TEMA 2

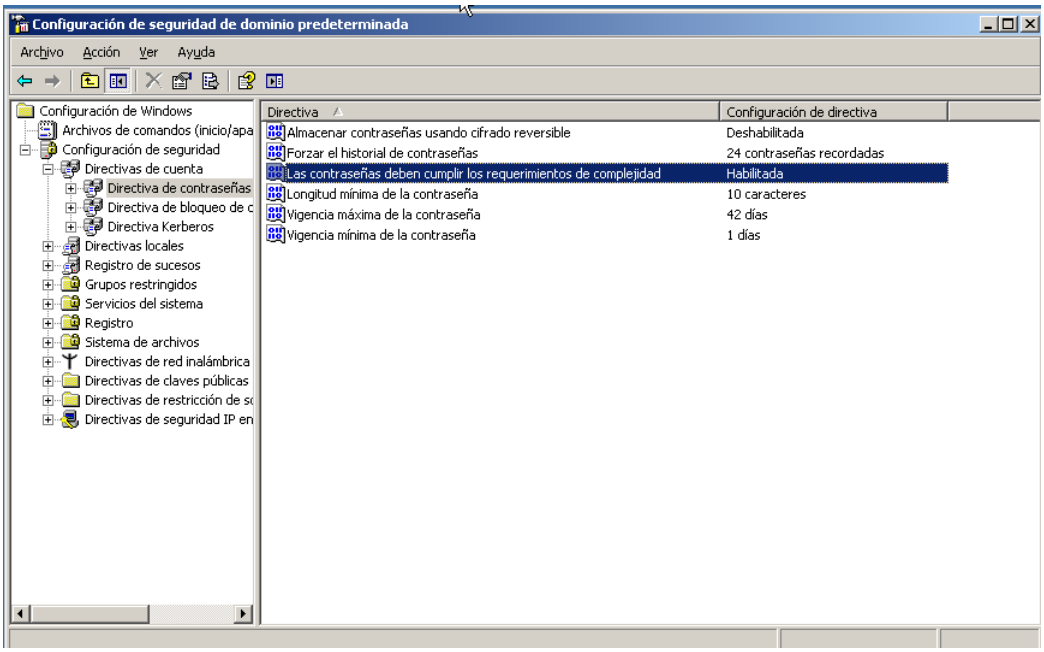
HERRAMIENTAS PREVENTIVAS

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- 2º ASIR-TEMA 2-SAD

a) **Configuración de contraseñas seguras:**

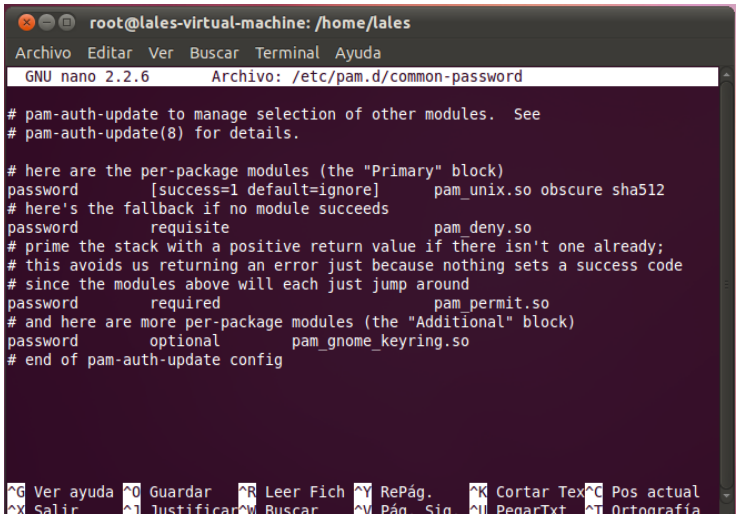
- En Windows: Políticas de directivas de cuentas.
- En GNU/Linux: Módulo pam_cracklib.

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

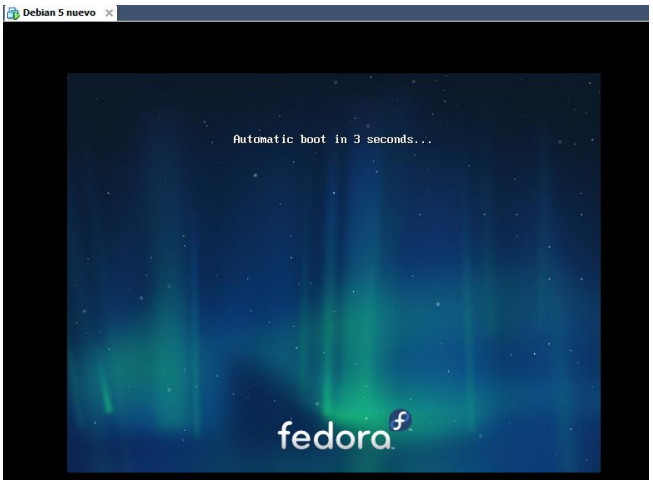
En Linux lo que tenemos que hacer es ir al fichero Common-password que encontramos en /etc/pam.d y ahí lo que hacemos es que podemos cambiar la contraseña y ponerle la política de usuario



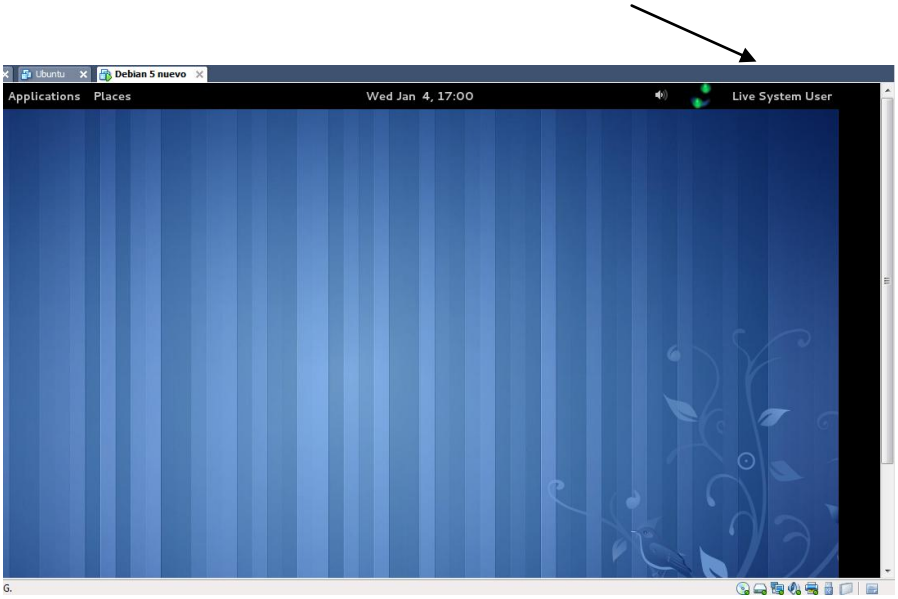
Ahora lo que vamos a hacer es crear un usuario con una contraseña corta, y vemos como nos dice que se necesita una más larga, mínimo 5 caracteres

