# Reset de una contraseña Windows desde Linux (hacking de un Windows) Habilitar una cuenta de administración en Windows

Alfredo Abad

https://www.nexolinux.com/howto-resetear-password-de-windows-con-linux/

ISOP406_ResetPasswWIN.pptx

UA: 9-nov-2022

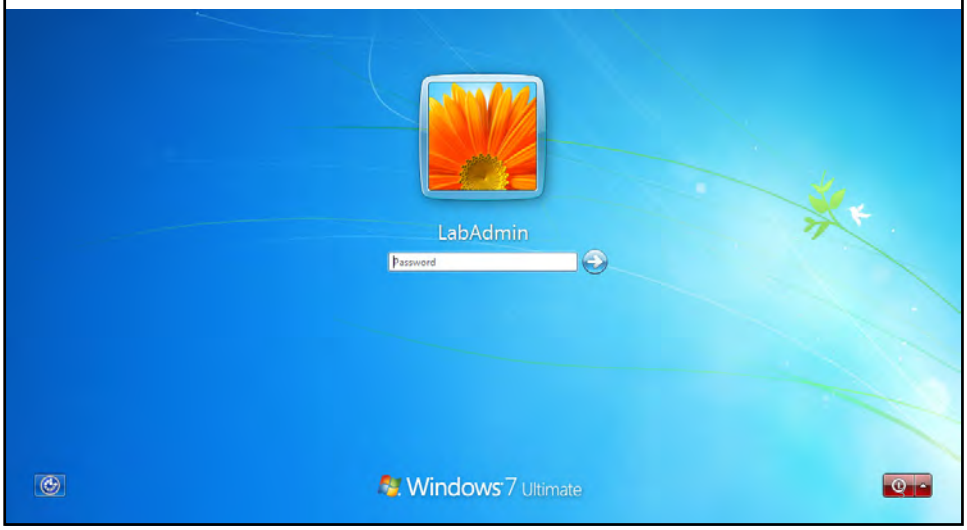
1

# Operación

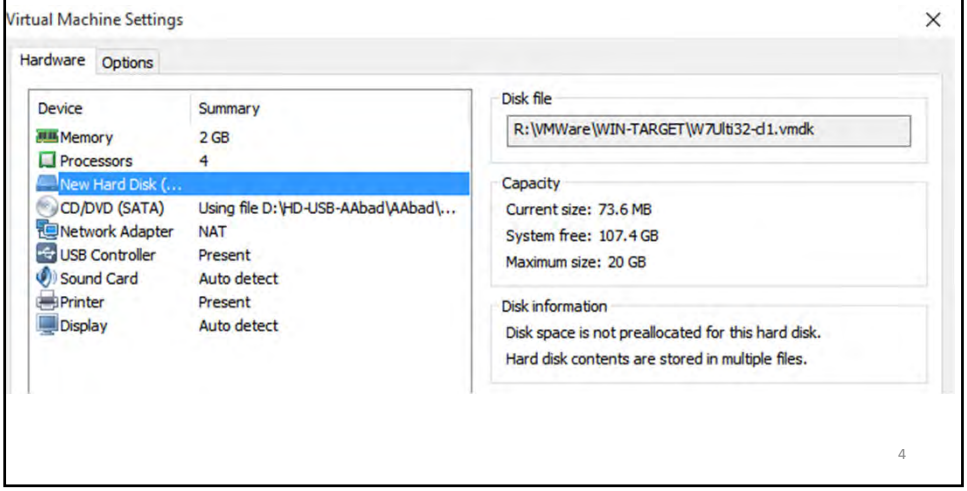
- Material necesario:
  - Un sistema Windows funcional del que conozcamos el nombre del administrador (no la contraseña)
    - **NOTA IMPORTANTE: la cuenta debe ser local y no de tipo nube Microsoft.**
  - Un LiveCD de Ubuntu
- Pasos a realizar
  - Crear máquina virtual LiveCD sin disco propio (tomará el disco del sistema Windows)
  - Gestión del paquete **chntpw** en el sistema Linux
  - Hacking de la contraseña Windows
  - Pruebas de conexión al sistema Windows (entrada al sistema como administrador)

