



Entrez le **numéro** correspondant à la partition où se trouve votre installation de Windows. Regardez les partitions trouvées sous **Candidate Windows partitions found** et fiez-vous à leur taille ou bien leur label pour trouver la bonne, celle où se trouve Windows.

```

**** Unlocking locked/disabled accounts also supported.
**** It also has a registry editor, and there is now support fo
**** adding and deleting keys and values.
**** Tested on: NT3.51 & NT4: Workstation, Server, PDC.
**** Win2k Prof & Server to SP4. Cannot change AD.
**** XP Home & Prof: up to SP3
**** Win 2003 Server (cannot change AD passwords)
**** Vista & Win7 32 and 64 bit, Server 2008 32+64 b
*****
***** HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOW
*****
=====
Here are several steps to go through:
- Disk select, with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
=====
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 107.3 GB, 107374182400 bytes
Disk /dev/sdb: 107.3 GB, 107374182400 bytes

Candidate Windows partitions found:
#-----#
# /dev/sda1 100MB BOOT
# /dev/sda2 422397MB
# /dev/sda3 600000MB
# /dev/sdb1 102399MB

Please select partition by number or
q == quit
d == automatically start disk drivers
m == manually select disk drivers to load
f == fetch additional drivers from floppy / usb
a == show all partitions found
l == show probable Windows (NTFS) partitions only
Select: [1] 2

```

Le programme nous demande quel est le chemin qui mène au Registre Windows. Laissez le choix par défaut en appuyant sur Entrée

```

=====
Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 107.3 GB, 107374182400 bytes
Disk /dev/sdb: 107.3 GB, 107374182400 bytes

Candidate Windows partitions found:
#-----#
# /dev/sda1 100MB BOOT
# /dev/sda2 422397MB
# /dev/sda3 600000MB
# /dev/sdb1 102399MB

Please select partition by number or
q == quit
d == automatically start disk drivers
m == manually select disk drivers to load
f == fetch additional drivers from floppy / usb
a == show all partitions found
l == show probable Windows (NTFS) partitions only
Select: [1] 2

Selected 2

Mounting from /dev/sda2, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes:
Success!

=====
Step TWO: Select PATH and registry files
=====
DEBUG path: windows found as Windows
DEBUG path: system32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config

What is the path to the registry directory? (relative to windows disk)
[Windows/System32/config] :

```

Appuyez une nouvelle fois sur Entrée pour charger la base de données SAM, le gestionnaire des comptes de sécurité de Windows

```

Selected 2
Mounting from /dev/sda2, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes!
Success!
=====
Step TWO: Select PATH and registry files
=====
DEBUG path: windows found as Windows
DEBUG path: system32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config
What is the path to the registry directory? (relative to windows disk)
[Windows/System32/config] :
DEBUG path: Windows found as Windows
DEBUG path: System32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config
-rwxrwxrwx 2 0 0 28672 Feb 15 10:05 BCD-Template
-rwxrwxrwx 2 0 0 37486392 Mar 16 10:05 COMPONENTS
-rwxrwxrwx 2 0 0 65536 Mar 16 10:01 COMPONENTS<016888b
-llde-8ald-001e0bcde3ec).TM.blf 524288 Mar 16 10:01 COMPONENTS<016888b
-rwxrwxrwx 2 0 0 524288 Feb 15 15:18 COMPONENTS<016888b
-llde-8ald-001e0bcde3ec).TMContainer 524288 Mar 16 10:01 regtrans-ms
-rwxrwxrwx 2 0 0 262144 Mar 16 10:22 DEFAULT
-rwxrwxrwx 1 0 0 4096 Jul 14 2009 Journal
drwxrwxrwx 1 0 0 4096 Feb 28 16:22 RegBack
-rwxrwxrwx 1 0 0 262144 Mar 16 10:05 SAM
-rwxrwxrwx 1 0 0 4325165904 Mar 16 10:05 SECURITY
-rwxrwxrwx 1 0 0 11010048 Mar 16 10:05 SOFTWARE
drwxrwxrwx 1 0 0 4096 Feb 15 10:05 TXR
drwxrwxrwx 1 0 0 4096 Feb 15 10:06 systemprofile
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :

