## SID

Imaginad que creamos una cuenta en nuestro equipo con nombre PACO y contraseña P1c4. Creamos varias carpetas que solo le pertenecen a el, ciframos archivos para que solo los pueda leer el, etc. Un día sin embargo por error borramos la cuenta PACO y todas esas informaciones quedan “huérfanas”.

Ni cortos ni perezosos decidimos crear otra vez la cuenta PACO con contraseña P1c4, para intentar acceder a dichos ficheros y carpetas. Pues bien, comprobaremos que nuestro sistema sabe perfectamente que ese nuevo PACO no tiene nada que ver con el antiguo PACO, y los considera usuarios totalmente distintos.

Esto es asi por que el sistema operativo no usa para referirse a las cuentas su nombre o su contraseña, esos son campos que usamos nosotros, al igual que nos llamamos entre nosotros con nuestro nombre, no con nuestro DNI.

El DNI que usa el sistema para referirse a las cuentas de usuario se denomina SID. (Security IDentifier o Identificador de Seguridad).

Un **SID** está formado de la siguiente manera:

S-1-5-21-448539723-413027322-839522115-1003

El último número, en este caso 1003 se conoce como **RID** (**identificador relativo del usuario)** y todo lo que está delante del mismo identifica el dominio al que pertenece ese usuario.

En concreto, esos tres grandes números que se observan (448539723-413027322-839522115) se generan automáticamente y al azar cada vez que instalamos un Windows, y aparecerán en todas las cuentas que creemos en dicho sistema. (Esta es la razón por la que no se debe simplemente “clonar” o copiar un Windows entero de una maquina a otra, puesto que este número será igual y esos sistemas no podrán trabajar adecuadamente en red).

La parte del SID S-1-5-21 nos da información sobre el objeto con el que estamos trabajando. Así por ejemplo si hablamos de algunos grupos o usuarios especiales tenemos:

S-1-1-0 es el SID del grupo Todos (Everyone)

S-1-2-0 es el SID del grupo Usuarios locales

S-1-3-1 es el SID de Creator – Owner

S-1-5 Este inicio de SID nos indica que estamos trabajando con un usuario o grupo normal. Dentro de este grupo algunos SID conocidos son:

S-1-5-32-544 SID del grupo Administradores

S-1-5-32-545 SID del grupo Usuarios

El RID del Administrador siempre es el 500.

Desde Windows es posible ver los SID que se le asignan a nuestros usuarios y grupos con la orden **whoami.exe**. Si veis que Windows no reconoce este comando, se puede instalar desde el CD de Windows o bien desde Internet. Esto es así porque esta orden no es de las que vienen incluidas en una instalación típica de Windows XP (si normalmente en Vista), para instalar esta orden (y otras varias también bastante interesantes) debéis instalar las herramientas de soporte de Windows.

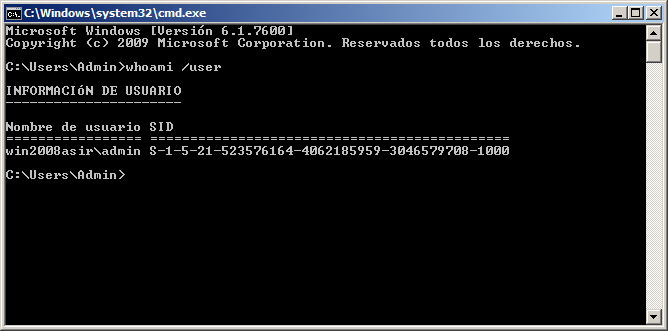
Para ello, introducid el CD de Windows XP Profesional en la unidad de CD con el sistema en marcha, explorad dicho CD y ejecutar el programa SETUP que está en la carpeta \SUPPORT\TOOLS. Esto instalará en vuestro sistema varias herramientas, entre las cuales estará el comando WHOAMI.EXE.

Una vez instalado, abrid un shell, y ejecutad la siguiente orden:

whoami /USER

Que os responderá algo como lo siguiente:

[User]="SIS\Joan" S-1-5-21-448539723-413027322-839522115-1003



Podemos ver aquí como nos dice el nombre de nuestro usuario actual y además nos indica que SID le ha sido otorgado por el sistema.

Si queremos ver no solo el SID que se le ha otorgado a nuestro usuario, sino el SID de todos los grupos a los que pertenece nuestro usuario, usad la orden con los parámetros /GROUPS.