

Offline NT Password & Registry Editor Walkthrough

The following is a walkthrough of using the CD to reset one user (admin) on a test Vista computer.

Insert the CD and convince your BIOS that it should boot from it. How to boot from a CD varies from computer make to computer make, so I cannot help you much. Some BIOS shows a boot device select menu if you press ESC, F8, F11 or F12 or something like that during the self test. (some even tell you on the screen what to press)

If it boots, you should see this:

```
ISOLINUX 3.51 2007-06-10 Copyright (C) 1994-2007 H. Peter Anvin
```

```
*****
*
* Windows NT/2k/XP/Vista Change Password / Registry Editor / Boot CD
*
* (c) 1998-2007 Petter Nordahl-Hagen. Distributed under GNU GPL v2
*
* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
*             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
*             CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
* More info at: http://home.eunet.no/~pnordahl/ntpasswd/
* Email       : pnordahl@eunet.no
*
* CD build date: Sun Sep 23 14:15:35 CEST 2007
*****
```

```
Press enter to boot, or give linux kernel boot options first if needed.
Some that I have to use once in a while:
boot nousb          - to turn off USB if not used and it causes problems
boot irqpoll        - if some drivers hang with irq problem messages
boot nodrivers      - skip automatic disk driver loading
```

```
boot:
```

Usually just press enter here. If you have linux knowledge, you can tweak kernel options if you need/like.

Then it boots and outputs a lot of kernel messages about your hardware and such.. most if not all are nothing to worry about.

```
Loading vmlinuz.....
Loading scsi.cgz.....

Loading initrd.cgz.....
Ready.
Linux version 2.6.22.6 (root@athene) (gcc version 4.1.1 20060724 (prerelease)
(4.1.1-3mdk)) #2 Sun Sep 9 16:59:48 CEST 2007
BIOS-provided physical RAM map:
  BIOS-e820: 0000000000000000 - 000000000009f800 (usable)
  BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)
```

Offline NT Password & Registry Editor Walkthrough

```
BIOS-e820: 000000000000ca000 - 000000000000cc000 (reserved)
BIOS-e820: 000000000000dc000 - 00000000000100000 (reserved)
BIOS-e820: 00000000000100000 - 000000000316f0000 (usable)
BIOS-e820: 000000000316f0000 - 000000000316ff000 (ACPI data)
BIOS-e820: 000000000316ff000 - 00000000031700000 (ACPI NVS)
BIOS-e820: 00000000031700000 - 00000000031800000 (usable)
BIOS-e820: 00000000fec000000 - 00000000fec100000 (reserved)
BIOS-e820: 00000000fee000000 - 00000000fee010000 (reserved)
BIOS-e820: 00000000fffe00000 - 00000001000000000 (reserved)
792MB LOWMEM available.
Zone PFN ranges:
  DMA             0 ->      4096
  Normal         4096 ->   202752
early_node_map[1] active PFN ranges

...

Serial: 8250/16550 driver $Revision: 1.90 $ 4 ports, IRQ sharing enabled
serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
Floppy drive(s): fd0 is 1.44M
FDC 0 is a post-1991 82077
RAMDISK driver initialized: 16 RAM disks of 32000K size 1024 blocksize
USB Universal Host Controller Interface driver v3.0
Initializing USB Mass Storage driver...
usbcore: registered new interface driver usb-storage
USB Mass Storage support registered.
serio: i8042 KBD port at 0x60,0x64 irq 1
serio: i8042 AUX port at 0x60,0x64 irq 12
usbcore: registered new interface driver usbhid
drivers/hid/usbhid/hid-core.c: v2.6:USB HID core driver
Using IPI Shortcut mode
BIOS EDD facility v0.16 2004-Jun-25, 1 devices found
Freeing unused kernel memory: 144k freed
Booting ntpasswd
Mounting: proc sys
Ramdisk setup complete, stage separation..
In stage 2
Spawning shells on console 2 - 6
Initialization complete!

** Preparing driver modules to dir /lib/modules/2.6.22.6
input: AT Translated Set 2 keyboard as /class/input/input0
```

Most of the generic linux boot now done, and we try to load the disk drivers. If you use the floppy version you will be asked to swap floppies at this point. Drivers are then tried based on PCI hardware identification.

```
** Will now try to auto-load relevant drivers based on PCI information

---- AUTO DISK DRIVER select ----
--- PROBE FOUND THE FOLLOWING DRIVERS:
ata_piix
ata_generic
mptspi
--- TRYING TO LOAD THE DRIVERS
### Loading ata_piix
```

