

Bypassing Windows Passwords with chntpw



CHNTPW is a utility to reset the password of any local user on the Windows system. Supports all Windows from NT 3.5 to Win 10 and Win 11 including 64 Bit operating systems.

It is the best utility to quickly reset Windows authentication passwords



Attacks

Attack -1

- You have physical access to a system which is **password locked**. The tool can be used to quickly remove the password

Attack -2

- You have physical access to a system which uses online account for authentication. The tool can be used to **enable local administrator account** which will allow access to the system



Where are Windows Passwords Stored

Windows stores its user information, including encrypted versions of the passwords, in a file called 'SAM', usually found in **\windows\system32\config**

CHNTPW utility manipulates the file in an interactive manner to clear the passwords

Step- 1

- ❖ Download the USB version of the utility from the official website

<https://pogostick.net/~pnh/ntpasswd/>

Download

Note: Some links may be offsite.

CD release, see below on how to use

- [cd140201.zip](#) (~18MB) - Bootable CD image. (md5sum: f274127bf8be9a7ed48b563fd951ae9e)
- [usb140201.zip](#) (~18MB) - Files for USB install (md5sum: a60dbb91016d93ec5f11e64650394afb)

Previous release:

- [cd110511.zip](#) (~4MB) - Bootable CD image. (md5sum: fe0d30a1c540ec6757e748c7c09e2e4f)
- [usb110511.zip](#) (~4MB) - Files for USB install (md5sum: 50ced8d2a5febe22199f99acec74e63b)

The files inside the USB zip are exactly the same as on the CD. See below for instructions on how to make USB disk bootable.

Floppy release (not updated anymore), see below on how to use them

- [bd080526.zip](#) (~1.4M) - Bootdisk image (md5sum: 37889e4c540504e59132bdcdfe7f9bb7)
- [drivers1-080526.zip](#) (~310K) - Disk drivers (mostly PATA/SATA) (md5sum: 72ac1731c6ba735d0ac2746a30dbc3ee)
- [drivers2-080526.zip](#) (~1.2M) - Disk drivers (mostly SCSI) (md5sum: 30172bec657c85a5f1a0b43601452fb7)

Step- 2

- ❖ Extract all files and copy the files to a USB drive

Ensure that the USB is formatted and there is no important data on it

PC > NEW VOLUME (F:)

| Name | Date modified | Type | Size |
|--------------|-------------------|----------------------|-----------|
| boot.msg | 2/1/2014 9:35 PM | Outlook Item | 2 KB |
| initrd.cgz | 2/1/2014 9:35 PM | CGZ File | 1,301 KB |
| isolinux.bin | 2/1/2014 9:35 PM | BIN File | 24 KB |
| isolinux.cfg | 8/27/2013 9:28 PM | Configuration Sou... | 1 KB |
| readme.txt | 2/1/2014 9:34 PM | Text Document | 3 KB |
| scsi.cgz | 2/1/2014 9:35 PM | CGZ File | 13,398 KB |
| syslinux.cfg | 8/27/2013 9:28 PM | Configuration Sou... | 1 KB |
| syslinux.exe | 5/11/2011 9:39 PM | Application | 70 KB |
| vmlinuz | 8/27/2013 6:38 PM | File | 2,366 KB |

Step- 3

- ❖ Run a command prompt on Windows as Administrator and use the following command

```
f:syslinux.exe -ma f:
```

Here :

- f is the drive letter name (change it as per your USB drive letter)

The USB will become bootable without any notification. A file `ldlinux.sys` may appear on the USB drive

Step- 4

- ❖ Now on your PC, press esc or F12 (whatever your system supports and boot from USB



Step- 5

- ❖ Chntpw utility will boot and search for windows installation drive

Type 1 (or whatever your drive is) and press enter

```
=====  
# Step ONE: Select disk partition where the Windows installation is  
=====  
n device bytes    GB    MB == DISK PARTITIONS: =====  
1 sda1 10474348  9  10228  
10228 MB partition sda1 is NTFS. Found windows on: WINDOWS/system32/config  
=====  
--- Possible windows installations found:  
1 sda1          10228MB WINDOWS/system32/config  
Please select partition by number or  
q = quit.  o = go to old disk select system  
d = automatically start disk drivers  
m = manually select disk drivers to load  
f = fetch additional drivers from floppy / usb  
a = show all partitions found (fdisk)  
l = show propbable Windows partitions only  
Select: [1]
```

Step- 6

- ❖ Chntpw utility will ask for which registry file you want to manipulate

Type 1 to select SAM and press enter

```
=====
# Step TWO: Select registry files
=====
-rwxrwxrwx      1 0      0      262144 Sep 15 14:11 SAM
-rwxrwxrwx      1 0      0      262144 Sep 15 14:11 SECURITY
-rwxrwxrwx      1 0      0      229376 Sep 15 14:11 default
-rwxrwxrwx      1 0      0      8912896 Sep 15 14:11 software
-rwxrwxrwx      1 0      0      3670016 Sep 15 14:11 system
drwxrwxrwx      1 0      0      4096 Sep 6 14:08 systemprofile
-rwxrwxrwx      1 0      0      262144 Sep 6 18:56 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam]
2 - RecoveryConsole parameters [software]
3 - Load almost all of it, for regedit tec [system software sam security]
q - quit - return to previous
[1]
```

Step- 7

- ❖ Now we need to select the option to edit user accounts

Type 1 and press enter

```
=====
■ Step THREE: Password or registry edit
=====
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 231/18000 blocks/bytes, unused: 6/2320 blocks/bytes.

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM>

 1 - Edit user data and passwords
 2 - List groups
  - -
 3 - Registry editor, now with full write support!
 4 - Quit (you will be asked if there is something to save)

What to do? [1] ->
```

Step- 8

- ❖ The utility will list all local accounts on the PC.

Type the respective ID of the user account we need to crack

```
==== chntpw Edit User Info & Passwords ====
RID - Username ----- Admin? - Lock? --
01f4 Administrator ADMIN *BLANK*
03eb Ammar ADMIN dis/lock
019c Guest dis/lock
03e8 HelpAssistant dis/lock
03ea SUPPORT_388945a0 dis/lock
Please enter user number (RID) or 0 to exit: [3eb] _
```

Step- 9

- ❖ Now select the option to clear password

Type 1 and press enter

```
- - - - User Edit Menu:  
1 - Clear (blank) user password  
2 - Unlock and enable user account [probably locked now]  
3 - Promote user (make user an administrator)  
4 - Add user to a group  
5 - Remove user from a group  
q - Quit editing user, back to user select  
Select: [q] >
```

Step- 10

- ❖ Now press quit and once it asks whether you want to save changes type Y and press enter

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

- ❖ Now reboot your system and your password will be removed



DEMO



THANKS