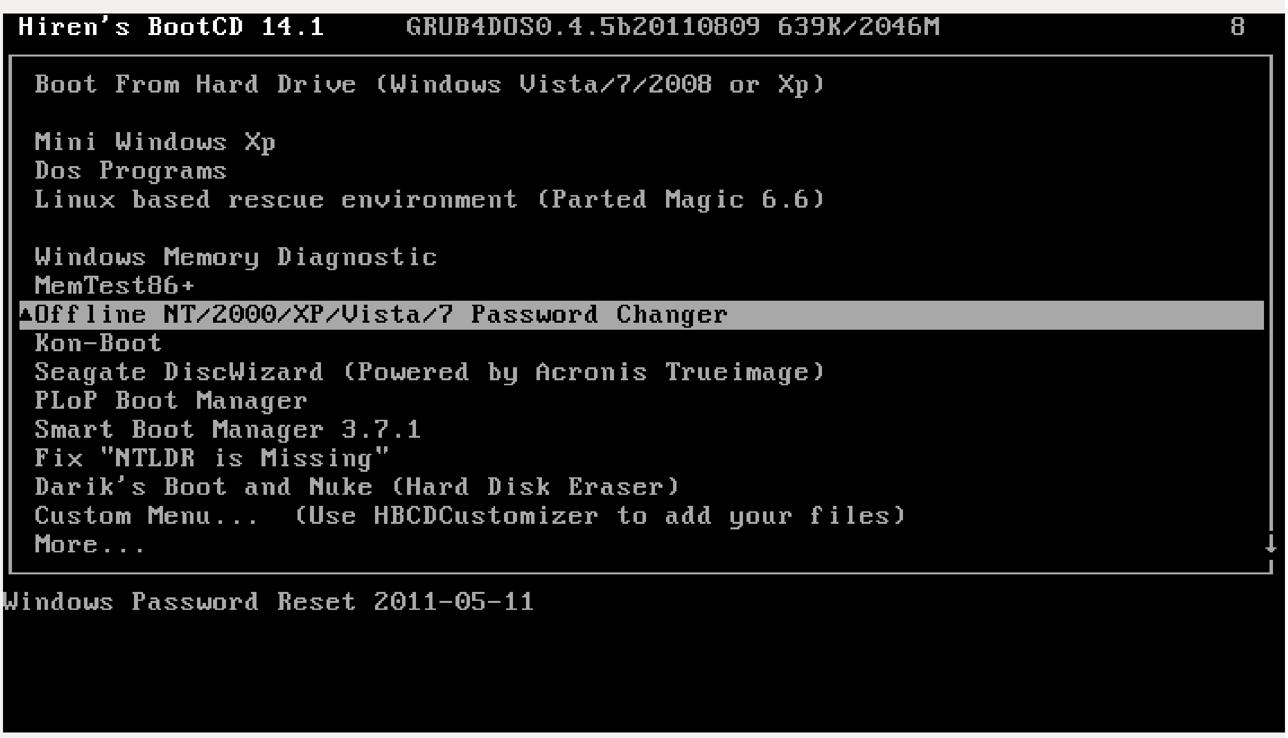
PRACTICA CON Hiren's Boot CD

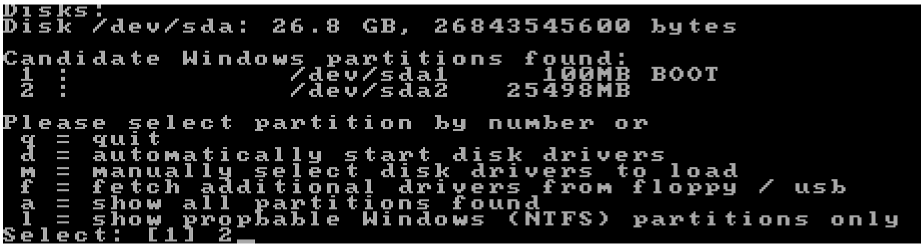
Lo primero que haremos sera iniciar el hirens boot con el sistema operativo.

