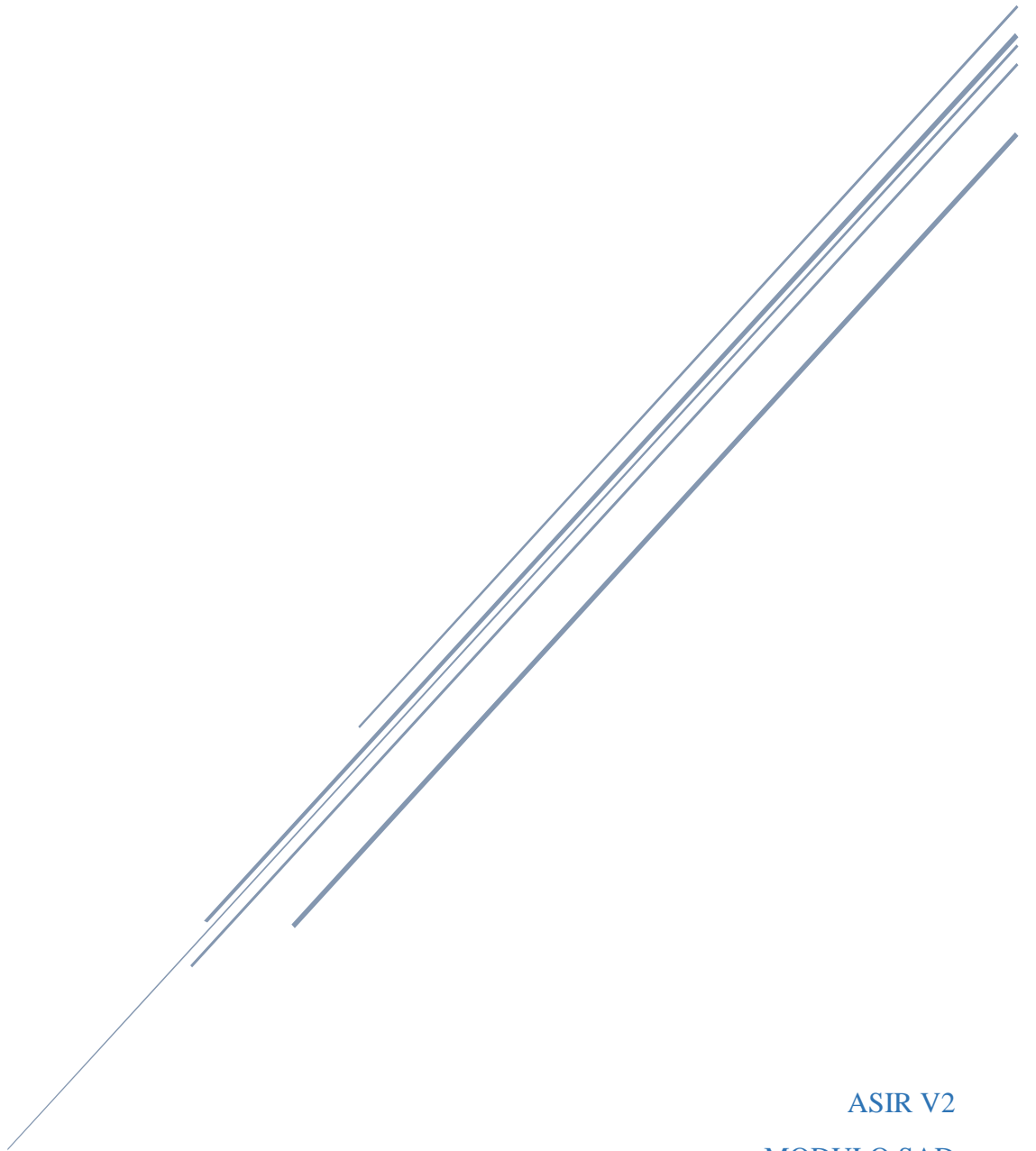


AUDITORIA DE CONTRASEÑAS



ASIR V2
MODULO SAD
Alberto Resa Pérez

INDICE

| | |
|-------------------------------------|----|
| 1. Objetivos..... | 2 |
| 2. Desarrollo..... | 3 |
| a. Recuperación de contraseñas..... | 3 |
| Windows..... | 3 |
| Kali Linux | 10 |
| b. Modificación de contraseñas..... | 12 |
| Ultimate Boot CD..... | 12 |
| ERD Commander..... | 16 |
| 3. Conclusión..... | 20 |
| 4. Bibliografía..... | 21 |

1. Objetivos.

En el desarrollo de esta práctica hemos tenido 2 objetivos diferentes

Por un lado hemos tenido el objetivo de averiguar las contraseñas de los usuarios de un sistema operativo Windows y después realizar el mismo proceso en un sistema operativo Kali Linux, para ello hemos utilizado 2 herramientas, LiveCD de ophcrack para intentar sacar las contraseñas de Windows y John de Ripper instalado en Kali Linux e intentar sacar las mismas contraseñas de los usuarios.

Por otro lado hemos tenido el objetivo de sustituir las contraseñas de los usuarios, primero lo realizaremos cambiando el StickyKeys, un software de ayuda y accesibilidad que se inicia en Windows al pulsar la tecla shift 5 veces, por el cmd con privilegios de administrador, lo cual nos permitiría modificar los usuarios y sus contraseñas y después lo realizaremos con la herramienta ERD Commander que tiene diferentes herramientas para reparación de sistemas operativos.

2. Desarrollo.

a. Recuperación de contraseñas.

En esta primera parte de la práctica vamos a intentar sacar las contraseñas de los usuarios en Windows como en Kali Linux, para ello vamos a utilizar 2 herramientas e intentar que nos descifre las contraseñas que hemos configurado en los sistemas operativos.

Windows

El primer paso que realizamos es crear los usuarios en el sistema operativo Windows. Para nuestro caso hemos configurado 4 cuentas con las siguientes combinaciones de contraseñas:

Alberto – A1b2c3d4.

Juan – Juan

Marta – 250715

Sara – S18ara



Iniciaremos la máquina virtual desde el la unidad CD donde tendremos un LiveCD de ophcrack. Este software es el que usaremos para sacar las contraseñas de los usuarios creados anteriormente.



