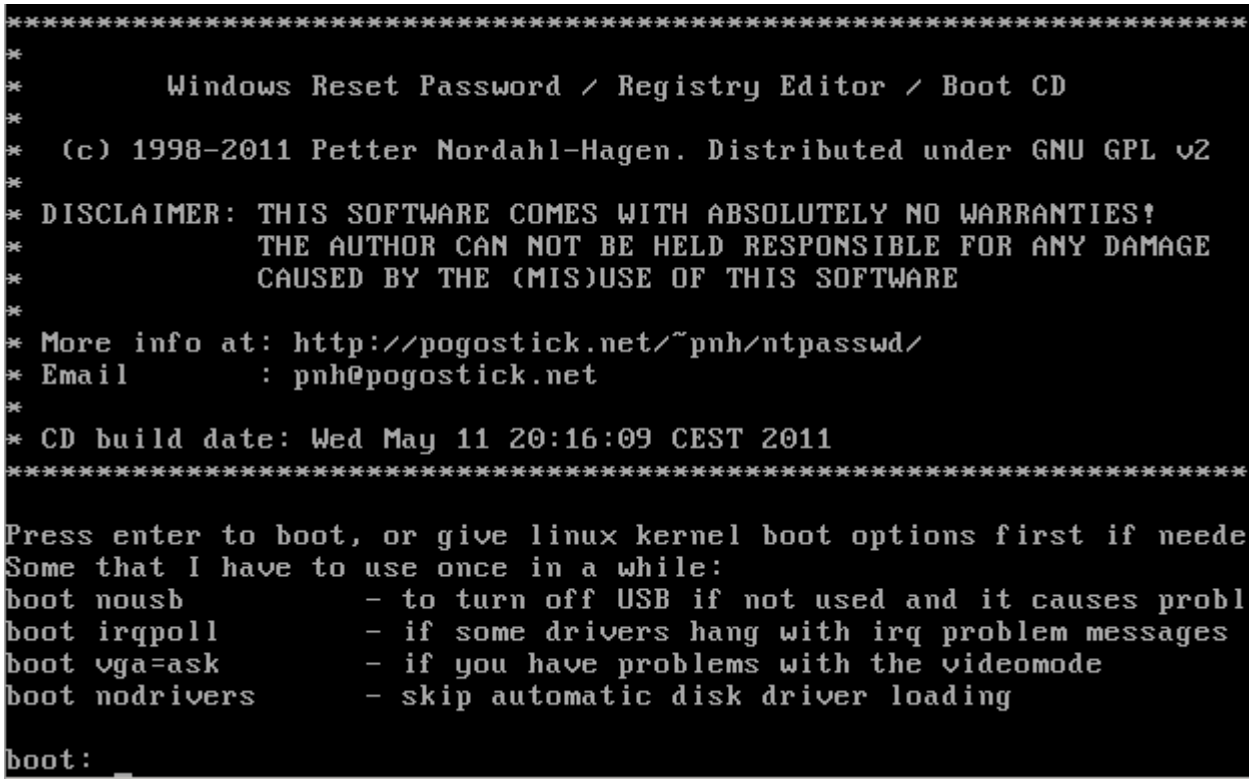
Offline NT Password Editor

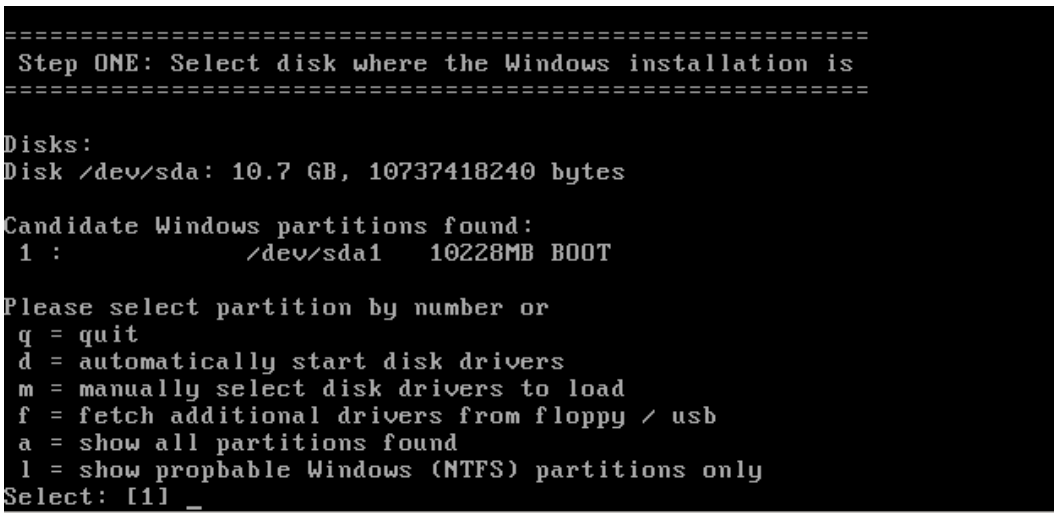
Записываем программу на Компакт диск или копируем на флэшку (смотрите файл ридми в распакованном архиве, для того, чтоб прописать на флэшке загрузчик), загружаемся с записанного сменного носителя. В случае необходимости, в BIOS и изменяем очередность загрузочных устройств.

