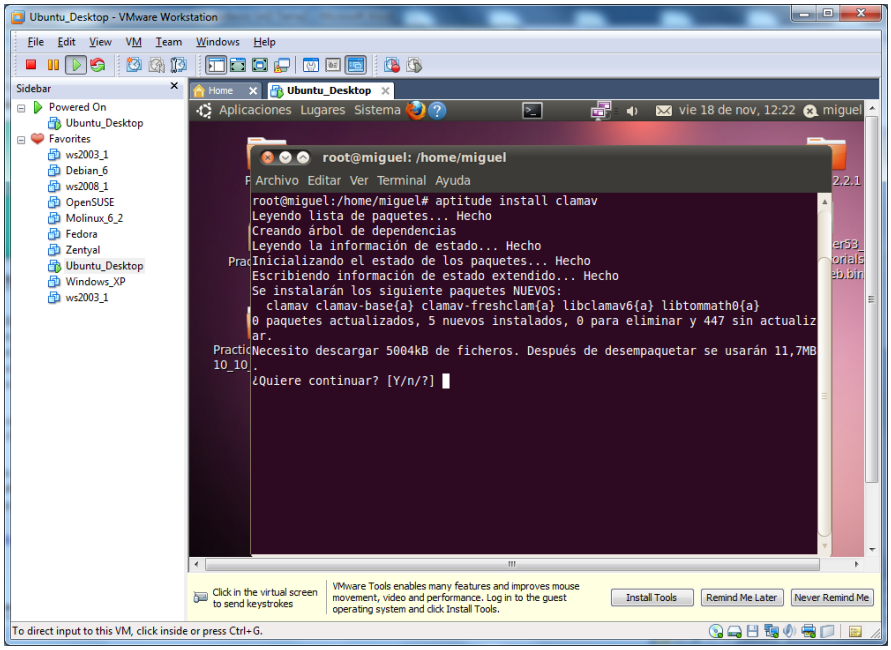
PRACTICAS SAD *TEMA 2*

ATAQUES Y CONTRAMEDIDAS EN SISTEMAS PERSONALES: 1. HERRAMIENTAS PALIATIVAS.

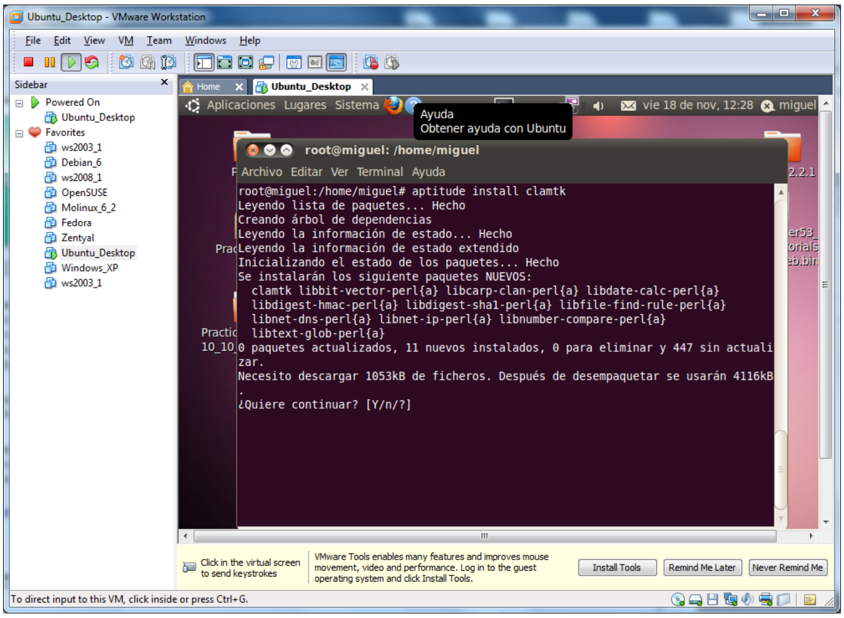
a) Instala en GNU/Linux el antivirus ClamAV, y su versión gráfica Clamtk.

sudo aptitude install clamav
sudo aptitude install clamtk
Escanear modo texto: sudo clamscan –r –i <directorio>
Escanear modo gráfico: sudo clamtk

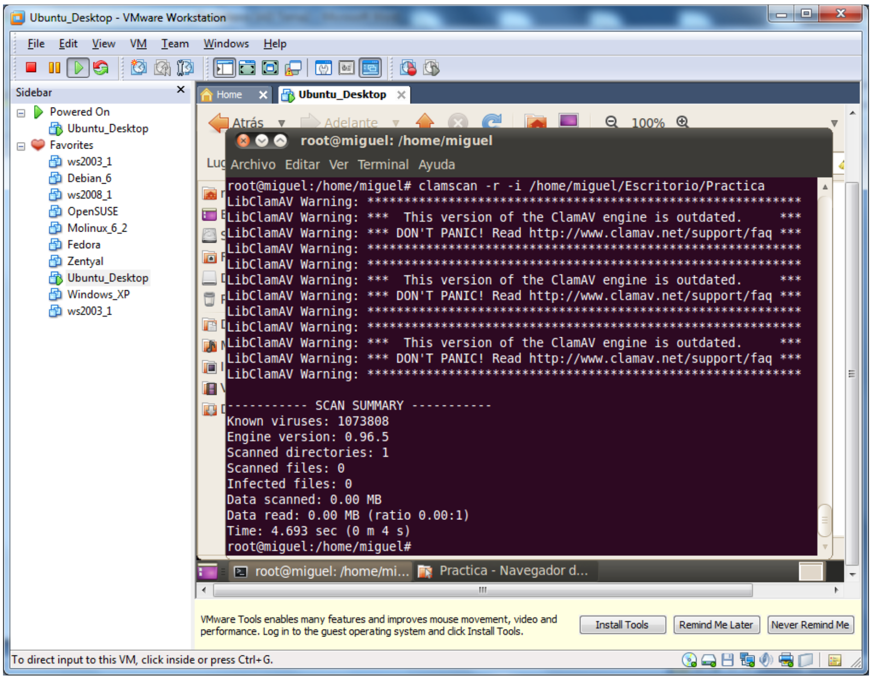
En primer lugar, instalamos la aplicación con el comando "**aptitude install clamav**".



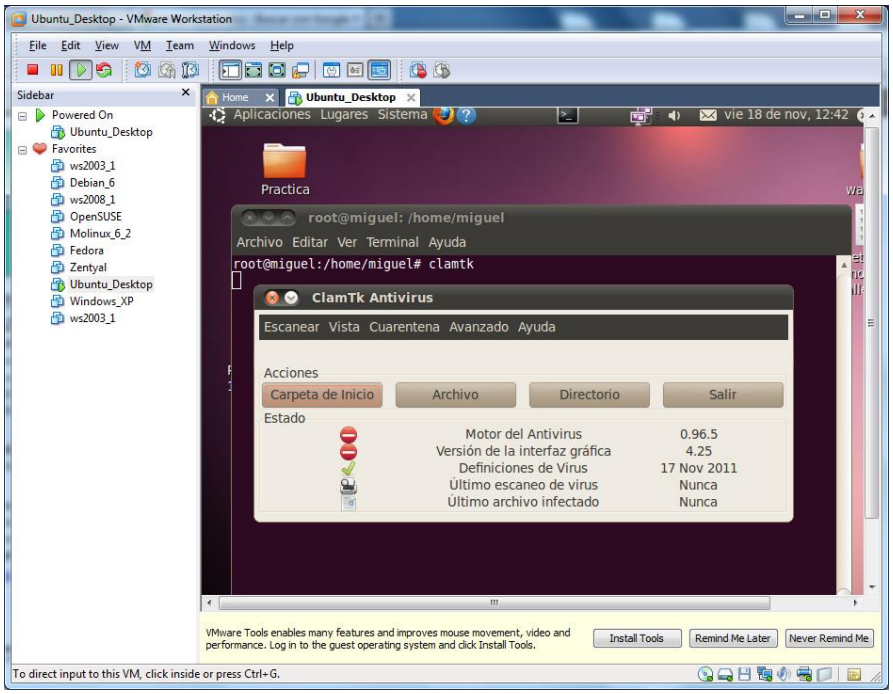
Le decimos que queremos continuar.



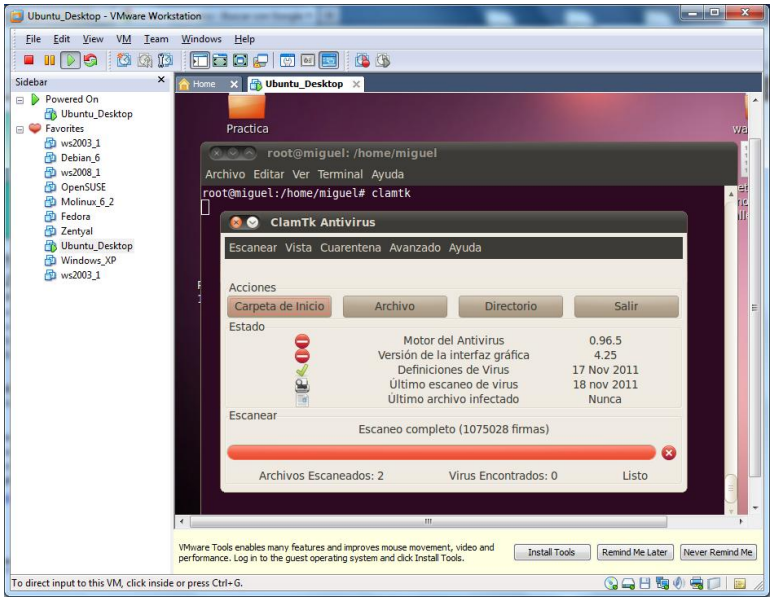
Finalmente se instalará el antivirus. Es probable que tengamos que actualizar el sistema, para actualizar la base de datos del antivirus, o para que simplemente funcione.



Ejecutamos el antivirus con el comando “**clamtk**”

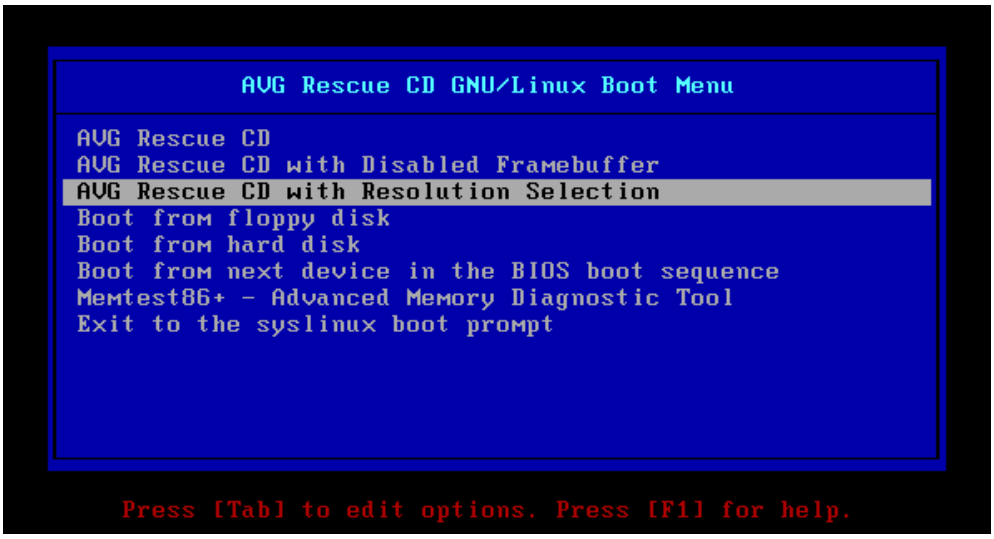


Y hacemos un pequeño análisis de una carpeta que tenemos creada en el escritorio. El resultado es que no hemos encontrado ningún tipo de virus.

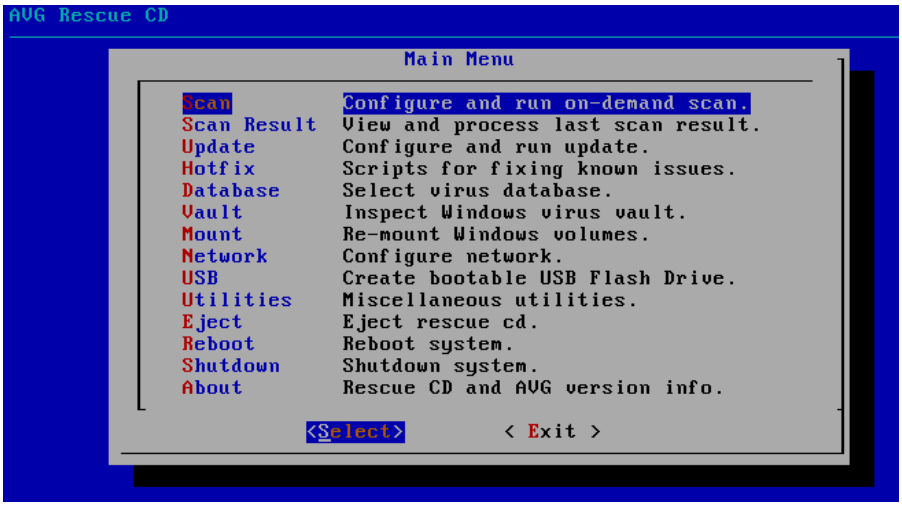


b) Instala y utiliza la herramienta de análisis antimalware Live AVG Rescue CD que se puede iniciar desde un CD o flash USB. Documenta dicho proceso.

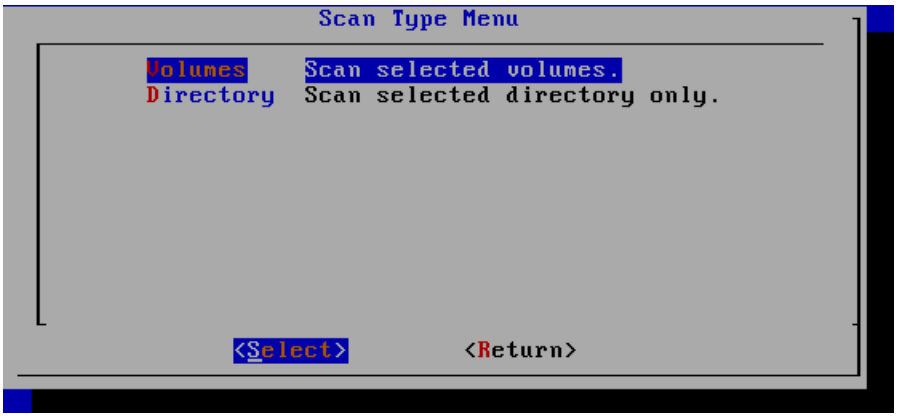
Arrancamos AVG Rescue CD, para poder analizar nuestro sistema fuera del sistema operativo. Elegimos la tercera opción de este menú para seleccionar lo que vamos a analizar.



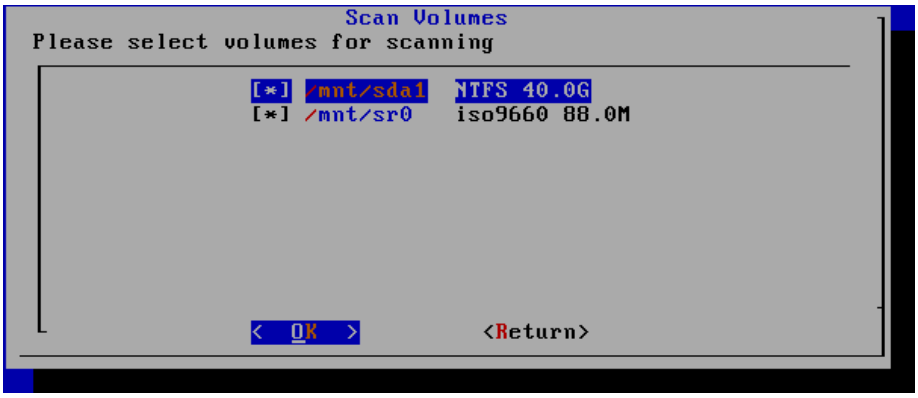
Elegimos la opción de escanear, para comenzar un análisis de nuestro sistema.



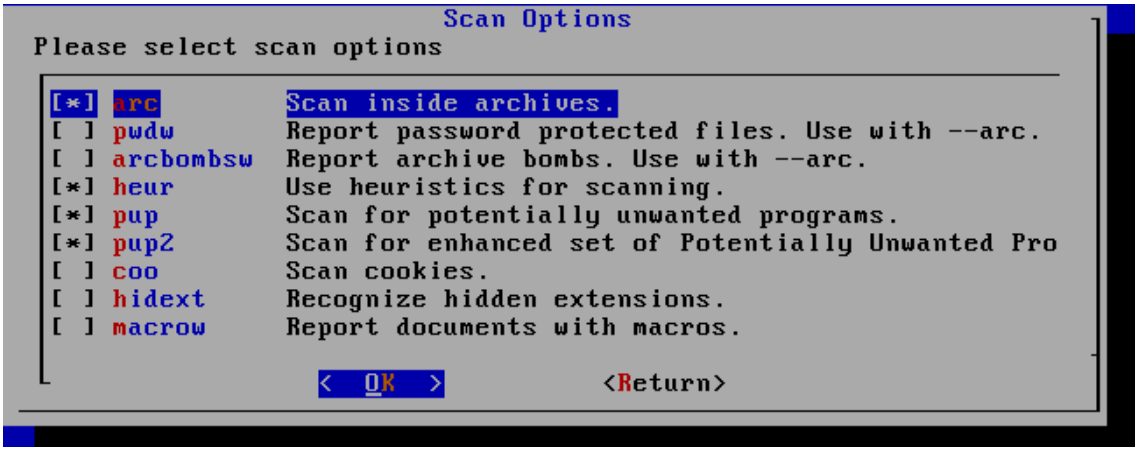
Elegimos la opción de volúmenes para elegir un volumen entero para analizarlo. Podemos también analizar un directorio concreto, pero no lo vamos a usar en este caso.



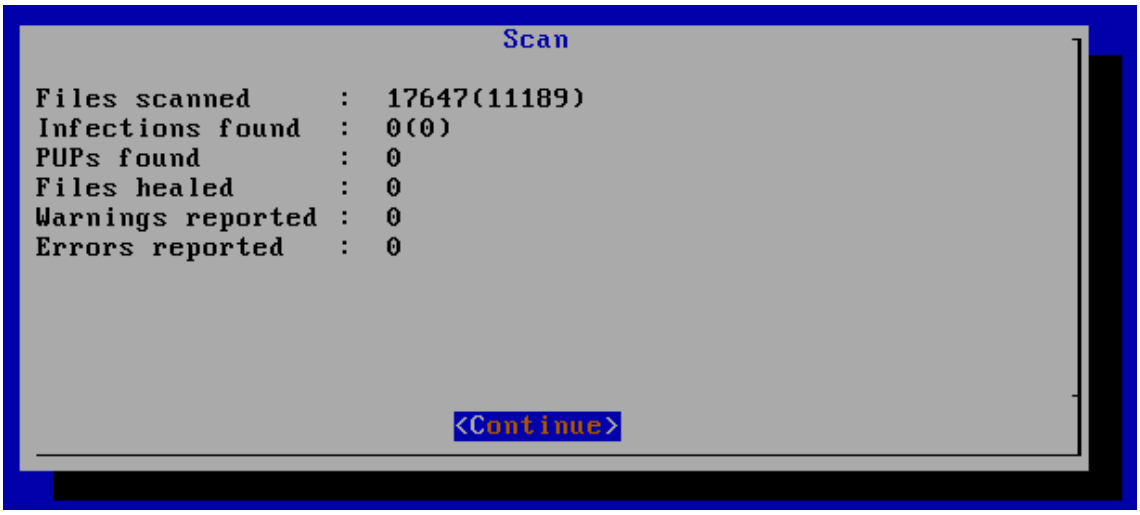
Elegimos el disco de nuestro Windows7 virtual, para comentar el análisis con este antivirus.



Hacemos un análisis de todos los archivos de nuestro disco.



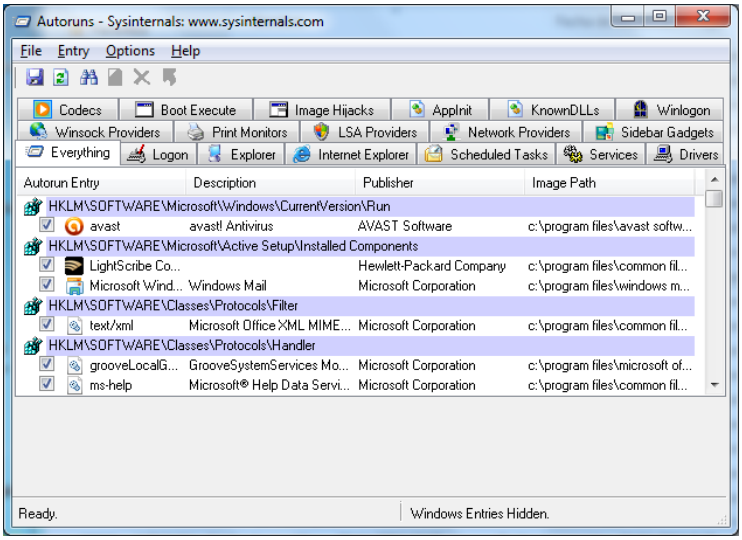
Una vez concluido el análisis de nuestro sistema, comprobamos que estamos libres de virus. Debemos de tener cuidado con la versión de nuestro antivirus, ya que una versión anticuada podría no detectar virus actuales.



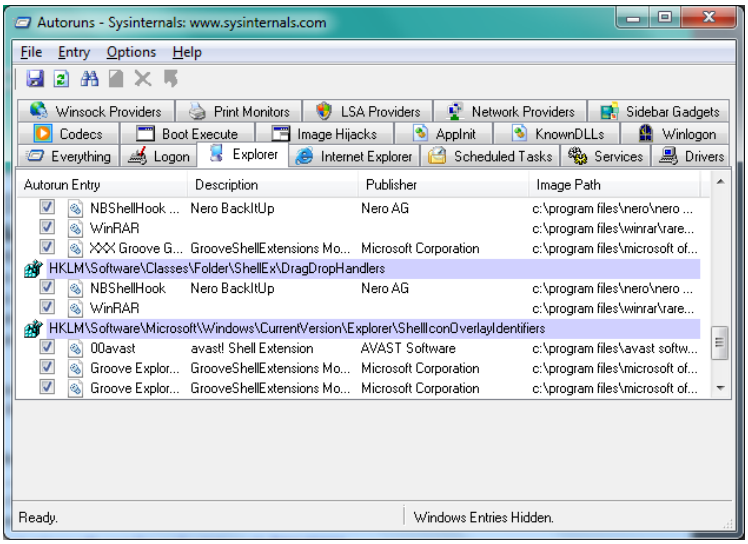
c) **En tu ordenador, realiza un análisis antimalware a fondo** (**msconfig**, procesos dudosos ejecutándose, …etc) mediante el **software de Microsoft** : suite **Sysinternals**. Indica en un documento todos las acciones que has realizado. Utiliza entre otros: **Autoruns** y **Process Explorer**

Nos descargamos de la página indicada la suite de aplicaciones Sysinternals. Y ejecutamos el ejecutable "**autoruns**".
Nos saldrá la siguiente pantalla. Vamos a hacer las siguientes pruebas.

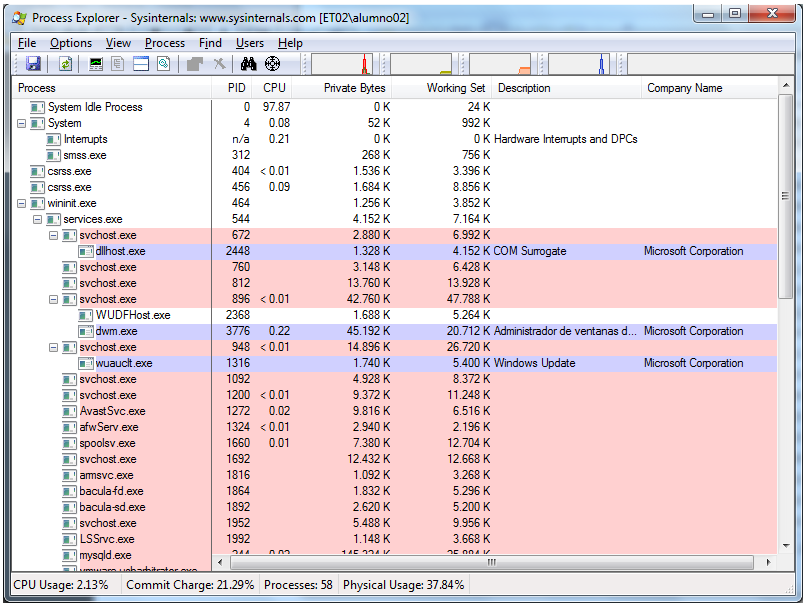
En la pestaña Everything marcamos, todas las aplicaciones que tenemos instaladas en el PC, y las analizamos.



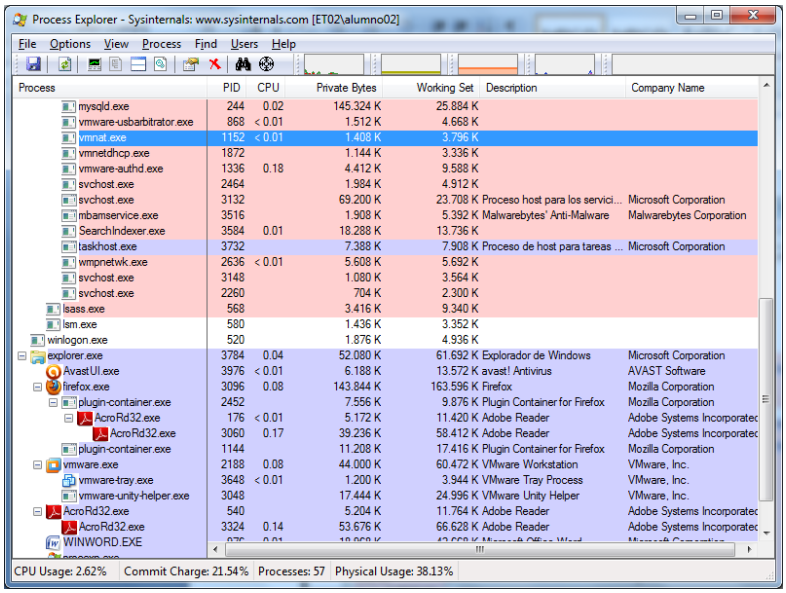
También podemos efectuar lo mismo, en la pestaña Explorer con los registros de nuestro sistema operativo.



Probamos la aplicación **Process Explorer** de la suite de aplicaciones systernals. Esta aplicación permite analizar todos los ejecutables del sistema.

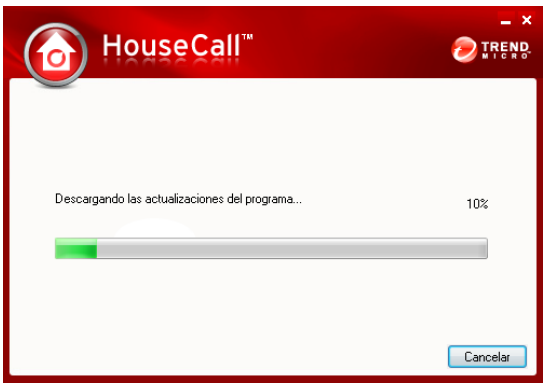


Hacemos un análisis a todos ellos.

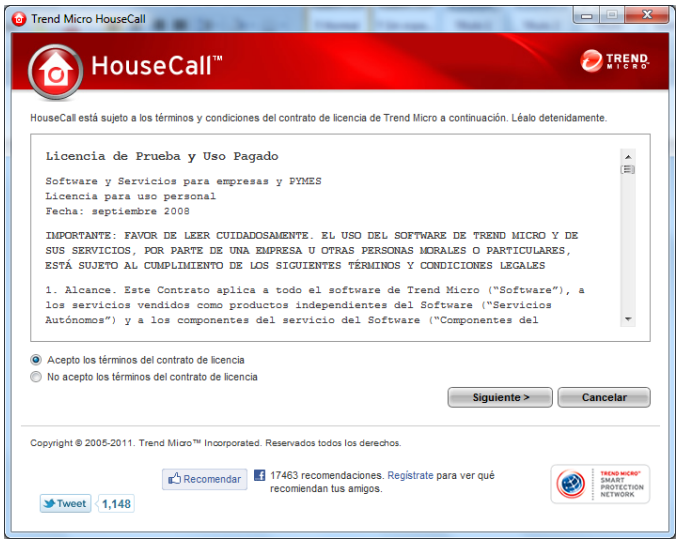


d) En tu ordenador, realiza un **análisis antimalware a fondo,** utilizando las herramientas gratuitas de **Trend Micro USA.** Documento dicho proceso. **Utiliza las herramientas: HouseCall, Browser Guard 2011, HiJackThis y RUBotted,**

HouseCall es una herramienta gratuita basada en la Web que está diseñada para detectar en el PC una amplia gama de amenazas en seguridad de Internet, como virus, gusanos, troyanos y spyware. También detecta las vulnerabilidades del sistema y proporciona un enlace que le permite descargar fácilmente los parches de seguridad que faltan. Después de cada exploración, HouseCall entrega un informe detallado que identifica las amenazas de seguridad detectadas en el equipo.



Instalamos la aplicación **house call**.



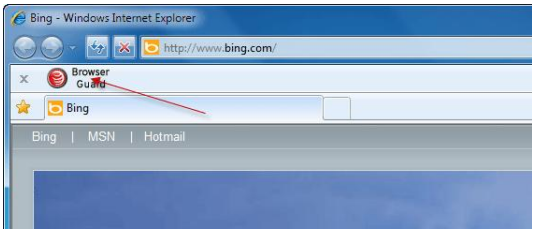
Una vez concluida la instalación procedemos a analizar el sistema.