Después elegimos esta opción :



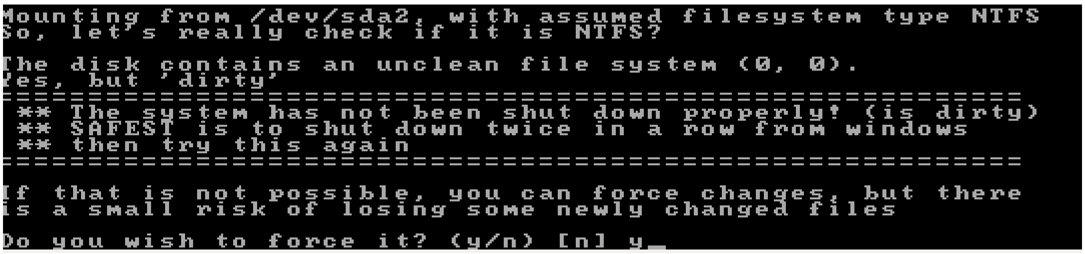
```
Hiren's BootCD 14.1     GRUB4DOS0.4.5b20110809 639K/2046M              8

 Boot From Hard Drive (Windows Vista/7/2008 or Xp)

 Mini Windows Xp
 Dos Programs
 Linux based rescue environment (Parted Magic 6.6)

 Windows Memory Diagnostic
 MemTest86+
▲Offline NT/2000/XP/Vista/7 Password Changer
 Kon-Boot
 Seagate DiscWizard (Powered by Acronis Trueimage)
 PLoP Boot Manager
 Smart Boot Manager 3.7.1
 Fix "NTLDR is Missing"
 Darik's Boot and Nuke (Hard Disk Eraser)
 Custom Menu...  (Use HBCDCustomizer to add your files)
 More...                                                              ↓

Windows Password Reset 2011-05-11
```

Elegimos la particion donde tenemos el so



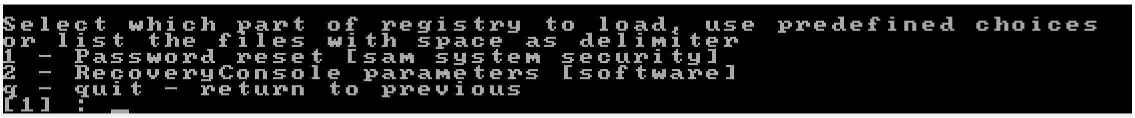
```
Disks:
Disk /dev/sda: 26.8 GB, 26843545600 bytes

Candidate Windows partitions found:
 1 :              /dev/sda1      100MB BOOT
 2 :              /dev/sda2    25498MB

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 propbable Windows (NTFS) partitions only
Select: [1] 2_
```

Nos pregunta si queremos conitnuar con el proceso : y

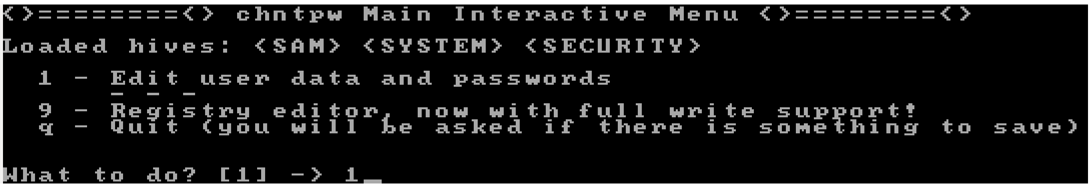


```
Mounting from /dev/sda2, with assumed filesystem type NTFS
So, let's really check if it is NTFS?

The disk contains an unclean file system (0, 0).
Yes, but 'dirty'
=========================================================
 ** The system has not been shut down properly! (is dirty)
 ** SAFEST is to shut down twice in a row from windows
 ** then try this again
=========================================================

If that is not possible, you can force changes, but there
is a small risk of losing some newly changed files

Do you wish to force it? (y/n) [n] y_
```

Nos pregunta que queremos hacer, elegimos la primera opción para resetear el password de la SAM.