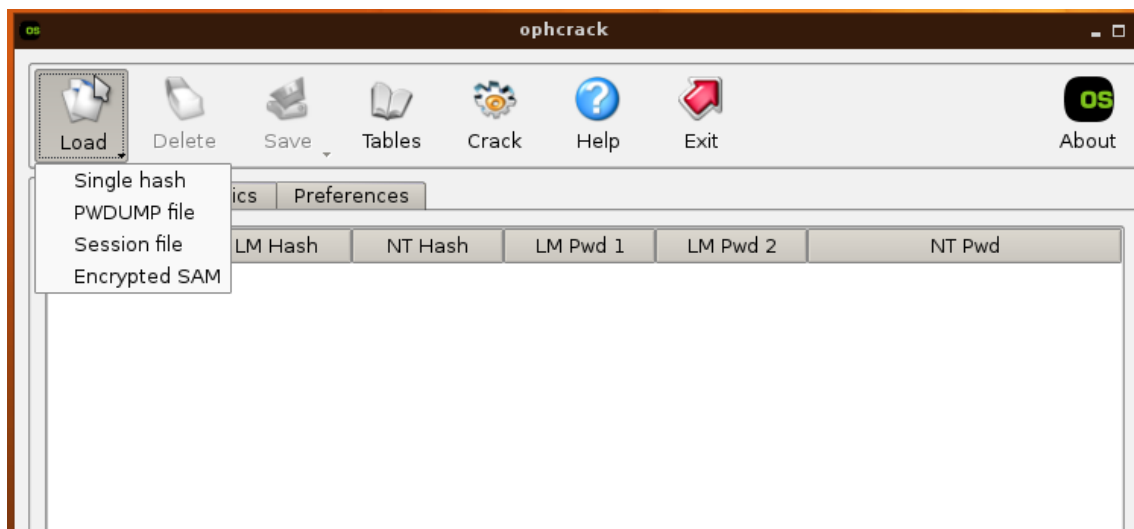
Una vez iniciado el programa tenemos que montar la partición que contiene instalado el sistema operativo. Como podemos comprobar tenemos montada la partición sda2 que por tamaño será la que contiene Windows.

```
tux@slitaz:~$ group
/bin/sh: group: not found
tux@slitaz:~$ ls /media/
cdrom  flash  sda1  sda2  sr0  usbdisk
tux@slitaz:~$ su
Password:
root@slitaz:/home/tux# fdisk -l

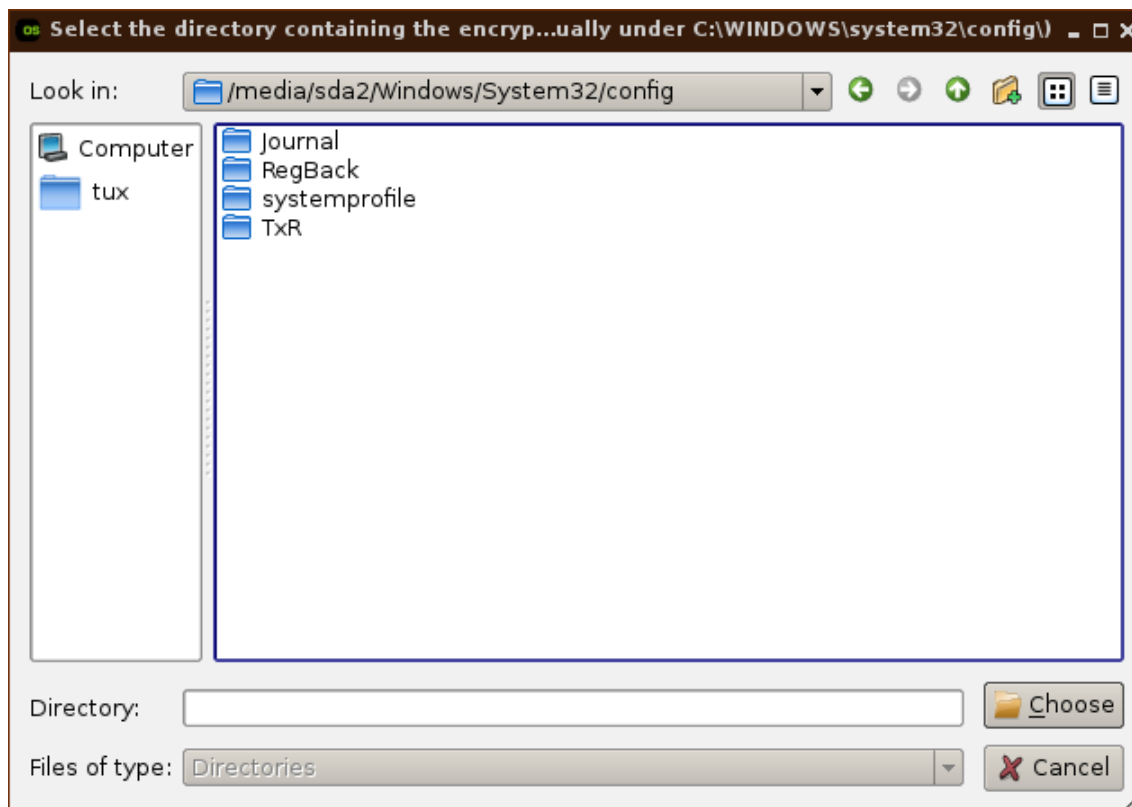
Disk /dev/sda: 64.4 GB, 64424509440 bytes
255 heads, 63 sectors/track, 7832 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *           1           13       102400    7  HPFS/NTFS
Partition 1 does not end on cylinder boundary
/dev/sda2           13        7833     62810112    7  HPFS/NTFS
root@slitaz:/home/tux# df
Filesystem            1K-blocks      Used Available Use% Mounted on
tmpfs                 1866504      176604   1689900   9% /
tmpfs                 1036944         0    1036944   0% /dev/shm
/dev/sr0               663860     663860         0 100% /media/sr0
/dev/sda1              102396      24920     77476  24% /media/sda1
/dev/sda2             62810108   20367060   42443048  32% /media/sda2
root@slitaz:/home/tux#
```

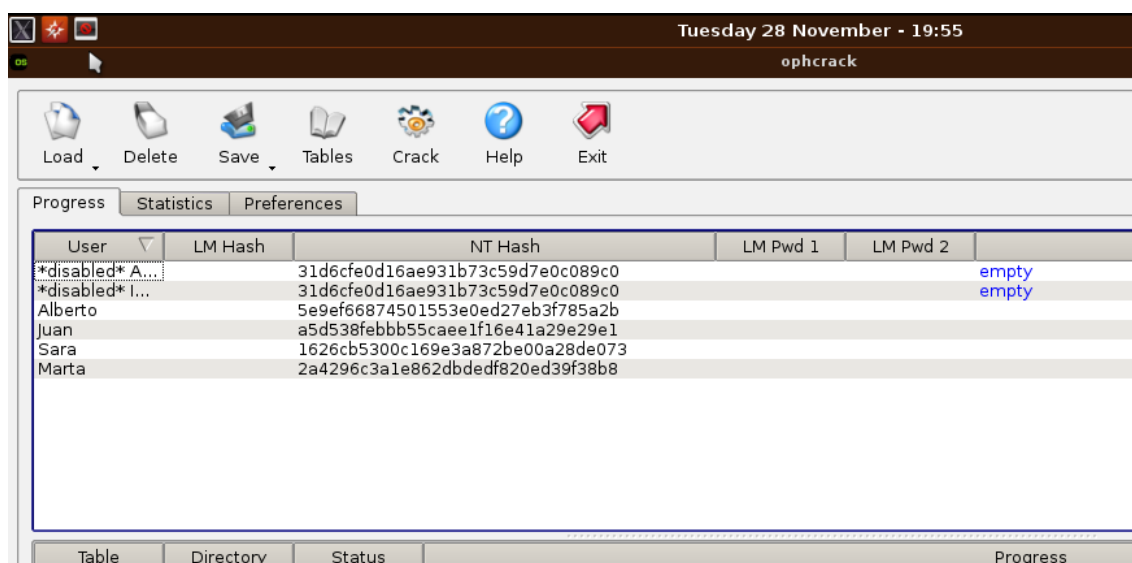
Ahora iniciamos el programa ophcrack y le indicaremos en la pestaña load que cargue SAM que es donde se guardan las contraseñas Windows.



