Práctica de laboratorio

Práctica de reseteo de contraseña en un Windows desde Linux

NOMBRE ALUMNO: Jhon Salazar Varela

ISOP406\_ResetPasswWind-JSVarela-ASIR122.docx

Índice

[Objetivo de la práctica 2](#_Toc99216898)

[Inventario de material necesario 2](#_Toc99216899)

[Ejecución, investigación y desarrollo 3](#_Toc99216900)

[Consideraciones finales y metacognición 11](#_Toc99216901)

# Objetivo de la práctica

En esta práctica se buscará conseguir resetear la contraseña de un Windows desde el sistema operativo contrario de Linux, aprender y empezar a ver las utilidades básicas para llegar a “Hackear” de forma licita un sistema operativo en caso de perder la posibilidad de acceder a el y evitar perder todo lo contenido con una nueva instalación, se aprenderá a usar combinaciones y conexiones desde Ubuntu hasta Windows para llegar a recuperar el acceso.

# Inventario de material necesario

Para esta práctica necesitaremos lo siguiente:

* Un entorno físico donde almacenar la Máquina Virtual
* Entorno de Virtualización (VMware)
* Conectividad a Internet
* Las ISO correspondientes de los SO que vamos a utilizar Windows 10 y Linux, Ubuntu GUI

