

TEMA 2

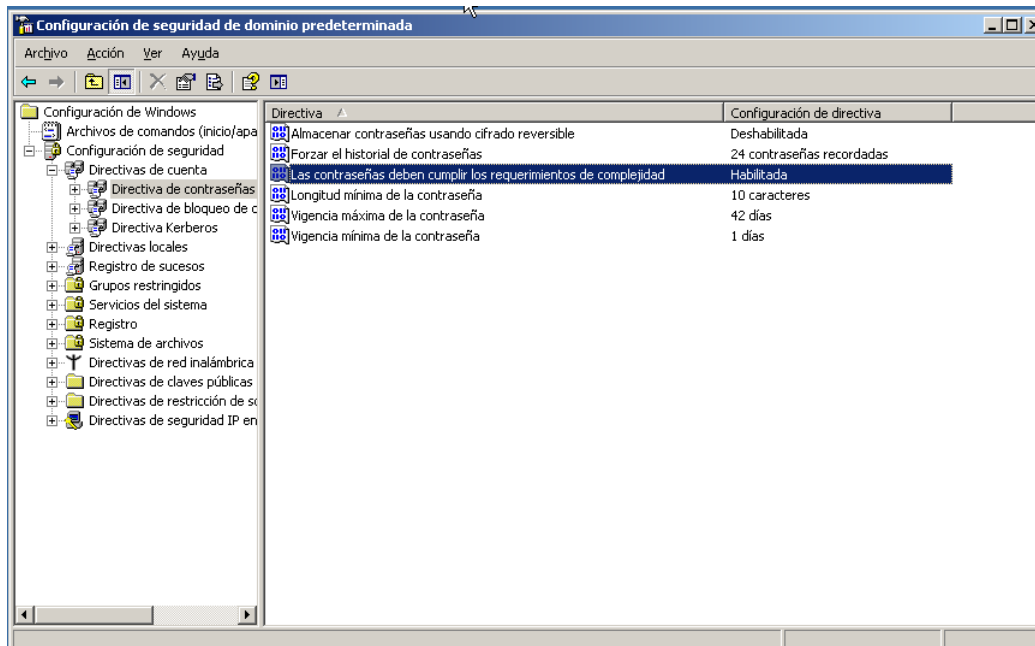
HERRAMIENTAS

PREVENTIVAS

a) Configuración de contraseñas seguras:

- En Windows: Políticas de directivas de cuentas.
- En GNU/Linux: Módulo pam_cracklib.

Vamos a hacer una política de directivas de cuentas, para ellos nos vamos a Editor de objetos de directiva de grupo y en Configuración del equipo, y en configuración de Windows, encontramos Configuración de seguridad, nos vamos a Directivas de cuenta y directivas de contraseña, ahí elegimos la longitud mínima que queremos que tenga la contraseña y vamos a poner 10 caracteres.



Y vamos también a habilitar que las contraseñas cumplan los requerimientos de complejidad

En Linux lo que tenemos que hacer es ir al fichero Common-password que encontramos en /etc/pam.d y ahí lo que hacemos es que podemos cambiar la contraseña y ponerle la política de usuario

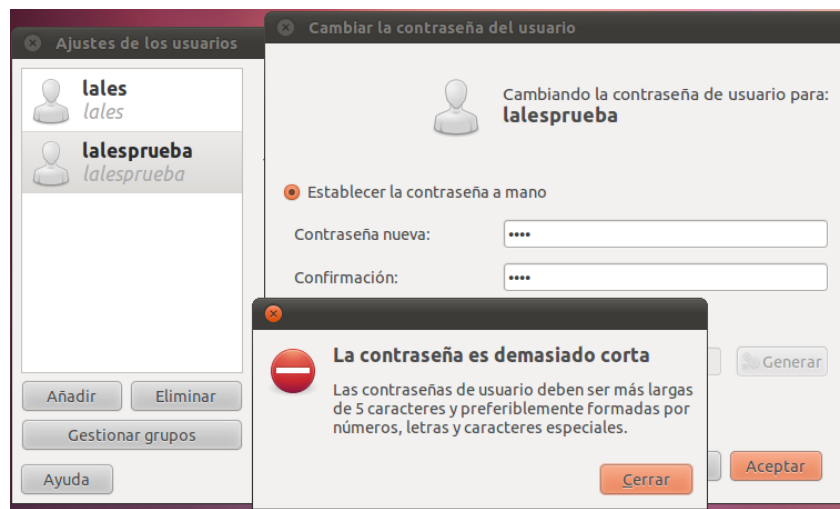
```
root@lales-virtual-machine: /home/lales
GNU nano 2.2.6 Archivo: /etc/pam.d/common-password

# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
password optional pam_gnome_keyring.so
# end of pam-auth-update config

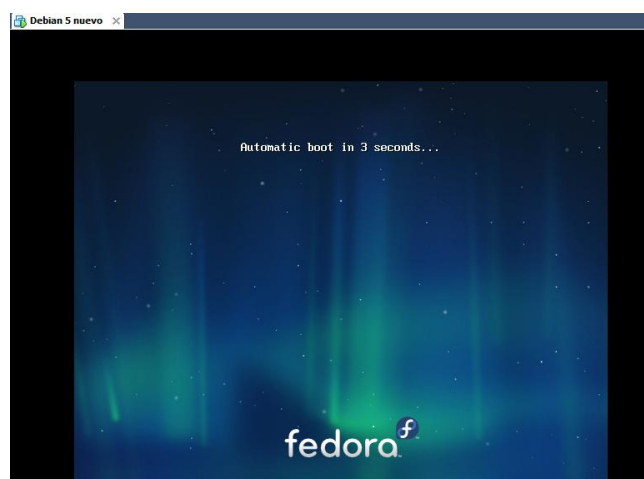
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^L Justificar ^W Buscar ^V Pág. Sig ^U ReparTxt ^T Ortografía
```

Ahora lo que vamos a hacer es crear un usuario con una contraseña corta, y vemos como nos dice que se necesita una más larga, mínimo 5 caracteres

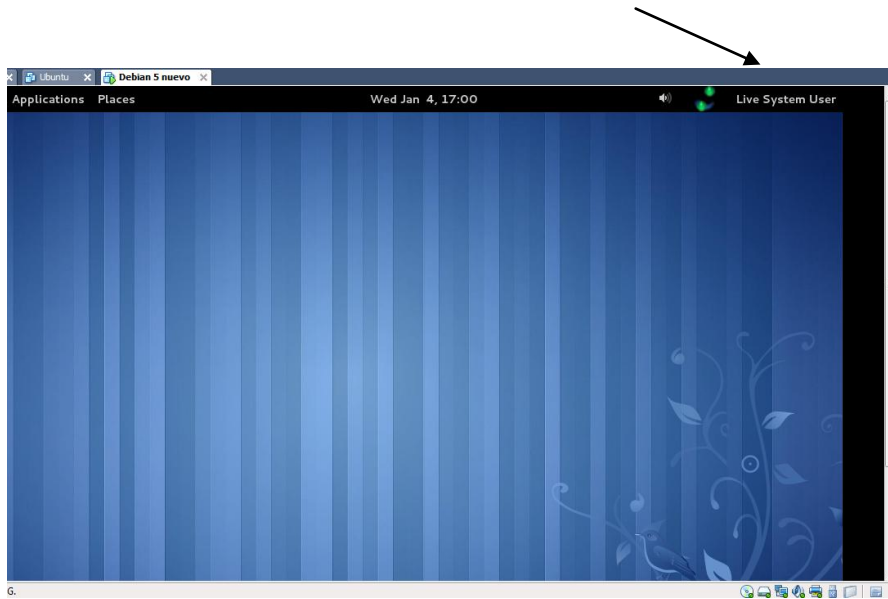


b) Peligros de distribuciones live: (Ultimate Boot CD – UBCD, Backtrack, Ophcrack, Slax, Wifiway, Wifislax).

