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

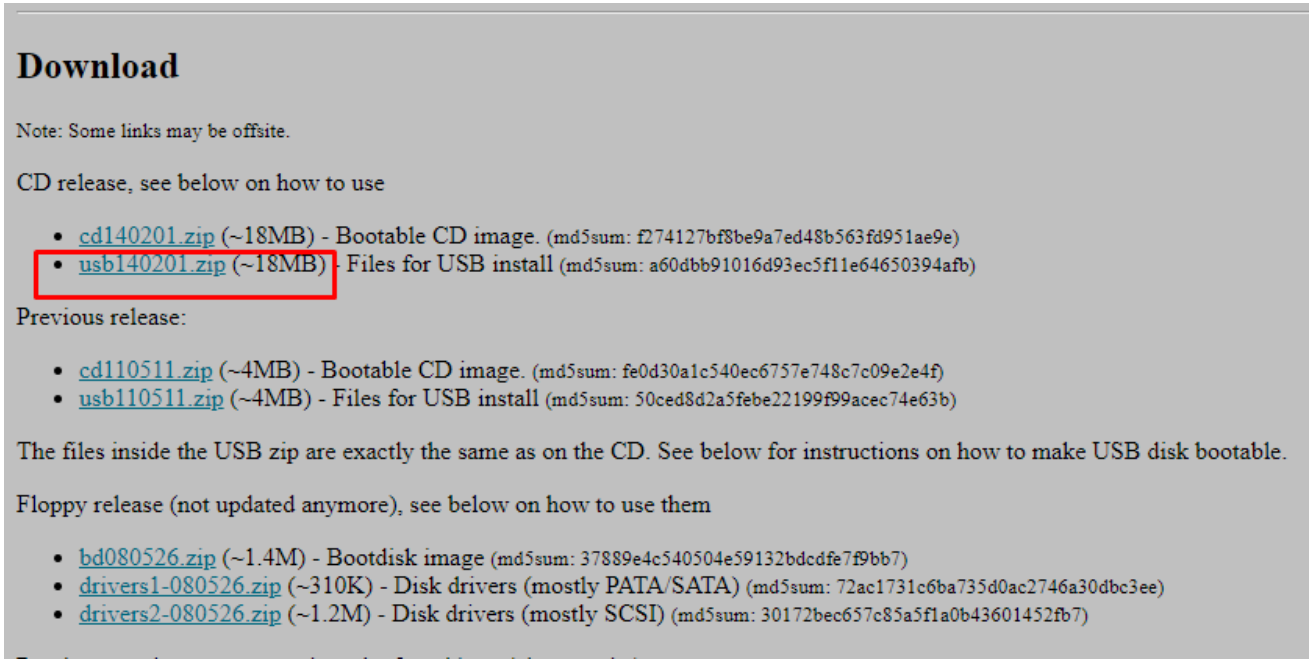
Windows stores its user information, including encrypted versions of the passwords, in a file called ‘SAM', usually found in \windows\system32\config

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.

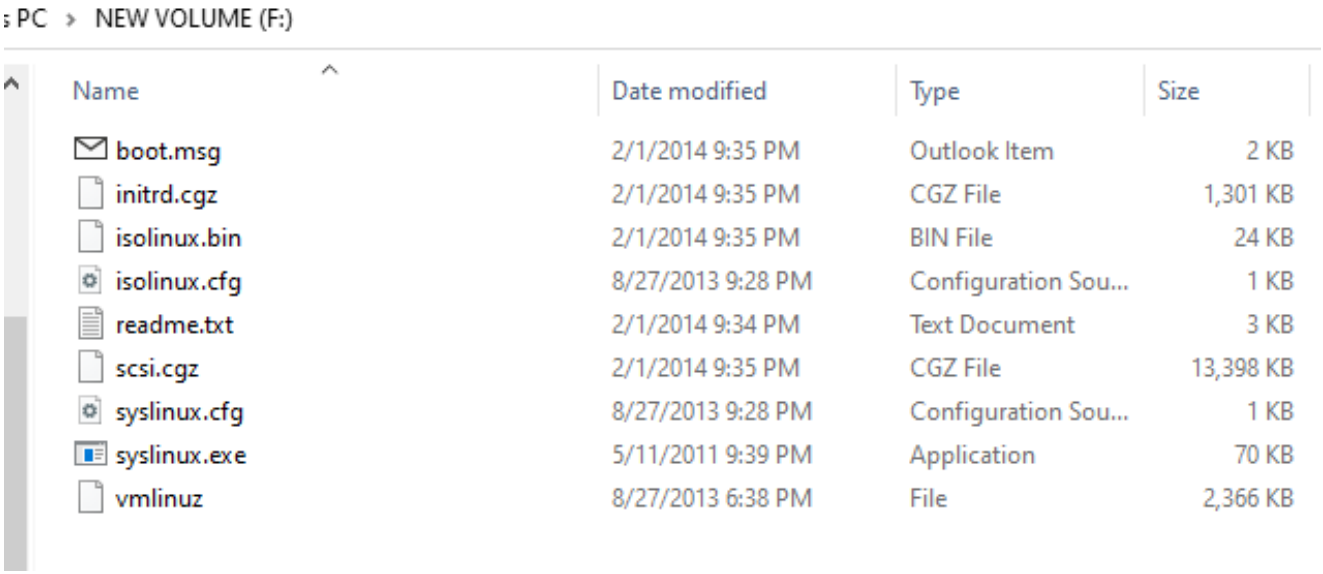
Floppy release (not updated anymore), see below on how to use them