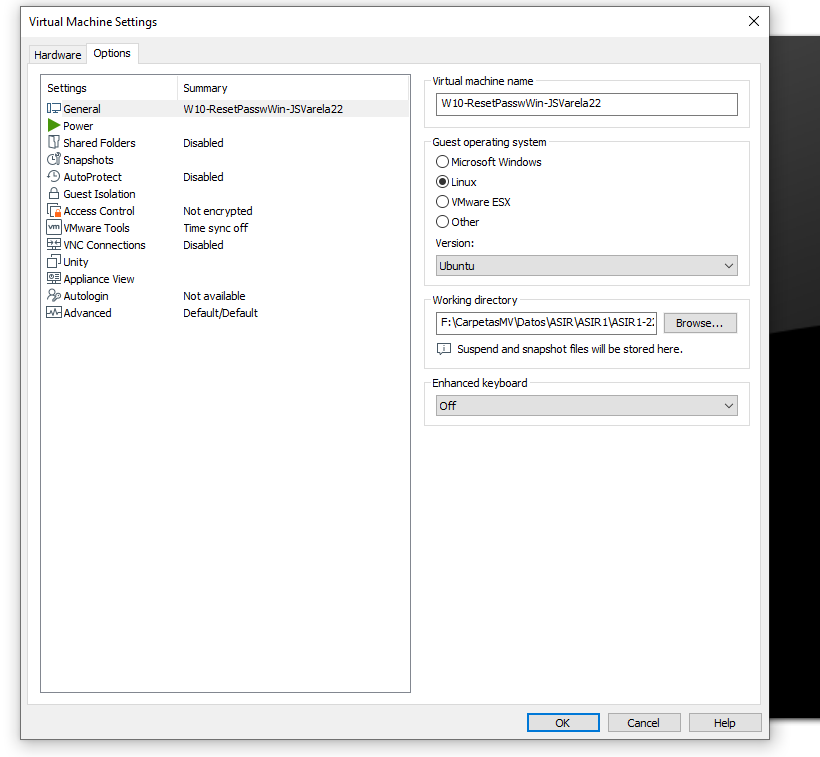
# Ejecución, investigación y desarrollo

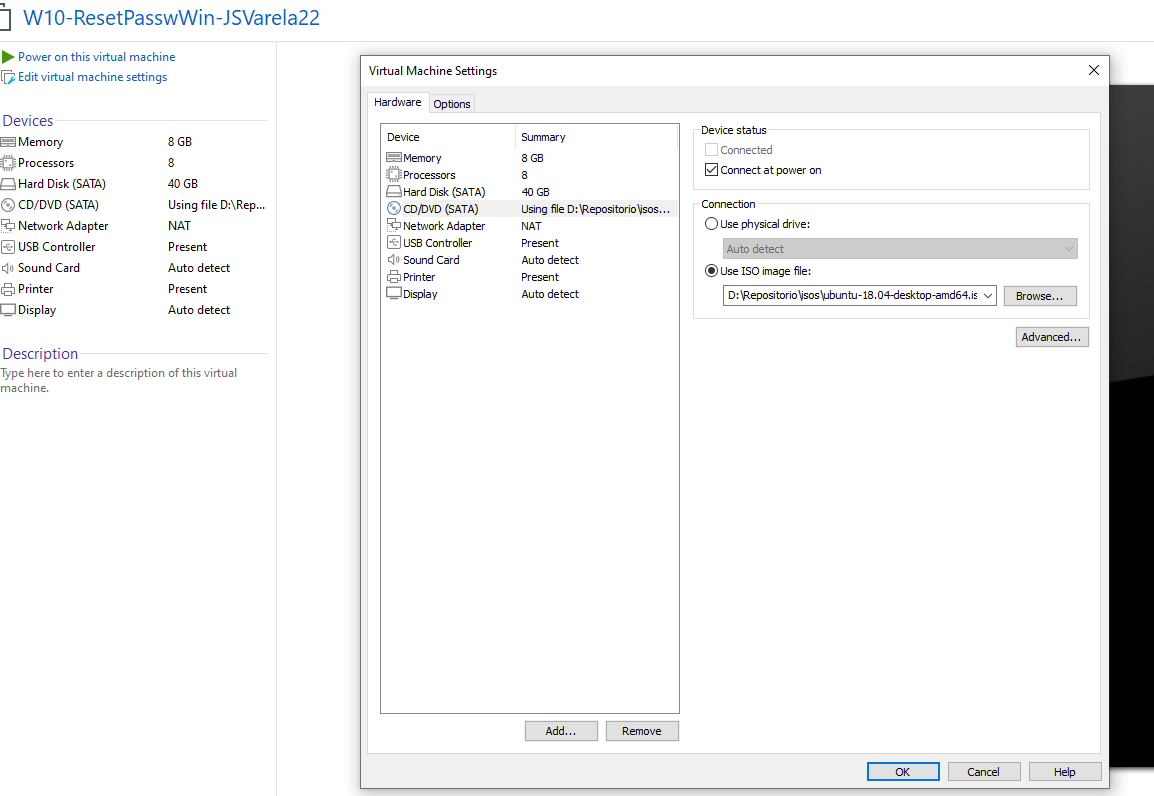
Para dar inicio en a esta practica crearemos o utilizaremos una maquina virtual con un sistema operativo de Windows 10, bastara con que la maquina tenga una sesión de administrador con un nombre que debemos conocer, pero de forma hipotética la contraseña no la sabremos (pues para realizar esta práctica se basara en recuperar el acceso a esta cuenta).

En mi caso estoy utilizando una máquina que ya había utilizado antes para crear diversas cuentas en una practica anterior, por lo que tendré mi propia sesión de administrador mas varias cuentas de prueba creadas con anterioridad.



Seguido de esta primera preparación, tendremos que apagar la maquina y en los ajustes, cambiar el SO (a Linux, Ubuntu GUI) y la configuración para la que está dispuesta la máquina.