Una vez finalizada la búsqueda de amenazas, comprobamos que no tenemos ninguna.

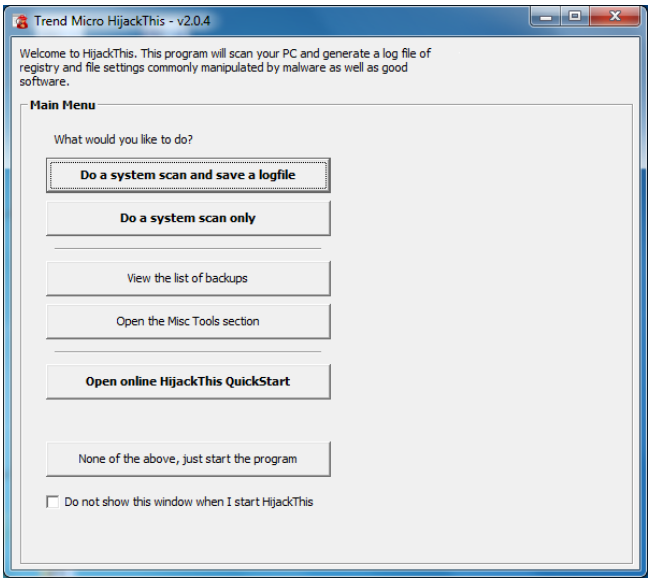
Browser Guard 2011 previene la vulnerabilidad de día 0 y protege contra JavaScript malintencionado que usa heurística avanzada y tecnologías de emulación.

Esta versión de Browser Guard se actualizará de forma rápida y permanente para proporcionar la tecnología más segura y avanzada. Las versiones habituales de Browser Guard 2011 actualizan las funciones de las herramientas actuales en función de la opinión del usuario.

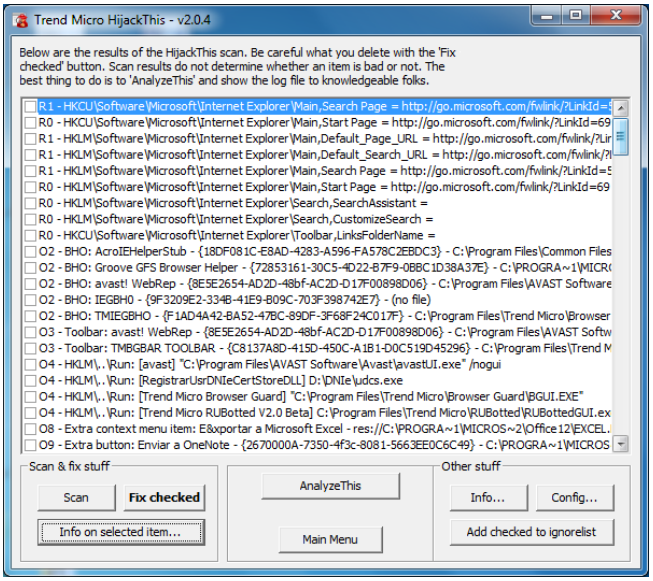
NOVEDADES
- Una mejora en la detección de troyanos Web
- Una mejora de detección en el seguimiento de las cadenas de infecciones



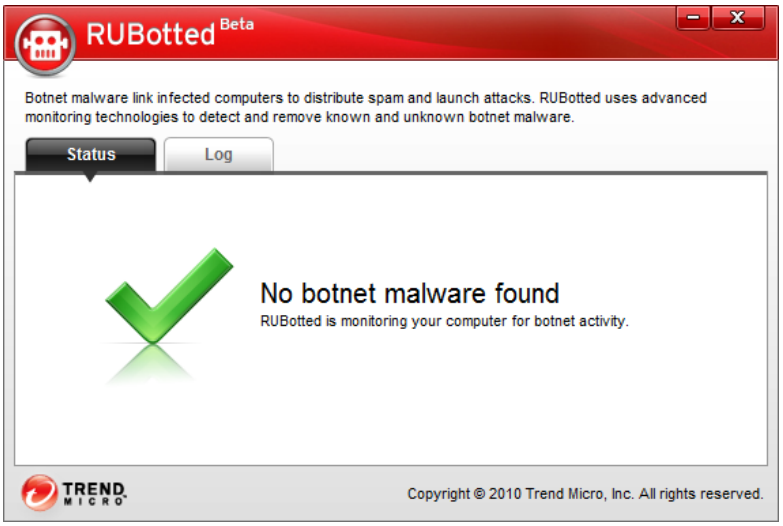
Con la aplicación HijackThis podemos escanear el registro de nuestro equipo, elegimos la primera opción para hacer un escanero de nuestro sistema.



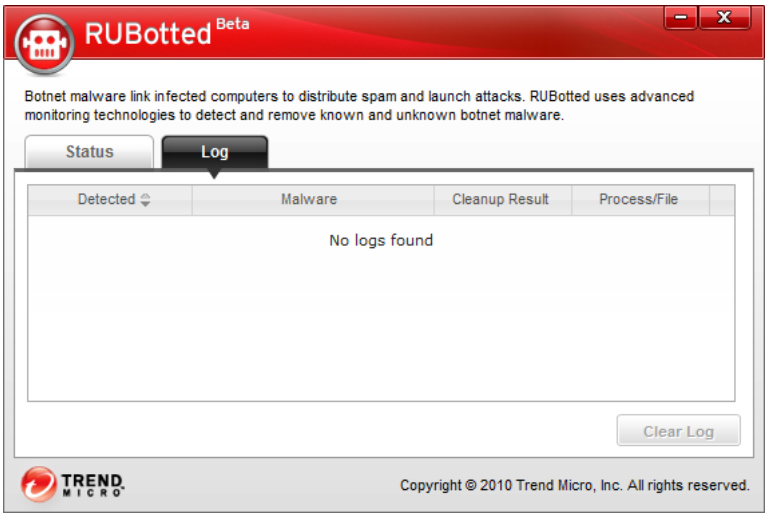
Comprobamos el resultado del registro de nuestro sistema.



RUBotted nos permite detectar, si tenemos en nuestro sistema, alguna aplicación infectada con algún tipo de malware. Tendremos esta aplicación arrancada y efectuará su trabajo en caso de detectar alguna amenaza.

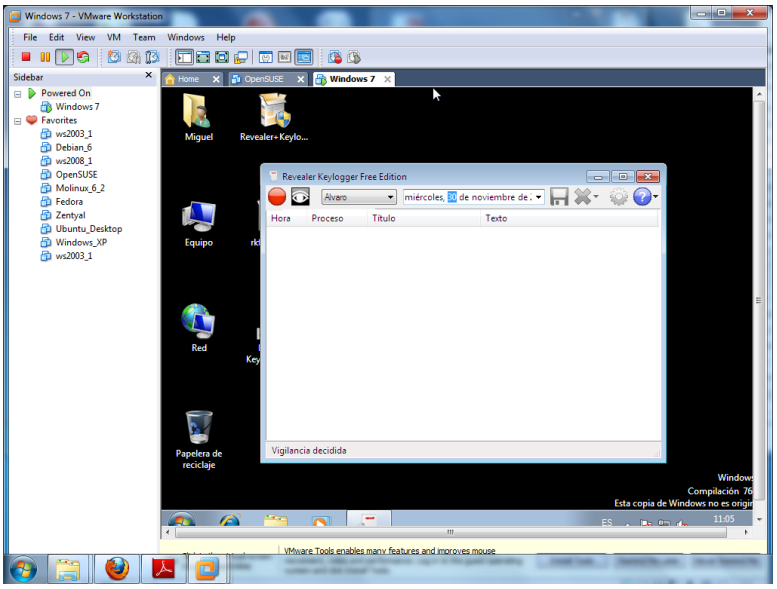


Como podemos comprobar, en la actualidad no tenemos ninguna amenaza en nuestro sistema.

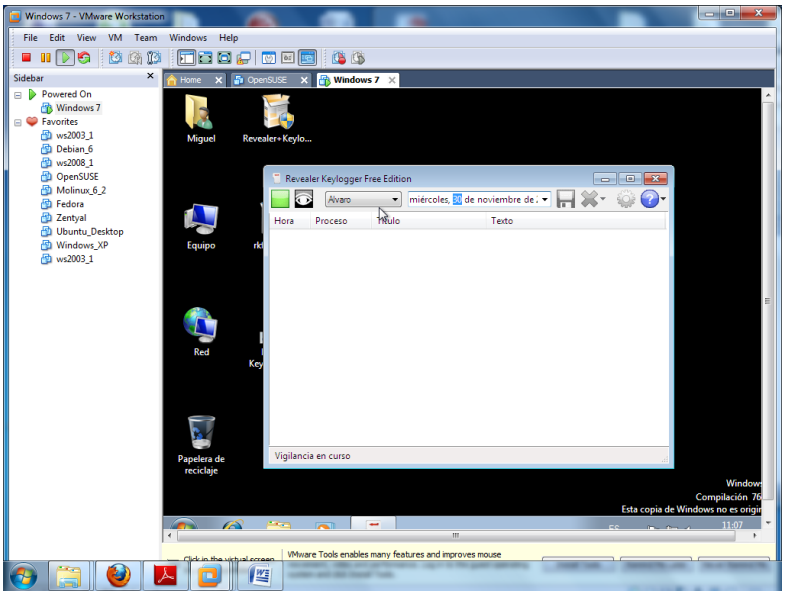


e) Instala y utiliza el **software de recuperación de pulsaciones de teclado denominado Revealer Keylogger.** Piensa como prevenir este software e informa en un documento. **Utiliza el software Malwarebytes para Windows. ¿Lo detecta?**

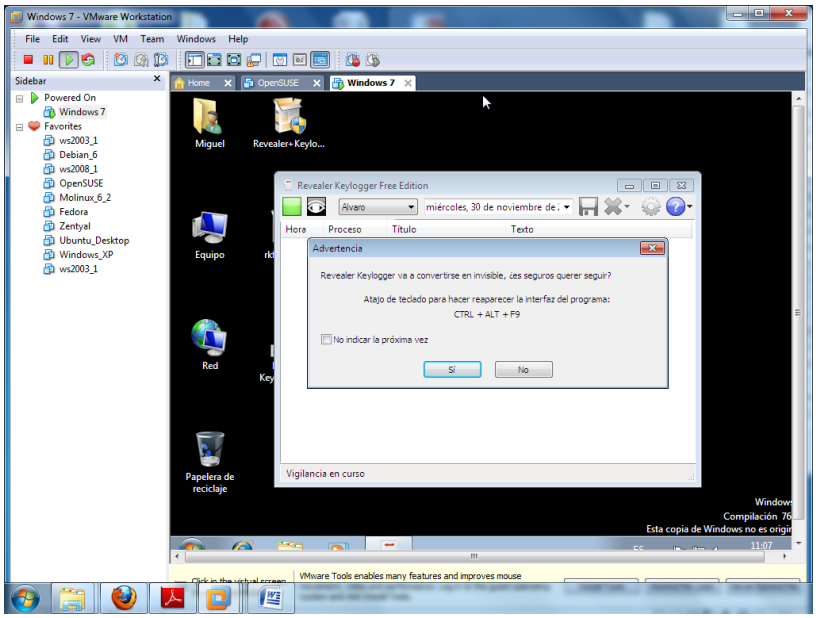
Una vez instalado el keylogger, una vez ejecutado, nos aparecerá la siguiente pantalla, con un botón en rojo, esto quiere decir, que el keylogger esta deshabilitado en estos momentos.



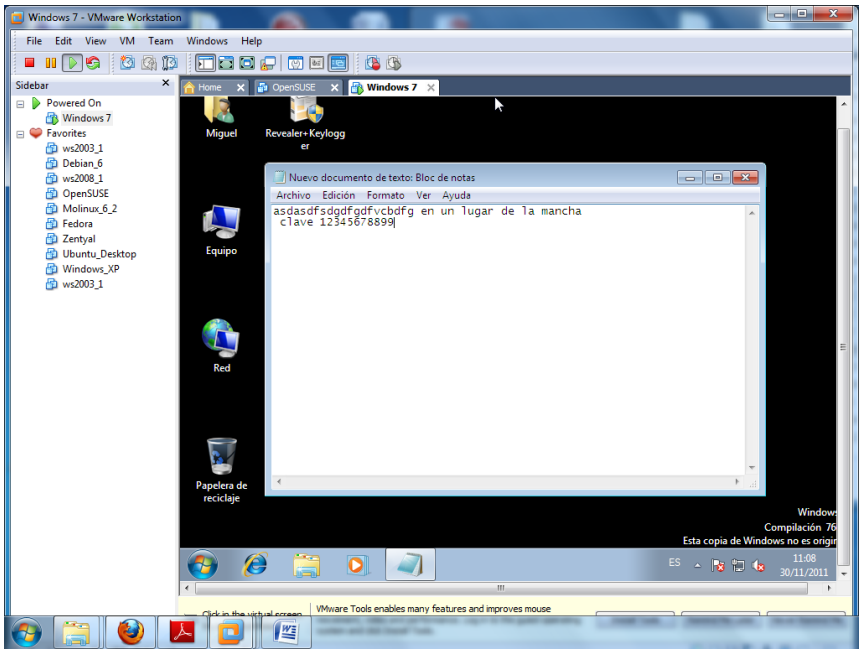
Para habilitarlo pulsamos el botón rojo, y automáticamente se pondrá en verde y listo para su uso.



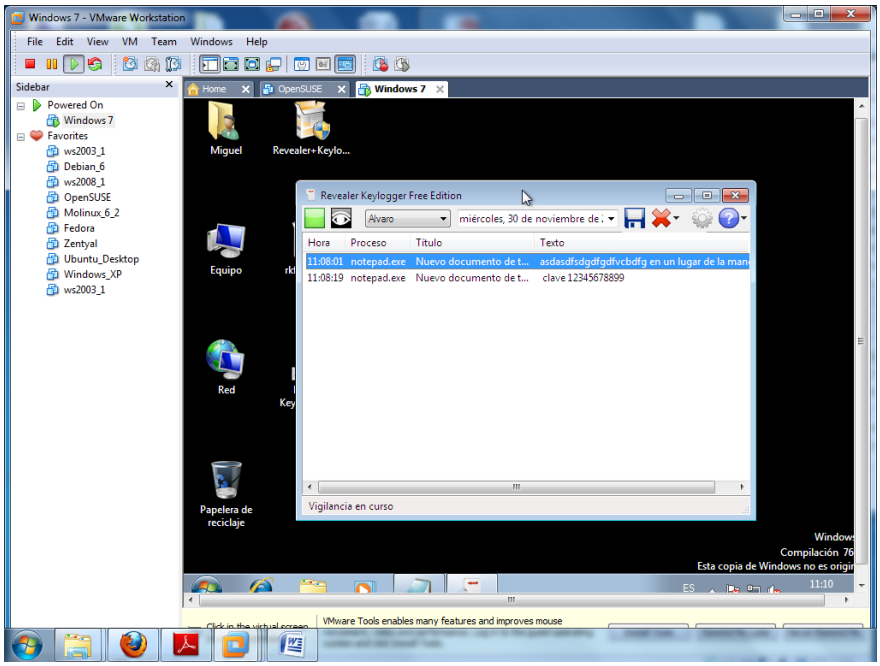
Podemos ocultar la aplicación para que el cliente, no lo detecte, para ello pulsamos el botón con el ojo, y seguidamente nos muestra la siguiente pantalla, para su posterior des ocultado.



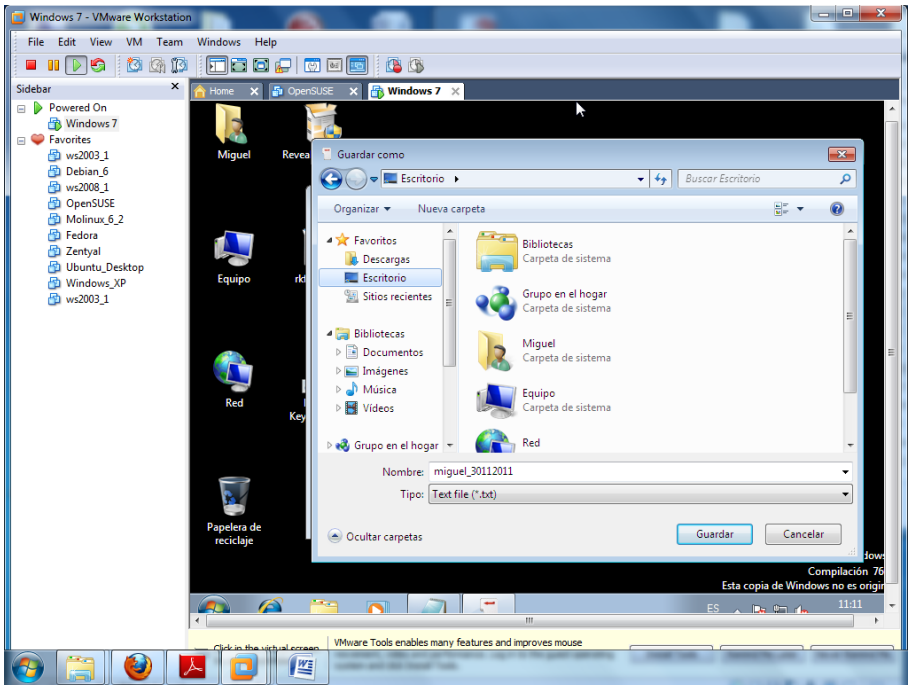
Probamos a abrir un nuevo documento, y hacer unas determinadas pulsaciones para verificar la utilidad de nuestra aplicación.



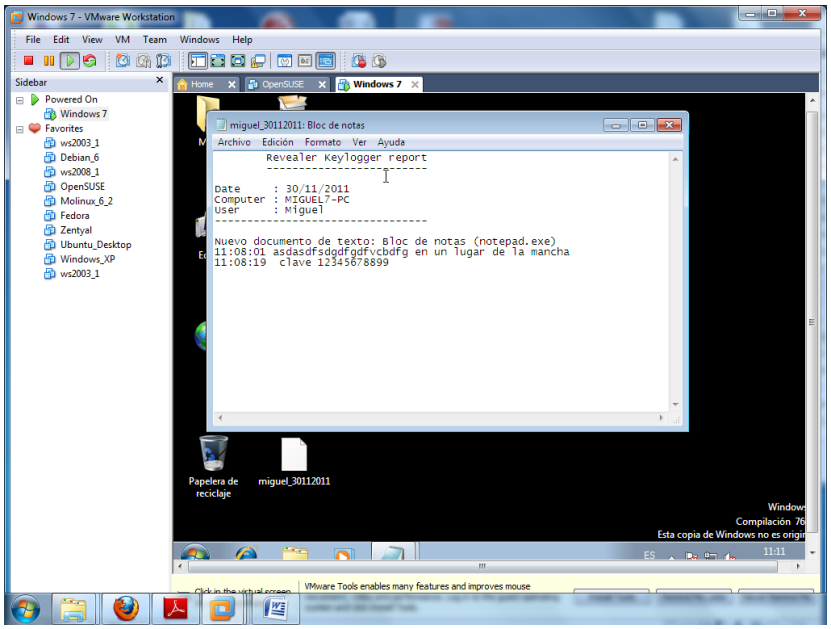
Volvemos a hacer visible, nuestra aplicación, y guardamos los resultados obtenidos por nuestra aplicación.



Guardamos por ejemplo en el escritorio.



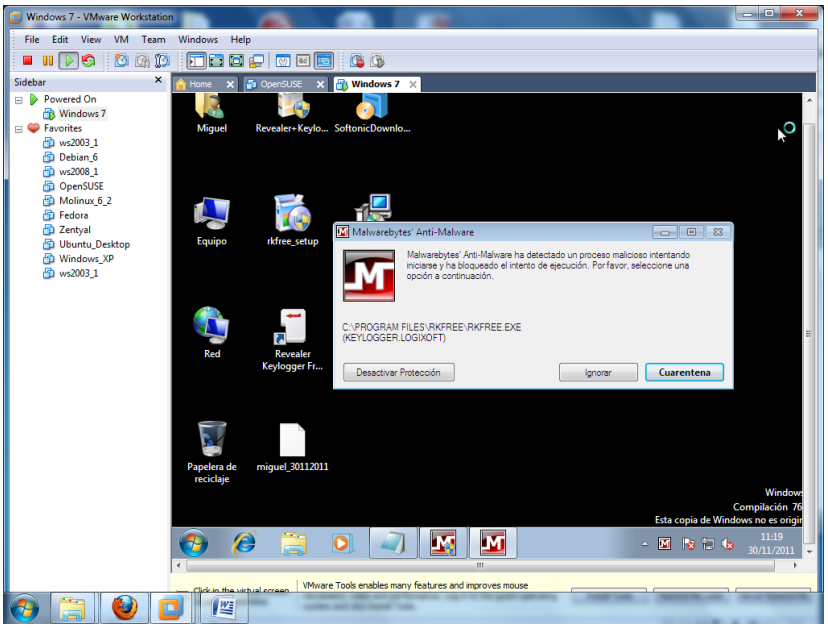
Abrimos, el documento y observamos la información capturada por nuestro programa, esto nos lleva a pensar la peligrosidad de estas aplicaciones en cuanto a la intimidad de la información, y que nos lleva a pensar tomar una serie de normas de seguridad, a la hora de utilizar un equipo que no sea el nuestro.



Hemos instalado la aplicación Anti-Malware y vamos a efectuar una prueba para comprobar si verdaderamente detecta la amenaza del keylogger.

Intentamos ejecutar el keylogger y automáticamente el Anti-Malware, nos salta, comunicando de una amenaza.

Sacamos en conclusión que el Anti-Malware detecta el Keylogger.

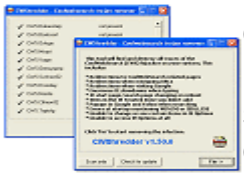


f) Investiga en Internet el término: **Hijacker**. Cómo puedes eliminar el **"Browser hijacker"**. ¿Qué efectos tiene sobre el sistema?

Hijacking significa "secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información) por parte de un atacante. Es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera podemos encontramos con el secuestro de conexiones de red, sesiones de terminal, servicios, modems y un largo etcétera en cuanto a servicios informáticos se refiere.

Browser hijacking: (*Secuestro de navegadores* en español). Se llama así al efecto de apropiación que realizan algunos spyware sobre el navegador web lanzando popups, modificando la página de inicio, modificando la página de búsqueda predeterminada etc. Es utilizado por un tipo de software malware el cual altera la configuración interna de los navegadores de internet de un ordenador. El término "secuestro" hace referencia a que estas modificaciones se hacen sin el permiso y el conocimiento del usuario. Algunos de éstos son fáciles de eliminar del sistema, mientras que otros son extremadamente complicados de eliminar y revertir sus cambios.

Para eliminar algunos de estos hijacker podemos utilizar:



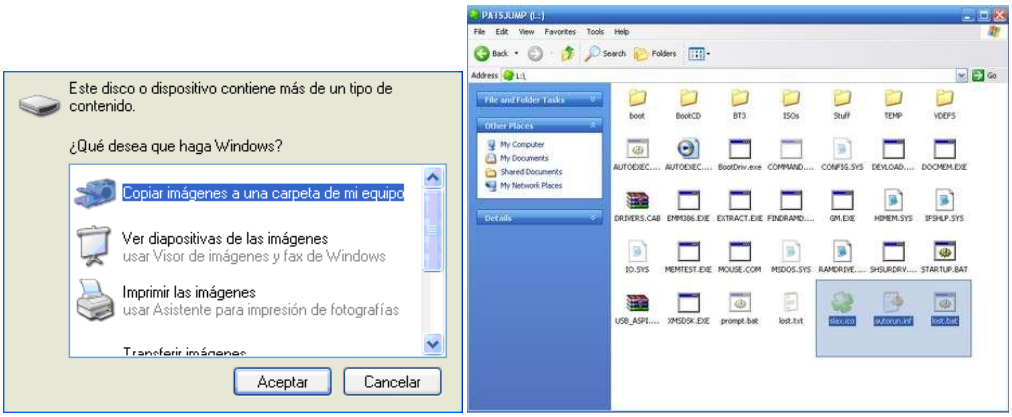
CWShredder 2.19
Esta herramienta está especialmente diseñada para eliminar de tu sistema todos los elementos de spyware relacionados con **CoolWebSearch**, actualizándose para eliminar todas sus variantes que ya son más de 50 y siguen apareciendo.

AboutBuster 6.02
Detecta y elimina spyware **"HomeSearch"** el cual se basa en un archivo .dll (res://random .dll/random) con la función de cambiar la página de inicio del IE y mostrar siempre una diferente cada determinado tiempo.

ToolbarCop
Elimina Toolbar (barra de herramientas) y botones extra de IE, Pero cuidado usela con precaución ya que no permite deshacer los cambios efectuados en el registro. Recomendamos que haga una copia de seguridad del mismo antes de borrar nada.

g) Busca información sobre el fichero **autorun.inf** que poseen los dispositivos de almacenamiento y cómo se camufla y opera malware a través de este archivo.

En el caso de las infecciones a través de dispositivos externos como por ejemplo los USB, el malware se vale de un archivo llamado “autorun.inf” que se encarga de ejecutar el código malicioso en forma automática cuando el dispositivo es insertado en la computadora. Esto sucede si el usuario no ha deshabilitado esta opción explícitamente (lo que la mayoría de los usuarios no hacemos) y que a continuación muestra la siguiente ventana:

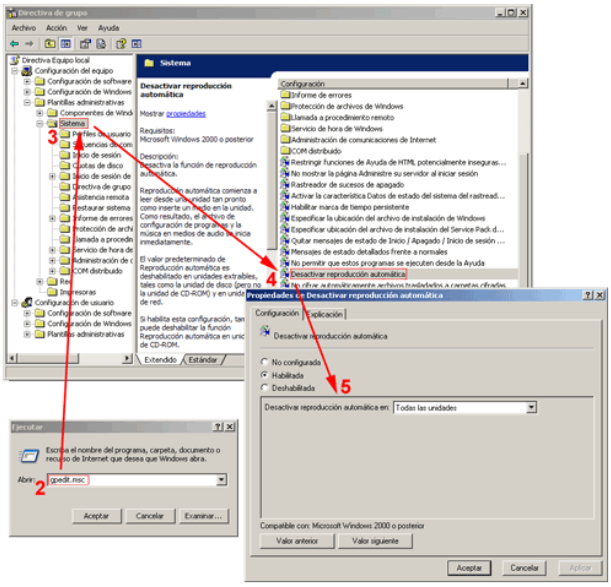


Estos programas dañinos trabajan de la siguiente manera: al conectar el dispositivo en uno de los puertos USB el malware se ejecuta en forma automática (valiéndose del archivo mencionado) y se copia en distintas ubicaciones de los discos locales (generalmente con atributos de oculto/sistema), infectando de esta manera a cada uno de los dispositivos donde se lo inserta. Asimismo, cada vez que un nuevo dispositivo de almacenamiento masivo es insertado en la computadora comprometida, el gusano se encargará de copiarse en el nuevo medio extraíble y así sucesivamente, infectando la máxima cantidad de dispositivos posibles.

Afectan a los sistemas Windows

Para desactivar la opción de reproducción automática:

1. *Menú Inicio > Ejecutar*
2. Escribir: **gpedit.msc** y pulsar "intro"
3. En el arbol de la izquierda, seguir esta ruta:
   Directiva de equipo local > Configuración del equipo > Plantillas administrativas > Sistema
4. Y en la ventana de la derecha, bajar hasta "Desactivar reproducción automática" (doble click)
5. Pinchar en "Habilitar", y elegir la opción:
   Desactivar reproducción automática en: Todas las unidades.



USB Vaccine: Sirve para tener "vacunado" nuestros sistemas de almacenamiento, impidiendo la propagación del autorun.inf

Algunos de los programas usados para desinfectar nuestro sistema del autorun.inf son:

Autorun Eater:

- una sencilla utilidad que remueve, monitorea, alerta y realiza marcas antes del eliminar virus de la memoria USB, es un instalador y reside en la memoria "RAM" y se ejecuta cada vez que prendes el computador o conectas alguna memoria infectada con virus, spiware o malware.

Flash_Disinfector:

- Una utilidad portable que no require instalacion, simplemente ejecutas el .exe con tu pendriver puesto y listo te lo desinfecta de una y rapidamente.

Ninja antivirus free:

- Es de lo mejor que he visto para la eliminacion y preveccion de la familia de los autorun, incluyendo soporte para:
- auto.exe
- autorun.inf
- autorun.ini

Entre otros.

2. HERRAMIENTAS PREVENTIVAS.

a) Configuración de contraseñas seguras:

-En Windows: Políticas de directivas de cuentas.

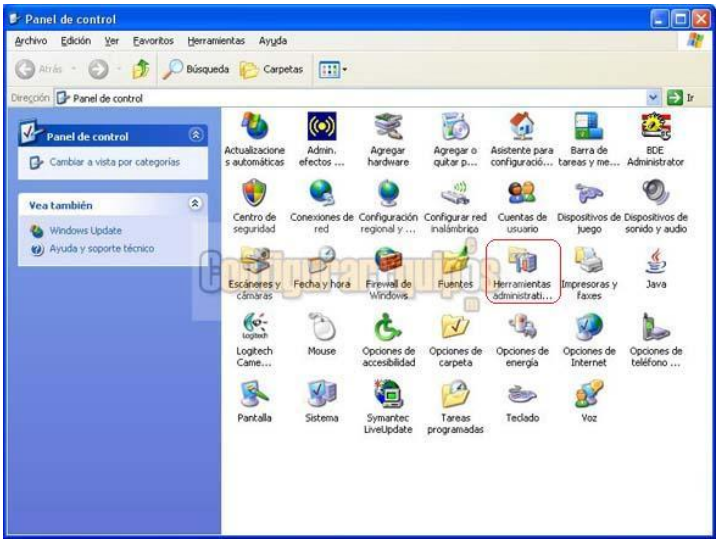
COMO CONFIGURAR LAS DIRECTIVAS DE CUENTAS EN WINDOWS XP.