- 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



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

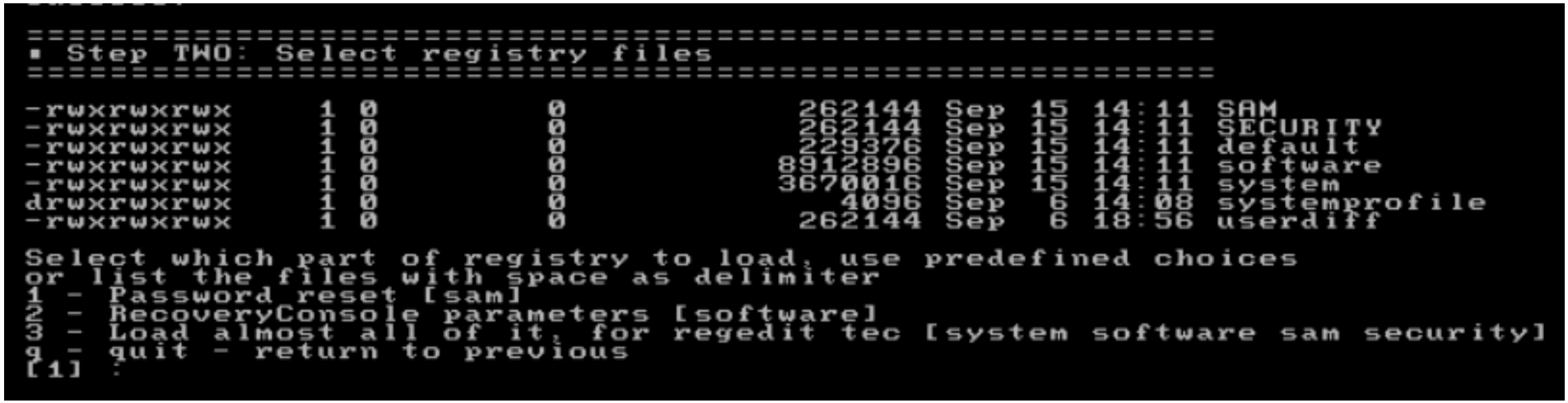
- Chntpw utility will boot and search for windows installation drive