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

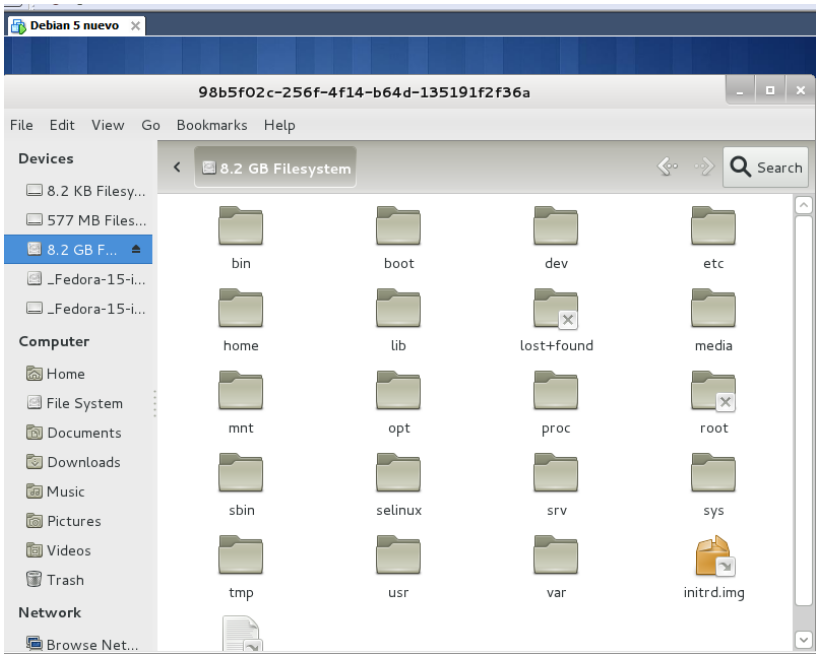
En una máquina virtual, vamos a arrancar Debian, pero con una imagen ISO de Fedora, para ello arrancamos con la imagen y nos aparece el escenario de Fedora



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



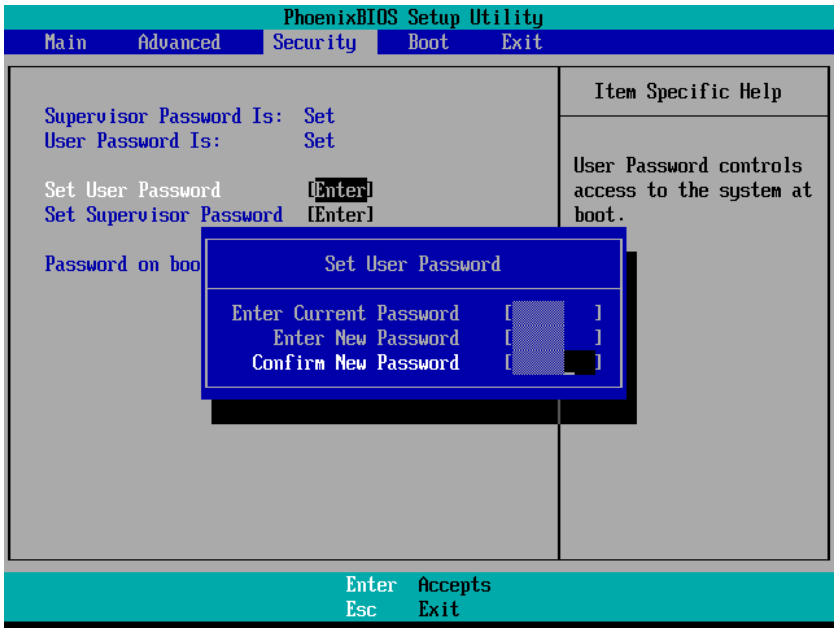
Aquí vemos que desde Fedora hemos entrado a Debian y podemos ver todas sus carpetas y archivos



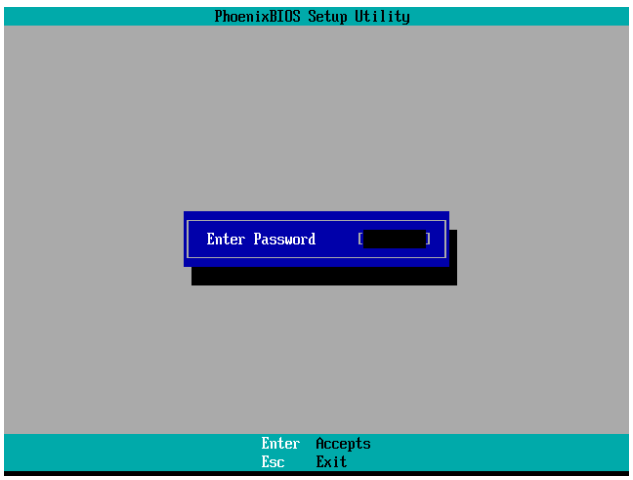
c) Configurando contraseñas en la BIOS:

- 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

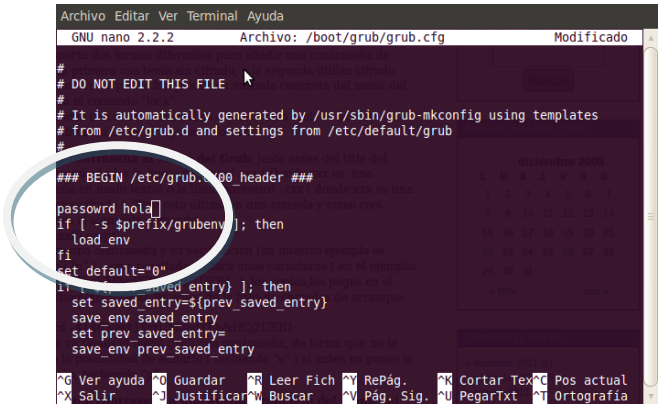


Y ya hemos entrado en la BIOS

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

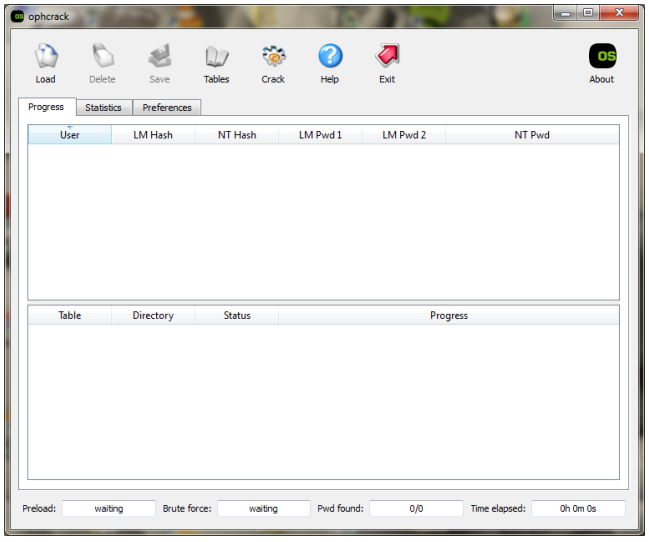


e) Recuperación de contraseñas:

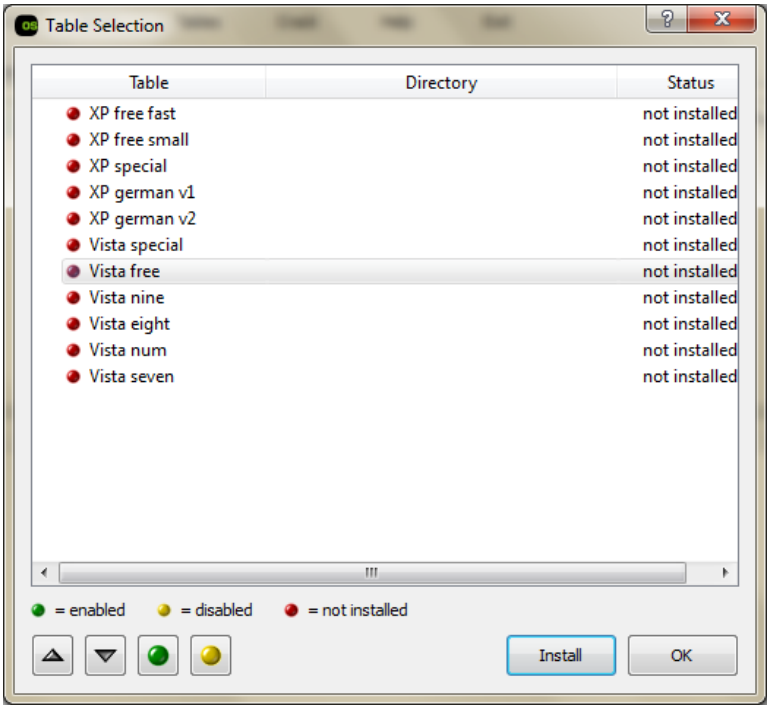
- En Windows: Ophcrack.
- En GNU/Linux: Aplicación John the Ripper.

OPHCRACK

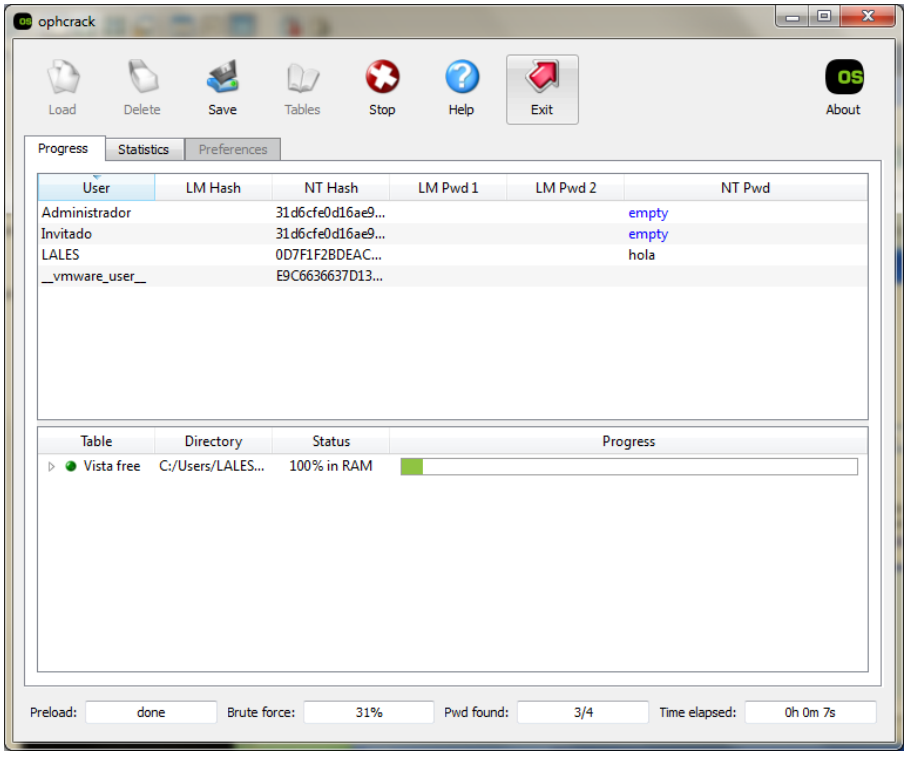
En Windows nos descargamos el programa Ophcrack y una vez descargado, le damos a la opción tables y buscamos donde tenemos las tablas guardadas



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

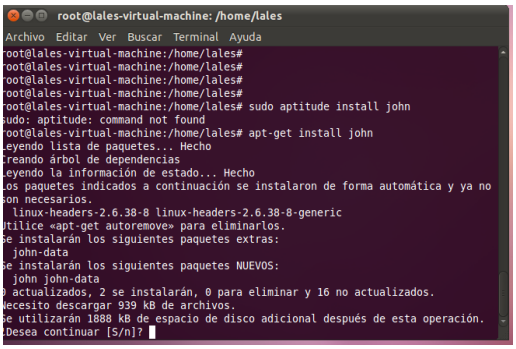


Cuando ya las tenemos las tablas metidas, le damos a Crack y empieza el análisis y nos muestra la contraseña de nuestro usuario.