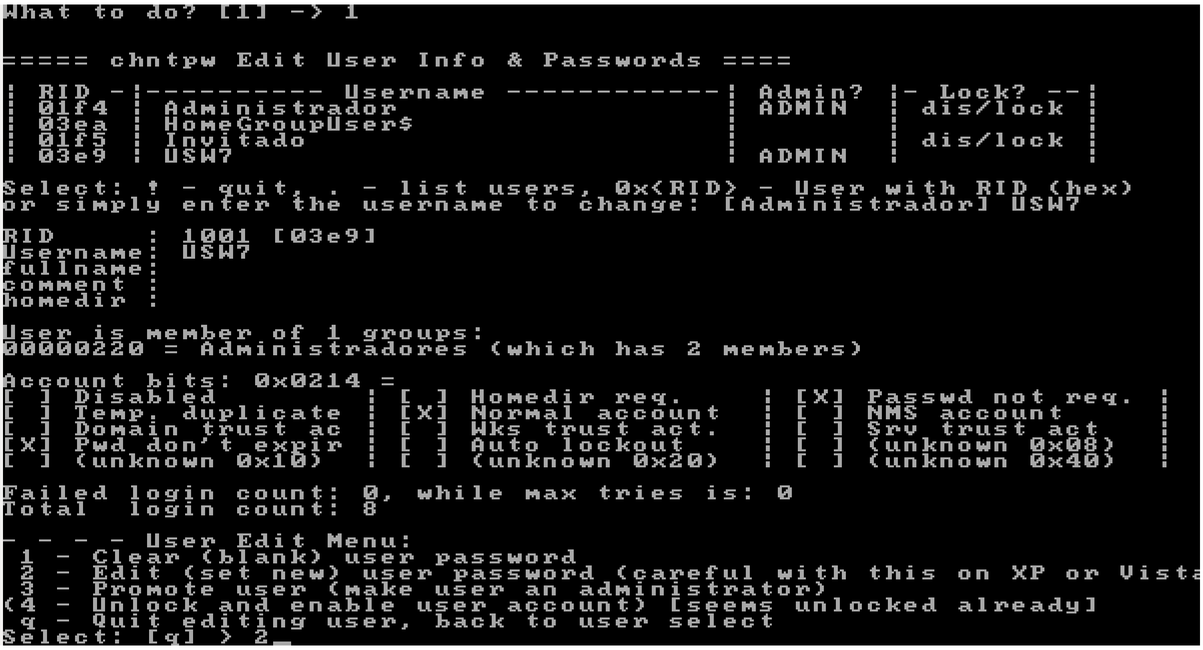


```
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : _
```



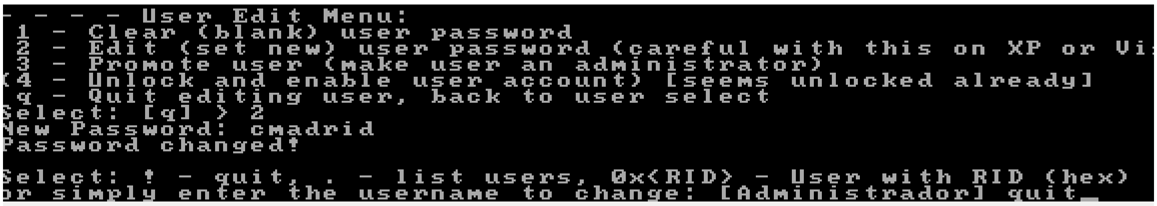
```
<>========<> chntpw Main Interactive Menu <>========<>

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] -> 1_
```

En estas capturas nos da a elegir todos los clientes del so para editarlos elegimos el usw7 que es el W7 que queremos editar



```
What to do? [1] -> 1

===== chntpw Edit User Info & Passwords ====

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrador                  | ADMIN  | dis/lock |
| 03ea | HomeGroupUser$                 |        |          |
| 01f5 | Invitado                       |        | dis/lock |
| 03e9 | USW7                           | ADMIN  |          |

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrador] USW7

RID     : 1001 [03e9]
Username: USW7
fullname:
comment :
homedir :

User is member of 1 groups:
00000220 = Administradores (which has 2 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: 8

- - - - 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: [q] > 2_
```

