Daniel Prieto Rodriguez

Mr. Alfredo Abad04/23

**ResetPasswWIN**

Content

[Objective of practice 2](#_Toc132883648)

[Inventory of required equipment 2](#_Toc132883649)

[Know the user of our Windows 2](#_Toc132883650)

[Insert the Linux CD on the Windows and start working with it without installing 3](#_Toc132883651)

[Installing the CHNTPW 4](#_Toc132883652)  Software Package

[How to reset or change Windows password? 8](#_Toc132883653)

[Final considerations 9](#_Toc132883654)

# Objective of the practice

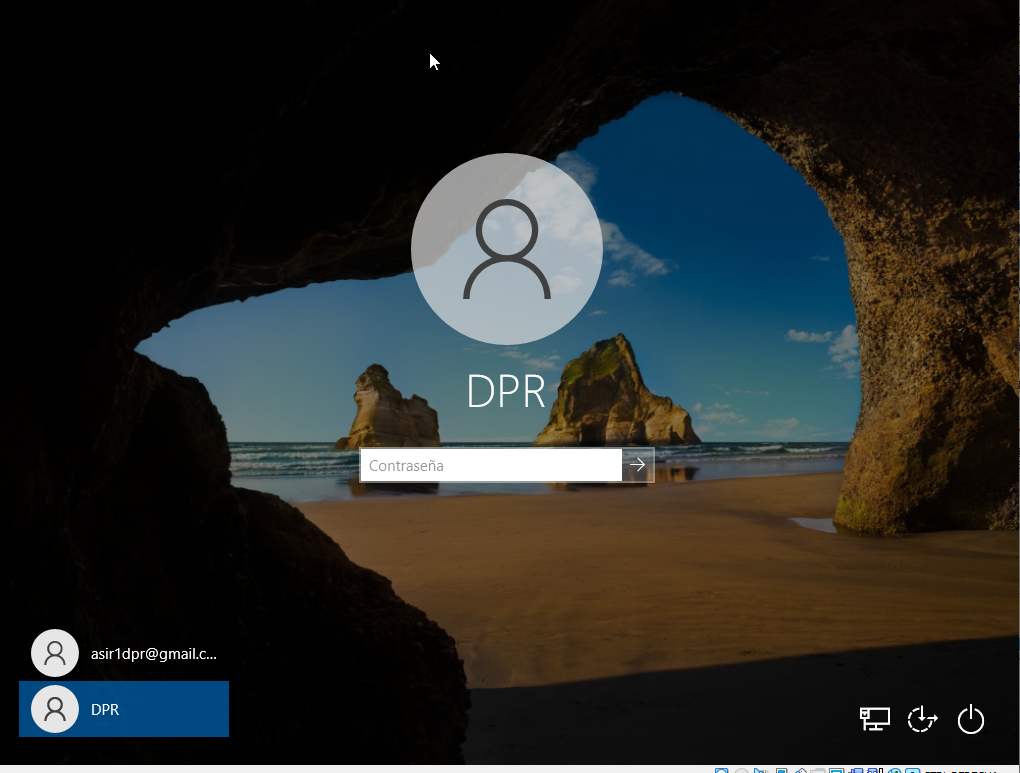
Our goal will be to remove the password to a Windows account from a Linux live/CD so that when we enter that account from Windows then it enters directly.

