Bypass Windows online authentication by activating a local **Administrator Account**

Attack Scenorio

- You have physical access to a system which is **password locked (online email password)**. We are going to use our Kali Live boot USB to activate a local administrator user to gain access to the system

We need to have Kali Live boot USB

(Check the lecture “Kali Linux as a bootable USB Drive”)

Step- 1

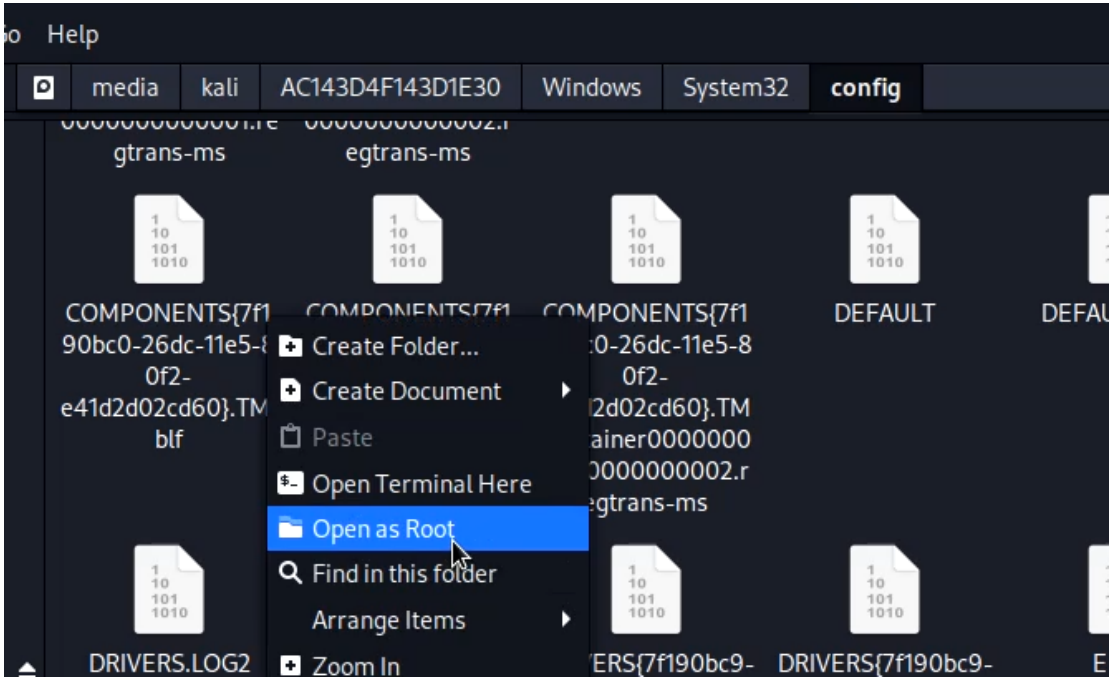
- Plug in the Kali Live USB on your target PC and boot from it

