

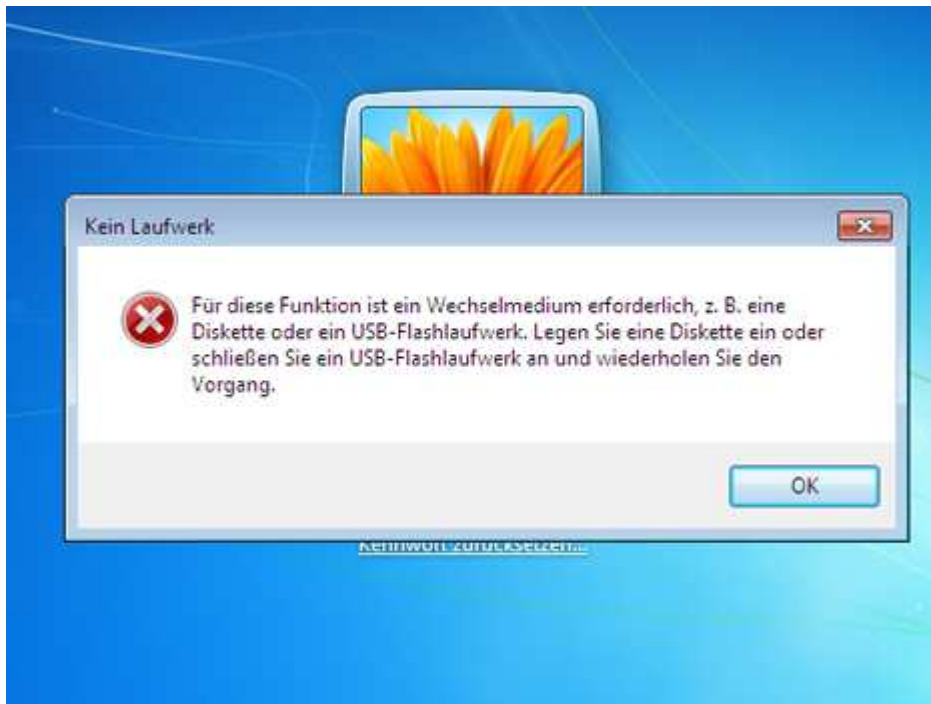
Windows Passwort knacken



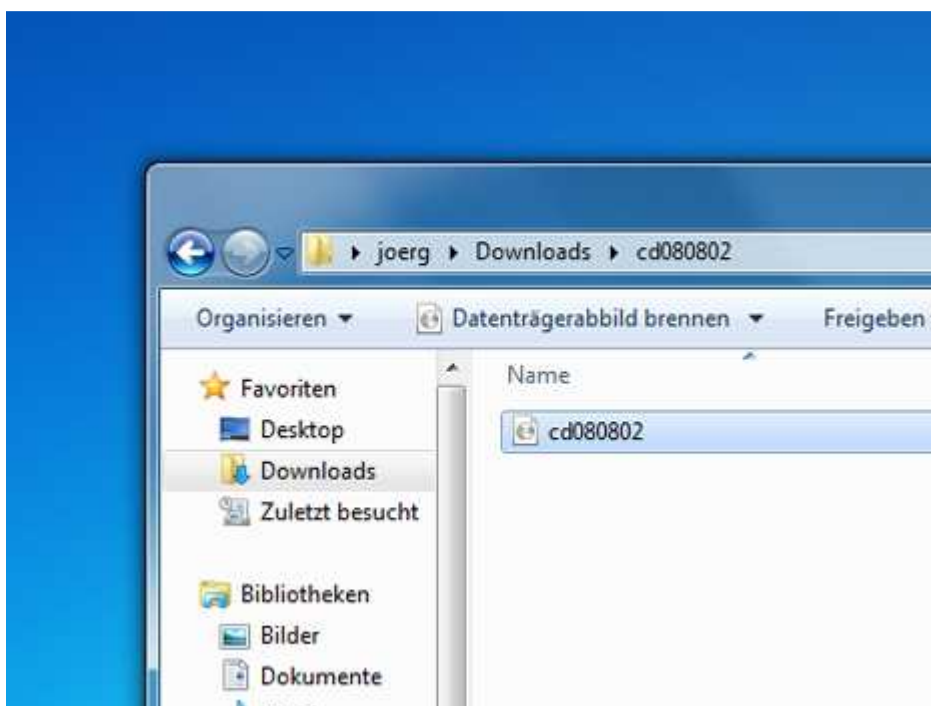
Wer sich am System anmeldet, braucht das richtige Passwort.