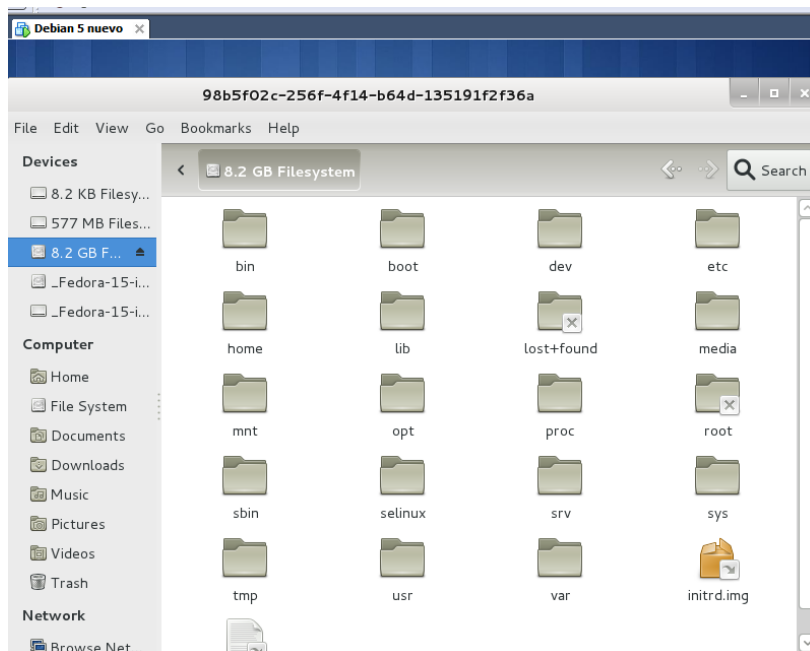
En una máquina virtual, vamos a arrancar Debian, pero con una imagen ISO de Fedora, para ello arrancamos con la imagen y nos aparece el escenario de Fedora



A continuación vemos que estamos de Live CD y nos metemos en el sistema de archivos de Debian



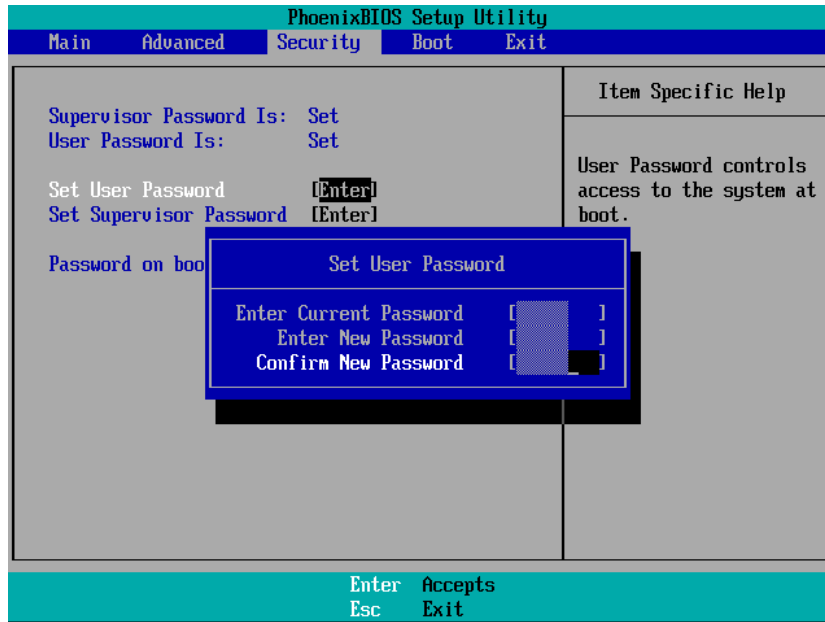
Aquí vemos que desde Fedora hemos entrado a Debian y podemos ver todas sus carpetas y archivos



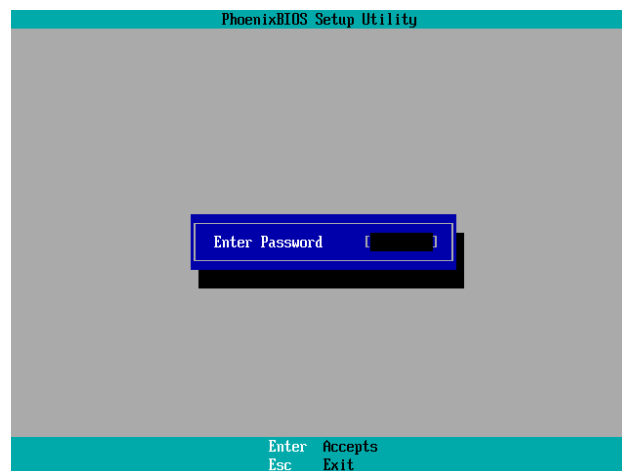
c) Configurando contraseñas en la BIOS:

- Asignar contraseña a la BIOS y observar su vulnerabilidad.

Entramos en la BIOS y nos vamos a Security, y nos pide la nueva contraseña



Luego volvemos a entrar en la BIOS y nos pone un cuadro para poner la contraseña

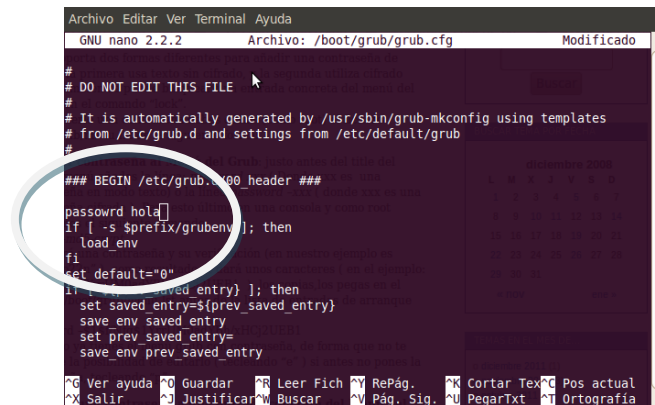


Y ya hemos entrado en la BIOS

d) Contraseñas en el gestor de arranque:

- Práctica con GRUB

Nos vamos a Linux y abrimos el fichero `/boot/grub/grub.cfg`, y ahí añadimos la palabra `password` y a continuación ponemos la contraseña que queremos, ahí guardamos y ya tenemos contraseña en el Grub