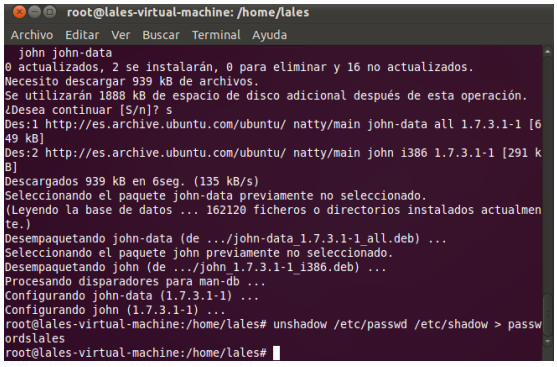


JOHN DE RIPPER

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



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



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

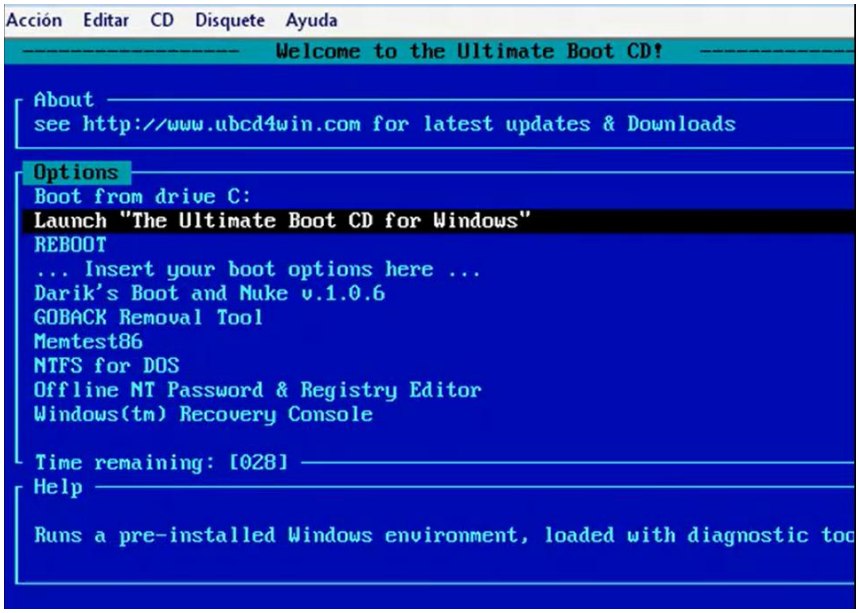
Por último introducimos john-incremental passwordslales y nos aparecerá al paso de un tiempo depende de cómo sean de complicadas, las contraseñas.

f) Modificación de contraseñas:

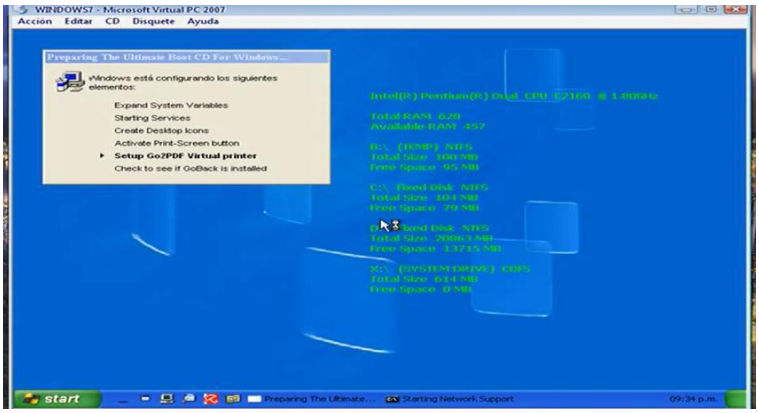
- En Windows: Distribución Live UBCD.
- En GNU/Linux: mediante el sistema, modificando /etc/shadow.

UBCD

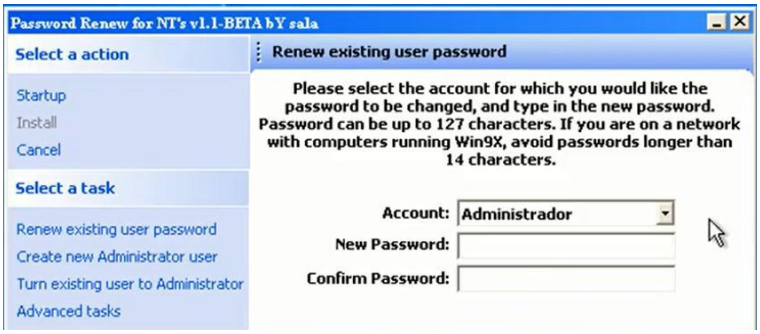
Entramos por medio del Live CD y le damos a la opción Launch



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

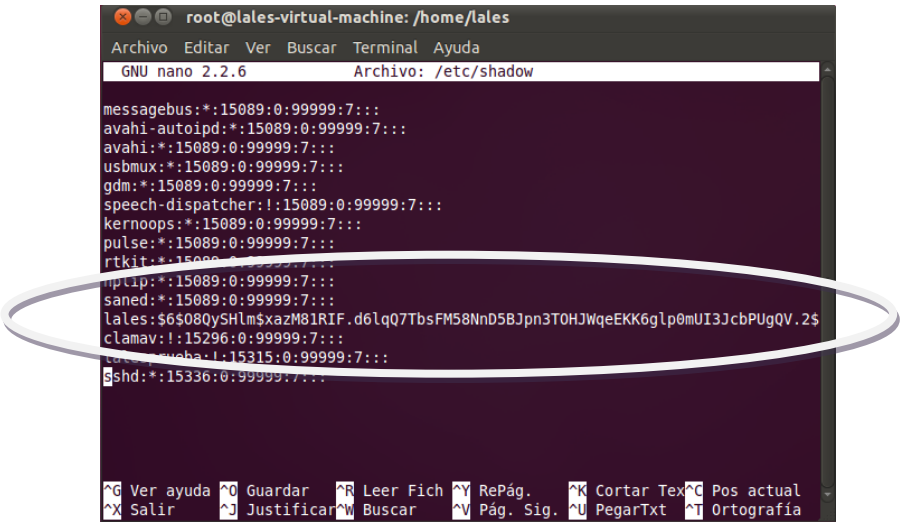


Renew existing user password, sería la siguiente opción, ponemos una contraseña y a la izquierda le damos a Install y ahí tenemos cambiada la contraseña