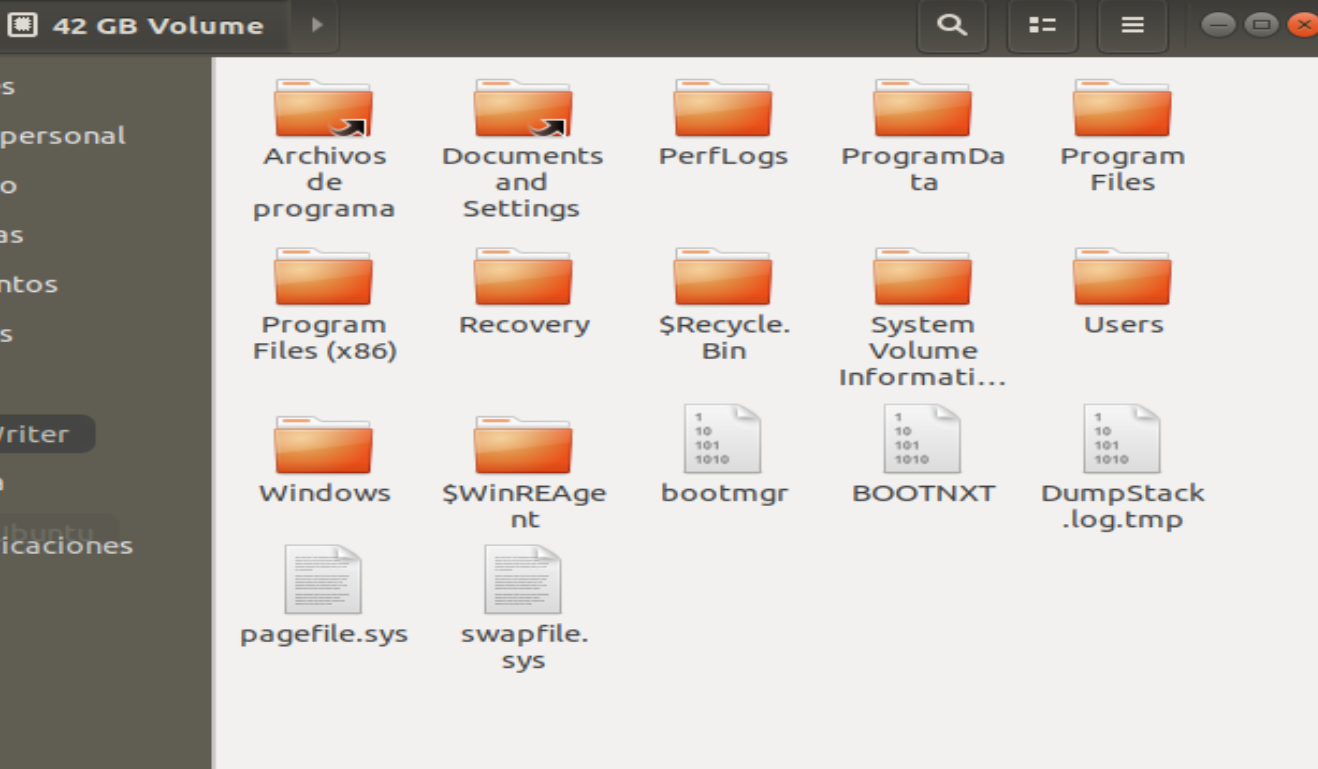


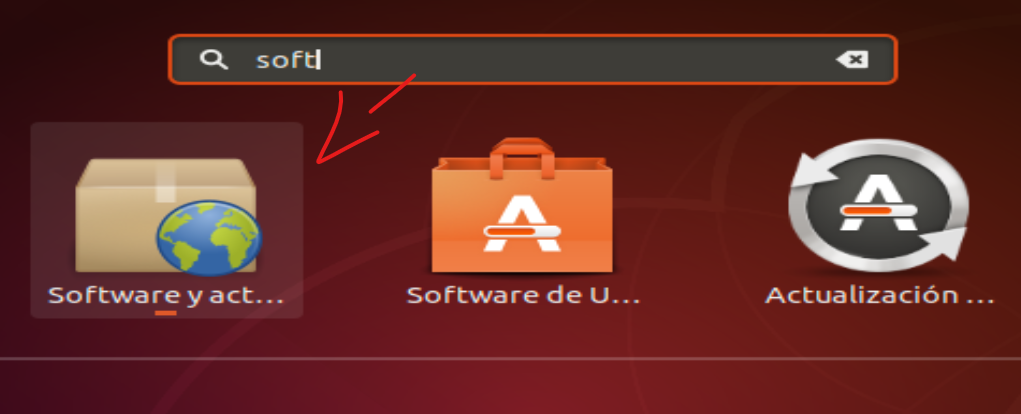


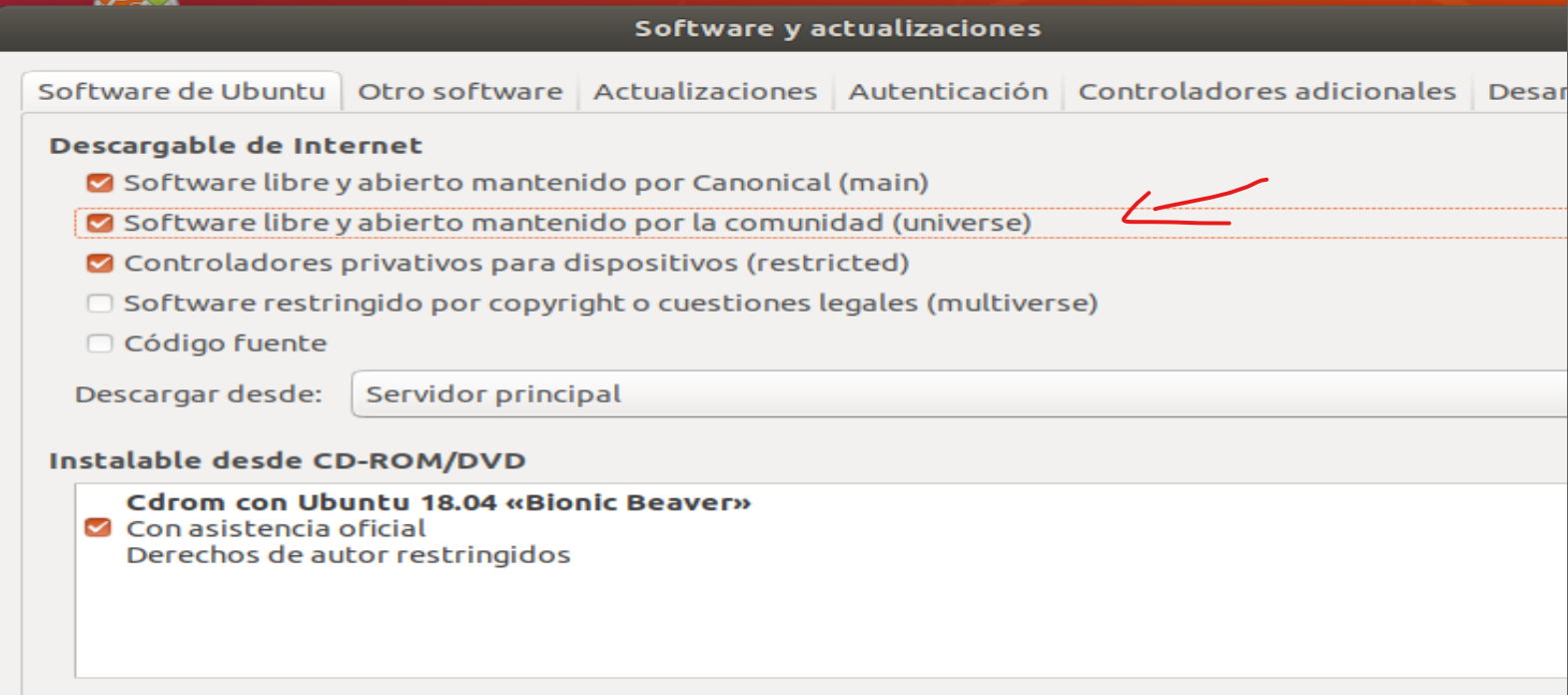
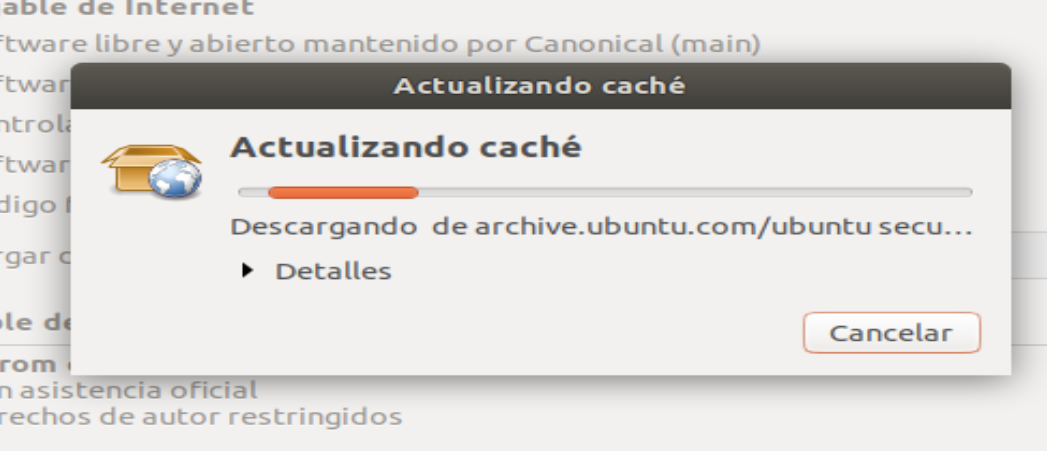
Utilizaremos ahora un inicio de sesión con Ubuntu, pero sin instalarlo, pues solo querremos utilizar el LiveCD con el que configuraremos el disco del Windows, pues como podemos comprobar, el disco de esta maquina ya esta formateado con el SO instalado de Windows, por lo que solo queremos configurar el disco y no instalar otro SO Ubuntu, para esto tendremos que irnos al Firmware y seleccionar la opción de arranque por CD o DVD, que ya sabremos cual es por prácticas anteriores.