Windows verweigert den Zugang bei Eingabe des falschen Passworts. Nutzer sind dann ausgesperrt und kommen nicht mehr an ihre Daten.



Windows bietet die Möglichkeit, das Passwort zurückzusetzen. Damit das aber funktioniert, müssen Sie vorher ein Notfallmedium angelegt haben. Die meisten Nutzer machen das nicht und stehen dann vor verschlossener Tür.



Mit der Freeware Offline NT Password & Registry Editor können Sie Ihr Windows-Passwort ändern. Laden Sie sich das Tool und brennen Sie sich die enthaltene ISO-Datei auf eine CD.

```

*****
*
* Windows NT/2k/XP/Vista Change Password / Registry Edit
*
* (c) 1998-2008 Petter Nordahl-Hagen. Distributed under
*
* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTY
*             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR
*             DAMAGES CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
* More info at: http://home.eunet.no/~pnordahl/ntpasswd/
* Email       : pnordahl@eunet.no
*
* CD build date: Sat Aug  2 00:59:36 CEST 2008
*****

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

boot:

```

Sie müssen jetzt Ihren Rechner von der gebrannten CD starten. Damit das klappt, muss in der Bootreihenfolge im BIOS das DVD-Laufwerk vor der Windows-Festplatte stehen. Ist das der Fall, sehen Sie diesen schlichten Startbildschirm. Drücken Sie auf [ENTER].

```

- 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: 21.4 GB, 21474836480 bytes

Candidate Windows partitions found:
 1 :          /dev/sda1    100MB BOOT
 2 :          /dev/sda2   20378MB

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_

```

Das verwendete Tool basiert auf Linux, deshalb sehen Sie immer wieder auch ein paar Kernel-Meldungen. Im ersten Schritt prüft das Tool Ihre Festplatte und listet die vorhandenen Partitionen auf. Wichtig: Im Bild sehen Sie wie das bei einer Windows-7-Installation aussieht. Es wird eine Bootpartition und die eigentliche Windows-Partition angezeigt. Wählen Sie in diesem Fall [2] aus. Bei einer einzelnen XP-Installation müssen Sie dagegen [1] auswählen.

```

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]

Selected 1

Mounting from /dev/sda1, 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
=====
What is the path to the registry directory? (relative to win
[windows/system32/config] :

```

Jetzt müssen Sie das Tool mit dem richtigen Pfad zur Registry führen. Das ist deshalb nötig, weil dort die Hashwerte des Passworts liegen. Genau dort manipuliert unser Passwort-Knacker das Windows-System. Ziel ist es nämlich nicht, das alte Passwort herauszufinden, sondern ein neues Passwort zu setzen. Der angezeigte Pfad stimmt in den meisten Fällen, sodass es ausreicht, mit [ENTER] zu bestätigen. Klappt das nicht, dann probieren Sie WINNT\System32\Config.

```

EXPAND Windows/System32/config
-rwxrwxrwx  2 0 0 28672 Jun 25 09:36 BCD-
-rwxrwxrwx  2 0 0 19398656 Jun 25 09:05 COME
-rwxrwxrwx  2 0 0 65536 Jun 25 09:05 COME
-11de-8bed-001e0bcd1824}.TM.blf
-rwxrwxrwx  2 0 0 524288 Jun 25 09:05 COME
-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.reg
-rwxrwxrwx  2 0 0 524288 Jul 14 2009 COME
-11de-8bed-001e0bcd1824}.TMContainer00000000000000000002.reg
-rwxrwxrwx  1 0 0 262144 Jun 25 09:05 DEFA
drwxrwxrwx  1 0 0 0 Jul 14 2009 Jour
drwxrwxrwx  1 0 0 0 Jun 25 08:37 RegE
-rwxrwxrwx  1 0 0 262144 Jun 25 09:05 SAM
-rwxrwxrwx  1 0 0 262144 Jun 25 09:05 SECU
-rwxrwxrwx  1 0 0 23330816 Jun 25 09:05 SOFT
-rwxrwxrwx  1 0 0 9437184 Jun 25 09:05 SYST
drwxrwxrwx  1 0 0 4096 Jun 25 08:41 TxR
drwxrwxrwx  1 0 0 4096 Jun 25 08:37 syst

Select which part of registry to load, use predefined choice
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : _

