identification es el método que un security principal utiliza para autoidentificarse frente al sistema operativo. En Windows este proceso se realiza cuando el security principal suministra un nombre unico o valor (En el caso de un smart card o cualquier otro token de seguridad). La identidad suministrada debe ser única en la base de datos de autenticación. En Windows la base de datos local de las identidades se llama Security Accounts Manager (SAM). En un entorno de AD la base de datos de los security principals está dentro del controlador de dominio en el archivo de base NTDS.DIT.

Cada security principal en un namespace de Windows debe tener un único identificador y único nombre amigable, un único número de GUID (Group Id) y un número de SID (Secure Indentifier), ya veremos en breve estos conceptos. La clave

SEGU-INFO.COM.AR

está en que el security principal debe poder manejar la autenticación contra la base de datos, ya sea local o de dominio a través de un único nombre o número que lo identifica.

Crear nombres para los security principals suele tener un trabajo más sofisticado que sólo crear nombres en forma aleatoria o randómica. Primero al crear un nombre de identificación se debe utilizar una convención de nombres común, en el caso de los usuarios suele ser por ejemplo la inicial del primer nombre y el apellido. Muchas empresas también usan nombres que recrean el rol laboral de la persona en la empresa o de acuerdo a su localización como ser SaltaAdmin. Por razones de seguridad cuando se crean los nombres identificatorios para los security principals, los mismos no deberían especificar el rol (En el caso de las cuentas con altos privilegios) y los mismos deberían ser documentados.

Authentication (Autenticación)

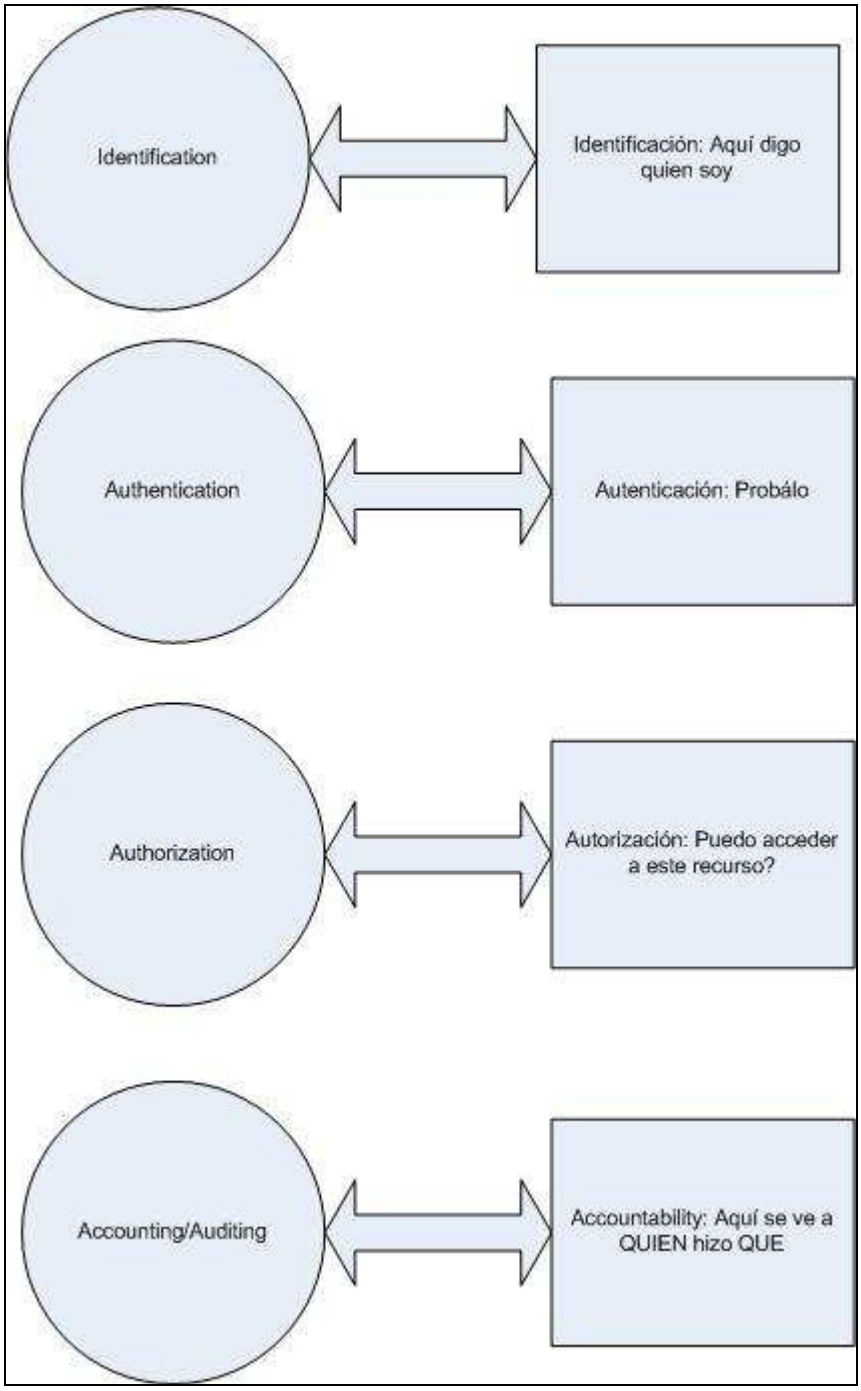
Una vez que la identificación de seguridad fue entregada la base de datos de autenticación (SAM o AD) necesita probar que la entidad suministrada realmente pertenece a quien la presenta, para eso el security principal debe suministrar información que sólo él y la base de datos de autenticación conocen, en la mayoría de los casos esta información es la password del usuario, pero podría ser una smart card o un token o credenciales biométricas. Si el security principal logra en forma exitosa proveer la información requerida por la base, el mismo es autenticado.