Las directivas de cuentas nos permiten configurar el comportamiento que van a tener estas ante una serie de sucesos. La importancia de una correcta configuración de estas directivas radica en que desde ellas vamos a poder controlar de una forma más eficiente la forma de acceder a nuestro ordenador.

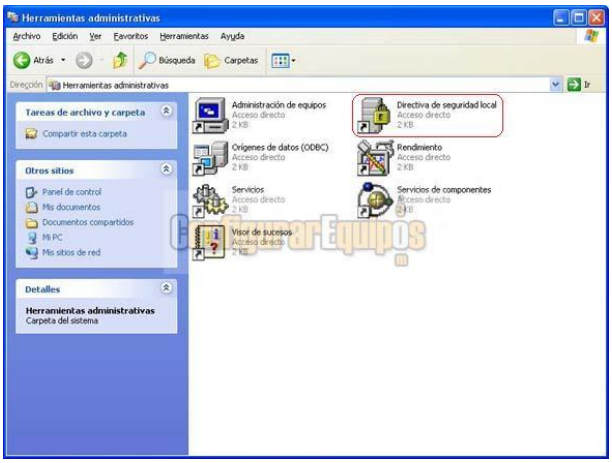
Vamos a ver cómo podemos configurar estas directivas en Windows XP Professional SP2.
Ante todo, estamos ante unas configuraciones **Administrativas**. Esto quiere decir dos cosas. En primer lugar, que solo los administradores de equipos pueden acceder a ellas, y en segundo lugar, que cuando toquemos algún parámetro dentro de este apartado debemos estar **muy seguros** de lo que estamos haciendo. No se trata de una parte de configuración con la que se puedan hacer experimentos, ya que podemos dejar inaccesible nuestro sistema operativo.

Dicho esto, vamos a ver en primer lugar como accedemos a la ventana de **Directivas de seguridad de cuentas**.

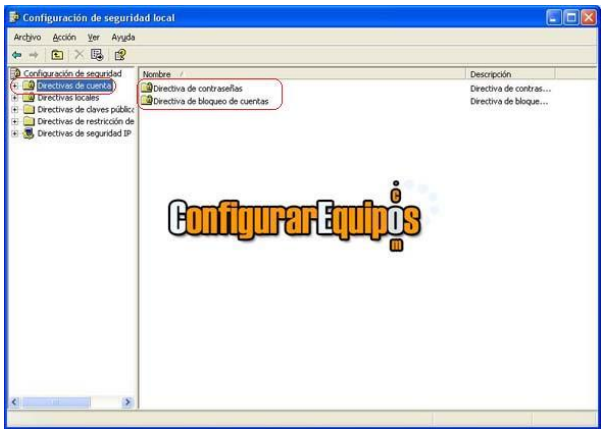
En primer lugar entramos en el **Panel de control** (es conveniente activarlo en modo *Vista clásica*).



Dentro de este tenemos el icono de acceso a **Herramientas administrativas**.



Una vez que entramos en **Herramientas administrativas**, tenemos el apartado **Directiva de seguridad local**.



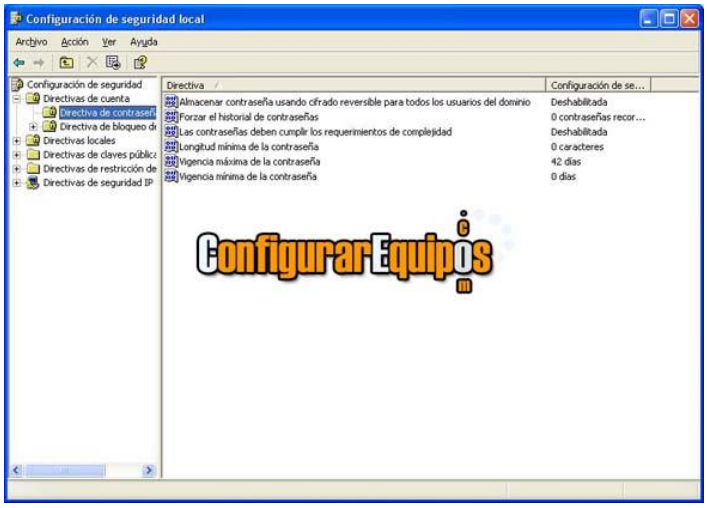
Una vez en la ventana de las **Directivas de seguridad local** nos encontramos a la izquierda con varias directivas. Estas son:

- Directivas de cuentas
- Directivas locales
- Directivas de claves públicas
- Directivas de restricción de software
- Directivas de seguridad IP en equipo local

Vamos a tratar la primera de ellas, que son las **Directivas de cuentas**.

Como podemos ver, en este grupo de directivas tenemos dos subgrupos, **Directiva de contraseñas** y **Directiva de bloqueo de cuentas**. Vamos a ver qué podemos hacer en cada uno de ellos:

DIRECTIVA DE CONTRASEÑAS:



Dentro de las directivas de contraseña nos encontramos con una serie de seis directivas, que vamos a estudiar a continuación.

Al hacer clic sobre ellas se nos muestran unas ventanas de configuración como las que podemos ver en las imágenes **A** y **B**, que dependiendo de la directiva nos mostrará un tipo de interfaz para seleccionar la opción correspondiente.

Imágenes **A** y **B** de las ventanas de selección.

Bien, veamos cuales son estas directivas:

Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio.
Su mismo nombre indica para qué se utiliza. Las opciones son **Habilitado** o **Deshabilitado**.

Forzar el historial de contraseñas.
Establece el número de contraseñas a recordar.

Las contraseñas deben cumplir los requerimientos de complejidad.
Obliga a que las contraseñas cumplan unos requisitos de complejidad.

Longitud mínima de la contraseña.
Obliga a que las contraseñas tengan un mínimo de caracteres, estableciendo este mínimo.

Vigencia máxima de la contraseña.
Establece el número de días máximo que una contraseña va a estar activa.

Vigencia mínima de la contraseña.
Establece el número de días mínimos que una contraseña va a estar activa.

- En GNU/Linux: Módulo pam_cracklib.

Una de las principales cuestiones que ha abordar en todo sistema en el que se quieran mantener contraseñas de calidad seria obligar a todos los usuarios de ese sistema a cumplir las mismas reglas, por eso una buena solución es utilizar una herrmanienta que rechace las contraseñas malas.

De modo, que cuando los usuarios cambien su contraseña sea verificada para ver si cumple los requisitos establecidos y si no los cumple sería rechazada.

Para conseguir este objetivo, podemos utilizar la libreria pam_cracklib.so, que es una versión de libreria cracklib desarrollada por Alee Muffet y transformada en modulo PAM que comprueba la fortaleza de las contraseñas.

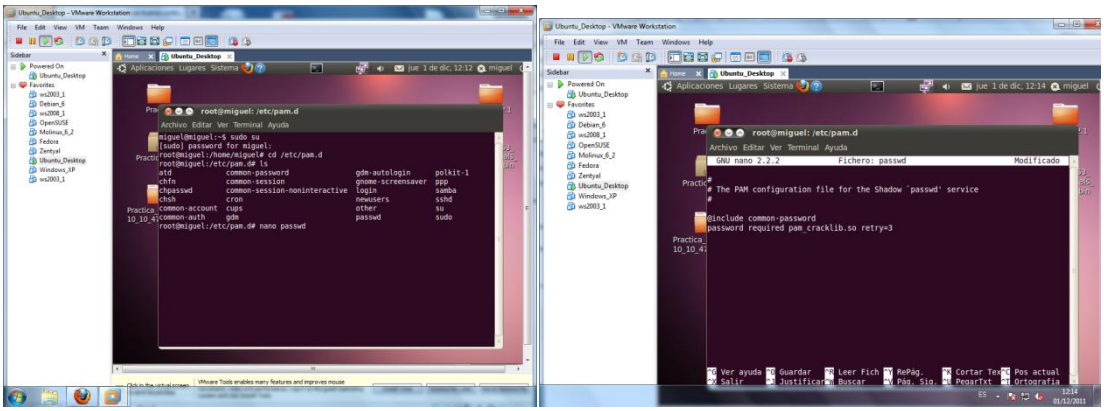
Lo primero que hace es llamar a la rutina cracklib para comprobar si la contraseña puede ser fácilmente averiguada, si se pasa este obstáculo, entonces el módulo pam_cracklib.so realiza las siguientes pruebas:

* Mira si la contraseña vieja es muy parecida a la nueva
* Mira si la contraseña es muy corta
* Comprueba que la contraseña no sea palíndroma.
* Comprueba si la vieja contraseña es una versión rotada de la vieja.

Para hacer que pam_cracklib.so sea el módulo encargado de verificar la calidad de las contraseñas, hay que sustituir el módulo existente pam_unix.so, simplemente añadiendo las siguientes líneas al fichero **/etc/pam.d/passwd**

pasword required pam_cracklib.so retry=3

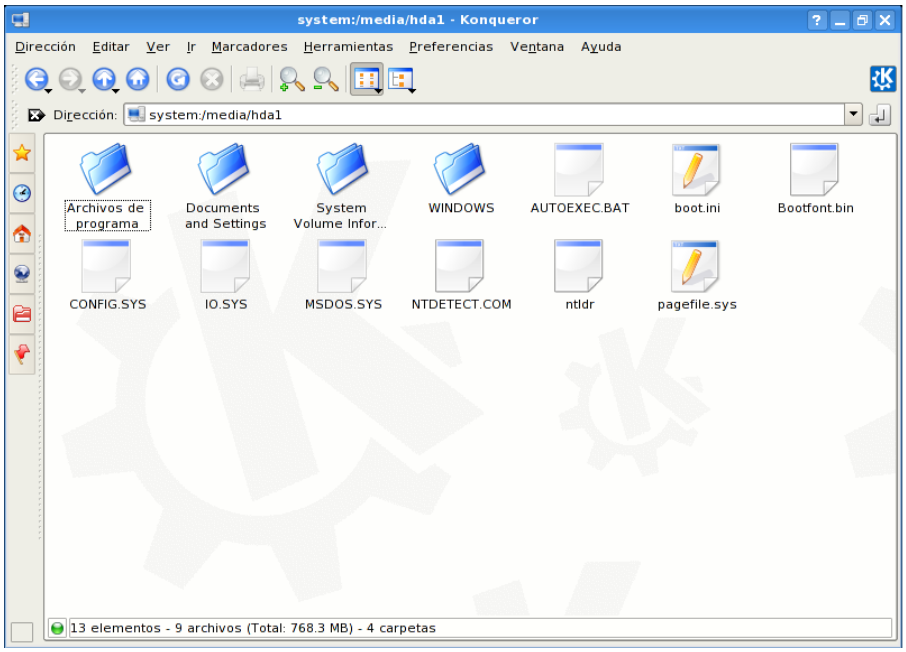
De esta forma le damos al usuario tres oportunidades para que genere una contraseña fuerte.



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

- Uso de DVD Live de Backtrack para acceder a los datos.

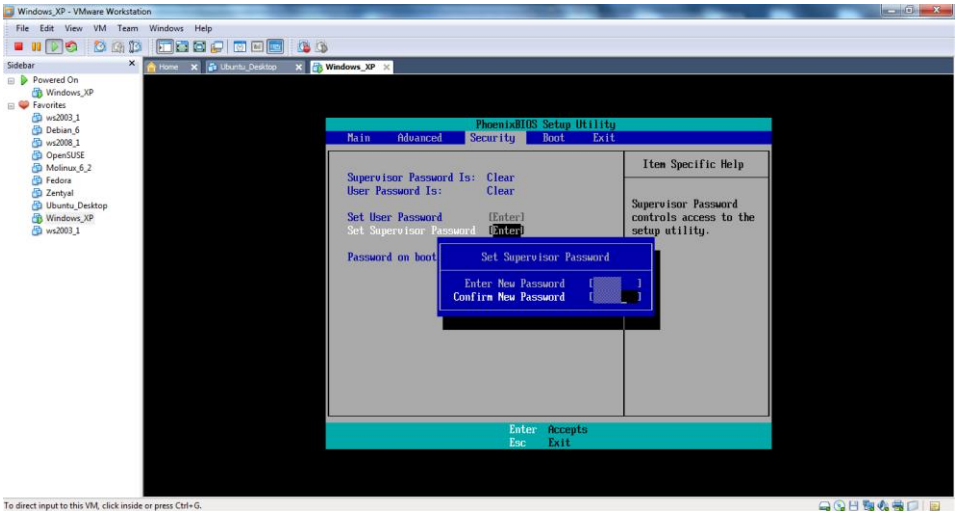
Podemos acceder a los datos de nuestra máquina virtual, arrancando con el live del Wifiway y usando el Konqueror de la aplicación Wifiway. Esto es un grave riesgo de seguridad de nuestros datos, ya que se puede tener acceso a estos archivos fácilmente.



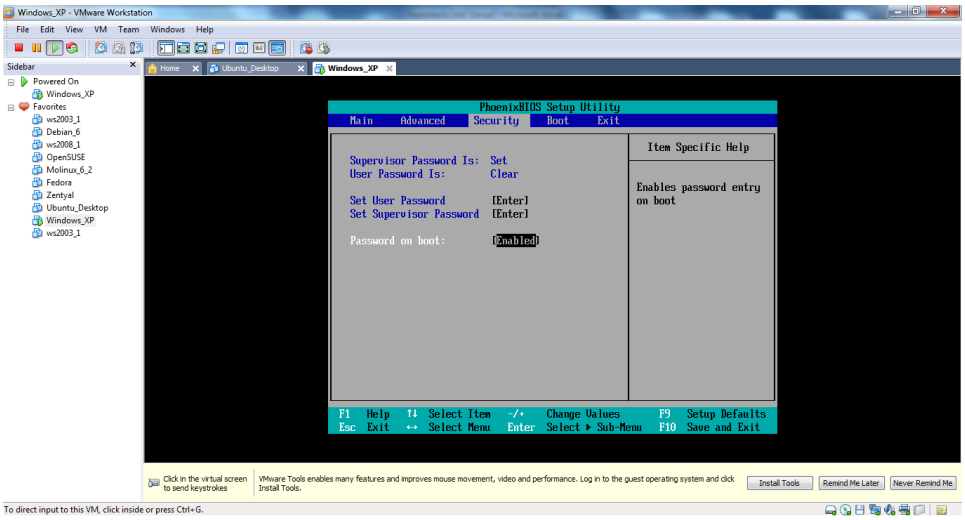
c) Configurando contraseñas en la BIOS:

- Asignar contraseña a la BIOS y observar su vulnerabilidad.

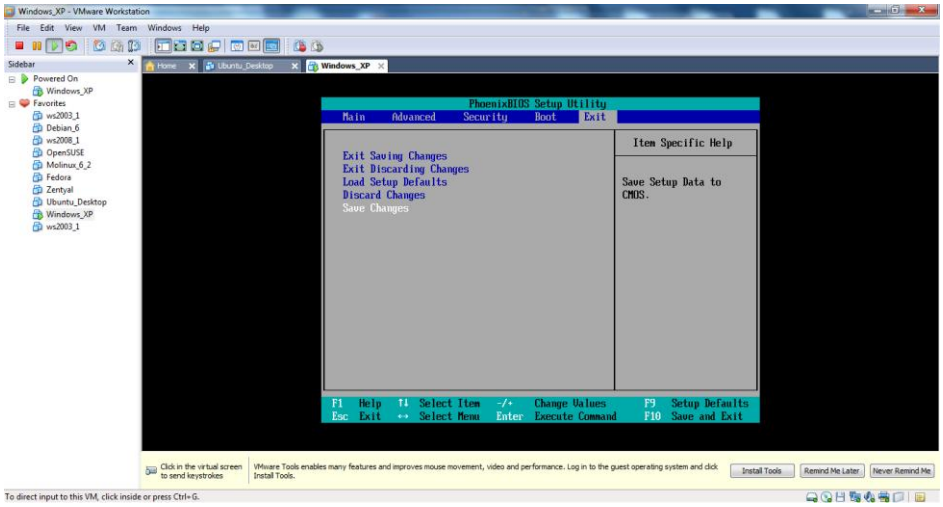
Una vez accedido a la BIOS del sistema, nos situamos en la pestaña **Security,** para habilitar la opción de contraseña en el arranque de la misma, nos vamos a la opción **Ser Supervisor Password** , la habilitamos y establecemos una contraseña.



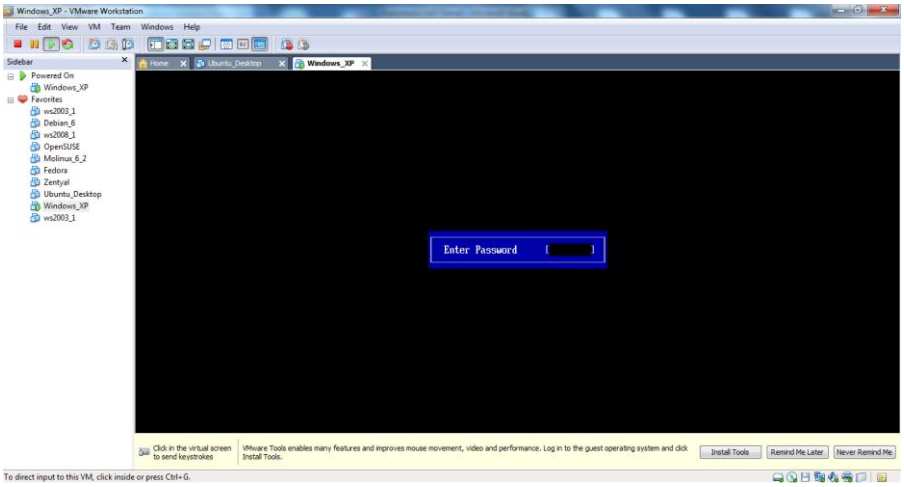
Habilitamos también la opción de **Password en boot.**



Una vez concluida la configuración, nos vamos a la pestaña **Exit**, y salimos **salvando los cambios.**



Si intentamos entrar a la BIOS de nuevo, nos pedirá la clave de acceso.



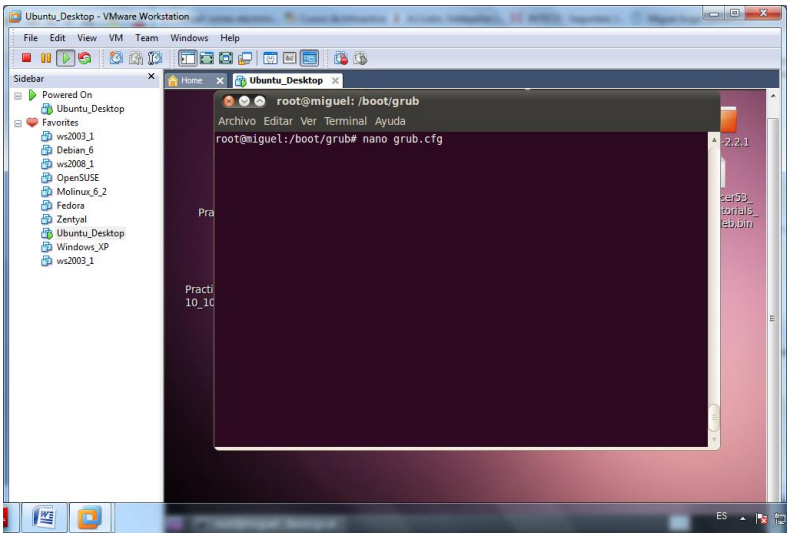
La vulnerabilidad de esta contraseña, reside en la memoria, donde se guarda ésta misma, la cual se suele alojar en una memoria alimentada por una pila o batería o bien se encuentra configurada con unos jumperes. Pues bien si modificamos cualquiera de estos conceptos, podemos eliminar la clave de acceso.

d) Contraseñas en el gestor de arranque:

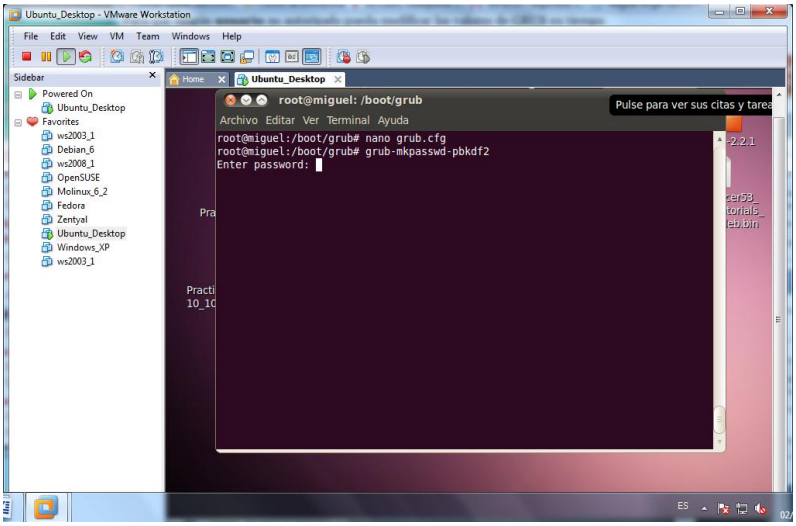
- Práctica con GRUB

Vamos a establecer una contraseña nueva, para el gestor de arranque o GRUB. Debemos situarnos en el directorio **/boot/grub**.

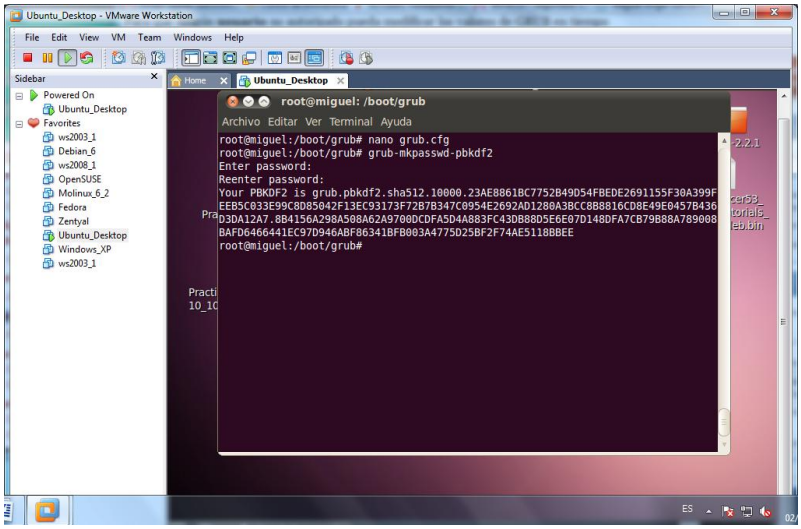
Podemos hacer un **nano grub.cfg** para comprobar el fichero de configuración del GRUB.



Como queremos establecer una contraseña, vamos a generar una nueva clave, por lo tanto introducimos el comando **grub-mkpasswd-pbkdf2**, a continuación introducimos la nueva clave, que le asignaremos al grub.

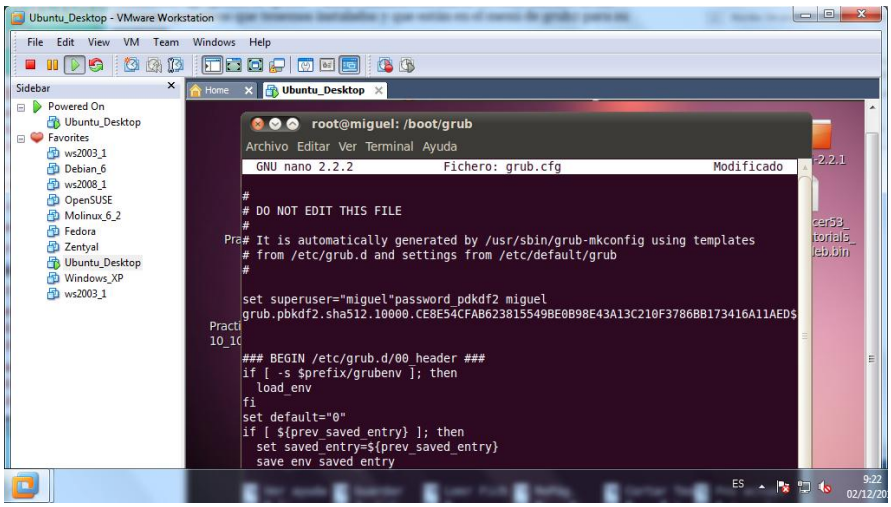


La clave nos la generará en hexadecimal, la cual vamos a copiar.

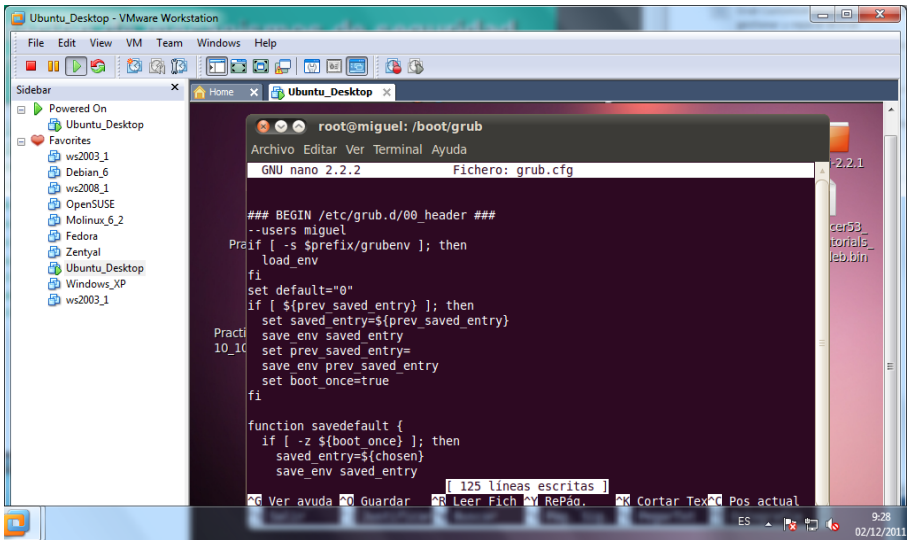


Editamos el fichero de configuración del grub, con el "**nano grug.cfg**".

Configuramos el fichero de la siguiente manera, pegando la clave de acceso al grub encriptado.



Por último podemos hacer referencia a nuestro usuario. En nuestro caso miguel.

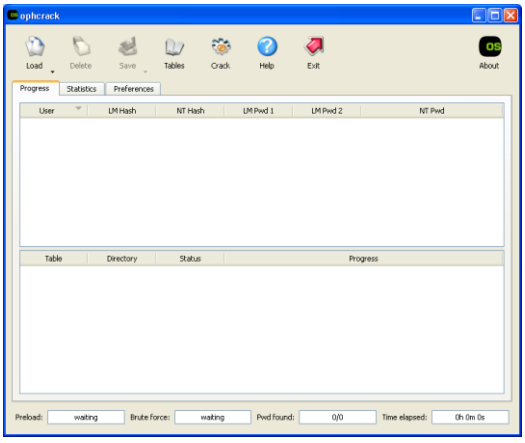


e) Recuperación de contraseñas:

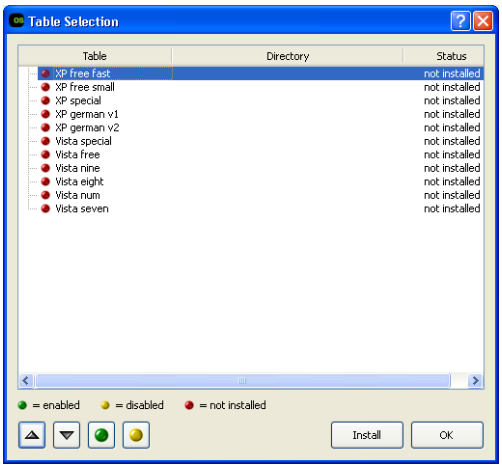
- En Windows: Ophcrack.

Instalamos esta aplicación para sacar las contraseñas de los usuarios de nuestro sistema operativo Wndows.

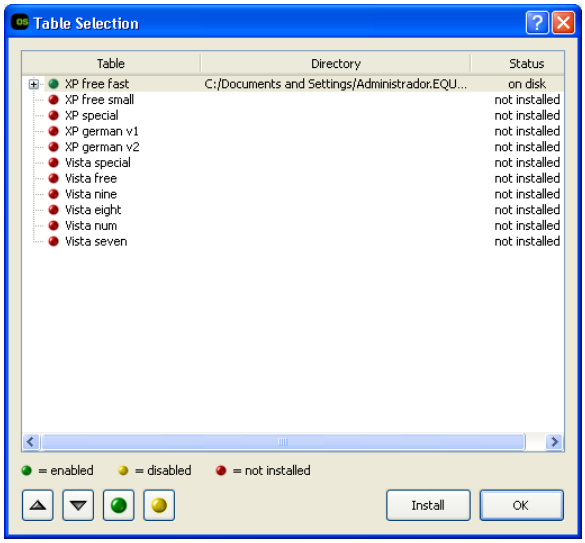
Una vez instalado el programa, lo arrancamos y nos debería salir la siguiente pantalla.



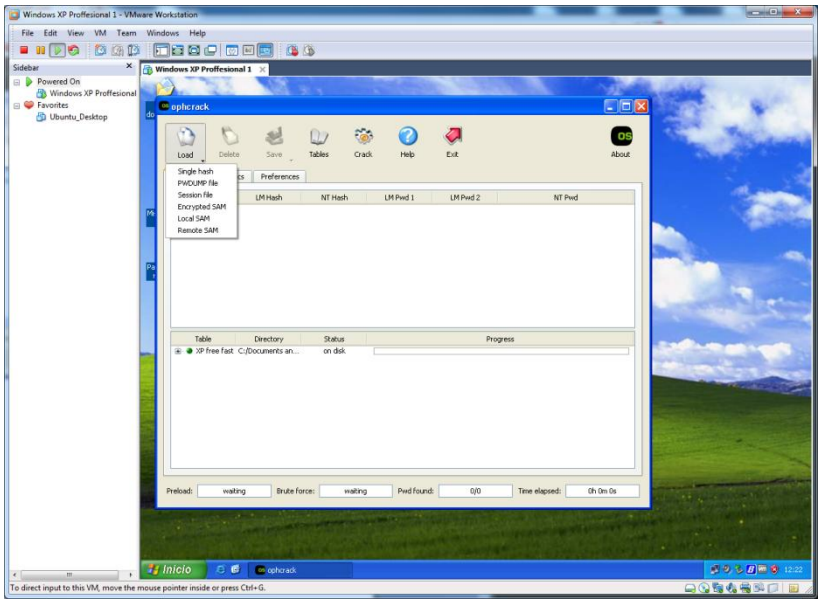
Para sacar las claves, debemos asignarles unas tablas, pulsamos el botón de tablas, y seleccionamos en nuestro caso, las tablas de XP.



