

Zapomniałeś hasła logowania do Twojego konta w systemie Windows XP !? Dzięki programowi "[Offline NT Password & Registry Editor](#)", możesz łatwo temu zaradzić . Operacja usunięcia hasła jest banalnie prosta i praktycznie ogranicza się do ciągłego "naciskania" klawisza ENTER . A więc zacznijmy od początku:

Musimy pobrać ze strony <http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html> program w wersji bootowalnej do wypalenia na CD bądź wgrania na dyskietkę.

[bd050303.zip](#) - w przypadku wersji dla FDD po rozpakowaniu otrzymamy 3 pliki :

bd040116.bin
install.bat
rawrite2.exe

Uruchamiamy "install.bat" , naszym oczom ukaże się napis "Enter target diskette drive" gdzie poniżej wpisujemy literę napędu dyskietki np: "A:" . Wkładamy czystą dyskietkę do napędu i zatwierdzamy [Enter] i dyskietka gotowa.

Ustawiamy w BIOS'ie aby system bootowany był z dyskietki FDD .

Teraz pozostało nam zaledwie 11 kroków aby pozbyć się hasła .

Krok 1

Wybieramy dysk na którym jest zainstalowany nasz system Windows XP . W naszym przypadku (partycja C:) wybieramy numer "1" [ENTER]

```
=====
. Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/ide/host0/bus0/target0/lun0/disk
dev/ide/host0/bus0/target1/lun0/disk NT partitions found:
 1 : /dev/ide/host0/bus0/target1/lun0/part1 19092MB Boot
 2 : /dev/ide/host0/bus0/target1/lun0/part1 47198MB Boot
 3 : /dev/ide/host0/bus0/target1/lun0/part2 10043MB

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1]
```

Krok 2

Ustawiamy ścieżkę dostępu do folderu w którym znajduje się plik "sam" i "security", tutaj najlepiej zostawić ustawienia domyślne [ENTER].

```
Selected 1
Mounting on /dev/ide/host0/bus0/target0/lun0/part1
NTFS volume version 3.1.
Filesystem is: NTFS

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

Krok 3

Chcemy usunąć hasło a więc wybieramy opcje "1" [ENTER]

```
-r----- 1 0 0 262144 Jan 12 18:01 SAM
-r----- 1 0 0 262144 Jan 12 18:01 SECURITY
-r----- 1 0 0 262144 Jan 12 18:01 default
-r----- 1 0 0 8912896 Jan 12 18:01 software
-r----- 1 0 0 2359296 Jan 12 18:01 system
dr-x----- 1 0 0 4096 Sep 8 11:37 systemprofile
-r----- 1 0 0 262144 Sep 8 11:53 userdiff

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] :
```

Krok 4

Kolejnym krokiem jest ponowne wciśnięcie [ENTER], gdyż mamy zamiar zmienić dane użytkownika i hasło.

```
=====
. Step THREE: Password or registry edit
=====
chntpw version 0.99.2 040105, (c) Petter N Hagen

[.. jakieś informacje o pliku ..]

* 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
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] -> 1
```

Krok 5

Wybieramy użytkownika którego hasła mamy zamiar się pozbyć . Może być to hasło Administratora (domyślnie wybrany) bądź innego. W naszym przypadku był to "mass" , wówczas należy wpisać jego ID w postaci : 0xRID tj. 0x03eb . Jeśli przy jakimś użytkowniku widnieje napis "*disabled or locked*", to oznacza iż dany osobnik nie ma hasła bądź jego konto jest zablokowane. I znów [ENTER]

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

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <ASPNET>, *disabled or locked*
RID: 03e8, Username: <Pomocnik>, *disabled or locked*
RID: 03eb, Username: <mass>
RID: 03ec, Username: <SUPPORT_388945a0>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] 0x03eb
```

Krok 6

Po wybraniu użytkownika, przechodzimy do zmiany hasła. Najpewniejszą metodą jest **jego kasacja**, gdyż zmiana hasła na inne czasem nie odnosi skutku. Dlatego w "Please enter new password" wpisujemy poprostu gwiazdkę "*" [ENTER].

```
RID      : 1003 [03eb]
Username: mass
fullname:
comment  :
homedir  :

Account bits: 0x0210 =
[ ] Disabled           | [ ] Homedir req.      | [ ] 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: 486

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *

Please enter new password: *
Blanking password!
```

Krok 7

Potwierdzamy chęć zmiany [ENTER]

```
Do you really wish to change it? (y/n) [n] y
Changed!
```

Krok 8

Wychodzimy z tego menu wyboru czyli "!" i [ENTER]

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

Krok 9

Tu kolejny raz opuszczamy menu : "q" i [ENTER]

```
<>=====<> 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] -> q
```

Krok 10

Teraz najważniejsze, gdyż zostały nam wyświetlone zmiany jakich dokonaliśmy, więc należy wpisać "y" i zatwierdzić [ENTER]

```
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
```

Krok 11

Jeśli chcemy coś poprawić bądź zmienić hasło kolejnego użytkownika to tutaj mamy taką możliwość. Jeśli jednak nasz cel został osiągnięty wówczas wpisujemy "n" i kolejny raz [ENTER]

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

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

Teraz już tylko pozostała nam przyjemność :-)) a więc wyciągamy dyskietkę i CTRL+ALT+DEL . Po ponownym uruchomieniu systemu zgłosi się CHKDSK , który sprawdzi ustawienia systemu . Po skończonym skanowaniu nastąpi ponowne uruchomienie komputera . I tym oto sposobem pozbyliśmy się hasła. Proste co !? :P