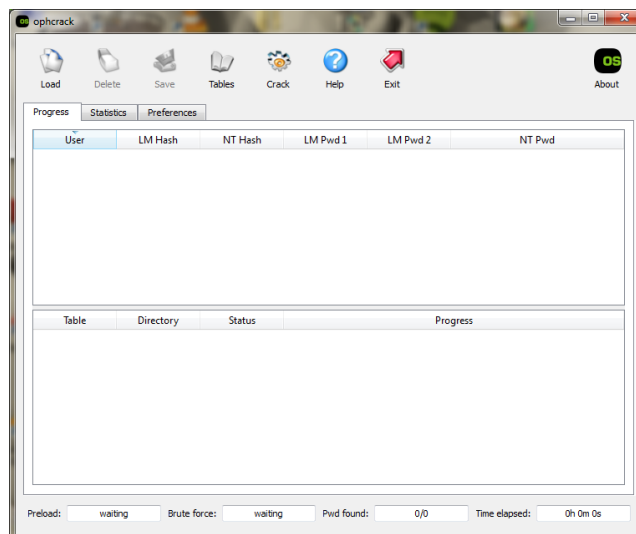
```
GNU nano 2.2.2 Archivo: /boot/grub/grub.cfg Modificado
#
# DO NOT EDIT THIS FILE
#
# It is automatically generated by /usr/sbin/grub-mkconfig using templates
# from /etc/grub.d and settings from /etc/default/grub
#
### BEGIN /etc/grub.d/00_header ###
password hold[]
if [ -s $prefix/grubenv ]; then
  load_env
fi
set default="0"
if [ -s $saved_entry ]; then
  set saved_entry=${prev_saved_entry}
  save_env saved_entry
  set prev_saved_entry=
  save_env prev_saved_entry
```

e) Recuperación de contraseñas:

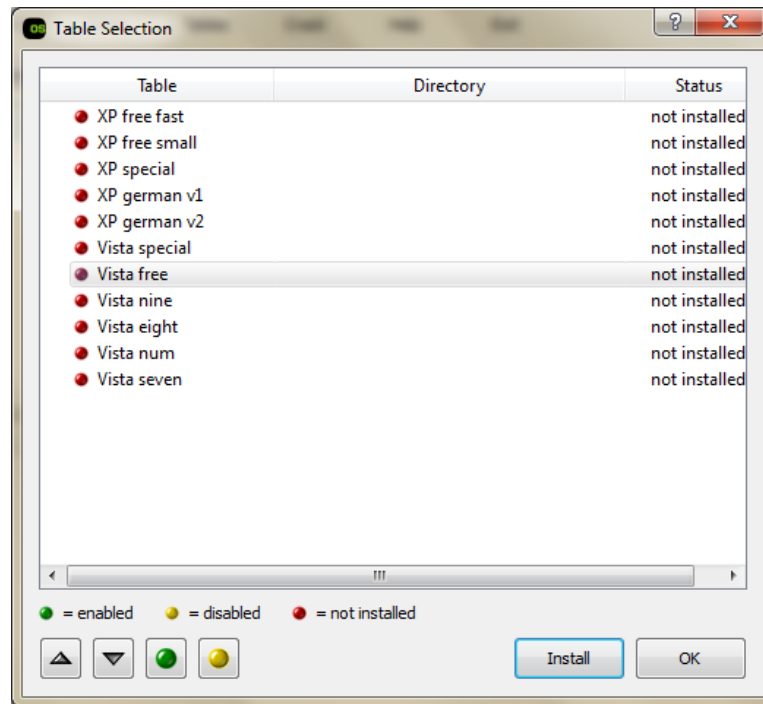
- En Windows: Ophcrack.
- En GNU/Linux: Aplicación John the Ripper.

OPHCRACK

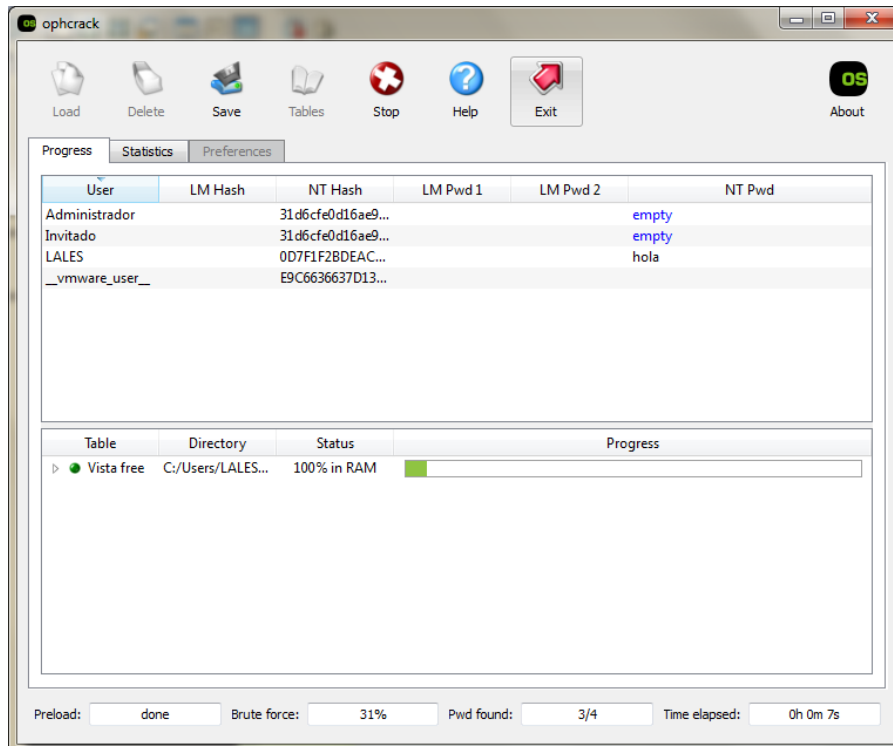
En Windows nos descargamos el programa Ophcrack y una vez descargado, le damos a la opción `tables` y buscamos donde tenemos las tablas guardadas



Nos aparece esta pantalla y le damos a vista free y las buscamos la ruta donde las tenemos



Cuando ya las tenemos las tablas metidas, le damos a Crack y empieza el análisis y nos muestra la contraseña de nuestro usuario.



JOHN DE RIPPER

Nos descargamos el programa por medio del siguiente comando
Apt-get install John

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
root@lales-virtual-machine:/home/lales#
root@lales-virtual-machine:/home/lales#
root@lales-virtual-machine:/home/lales#
root@lales-virtual-machine:/home/lales#
root@lales-virtual-machine:/home/lales# sudo aptitude install john
sudo: aptitude: command not found
root@lales-virtual-machine:/home/lales# apt-get install john
leyendo lista de paquetes... Hecho
creando árbol de dependencias
leyendo la información de estado... Hecho
los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
linux-headers-2.6.38-8 linux-headers-2.6.38-8-generic
utilice «apt-get autoremove» para eliminarlos.
se instalarán los siguientes paquetes extras:
 john-data
se instalarán los siguientes paquetes NUEVOS:
 john john-data
0 actualizados, 2 se instalarán, 0 para eliminar y 16 no actualizados.
Necesito descargar 939 kB de archivos.
Se utilizarán 1888 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?
```

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
john-data
Se instalarán los siguientes paquetes NUEVOS:
 john john-data
0 actualizados, 2 se instalarán, 0 para eliminar y 16 no actualizados.
Necesito descargar 939 kB de archivos.
Se utilizarán 1888 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
Des:1 http://es.archive.ubuntu.com/ubuntu/ natty/main john-data all 1.7.3.1-1 [649 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu/ natty/main john i386 1.7.3.1-1 [291 kB]
Descargados 939 kB en 6seg. (135 kB/s)
Seleccionando el paquete john-data previamente no seleccionado.
(Leyendo la base de datos ... 162120 ficheros o directorios instalados actualmente.)
Desempaquetando john-data (de .../john-data 1.7.3.1-1 all.deb) ...
Seleccionando el paquete john previamente no seleccionado.
Desempaquetando john (de .../john 1.7.3.1-1 i386.deb) ...
Procesando disparadores para man-db ...
Configurando john-data (1.7.3.1-1) ...
Configurando john (1.7.3.1-1) ...
root@lales-virtual-machine:/home/lales#
```