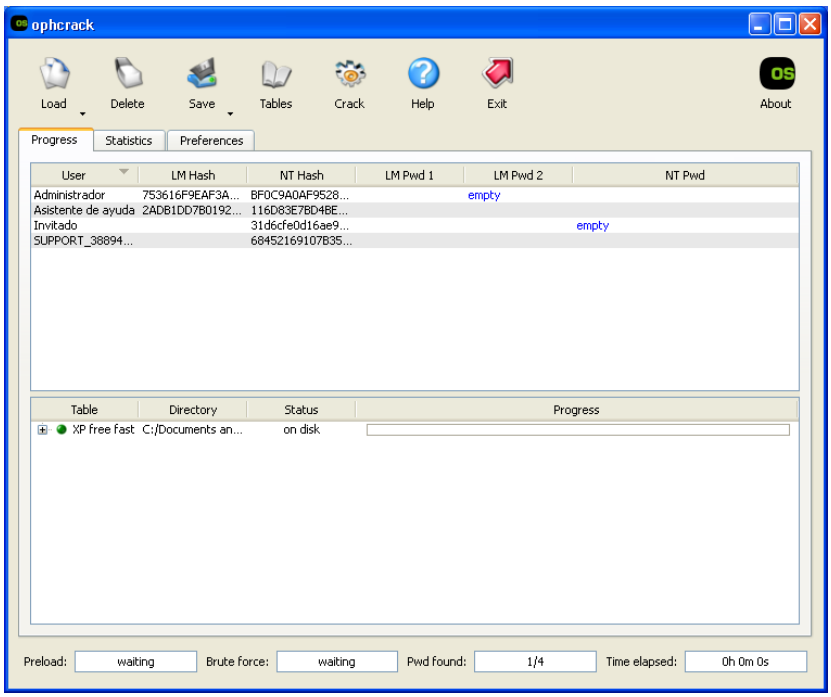
Una vez seleccionado, instalamos las tablas que necesitamos, situadas en el escritorio, que hemos preparado y descargado anteriormente.



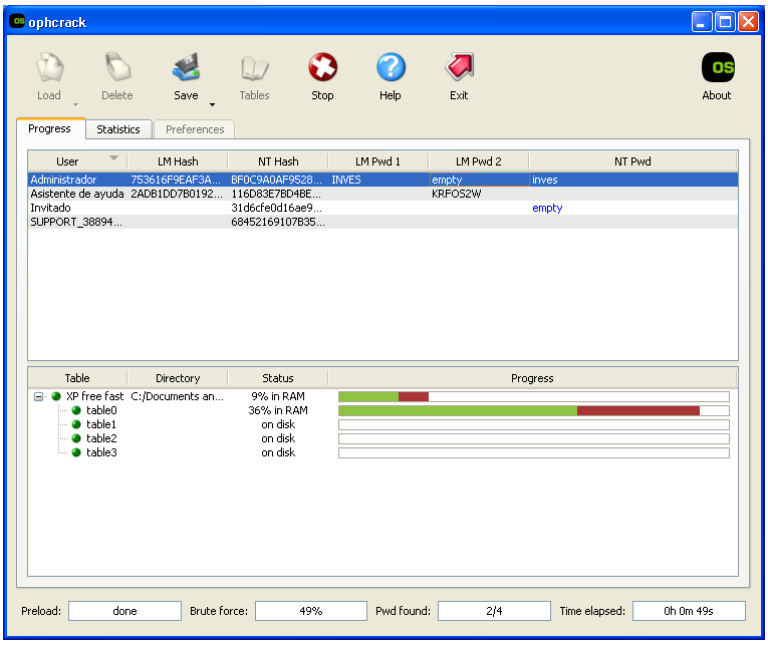
Una vez que tengamos las tablas instaladas correctamente, es el momento de escanear la información de nuestro sistema para sacar las claves.



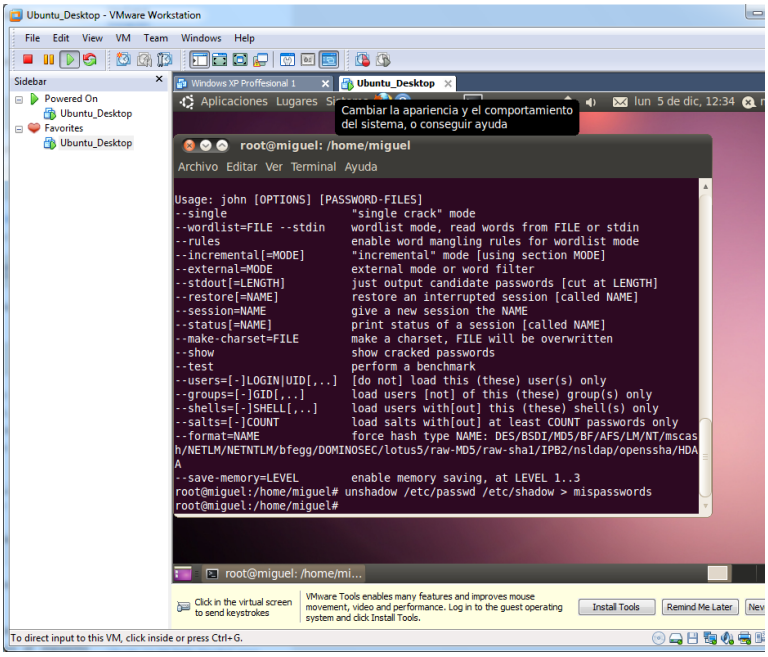
Pulsamos el botón de **load**, para iniciar el escaneamiento.



Una vez concluida esta operación, ya tendremos disponible la clave de los usuarios que tengamos en nuestro sistema operativo.



- En GNU/Linux: Aplicación John the Ripper.



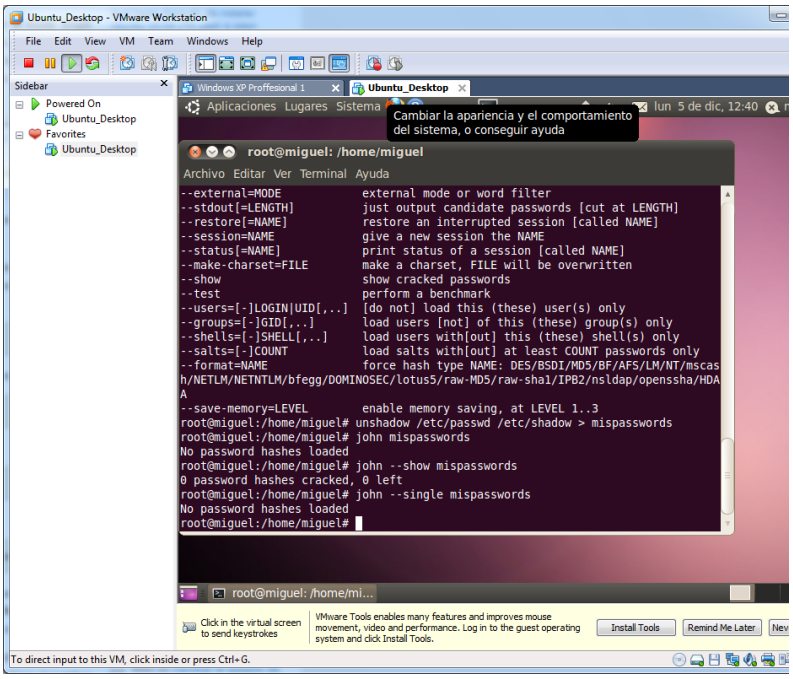
Combinamos los arhivos /etc/passwd y /etc/shadow con el comando *unshadow* en un nuevo archivo con el nombre *mispasswords*:

```
sudo unshadow /etc/passwd /etc/shadow > mispasswords
```

Por último, ejecutamos John the Ripper sobre el archivo que hemos creado con *unshadow*.

john mispasswords

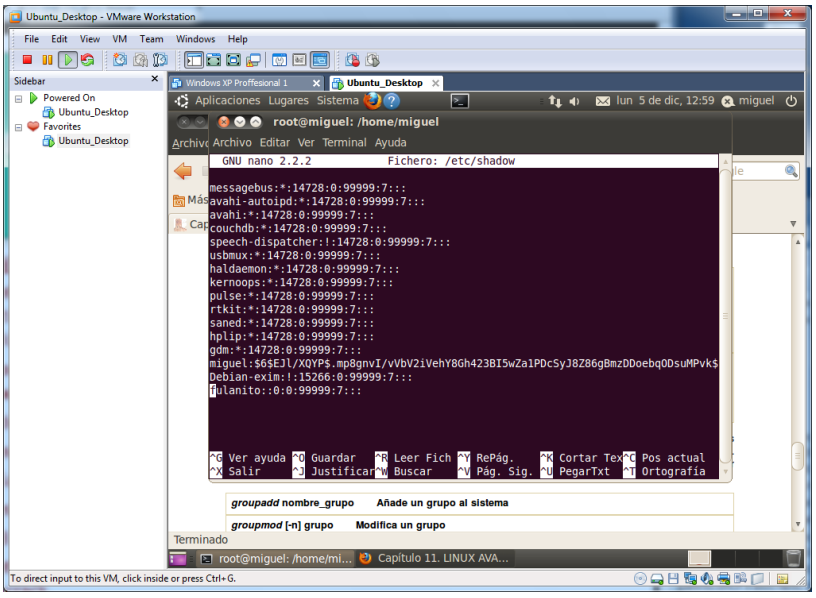
Actualizamos, todo el sistema, por si nos falta algún archivo. Pero no nos funciona esta aplicación.



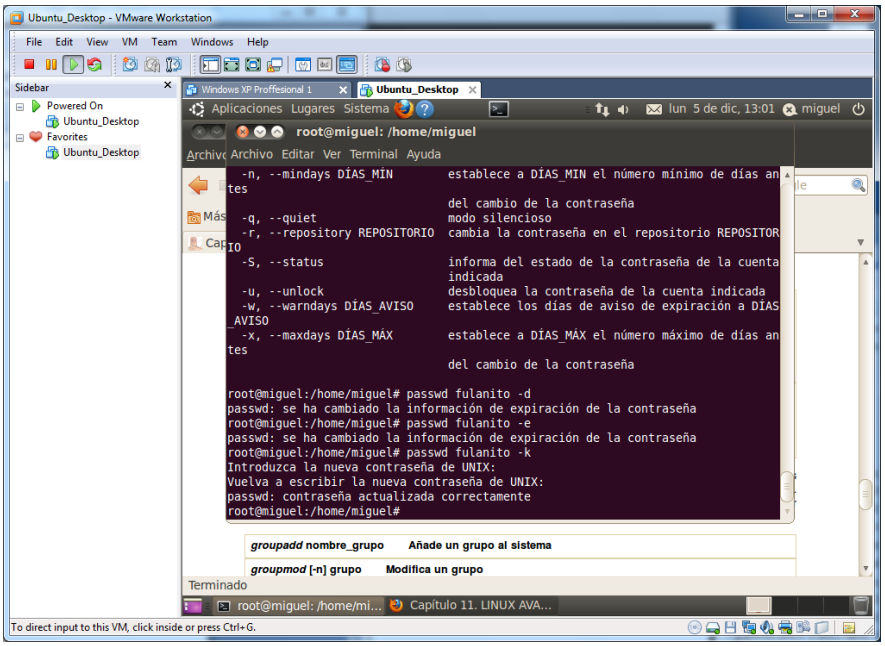
f) Modificación de contraseñas:

- En GNU/Linux: mediante el sistema, modificando /etc/shadow.

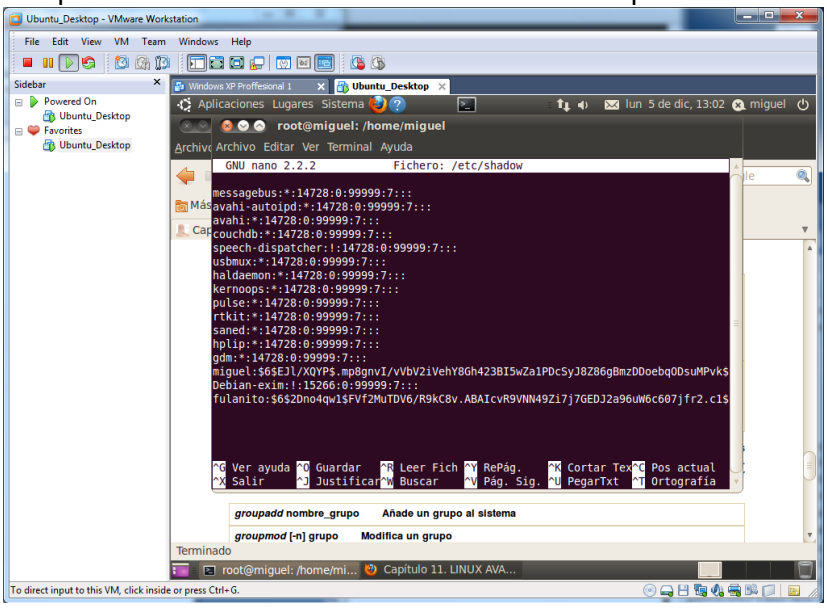
Abrimos el fichero shadow mediante el comando "**nano /etc/shadow**".
Queremos cambiar la contraseña al usuario "fulanito"



En primer lugar tenemos que eliminar la contraseña vieja de este usuario, para ellos utilizamos el comando "**passwd fulanito -d**", más tarde usamos el comando "**passwd fulanito -e**", para eliminar la información de expiración de la contraseña, y por último utilizamos "**passwd fulanito -k**", para introducir una nueva contraseña.



Podemos ver que se ha creado la nueva contraseña en el fichero "**/etc/shadow**", en nuestro usuario podemos observar nuestra contraseña encriptada.



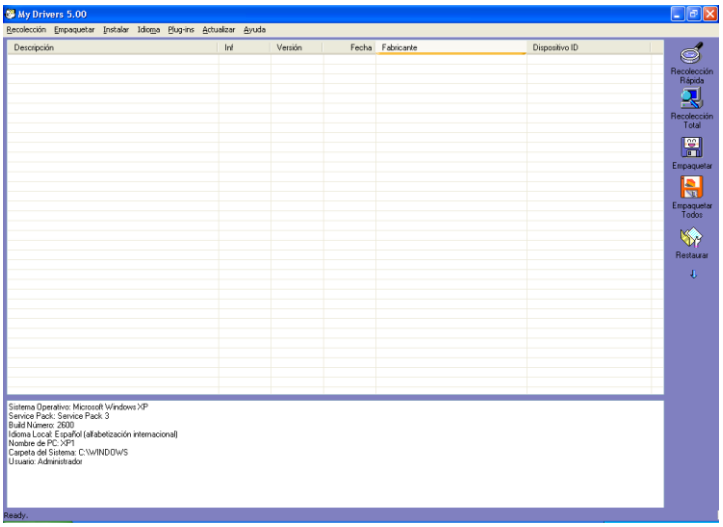
g) Realizar una copia de seguridad de drivers

- Utiliza el software "DriverMax" o similar.

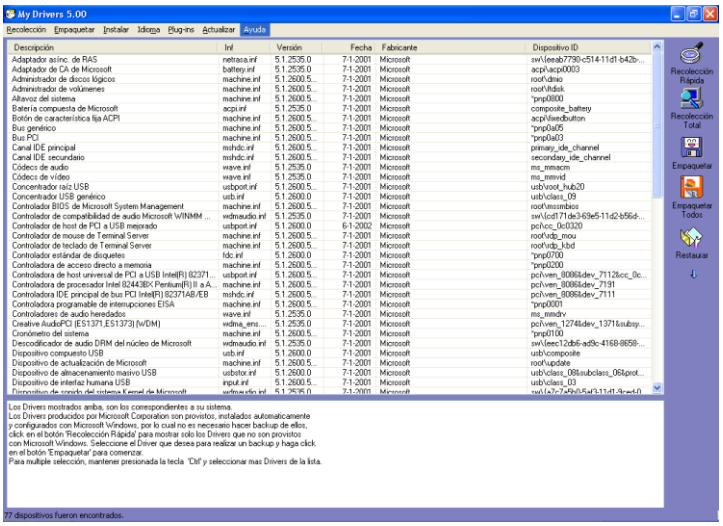
Vamos a utilizar la aplicación *MyDrivers,* esta aplicación nos puede proporcionar una copia de todos los driver de nuestro sistema.

Una vez lo tengamos instalado, administramos los driver de todos los dispositivos.

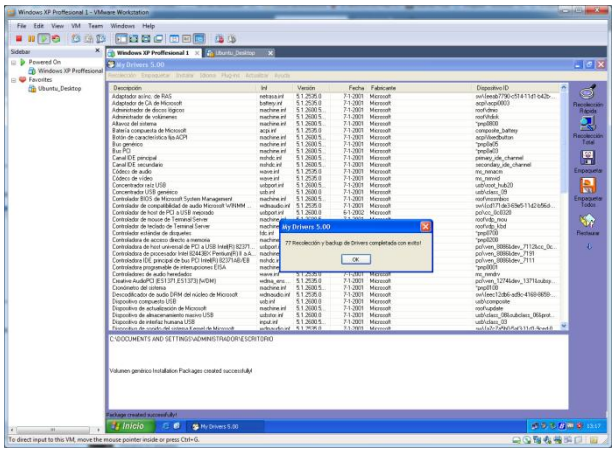
Nos abrirá la siguiente ventana, y tenemos opciones como por ejemplo, la de recopilación total, que es la que vamos a usar para reunir los drivers.



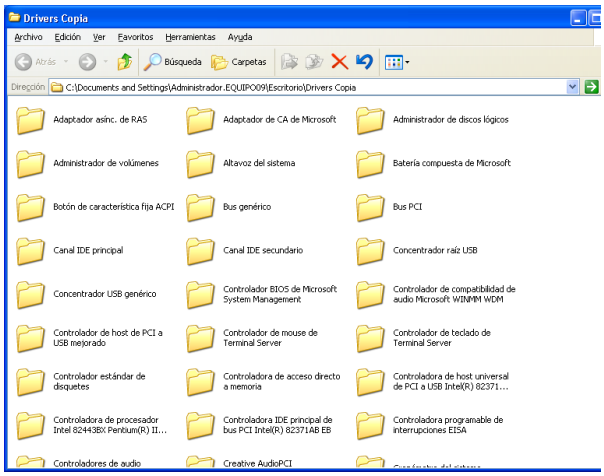
Nos aparecerán todos los drivers que se han reconocido de nuestro sistema.



Una vez identificado, guardamos la copia de los driver con el botón de empaquetar, y los guardamos en el escritorio por ejemplo.

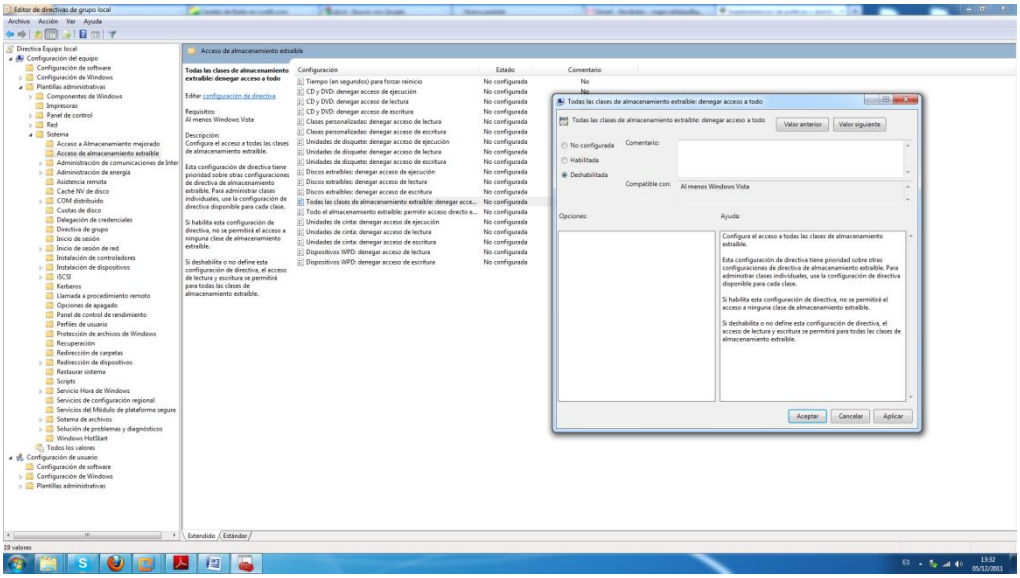


Comprobamos que nos ha efectuado las copias, y efectivamente obtenemos nuestro resultado.



h) Control de acceso a datos y aplicaciones:

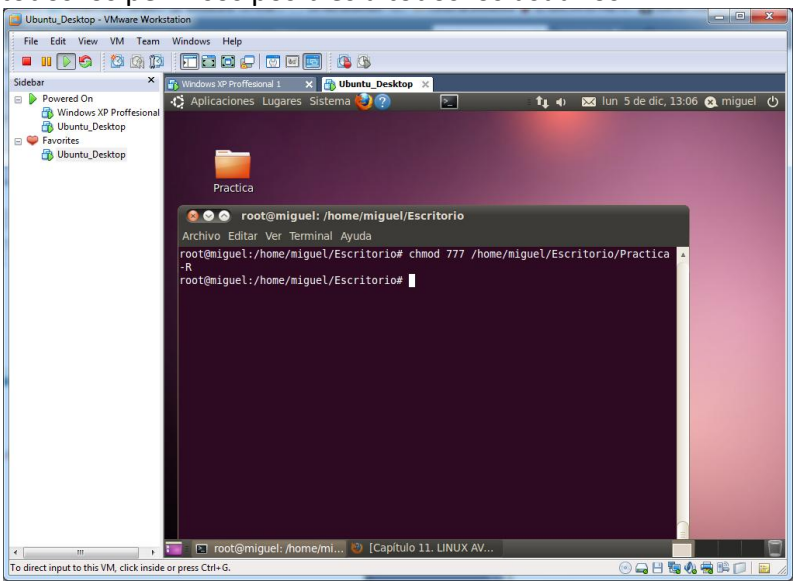
- En Windows: Política de directivas de seguridad local.



- En GNU/Linux: chmod, chown, chgrp, getfacl, setfacl.

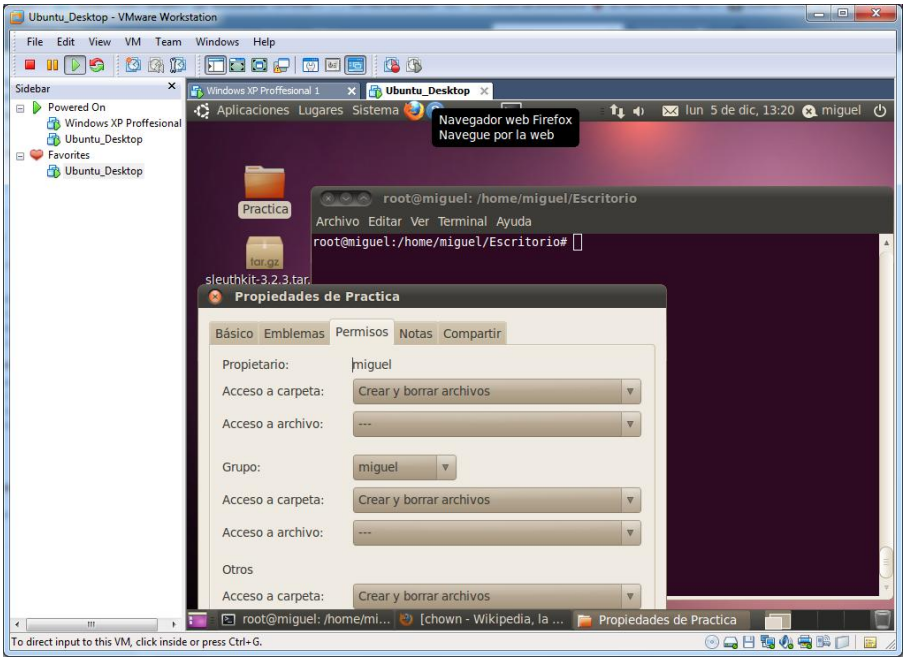
Chmod

Con este comando, podemos cambiar los permisos de nuestros ficheros y directorios, para ello asignamos unos números del 1 al 7 basándonos en los permisos UGO.
Por ejemplo vamos a cambiar los permisos al directorio Practica del escritorio, dando todos los permisos posibles a todos los usuarios.

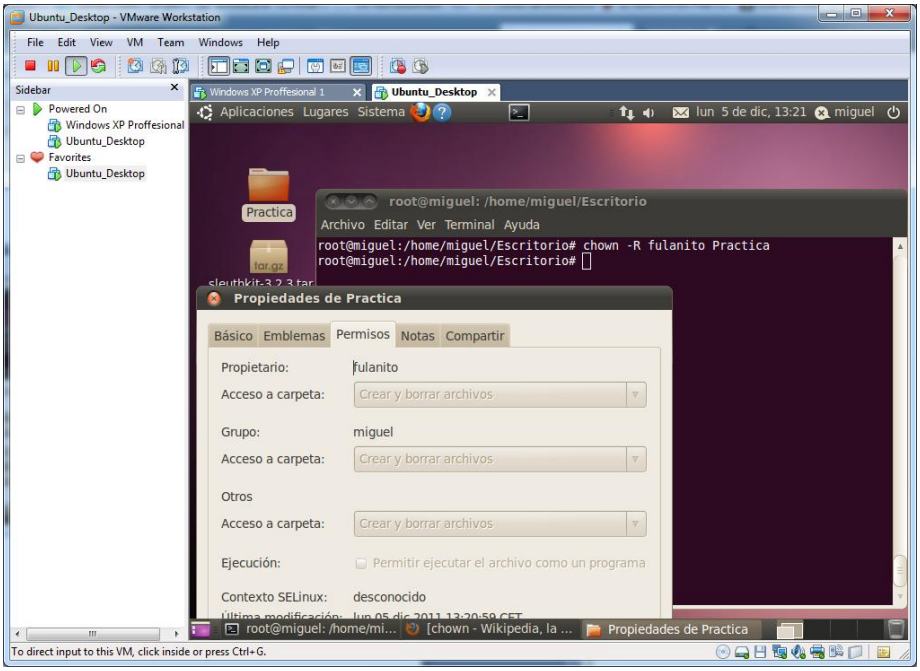


Chown

Cambiamos el propietario para que pase a ser fulanito a *Practica*, todos los archivos y subdirectorios contenidos en él, cambiándolos también de forma recursiva en todos archivos de los subdirectorios.

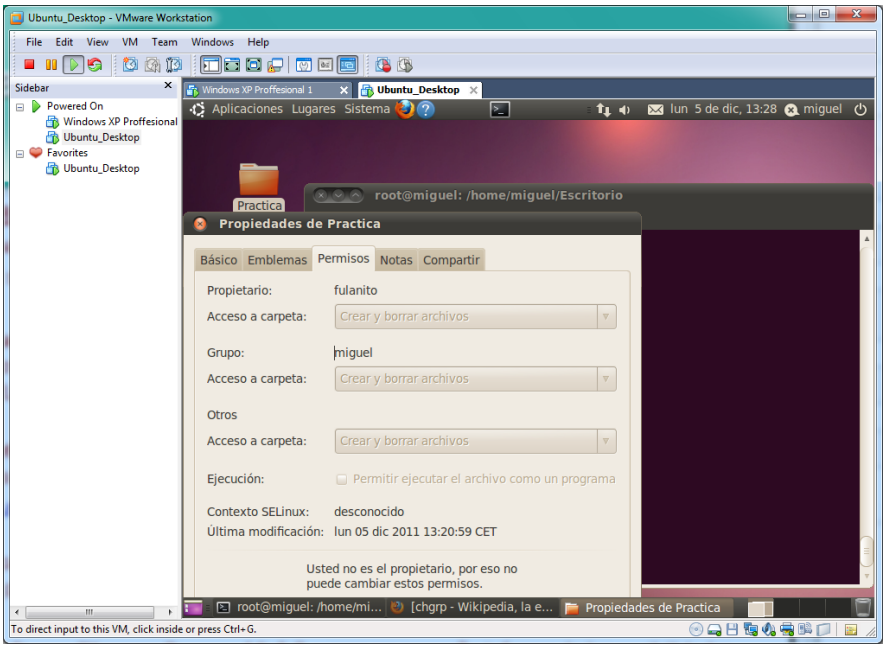


Para ello usamos el comando "**chown –R fulanito Practica**"

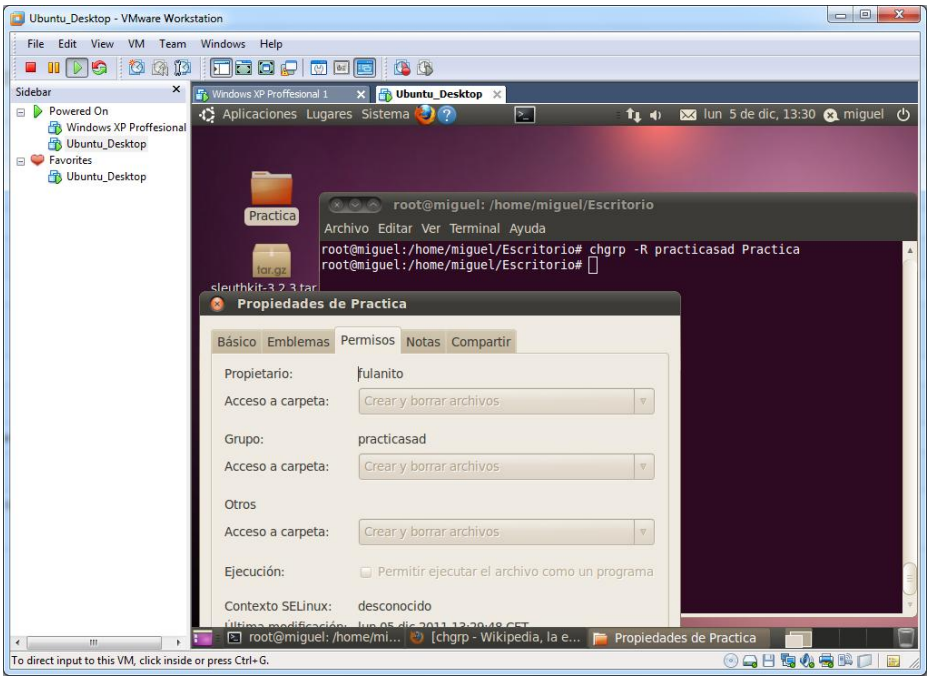


Chgrp

El comando **chgrp** permite cambiar el grupo de usuarios de un archivo o directorio en sistemas tipo UNIX.



