


RECUPERA TU SISTEMA WINDOWS CON HIREN'S BOOT

SEGURIDAD INFORMÁTICA 2º C.F.I

Diego García
Manuel Moscoso
Francisco Izquierdo
Rafael Polo



HIREN'S BOOT

¿CUÁLES SON NUESTROS PASOS A SEGUIR?

1.ACEDER A LA BIOS Y CONFIGURAR LOS PARÁMETROS NECESARIOS

2.ARRANCAR NUESTRO SISTEMA DESDE EL USB BOOTEADO

3.ACEDER A LA UTILIDAD ADECUADA DEL LINUX QUE UTILIZAREMOS

4.COMPROBAR QUE EL HACKEO SE HIZO CON ÉXITO

BIOS

- **CAMBIAR ARRANQUE DEL SISTEMA EN USB**
- **ASEGURARNOS DE GUARDAR LOS CAMBIOS CORRECTAMENTE**
- **SALIR DE LA BIOS DE FORMA SEGURA**

USB BOOTEADO

- **COMPROBAR QUE TIENE LA CAPACIDAD ADECUADA**
- **USAR NUESTRO SOFTWARE PREFERIDO PARA EL BOOTEO**
- **ALBERGAR EL HIREN'S BOOT AL NUESTRO USB**
- **ARRANCAR EL SISTEMA DESDE EL PENDRIVE BOOTEADO**



HIREN'S
BOOT

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

Mini Windows Xp

Dos Programs

Linux based rescue environment (Parted Magic 6.7)

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...

```

(c) 1997 - 2010 Petter N Hagen - pnordahl@eunet.no
GNU GPL v2 license, see files on CD

This utility will enable you to change or blank the password of
any user (incl. administrator) on an Windows NT/2k/XP/Vista
WITHOUT knowing the old password.
Unlocking locked/disabled accounts also supported.

It also has a registry editor, and there is now support for
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 bit

HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...
*****

```

```

=====
There 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: 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 propable Windows (NTFS) partitions only
Select: [1]

```

Elegimos la partición de disco que
queremos cargar...

There 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: 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 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] : _

There 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: 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 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] : _

Damos enter ahí donde
está señalado...

AHORA SE CARGARÁN UNOS CÓDIGOS
Y APARECERÁ UN MENÚ DE OPCIONES

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

-rw-rw-rw-r	2	0	0	28672	Nov	23	2012	BCD-Template
-rw-rw-rw-r	2	0	0	30932992	Nov	23	2012	COMPONENTS
-rw-rw-rw-r	2	0	0	65536	Nov	23	2012	COMPONENTS{6ccced2ed-6e01
-l1de-8bed-001e0bcd1824}	TM.blf							
-rw-rw-rw-r	2	0	0	524288	Nov	23	2012	COMPONENTS{6ccced2ed-6e01
-l1de-8bed-001e0bcd1824}	TMContainer	00000000	00000000	00000000	00000000	00000000	00000000	1.regtrans-ms
-rw-rw-rw-r	2	0	0	524288	Jul	14	2009	COMPONENTS{6ccced2ed-6e01
-l1de-8bed-001e0bcd1824}	TMContainer	00000000	00000000	00000000	00000000	00000000	00000000	2.regtrans-ms
-rw-rw-rw-r	1	0	0	262144	Nov	23	2012	DEFAULT
-rw-rw-rw-r	1	0	0	0	Jul	14	2009	Journal
-rw-rw-rw-r	1	0	0	0	Nov	23	2012	RegBack
-rw-rw-rw-r	1	0	0	262144	Nov	23	2012	SAM
-rw-rw-rw-r	1	0	0	262144	Nov	23	2012	SECURITY
-rw-rw-rw-r	1	0	0	22806528	Nov	23	2012	SOFTWARE
-rw-rw-rw-r	1	0	0	9961472	Nov	23	2012	SYSTEM
-rw-rw-rw-r	1	0	0	4096	Nov	23	2012	TxR
-rw-rw-rw-r	1	0	0	4096	Nov	23	2012	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] : _

Seleccionamos la opción 1
en nuestro caso...

NUEVA CARGA DE CÓDIGOS Y MENÚ DE OPCIONES


```
-rwxrwxrwx 1 0 0 9961472 Nov 23 2012 SYSTEM
drwxrwxrwx 1 0 0 4096 Nov 23 2012 TxR
drwxrwxrwx 1 0 0 4096 Nov 23 2012 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] : 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 [40000] bytes, containing 6 pages (+ 1 headerpage)

Used for data: 206/48040 blocks/bytes, unused: 12/9112 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>

ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>

File size 9961472 [980000] bytes, containing 2202 pages (+ 1 headerpage)

Used for data: 149983/9633552 blocks/bytes, unused: 4141/105904 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 [40000] bytes, containing 5 pages (+ 1 headerpage)

Used for data: 326/15672 blocks/bytes, unused: 10/4648 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] -> _

Opción 1...

