In this practice we are going to learn how to remove the password from a local account on a Windows machine.

Daniel Sánchez Fernández – 04/05/2023

Reset Password Win

Implantación de Sistemas Operativos

Contents

[Materials needed: 2](#_Toc134118284)

[Operation: 2](#_Toc134118285)

[Machine creations 2](#_Toc134118286)

[Start the Ubuntu LiveCD 3](#_Toc134118287)

[Operations with “chntpw” 4](#_Toc134118288)

[Installing "chntpw” 4](#_Toc134118289)

[Password erasing with "chntpw". 4](#_Toc134118290)

[Checking the access to the Windows account 5](#_Toc134118291)

[Changing the password 5](#_Toc134118292)

[Access as administrator 6](#_Toc134118293)

[Legal Disclaimer 7](#_Toc134118294)

[Conclusion 7](#_Toc134118295)

[Copyright 7](#_Toc134118296)

[Social networks 7](#_Toc134118297)

[Webgraphy 7](#_Toc134118298)

# Materials needed:

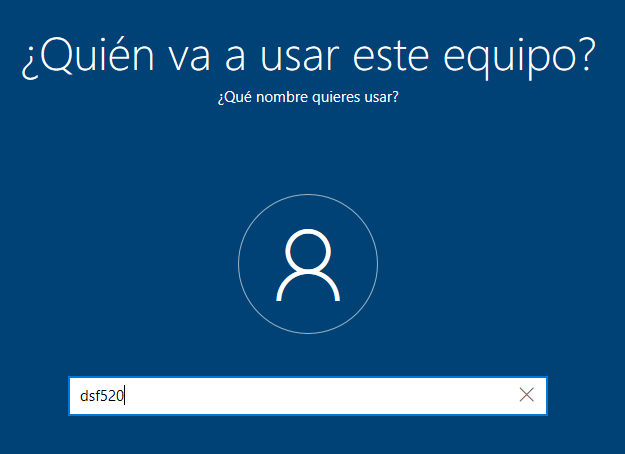
* For this practice we will need:
  + A Windows system with a local account whose administrator account name we know but not its password.
  + An Ubuntu LiveCD (Ubuntu ISO)

# Operation:

* We create the Windows machine and its account whose password we do not know.
* We create a virtual machine to start the LiveCD:
  + This machine will not have any disk of its own since it will use the Windows machine's disk.
* We will manage (install) the "**chntpw**" package on the LiveCD
* Log in to the account and delete your password
* Test that we can access the account inside Windows and confirm that we have administrator permissions.

# Machine creations

* The first thing to do will be to start the Windows machine and create the new user account:
* I will make a local account whose name I know (dfs520), but it is not necessary that we know its password (I have let a colleague set the password so that I don't know it).



I know the account

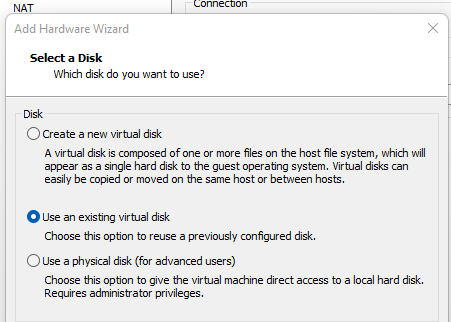
But not the password



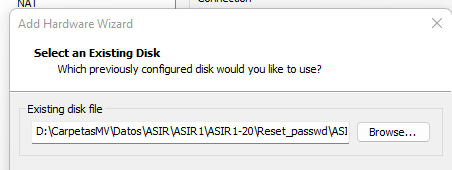
* To remove the password, we must completely shut down the computer.

## Start the Ubuntu LiveCD

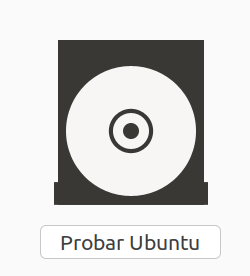
* We are now going to create a new Ubuntu virtual machine which we will access using a "LiveCD" (i.e. Ubuntu without installation) and the Windows machine disk.



During the creation of the machine. It will appear to select a disk. We click on "Use an existing virtual disk" and then we look for the virtual disk of the Windows machine and we assign it to it.

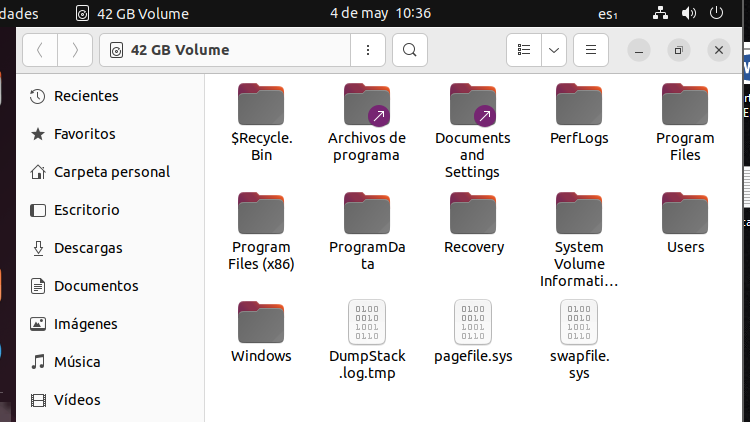


* Now we just put the Ubuntu desktop ISO and start the virtual machine



Once in the "try or install Ubuntu" section, select "try" (to access as LiveCD).