Una vez instalado creamos un fichero de la unión del fichero /etc/passwd y /etc/shadow y le llamamos passwordslales

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
john john-data
0 actualizados, 2 se instalarán, 0 para eliminar y 16 no actualizados.
Necesito descargar 939 kB de archivos.
Se utilizarán 1888 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
Des:1 http://es.archive.ubuntu.com/ubuntu/ natty/main john-data all 1.7.3.1-1 [649 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu/ natty/main john i386 1.7.3.1-1 [291 kB]
Descargados 939 kB en 6seg. (135 kB/s)
Seleccionando el paquete john-data previamente no seleccionado.
(Leyendo la base de datos ... 162120 ficheros o directorios instalados actualmente.)
Desempaquetando john-data (de .../john-data 1.7.3.1-1 all.deb) ...
Seleccionando el paquete john previamente no seleccionado.
Desempaquetando john (de .../john 1.7.3.1-1 i386.deb) ...
Procesando disparadores para man-db ...
Configurando john-data (1.7.3.1-1) ...
Configurando john (1.7.3.1-1) ...
root@lales-virtual-machine:/home/lales# unshadow /etc/passwd /etc/shadow > passwordslales
root@lales-virtual-machine:/home/lales#
```

A continuación ejecutamos john the ripper sobre el archivo que hemos creado con unshadow

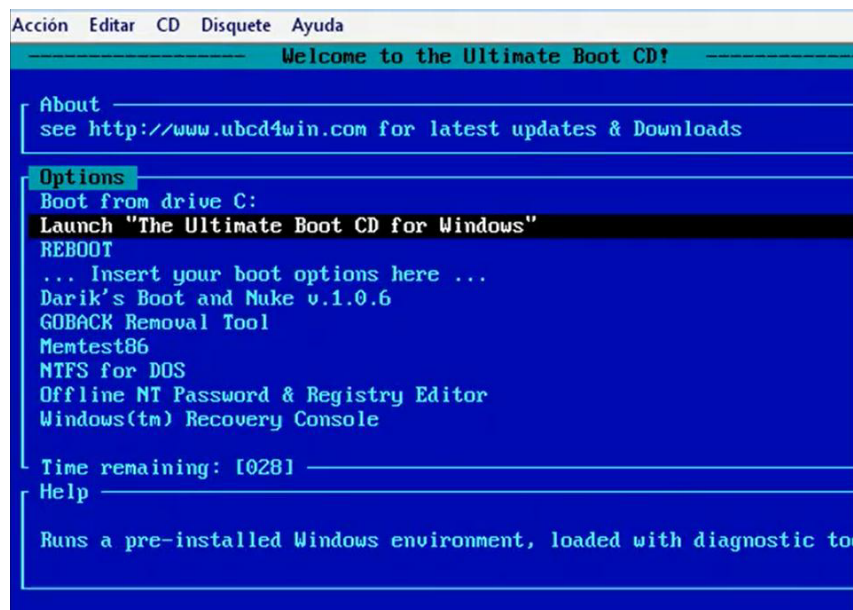
Por último introducimos john-incremental passwordslales y nos aparecerá al paso de un tiempo depende de cómo sean de complicadas, las contraseñas.

f) Modificación de contraseñas:

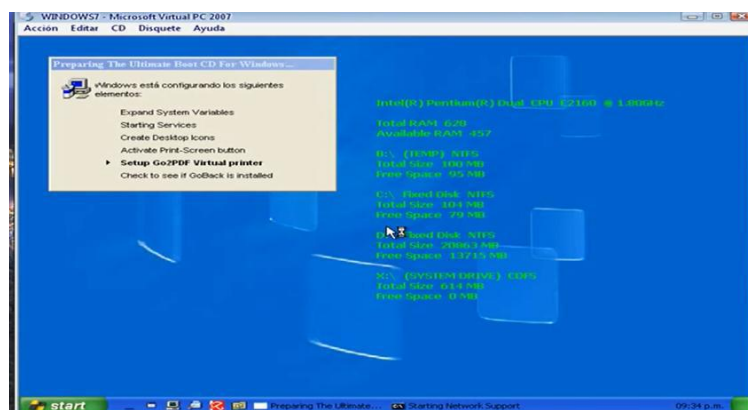
- En Windows: Distribución Live UBCD.
- En GNU/Linux: mediante el sistema, modificando /etc/shadow.

UBCD

Entramos por medio del Live CD y le damos a la opción Launch



Cuando ya hemos iniciado nos vamos a Programas y a passwd tolos, y seleccionamos C: Windows

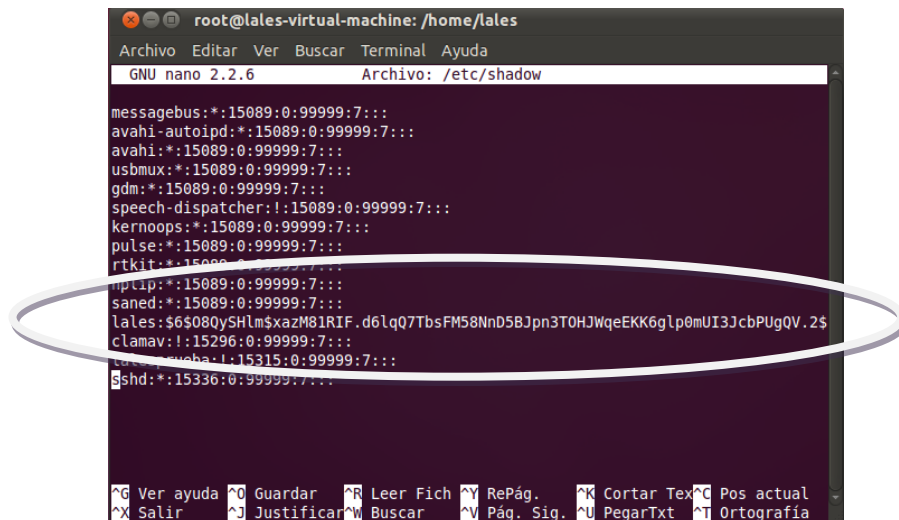


Renew existing user password, sería la siguiente opción, ponemos una contraseña y a la izquierda le damos a Install y ahí tenemos cambiada la contraseña

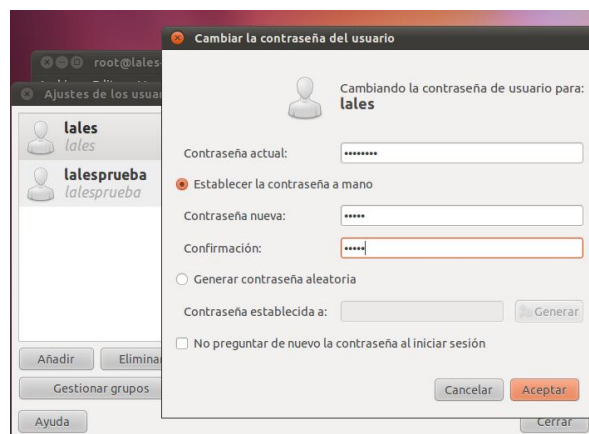


EN LINUX

En el fichero /etc/shadow, podemos ver que en la cuenta de usuario lales tenemos la contraseña encriptada



A continuación, si cambiamos la contraseña del usuario y volvemos a ir al fichero /etc/shadow, podemos ver cómo ha cambiado la contraseña