```

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 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 206/48040 blocks/bytes, unused: 12/9112 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 9961472 [980000] bytes, containing 2202 pages (+ 1 headerpage)
Used for data: 149983/9633552 blocks/bytes, unused: 4141/105904 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 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 326/15672 blocks/bytes, unused: 10/4648 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] -> 1

===== chntpw Edit User Info & Passwords =====
RID  Username  Admin?  Lock?
01f4  Administrator  ADMIN  dis/lock
01f5  Guest          ADMIN  dis/lock
03e8  Juan           ADMIN  dis/lock

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

```

Aparece lista de usuarios... seleccionamos el que convenga.

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 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 206/48040 blocks/bytes, unused: 12/9112 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 9961472 [980000] bytes, containing 2202 pages (+ 1 headerpage)
Used for data: 149983/9633552 blocks/bytes, unused: 4141/105904 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 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 326/15672 blocks/bytes, unused: 10/4648 blocks/bytes.

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

Escribimos el nombre del
usuario...

```
<>=====<> 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
```

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

RID	Username	Admin?	Lock?
01f4	Administrator	ADMIN	dis/lock
01f5	Guest		dis/lock
03e8	Juan	ADMIN	

Select: ? - quit, . - list users, 0x<RID> - User with RID (1..n)
or simply enter the username to change: [Administrator] Juan



<>=====<> 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

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

RID	Username	Admin?	Lock?
01f4	Administrator	ADMIN	dis/lock
01f5	Guest		dis/lock
03e8	Juan	ADMIN	

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

RID : 1000 [03e8]
Username: Juan
fullname:
comment:
homedir :

Lista de tareas
numeradas...elegimos 1

User is member of 1 groups:
00000220 = Administrators (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: 3

----- 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] >

- 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

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

RID	Username	Admin?	Lock?
01f4	Administrator	ADMIN	dis/lock
01f5	Guest		dis/lock
03e8	Juan	ADMIN	

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

RID : 1000 [03e8]
Username: Juan
fullname:
comment:
homedir :

Nuestra contraseña quedó eliminada...

User is member of 1 groups:
000000220 = Administrators (which has 2 members)

Account bits: 0x0214 =

<input type="checkbox"/> Disabled	<input type="checkbox"/> Homedir req.	<input checked="" type="checkbox"/> Passwd not req.
<input type="checkbox"/> Temp. duplicate	<input checked="" type="checkbox"/> Normal account	<input type="checkbox"/> NMS account
<input type="checkbox"/> Domain trust ac	<input type="checkbox"/> Wks trust act.	<input type="checkbox"/> Srv trust act
<input checked="" type="checkbox"/> Pwd don't expir	<input type="checkbox"/> Auto lockout	<input type="checkbox"/> (unknown 0x08)
<input type="checkbox"/> (unknown 0x10)	<input type="checkbox"/> (unknown 0x20)	<input type="checkbox"/> (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 3

- - - 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] -> 1

Password cleared!

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

- 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

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

RID	Username	Admin?	Lock?
01f4	Administrator	ADMIN	dis/lock
01f5	Guest		dis/lock
03e8	Juan	ADMIN	

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

RID : 1000 [03e8]
Username: Juan
fullname:
comment:
homedir :

Salimos con opción "QUIT".... para
ello escribir símbolo !

User is member of 1 groups:
00000220 = Administrators (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: 3

- - - 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] > 1

Password cleared!

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

- 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

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

RID	Username	Admin?	Lock?
01f4	Administrator	ADMIN	dis/lock
01f5	Guest		dis/lock
03e8	Juan	ADMIN	

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

RID : 1000 [03e8]
Username: Juan
fullname:
comment:
homedir :

User is member of 1 groups:
00000220 = Administrators (which has 2 members)

Account bits: 0x0214 =

<input type="checkbox"/> Disabled	<input type="checkbox"/> Homedir req.	<input checked="" type="checkbox"/> Pw not req.
<input type="checkbox"/> Temp. duplicate	<input checked="" type="checkbox"/> Normal account	<input type="checkbox"/> NMS account
<input type="checkbox"/> Domain trust ac	<input type="checkbox"/> Wks trust act.	<input type="checkbox"/> Srv trust act
<input checked="" type="checkbox"/> Pwd don't expir	<input type="checkbox"/> Auto lockout	<input type="checkbox"/> (unknown 0x08)
<input type="checkbox"/> (unknown 0x10)	<input type="checkbox"/> (unknown 0x20)	<input type="checkbox"/> (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 3

- - - 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] > 1
Password cleared?

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



```
01f4 : Administrator      ADMIN      dis/lock
01f5 : Guest                ADMIN      dis/lock
03e8 : Juan                  ADMIN
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] Juan
```

```
RID      : 1000 [03e8]
Username: Juan
fullname:
comment :
homedir :
```

```
User is member of 1 groups:
000000220 = Administrators (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: 3
```

```
- - - - 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] > 1
Password cleared?
```

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

```
<>=====<> 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] -> _
```



```

comment :
homedir :

User is member of 1 groups:
00000220 = Administrators (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: 3

- - - - 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] > 1
Password cleared?