# Inventory of required equipment

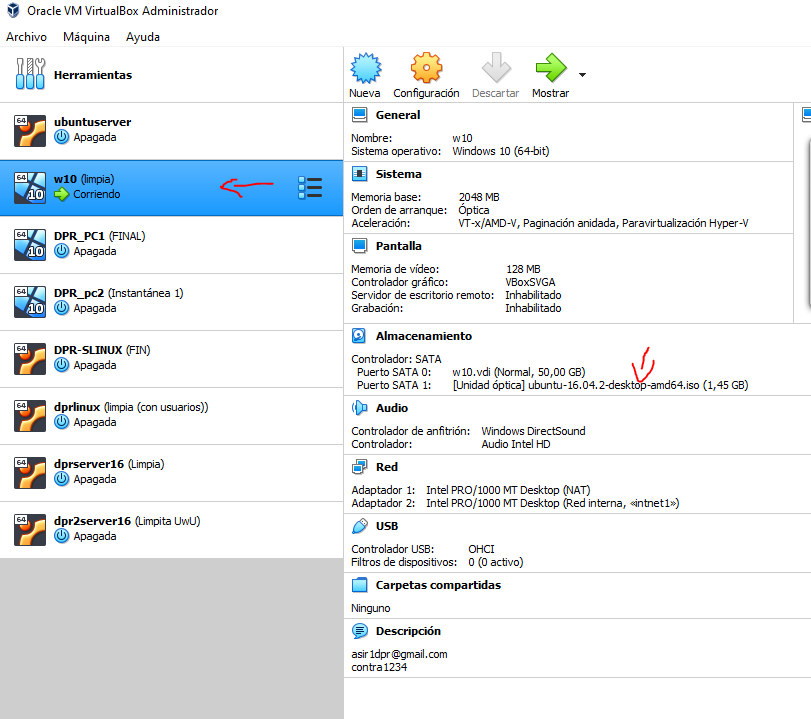
Single Windows machine and Linux live/CD

# Know the user of our Windows

1º we will enter our Windows to know the username with which we will work (The account will have to be administrator)



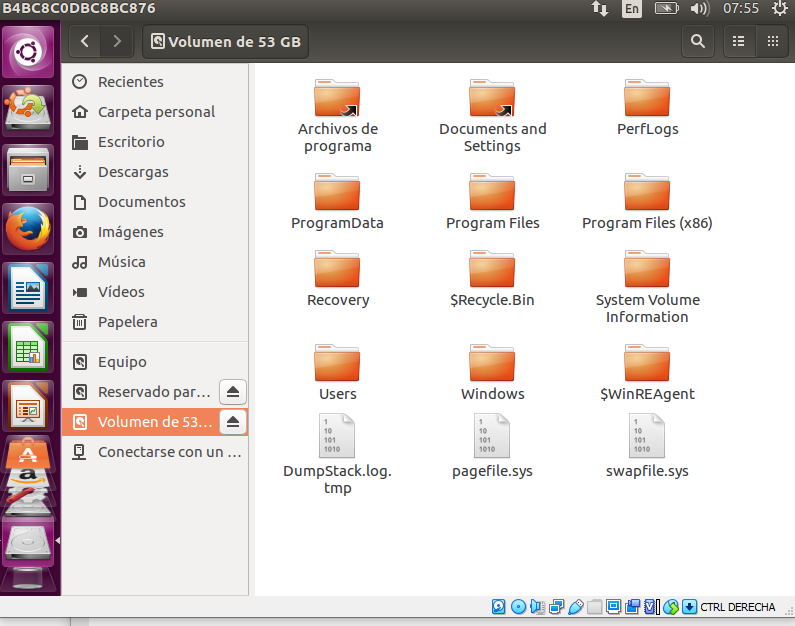
# Insert the Linux CD over the Windows and start working with it without installing



Once started we will give you to "try Ubuntu"