```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Archivo: /etc/shadow

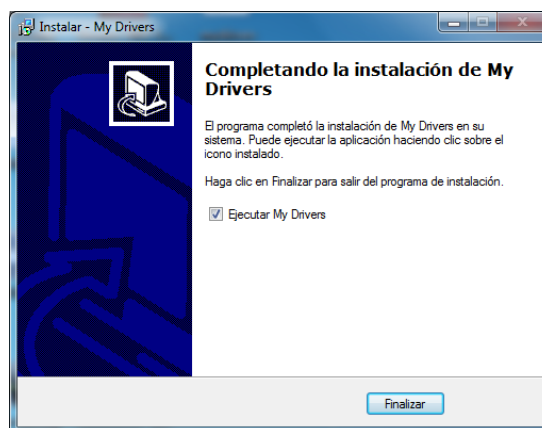
messagebus:*:15089:0:99999:7:::
avahi-autoipd:*:15089:0:99999:7:::
avahi:*:15089:0:99999:7:::
usbmux:*:15089:0:99999:7:::
gdm:*:15089:0:99999:7:::
speech-dispatcher:!:15089:0:99999:7:::
kernoops:*:15089:0:99999:7:::
pulse:*:15089:0:99999:7:::
rtkit:*:15089:0:99999:7:::
hplip:*:15089:0:99999:7:::
saned:*:15089:0:99999:7:::
lales:$6$lx3MMq4.$wQVikbrfX00NK8cjEE825JURLBfncNwpXa20KVYZ9YDKVAMFYR6LZ.d1Y5rQ$
clamav:!:15296:0:99999:7:::
lalesprueba:!:15315:0:99999:7:::
sshd:!:15336:0:99999:7:::