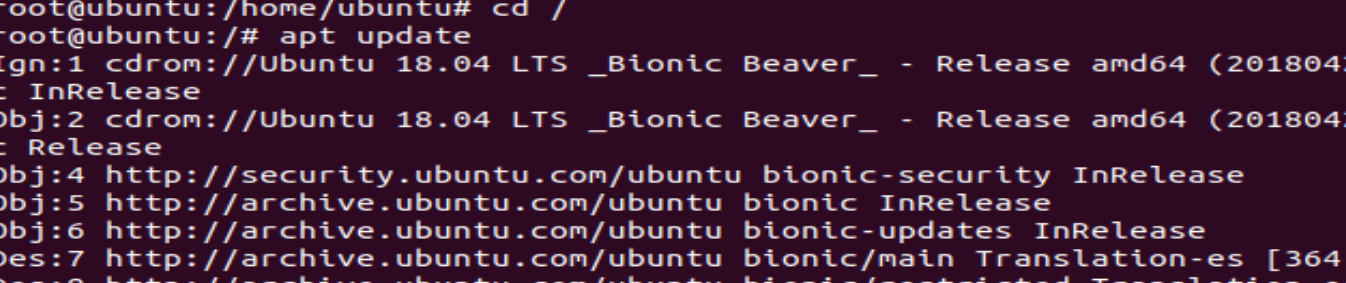
(En caso de que no se recuerdo como acceder al Firmware, tendremos que ir a la opción de power de la barra de superior en la sección VM, y ahí nos aparecerá “power for firmware” le clicaremos y accederemos por medio del Firmware a la maquina)

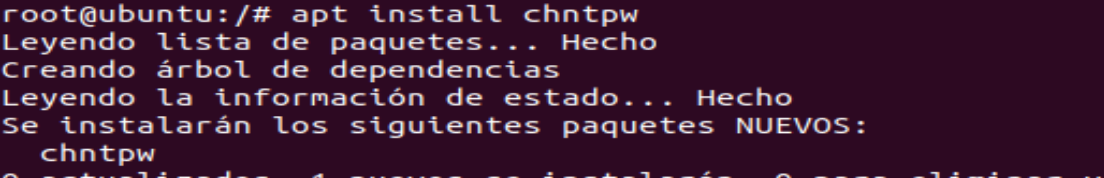
Ya una vez hecho esto, nos aparecerá la ventana que nos preguntará si queremos instalar o probar Ubuntu, a lo cual iremos a probar con LiveCD.