Authorization and Accounting

Como dijimos en las líneas anteriores cuando un security principal quiere acceder a un objeto se somete primero al mecanismo de acceso de control, junto a su credencial de seguridad. La credencial de seguridad del security principal contiene los permisos que le son dados a través del sistema operativo. En Windows el owner o dueño de un objeto, al cual un security principal pueda querer acceder, ya seteó previamente los permisos sobre que security principals van a poder acceder o no a dicho recursos y con que privilegios, asi es como trabaja el sistema discrecional (DAC).

SEGU-INFO.COM.AR

En Windows, el mecanismo de control de acceso, llamado security reference monitor (Monitor de referencia de seguridad) determina cuando el security principal tendra o no acceso a determinado recurso y que tipo de acceso tendrá. Si el requerimiento del security principal es exitoso, el requerimiento es autorizado. Por último el requerimiento junto a sus subsecuentes accesos exitosos o fallidos pueden ser logueados dentro del proceso llamado Accounting or auditing. En Windows todos los security principals deben someterse a si mismos al proceso de acceso de control (Access Control) como se muestra en la siguiente figura:



SEGU-INFO.COM.AR

JUNTANDO LAS PIEZAS DEL ROMPECABEZAS

Hasta ahora estuvimos viendo de forma muy genérica cómo trabaja el sistema discrecional de Windows junto a sus 4 etapas, pero técnicamente cómo trabaja este modelo?

Eso es lo que vamos a empezar a ver, por lo cual vamos a empezar a empaparnos de algunos términos cómo Security Descriptor (SD), ACL (Access Control List), Discretionary Access Control List (DACL), System Access Control List (SACL), Access Control Entry (ACE) y demás términos que están involucrados en la arquitectura de seguridad de Windows.

Todos los objetos y sus propiedades en Active Directory tienen descriptores de seguridad para controlar el acceso al objeto y los valores de los atributos del objeto. Al igual que con los objetos del sistema de archivos NTFS, el descriptor de seguridad del objeto active directory incluirá una lista de control de acceso discrecional (DACL, discretionary Access Control list) y una lista de control de acceso al sistema (SACL, System Access control List), además de los datos de propiedad del objeto.

La siguiente figura muestra un descriptor de seguridad:

DESCRIPTOR DE SEGURIDAD
ENCABEZADO
SID DEL PROPIETARIO
SID DEL GRUPO
DACL ACEs
SACL ACEs

NOTA: Ya vamos a estar llegando a los SID de grupos y usuarios como los GUID y el funcionamiento de ambos.

Veamos de acuerdo a lo explicado recién algunas definiciones sobre que es cada cosa para después poder entrar más en detalle con cada una de ellas:

Descriptor de seguridad (SD): Un descriptor de seguridad (SD) contiene información de seguridad asociada a un objeto asegurable como un archivo o proceso. Un descriptor de seguridad contiene atributos que incluyen una identificación del propietario del objeto, los grupos de seguridad a los que pertenece y dos *listas de control de acceso* (ACL): la *lista de control de acceso discrecional* (DACL) que define los derechos de acceso de cada usuario y grupo de usuarios, y la *lista de control de acceso al sistema* (SACL) que define los tipos de operación que se ejecutan en el objeto y que deberían generar mensajes de auditoria.

SEGU-INFO.COM.AR

Lista de control de acceso (ACL): Una lista de control de acceso (ACL) es una lista ordenada de *entradas de control de acceso* (ACE) adjuntas a un objeto asegurable. El sistema operativo Windows utiliza dos tipos de ACL: una *lista de control de acceso discrecional* (DACL) que se utiliza para especificar los derechos de acceso de un usuario o grupo de usuarios y una *lista de control de acceso al sistema* (SACL) que se utiliza para determinar cuándo deben generar mensajes de auditoría los tipos de acceso específicos.

