

Reset de una contraseña Windows desde Linux (hacking de un Windows)

Alfredo Abad

<http://www.nexolinux.com/howto-resetear-password-de-windows-con-linux/>

ISOP406_ResetPasswWIN.pptx

UA: 13-ago-2018

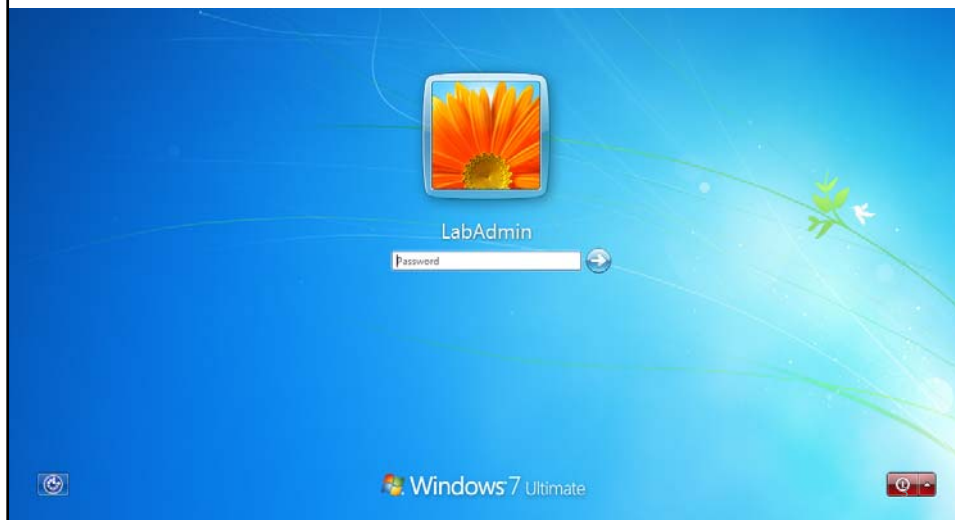
1

Operación

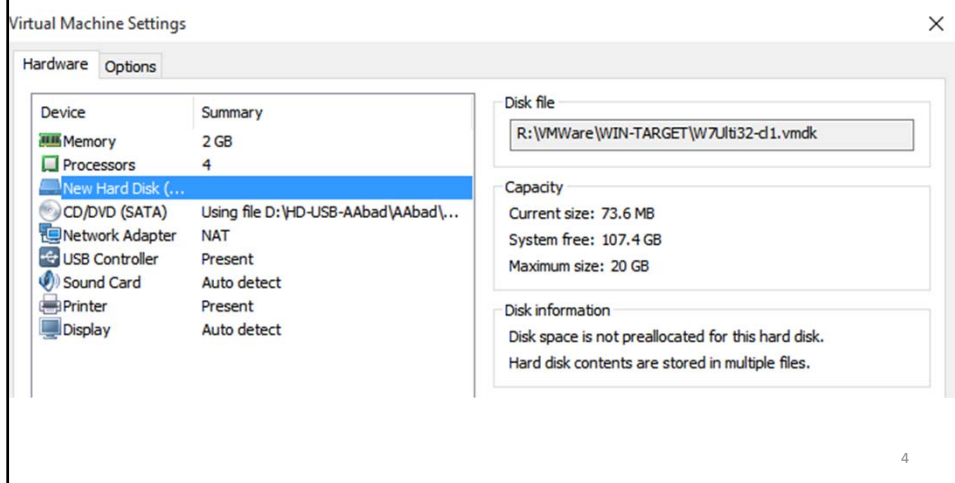
- **Material necesario:**
 - Un sistema Windows funcional del que conozcamos el nombre del administrador (no la contraseña)
 - Un LiveCD de Ubuntu
- **Pasos a realizar**
 - Crear máquina virtual LiveCD sin disco propio (tomará el disco del sistema Windows)
 - Gestión del paquete chntpw en el sistema 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)