^G Ver ayuda ^O Guardar ^R Leer Fich ^V RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía
```

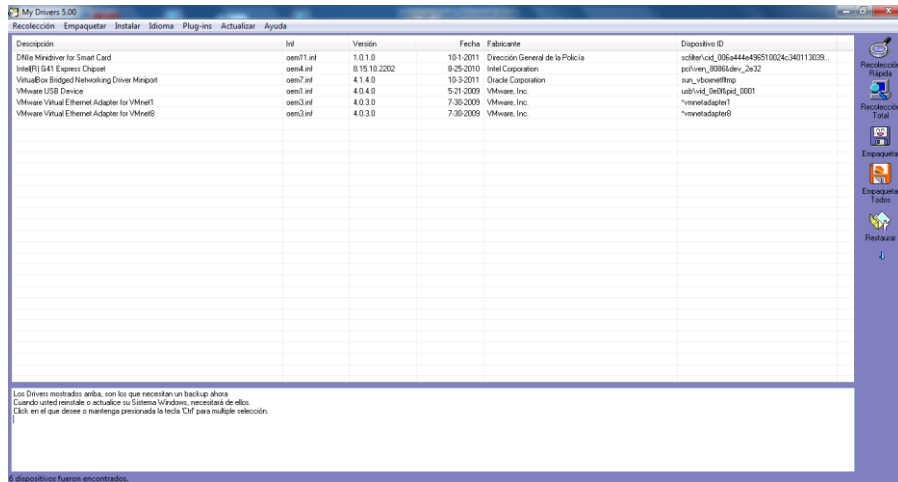
g) Realizar una copia de seguridad de drivers

- Utiliza el software “DriverMax” o similar.

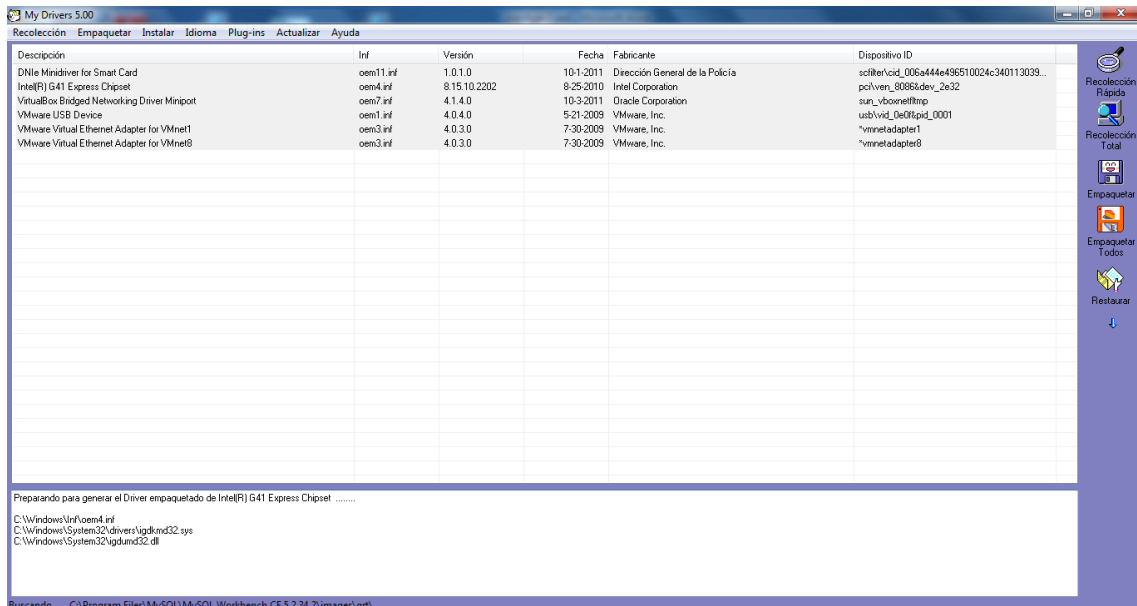
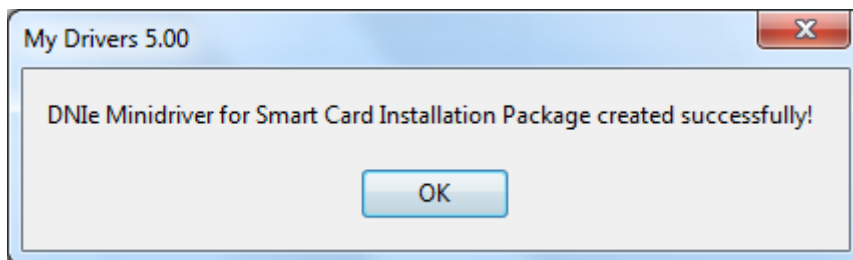
Vamos a instalar Mydrivers que es un software parecido a DriverMax y vamos a hacer una copia de seguridad de los drivers del ordenador



A continuación recopilamos todos los drives que tiene nuestro equipo y le damos a empaquetar



Nos va creando uno a uno la copia de los drivers encontrados

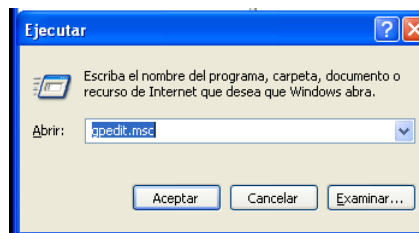


h) Control de acceso a datos y aplicaciones:

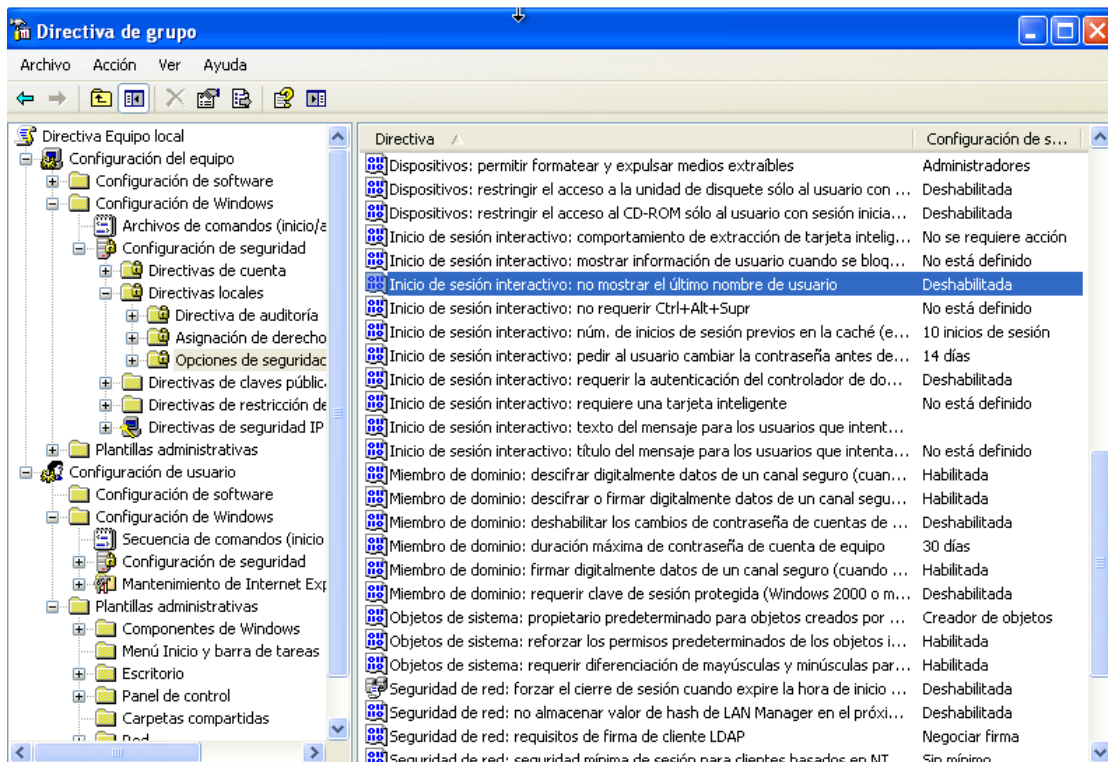
- En Windows: Política de directivas de seguridad local.
- En GNU/Linux: chmod, chown, chgrp, getfacl, setfacl.

EN WINDOWS

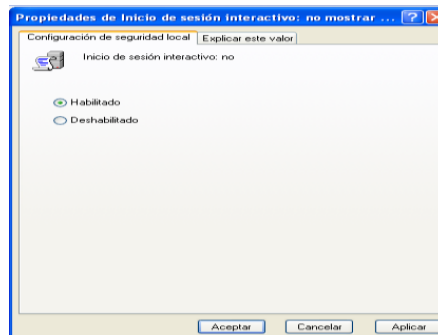
En Windows ponemos en ejecutar, gpedit.msc y nos aparece la ventana de Directivas de grupo



Ahora en Configuración del equipo, Configuración de Windows, Directivas locales y opciones de seguridad, vamos a hacer que al iniciar sesión un usuario, no aparezca el último nombre del usuario que ha entrado y lo que hacemos es que hacemos doble clic sobre esa directiva local

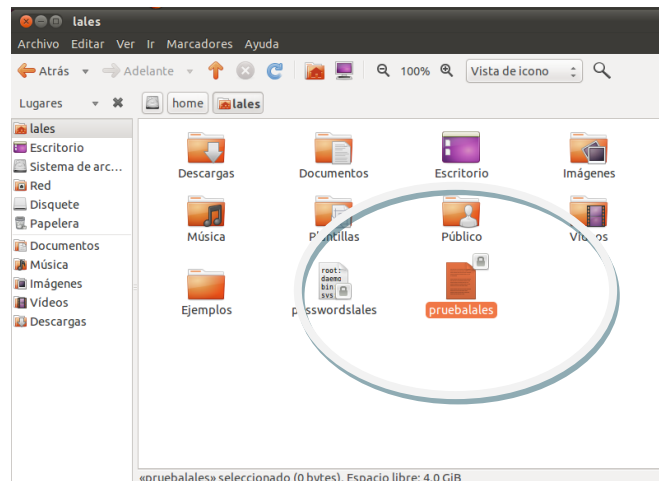


Y la habilitamos y aceptamos

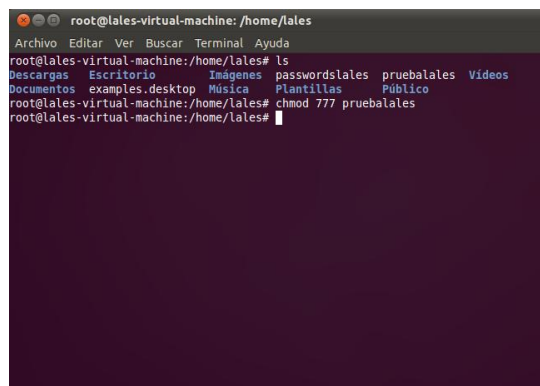


EN LINUX

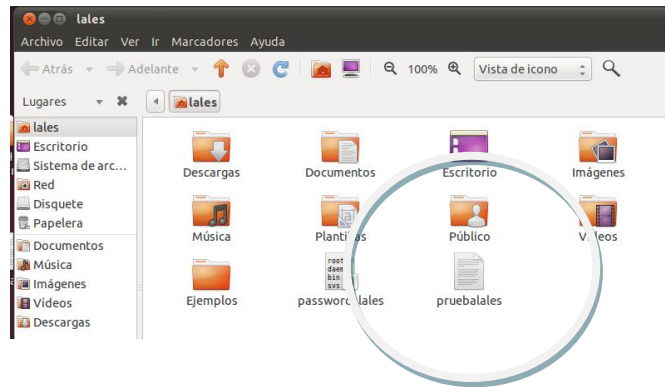
CHMOD: Hacemos un fichero en /home/lales que se llama pruebalales solamente con permisos de lectura



Y en un terminal ponemos chmod 777 pruebalales para darle todos los permisos



Y ya vemos como tiene el fichero todos los permisos



CHOWN Y CHGRP

Vamos a cambiar el usuario al que pertenece el fichero que hemos creado y vamos a cambiarlo con chown, para ello vemos que el fichero pruebalales es del usuario lales

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
root@lales-virtual-machine: /home/lales# ls
Descargas Escritorio Imágenes passwordslales pruebalales Videos
Documentos ejemplos.desktop Música Plantillas Público
root@lales-virtual-machine: /home/lales# chmod 777 pruebalales
root@lales-virtual-machine: /home/lales# ls -l
total 40
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Descargas
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Documentos
drwxr-xr-x 4 lales lales 4096 2011-12-12 10:02 Escritorio
-rw-r--r-- 1 lales lales 179 2011-09-30 13:42 ejemplos.desktop
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Imágenes
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Música
-rw-r--r-- 1 root root 1787 2012-01-05 00:27 passwordslales
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Plantillas
-rwxrwxrwx 1 lales lales 0 2012-01-05 11:59 pruebalales
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Público
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Videos
root@lales-virtual-machine: /home/lales#
```

Ahora ponemos chown lalesprueba pruebalales, y así asignamos el fichero pruebalales al usuario lalesprueba, y comprobamos que ya es de ese usuario.