Lista de control de acceso discrecional (DACL): Una DACL se asocia a un objeto asegurable (mediante un *descriptor de seguridad*) y especifica el conjunto de derechos de acceso que se concede a los usuarios o grupos de usuarios. El propietario de un objeto controla la DACL, que consiste en una lista ordenada de *entradas de control de acceso* (ACE) que determinan los tipos de operaciones que puede ejecutar un usuario o un grupo de usuarios en el objeto.

SACL (lista de control de acceso al sistema): Una SACL se asocia a un objeto asegurable (mediante un *descriptor de seguridad*) y especifica los tipos de operaciones ejecutadas por usuarios concretos que deberían generar mensajes de auditoria.

LSA (autoridad de seguridad local): La Autoridad de seguridad local (LSA) es un subsistema de Windows local que proporciona servicios de autenticación.

SRM (Security Referente Monitor): Subsistema del LSA, que se encarga de chequear los permisos de las tablas DACL de los objetos asegurados con las DACL del security principal (A través del Access Token o testigo de accesso) que quiere acceder a dicho objeto asegurado. Es quien habilita o Deniega el acceso al mismo.

Access Token (**Testigo de acceso):** Un testigo de acceso es una estructura de datos adjunta a cada proceso de Windows. Mantiene información del *contexto de seguridad* del proceso, que incluye un *SID* de usuario que identifica el *principal* que representa al inicio de sesión y los atributos de autorización, como los privilegios y los SID del grupo del usuario.

Cada testigo de acceso se asocia exactamente con un *inicio de sesión*, mientras que un inicio de sesión puede contener varios testigos de acceso, uno por cada proceso que se inicie en la sesión y, opcionalmente, otros *testigos del subproceso* adjuntos a subprocesos individuales.

Entrando un poco más en detalle para juntar las piezas:

Las listas de control de acceso discrecionales se pueden configurar en función del criterio de cualquier cuenta que posea los permisos adecuados para modificar la configuración, incluyendo los permisos tomar posesión (Take Ownership), cambiar permisos o control total. Las DACL constan de varios elementos los cuales se describen a continuación:

- **Encabezado**: Metadatos pertenecientes a las entradas de control de acceso ACE (Access Control Entry) asociadas con la DACL.
- **SID (Usuario**): Identificador de seguridad del propietario del objeto.
- **SID (Grupo**): Identificador de seguridad del grupo administradores o administradores de dominio integrados, si la cuenta que posee el objeto es miembro de cualquiera de estos grupos.

SEGU-INFO.COM.AR

- **ACE Denegar Genéricas**: Entradas de control de acceso que deniegan el acceso a una cuenta o grupo de seguridad en función de sus SID. Estas ACE se pueden heredar del objeto principal o se pueden asignar directamente al objeto, y son específicas de ese objeto y de sus objetos secundarios.
- **ACE Permitir Genéricas**: Entradas de control de acceso que permiten tener acceso a objetos a cuentas o grupos de seguridad en función de sus SIDs. Estas ACE se pueden heredar del objeto principal, o se pueden asignar en forma directa al objeto y son específicas del objeto y sus objetos secundarios.
- **ACE DENEGAR ESPECIFICAS DE OBJETO:** Entradas de control de acceso que deniegan el acceso a objetos secundarios a una cuenta o grupo de seguridad en función de sus SID. Estas ACE se pueden heredar del objeto principal o se asignan directamente al objeto, y se aplican a clases específicas de objeto secundarios.
- **ACE especificas de objetos:** Entradas de control de acceso que deniegan acceso a una cuenta o grupo de seguridad en función de sus SID. Estas ACE se pueden heredar del objeto principal o se pueden otorgar directamente al objeto y se aplican a clases específicas de objetos secundarios.

En la siguiente tabla se muestra una configuración de una DACL para un objeto de OU:

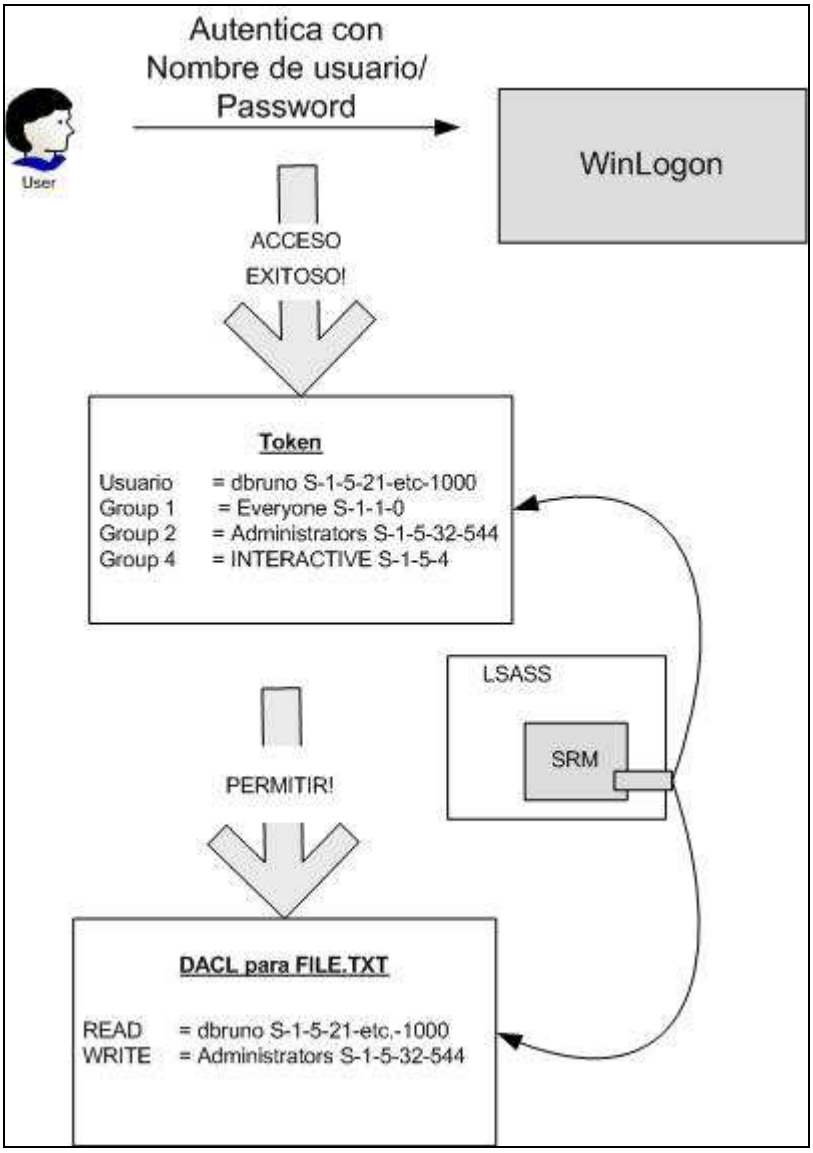
GRUPO	PERMISOS	AMBITO
Enterprise Admin.	Control Total	Este objeto y todos sus objetos secundarios
Authenticated Users	Leer	Este Objeto
Security Administrators	Restablecer contraseña	Objetos de usuario

La siguiente figura muestra una imagen de gráfico mas visual de la tabla, la cual grafica las partes de las DACL:

<table>
<tr><td colspan="2">DACL</td></tr>
<tr><td colspan="2">ENCABEZADO</td></tr>
<tr><td>SID del propietario</td><td>SID del Propietario del grupo</td></tr>
<tr><td colspan="2">ACE Denegar Genéricas</td></tr>
<tr><td colspan="2">ACE Permitir Genéricas</td></tr>
<tr><td colspan="2">ACE Denegar Especificas de Objetos</td></tr>
<tr><td colspan="2">ACE Permitir específicas de Objetos</td></tr>
</table>