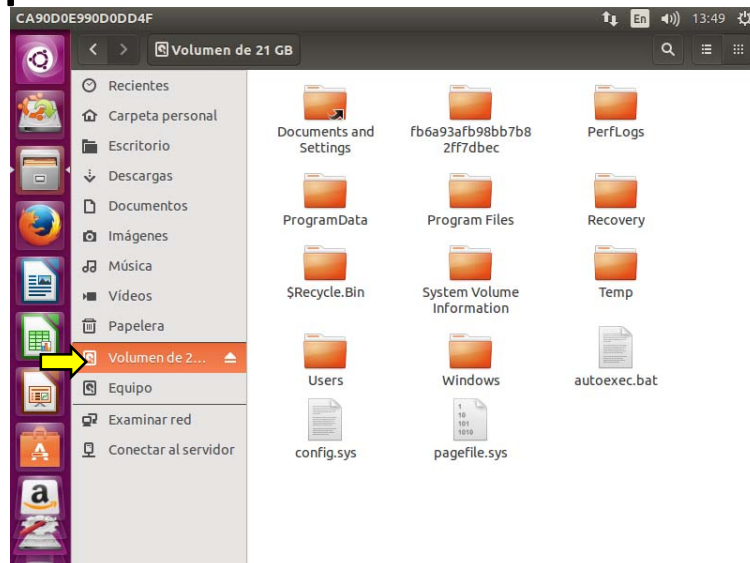


Iniciamos el sistema Live-CD



5

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



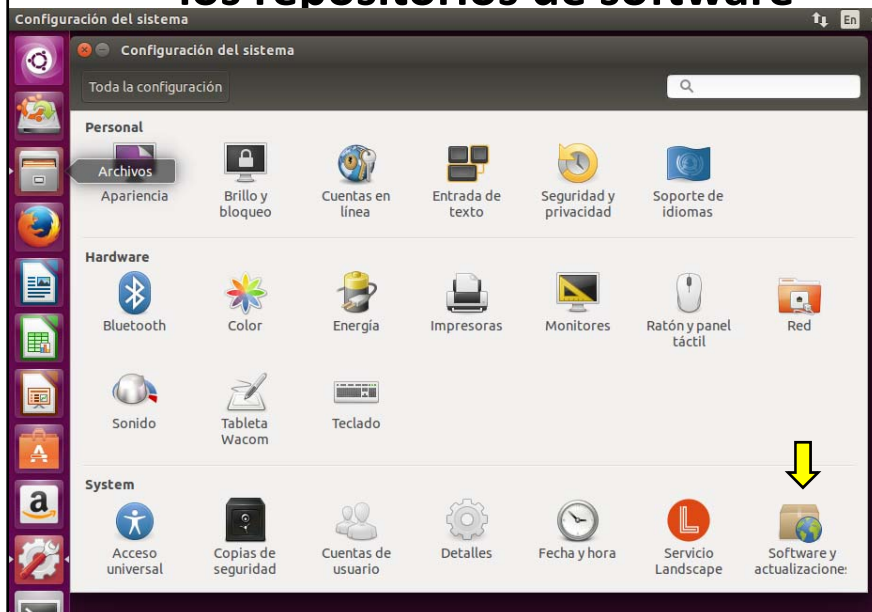
6

No está en los repositorios estándar de Ubuntu, por lo que hay que descargarlo de la web o buscar un repositorio 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