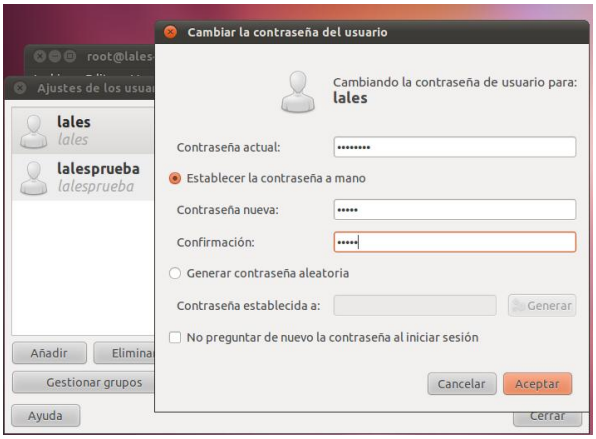


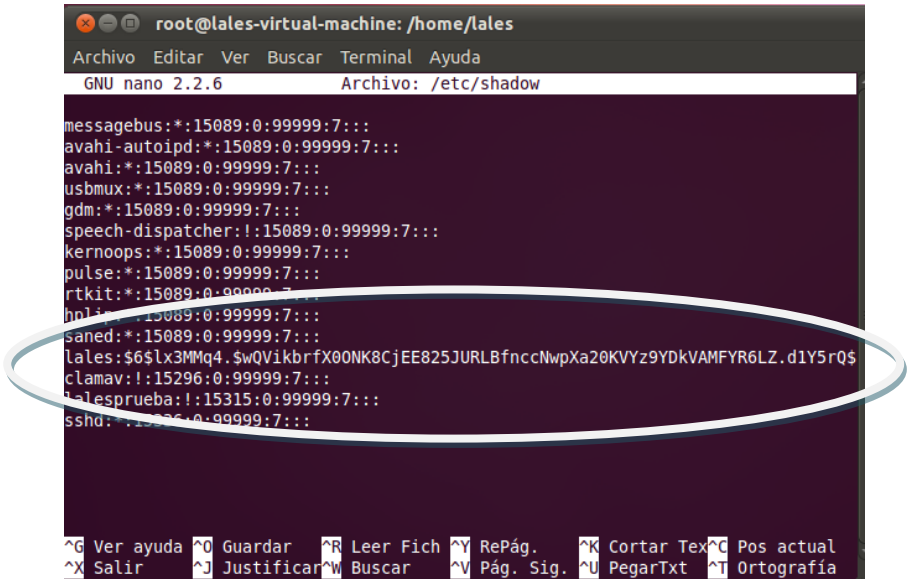
EN LINUX

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

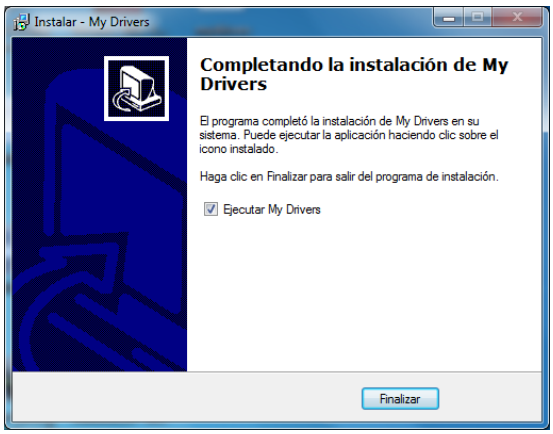




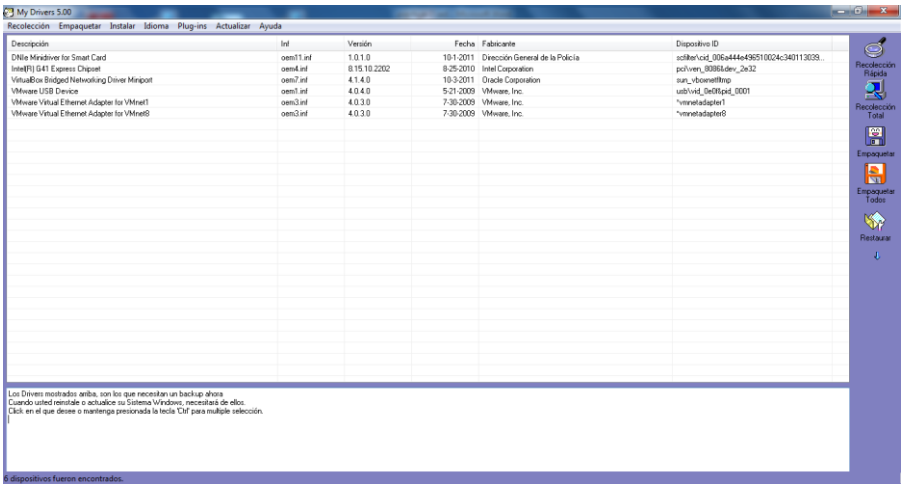
g) Realizar una copia de seguridad de drivers

- Utiliza el software “DriverMax” o similar.

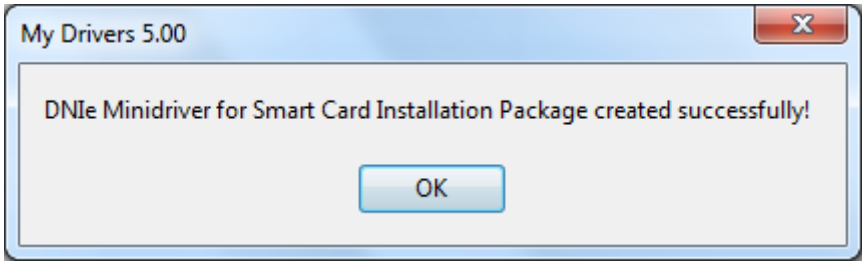
Vamos a instalar Mydrivers que es un software parecido a DriverMax y vamos a hacer una copia de seguridad de los drivers del ordenador

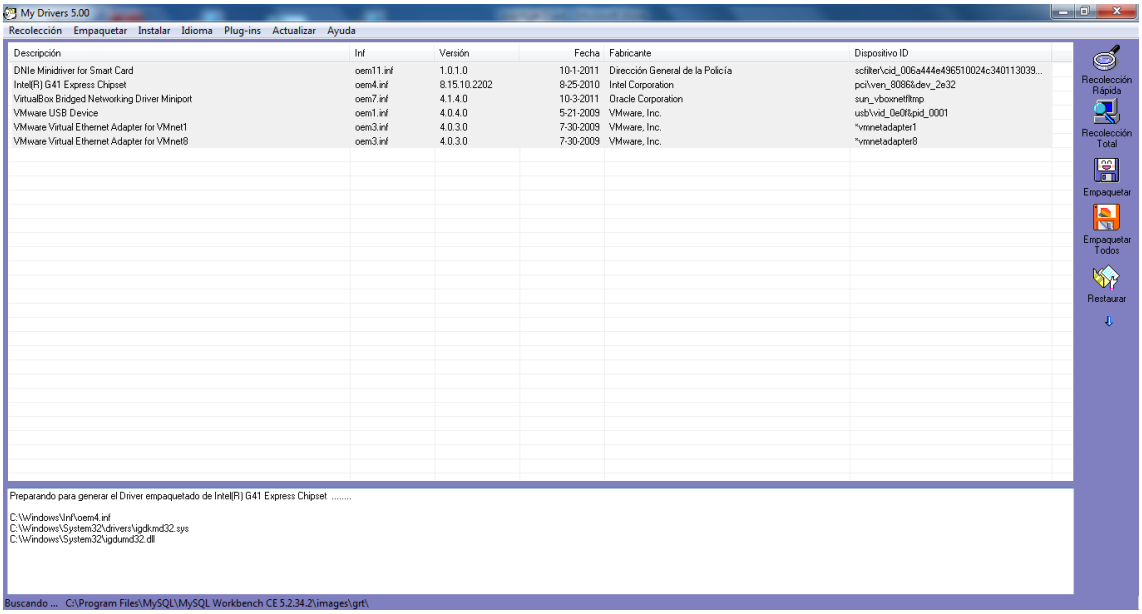


A continuación recopilamos todos los drives que tiene nuestro equipo y le damos a empaquetar



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



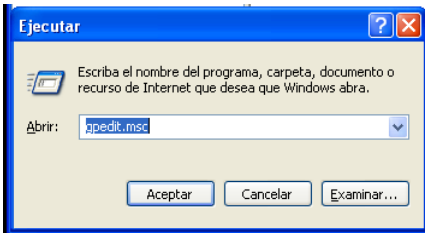


h) Control de acceso a datos y aplicaciones:

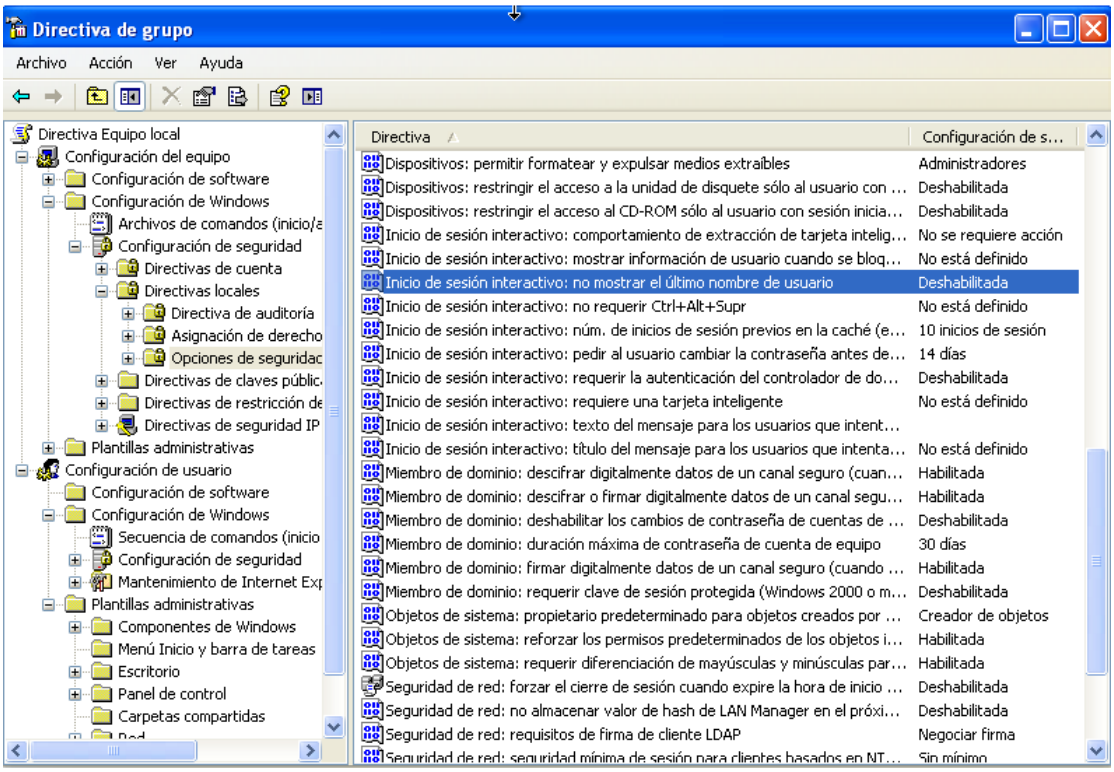
- En Windows: Política de directivas de seguridad local.
- En GNU/Linux: chmod, chown, chgrp, getfacl, setfacl.

EN WINDOWS

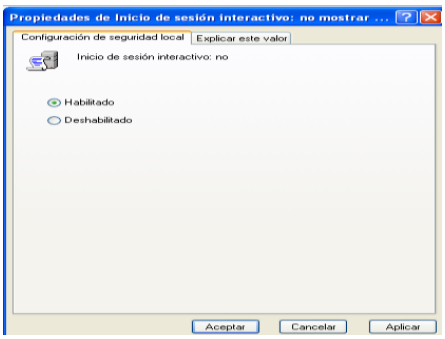
En Windows ponemos en ejecutar, gpedit.msc y nos aparece la ventana de Directivas de grupo



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

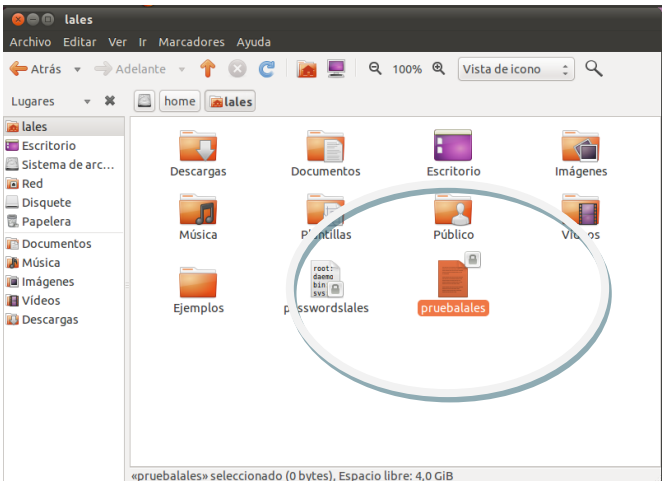


Y la habilitamos y aceptamos

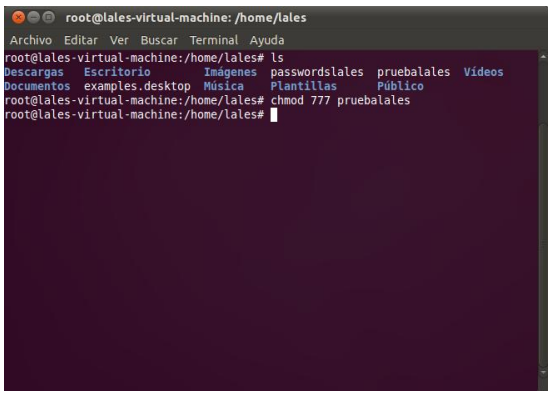


EN LINUX

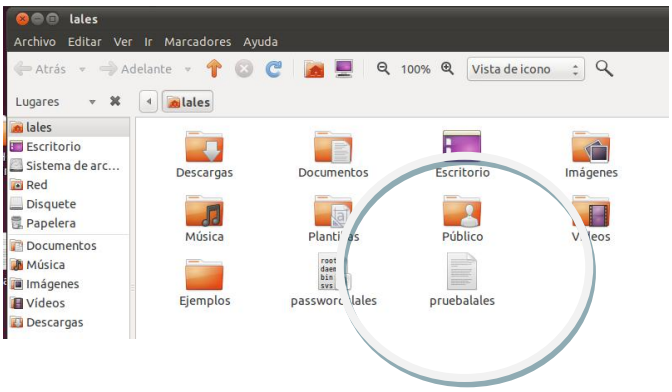
CHMOD: Hacemos un fichero en /home/lales que se llama pruebalales solamente con permisos de lectura