* If we have set the Windows disk correctly, we will be able to access its files and directories from the Ubuntu File Explorer



Here is all the information contained by the virtual disk on the Windows machine

* Once we confirm the access to the disk, we can start to clean the password

# Operations with “chntpw”

## Installing "chntpw”

* In order to use "chntpw", we must first download and install it.
* This package is not found in any official repository, so we must add a repository or allow the download of packages from third-party repositories
* Add "universe" repository

We add your repository and we run an “update.”



* After that, we install "chntpw".



* We will have it installed.

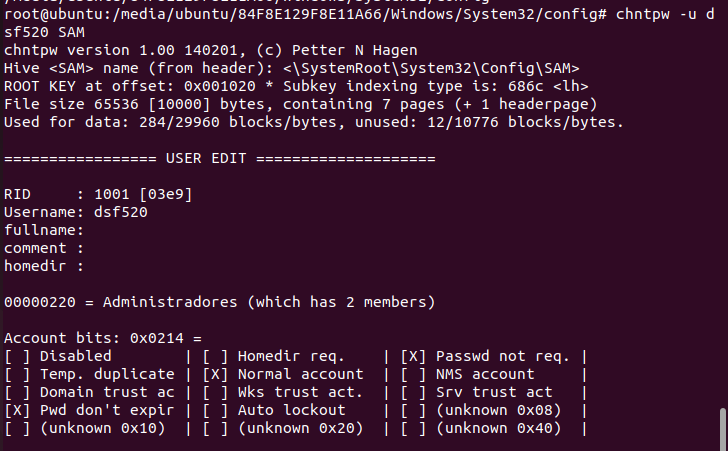
## Password erasing with "chntpw".

* We will have to go to the directory of the Windows disk that we are going to modify. That is, the one that stores the hashes of the local user accounts.

Directory where to execute the command

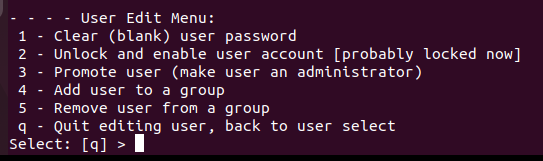


* Once in that directory, run the command "chntpw -u <username> SAM".
  + This command will allow us full access and control of the local account that we have indicated.



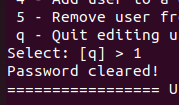
This tab will appear with user information (such as user ID) and other parameters.

* Now we have access to the configuration of the user that we have created before.
* In the console, the option "Clear (blank) user password" appears in the first option (1).



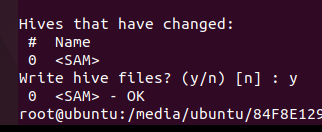
Underneath, a console will appear where we can execute the following options by pressing a specific character:

* When pressing "1" the following message will appear:



We press 1 to clear the user's password and if it succeeds in doing so, we will see "Password cleared!"

* With this we will have cleared the password. Save and exit by pressing "q".
* You will be asked for confirmation, press "y" to confirm.



Save and exit

* With this, the password is now removed

# Checking the access to the Windows account

* We shut down the Ubuntu and open the other machine (Windows).
* In case of having "Secure Boot" activated, it could give us a problem or indicate that the disk has been modified. In the case of my virtual machine, as I do not have Secure Boot enabled, this message has not appeared.



The user is self-represented and does not ask for a password. It directly unlocks it

* We could, for example, assign a password by pressing "Ctrl + alt + delete" and clicking on "change a password".

## Changing the password

* Now that we have taken control of the account, we can change the password by going to the option "Change a password".





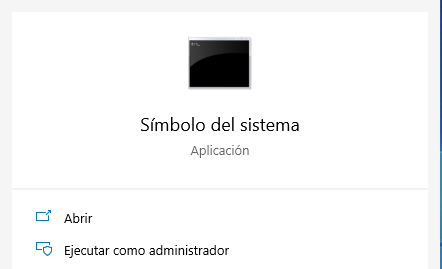
We determine the user we want to change the password, in "Previous password" we leave it empty since he/she does not have a password and we enter his/her new password.



* With this, we would have already set the password of our choice for this device.

## Access as administrator

* Finally, I am going to demonstrate that indeed I have administrator permissions

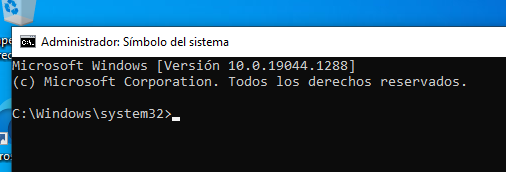


For example, by opening the CMD as administrator



A confirmation UAC will appear

* After accepting it, we access the CMD as administrators



Indeed, we are administrators

* So we have already reset the password and we still have administrator permissions.

# Legal Disclaimer

* This is a practice performed and tested in a lab environment. Doing this to a real disk that we do not own or do not have the explicit permission of the real owner of the disk, constitutes a crime and should not be done at the risk of penalty (both monetary and criminal).

# Conclusion

* In this practice we have learned how to clear the local password of a Windows computer. This practice teaches us that as network administrators, we should always use network accounts (such as those offered by Microsoft) instead of local ones which are more vulnerable. It is also important to use accounts other than the default (As Administrator), since offering cybercriminals one of the two credentials needed to access the system can be the key to being attacked.

# Copyright

* All the practice has been done and tested by me: Daniel Sánchez Fernández - ASIR1-20, with the information provided by the teacher and indicated in the webgraphy of the document.

# Social networks

* LinkedIn
  + <https://www.linkedin.com/in/daniel-s%C3%A1nchez-fern%C3%A1ndez-6b948923a/>

# Webgraphy

<https://askubuntu.com/questions/388612/unable-to-locate-package-chntpw>