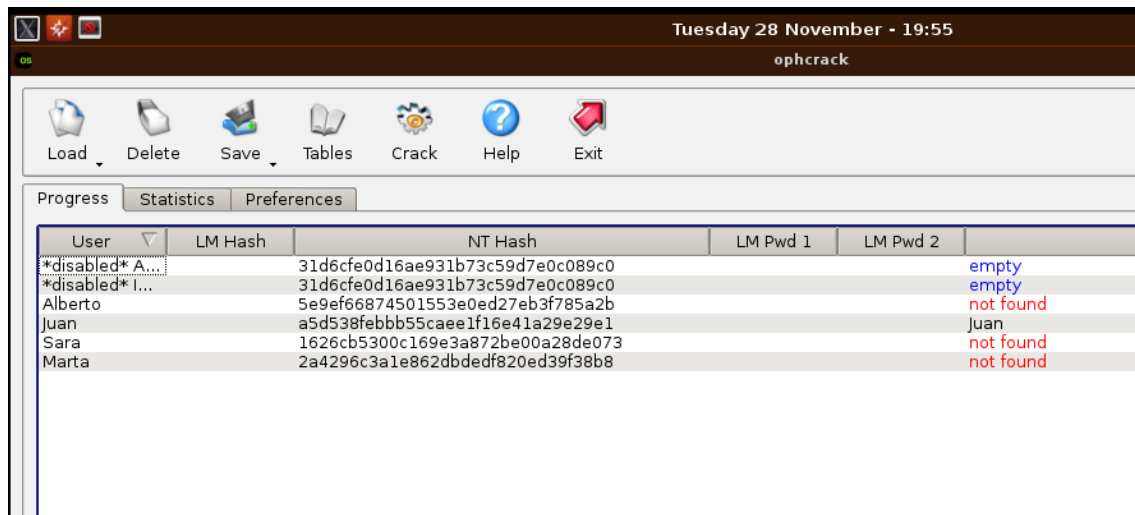
Nos abrirá una nueva ventana donde le tenemos que indicar la ruta hasta el SAM. Como podemos ver en la imagen entramos en la unidad montada y nos dirigimos hasta la carpeta donde se almacenan estas contraseñas.



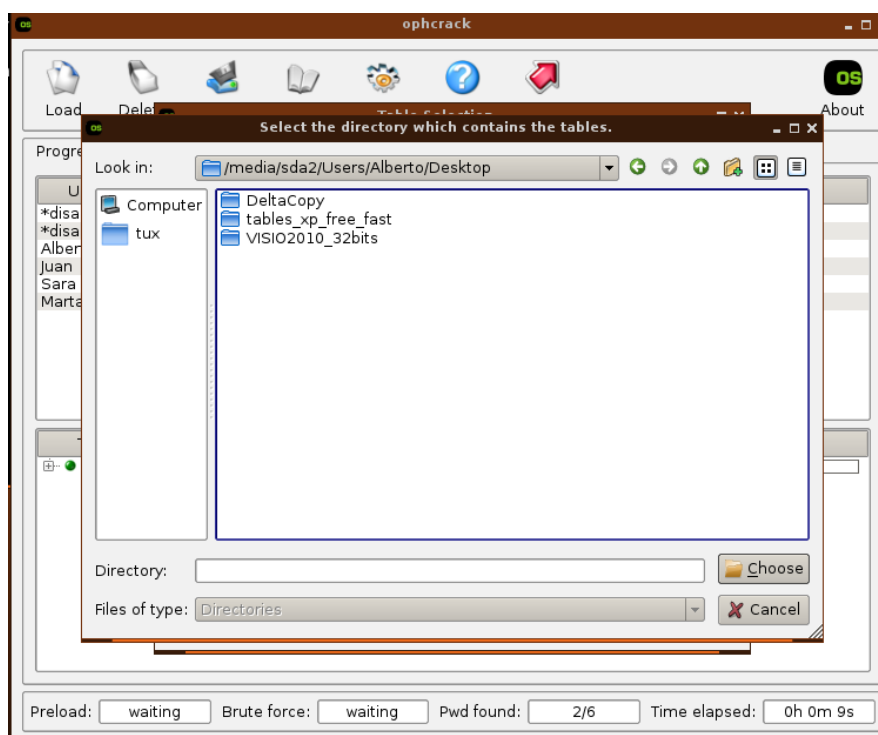
Como podemos ver en la imagen se nos cargan los 4 usuarios que hemos creado y podemos ver la contraseña encriptada de cada uno de ellos.



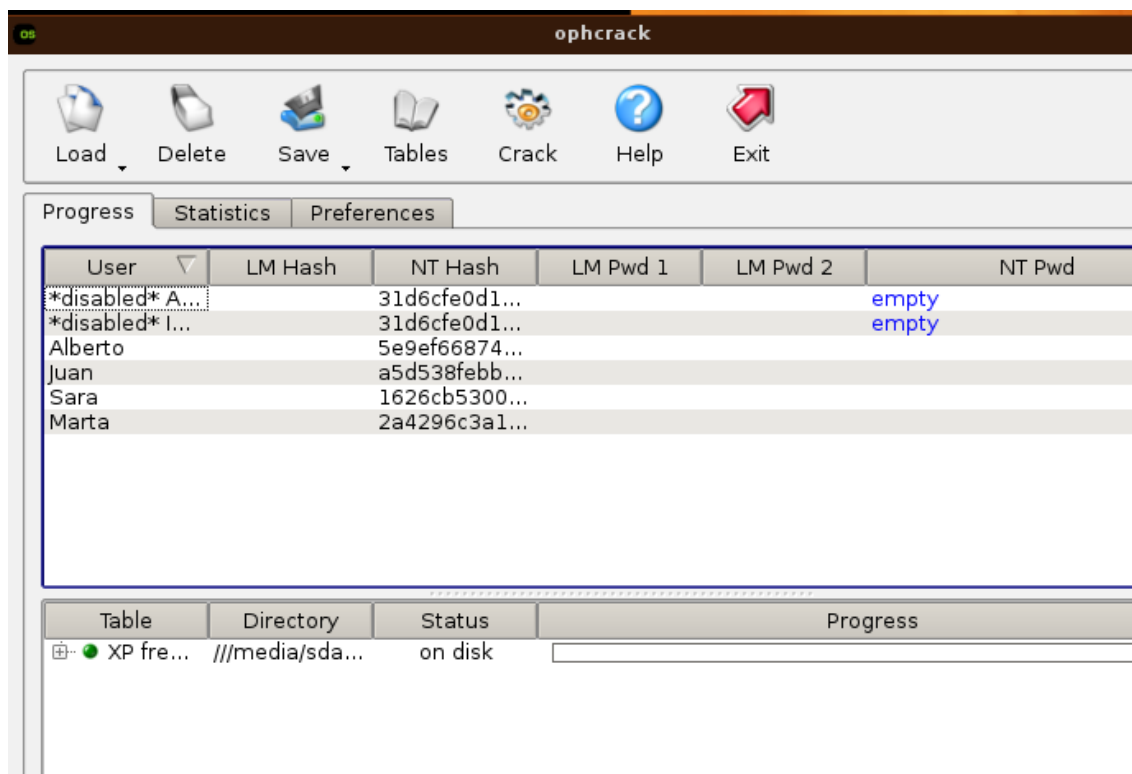
Lo siguiente que tenemos que realizar es pulsar sobre crack para comenzar el proceso por fuerza bruta. Después de un tiempo de proceso podemos comprobar que solo es capaz de descifrar la contraseña que coincide con el nombre del propio usuario.



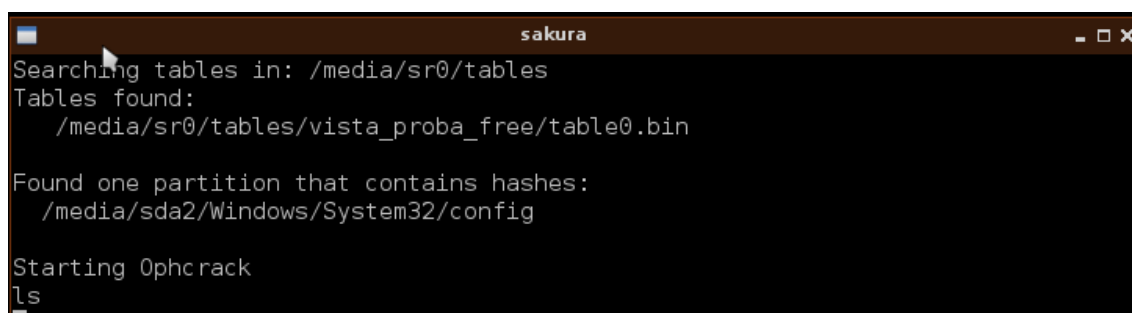
Como no ha sido capaz de sacar el resto de contraseñas vamos a realizar la carga de diccionarios con los que intentaremos descifrarlas. Para ello pulsamos sobre tables y le indicamos la ruta a una carpeta en la que hemos guardado unas tablas llamadas tables_xp_free_fast.