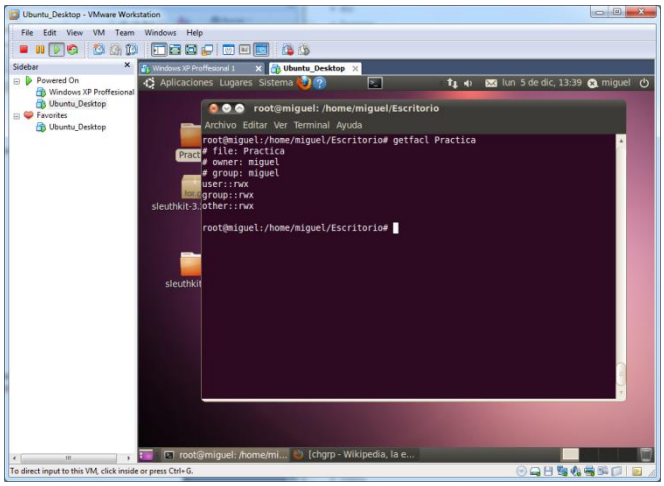
Cambiamos el grupo para que pase a ser practicasad a *Practica*, todos los archivos y subdirectorios contenidos en él, cambiándolos también de forma recursiva en todos archivos de los subdirectorios.



Getfacl

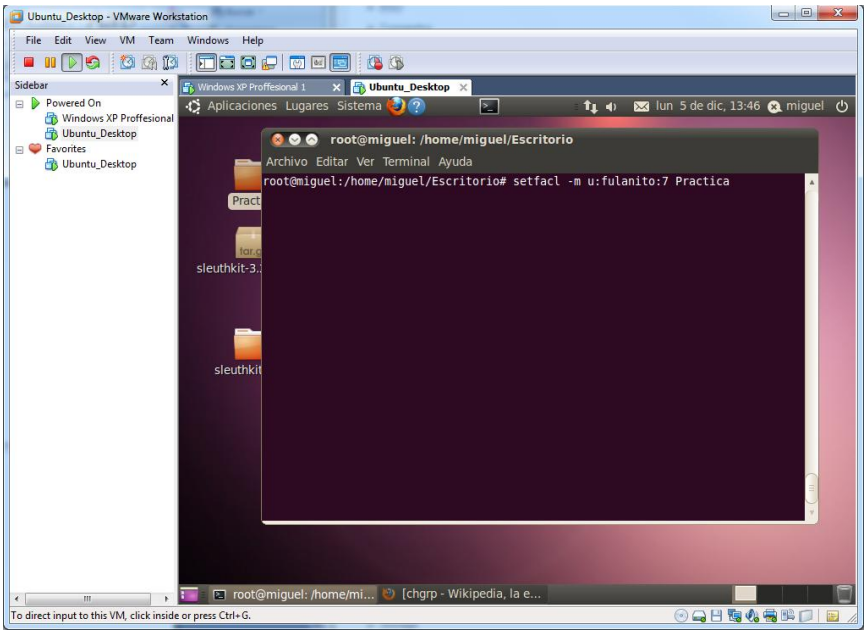
Para listar los permisos genéricos de un fichero o directorio y las ACL utilizamos el comando **getfacl**

Por ejemplo "**getfacl Practica**".



Setfacl

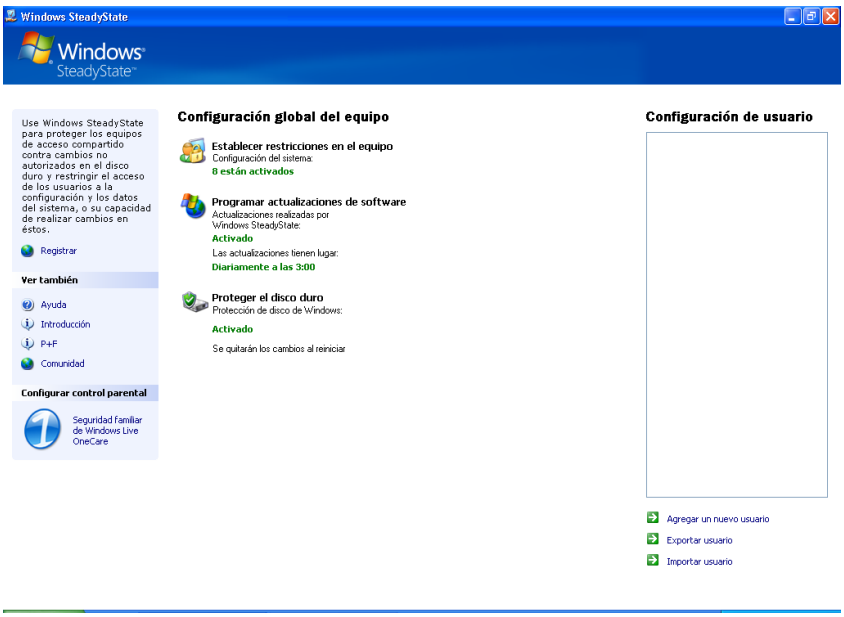
Permite cambiar permisos de un fichero o directorio. En este caso vamos a asignar permiso total (777) al usuario fulanito contra el fichero anterior, del cual es propietario miguel.



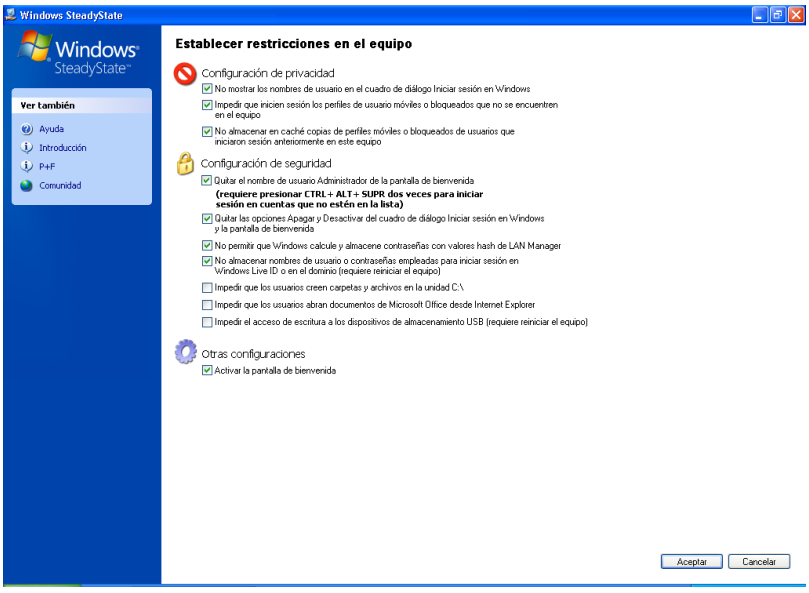
i) Utiliza el sotware "Windows SteadyState", y crea un pequeño informe de las posibilidades del mismo, desde un punto de vista de seguridad informática.

Windows Steady State es un software gratuito de Microsoft para los sistemas operativos *Windows XP* y *Windows Vista* que permite una gestión avanzada del sistema enfocada al uso compartido del sistema, por decirlo de alguna manera permite

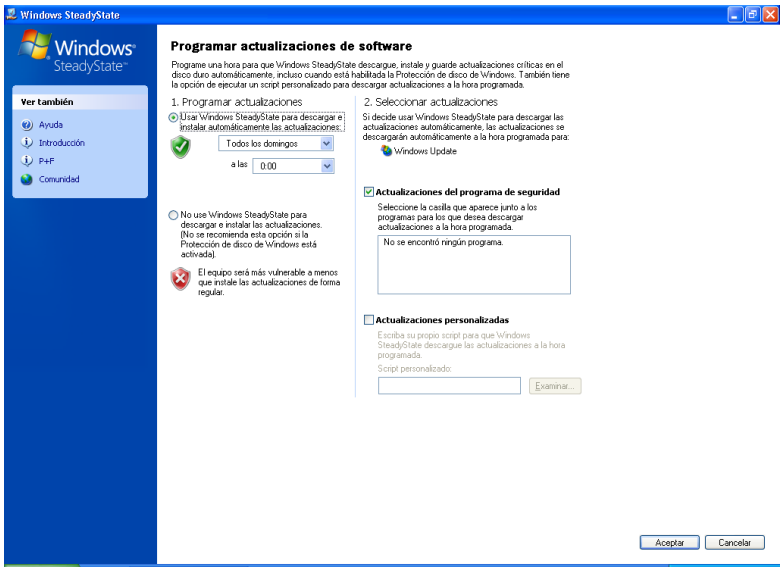
modificar ciertos parámetros para establecer un nivel de seguridad y estabilidad adecuado al uso público de un PC con Windows.



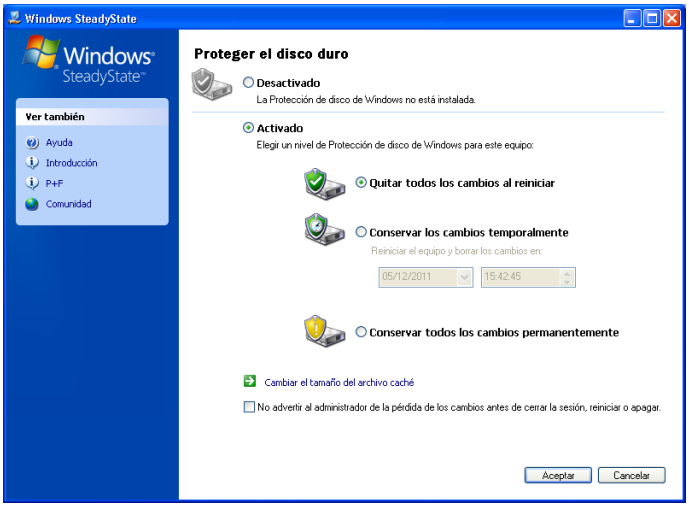
Podemos configurar algunas políticas de seguridad en nuestro sistema operativo, asimismo como elegir los usuarios indicados.



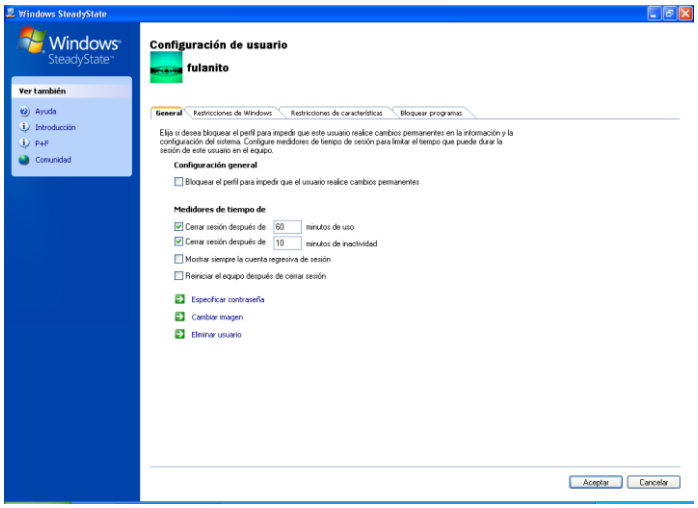
Podemos programar las actualizaciones de software para elegir cómo y cuándo actualizar el sistema.



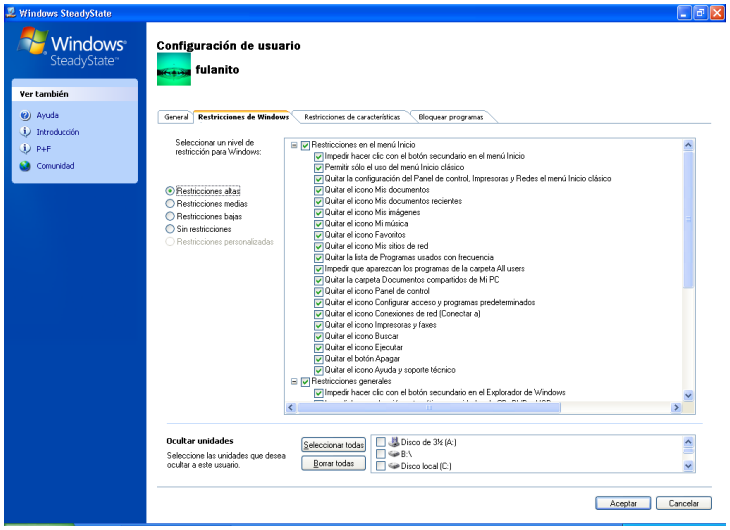
También podemos proteger o *congelar* el disco duro, para no guardar los cambios del sistema al reiniciar.



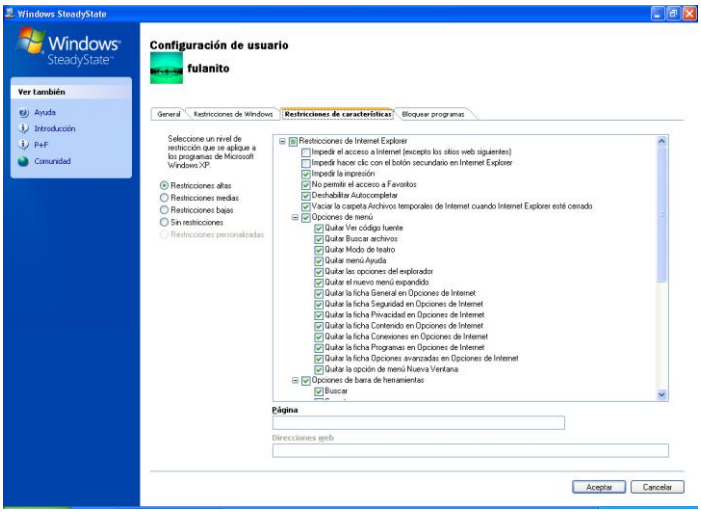
En el control de usuario podemos configurar distintos parámetros de nuestros usuarios, para que tengan unas políticas determinadas.



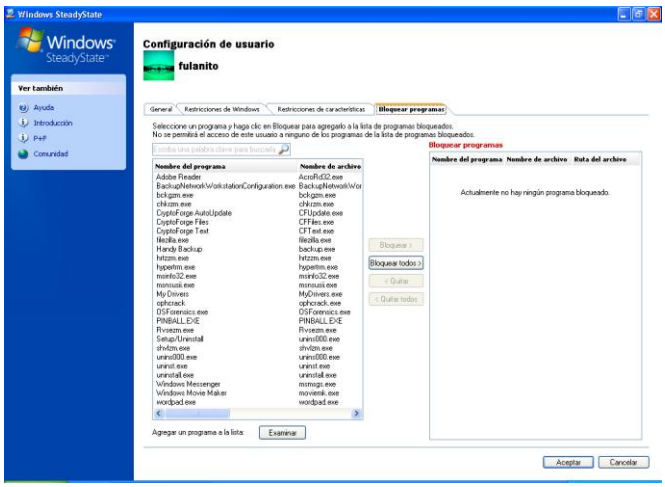
Podemos indicar una serie de restricciones en nuestros usuarios relacionadas con nuestro sistema operativo.



Podemos restringir a nuestros usuarios algunas características.



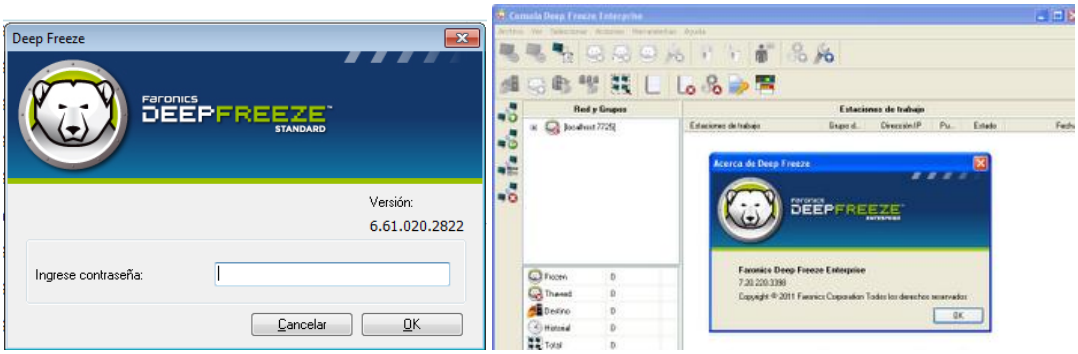
Por último también podemos bloquear usuarios para que no dispongan de diferentes aplicaciones.



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

WINDOWS:

- **Deepfreeze**



Funcionamiento

El programa permite congelar nuestro disco duro de manera que trabajamos normalmente con él (crear y borrar archivos, instalar y desinstalar programas, modificar el aspecto del escritorio, etc) pero cuando arranquemos de nuevo, ningún cambio habrá tenido efecto, es decir: el disco duro tendrá exactamente el mismo contenido que al principio. Si queremos instalar un programa debemos desactivar la congelación, instalarlo y volver a activar la congelación. Estas activaciones y desactivaciones no se producen de forma instantánea sino que surten efecto en el siguiente arranque del sistema, por lo que para instalar un programa habrá que volver a arrancar el sistema 2 veces (aparte de la que la propia instalación del programa pueda requerir).

Inconvenientes

Los inconvenientes de este sistema de protección están en los mecanismos de activación y desactivación anteriormente mencionados. Es verdad que no se instalan programas todos los días, pero hay otras operaciones más cotidianas como recibir y enviar correo, agregar una dirección a Favoritos, crear y guardar un archivo, etc… que requerirían la desactivación del Congelador, lo que haría su uso especialmente incómodo.

Posibilidades

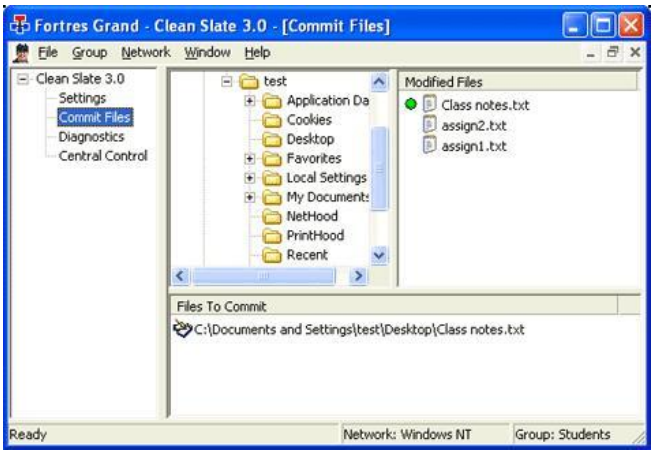
Entre sus múltiples posibilidades, Deep Freeze Standard permite la protección por password, protege el CMOS, el Master Boot Record, soporta múltiples discos duros y particiones, soporta SCSI, ATA, SATA, IDE y es compatible con FAT, FAT32 y NTFS.
Deep Freeze no protege contra los reinicios con disquetes de arranque o unidades de CD-ROM.
Es recomendable configurar el CMOS para evitar el inicio del equipo con disquetes de arranque o unidades de CD-ROM y el CMOS debe ser protegido con una contraseña.
Deep Freeze Enterprise es ideal para grandes entornos informáticos.

- **Shadow User**

La ventaja que tiene es que puedes elegir las carpetas que no quieras que se restauren cuando reinicias el pc. Así por ej., elegimos la carpeta donde se guarda una copia de seguridad diaria, etc.
La desventaja, es que consume muchos recursos, relentiza el pc, y no permite usar algunos programas (como por ejemplo msn.) Además de otros problemas que no lo hacen comparable con otros congeladores como el DeepFreeze.

- Puedes congelerar Document & Settings, o solo algunas carpetas de usuario.
- Puedes congelar solo las carpetas Temp de los usuarios.
- Puedes congelar directorios completos, como Windows y Archivos de programas, o cualquiera de sus sub carpetas.

- **Clean Slate**



Similar al Shadow user, con las mismas ventajas, y las mismas desventajas. Es una alternativa de aplicación de congelamiento de discos.

El programa está diseñado para garantizar la integridad de un sistema operativo utilizado por varios usuarios inexpertos o malintencionados. En una serie de ventanas, el administrador puede controlar los privilegios y permisos. El principal se refiere a que la alteración de los archivos de sistema no es permanente. Cuando un usuario reinicie su sesión todo volverá a estar como estaba: ficheros borrados, programas instalados, descargas, virus, troyanos, carpetas, iconos, etc.

GNU/LINUX:

- **Lethe**

Lethe es un congelador de particiones similar a Deep Freeze totalmente libre para Lihuen GNU/Linux y Debian GNU/Linux (probablemente funcione en otras distribuciones derivadas como Ubuntu, pero no se han hecho pruebas). Lethe hace funcionar las particiones del o los discos rígidos como si fueran un Live CD. Todos los cambios que se realicen sobre el sistema de archivos en realidad no se guardan si no que se escriben en RAM. Cuando el sistema reinicia, el contenido nuevo es "olvidado" y se pierde, restaurando el o los discos a su estado original.

Lethe incluye todas las particiones y las congela, pero es posible excluir algunos puntos de montaje para que no se congelen. Basta solo con remover por ejemplo *home* de la variable **MOUNTP** para permitir que los cambios realizados a */home* sean permanentes entre reinicios.

Sin embargo no es posible no congelar la particion /.

Bugs conocidos

- El sistema no funciona correctamente cuando */var* es una partición. Debido a que el proceso de montaje de /var no es como */home* o */user*, cuando se trata de montar como read only, el script falla.
- El paquete da problemas si se trata de instalar 2 o mas veces. La desinstalación con dpkg -r no funciona.

- **Deepfreeze**

Tiene las mismas funcionalidades que en Windows, con la contra partida que se a implementado en Linux tipo SUSE

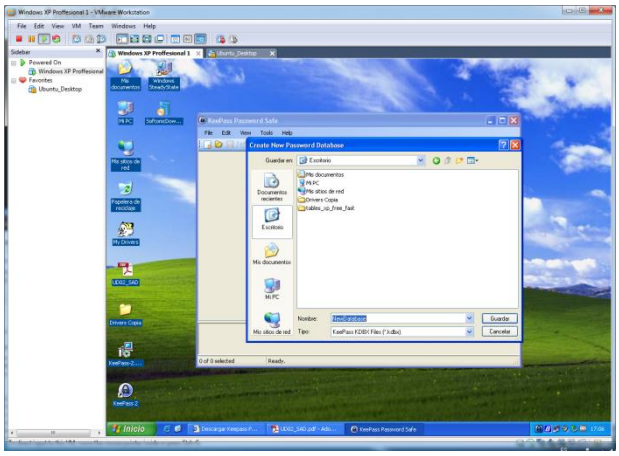
k) Utiliza el software "Keepass Passwrod Safe", y crea un pequeño informe de las posibilidades del mismo, desde un punto de vista de seguridad informática.

En internet nosotros como usuarios cada vez nos registramos en más y mas sitios web, ya sea para acceder a todas las funciones de la pagina o cualquier otra razón. El problema es que generalmente solemos cambiar las contraseñas que usamos para registrarnos y esto ocasiona que olvidemos las contraseñas.

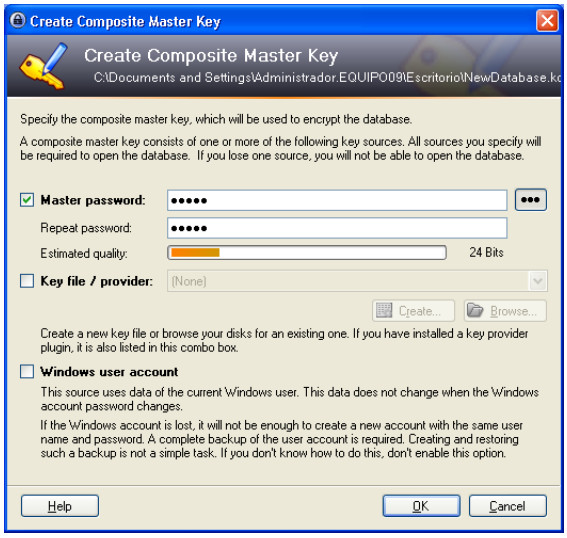
KeePass Password Safe es un programa que sirve para guardar contraseñas en el que podemos introducir nuestras contraseñas para evitar olvidarlas en el futuro. El programa es bastante funcional, además de permitirnos guardar nuestras contraseñas, podemos ordenarlas de miles de formas para hacer más fácil su localización, y si no es suficiente para ti también podemos relacionar las contraseñas con servicios o páginas web.

Una característica importante de este programa es la seguridad, ya que este nos proporciona varias opciones de seguridad como por ejemplo: establecer una **contraseña de seguridad** para acceder al programa. Cabe destacar que todas las contraseñas están encriptadas para una mayor seguridad.

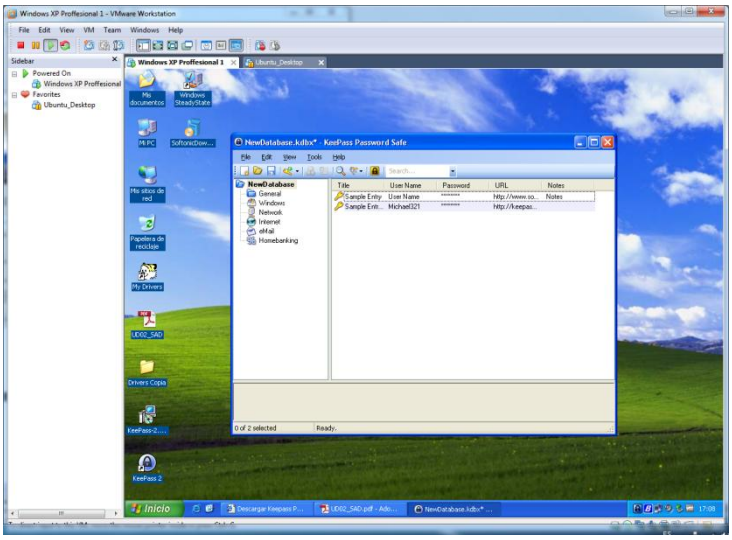
Una vez instalada nuestra aplicación vamos a guardar una contraseña nueva, la guardamos en el escritorio. Elegimos la opción de general.



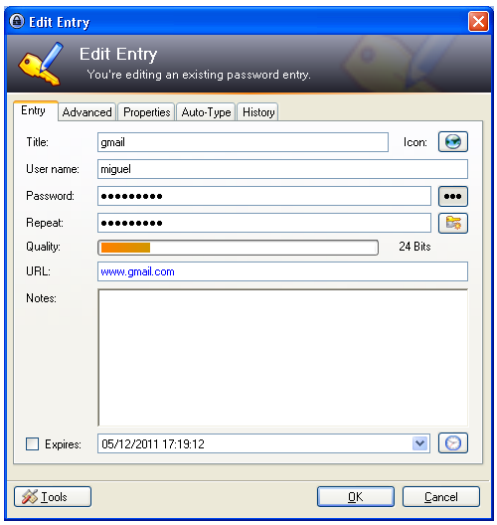
Introducimos la nueva contraseña que queremos guardar.



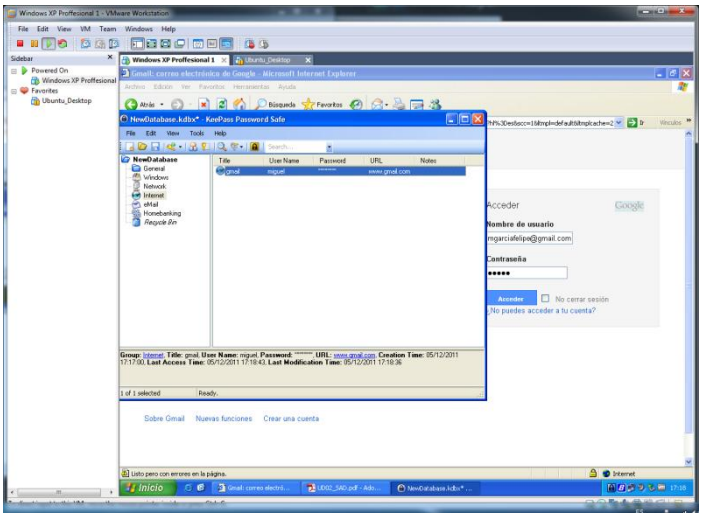
Si por el contrario queremos, queremos guardar una contraseña de una página web que visitamos habitualmente, nos situamos en la opción Internet, y creamos la nueva clave.



Introducimos la contraseña, el nombre de la contraseña, el usuario que la va a utilizar, y la dirección de la página a la que se va a referir.



Una vez creada la probamos, abrimos una cuenta de gmail en mi caso, y arrastramos a la casilla de contraseña, la contraseña de nuestro programa, y vemos que funciona correctamente.