Use Esc or F12 (whatever your system supports and boot from USB

Step- 2

- Once Kali is booted, Open the drive containing Windows files

Navigate to Windows/system32/config, Open it as root



Step- 3

- Open a terminal and run the following command

```
Chntpw –i  SAM
```

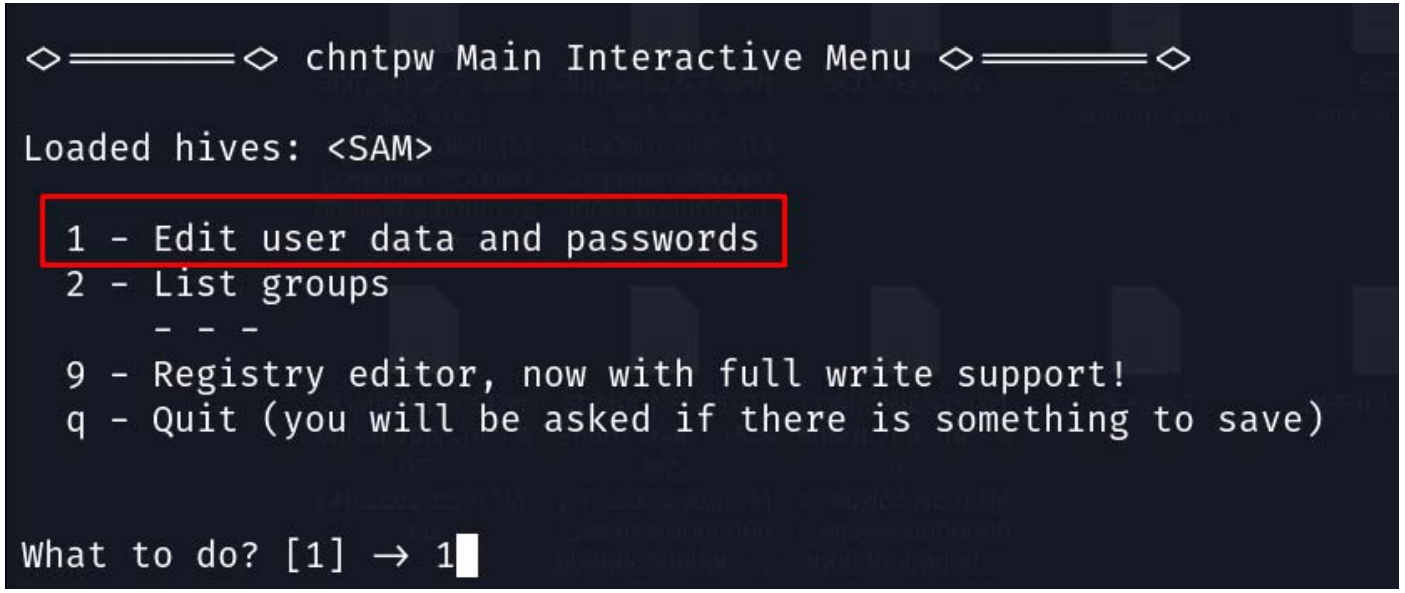
Here :

- -i opens the chntpw utility in interactive mode
- SAM contains the passwords of all users on Windows