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Imágenes
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Música
-rw-r--r-- 1 root root 1787 2012-01-05 00:27 passwordslales
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Plantillas
-rwxrwxrwx 1 lales lales 0 2012-01-05 11:59 pruebalales
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Público
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Videos
root@lales-virtual-machine: /home/lales# chown prueba pruebalales
chown: usuario inválido: «prueba»
root@lales-virtual-machine: /home/lales# chown lalesprueba pruebalales
root@lales-virtual-machine: /home/lales# ls -l
total 40
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Descargas
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Documentos
drwxr-xr-x 4 lales lales 4096 2011-12-12 10:02 Escritorio
-rw-r--r-- 1 lales lales 179 2011-09-30 13:42 ejemplos.desktop
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Imágenes
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Música
-rw-r--r-- 1 root root 1787 2012-01-05 00:27 passwordslales
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Plantillas
-rwxrwxrwx 1 lalesprueba lales 0 2012-01-05 11:59 pruebalales
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Público
drwxr-xr-x 2 lales lales 4096 2011-09-30 13:57 Videos
root@lales-virtual-machine: /home/lales#
```


GETFACL Y SETFACL

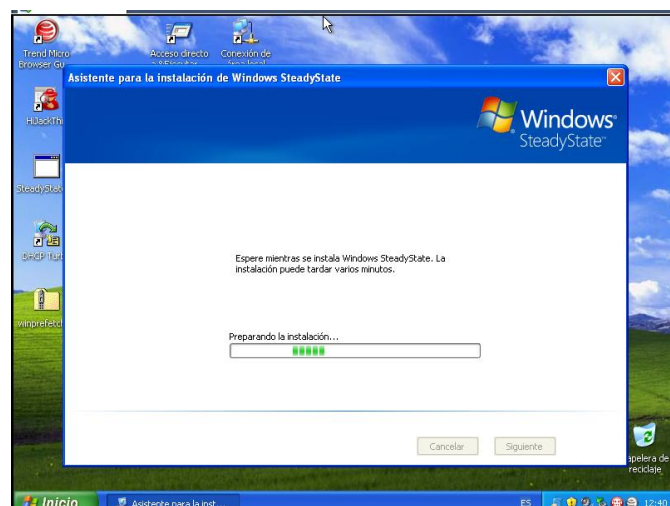
Con estos comandos vemos el propietario, grupo, permisos de una carpeta
Ponemos getfacl y el nombre de la carpeta y nos muestra la información

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
acl
0 actualizados, 1 se instalarán, 0 para eliminar y 16 no actualizados.
Necesito descargar 40,3 kB de archivos.
Se utilizarán 176 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu/ natty/main acl i386 2.2.49-4ubuntu2 [
40,3 kB]
Descargados 40,3 kB en 0seg. (41,9 kB/s)
Seleccionando el paquete acl previamente no seleccionado.
(Leyendo la base de datos ... 162170 ficheros o directorios instalados actualmen
te.)
Desempaquetando acl (de ../acl 2.2.49-4ubuntu2_i386.deb) ...
Procesando disparadores para man-db ...
Configurando acl (2.2.49-4ubuntu2) ...
root@lales-virtual-machine:/home/lales# getfacl Plantillas
# file: Plantillas
# owner: lales
# group: lales
user::rwx
group::r-x
other::r-x
root@lales-virtual-machine:/home/lales#
```

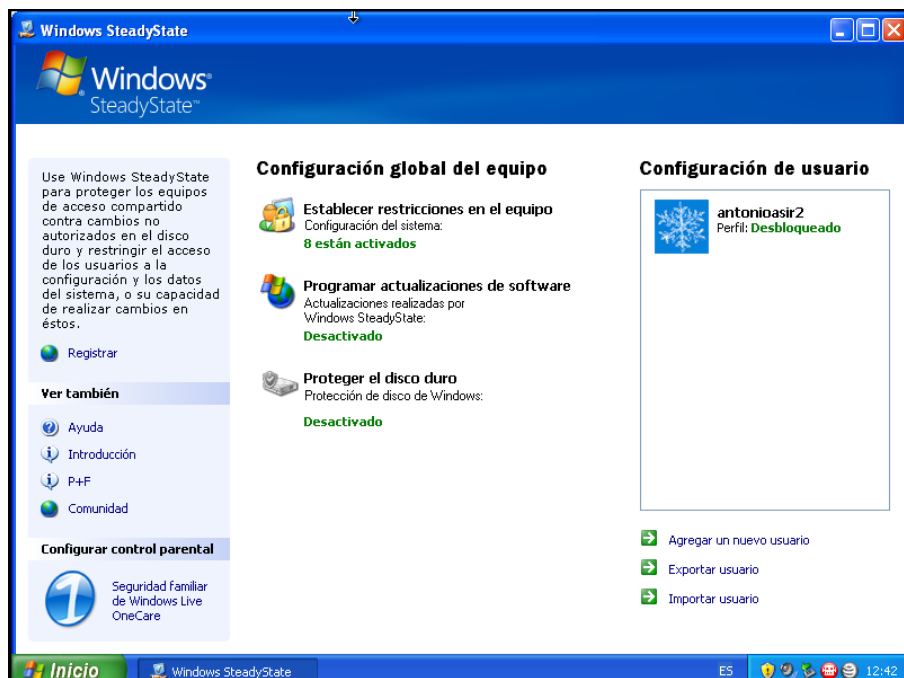
i) Utiliza el software “Windows SteadyState”, y crea un pequeño informe de las posibilidades del mismo, desde un punto de vista de seguridad informática

<http://recursostic.educacion.es/observatorio/web/es/software/software-general/785-windows-steady-state>