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

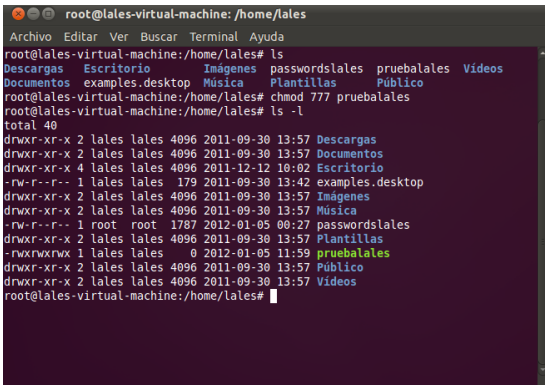


Y ya vemos como tiene el fichero todos los permisos

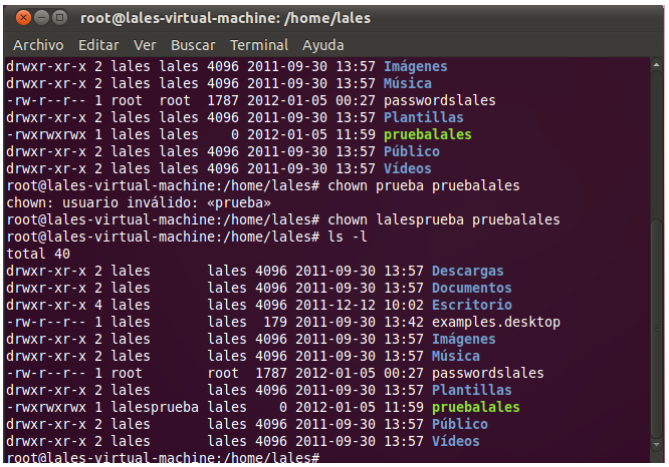


CHOWN Y CHGRP

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

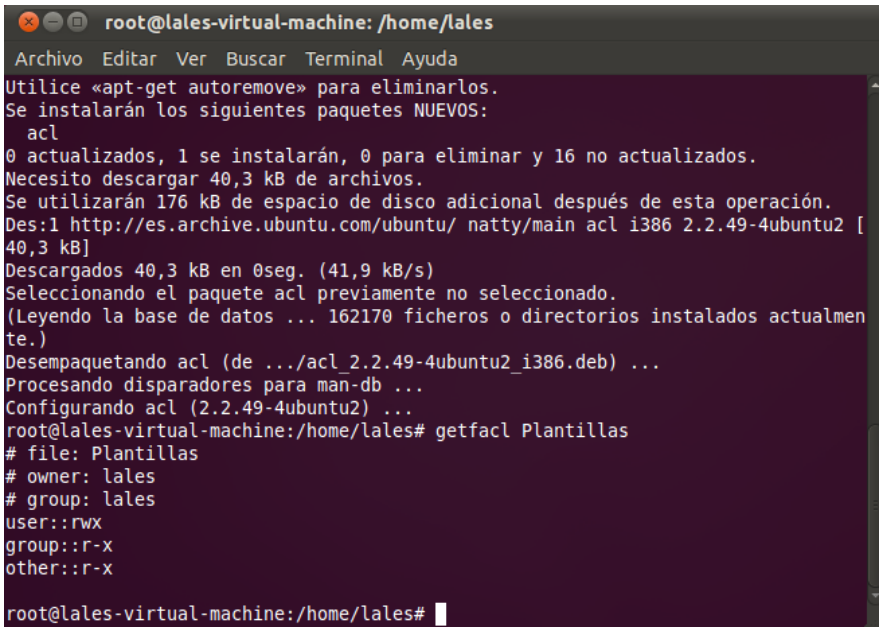


Ahora ponemos chown lalesprueba pruebalales, y así asignamos el fichero pruebalales al usuario lalesprueba, y comprobamos que ya es de ese usuario.



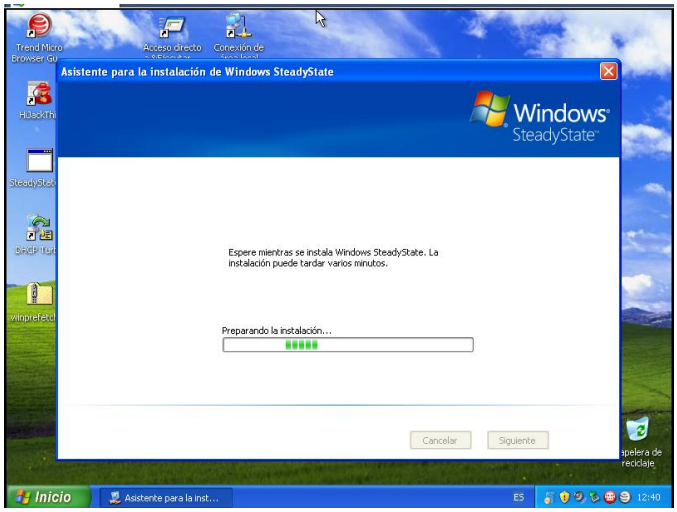
GETFACL Y SETFACL

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

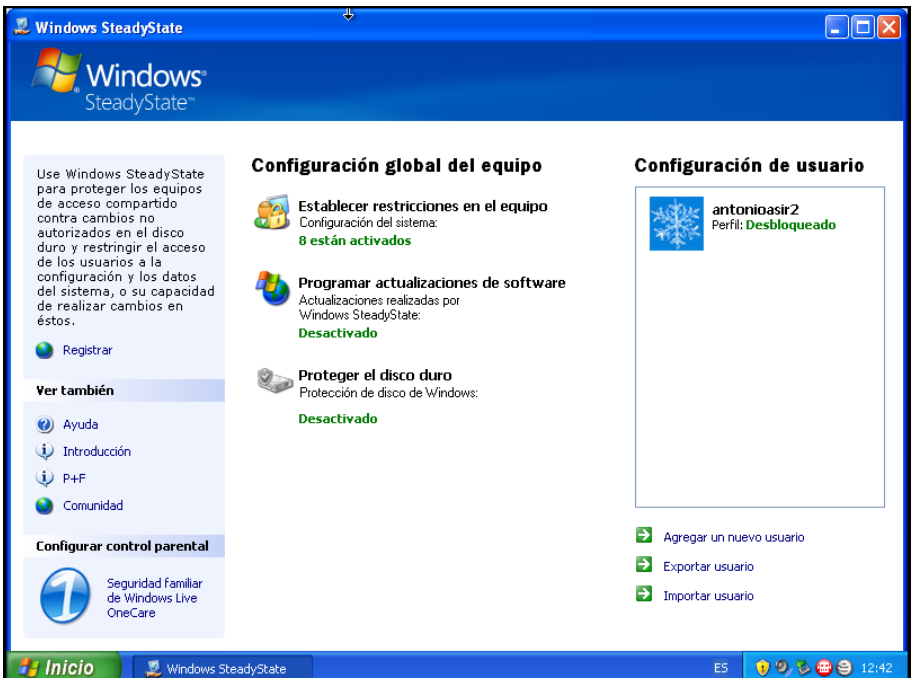


i) Utiliza el software "Windows SteadyState", y crea un pequeño informe de las posibilidades del mismo, desde un punto de vista de seguridad informática
http://recursostic.educacion.es/observatorio/web/es/software/software-general/785-windows-steady-state