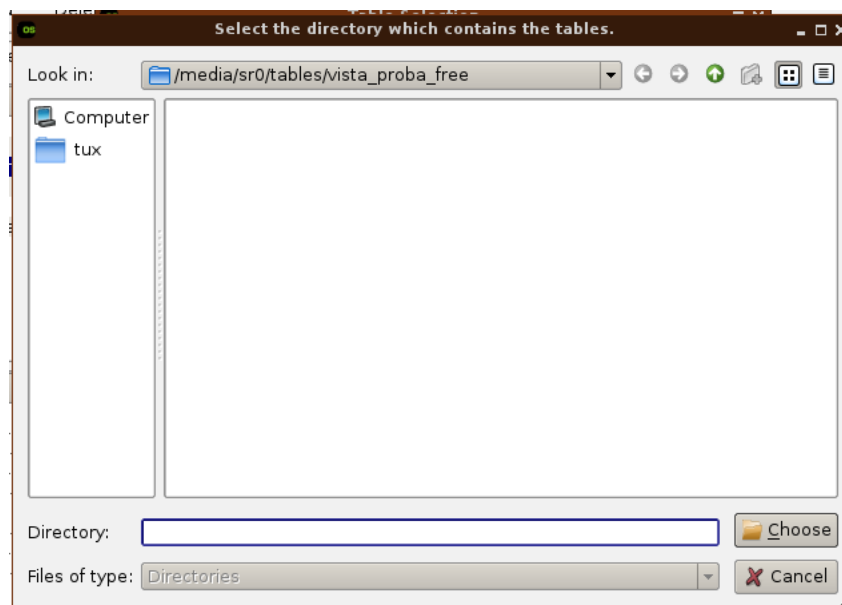
Como vemos se nos han vuelto a cargar los usuarios y en la parte inferior ya tenemos cargada la tabla indicada.



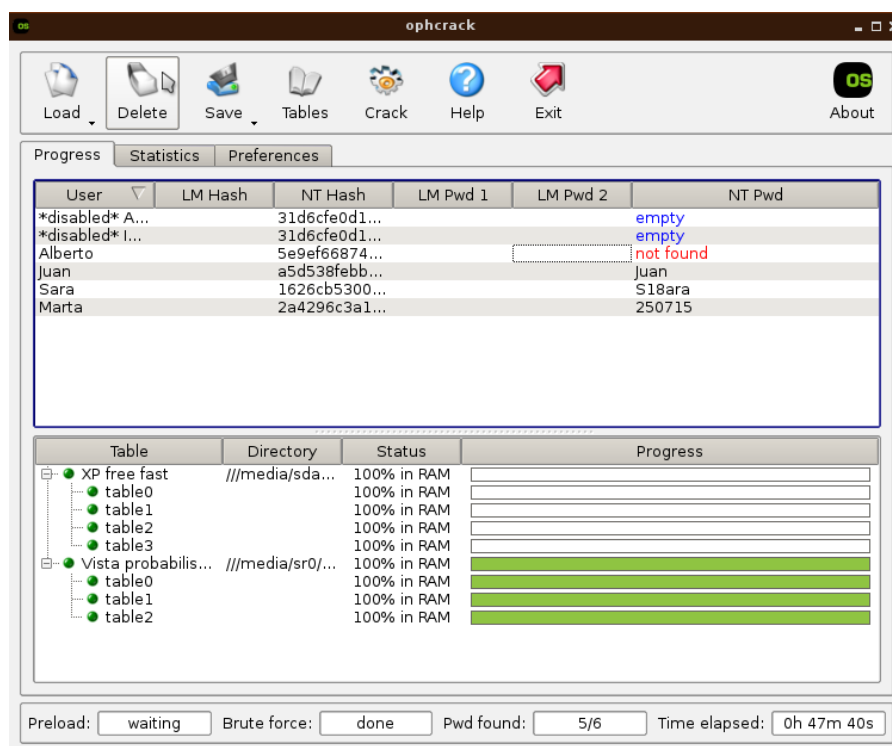
Pero además de esta tabla el propio LiveCD tiene unas tablas en la propia distribución. Para descubrir la ruta nada más iniciar el LiveCD vemos que nos abre un terminal en el cual no indica la ruta a la tabla que guarda y otra donde se encuentra el archivo en que Windows almacena las contraseñas y que automáticamente a localizado.



Como ya hemos realizado anteriormente volveremos a pulsar en tables para indicarle la ruta de acceso a estas otras tablas llamadas vista_proba_free.

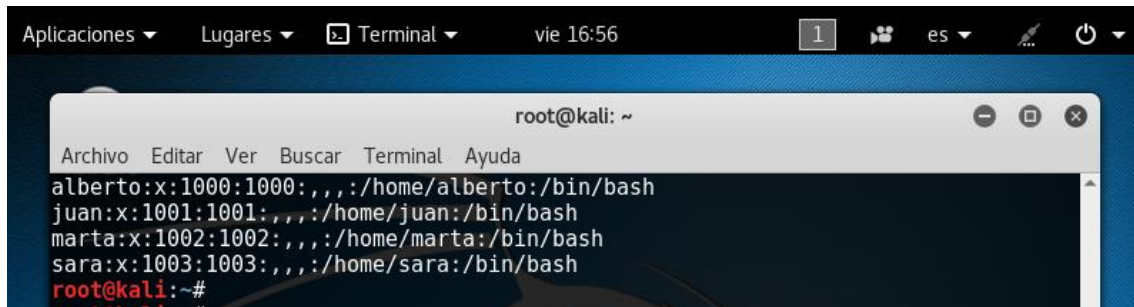


Una vez esta la tabla agregada iniciaremos el proceso de crackeo de contraseñas el cual durara para este caso 47 minutos. Al finalizar veremos que tenemos sacadas las contraseñas de 3 de los usuarios, solo ha sido imposible averiguar la contraseña mas complicada.



Kali Linux

La siguiente parte vamos a realizar el mismo proceso pero en este caso intentaremos averiguar las contraseñas almacenada en un sistema operativo Kali Linux. Para ello hemos realizado el proceso de crear los mismos usuarios y las mismas contraseñas que teníamos en Windows.