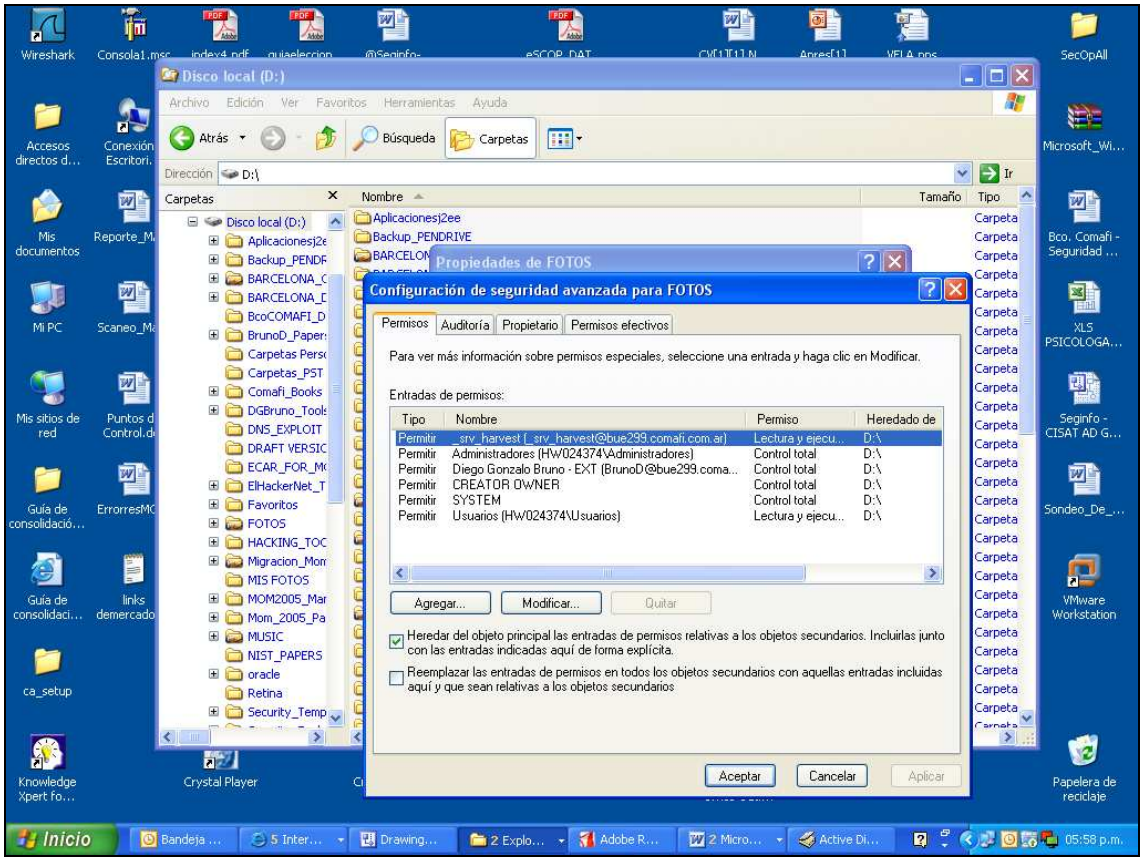
SEGU-INFO.COM.AR

Vemos entonces a modo de resumen final un boceto que explica en forma resumida lo ya expuesto hasta ahora en cuanto al modelo discrecional que maneja Windows:



SEGU-INFO.COM.AR

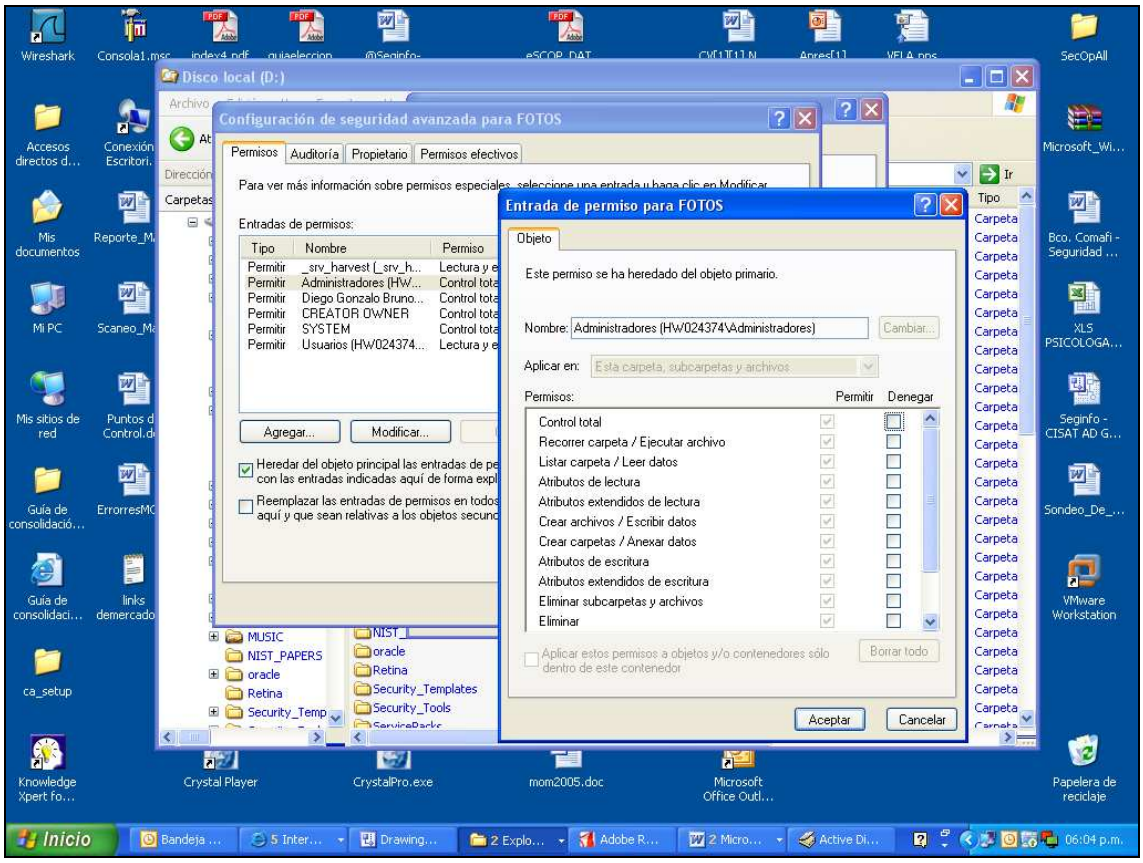
A continuación vemos en la captura de pantalla una DACL a través de la GUI de Windows:



La idea de mostrarlo asi de esta forma empezando desde la parte conceptual y luego recién al final la GUI de usuario es justamente para poder asimilar bien los conceptos explicados y así de esta forma “Realmente entender” que es lo que toco cuando manipulo la GUI de usuario.