SEGURIDAD EN LA CONEXIÓN CON REDES PÚBLICAS:

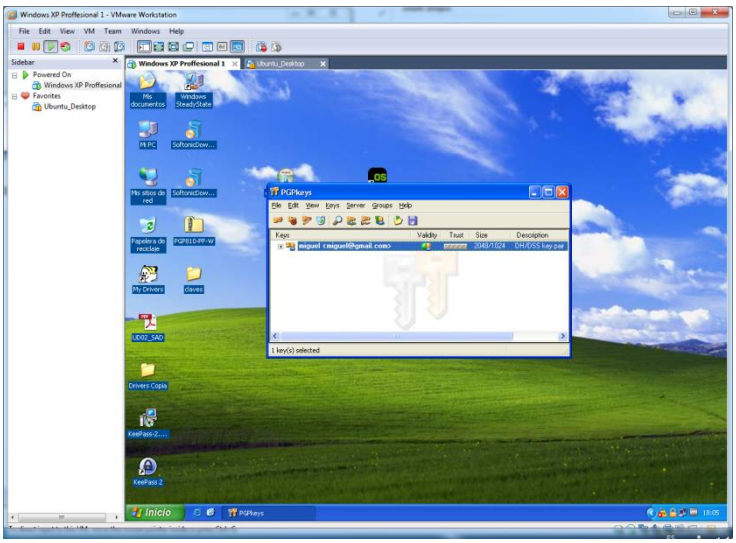
3. TÉCNICAS DE CIFRADO:

a) Cifrado simétrico:

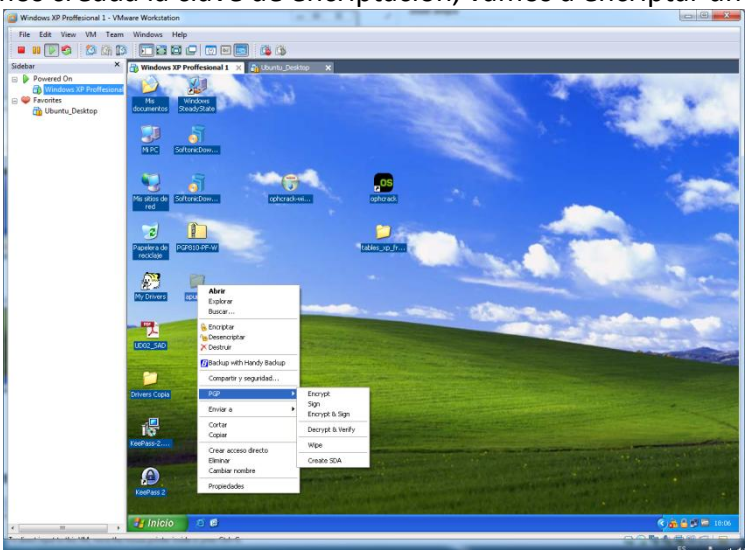
- Uso de PGP

El PGP es una aplicación que nos permite encriptar-desencriptar datos.

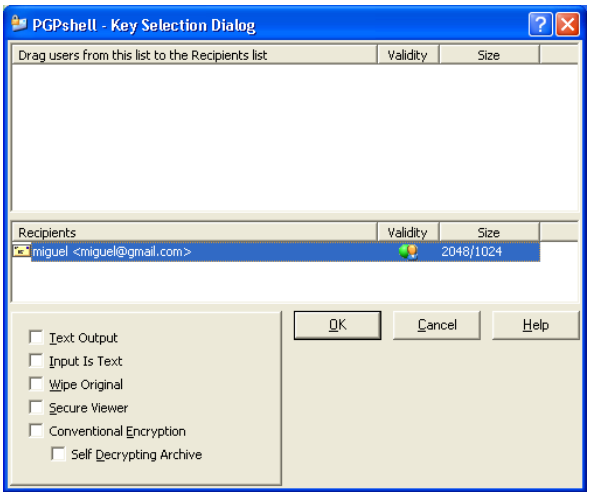
Instalamos la aplicación, y creamos un usuario, con una contraseña, que el destinatario debe de saber también.



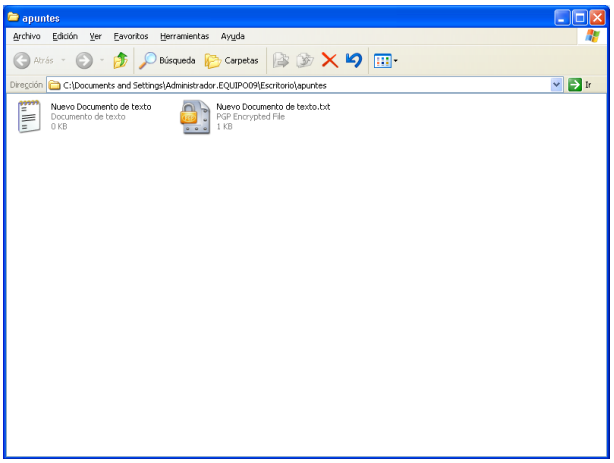
Una vez tengamos creada la clave de encriptación, vamos a encriptar un fichero.



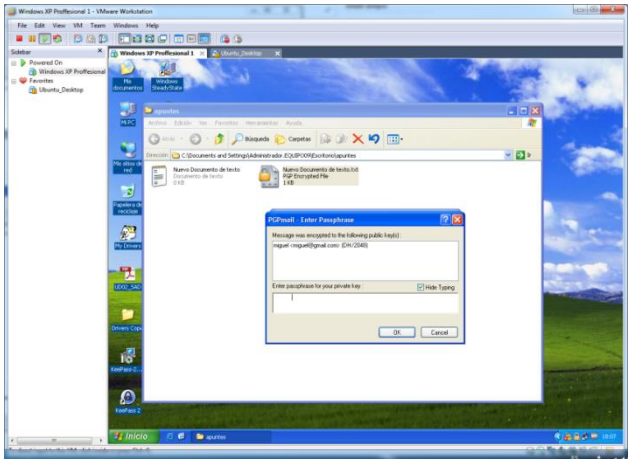
Elegimos la clave de encriptación deseada, en nuestro caso la que hemos creado anteriormente.



Verificamos que nos ha cifrado el documento correctamente.

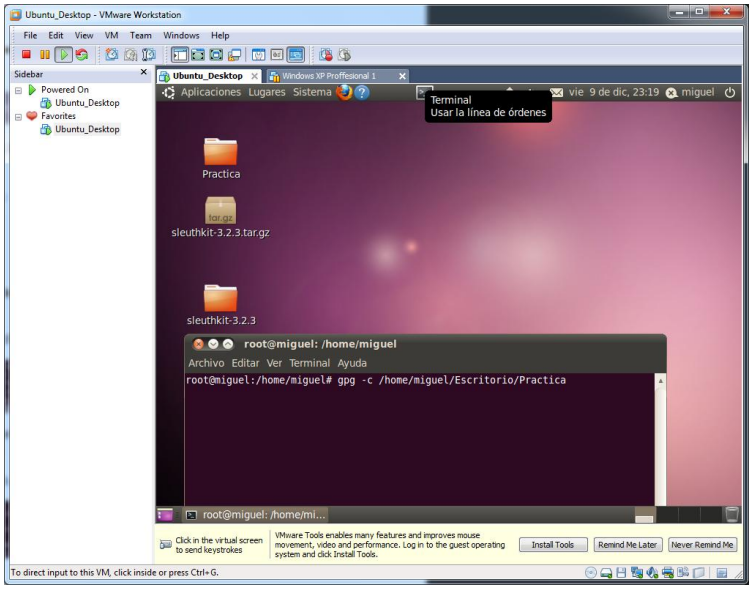


De tal manera que si intentamos abrirlo, necesitaremos la clave de desencriptación.



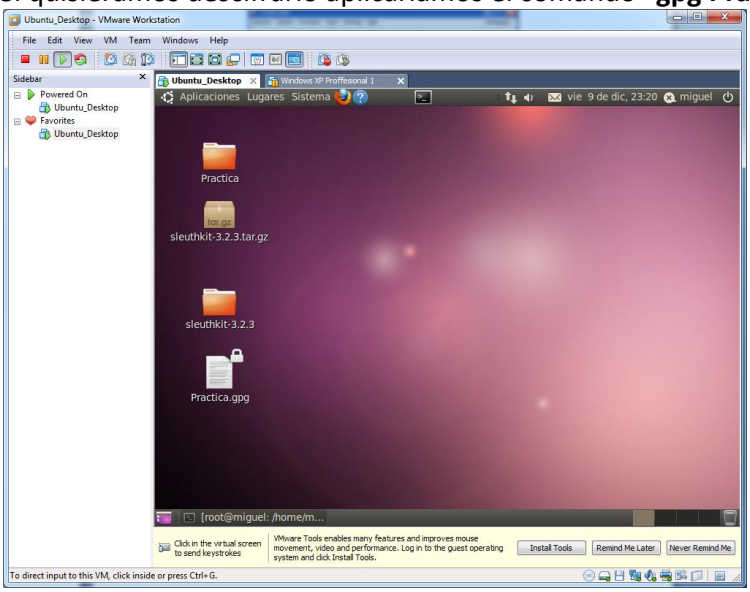
- Uso de GPG

Debemos tener instalado gpg en nuestro equipo, una vez instalado, podemos encriptar con gpg un archivo o directorio de forma simétrica en Ubuntu.
Para ello usamos el comando **"gpg –c /home/miguel/Escritorio/Prueba"**



Comprobamos que efectivamente, nos a encriptado en el escritorio nuestro directorio de Prueba.

Si quisiéramos descifrarlo aplicaríamos el comando "**gpg Practica.gpg**"

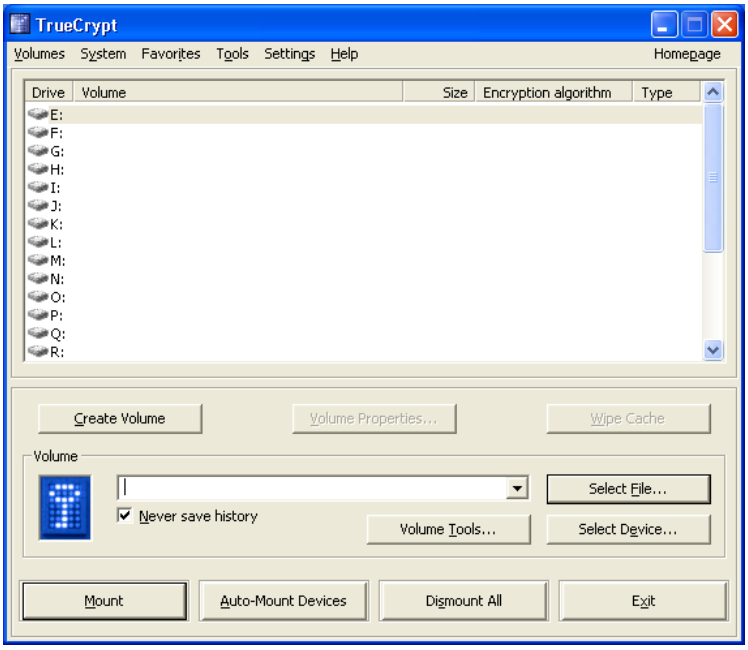


b) Cifrado de datos y particiones:

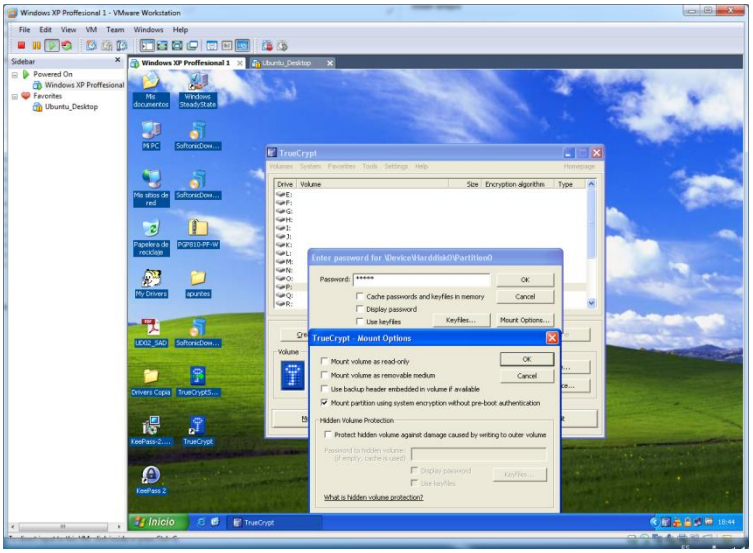
- En Windows: Uso de TrueCrypt.

Esta aplicación nos permite la encriptación de particiones de nuestro sistema.

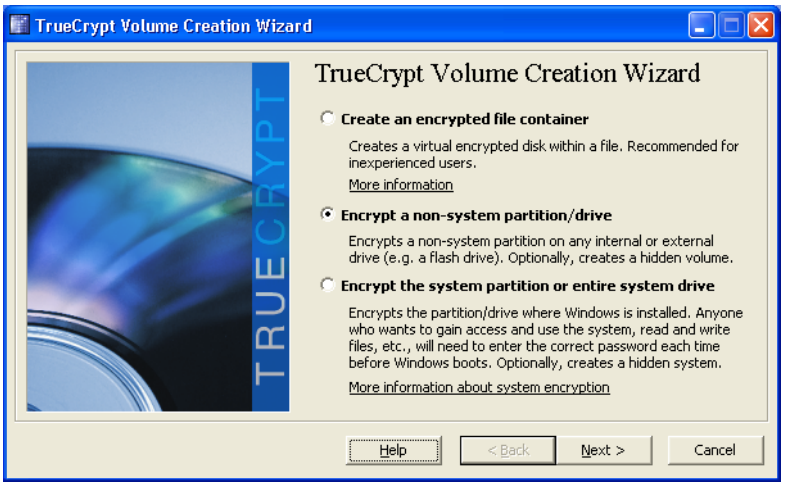
Una vez tengamos instalada nuestra aplicación, nos situamos en esta ventana que mostramos a continuación.



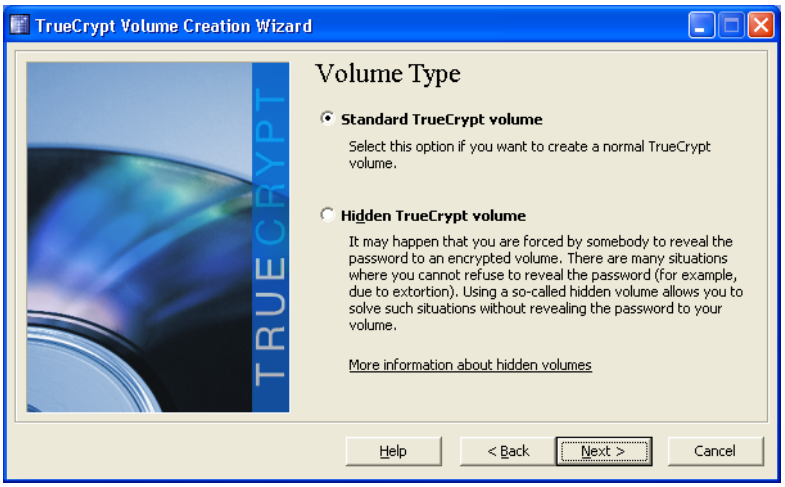
Elegimos un volumen, y establecemos una contraseña que vayamos a utilizar.



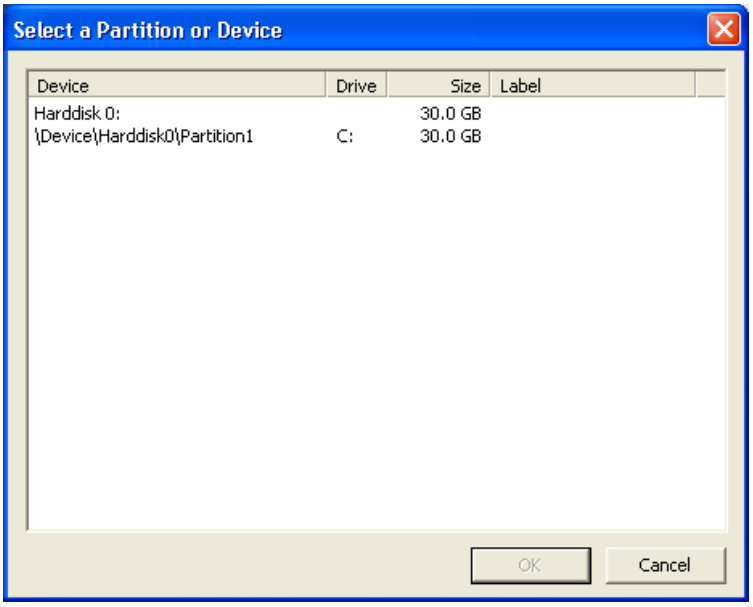
Vamos a encriptar una partición, seguimos el siguiente asistente.



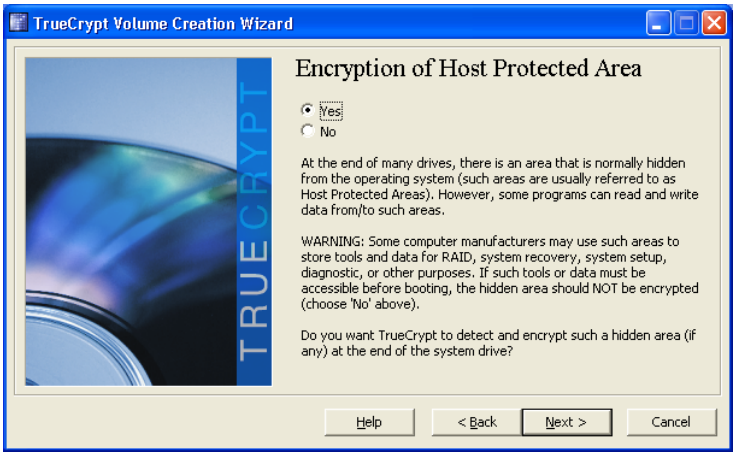
Elegimos la opción estándar.



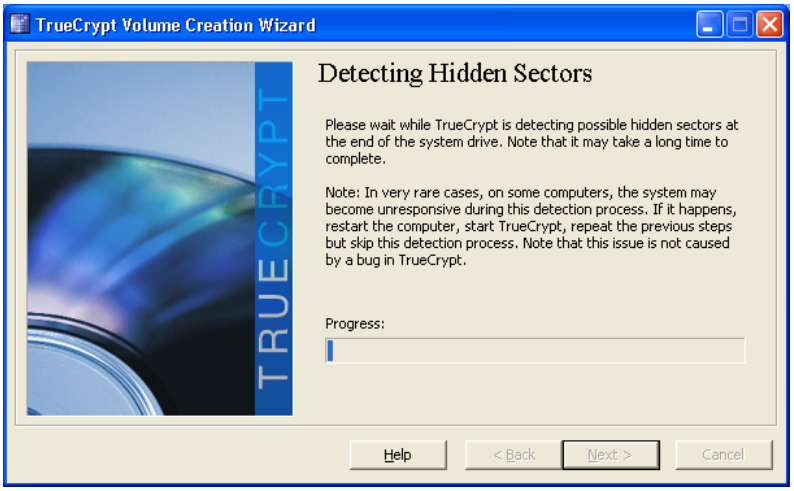
Seleccionamos en nuestro caso, la unidad C.



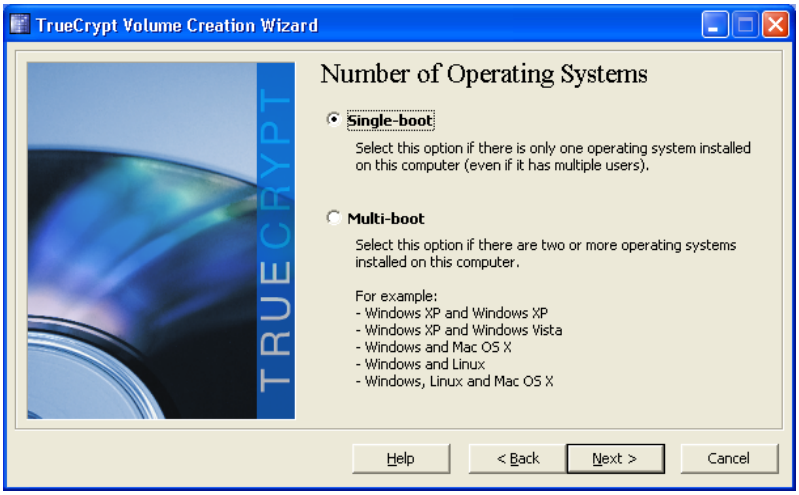
Dejamos la opción sí por defecto.



De ésta manera comenzara el proceso de encriptación.



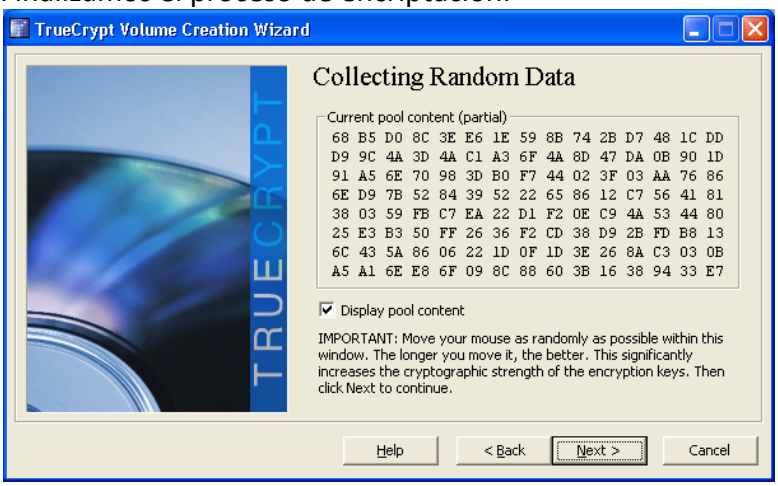
Elegimos la opción por defecto.



Elegimos un algoritmo de encriptación, nosotros en nuestro caso hemos escogido el tipo **AES.**

Establecemos la contraseña.

Finalizamos el proceso de encriptación.



Podemos guardar una imagen de respaldo. Como en mis documentos.

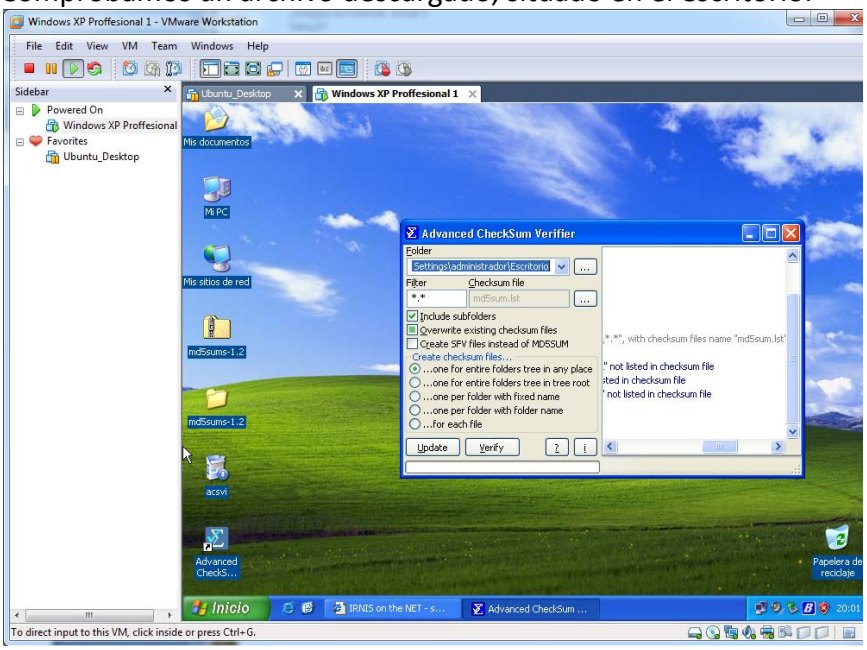
c) Funciones HASH

- En Window: md5sum.

EL utilitario **md5sum** permite calcular lo que se llama la huella digital de un archivo. En inglés, *fingerprint, message-digest* o *checksum* es un valor de 128 bits que corresponde a la suma de control calculada a partir del archivo.

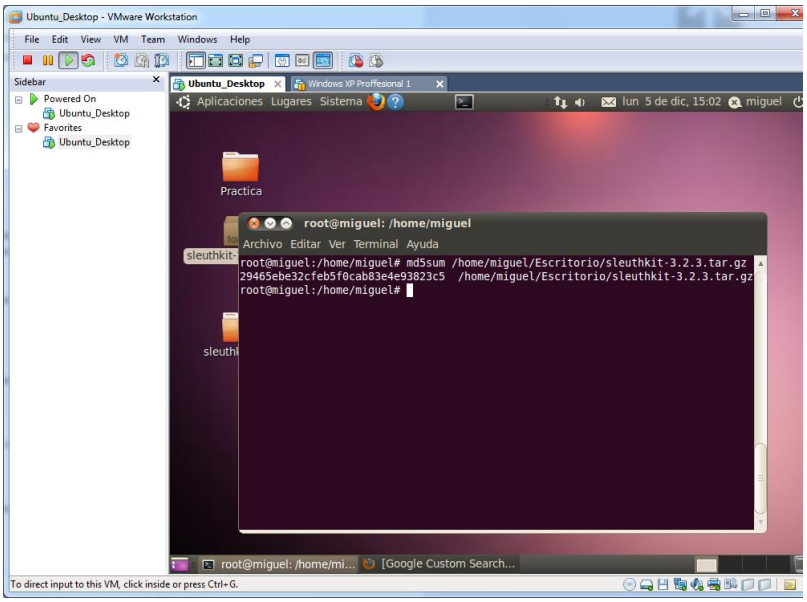
El objetivo de un checksum MD5 no es garantizar la procedencia de un archivo o grupo de estos. Su interés es el de verificar la integridad de los datos descargados. En efecto, nadie está al abrigo de una perturbación o de un problema de red que tengan como consecuencia la alteración de un archivo durante la descarga.

Comprobamos un archivo descargado, situado en el escritorio.



- En GNU/Linux: md5sum.

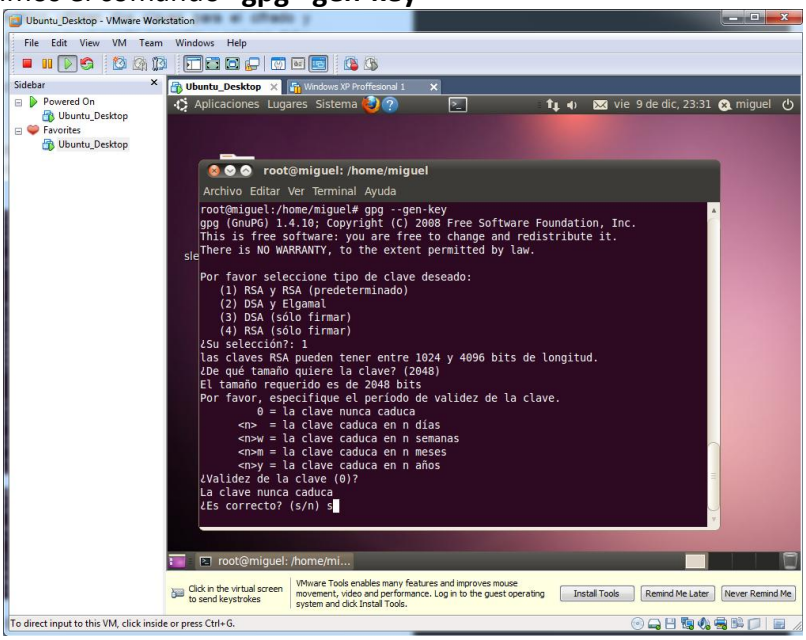
Utilizamos md5sum en Ubuntu.



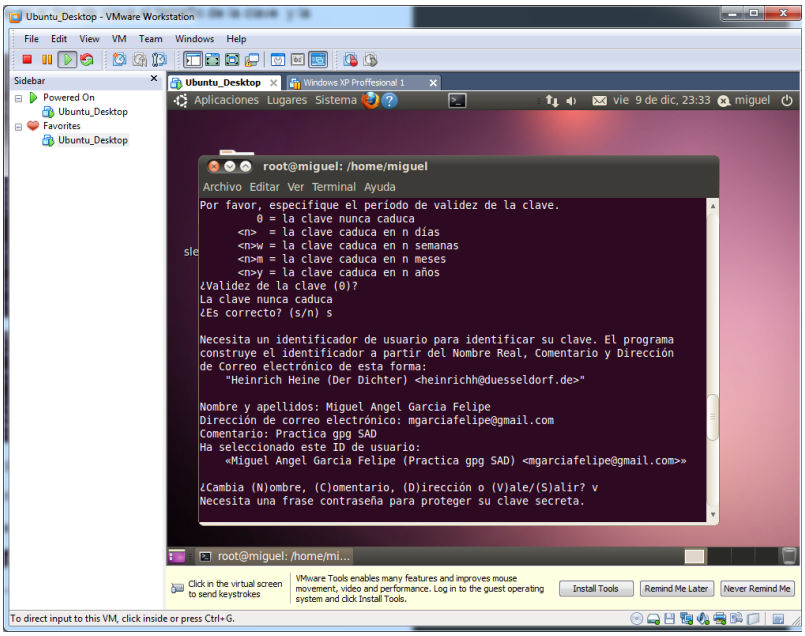
d) Cifrado asimétrico:

- En GNU/Linux: gpg.