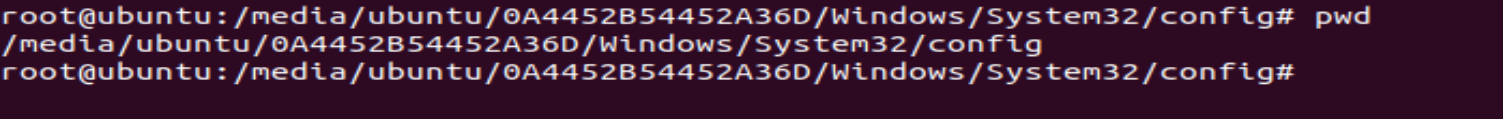
Ya una vez que estemos en la parte de inicio de una Ubuntu LiveCD, deberemos acceder al sistema de archivos grafico para encontrar el disco de Windows, que habrá sido configurado automáticamente por el LiveCD. Una vez lo encontremos nos fijaremos que tiene las carpetas de configuración y la ruta para acceder a estas.

Ahora tendremos que irnos a la actualización de software de Ubuntu, en donde activaremos una opción que nos permitirá descargarnos herramientas de librerías externas, será de necesidad para poder utilizar un programa que nos permita recuperar el acceso a nuestra cuenta de Windows.

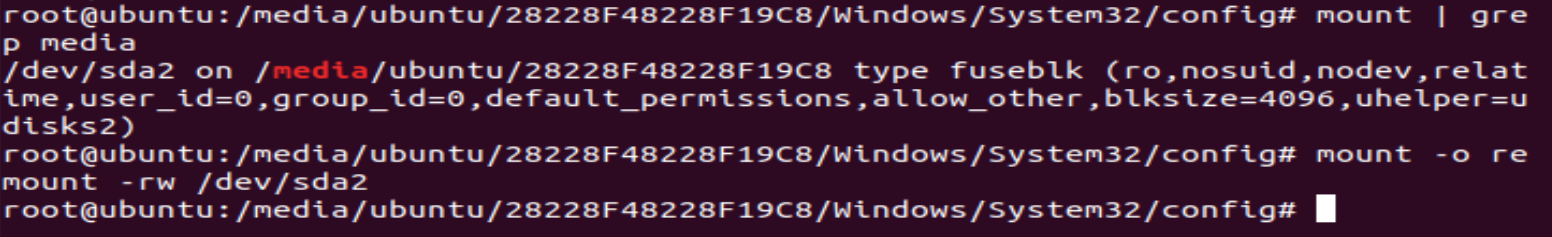


Ya realizado la actualización del software, ahora tendremos que actualizar la librería por medio de comandos, utilizando el “apt Update”.

Una vez realizado esto, tendremos que instalar ahora la herramienta que nos va a permitir realizar esta practica “chntpw” (sino actualizamos el software con anterioridad nos aparecerá que no se encuentra tal programa en la base de Ubuntu)

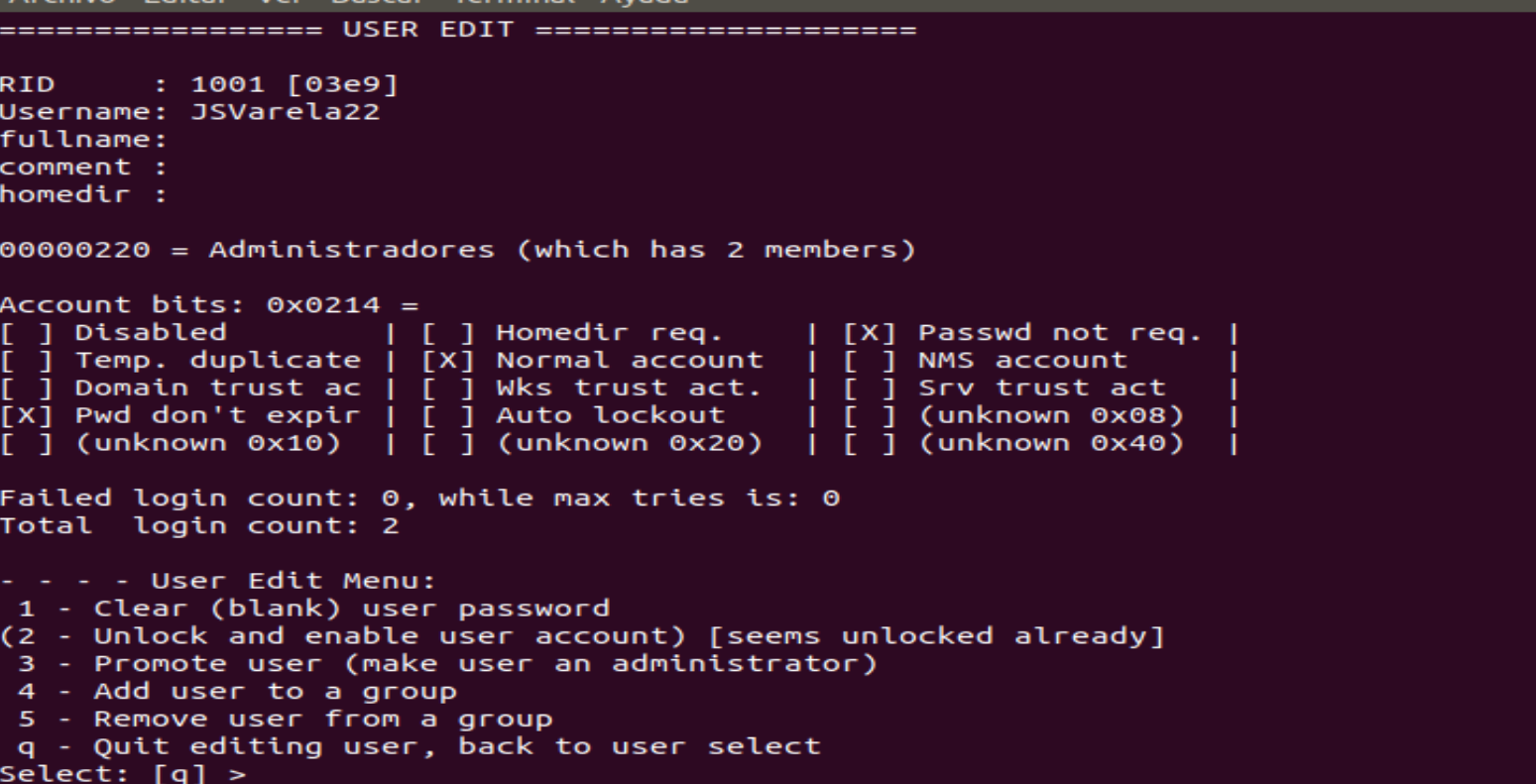
Ahora nos iremos a la ruta donde se encontraban los archivos de configuración de Windows, por lo que tendremos que echar de memoria o consultar de nuevo en el navegador de ficheros gráfico.