SEGU-INFO.COM.AR

Entonces la pregunta lógica que surgiría viendo esta captura de pantalla de una DACL sería, que es una ACE? Bueno uno puede agregar o quitar ACEs de una DACL como se ve en la siguiente pantalla:



Puedo editar las ACE ya existente o clickear el botón agregar de la DACL y crear una nueva específica al objeto y especificar que security principals podrán o no acceder al objeto y con qué privilegios.

MÁS A DETALLE

GUIDs y SIDs

Asi como nosotros identificamos a los security principals por su nombre amigable como ser *dbruno*, Windows identifica a los security principals a través de los números llamados Globally Unique Identifier (GUID) y Security Identifier (SID), los cuales son asignados en forma permanente. Es por eso que inclusive aunque se renombre un security principal el sistema operativo lo puede mapear, ya que es un número único e irrepetible, inclusive si se borra un security principal y se lo vuelve a crear el número de SID será diferente.

GUIDs

Cada objeto y security principal en Windows tiene un número unico de GUID de 128 bits. Los GUID son asignados por el sistema operativo a casi todo posible objeto de Windows, incluyendo usuarios, computadoras, grupos, programas, elementos de datos y componentes de programación.

SEGU-INFO.COM.AR

Muchos programas referenciados en la registry son identificados por el GUID. Para Microsoft el GUID debe ser único para cada objeto de Windows. Es calculado usando una fórmula que envuelve a la fecha y hora, información de la red y una rutina randómica que usa frecuencias de ciclo del chip de la hora del equipo.

Los GUID's están a través de toda la regedit del sistema operativo, identificando a programas específicos, identificando controles de ActiveX, e inclusive podría ser utilizado como datos dentro de bases de datos. Sim embargo tratar de localizar un objeto de usuario a través de su GUID puede llegar a ser verdaderamente difícil. Muchas veces, el GUID se "revelará" cuando usemos alguna herramienta de troubleshooting, pero como dijimos requiere de alguna utilidad especial o de coding.

Se puede utilizar los programas LDP.exe o ADsiedit.msc, los cuales se encuentran dentro del cd de Windows XP o Windows 2003, en la ruta \Support\Tools\Support.cab, para poder hacer un Query a los GUID que están almacenados en el Active Directory. Desafortunadamente, los GUID son almacenados en sistema hexadecimal dentro del AD y deben ser convertidos para poder ser leídos correctamente. El artículo de Microsoft de la base de datos de conocimiento localizado en http://support.microsoft.com/default.aspx?scid=kb;en-us;325648 contiene un script .VBS de conversión y explica cómo utilizarlo.

SID's

Todos los security principals tienen uno o más SIDs pero no todos los objetos. Por ejemplo, los objetos de impresora no tienen SID. En Windows, sólo los security principals (Cómo por ejemplo usuarios, grupos, computadoras y cuentas de servicio) tienen SIDs, y los mismos son asignados cuando el security principal es creado por primera vez. Los SIDs están compuestos por una serie de cadenas de números variables separados por un guión (-).

Los SIDs son únicos en el dominio a diferencia de los GUID, los cuales son únicos en el universo ya explicado anteriormente.

Nota: Si se borra un security principal y luego se lo vuelve a crear con el mismo nombre (cómo ser *dbruno*) el mismo tendrá cuando lo volvamos a crear un SID diferente.

Un ejemplo de un SID sería:

```
S-1-5-21-3333797343-2748683396-701768906-1111
```

Todos los SIDs comienzan con S-1- y luego son seguidos por una secuencia de números separados cada uno de ellos con un guión (-). El próximo número que le sigue al S-1 es llamado SID Top-Level Authority value, el cual es usualmente un número entre el 0 y el 5.

El SID para las cuentas locales es de un 2. Para los security principals de dominio es un 5 (A partir de Windows 2000 en adelante). Después de este valor, el SID esta compuesto por uno o más campos de 32 bits separados por guiones (-). Los valores del medio usualmente indican el dominio en el cual el security principal está alojado. La porción de dominio siempre será idéntica para todos los objetos dentro del mismo dominio. El último valor es llamado Relative Identifier (RID).

SEGU-INFO.COM.AR

El RID es generado en el momento en que el objeto es creado. Los security principals built in (Cómo ser administrator, Everyone, Guest, etc) tienen RIDs bien conocidos (Well-Known RIDs) que son idénticos para cada security principal en cada dominio.