2

## Vista del sistema Windows con usuario LabAdmin (desconocemos su contraseña) Apagamos el sistema para usar su disco



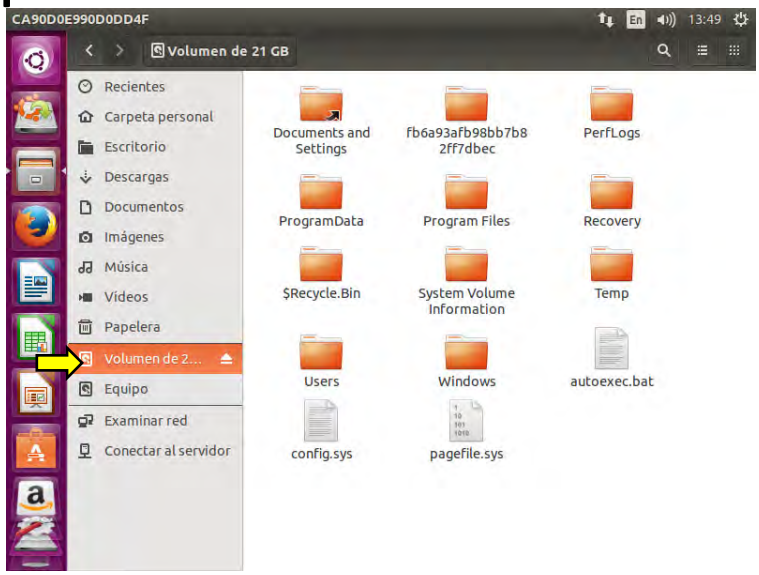

## Creamos una mv Linux con LiveCD y disco ya existente (el del sistema Windows)



# Iniciamos el sistema Live-CD


5

# Comprobamos que vemos el disco (el explorador de ficheros lo automontará)




6

No está en los respositorios estándar de Ubuntu, por lo que hay que descargarlo de la web o buscar un respositorio en donde se encuentre.

En concreto, en Ubuntu está en el repositorio de desarrolladores de la comunidad: añadiremos este repositorio y lo instalaremos desde él

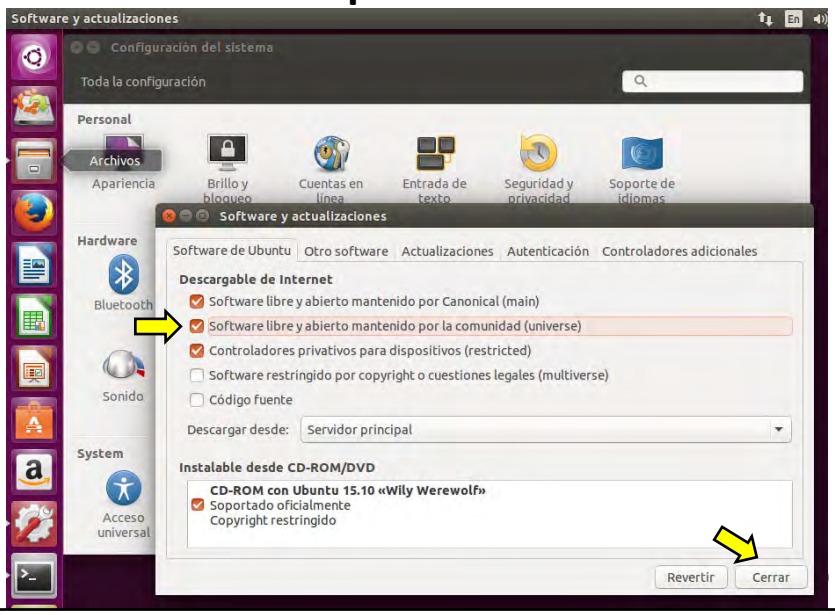
## INSTALACIÓN DEL PAQUETE DE SOFTWARE CHNTPW