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

<>=====<> 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] : _

```

Volvemos a salir.... escribimos letra “q”

```

comment :
homedir :

User is member of 1 groups:
00000220 = Administrators (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: 3

- - - 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] > 1
Password cleared!

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

<>=====<> 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

```

Pregunta si queremos escribir los datos en Windows y decimos que sí.... “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: 3
```

```
- - - - 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] > 1
Password cleared!
```

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

```
<>=====<> 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
```

ENTER, y nos aparecerá este letrero...

```
=====
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] :
```

```
- - - 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] > 1
Password cleared!
```

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

```
<>=====<> 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 *****
```

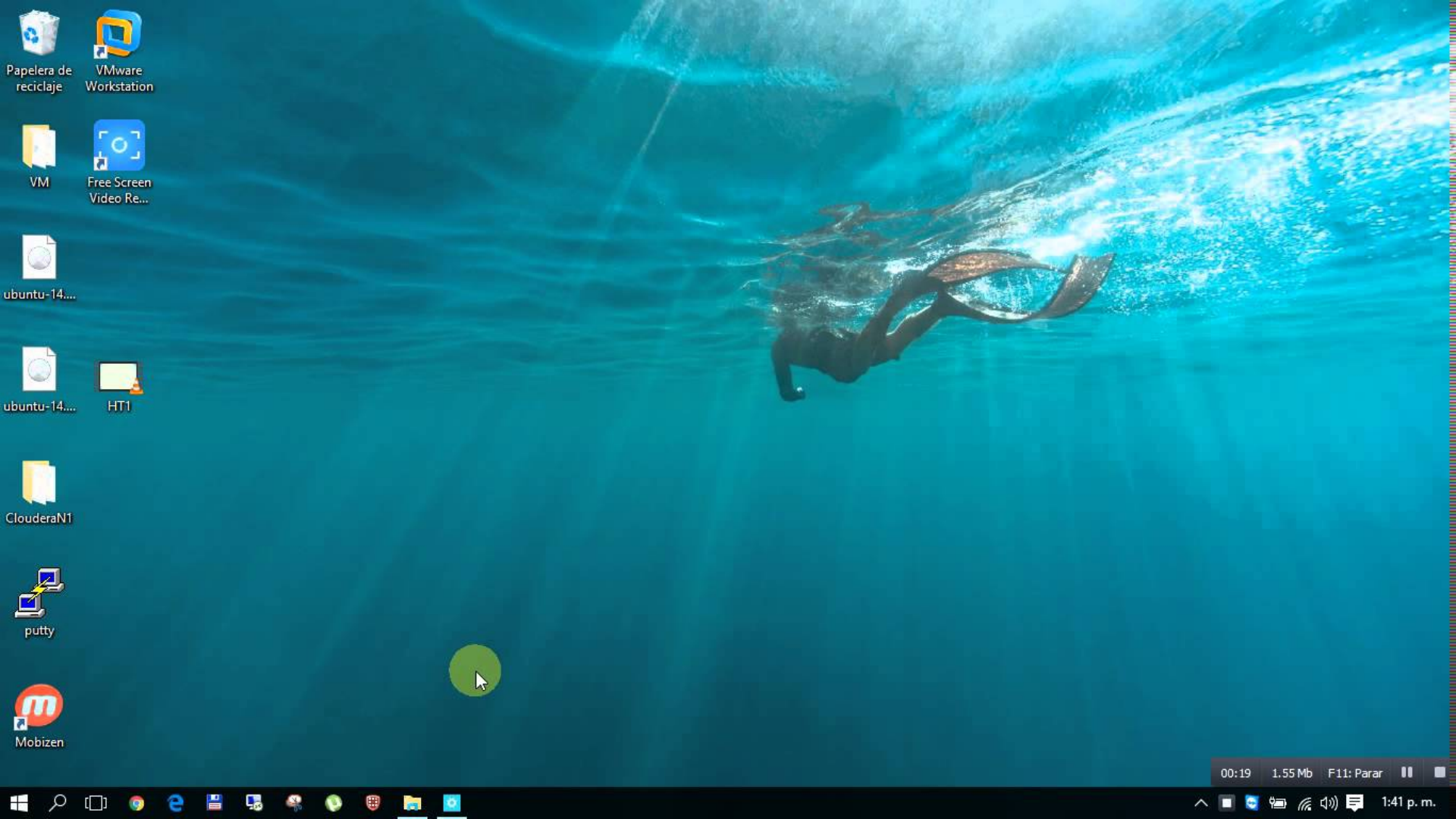
```
You can try again if it somehow failed, or you selected wrong
```

```
New run? [n] :
```

```
=====
* end of scripts.. returning to the shell..
* Press CTRL-ALT-DEL to reboot now (remove floppy first)
* or do whatever you want from the shell..
* However, if you mount something, remember to umount before reboot
* You may also restart the script procedure with 'sh /scripts/main.sh'
```

```
# reboot_
```

Junto a este símbolo #, escribimos reboot y damos ENTER



Papelera de reciclaje

VMware Workstation

VM

Free Screen Video Re...

ubuntu-14....

ubuntu-14....

HT1

ClouderaN1

putty

Mobizen