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



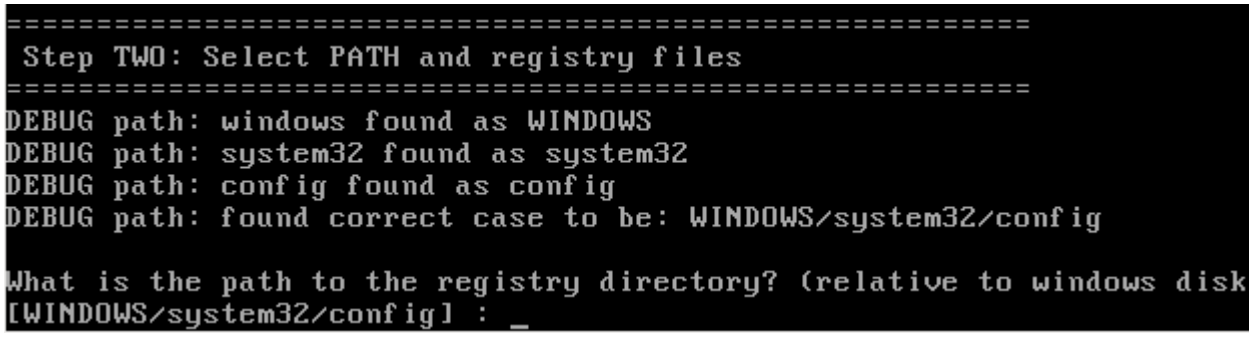
Шаг 1: Выбираем жесткий диск, на котором установлен Windows

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

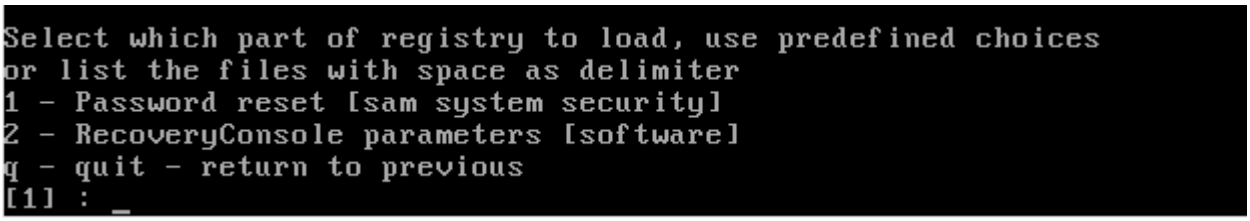


Шаг 2: Выбираем путь к файлам реестра

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



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

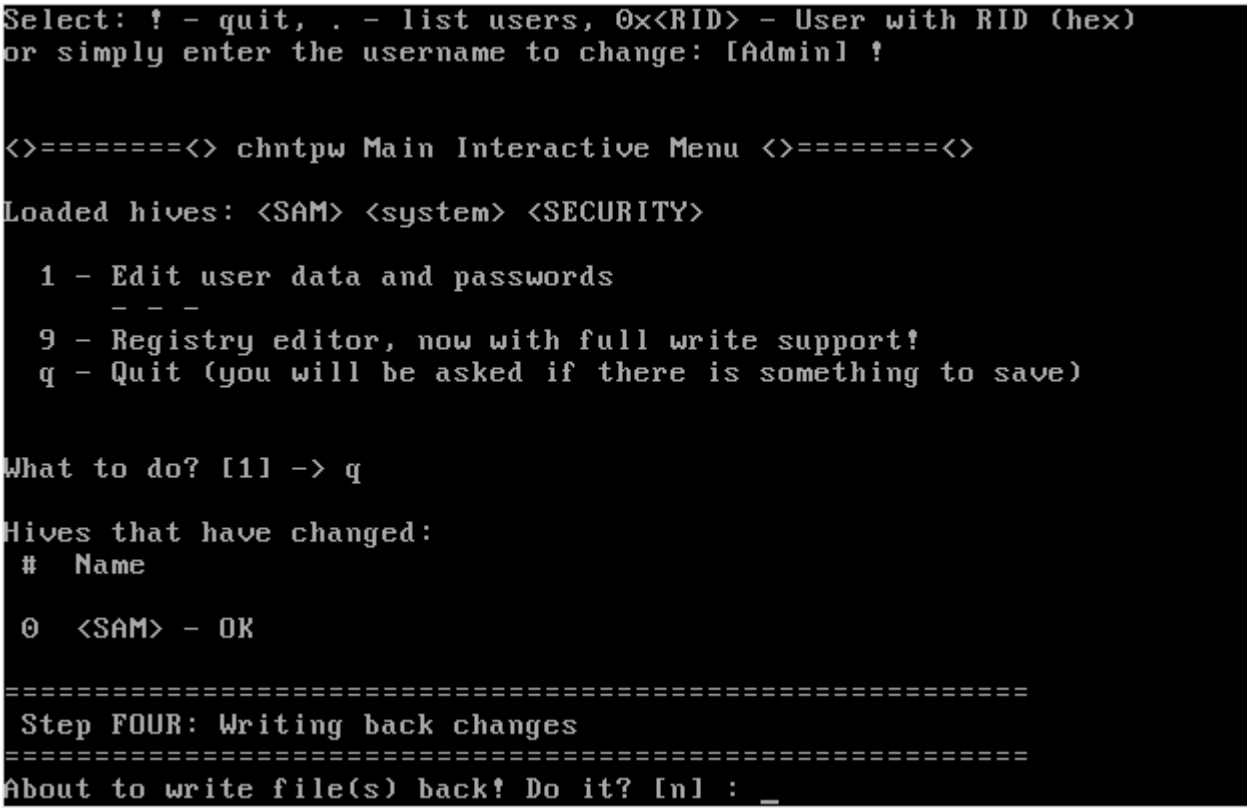
```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] > 1
Password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



- 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.