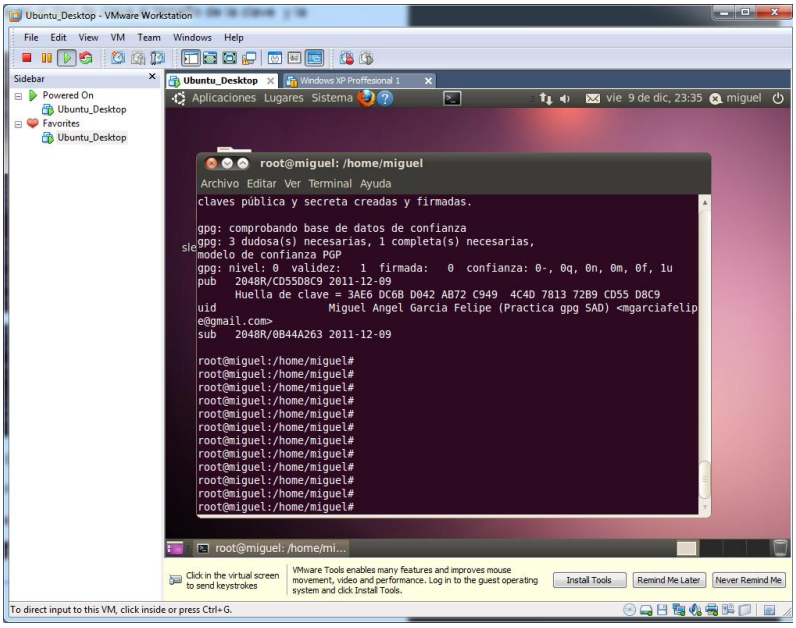
Para crear una cifrado asimétrico, primero tenemos que crear una clave cifrada, para ello introducimos el comando "**gpg –gen-key**"



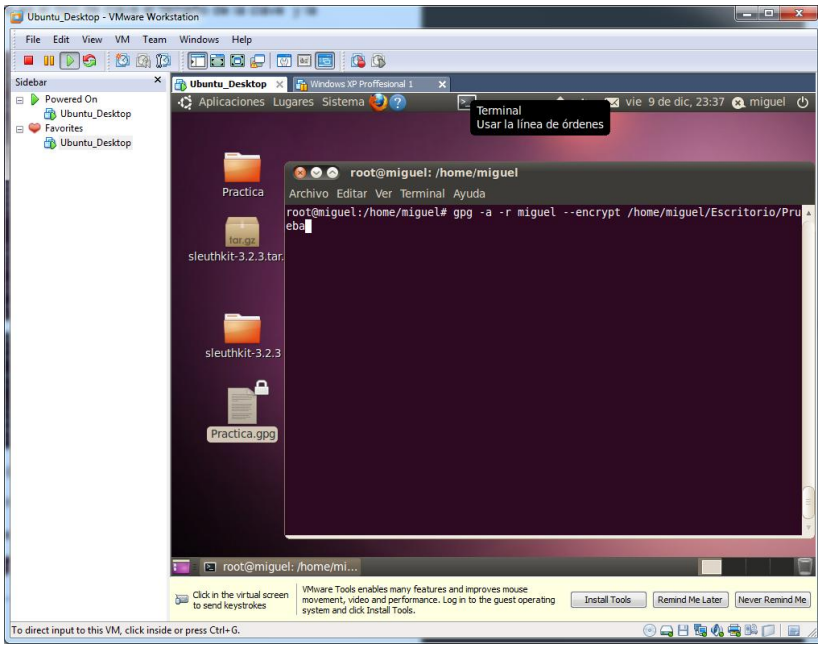
Seguimos los parámetros indicados, indicando nombre, correo, etc.



Concluimos con la creación de la clave.



Finalmente, una vez tengamos creada la clave encriptada, podemos proceder a encriptar el documento, para ello introducimos el comando "**gpg –a –r miguel /home/miguel/Escritorio/Prueba".**



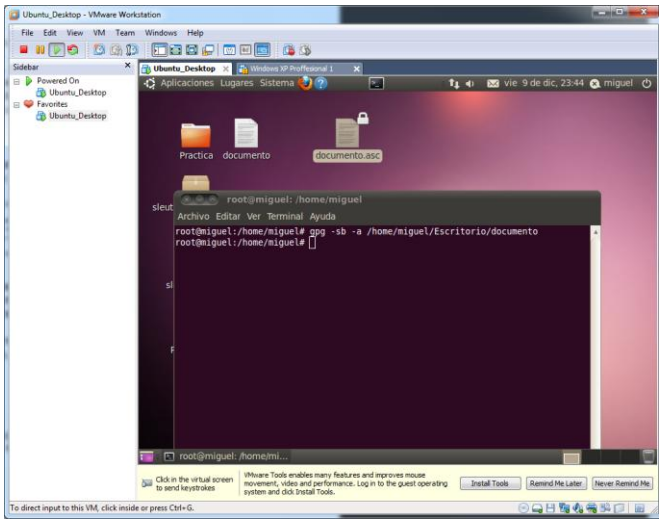
SEGURIDAD EN LA CONEXIÓN CON REDES PÚBLICAS:

4. IDENTIDAD DIGITAL:

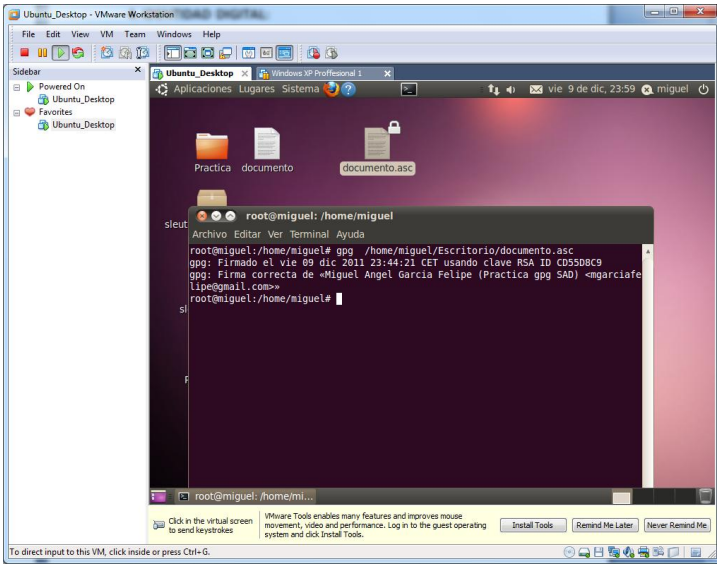
a) Firma digital de un documento

- En GNU/Linux: gpg.

Vamos a hacer una firma digital de un documento, antes de cifrarlo. Usamos el comando "**gpg –sb –a /home/miguel/Escritorio/documento**"



Una vez tengamos firmado el documento, lo ciframos con el comando "**gpg /home/miguel/Escritorio/documento.asc**".



b) Certificados digitales. - Busca que Autoridades Certificadoras Admitidas de certificados digitales existen en España. Describe el proceso para la obtención del certificado digital. Visita la web www.fnmt.es

- Autoridades Certificadoras:

CERES (CERtificación Española)
* AC Abogacía
* ANCERT – Agencia Notarial de Certificación
* ANF AC
* Autoritat de Certificació de la Comunitat Valenciana – ACCV
* Banesto CA
* AC Camerfirma
* CATCert

* CERES Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM)
* CertiVer
* CICCP
* Colegio Oficial de Arquitectos de Sevilla
* Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía
* EADTrust
* EDICOM
* Firmaprofesional
* Gerencia de Informática de la Seguridad Social
* Healthsign
* ipsCA
* Izenpe
* Ministerio de Defensa de España
* Registradores de España
* Santander
* Servicio de Salud de Castilla-La Mancha (SESCAM)
* Telefónica Empresas

Proceso de obtención del certificado digital:
Solicitud del proceso via internet, después de rellenar todos los campos, al final de este proceso obtendrá un código que deberá presentar al acreditar su identidad.

Acreditación de la identidad en una Oficina de Registro.
Si usted ha solicitado un certificado de persona fisica, puede dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.

Descarga de su Certificado de Usuario.
Unos minutos después de haber acreditado su identidad en una Oficina de Registro, haciendo uso del código de solicitud obtenido en el paso 1, podrá descargar su certificado desde esta página web entrando en el apartado Descarga del Certificado.

¿Es válido para todos los navegadores web?

No, sólo son soportados por firefox y explorer.

¿Puede emplearse para firmar otro tipo de archivos?
Sí, para confirmar que somos la persona concreta.

¿Es posible exportarlo o solamente se puede emplear en un solo equipo?

Si, es posible exportar la firma electrónica si se trata del certificado de DNI, porque haremos uso del lector.
Si se trata del usuario electrónico el certificado está instalado en nuestro navegador, entonces no podemos explotarlo en diferentes equipos.

¿Qué precauciones podemos tener con el certificado digital en cuanto a protección mediante contraseñas a la exportación?

Las precauciones que debemos utilizar es, tener contraseñas con mayúsculas, minúsculas, números, caracteres especiales, la contraseña debe tener un mínimo de 8 dígitos, y se debe cambiar cada cierto tiempo para mayor seguridad.

c) Certificados digitales.- Revisa en la web www.camerfirma.com, uno de los usos que tiene el certificado digital para la firma y el envío de correos electrónicos con certificado digital. Describe el proceso. ¿Qué garantiza? ¿Qué es S-MIME?

- Su uso es validar documentos de manera electrónica. Para que un certificado digital tenga validez legal, la autoridad de certificación debe de estar acreditada por la entidad pública de certificación del país correspondiente. En España es CERES (CERtificación ESpañola) la entidad que se encarga de gestionar este tipo de certificados
- El proceso de envío de correos electrónicos con certificado digital sería el siguiente: El que he utilizado es un gestor de correos llamado thuntherbird que es el que tengo instalado para hacer unas prácticas y ya he aprovechado. Empezamos a redactar el mensaje y cuando este redactado, colocamos la dirección, para validar nuestro correo con el certificado digital pulsamos en seguridad, cifrar mensaje y enviar, así estará firmado digitalmente.

Garantiza la autenticidad de los destinatarios.

¿Qué es S-MIME?

S/MIME proporciona dos servicios de seguridad:

- Firmas digitales
- Cifrado de mensajes

Estos dos servicios son el núcleo de la seguridad de los mensajes basada en S/MIME. Todos los demás conceptos relacionados con la seguridad de los mensajes sirven de apoyo a estos dos servicios. Si bien todo el ámbito de la seguridad de los mensajes puede parecer complejo, estos dos servicios son la base de dicha seguridad. Una vez que adquiera unos conocimientos básicos de las firmas digitales y del cifrado de mensajes, podrá aprender cómo otros conceptos sirven de apoyo a estos servicios.

d) Certificados digitales.- Realiza los trámites para la obtención de tu certificado digital.

- ¿Dónde lo tienes que descargar?

Hay que descargarlo en www.fntm.es.

- ¿Dónde tienes que ir a recogerlo?

En una oficina acreditada.

- ¿Qué caducidad posee?
Tiene una caducidad de 2 años desde el día de la obtención del mismo

- Una persona que acceda a nuestro equipo en el que tenemos instalado un certificado digital, ¿puede acceder a distintos sitios web de información personal de tipo legal?

Sí, y esto supone un riesgo a nuestra seguridad en la red.

e) Certificados digitales/ DNIe. – Realiza una búsqueda de los servicios de empresas como bancos, y de la administración pública (seguridad social, hacienda, etc) a los que se puede acceder de forma segura, mediante certificado digital y mediante DNIe.
- Acceder a un organismo público en Internet utilizando el Dni-e.

Como ya sabemos la seguridad en Informática no es 100% segura, lo podemos utilizar para:
-Realizar compras a través de internet.
-Hacer trámites completos en las administraciones públicas a cualquier hora y sin tener que desplazarse y hacer colas.
-Realizar transacciones seguras con entidades bancarias.
-Acceder al edificio donde trabajamos.
-Utilizar de forma segura nuestro ordenador personal
-Participar en una conversación por internet con la certeza de que nuestro interlocutor es quien dice ser.

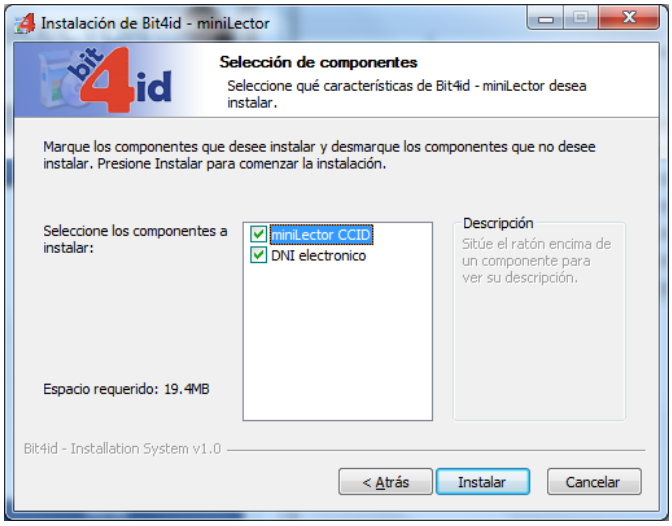
Vamos a instalar el lector de DNIe

Pulsamos el botón de instalación Lector y DNIe.

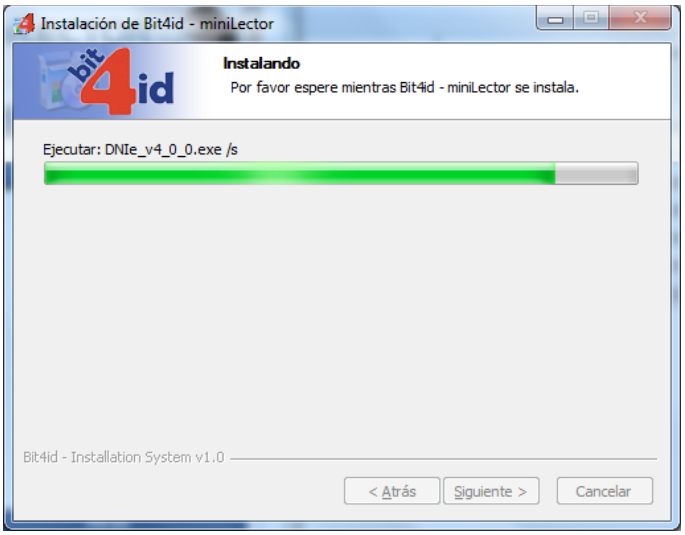
En éste caso elegimos sistemas Windows.

Pulsamos el botón de siguiente para comenzar la instalación.

Elegimos los elementos que queremos instalar.

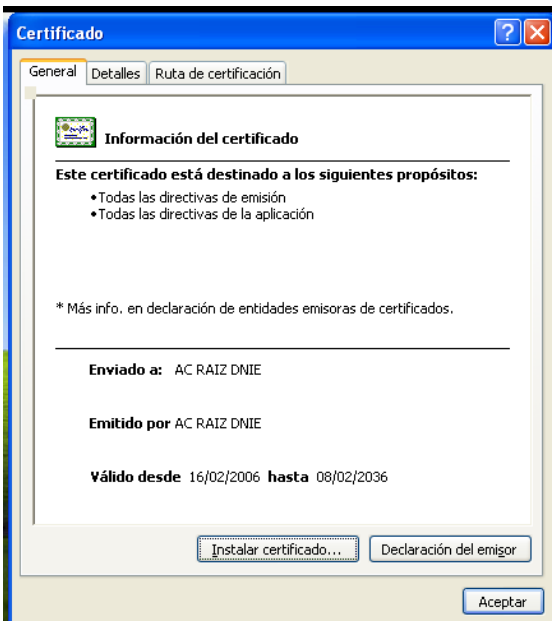


Comenzamos el proceso de instalación.

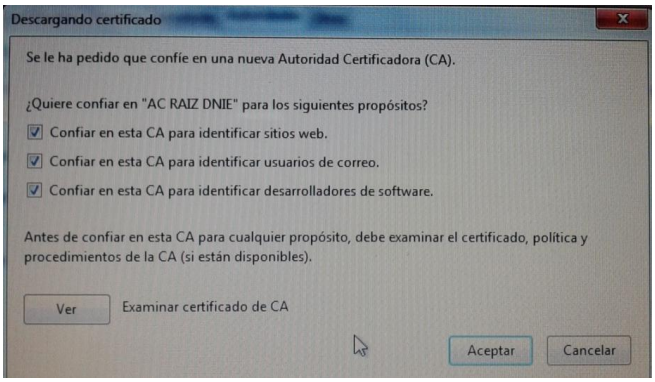


Una vez instalado, pulsamos el botón de terminar, más tarde debemos de reiniciar.

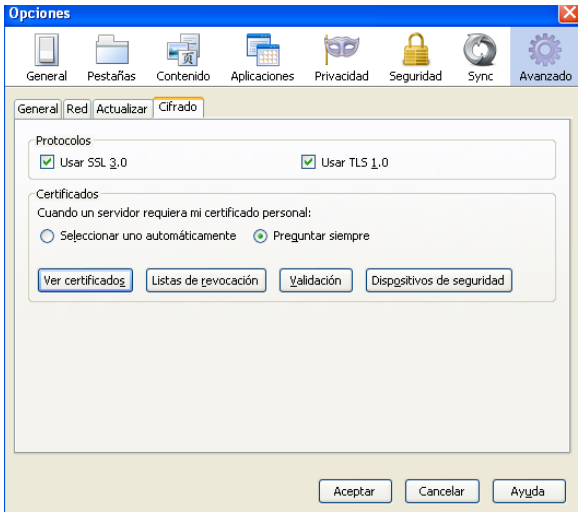
Una vez reiniciado el sistema, nos aparecerá la siguiente ventana para instalar un certificado digital en nuestro equipo.



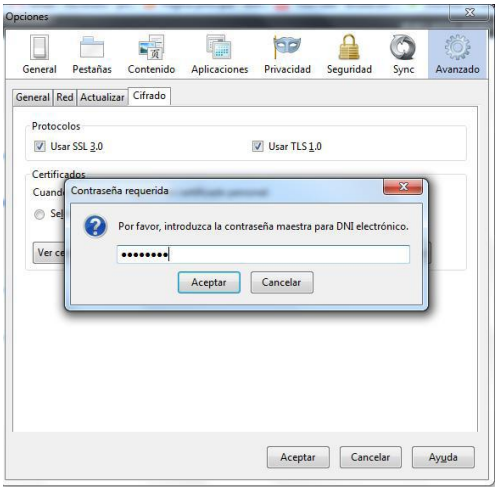
Marcamos los parámetros deseados.



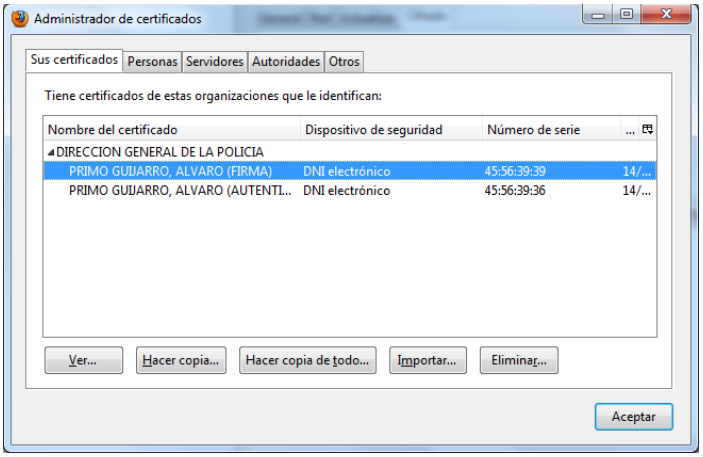
Una vez instalado, debemos reiniciar de nuevo. Y posteriormente comprobamos la instalación de nuestro certificado digital.



Ingresamos nuestra clave del DNI.

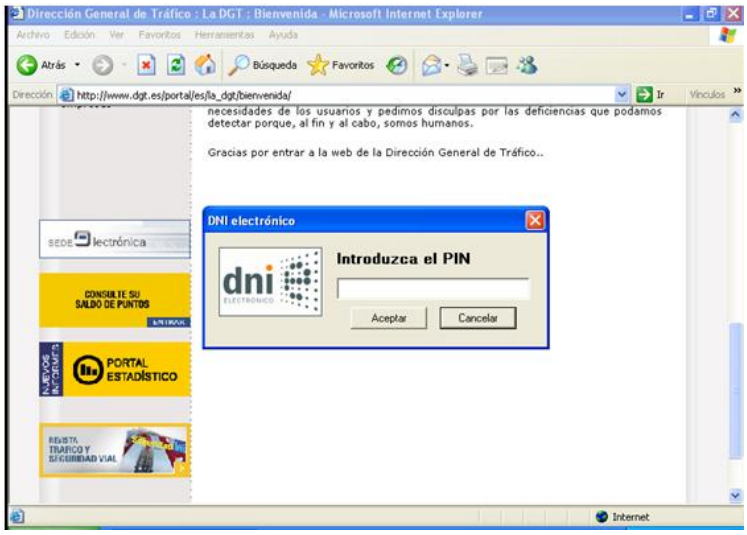


Y comprobamos el certificado en nuestro navegador.

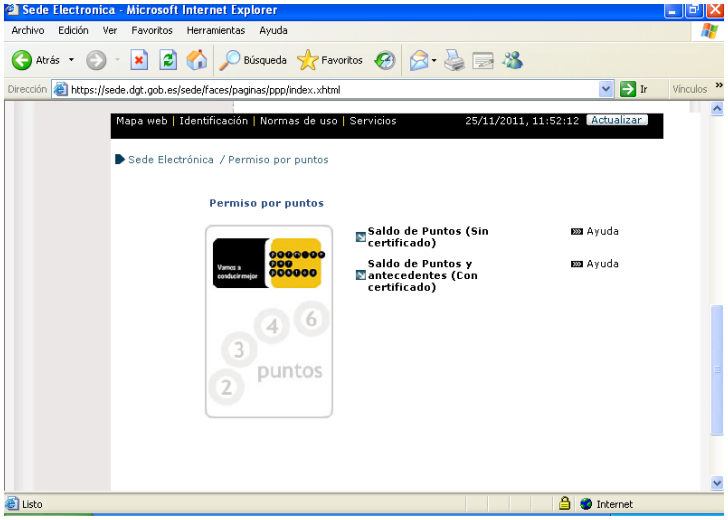


Introducimos nuestro DNIe en el lector.

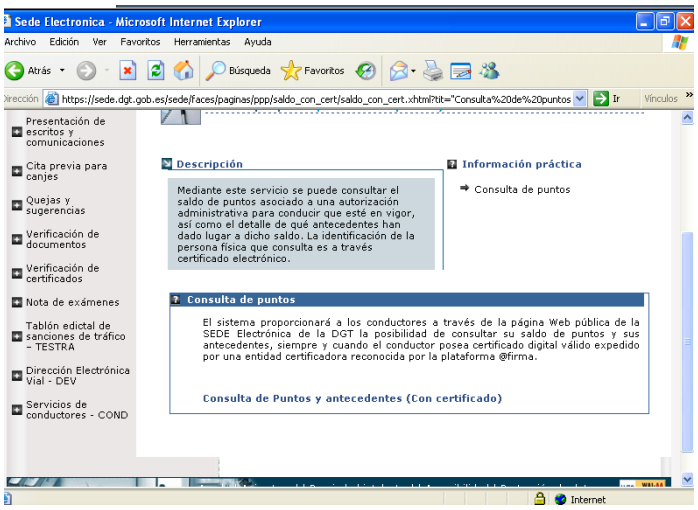
Comprobamos en una página como en la de dgt, introduciendo nuestro PIN del DNIe.



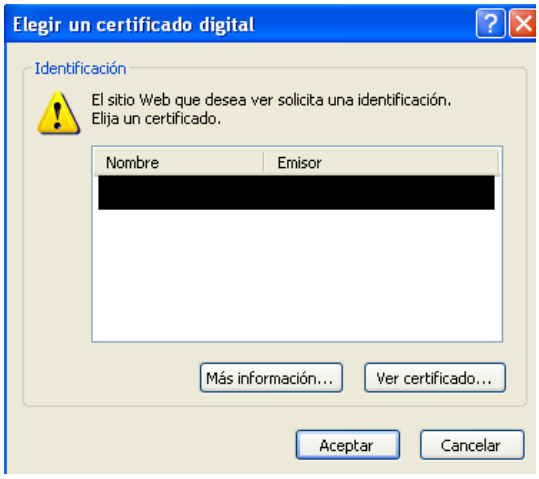
Vamos a consultar un dato nuestro, como por ejemplo los puntos del carnet de conducir.



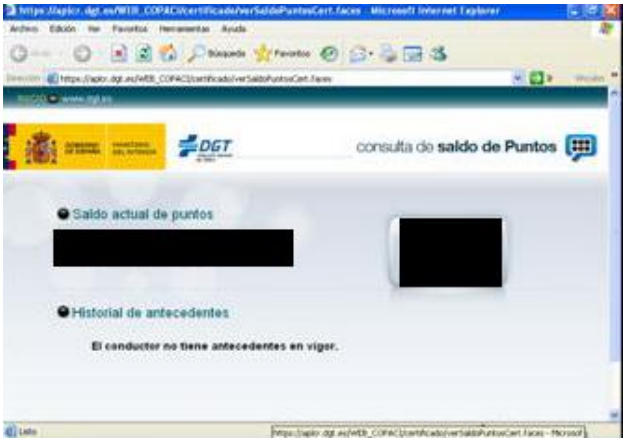
Consultamos los datos exigiendo un certificado de seguridad.



El resultado podemos verlo a continuación.

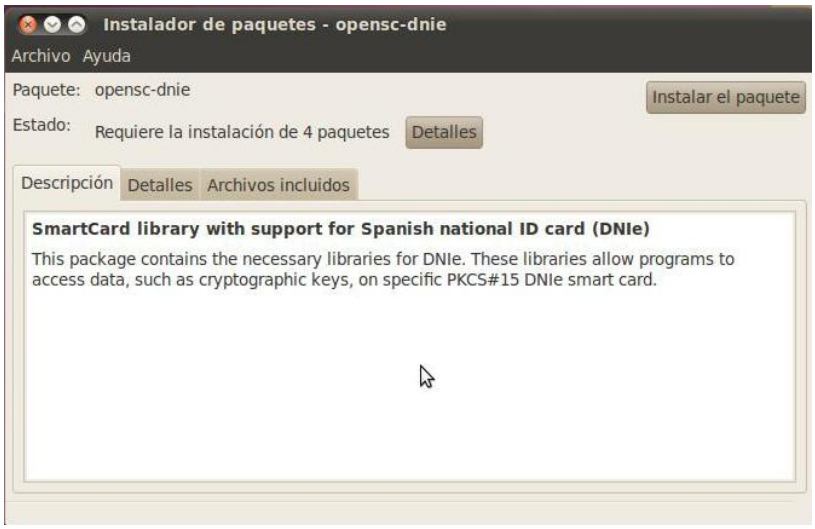


Por último podemos observar los puntos.

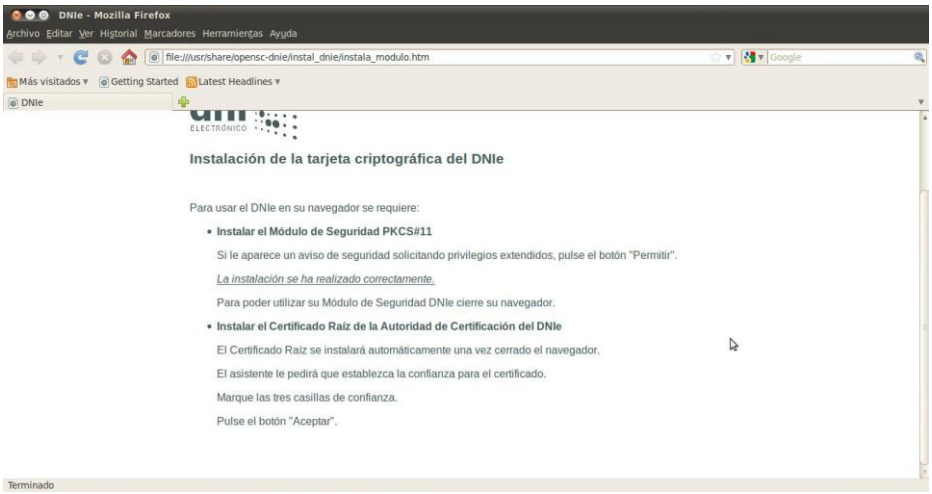


INSTALACIÓN EN LINUX:

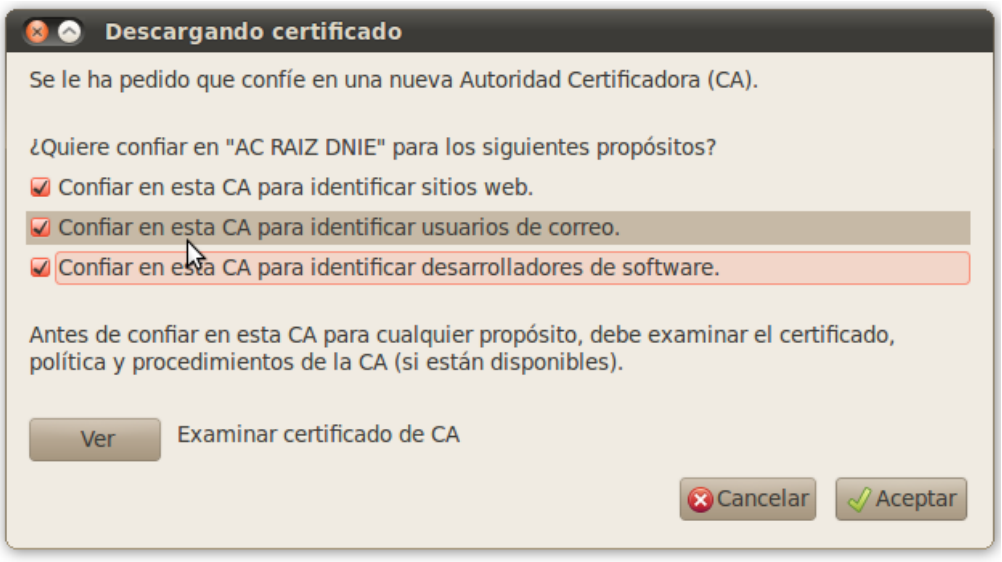
Nos descargamos el paquete “opensc-dnie” para GNU/LINUX en nuestro caso Ubuntu y lo instalamos en nuestro equipo.