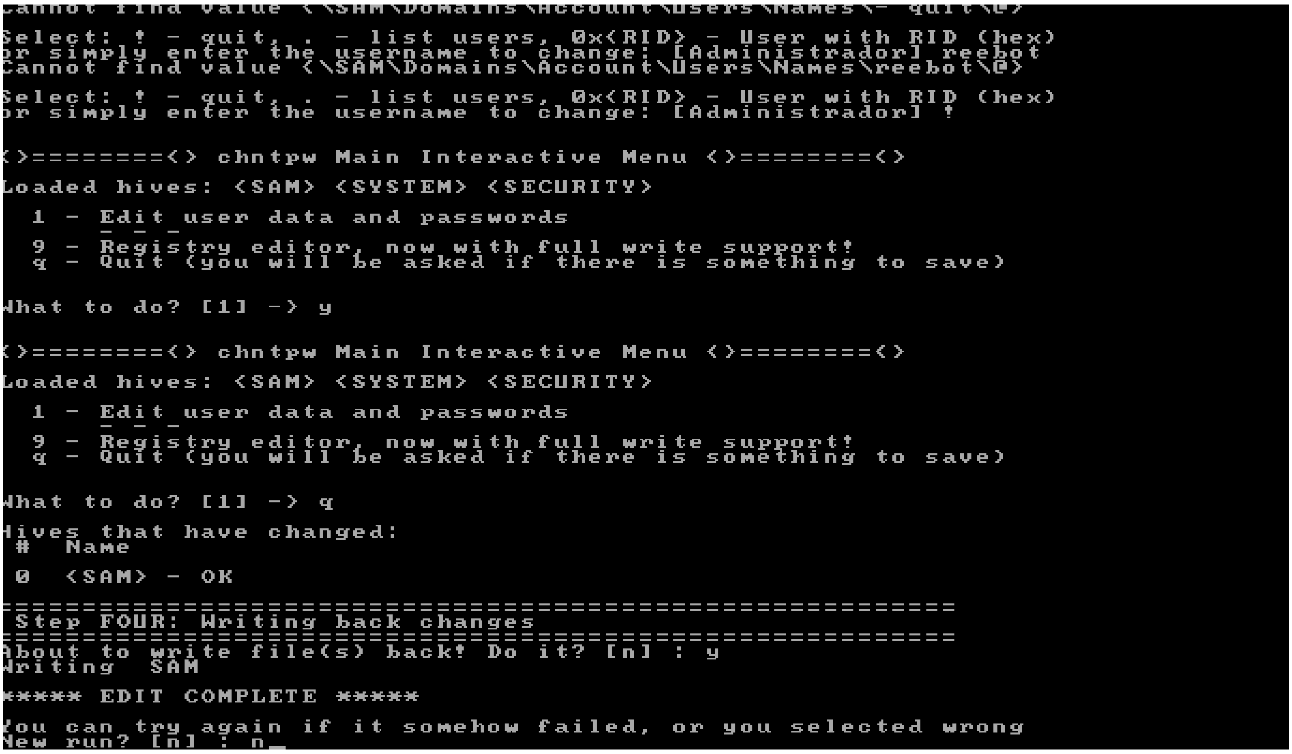
Elegimos de que forma queremos editarlo



```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vi
 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: [q] > 2
New Password: cmadrid
Password changed!

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

Nos preguntará si queremos guardarlo en la SAM ponemos : y

Depues nos dira que queremos hacer y ponemos : q para terminar y nos dora que se ha erminado la edicion y ponemos : n



```
Cannot find value <\SAM\Domains\Account\Users\Names\- quit\@>

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrador] reebot
Cannot find value <\SAM\Domains\Account\Users\Names\reebot\@>

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

<>========<> 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] -> y

<>========<> 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

Hives that have changed:
 #  Name

 0  <SAM> - OK

=========================================================
 Step FOUR: Writing back changes
=========================================================
About to write file(s) back! Do it? [n] : y
Writing  SAM

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] : n_
```