Los security principal que no vienen por default tienen un RID que arranca a partir del número 1003, y dicho valor de RID se va incrementando a medida que se crea un security principal. La mayoría de los security principals creados manualmente tienen un RID que empieza en el 1100 y de ahí para arriba. Un formato de SID se ve de esta manera:

```
S-1-X-X-X-X-RID
```

Debido entonces a los bien conocidos SID y RID, es posible identificar a muchos security principals, no importa como sean llamados. En la siguiente tabla vemos listados los SID y RID bien conocidos. Los valores más importantes para los administradores de seguridad están marcados en negrita

SID	Description
S-1-0	Null Authority
S-1-0-0	Nobody or Anonymous Null Session ID. Assigned when a security principal or its SID can't be identified or is non-existent.
S-1-1	World Authority
S-1-1-0	Everyone group
S-1-2	Local Authority
S-1-2-0	Local group
S-1-3	Creator Authority
S-1-3-0	Creator Owner group
S-1-3-1	Creator group.
S-1-3-2	Creator Owner Server, not used in Windows 2000 and later
S-1-3-3	Creator Group Server, not used in Windows 2000 and later
S-1-4	Non-unique Authority
S-1-5	NT Authority
S-1-5-1	Dialup group
S-1-5-2	Network group
S-1-5-3	Batch group
S-1-5-4	Interactive group
S-1-5-5-X-X	Logon session; X-X is a random unique number assigned to a particular logon session.
S-1-5-6	Service group
S-1-5-7	Anonymous Logon or null session
S-1-5-8	Proxy SID; not used in Windows 2000 and later
S-1-5-9	Enterprise Domain Controllers group
S-1-5-10	Self
S-1-5-11	Authenticated Users group
S-1-5-12	Restricted Code group
S-1-5-13	Terminal Server Users group
S-1-5-14	Remote Interactive Logon group
S-1-5-15	This Organization group
S-1-5-18	LocalSystem (or System) account

SEGU-INFO.COM.AR

S-1-5-19	LocalService
S-1-5-20	NetworkService
S-1-5-21	Non-unique; SIDs are not unique
S-1-5-32	Built-in Domain
S-1-5-1000	Other Organization group
S-1-5-64-10	NTLM Authentication protocol
S-1-5-64-14	SChannel Authentication protocol
S-1-5-64-21	Digest Authentication protocol
S-1-5-x-x-x-500	Local or Domain Administrator
S-1-5-x-x-x-501	Local or Domain Guest
S-1-5-x-x-x-502	Krbtgt
S-1-5-x-x-x-512	Domain Admins
S-1-5-x-x-x-513	Domain Users group
S-1-5-x-x-x-514	Domain Guests group
S-1-5-x-x-x-515	Domain Computers group
S-1-5-x-x-x-516	Domain Controllers group
S-1-5-x-x-x-517	Cert Publishers group
S-1-5-x-x-x-518	Schema Admins group
S-1-5-x-x-x-519	Enterprise Admins group
S-1-5-x-x-x-520	Group Policy Creator Owners group
S-1-5-x-x-x-553	RAS and IAS Servers group
S-1-5-x-x-x-544	Administrators group
S-1-5-x-x-x-545	Users group
S-1-5-x-x-x-546	Guests group
S-1-5-x-x-x-547	Power Users group
S-1-5-x-x-x-548	Account Operators group
S-1-5-x-x-x-549	Server Operators group
S-1-5-x-x-x-550	Print Operators group
S-1-5-x-x-x-551	Backup Operators group
S-1-5-x-x-x-552	Replicator group
S-1-5-x-x-x-553	RAS Servers group
S-1-5-x-x-x-554	Pre-Windows 2000 Compatibility Access group
S-1-5-x-x-x-555	Remote Desktop Users group
S-1-5-x-x-x-556	Network Configuration Operators group
S-1-5-x-x-x-557	Incoming forest trust builders group
S-1-5-x-x-x-558	Performance monitor users group
S-1-5-x-x-x-559	Performance log users group
S-1-5-x-x-x-560	Windows Authorization Access group
S-1-5-x-x-x-561	Terminal Server License Servers group
S-1-5-x-x-x-562	Distributed COM Users group
S-1-6	Site Server Authority
S-1-7	Internet Site Authority
S-1-8	Exchange Authority
S-1-9	Resource Manager Authority

Las x-x-x representan el SID del dominio y del workgroup.

SEGU-INFO.COM.AR

Nota: Esta guía de SID y RID bien conocidos la relevé investigando por mi cuenta tanto recursos varios publicados en la web como en la documentación de Microsoft localizada en:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/well_known_sids.asp

www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/Windows/XP/all/reskit/en-us/prnc_sid_cids.asp

http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q243330

También del material de Jan De Clercq's Windows Server 2003 Security Infrastructures (Elsevier Digital Press, 2004).