7

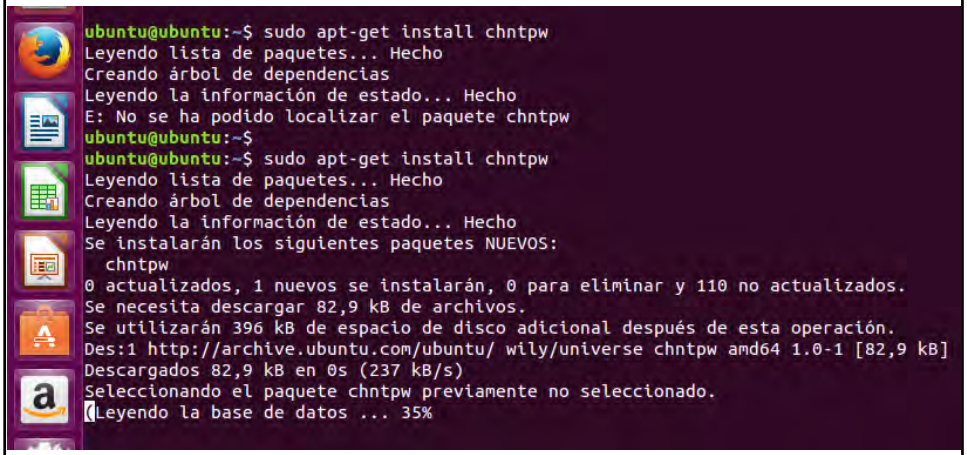
## Iniciamos el panel de control que gestiona los repositorios de software