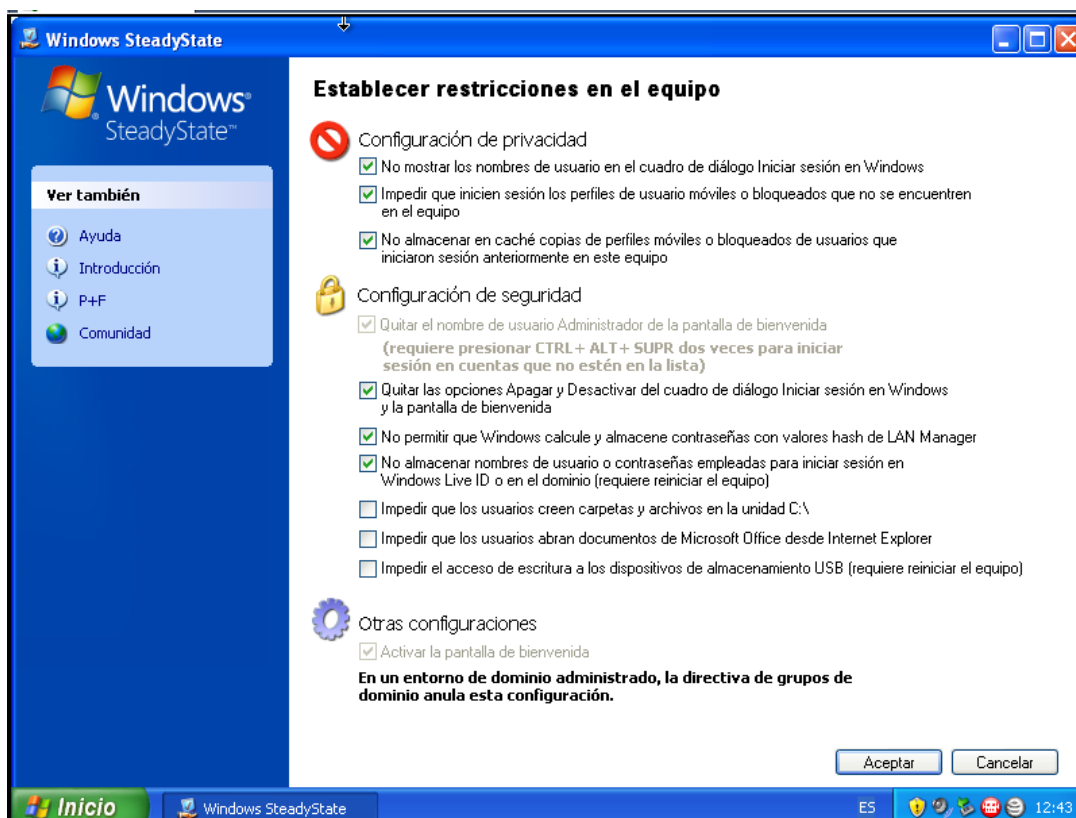
Nos descargamos el programa Windows SteadyState que nos sirve para establecer a los diferentes usuarios del sistema una serie de restricciones



Una vez descargado, nos vamos a configuración global del equipo y nos pone que hay 8 usuarios que pueden entrar a él

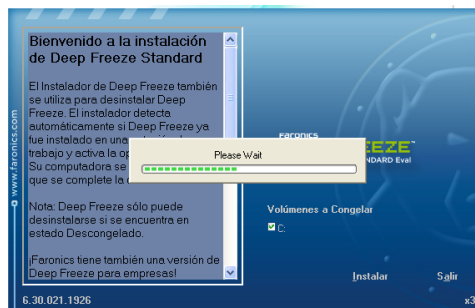


Ahí podemos cambiar la configuración de privacidad y de seguridad, para que no todos los usuarios tengan acceso y puedan modificar las opciones de Windows

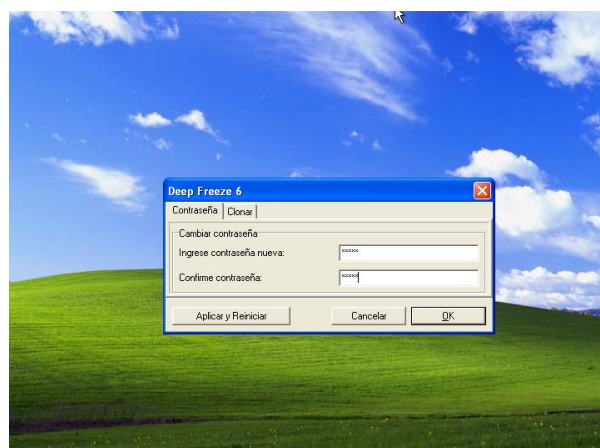


j) Busca aplicaciones “congelador” disponibles para Windows y GNU/Linux como “DeepFreeze”. Indica que protección ofrecen.

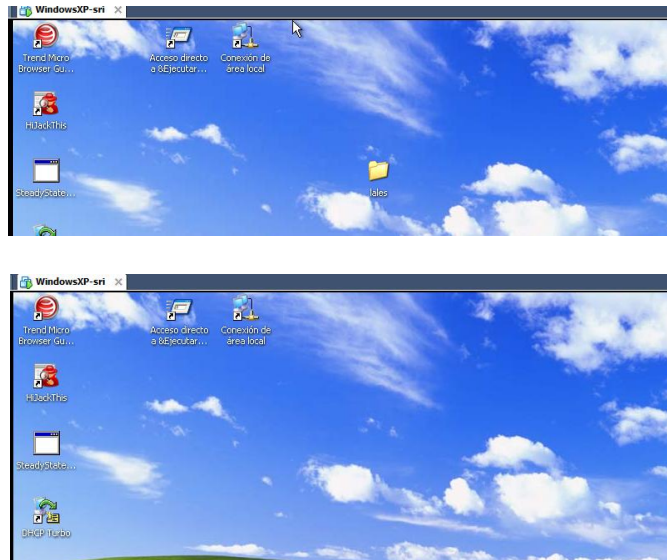
Nos descargamos DeepFreeze, que nos permite congelar el disco duro y así todo lo que hagamos durante la sesión se borrará cuando salgamos de esta



Una vez descargado nos pide una contraseña para poder activarlo o desactivarlo cuando queramos, importante recordarla porque si no, sería muy difícil poder desactivar este programa, ya que está activo siempre que estés en la sesión



Creamos una carpeta en el escritorio y al salir de la sesión, cuando volvemos a ella vemos que no está, ya que todo lo que hemos hecho en esa sesión desaparece

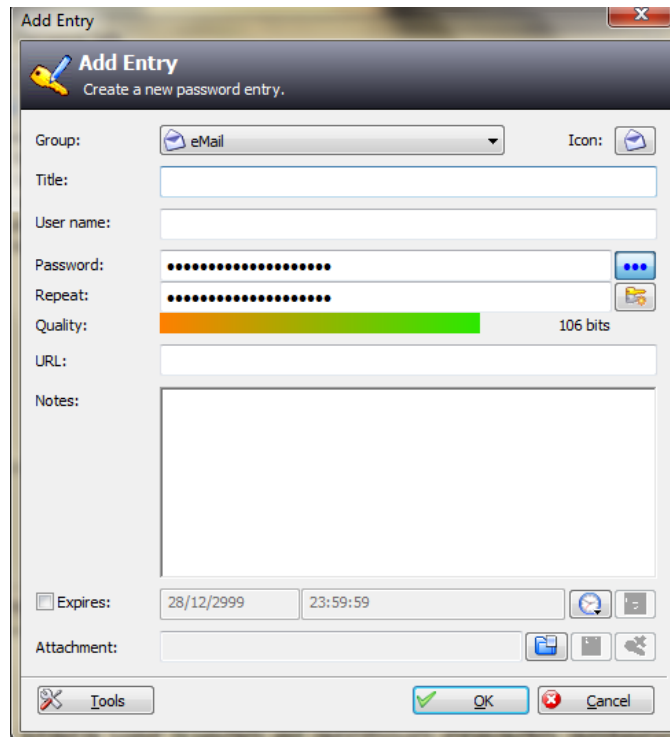


k) Utiliza el software “Keepass Password Safe”, y crea un pequeño informe de las posibilidades del mismo, desde un punto de vista de seguridad informática.

Descargamos el programa y vemos que nos pide esta contraseña, esta contraseña es la que debemos de recordar siempre, ya que es la clave para poder entrar al programa donde tenemos guardadas todas las demás



Vamos a guardar por ejemplo una contraseña de una cuenta de correo, para ellos hacemos añadir entrada de correo y nos pide los datos, ponemos la contraseña que tenemos en ese correo electrónico



Y ya tenemos añadido el correo con la contraseña para hacer uso de ella cuando nos haga falta, sin necesidad de recordarla

