

Offline NT Password Editor

Записываем программу на Компакт диск или копируем на флэшку (смотрите файл [риджи](#) в распакованном архиве, для того, чтоб прописать на флэшке загрузчик), загружаемся с записанного сменного носителя. В случае необходимости, [в BIOS и изменяем очередность загрузочных устройств](#).

Сменный носитель, с записанным Offline NT Password Editor, должен быть первым в списке загрузочных устройств.

```
*****
*
*      Windows Reset Password / Registry Editor / Boot CD
*
*      (c) 1998-2011 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://pogostick.net/~pnh/ntpasswd/
*      Email       : pnh@pogostick.net
*
*      CD build date: Wed May 11 20:16:09 CEST 2011
*****

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

boot: _
```

Шаг 1: Выбираем жесткий диск, на котором установлен Windows

В данном случае следует выбрать пункт 1, который выбран по умолчанию, поэтому можно просто нажать энтер. В вашем случае номер может отличаться, выбирайте правильный системный диск ориентируясь по его размеру - введите его цифру и нажмите энтер:

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

Disks:
Disk /dev/sda: 10.7 GB, 10737418240 bytes

Candidate Windows partitions found:
 1 :          /dev/sda1   10228MB BOOT

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] _
```

Шаг 2: Выбираем путь к файлам реестра

Путь по умолчанию, предложенный программой нас устраивает - нажимаем энтер:

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

Система спрашивает какую часть реестра загружать. Нас интересует сброс пароля, поэтому выбираем "1":

```
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] : _
```

Шаг 3: Изменение пароля или редактирование реестра

В открывшемся меню "chntpw Main Interactive Menu", можно менять информацию о пользователях и их пароли. Для того чтоб сбросить пароль пользователя нам нужен 1-й пункт, который уже выбран по умолчанию, поэтому просто нажимаем энтер:

```

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

```

Сбрасываем пароль Администратора

Если у вас система русскоязычная и имя пользователя "Администратор" записано на русском - вместо имени вы увидите непонятный набор символов.

Для такого случая предусмотрена возможность выбора пользователя по его шестнадцатеричному коду (RID). Например у моего админа RID - **0x01f4** (первые два символа - Ноль и Екс, обозначают что число шестнадцатеричное). Если у вашего пользователя другой RID, вводите такой как у вас.

В моем случае по умолчанию выбран пользователь Admin, поэтому мне ничего набирать не нужно - просто нажимаю энтер:

```

===== chntpw Edit User Info & Passwords =====
| RID -|----- Username -----| Admin? |- Lock? --|
| 01f4 | Admin          | ADMIN  | *BLANK*  |
| 03eb | ASPNET         |        |          |
| 03e8 | HelpAssistant  |        | dis/lock |
| 03ea | SUPPORT_388945a0 |        | dis/lock |
| 03f0 | vpn            |        | *BLANK*  |
| 01f5 | >ABL           |        | dis/lock |

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

```

Теперь само действие, которое нужно выполнить в отношении выбранного пользователя. Вводим цифру 1 - "Clear (blank) user password" и нажимаем энтер:

```

- - - - 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: [Admin] _

```

В случае успеха, программа сообщает **Password cleared!**

Теперь осталось сохранить изменения и выйти из системы.

Шаг 4: Сохраняем изменения

- Вводим (!) и нажимаем энтер для выхода из "User Edit Menu".
- Вводим (q) и нажимаем энтер для выхода из "chntpw Main Interactive Menu".
- Система предупреждает, что были сделаны изменения и предложит их сохранить.

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

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

- На вопрос **About to write file(s) back! Do it?** отвечаем утвердительно (y)
- На вопрос **New Run?** (по умолчанию нет), отвечаем отрицательно, то-есть просто нажимаем энтер.
- Пишем команду **reboot**, или нажимаем резет на системном блоке.

```
=====
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

=====

* 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_
```