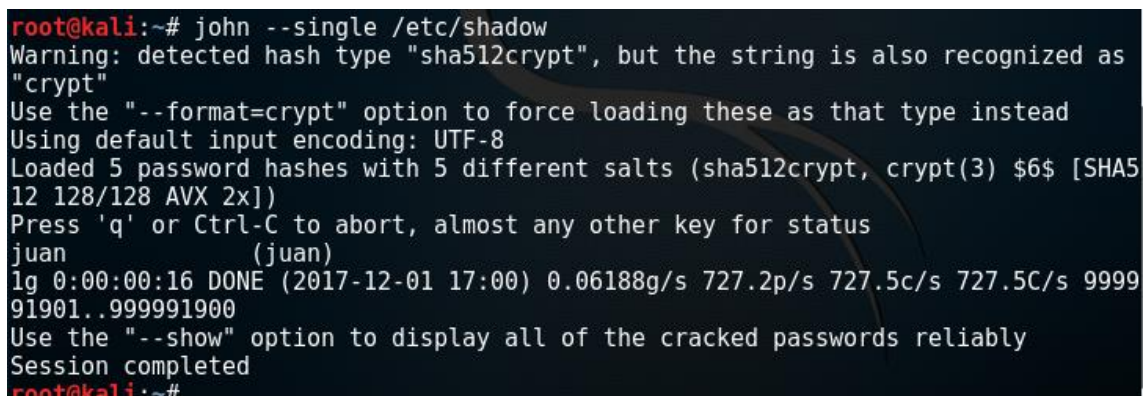


```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
alberto:x:1000:1000:,,,:/home/alberto:/bin/bash  
juan:x:1001:1001:,,,:/home/juan:/bin/bash  
marta:x:1002:1002:,,,:/home/marta:/bin/bash  
sara:x:1003:1003:,,,:/home/sara:/bin/bash  
root@kali:~#
```

En esta práctica vamos a utilizar el programa John de Ripper. Como vemos en la imagen iniciamos el programa y se nos carga un terminal.

El primer intento que realizaremos será el simple de este programa, la cual consiste en utilizar el nombre de los usuarios y otras palabras de uso habitual.

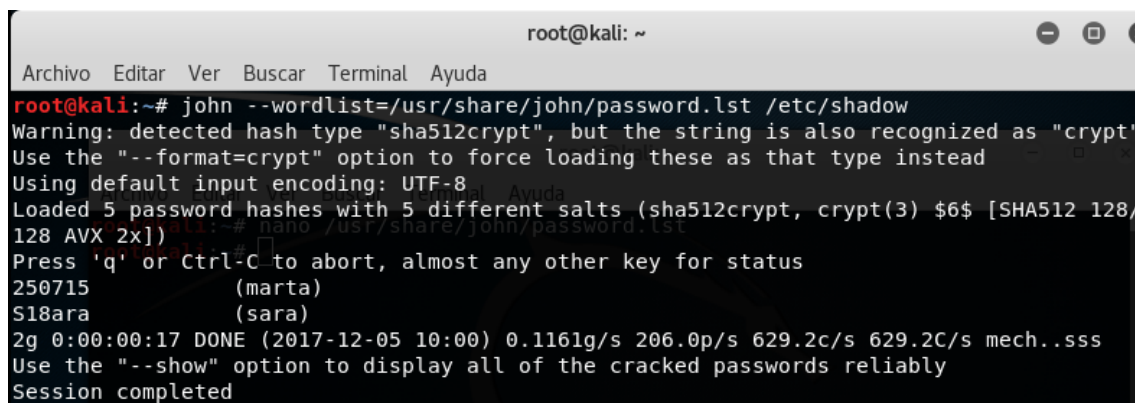
Tras finalizar el proceso podemos comprobar como la única clave que ha conseguido sacar es la del usuario que coincide con el propio nombre de usuario.



```
root@kali:~# john --single /etc/shadow  
Warning: detected hash type "sha512crypt", but the string is also recognized as  
"crypt"  
Use the "--format=crypt" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA5  
12 128/128 AVX 2x])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
juan (juan)  
1g 0:00:00:16 DONE (2017-12-01 17:00) 0.06188g/s 727.2p/s 727.5c/s 727.5C/s 9999  
91901..999991900  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
root@kali:~#
```

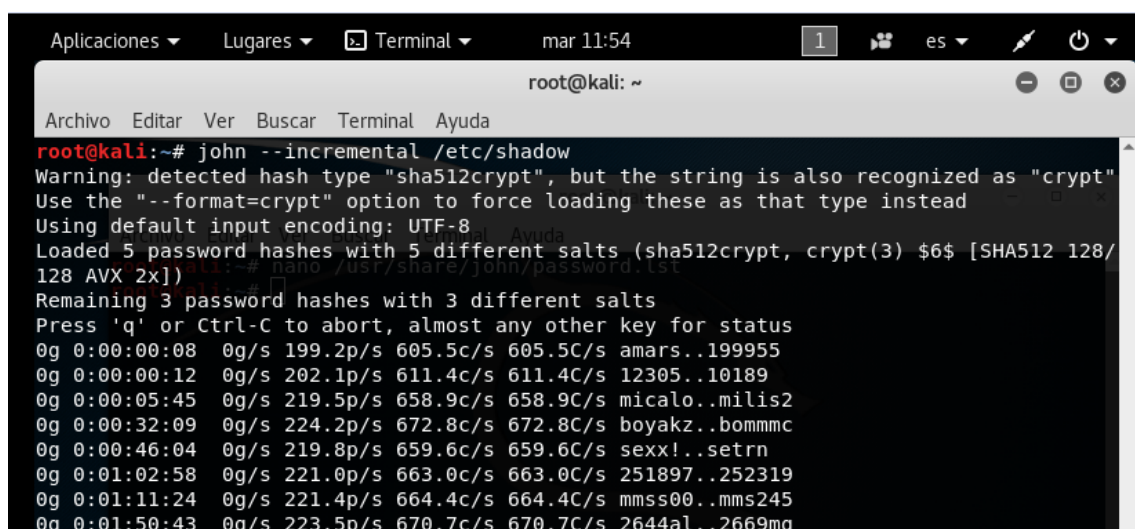
El siguiente paso es usar un diccionario para intentar sacar el resto de contraseñas. El propio programa trae un diccionario con palabras en el cual nosotros vamos a introducir las contraseñas de dos de los usuarios.

Después iniciaremos el proceso con el comando que vemos en la imagen y al finalizar el proceso comprobamos que nos ha localizado las 2 contraseñas introducidas dado que el proceso es simplemente coger las palabras del archivo y comprobar si coinciden con las de los usuarios.



```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# john --wordlist=/usr/share/john/password.lst /etc/shadow  
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"  
Use the "--format=crypt" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/  
128 AVX 2x])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
250715 (marta)  
S18ara (sara)  
2g 0:00:00:17 DONE (2017-12-05 10:00) 0.1161g/s 206.0p/s 629.2c/s 629.2C/s mech..sss  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed
```

El último proceso será intentar la localización de las contraseñas por fuerza bruta. El proceso lo iniciamos con el comando que vemos en pantalla y durante horas buscara todas las combinaciones posibles para cada contraseña. Como vemos en la imagen lleva ya casi 2 horas de trabajo y no ha podido averiguar ninguna de las contraseñas. Sería necesario el trabajo de varias horas o incluso días para descifrarlas.