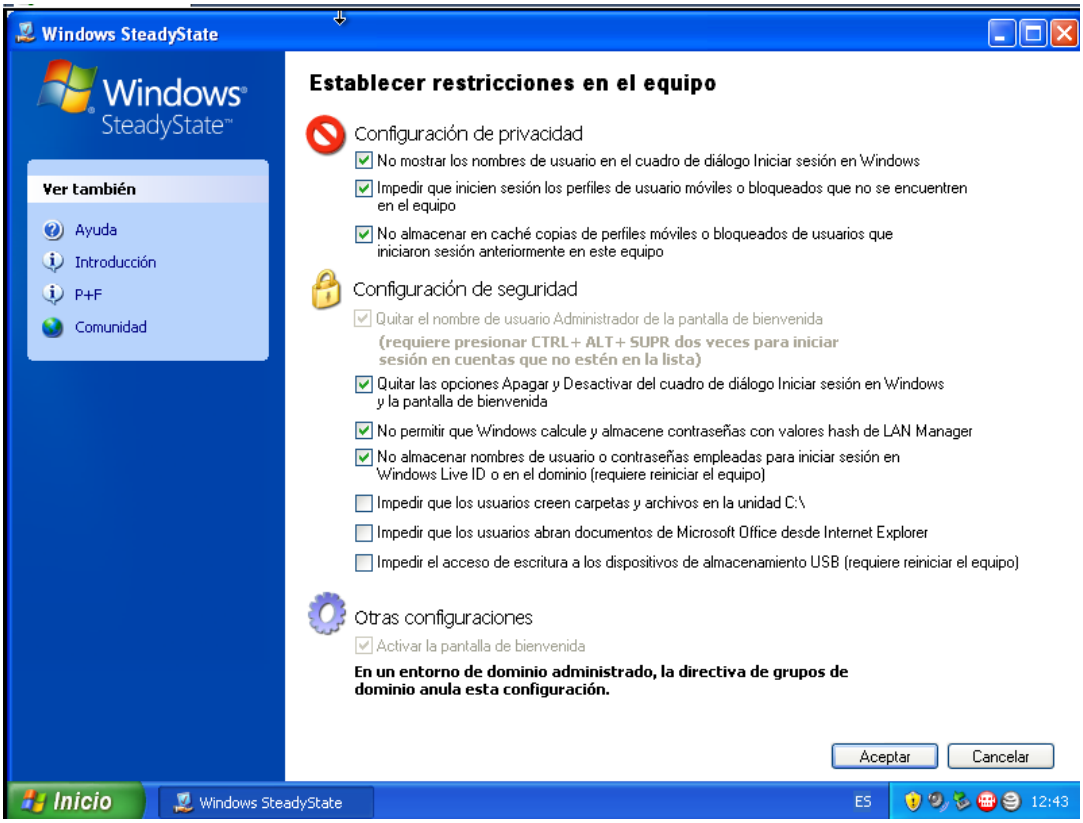
Nos descargamos el programa Windows SteadyState que nos sirve para establecer a los diferentes usuarios del sistema una serie de restricciones



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

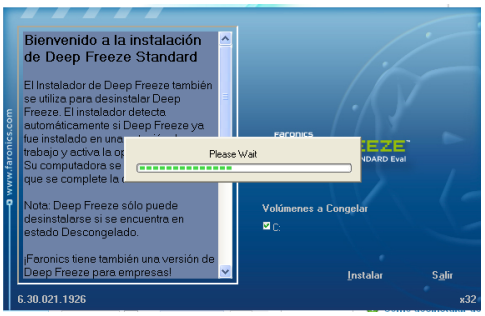


Ahí podemos cambiar la configuración de privacidad y de seguridad, para que no todos los usuarios tengan acceso y puedan modificar las opciones de Windows

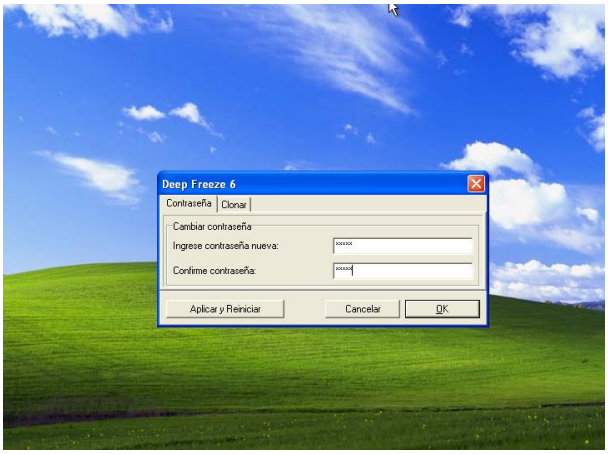


j) Busca aplicaciones “congelador” disponibles para Windows y GNU/Linux como “DeepFreeze”. Indica que protección ofrecen.

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

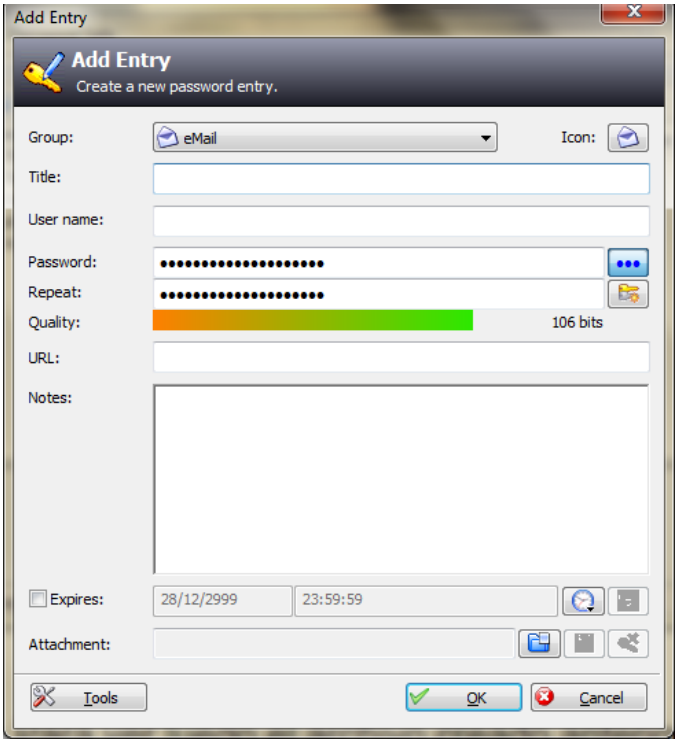


Creamos una carpeta en el escritorio y al salir de la sesión, cuando volvemos a ella vemos que no está, ya que todo lo que hemos hecho en esa sesión desaparece

k) Utiliza el software "Keepass Passwrod 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