Offline NT Password & Registry Editor Walkthrough

```
scsi0 : ata_piix
scsil : ata_piix
ata1: PATA max UDMA/33 cmd 0x000101f0 ctl 0x000103f6 bmdma 0x00011050 irq 14
ata2: PATA max UDMA/33 cmd 0x00010170 ctl 0x00010376 bmdma 0x00011058 irq 15
ata2.00: ATAPI: VMware Virtual IDE CDROM Drive, 00000001, max UDMA/33
ata2.00: configured for UDMA/33
scsi 1:0:0:0: CD-ROM          NECVMWar VMware IDE CDR10 1.00 PQ: 0 ANSI: 5
sr0: scsi3-mmc drive: 1x/1x xa/form2 cdda tray
Uniform CD-ROM driver Revision: 3.20
```

```
### Loading ata_generic
```

```
### Loading mptspi
```

```
Fusion MPT base driver 3.04.04
Copyright (c) 1999-2007 LSI Logic Corporation
Fusion MPT SPI Host driver 3.04.04
PCI: Found IRQ 9 for device 0000:00:10.0
mptbase: Initiating ioc0 bringup
ioc0: 53C1030: Capabilities={Initiator}
scsi2 : ioc0: LSI53C1030, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=9
scsi 2:0:0:0: Direct-Access    VMware, VMware Virtual S 1.0 PQ: 0 ANSI: 2
target2:0:0: Beginning Domain Validation
target2:0:0: Domain Validation skipping write tests
target2:0:0: Ending Domain Validation
target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
sd 2:0:0:0: [sda] 83886080 512-byte hardware sectors (42950 MB)
sd 2:0:0:0: [sda] Write Protect is off
sd 2:0:0:0: [sda] Cache data unavailable
sd 2:0:0:0: [sda] Assuming drive cache: write through
sd 2:0:0:0: [sda] 83886080 512-byte hardware sectors (42950 MB)
sd 2:0:0:0: [sda] Write Protect is off
sd 2:0:0:0: [sda] Cache data unavailable
sd 2:0:0:0: [sda] Assuming drive cache: write through
sda: sda1
sd 2:0:0:0: [sda] Attached SCSI disk
```

Most of these messages are from the drivers themselves. Some talk a lot, some doesn't. But all give info on the brand and model and size of the disks found, if any.

```
-----
Driver load done, if none loaded, you may try manual instead.
-----
```

```
** If no disk show up, you may have to try again (d option) or manual (m).
```

You can later load more drivers..

```
*****
* Windows Registry Edit Utility Floppy / chntpw *
* (c) 1997 - 2007 Petter N Hagen - pnordahl@eunet.no *
* GNU GPL v2 license, see files on CD *
*****
```

Offline NT Password & Registry Editor Walkthrough

```
*
* 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 SP2
*           Win 2003 Server (cannot change AD passwords)
*           Vista 32 and 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

```
=====
a Step ONE: Select disk where the Windows installation is
=====
```

Disks:
Disk /dev/sda: 42.9 GB, 42949672960 bytes

Candidate Windows partitions found:
1 : /dev/sda1 40958MB BOOT

Here it has found one disk with one partition

```
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]
```

Here you select one of the partitions listed above (in this case there is only one) or one of the letters from the menu.

Floppy users may need to do 'f' to load in more drivers from another floppy.

Offline NT Password & Registry Editor Walkthrough

The 'd' option will re-run the PCI scan and start relevant drivers (they must already be loaded from floppy with 'f' option)

The 'm' for manual load will present a list of all the drivers with short description if available, and allow you to specify which to load. (Dependencies are handled automatically)

Here we only have one partition, so we just press enter to select it.

```
Selected 1

Mounting from /dev/sda1, with filesystem type NTFS

NTFS volume version 3.1.
```

It was an NTFS filesystem, and it mounted successfully.

```
=====
a Step TWO: Select PATH and registry files
=====
What is the path to the registry directory? (relative to windows disk)
[WINDOWS/system32/config] :
```

The registry is usually system32/config under WINDOWS or WINNT directory, depending on the windows version (and it may be changed during installation).

If the correct partition has been selected, the default prompt will be adjusted to match if it can find one of the usual variants.

We accept the defaults.. and get a (bit filtered) directory listing showing most of the interesting registry files

```
-rw----- 2 0 0 262144 Feb 28 2007 BCD-Template
-rw----- 2 0 0 6815744 Sep 23 12:33 COMPONENTS
-rw----- 1 0 0 262144 Sep 23 12:33 DEFAULT
drwx----- 1 0 0 0 Nov 2 2006 Journal
drwx----- 1 0 0 8192 Sep 23 12:33 RegBack
-rw----- 1 0 0 524288 Sep 23 12:33 SAM
-rw----- 1 0 0 262144 Sep 23 12:33 SECURITY
-rw----- 1 0 0 15728640 Sep 23 12:33 SOFTWARE
-rw----- 1 0 0 9175040 Sep 23 12:33 SYSTEM
drwx----- 1 0 0 4096 Nov 2 2006 TxR
drwx----- 1 0 0 4096 Feb 27 2007 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] :
```

Offline NT Password & Registry Editor Walkthrough

Choice 1 is for password edit, most used.

But if you wish, you can load any of the files (just enter it's name) and do manual registry edit on them.

But here, we select 1 for password edit, some files are copied around into memory and the edit application is invoked.