Esta tabla si bien uno sabe que no se la va a acordar de memoria, tampoco persigue ese fin pero la misma puede sernos muy útil cuando Windows nos muestra el SID en vez del nombre del objeto. Por ejemplo es común ver el SID S-1-5-32-547 cuando uno observa los permisos NTFS default en un domain controller Windows 2003. Si me encuentro con este cuadro y me remito a la tabla voy a ver que ese SID pertenece al grupo Power Users. Esto ocurre entonces debido a que Windows 2003 elimina al grupo Power Users cuando se lo promociona cómo controlador de dominio.

Herramientas para Visualizar los SIDs

Existen hoy en el mercado varias herramientas de visualización de los SID, vamos a enumerar sólo dos para el caso, las cuales son:

- Whoami.exe
- Sid2user.exe and User2sid.exe (Programada por Evgenii B. Rudnyi)

Hay muchos programas de whoami en el mundo, pero la versión que despliega los Windows SIDs está incluida en Windows XP Profesional y Windows Server 2003 (La versión de Windows 2003 es mucho mas rica funcionalmente hablando y se la puede copiar en el Windows XP). Si uno tipea el comando **Whoami** por cuenta propia nos va a traer sólo el nombre de usuario del usuario logueado, precedido por el nombre del dominio o del grupo de trabajo (Workgroup), cómo por ejemplo example\dbruno.

Si uno tipea entonces **Whoami /user,** se obtendrá el SID del usuario logueado, ejemplo:

```
C:\WINDOWS\system32>whoami /user

USER INFORMATION
----------------
User Name      SID
============== ============================================
example\dbruno S-1-5-21-3334797343-2748683396-701868904-1111
```

SEGU-INFO.COM.AR

En cambio si uno tipea **Whoami /user /groups,** se obtendrá una lista de los SIDs de todos los grupos a los que el usuario pertenece, por ejemplo:

```
USER INFORMATION
----------------
User Name      SID
============== ============================================
Example\dbruno S-1-5-21-3334797343-2748683396-701868904-1114

GROUP INFORMATION
-----------------
Group Name                           Type             SID
Attributes
==================
============================================================
Everyone                               Well-known group S-1-1-0
                    Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                 Alias            S-1-5-32-544
                    Mandatory group, Enabled by default, Enabled group,
Group owner
BUILTIN\Users                          Alias            S-1-5-32-545

                    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4
                    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11
                    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0
                    Mandatory group, Enabled by default, Enabled group
Example\Data                        Group            S-1-5-21-3334797343-274868
3396-701868904-1131 Mandatory group, Enabled by default, Enabled group
Example\Group Policy Creator Owners Group            S-1-5-21-3334797343-
274868
3396-701868904-520  Mandatory group, Enabled by default, Enabled group
Example\Domain Admins                Group           S-1-5-21-3334797343-
274868
3396-701868904-512  Mandatory group, Enabled by default, Enabled group
Example\Enterprise Admins            Group           S-1-5-21-3334797343-
274868
3396-701868904-519  Mandatory group, Enabled by default, Enabled group
```

Nota: Estas salidas se realizaron con la versión de Whoami de Windows 2003 ya que la versión que viene en el XP sólo utiliza el /all para desplegar los SID tanto de la cuenta del usuario como de los grupos a los que pertenece.

Para ver al SID del usuario actualmente logueado en el equipo es suficiente con la herramienta Whoami de Microsoft, pero se necesita de otra herramienta diferente para poder visualizar el SID de una cuenta que no esté logueada. Si bien cómo dijimos antes existen varias, la mas reconocida es la llamada Sid2user (La cual convierte o mapea un determinado SID a un usuario, grupo, o computadora. Y User2SID (El cual convierte el nombre común de un security principal en un SID).

SEGU-INFO.COM.AR

Aquí vemos un ejemplo de la salida de dicha herramienta:

```
C:\>user2sid dbruno
S-1-5-21-3334797343-2748683396-701868904-1117
Number of subauthorities is 5
Domain is example
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\>sid2user 5 21 3334797343 2748683396 701868904 500
Name is dbruno
Domain is example
Type of SID is SidTypeUser
```

Existen muchas otras herramientas con las que se podrían hacer querys a los SIDs de usuarios, para el caso concreto del curso mostramos sólo estas dos para que se entienda el concepto, una vez entendido el concepto se puede utilizar cualquier otra.

Si bien Microsoft sigue recomendando en sus buenas prácticas que se renombre la cuenta del administrador, la realidad es que un atacante con los conocimientos necesarios, lo primero que va a realizar es un Query de SID para identificar rápidamente la cuenta del administrador o alguna built in en particular que esté buscando para una vez identificada pasar a intentar romperla.

SEGU-INFO.COM.AR