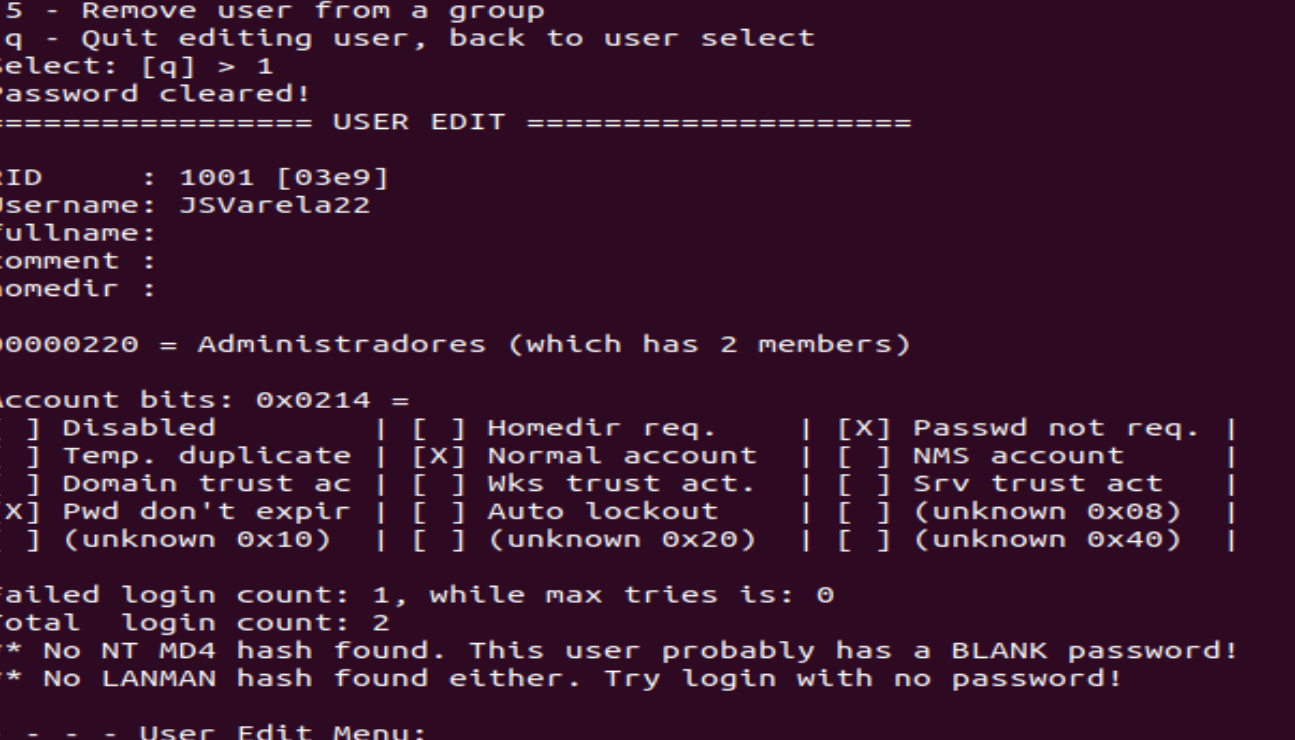
Una vez aquí, realizaremos un paso previo para evitarnos un posible errore de lectura en el disco de Windows, ejecutaremos los siguientes comandos que nos permitirán montar el disco con los sistemas de archivos que permitan ejecutar lectura y escritura en los archivos de configuración.