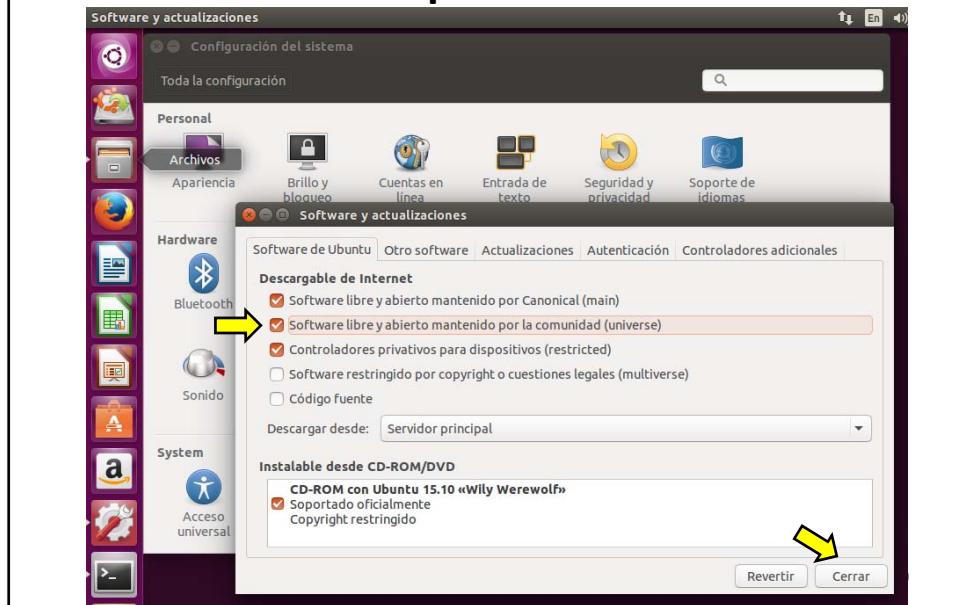
7

Iniciamos el panel de control que gestiona los repositorios de software

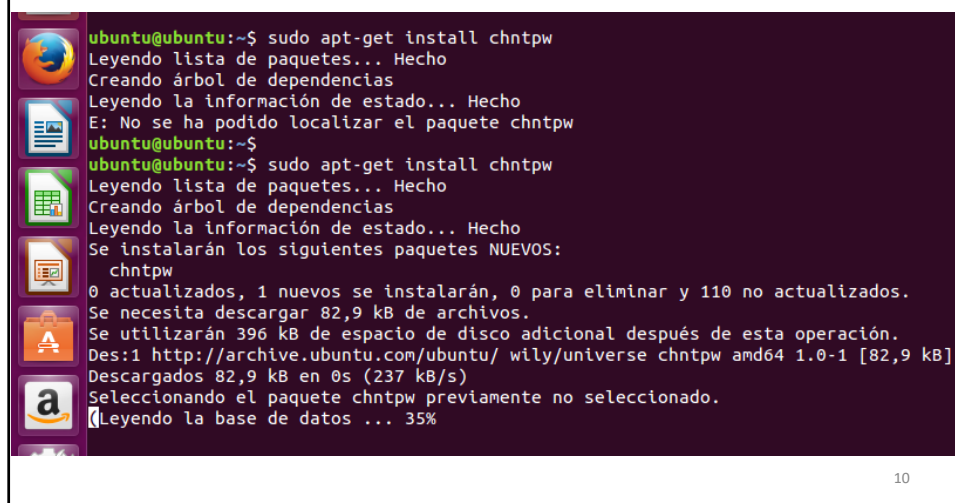


8

Añadimos el repositorio de desarrolladores mantenido por la comunidad



Hacemos update e instalamos el paquete



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

```
Terminal Archivo Editar Ver Buscar Terminal Ayuda
ubuntu@ubuntu:/media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config$ pwd
/media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config
ubuntu@ubuntu:/media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config$
```

11

**Ejecutamos chntpw -u LabAdmin SAM
(muy importante: may/min)**

```
ubuntu@ubuntu:/media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config$ sudo chntpw -u LabAdmin SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 060c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 247/19496 blocks/bytes, unused: 8/824 blocks/bytes.

===== USER EDIT =====
RID      : 1000 [03e0]
Username: LabAdmin
Fullname:
Comment:
Homedir:

00000220 = Administrators (which has 2 members)

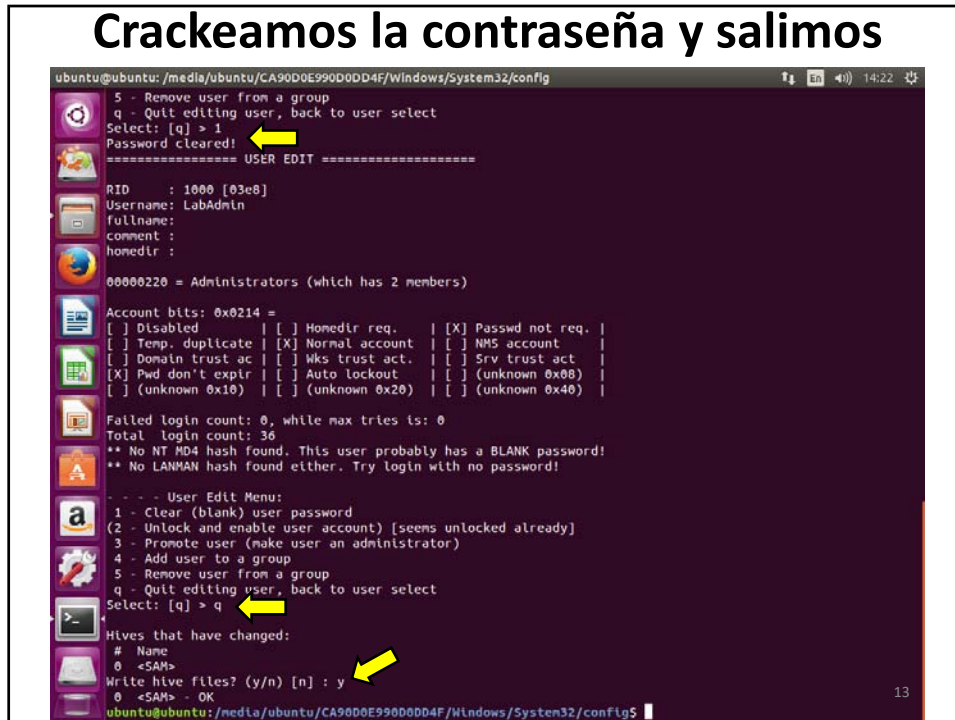
Account bits: 0x0214 =
[ ] Disabled      [ ] Homedir req.    [X] Password not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act.  [ ] Srv trust act
[X] Pwd don't expir [ ] Auto lockout   [ ] (unknown 0x08)
[ ] (unknown 0x10)  [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 36

- - - 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] >
```