```
Selected files: sam system security
Copying sam system security to /tmp
```

```
=====
a Step THREE: Password or registry edit
=====
chntpw version 0.99.5 070923 (decade), (c) Petter N Hagen
Hive name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x44000 is not 'hbin', assuming file contains garbage at end
File size 524288 [80000] bytes, containing 11 pages (+ 1 headerpage)
Used for data: 288/250904 blocks/bytes, unused: 15/23176 blocks/bytes.

Hive name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x8b4000 is not 'hbin', assuming file contains garbage at end
File size 9175040 [8c0000] bytes, containing 2117 pages (+ 1 headerpage)
Used for data: 96982/6224016 blocks/bytes, unused: 4381/2830032 blocks/bytes.

Hive name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x6000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 334/17312 blocks/bytes, unused: 7/3008 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:

- 1 - Edit user data and passwords
- 2 - Syskey status & change
- 3 - RecoveryConsole settings
- - -
- 9 - Registry editor, now with full write support!
- q - Quit (you will be asked if there is something to save)

What to do? [1] ->

Offline NT Password & Registry Editor Walkthrough

This demo shows selection 1 for password edit, but you can also do other things.

Note that 2, Syskey may be dangerous! AND NOT NEEDED TO RESET PASSWORDS! and does not work at all on Vista, but you get some info before you do any changes.

Selection 3, RecoveryConsole is only relevant for Win2k, XP and 2003 and you must have selected to load the SOFTWARE part of the registry (selection 2) earlier.

The manual registry editor is always available, it is not the most user-friendly thing, but anyway..

We continue our quest to change our "admin" users password..

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

RID	Username	Admin?	Lock?
03e8	admin	ADMIN	
01f4	Administrator	ADMIN	dis/lock
03ec	grumf1		
03ed	grumf2		
03ee	grumf3		
01f5	Guest		dis/lock
03ea	jalla1	ADMIN	*BLANK*
03eb	jalla2		*BLANK*
03e9	petro	ADMIN	*BLANK*

This is a list of all local users on the machine. You may see more users here than in the overly user-friendly control panel, for example XP has some help and support built in users.

The users marked "ADMIN" are members of the administrators group, which means they have admin rights, if you can login to one of them you can get control of the machine.

The built in (at install time in all windows versions) administrator is always RID 01f4. This example is from Vista, and Vista by default has this locked down (the installer instead asks and makes another user the regular use administrator, in this case RID 03e8)

The "lock?" column show if the user account is disabled or locked out (due to many logon attempts for example) or BLANK if the password seems to be blank.

We select to edit the "admin" user (this was the user made administrator by the Vista installer)

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

```
RID      : 1000 [03e8]
Username: admin
fullname:
comment :
```

Offline NT Password & Registry Editor Walkthrough

homedir :

User is member of 1 groups:
00000220 = Administrators (which has 4 members)

Group 220 is THE BOSS GROUP! :)

```
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
```

Some status info, user is locked out if "Disabled" is set or "Failed login count" is larger than "max tries" policy setting. This user is not locked in any way. The lockout can be reset with option 4 below.

```
- - - - 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!
```

Here we just reset/clear/blank the password.

But you can also try to set a new password with option 2, but it will only work if the password is not blank already. Also, it often fails to work on XP and newer systems.

Number 3 is to put a non-admin user into the administrators (220) group, thus making the user an administrator. IT IS STILL EXPERIMENTAL AND IT MAY sometimes RESULT IN STRANGE ERRORS WHEN LATER EDITING THE GROUP FROM WINDOWS! Also, usually pointless in promoting the Guest user, as it is most likely forbidden to log in by the security policy settings.

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

Exclamation point ! quits out (it's SHIFT 1 on the US keyboard layout used on the boot CD)

Then we get back to the main menu, and select to quit..

```
===== chntpw Main Interactive Menu =====
Loaded hives: <sam> <system> <security>
```

Offline NT Password & Registry Editor Walkthrough

- 1 - Edit user data and passwords
- 2 - Syskey status & change
- 3 - RecoveryConsole settings
- - -
- 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 - OK
```

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

You must answer y, or the changes will not be saved. This is the last chance to change your mind!

Writing sam

Only changed files of the registry are actually written back.

If you forgot something, you may run again, else press CTRL-ALT-DEL to reboot.

```
***** EDIT COMPLETE *****
```

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

```
(Please ignore the message about job control, it is not relevant)
```

```
BusyBox v1.1.0-pre1 (2005.12.30-19:45+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
sh: can't access tty; job control turned off
```

And I got about a gazillion questions on this error message, even if it is mentioned in the [FAQ](#). It is from the shell telling it cannot do "job control" which means it cannot handle CTRL-C etc. It HAS NOTHING TO DO WITH YOUR PASSWORD RESET DID NOT WORK! That is caused by a lot of other things.