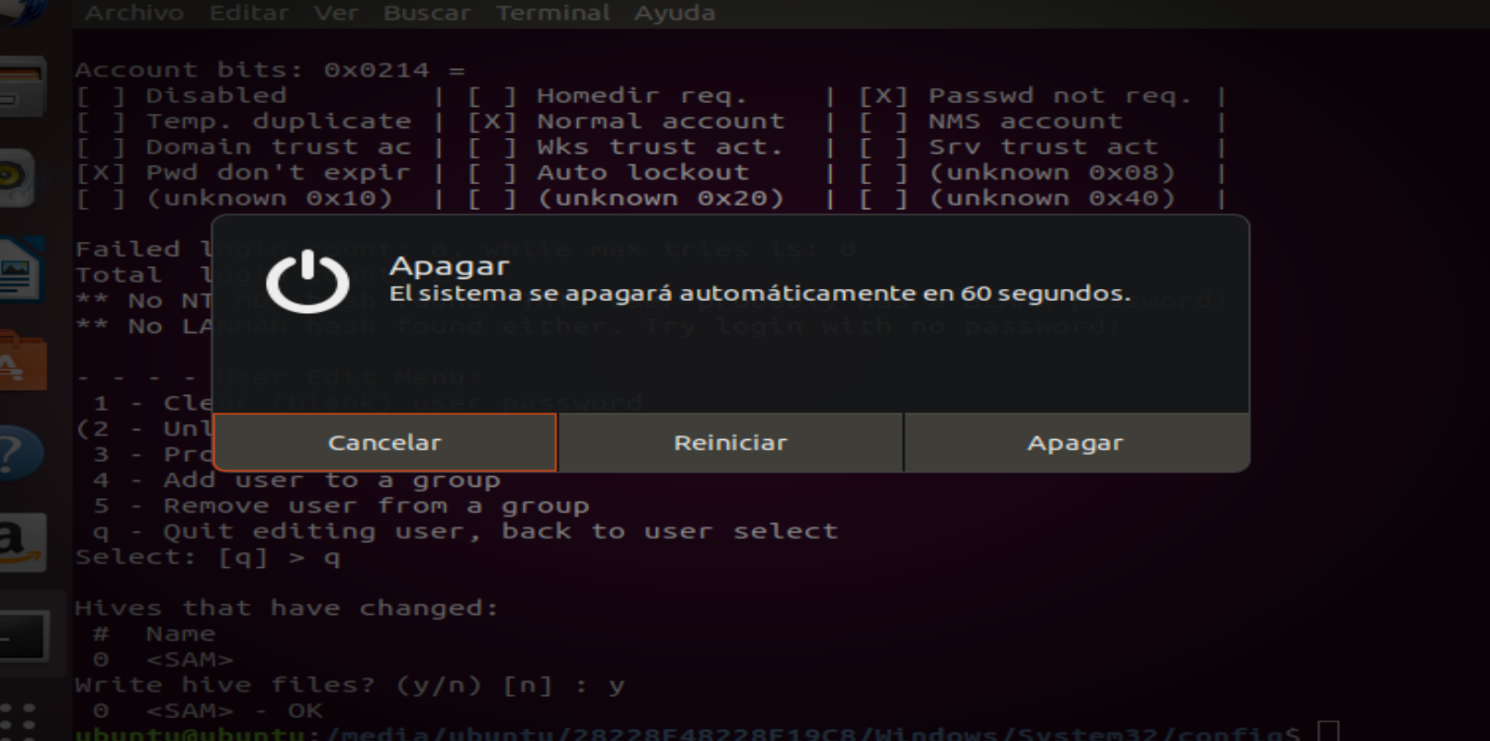


Y ahora nos dispondremos a utilizar la herramienta que hemos descargado para modificar el disco, utilizaremos el siguiente comando “chntpw -u \*nombre del administrador de Windows\* SAM”