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

Step- 6

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

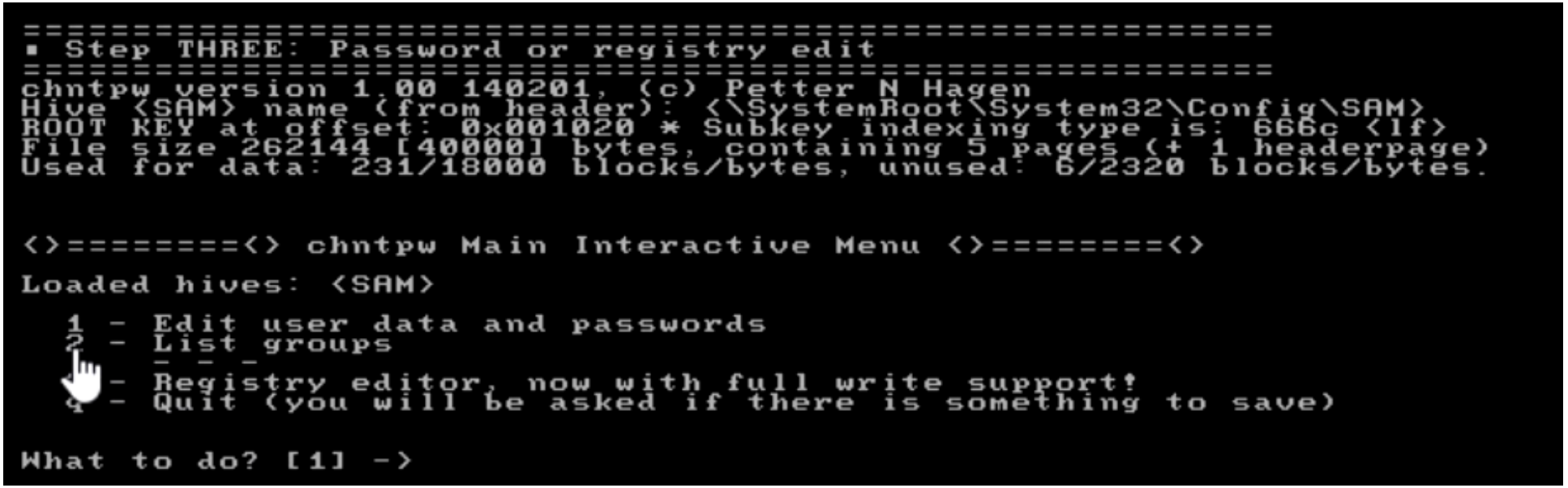
Type 1 to select SAM and press enter



Step- 7

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

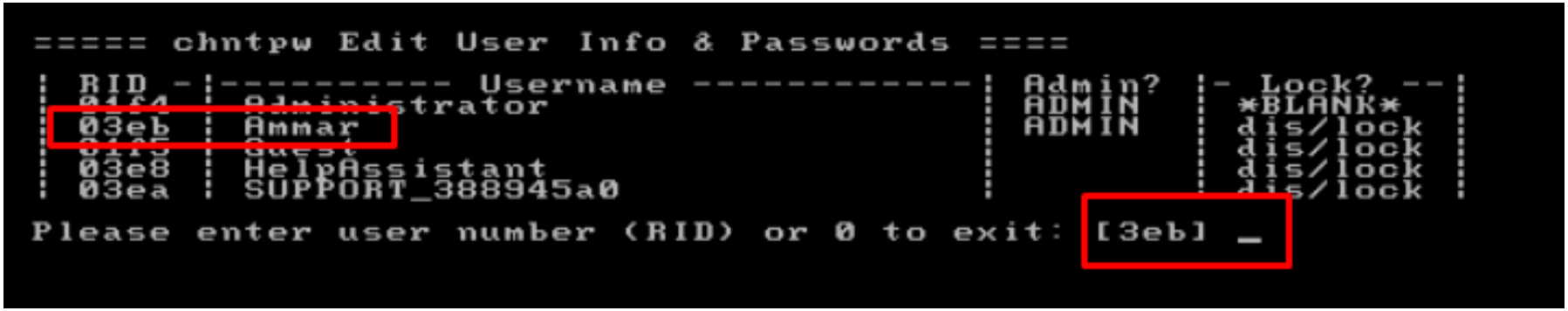
Type 1 and press enter



Step- 8

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

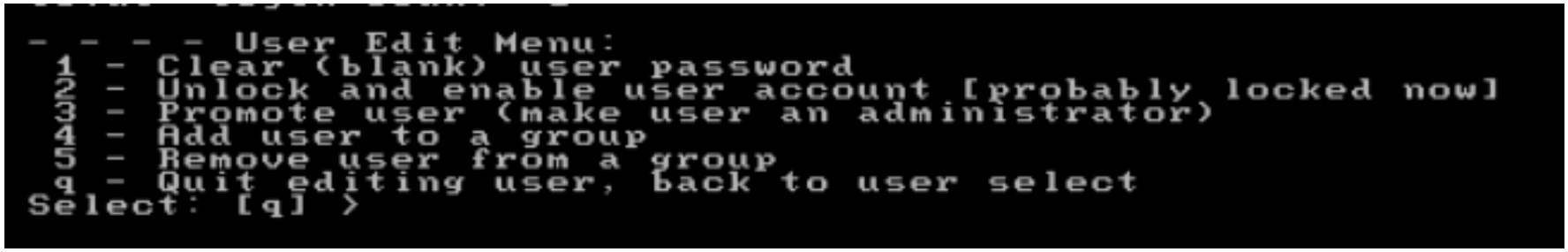
Type the respective ID of the user account we need to crack



Step- 9

- Now select the option to clear password

Type 1 and press enter



Step- 10

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

- Now reboot your system and your password will be removed

DEMO

THANKS