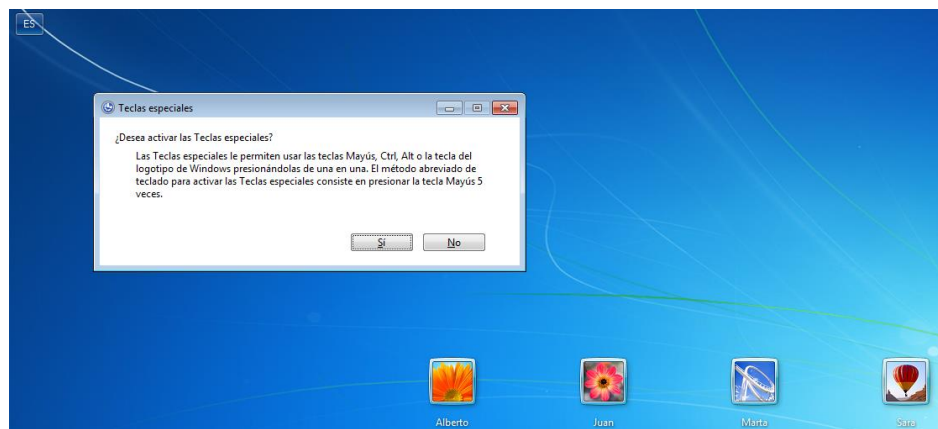
```
Aplicaciones Lugares Terminal mar 11:54  
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# john --incremental /etc/shadow  
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"  
Use the "--format=crypt" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/  
128 AVX 2x])  
Remaining 3 password hashes with 3 different salts  
Press 'q' or Ctrl-C to abort, almost any other key for status  
0g 0:00:00:08 0g/s 199.2p/s 605.5c/s 605.5C/s amars..199955  
0g 0:00:00:12 0g/s 202.1p/s 611.4c/s 611.4C/s 12305..10189  
0g 0:00:05:45 0g/s 219.5p/s 658.9c/s 658.9C/s micalo..milis2  
0g 0:00:32:09 0g/s 224.2p/s 672.8c/s 672.8C/s boyakz..bommmc  
0g 0:00:46:04 0g/s 219.8p/s 659.6c/s 659.6C/s sexx!..setrn  
0g 0:01:02:58 0g/s 221.0p/s 663.0c/s 663.0C/s 251897..252319  
0g 0:01:11:24 0g/s 221.4p/s 664.4c/s 664.4C/s mmss00..mms245  
0g 0:01:50:43 0g/s 223.5p/s 670.7c/s 670.7C/s 2644al..2669mg
```

b. Modificación de contraseñas.

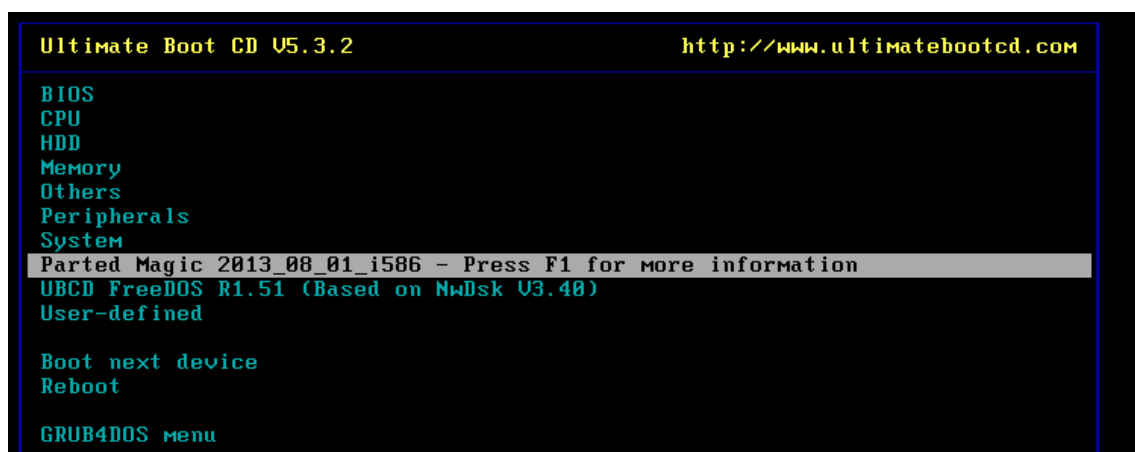
En esta parte de la práctica no queremos averiguar las contraseñas de los usuarios sino que vamos a utilizar 2 herramientas para entrar en el sistema y modificar las contraseñas del usuario que queramos para poder acceder a su sesión con una nueva contraseña.

Ultimate Boot CD

Vamos a utilizar el LiveCD de Ultimate Boot CD para modificar el StickyKeys y que al pulsar la tecla SHIFT 5 veces en el inicio de sesión se nos abra el terminal. Como vemos en la imagen se nos abre una ventana de teclas especiales y eso es precisamente lo que queremos modificar.



Para empezar tenemos que iniciar desde la unidad de CD, cuando inicie el programa seleccionamos la opción que se puede ver en la imagen para que inicie el sistema operativo con el entorno gráfico.



Una vez se inicia abriremos un terminal desde el que vamos a montar la partición. Como vemos en la imagen nos muestra las particiones y después le indicamos donde la queremos montar para poder trabajar con los archivos. Por ultimo vemos como ya nos ha montado la partición y nos enseña las carpetas de Windows.

```
ROXTerm
root@partedmagic:~# fdisk -l

Disk /dev/sda: 64.4 GB, 64424509440 bytes, 125829120 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Identificador del disco: 0xd8db0818

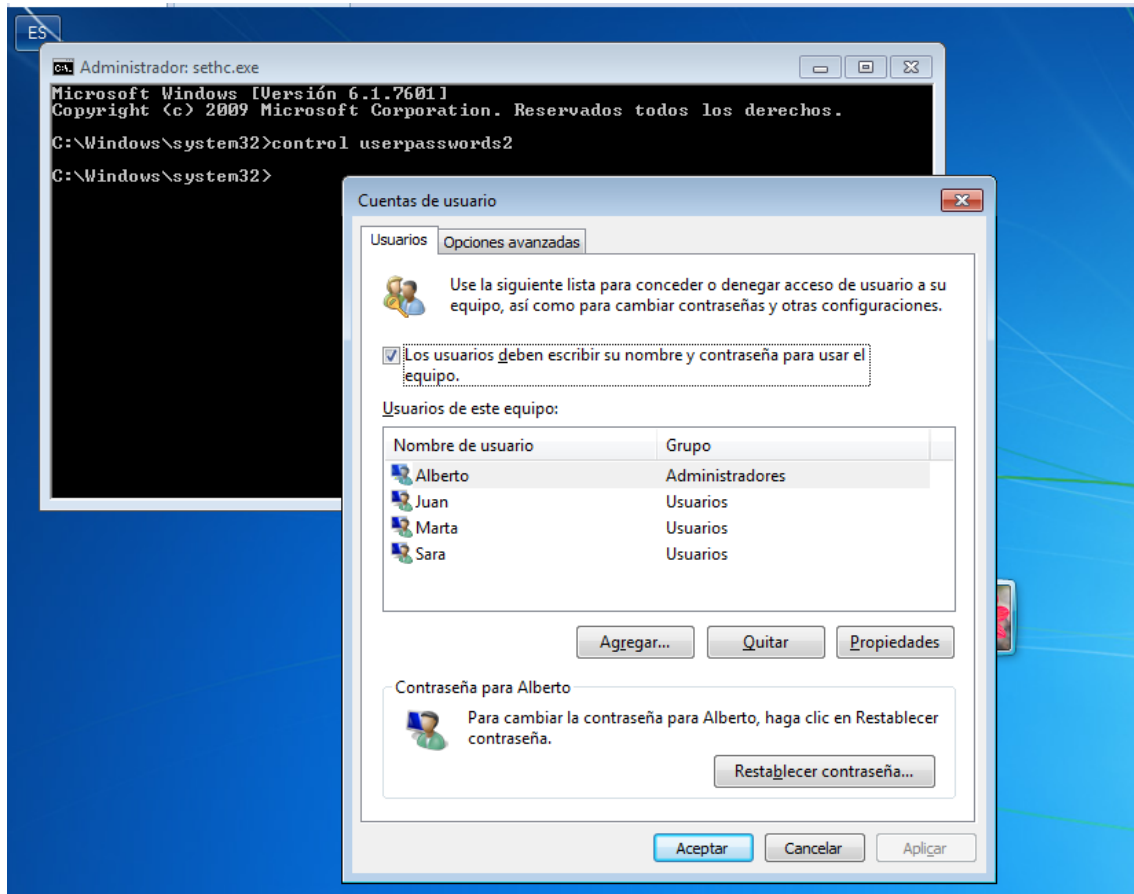
Disposit. Inicio    Comienzo      Fin          Bloques  Id Sistema
/dev/sda1 *        2048          206847       102400   7  HPFS/NTFS/exFAT
/dev/sda2          206848       125827071    62810112  7  HPFS/NTFS/exFAT

root@partedmagic:~# ls /media/
sda1 sda2 sr0
root@partedmagic:~# mount /dev/sda2 /media/sda2/
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
root@partedmagic:~# ls /media/sda2/
$Recycle.Bin      MS0Cache          ProgramData        Windows
Archivos de programa  PerfLogs          Recovery           pagefile.sys
DeltaCopy         Program Files      System Volume Information
Documents and Settings  Program Files (x86)  Users
root@partedmagic:~#
```