Step- 4

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

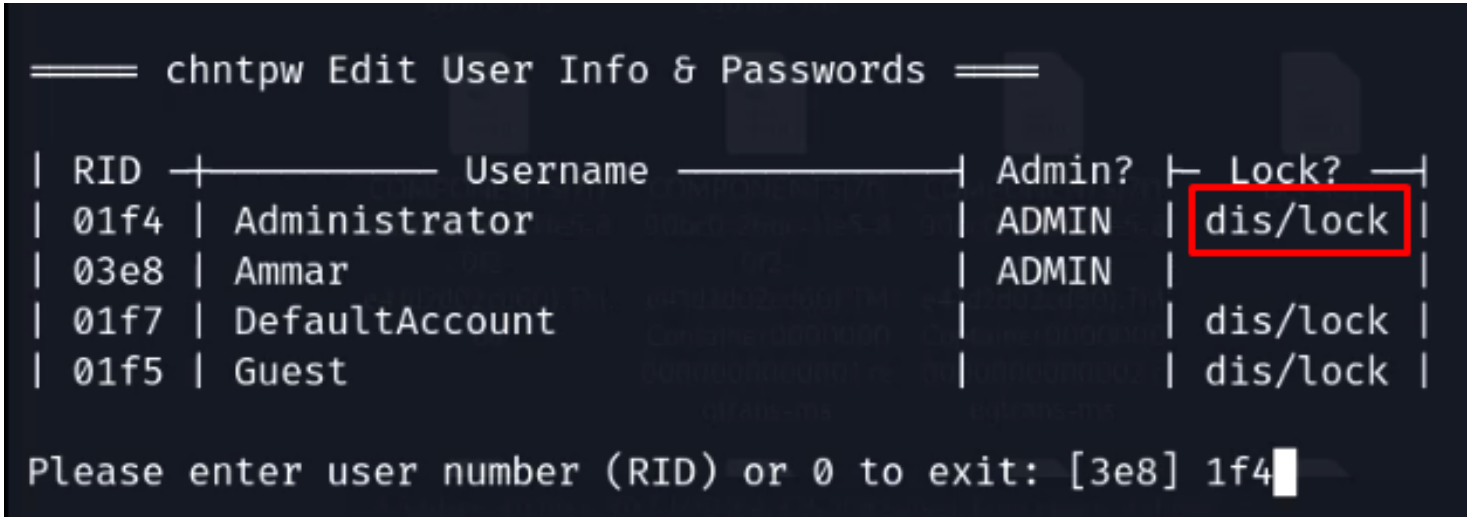
Type 1 and press enter



Step- 5

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

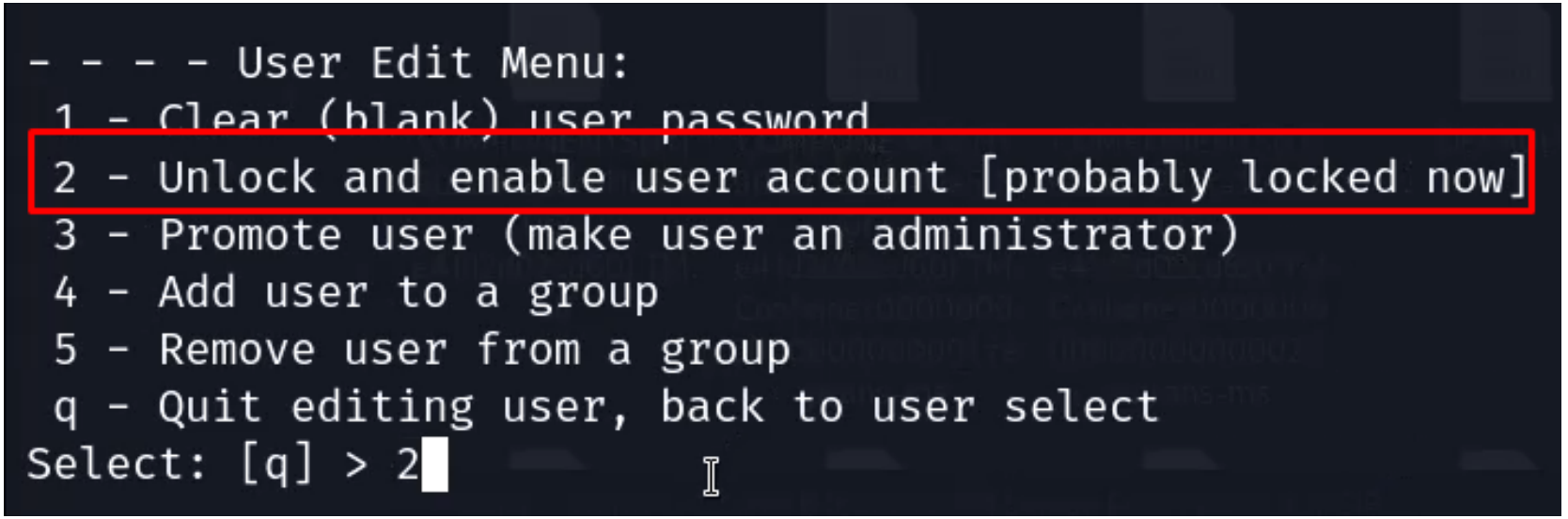
Type the ID of the administrator account we need to unlock



Step- 6

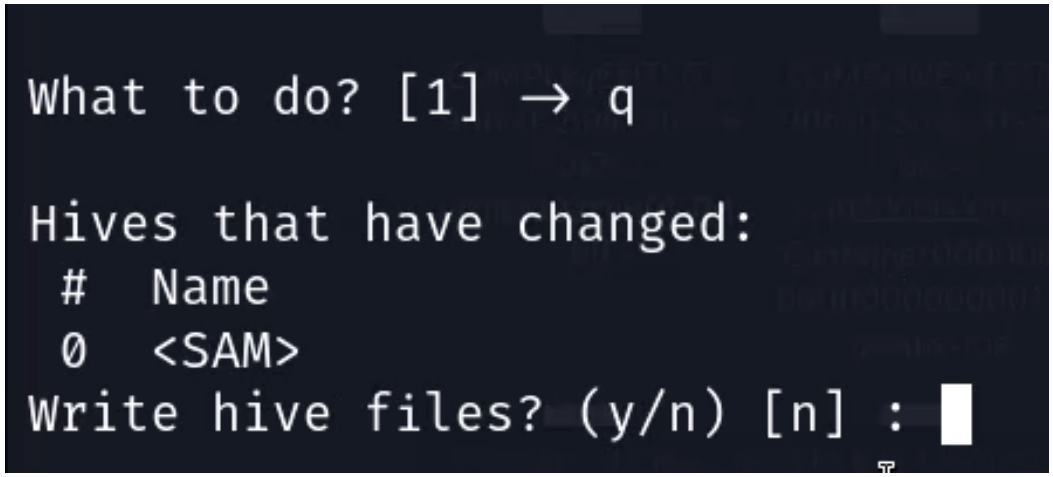
- Now choose the option to unlock and enable user

Type 2 and press enter



Step- 7

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



Step- 8

- Remove the USB drive, reboot your system to Windows and an administrator account will appear with a blank password

DEMO

THANKS