```

Wählen Sie [1], denn Sie wollen das Passwort zurücksetzen.

```

ROOT KEY at offset: 0x001020 * Subkey indexing type is: 6660
Page at 0x6000 is not 'hbin', assuming file contains garbage
File size 262144 [40000] bytes, containing 5 pages (+ 1 head
Used for data: 341/16368 blocks/bytes, unused: 8/3952 blocks

* 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] -> _

```

Wieder ist [1] die richtige Option für das Ändern des Passworts.

```

=====<> chntpw Main Interactive Menu <>=====<>

Loaded hives: <SAM> <SYSTEM> <SECURITY>

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

What to do? [1] ->

== chntpw Edit User Info & Passwords ==

RID |----- Username -----| Admin? | Lock? --|
f4 | Administrator             | ADMIN | dis/lock |
f5 | Gast                       |      | dis/lock |
lea | HomeGroupUser$            |      |          |
e9 | joerg                     | ADMIN | dis/lock |

act: ! - quit, . - list users, 0x<RID> - User with RID (hex)
Simply enter the username to change: [Administrator] joerg_

```

Sie müssen jetzt noch den richtigen Benutzer auswählen. Das Tool listet alle angelegten Nutzer des Systems auf. "Administrator" ist Standard, wir wählen in diesem Beispiel den Benutzer "joerg".

```

Username: joerg
fullname:
comment:
homedir:

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

Account bits: 0x0214 =
[ ] Disabled           ; [ ] Homedir req.       ; [X] Passwd not
[ ] Temp. duplicate   ; [X] Normal account  ; [ ] NMS account
[ ] Domain trust ac  ; [ ] Wks trust act.  ; [ ] Srv trust a
[X] Pwd don't expir  ; [ ] Auto lockout   ; [ ] (unknown 0x
[ ] (unknown 0x10)   ; [ ] (unknown 0x20) ; [ ] (unknown 0x

Failed login count: 2, while max tries is: 0
Total login count: 1

- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > 1_

```

Bei den Tests von CHIP Online zeigte sich, dass es am sichersten ist, wenn man das Passwort löscht. Die Option [1] klappte immer. Beim Neusetzen des Passworts gibt es Unterschiede je nach Windows- und NTFS-Version. Das klappte bei uns im Test mit Windows XP ganz gut, unter Windows 7 jedoch nicht.

```

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

Account bits: 0x0214 =
[ ] Disabled           ; [ ] Homedir req.       ; [X] Passwd not
[ ] Temp. duplicate   ; [X] Normal account  ; [ ] NMS account
[ ] Domain trust ac  ; [ ] Wks trust act.  ; [ ] Srv trust a
[X] Pwd don't expir  ; [ ] Auto lockout   ; [ ] (unknown 0x
[ ] (unknown 0x10)   ; [ ] (unknown 0x20) ; [ ] (unknown 0x

Failed login count: 2, while max tries is: 0
Total login count: 1

- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

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

```

Das war es auch schon, jetzt können Sie mit "!" den Dialog verlassen.

```

1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

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

<>=====<> chmtpw 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] -> q_

```

Via "q" können Sie das Tool verlassen.

```

or simply enter the username to change: [Administrator] !

<>=====<> chmtpw 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] -> q

Hives that have changed:
# Name
0 <SAM> - OK

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

```

Etwas unglücklich kommt erst ganz zum Schluss der Speichern-Dialog. Jetzt müssen Sie ungedingt [z] eingeben. Der Grund: Beim amerikanischen Tastatur-Layout sind "y" und "z" vertauscht, sodass beim Druck auf [z] ein "y" im Fenster erscheint. Damit bestätigen Sie, dass Sie die gemachten Änderungen abspeichern wollen.



Beenden Sie das Tool, entfernen Sie die CD und starten Sie den Rechner neu. Gibt es nur einen Benutzer auf dem PC, dann wird dieser automatisch angemeldet. Bei mehreren Nutzern müssen Sie Ihr Konto noch auf dem Willkommensbildschirm anklicken. Setzen Sie jetzt unbedingt in der Benutzerverwaltung ein neues Passwort und merken Sie es sich. Falls Sie es wieder vergessen, gehen Sie zurück zu Bild 5.