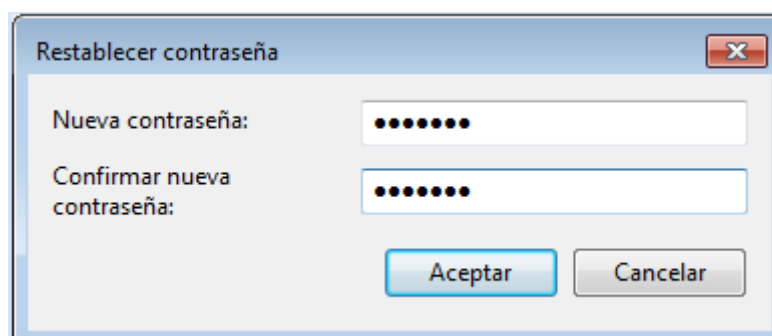
Lo siguiente que hacemos es entrar en la ruta que guarda el archivo sethc.exe el cual se ejecuta al pulsar 5 veces la tecla SHIFT y el cmd.exe que abre el terminal. Cuando estemos en la ruta vamos a cambiar el nombre del archivo cmd.exe por el de sethc.exe lo cual no permitirá que al realizar las pulsaciones nos abra el terminal.

```
ROXTerm
root@partedmagic:~# cd /media/sda2/Windows/System32/
root@partedmagic:/media/sda2/Windows/System32# ls sethc.exe
sethc.exe
root@partedmagic:/media/sda2/Windows/System32# cp sethc.exe sethc_bueno.exe
root@partedmagic:/media/sda2/Windows/System32# mv cmd.exe sethc.exe
mv: ¿sobreescribir «sethc.exe»? (s/n) s
root@partedmagic:/media/sda2/Windows/System32#
```

Reiniciamos el equipo y comprobamos que al pulsar la tecla 5 veces nos abre un nuevo terminal. Dentro del terminal usaremos el comando `control userpassword2` para que nos abra una ventana desde la que podemos crear usuarios, modificar los existentes y cambiar la contraseña. Nosotros elegimos el usuario Alberto y pulsamos en la parte de debajo de restablecer contraseña.



Esta opción nos abrirá una ventana en la que nos pide la nueva contraseña que queremos configurar para ese usuario. Pondremos la contraseña deseada y reiniciaremos la máquina con el sistema operativo.



Como podemos observar iniciamos la sesión con el usuario Alberto y en el hemos utilizado la contraseña configurada en el paso anterior.

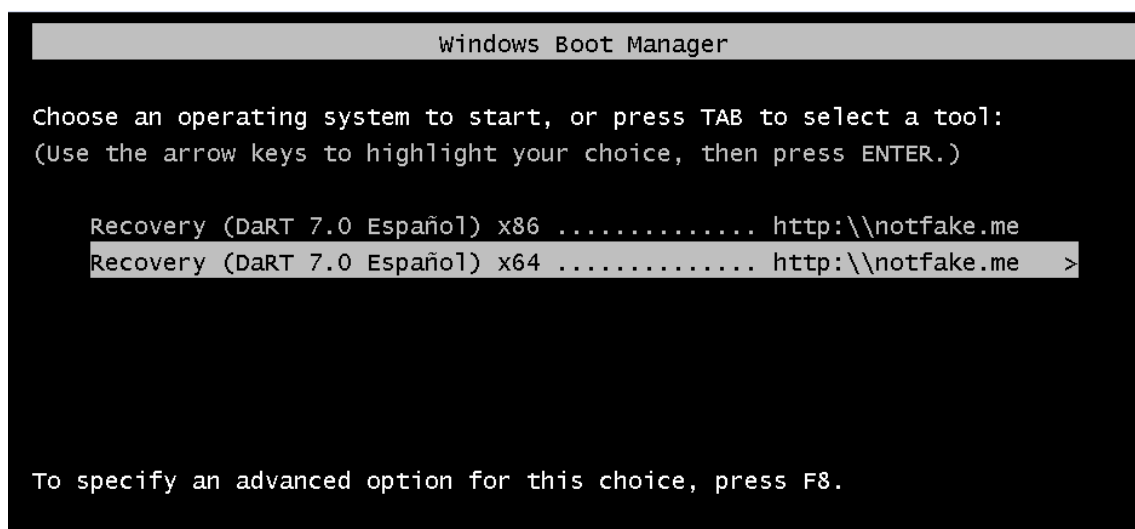


ERD Commander.

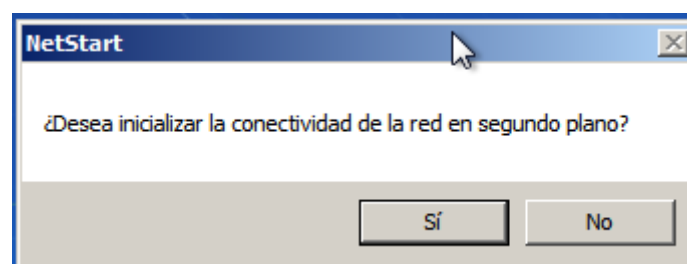
Ahora vamos a realizar un proceso parecido para modificar las contraseñas. En este caso vamos a utilizar una herramienta de Windows utilizada para mantenimiento de equipos averiados.

Esta herramienta trabaja también como un LiveCD y por lo tanto iniciaremos el equipo desde la unidad de CD para que nos arranque la herramienta.

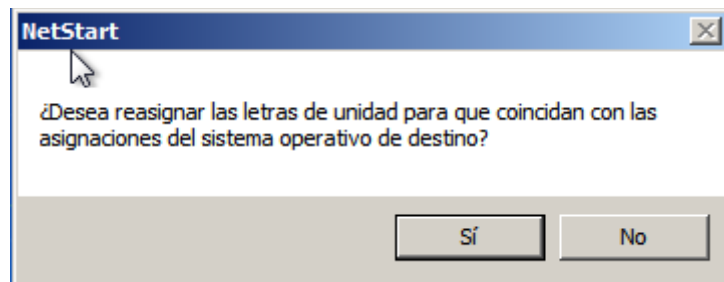
Se nos iniciara en una primera ventana en la cual elegiremos arrancar en versión x64.



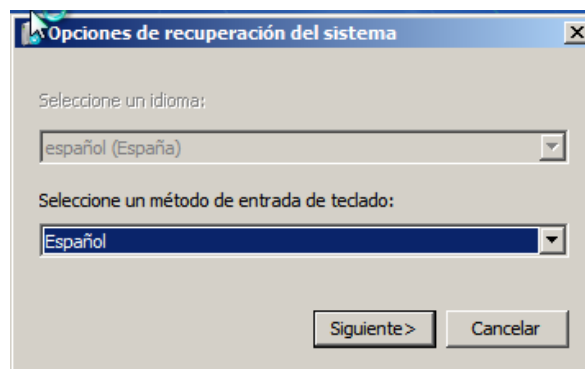
Cuando inicie tenemos que configurar varias opciones. La primera de las opciones es iniciar la red en segundo plano para la cual indicaremos que si aunque no influye en nuestro objetivo.