```

Appuyez encore une fois sur Entrée pour modifier les mots de passes des comptes utilisateur.

```

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :
Selected files: sam system security
Copying sam system security to /tmp
=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 110511 (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [400000] bytes, containing 8 pages (+ 1 headerpage)
Used for data: 294/57128 blocks/bytes, unused: 11/8152 blocks/bytes.
Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 11010048 [380000] bytes, containing 2395 pages (+ 1 headerp
Used for data: 167457/10761936 blocks/bytes, unused: 4955/52688 block
Hive <SECURITY> name (from header): <ewRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [400000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 341/16384 blocks/bytes, unused: 8/3936 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0

(<)=====(<) chntpw Main Interactive Menu (<)=====(<)
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] ->

```

Le programme affiche maintenant tous les comptes utilisateur du système. Pour chaque compte, on voit son nom (Username), s'il s'agit d'un compte administrateur (Admin) et si le compte est désactivé ou verrouillé (dis/lock). Entrez le nom du compte utilisateur pour lequel vous souhaitez effacer ou modifier le mot de passe puis faites Entrée. Dans l'exemple ci-dessous, je saisis l'utilisateur « Le Crabe »

```

=====
chntpw version 0.99.6 110511 (c) Petter N Hagen
Hive <SAM> name (from header): (\SystemRoot\System32\Config\SAM)
Root KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [400000] bytes, containing 8 pages (+ 1 headerpage)
Used for data: 294/57128 blocks/bytes, unused: 11/8152 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
Root KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 11010048 [480000] bytes, containing 2395 pages (+ 1 headerpage)
Used for data: 167457/16761936 blocks/bytes, unused: 4955/52688 blocks/bytes.

Hive <SECURITY> name (from header): (\emRoot\System32\Config\SECURITY)
Root KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [400000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 341/16384 blocks/bytes, unused: 8/3936 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0

<=====<> chntpw Main Interactive Menu <=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
  1 - Edit user data and passwords
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords =====
RID - Username - Admin? - Lock? --
01f4 Administrateur ADMIN dis/lock
03ea HomeGroupUser$
01f5 Invit : dis/lock !
03e9 Le Crabe ADMIN
03ed Madame Crabe ADMIN

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur] Le Crabe

```

☐ Plusieurs choix s’offrent à vous :

1. Effacer le mot de passe du compte utilisateur.
2. Définir un nouveau mot de passe.
3. Changer le type du compte : d’utilisateur standard à administrateur.
4. Débloquer et activer le compte utilisateur.

☐ Choisissez si vous préférez **effacer le mot de passe** ou **définir un nouveau mot de passe** pour votre compte utilisateur en entrant le chiffre adéquat. Dans l’exemple ci-dessous, je choisis d’effacer le mot de passe en entrant le chiffre 1 puis en faisant Entrée

```

  1 - Edit user data and passwords
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords =====
RID - Username - Admin? - Lock? --
01f4 Administrateur ADMIN dis/lock
03ea HomeGroupUser$
01f5 Invit : dis/lock !
03e9 Le Crabe ADMIN
03ed Madame Crabe ADMIN

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur] Le Crabe
RID: 1001 [03e9]
Username: Le Crabe
Fullname:
Comment:
Homedir:

User is member of 1 groups:
00000220 = Administrateurs (which has 3 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: 31

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [seems unlocked already]
q - Quit editing user, back to user select
Select: [1] ->

```

Entrez ! (le point d'exclamation) pour quitter le menu d'édition des comptes utilisateur. Attention le clavier est en QWERTY : pour saisir le point d'exclamation, il faut appuyer simultanément sur les touches MAJ (⇧) + &

```
Failed login count: 0 while max tries is: 0
Total login count: 31
- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [seems unlocked already]
5 - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [administrateur] !
```

Saisissez a (comme le clavier est en QWERTY, appuyez sur la touche q) pour quitter

```
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [administrateur] !

<=====> chntpw Main Interactive Menu <=====>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
 1 - Edit user data and passwords
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)
What to do? [1] -> q
```

Confirmez les changements que vous venez d'effectuer en entrant y et en appuyant sur Entrée

```
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM> - OK
=====
Step FOUR: Writing back changes
=====
About to write file(s) back! Do it? [n] : q
```

☑ Quittez définitivement le programme en entrant n.

☑ Il ne vous reste plus qu'à redémarrer votre ordinateur en appuyant sur les touches Ctrl + Alt + Suppr et à vous connecter avec votre compte utilisateur