8

# Añadimos el respositorio de desarrolladores mantenido por la comunidad

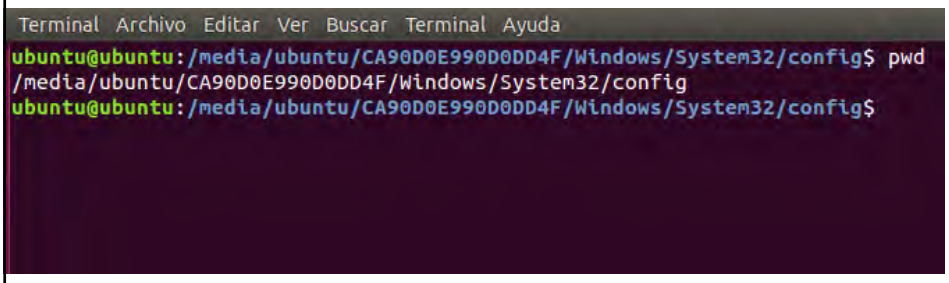



# Hacemos update e instalamos el paquete



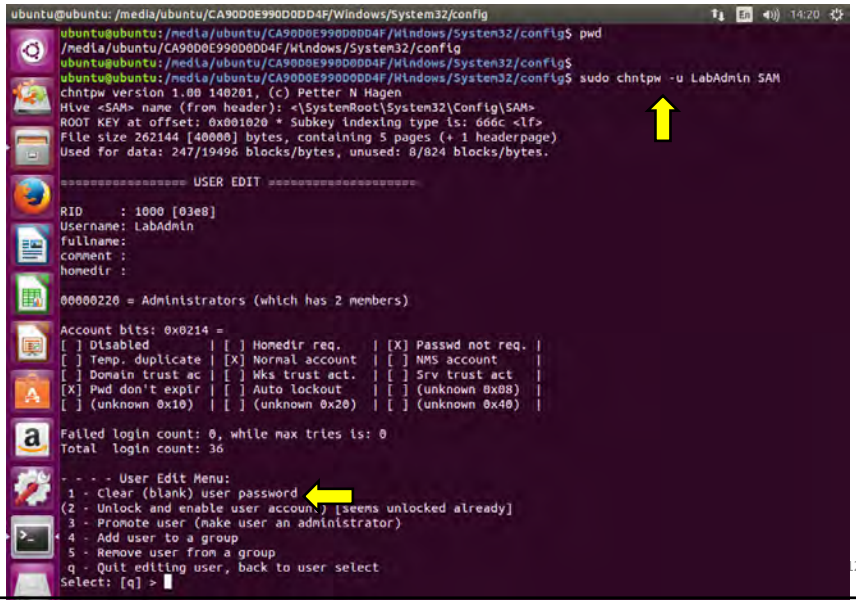

10

## Nos vamos al directorio de configuración de Windows (la orden mount nos indicará la ruta del disco)



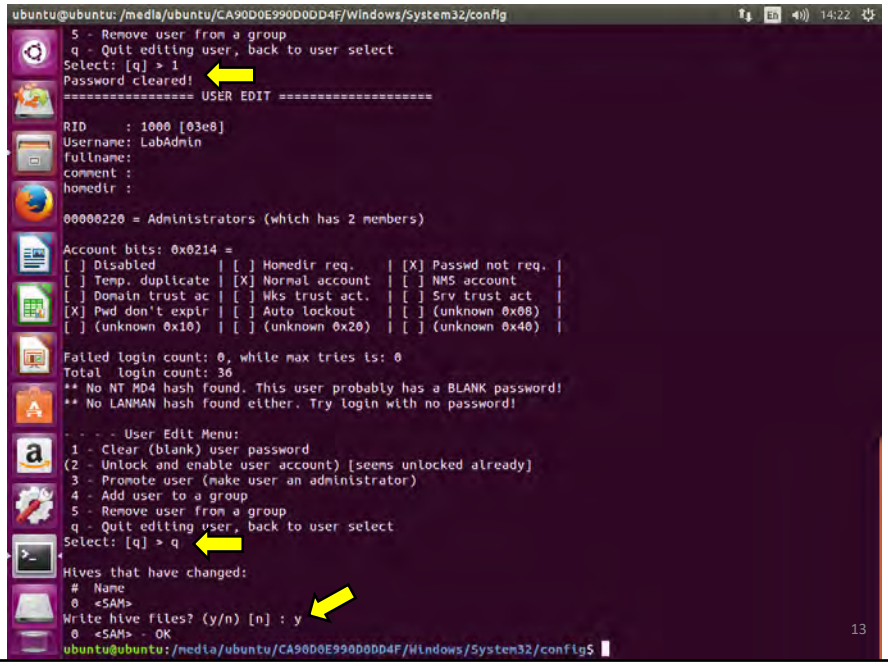

11

## Ejecutamos chntpw –u LabAdmin SAM (muy importante: may/min)

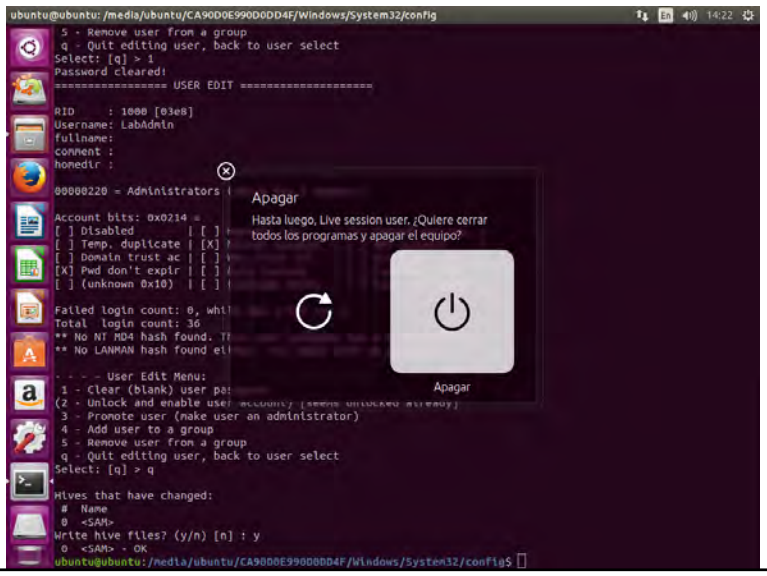



12

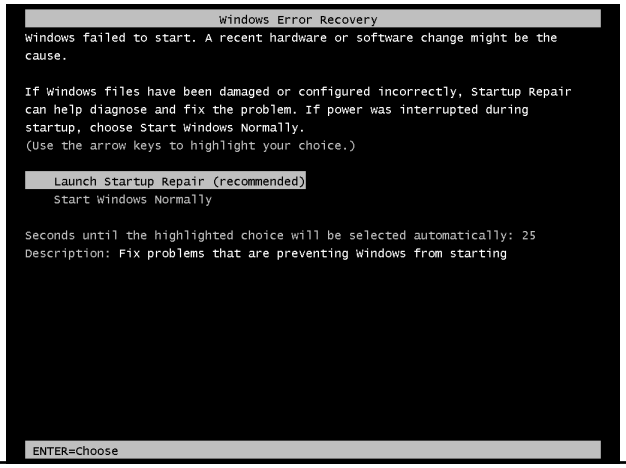
# Crackeamos la contraseña y salimos




# Apagamos el sistema Live-CD para liberar el disco del sistema Windows

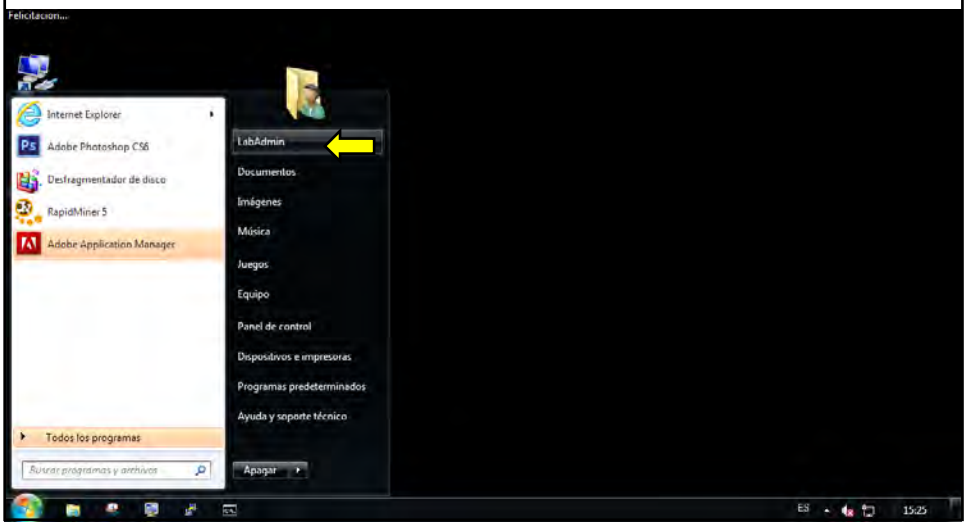


## Iniciamos Windows (el sistema se da cuenta de que el disco ha sido manipulado y nos propone un chequeo, que omitimos




15

## Al iniciar el sistema, LabAdmin no tiene contraseña y se autopresenta: ¡Ya somos administradores!




https://www.solvetic.com/tutoriales/article/3958-habilitar-cuenta-administrador-windows-10-sin-iniciar-sesion/

**¿CÓMO RESETEAR O CAMBIAR CONTRASEÑA DE WINDOWS?**

17

# Para entregar

- Una vez finalizada la práctica deberás entregar:
  - El informe de práctica con los detalles de ejecución según la plantilla de prácticas
  - Las pantallas más significativas que demuestren la ejecución
- Nomenclatura identificativa de práctica:
  - **ISOP406_ResetPasswWIN**

18