12

Crackeamos la contraseña y salimos



```

ubuntu@ubuntu: /media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
===== USER EDIT =====
RID      : 1000 [03e8]
Username: LabAdmin
fullname:
comment :
homedir :
00000220 = Administrators (which has 2 members)
Account bits: 0x0214 =
[ ] Disabled      [ ] Homedir req.    [X] Password not req.
[ ] Temp. duplicate [X] Normal account [ ] Nt5 account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir [ ] Auto lockout  [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)
Failed login count: 0, while max tries is: 0
Total login count: 36
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!
- - - 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] > q
Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
ubuntu@ubuntu: /media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config$
  
```

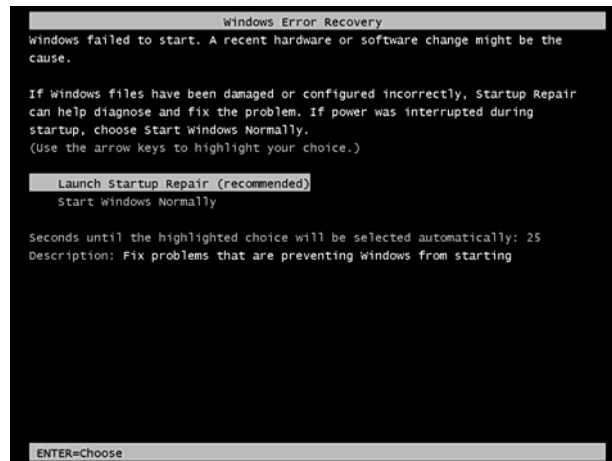
Apagamos el sistema Live-CD para liberar el disco del sistema Windows



```

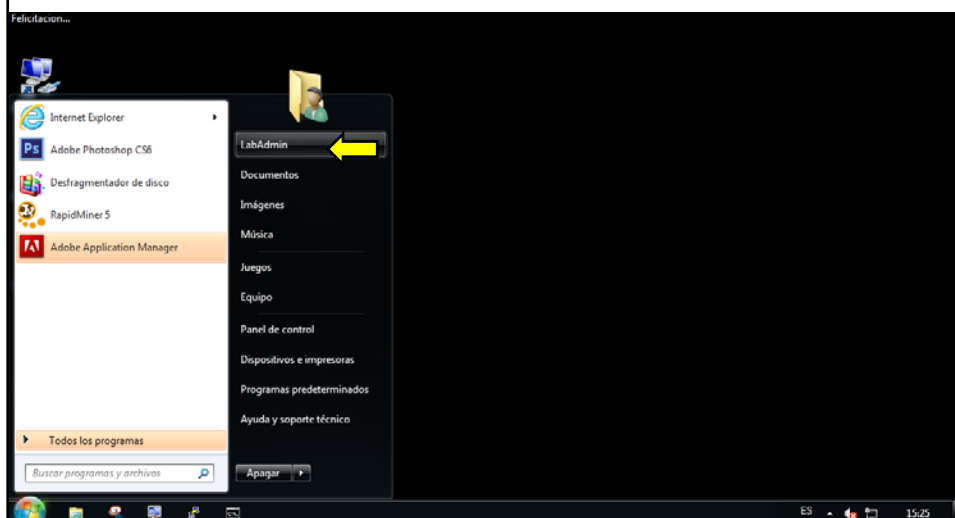
ubuntu@ubuntu: /media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
===== USER EDIT =====
RID      : 1000 [03e8]
Username: LabAdmin
fullname:
comment :
homedir :
00000220 = Administrators
Account bits: 0x0214 =
[ ] Disabled      [ ] Homedir req.    [X] Password not req.
[ ] Temp. duplicate [X] Normal account [ ] Nt5 account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir [ ] Auto lockout  [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)
Failed login count: 0, while max tries is: 0
Total login count: 36
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!
- - - 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] > q
Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
ubuntu@ubuntu: /media/ubuntu/CA90D0E990D0DD4F/Windows/System32/config$
  
```


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!



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**

17