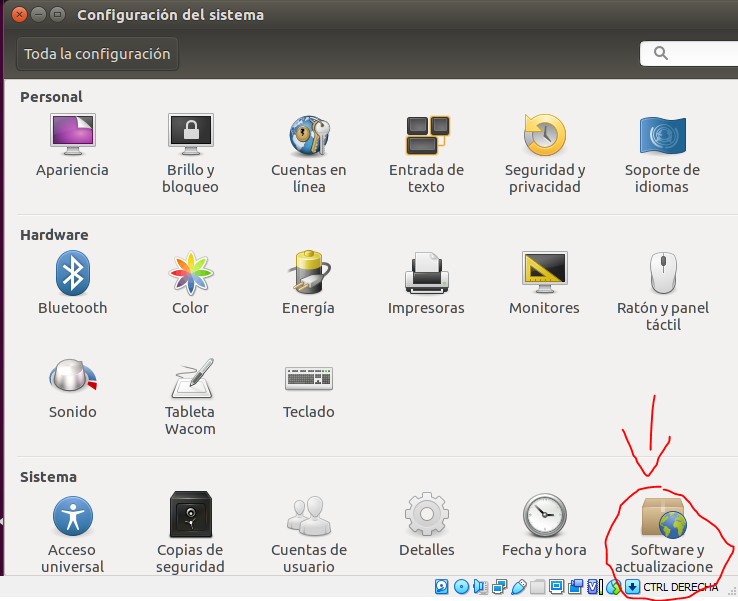


Once inside, we will check that we see the disk with the Windows from the Linux

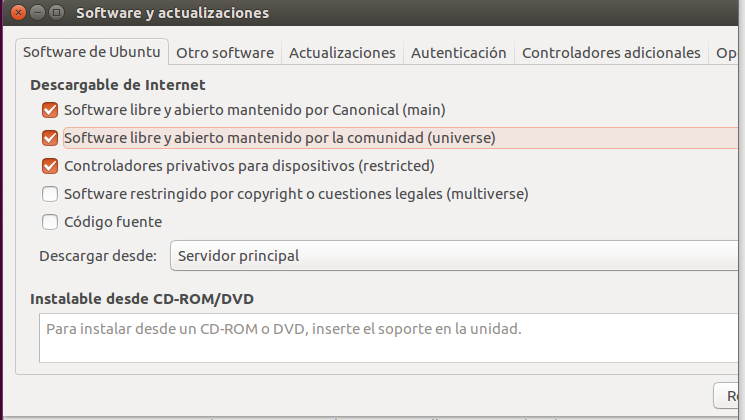


# Installing the CHNTPW Software Package

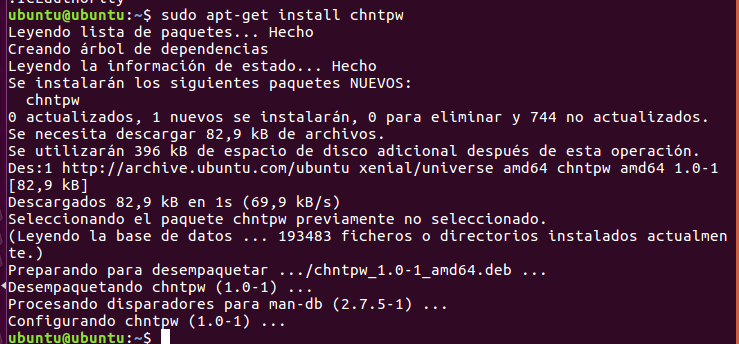
First we will look for the "system configuration" in which we will click the "software and updates"



We will select the second option " **Free and open software maintained by the community (Universe)"** Once selected we will close the window.



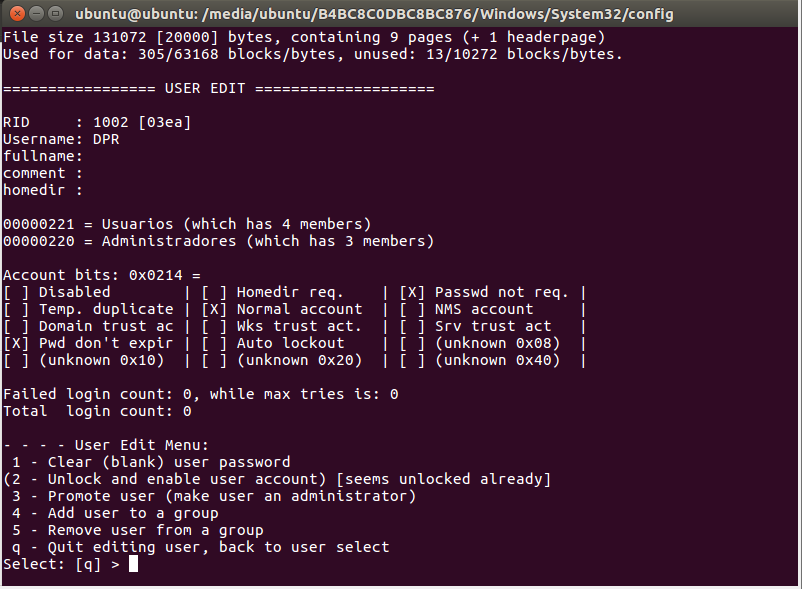
Now, mexºdiante the command line, we will write a "sudo apt-get install chntpw" to download the necessary tools