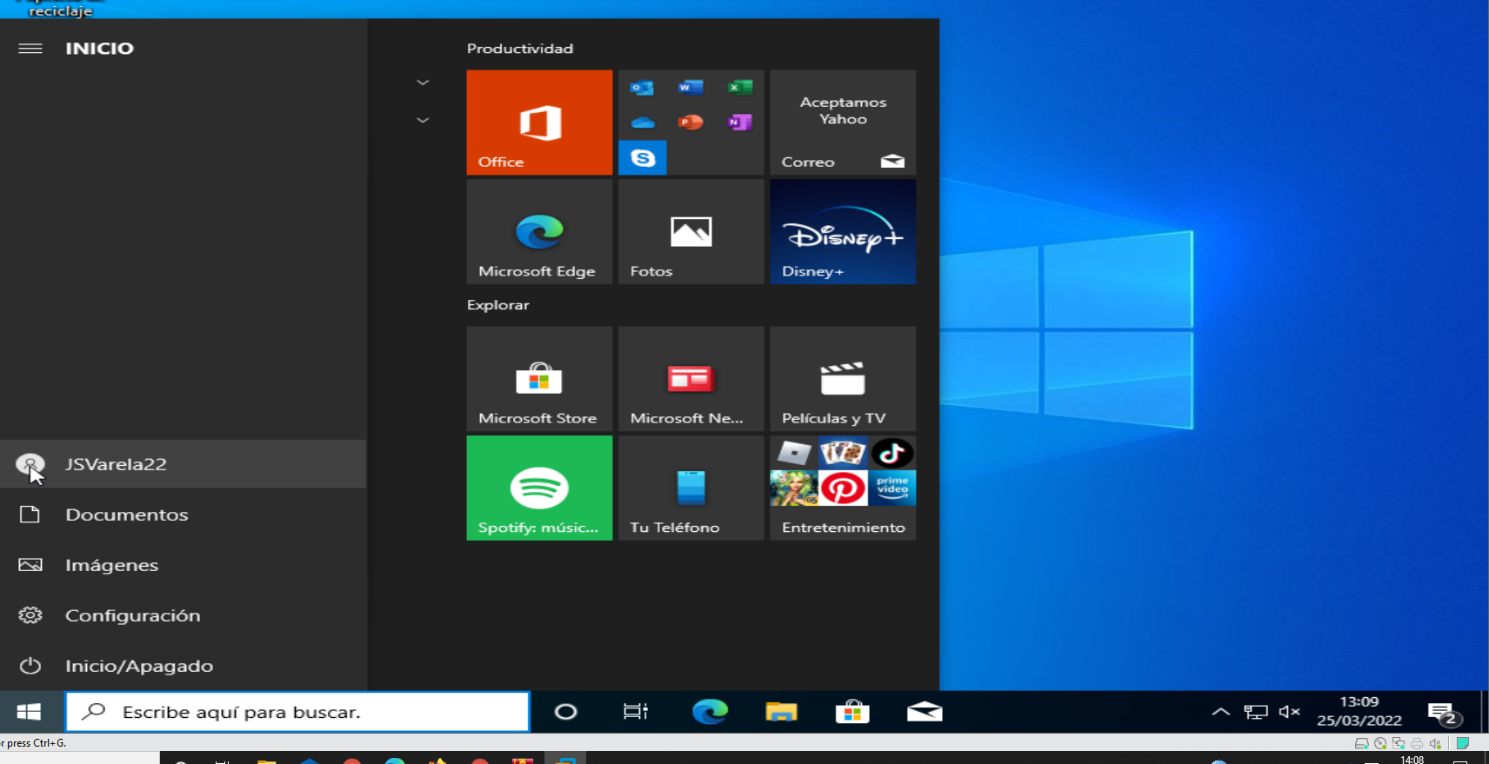
Se nos aparecerá una lista de opciones que podremos realizar en el disco y mas concretamente en la sección donde esta guardada nuestra cuenta de administrador.

aquí podremos realizar diversas acciones, entre las cuales se encuentra la “limpieza de contraseña” que será la que activemos para poder acceder a nuestra cuenta de administrador de Windows, para ello daremos como subcomando “1” que nos permitirá realizar esta acción.

Siguiente de esto, nos dirá que la contraseña ha sido limpiado y el usuario desbloqueado, por lo que en principio ya podremos acceder de nuevo a nuestra cuenta sin necesidad de introducir la contraseña.

Ahora tendremos que salirnos de esta sección con el subcomando “q” que aplicara los cambios y cerrara la configuración, y seguido de estos apagaremos la maquina para volver acceder al SO de Windows 10 instalado en el disco.

Ya fuera, volveremos a cambiar las opciones de arranque desde el Firmware y seleccionaremos que el sistema arranque por medio normal, y ya se nos iniciara el Windows 10 de vuelta. (Importante cambiar la configuración de la maquina que antes estaba para soportar un so Linux y ahora deberemos volver a ponerla para un Windows)



Y como vemos, la recuperación de la cuenta se habrá conseguir exitosamente, de esta manera y sin necesidad de haber instalado un Ubuntu en el disco evitando así alterar el sistema de archivo y el formateo que hubiese requerido para meter dos SO.

# Consideraciones finales y metacognición

En mi opinión, esta practica ha sido una de las mas interesantes y divertidas de realizar, pues nos ha introducido por unos instantes en el mundo del Hacking, aunque de esta manera pueda resultar ilícito, debemos entender que sirve para realizar acciones como la de esta practica para en caso de perder el acceso a nuestro usuario personal y evitar perder nuestros archivos mas importantes con un formateo de disco o acciones más peligrosas, por lo que es un beneficioso para el día de mañana en administración de sistemas, entender que hay formas de resolver problemas que aparentemente pueden ser difíciles pero con los conocimientos necesarios y podemos resolverlos eficazmente.