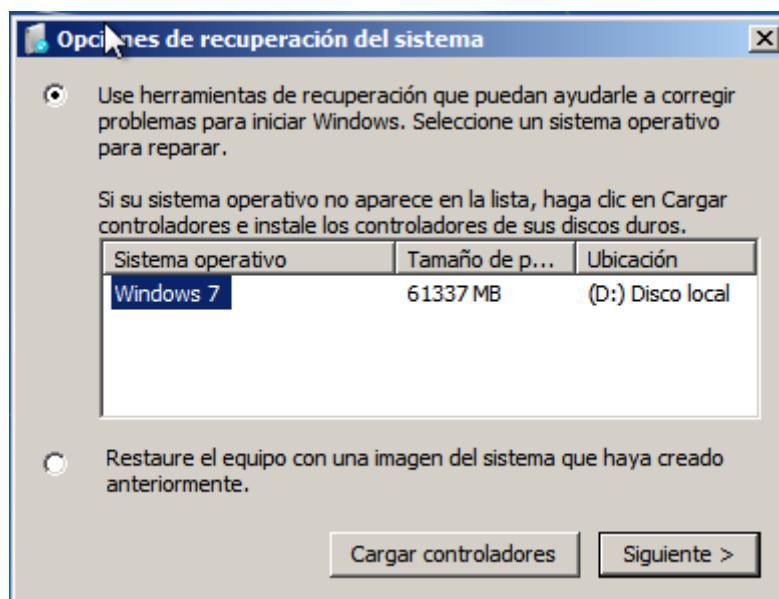
Después nos pedirá si coincidir las letras de unidad, volveremos a indicar sí.



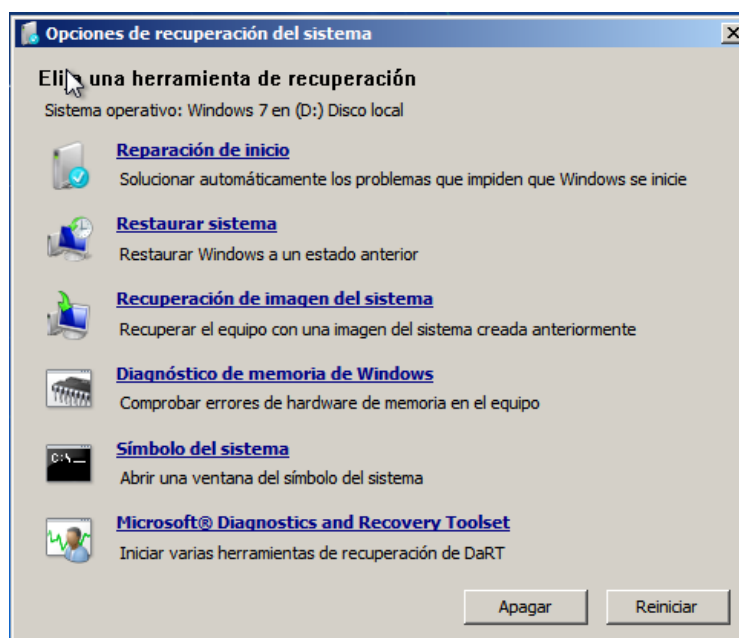
Ahora nos pide especificar el idioma de entrada de teclado. Detecta por defecto el idioma español y también te deja por defecto el idioma español del teclado.



Después nos analizará el disco duro en busca del sistema operativo instalado. Cuando termine podremos ver que tenemos el windows7 para la cual lo seleccionaremos y daremos en siguiente.



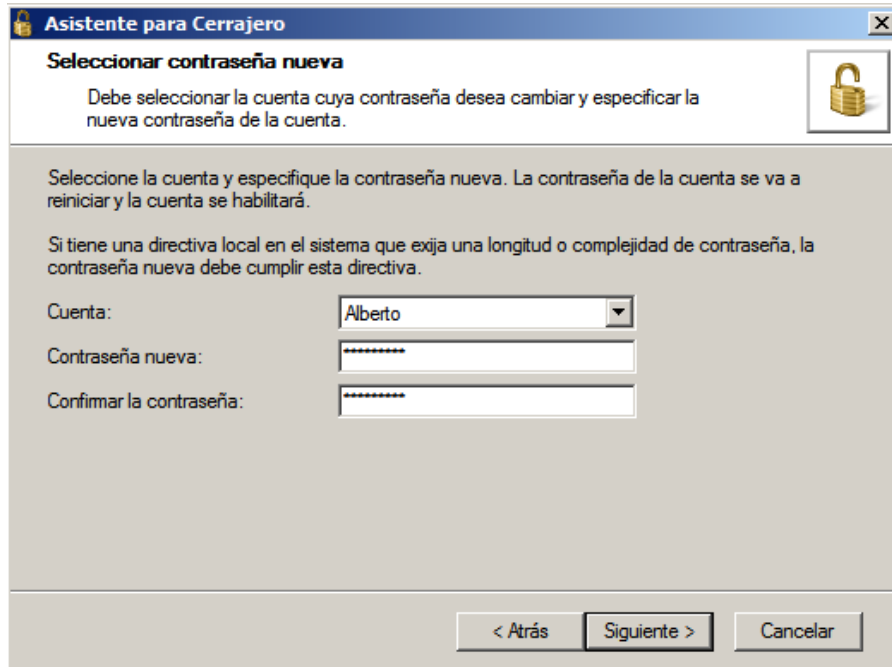
Se nos abrirá la venta principal de recuperación en la cual podemos ver diferentes opciones para reparar posibles errores del sistema. Nosotros elegiremos la última opción que consta de varias herramientas.



Como vemos en la imagen se nos abre una nueva ventana con diferentes opciones para posibles necesidades de errores que tengamos sistema. Nosotros elegiremos la segunda opción de cerrajero que no permite restablecer la contraseña de las cuentas locales.



Se nos iniciara un asistente en el cual tenemos que indicar una nueva contraseña para este usuario.



Cuando reiniciamos el equipo normalmente nos pedirá la nueva contraseña y se abrirá la opción de restablecer la contraseña. Tendremos que introducir la contraseña configurada en el asistente y después introducir una nueva contraseña. Básicamente este proceso lo que realiza es rehabilitar el usuario y pedir que se modifique la contraseña en el primer inicio de sesión.



Una vez realizamos los diferentes pasos vemos que hemos iniciado sesión nuevamente con la contraseña especificado en el paso anterior.



3. Conclusión.

En la realización de esta práctica hemos podido comprobar la importancia de elegir una buena para evitar el inicio de sesión en nuestro sistema operativo.

Como hemos podido comprobar cualquier programa es capaz de averiguar la contraseña que coincide con el nombre de usuario dado que es lo primero que comprueban estas herramientas.

Después hemos podido comprobar que con el uso de unos diccionarios y con algo de tiempo los programas son también capaces de averiguar otras contraseñas numéricas o alfanuméricas.

Por lo tanto hemos podido averiguar que para tener la mayor protección es mejor usar una contraseña alfanumérica, que utilice mayúsculas y minúsculas y además utilizar algún carácter especial como una @, punto u otro tipo.

4. Bibliografía.

Software.

- a. VMWare Workstation Pro 12.
- b. Máquina virtual con Windows 7.
- c. Máquina virtual con Kali Linux.
- **Recuperación de contraseñas.**
 - d. Ophcrack para Windows.
 - e. John de Ripper Kali Linux.
- **Sustitución de contraseñas**
 - f. ERD Commander
 - g. Ultimate Boot CD

Documentación.

- h. Diferentes pdf entregados en clase.
- i. Diferentes webs.