Now we will move to the Windows directory, to know which is we can look for it through the graphical interface or the command line with the command "mount" and looking for what it is, once we move we can make a "pwd" to see what we have inside



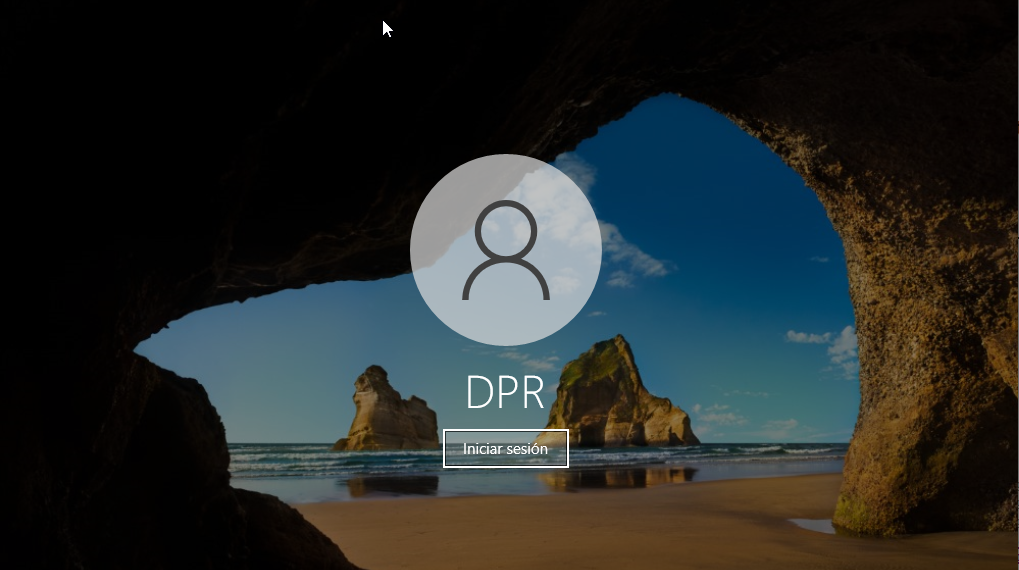
Now we must write the following: " **sudo chntpw -u [username] SAM"** (watch out for the user, with upper and lower case)



Now we will crack the password and we will leave, just at the end where it says "Select: [q] >" we will write "1" in lowercase after "q" and if you ask usto write "y"

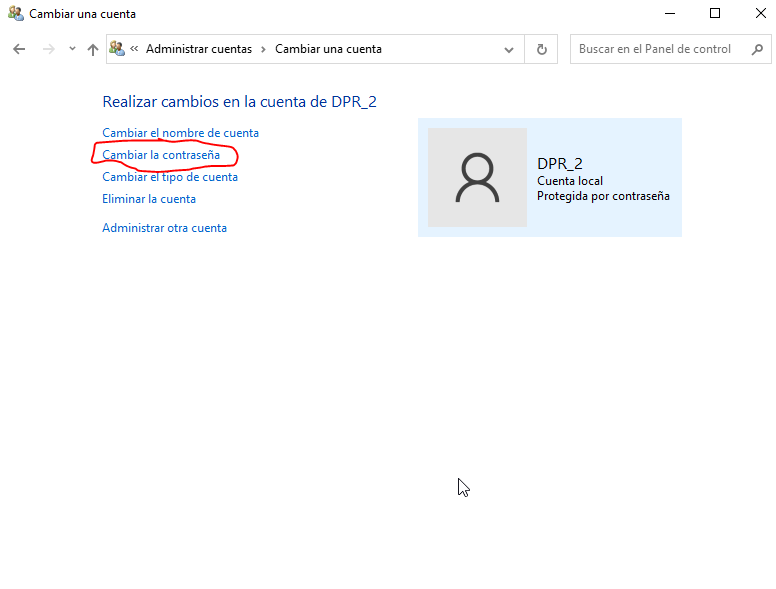


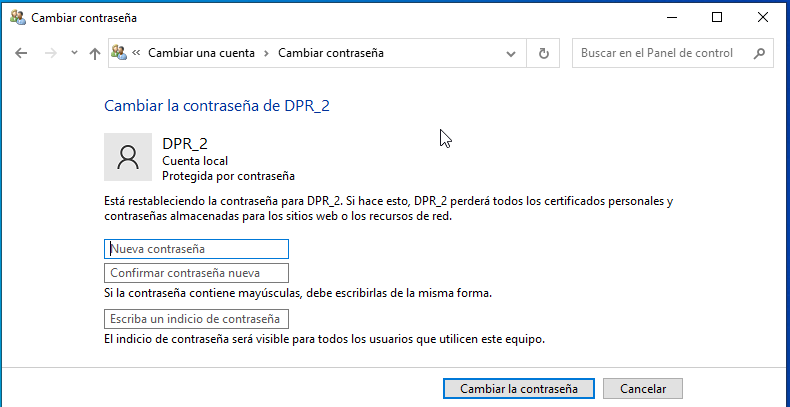
When we finish, we will turn off the system and start it from the disk (We will have to be careful since Windows does not like to touch the disks and will propose a check, we have to omit it) on the contrary, simply start the system we will go to the "DPR" account and check that now it has no password and will enter automatically.



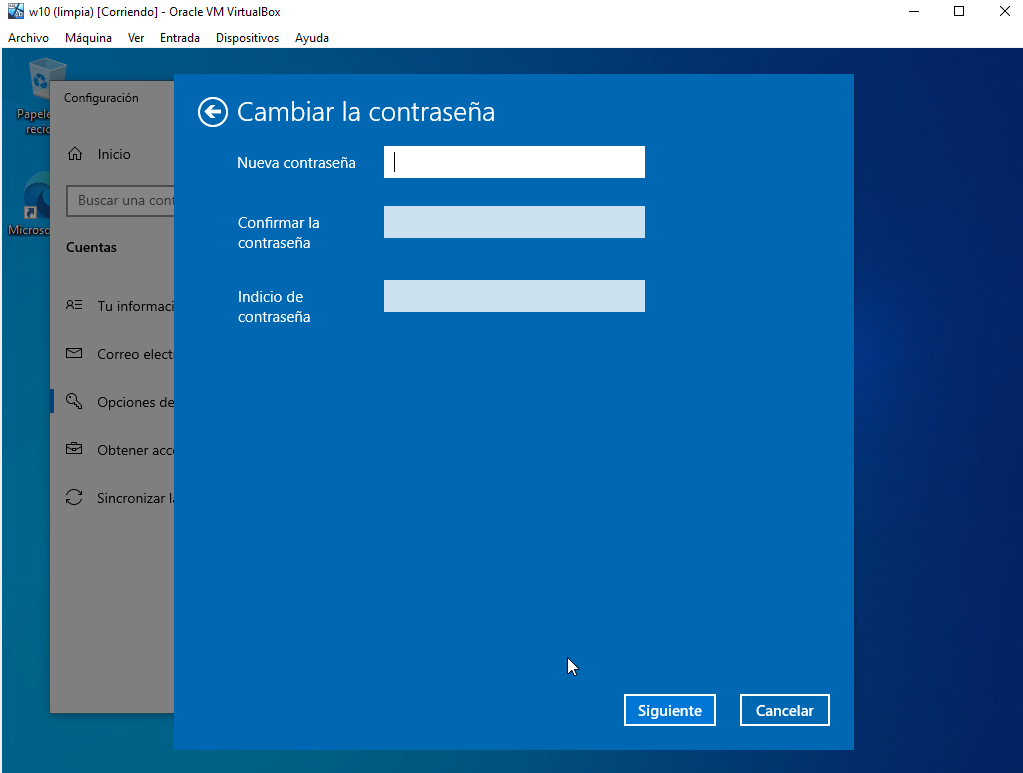
# How to reset or change Windows password?

If we are administrators we can simply open the control panel, search for accounts and users and inside we look for the manage accounts, which we will choose the account of which the user has lost or forgotten his password and we will change it





When the user has the new password we must force him to put his own that we do not know (for security)



# Final considerations

An interesting practice to sensitize us to the issue of computer security and not leave an important team in the hands of anyone.