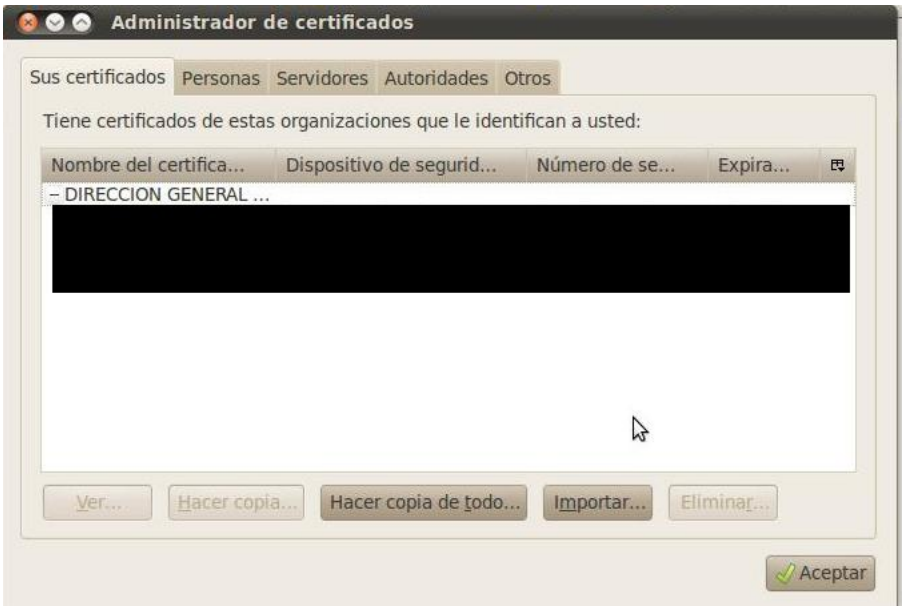
Una vez instalado, una ventana en nuestro navegador nos pedirá los elementos que nos falten para su correcta instalación.



Confiaremos en los sitios que nos interesen.



Por último comprobamos que se nos ha instalado correctamente el certificado.



5. AMENAZAS Y ATAQUES EN REDES CORPORATIVAS:

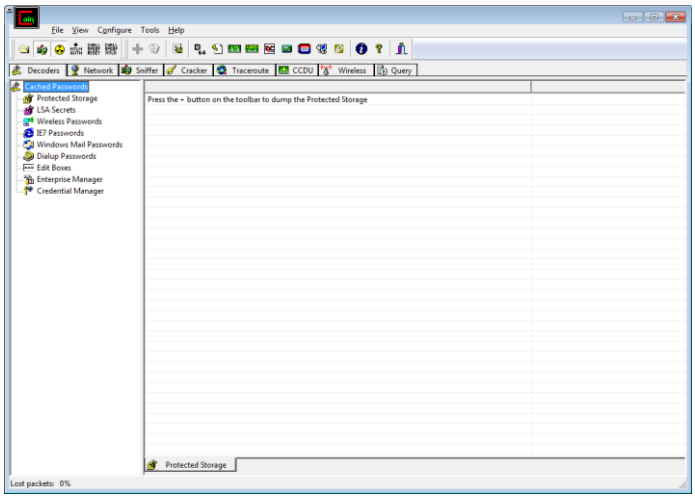
a) Identidad digital.- ¿Qué diferencias existen entre la instalación de un certificado en un servidor web y un servidor de certificaciones? Busca cómo se instala y qué opciones ofrece el servidor de certificados integrados en el servidor IIS de Microsoft. Realiza una petición por parte de un cliente de un certificado digital.

La instalación de un certificado en un servidor web es el proceso de obtención de un certificado por parte de un cliente, mientras que el servidor de certificaciones es el que se los proporciona al cliente.

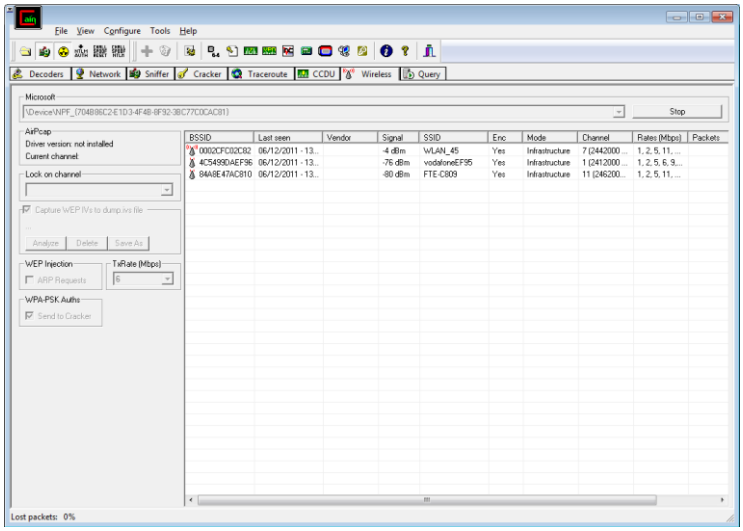
b) Seguridad en redes corporativas:

- Windows: Uso de **Caín & Abel** como Sniffing – MitM- ARP Spoofing – Pharming.

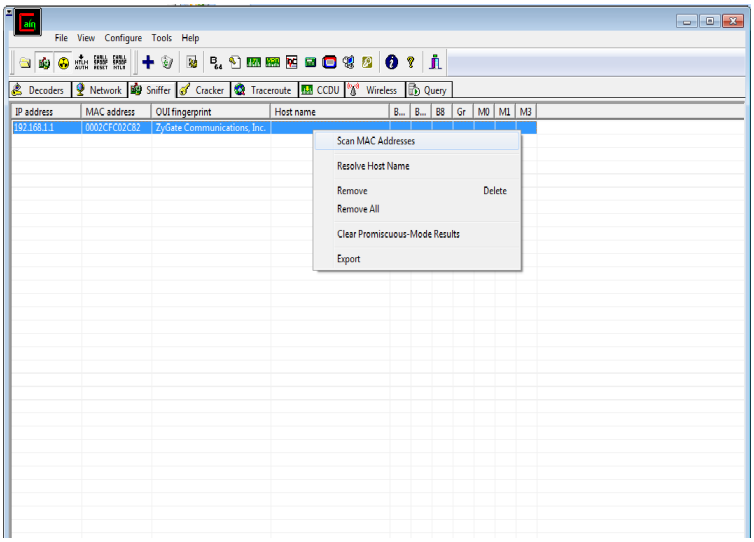
Una vez que tenemos esta aplicación instalada, vamos a dar uso de ella, ejecutamos el programa.



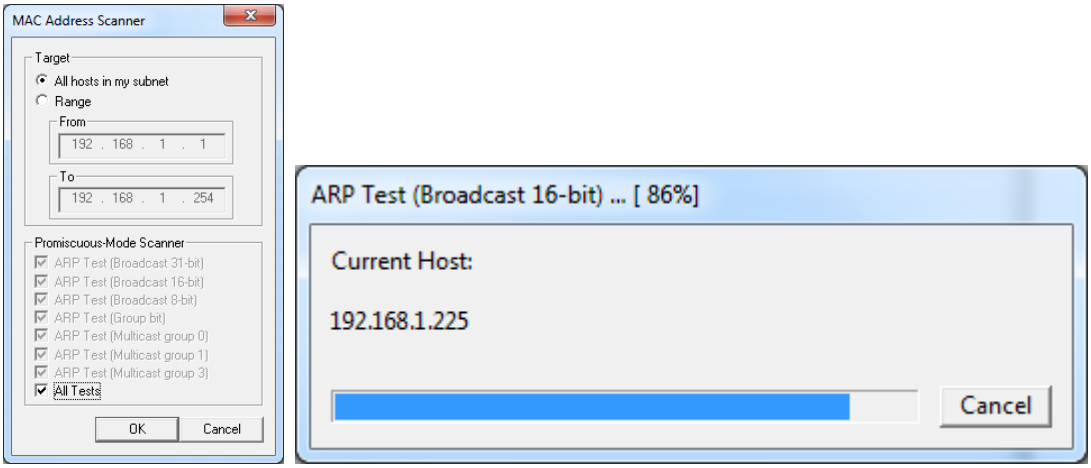
En la pestaña Wireless comprobamos los puntos de acceso inalámbricos disponibles.



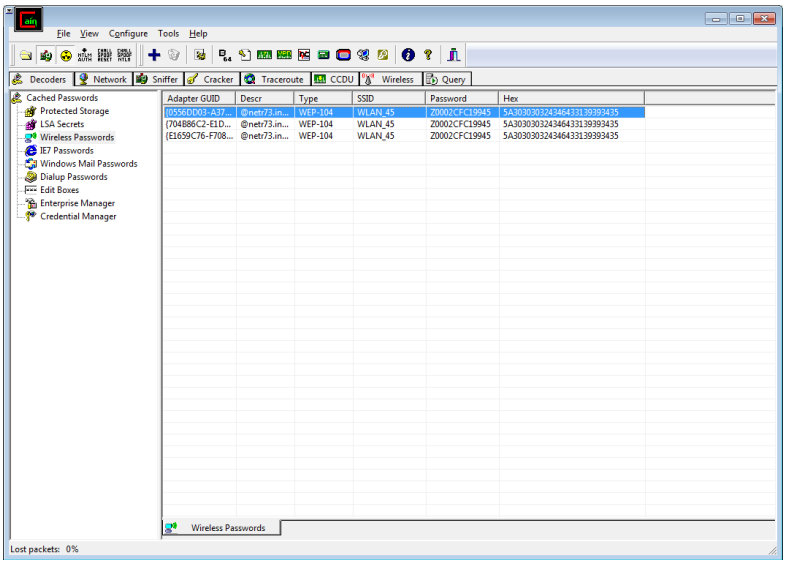
En mi caso voy a utilizar un sniffer para capturar información de mi router.



Escaneamos la dirección Mac de todas las tarjetas de la red.

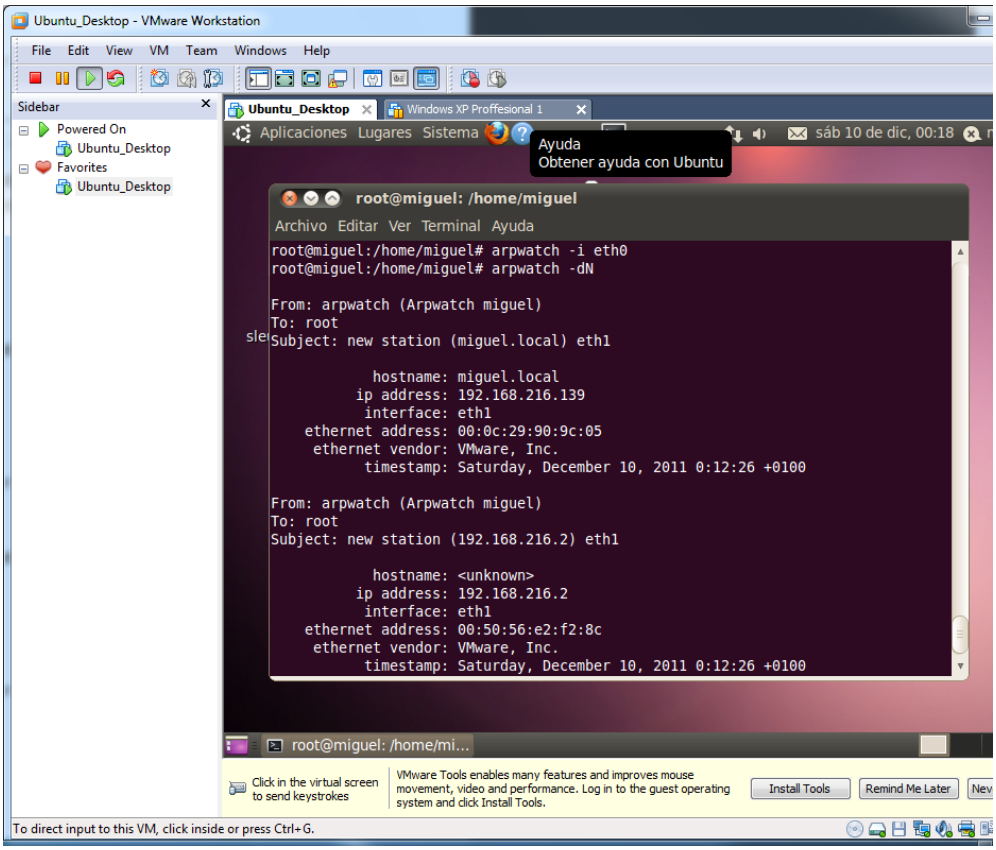


Si nos vamos al apartado Wireless Passwords, comprobamos que nos ha resuelto la clave del router.



- GNU/Linux: Uso de **ArpWatch.**

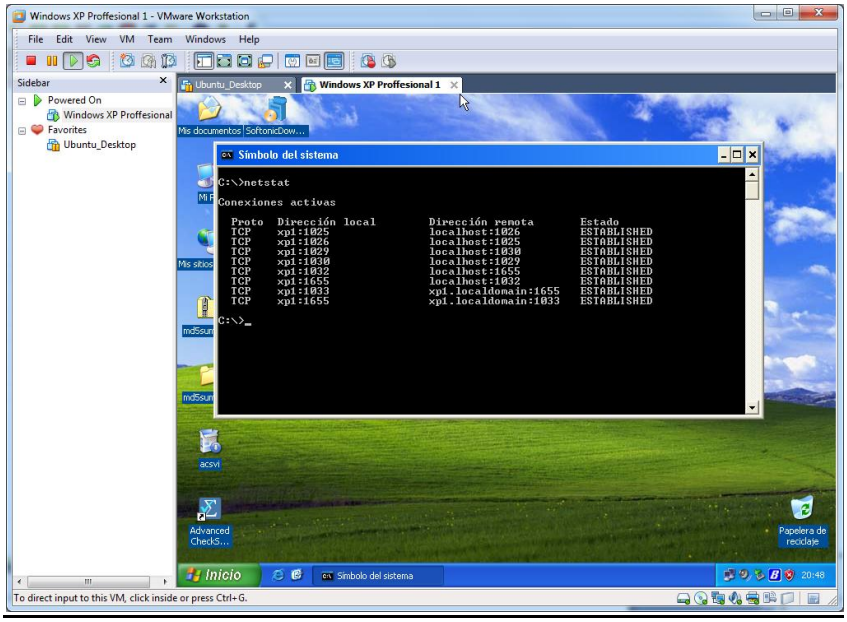
Utilizamos ArpWatch, para monitorizar información de nuestro equipo, a través de una interfaz de red. Para escoger una interfaz de red introducimos el comando **“arpwatch –i eth0”,** y para monitorizar la información acerca de equipos que se han conectado al nuestro con el comando “**arpwatch -dN**”.



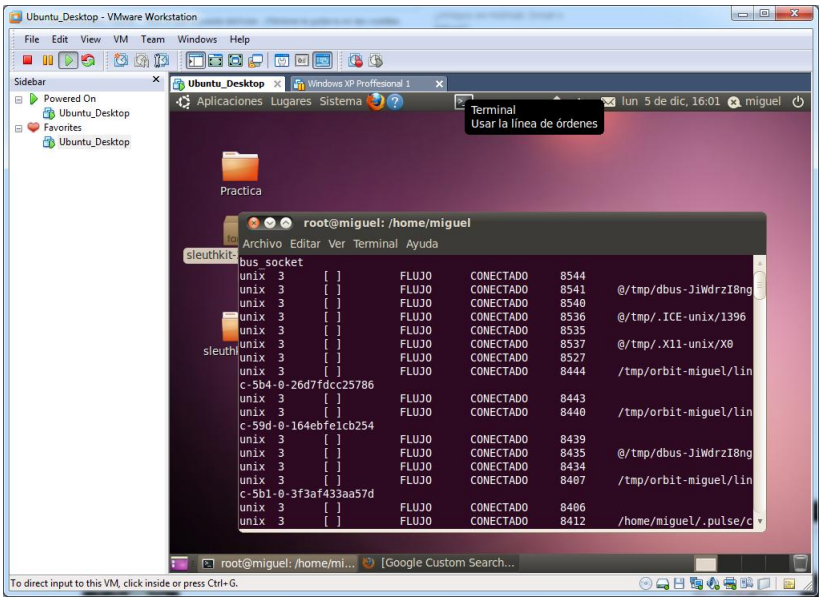
c) Seguridad en redes corporativas:

- Uso de **netstat** para análisis de puertos en Window y GNU/Linux.

-Windows:



-GNU/Linux:



<u>- Uso de un análisis de puertos on line:</u>

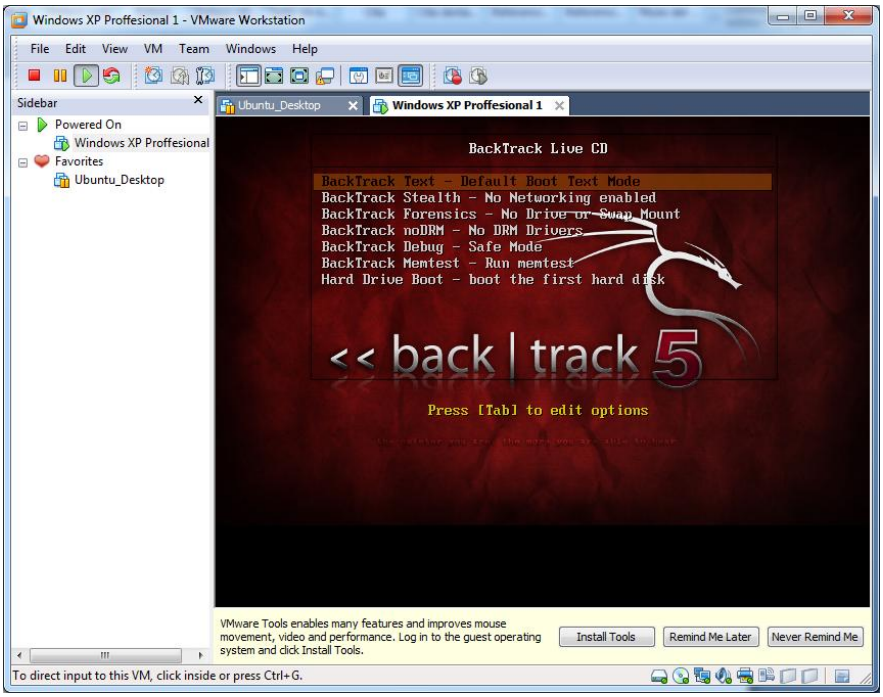
Accedemos a la página http://www.internautas.org/w-scanonline.php y comprobamos los puertos más básicos del equipo, y obtenemos el siguiente resultado.

Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	cerrado	Secure Shell.
23	TELNET	cerrado	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	cerrado	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	cerrado	Servidor web
110	POP3	cerrado	Servidor de correo POP3
119	NNTP	cerrado	Servidor de noticias
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
143	IMAP	cerrado	Servidor de correo IMAP
389	LDAP	cerrado	LDAP. Tambien Puede ser utilizado por Neetmeting
443	HTTPS	cerrado	Servidor web seguro
445	MSFT DS	cerrado	Server Message Block.
631	IPP	cerrado	Servidor de Impresion
1433	MS SQL	cerrado	Base de Datos de Microsoft
3306	MYSQL	cerrado	Base de Datos. MYSQL
5000	UPnP	cerrado	En windows está activado este puerto por defecto.

d) Uso de la **distribución Backtrack de GNU/Linux** con la finalidad de investigar sobre la **inyección de código SQL (SQL Inyection)** con la finalidad de obtener las tablas de usuarios y contraseñas de las bases de datos de sitios web.
Prueba en un sitio web en el que sea necesario registrarse.

¿Qué tipo de precauciones tendrías como administrador web para evitar inyecciones SQL?

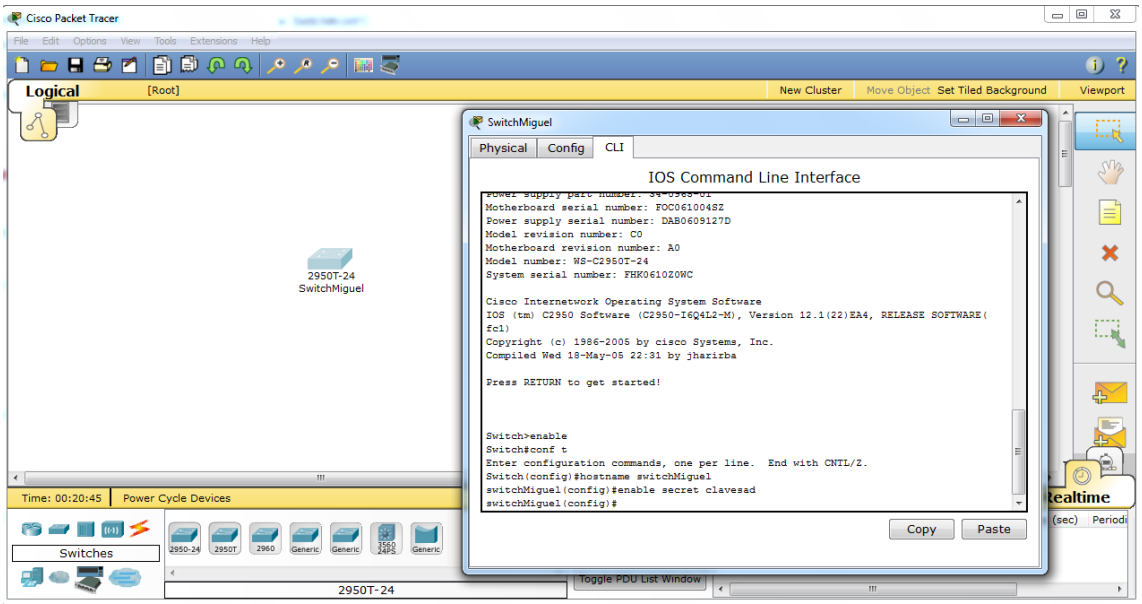
Arrancamos el BackTrack con un live CD.



SEGURIDAD EN LA RED CORPORATIVA:
6. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED:

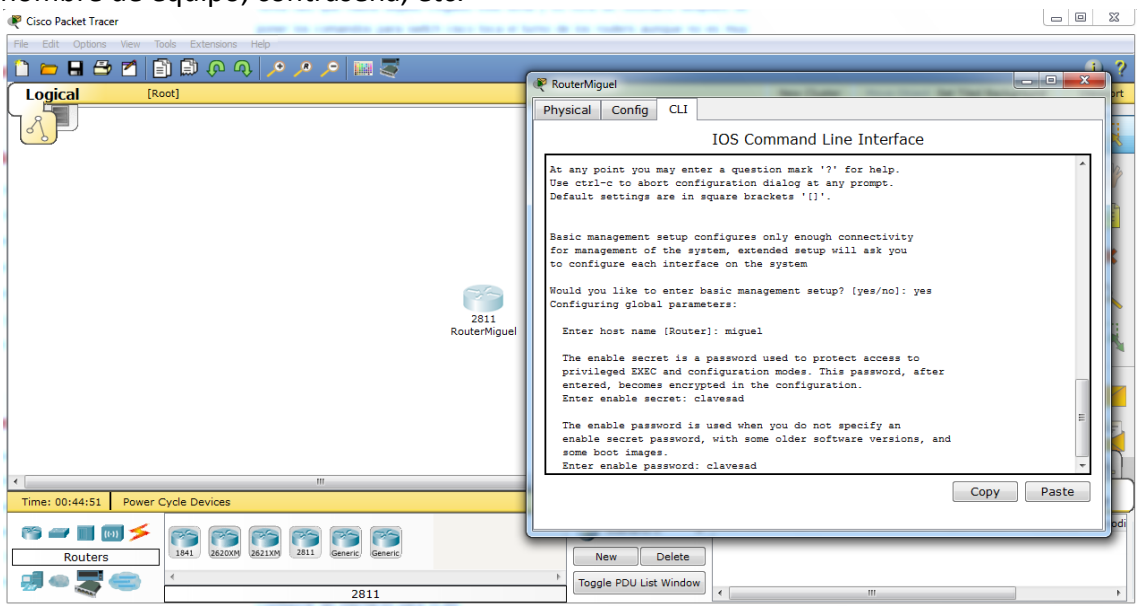
a) Configura en modo seguro un switch CISCO (Packet Tracer)

En el Packet Tracer, insertamos un switch, y lo configuramos con los comandos que escribimos a continuación, para configurar una contraseña para hacerlo seguro.



b) Configura en modo seguro un router CISCO

Insertamos un router cisco en el Packet Tracer, y configuramos en modo comando, el nombre de equipo, contraseña, etc.



c) Elabora un documento que manifieste las vulnerabilidades en las capas enlace, red (IP), TCP-UDP y Aplicación (DHCP, DNS,…) y como protegerse de las mismas.

Vulnerabilidades:

CAPA DE RED

Los principales inconvenientes en esta capa pueden ocurrir si alguien tuviera acceso a los equipos con los que la red opera, es decir, acceso al cuarto de telecomunicaciones, al cableado o a los equipos remotos establecidos para la comunicación

CAPA DE ENLACE
Es la capa de donde mayor información se puede obtener para vulnerar un sistema. Lo fundamental para acceder a ésta es tener acceso a los datagramas IP los que se pueden encontrar en cada paquete que circula por la red, mediante Software espías.

CAPA DE TRANSPORTE
Las principales vulnerabilidades están asociadas a la autenticación de integración y autenticación de confidencialidad. Estos términos se relacionan con el acceso a los protocolos de comunicación entre capas, permitiendo la denegación o manipulación de ellos

CAPA DE APLICACIÓN
Los posibles inconvenientes a presentarse pueden ser ocasionados por cuatro puntos, principalmente los que están asociados a la autenticación de datos y los protocolos presentes en ésta capa.

- Se establecen las deficiencias del servicio de nombres de dominio. Lo que ocurre con éste servicio, es que se encarga de generarlas solicitudes de cada usuario que circulan por la red, es decir, en el momento que una persona solicita una conexión a un servicio determinado, se solicita una dirección IP y un nombre de dominio, se envía un paquete UDP (Protocolo de Comunicación el cual envía los datos del usuario) a un servidor DNS (Dominio de Nombre de Servicio). Lo que hace el servidor DNS es responder a ésta solicitud y entregar los datos que fueron pedidos, donde éste servidor DNS funciona como una base de datos en donde se encuentran las direcciones que solicitan los usuarios, por lo tanto, cuando se tiene acceso a esta especie de base de datos se presenta un inconveniente, el cual hace vulnerable al sistema, ya que puede ser modificada a gusto de la persona que le quiere sacar provecho a esa información.
- Está dado por el servicio Telnet, el cual se encarga de autentificar la solicitud de usuario, de nombre y contraseña que se trasmiten por la red, tanto por el canal de datos como por el canal de comandos.
- Está dado por File Transfer Protocol (FTP), el cual al igual que el servicio Telnet, se encarga de autentificar. La diferencia se encuentra en que el FTP lo hace más vulnerable ya que es de carácter anónimo.
- Está dado por el protocolo HTTP, el cual es responsable del servicio World Wide Web. La principal vulnerabilidad de este protocolo, está asociado a las deficiencias de programación que puede presentar un link determinado lo cual puede poner en serio riesgo el equipo que soporta este link, es decir, el computador servidor.

Medidas de Protección:

CAPA DE ENLACE

Seguridad inalámbrica: La seguridad en las redes inalámbricas es sumamente importante, por la facilidad con que cualquiera puede encontrarlas y acceder a ellas. Cualquier persona con un ordenador portátil puede encontrar fácilmente el punto de acceso inalámbrico de nuestra red inalámbrica, pudiendo así ingresar en nuestros archivos, utilizar nuestra conexión a internet, obtener datos importantes que se transfieran en la red inalámbrica, etc. Por ejemplo, la ausencia de seguridad en nuestra red inalámbrica o nuestro punto de acceso a internet inalámbrico puede hacernos víctimas del piggybacking, del phishing, del robo de información, etc.

CAPA DE RED

IPSec: IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

CAPA DE TRANSPORTE

SSL (TLS): Secure Sockets Layer (SSL; protocolo de capa de conexión segura) y su sucesor Transport Layer Security (TLS; seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

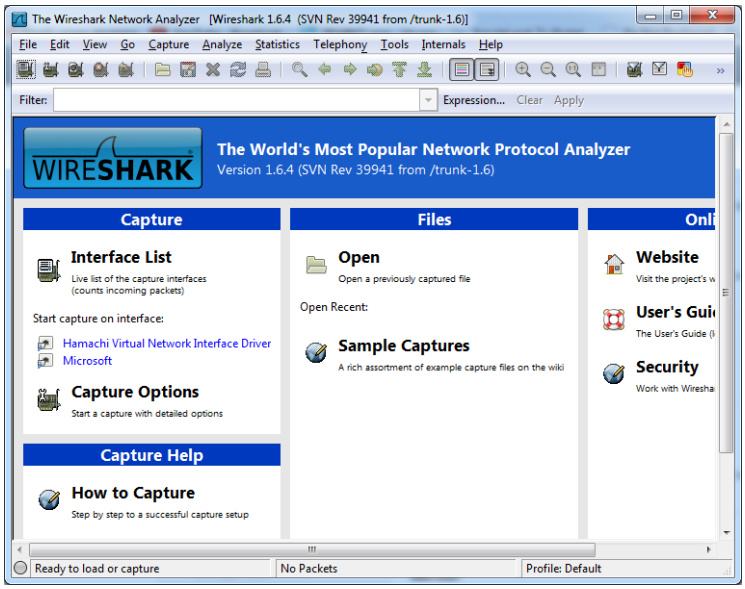
CAPA DE APLICACIÓN

PGP: Pretty Good Privacy o PGP (privacidad bastante buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

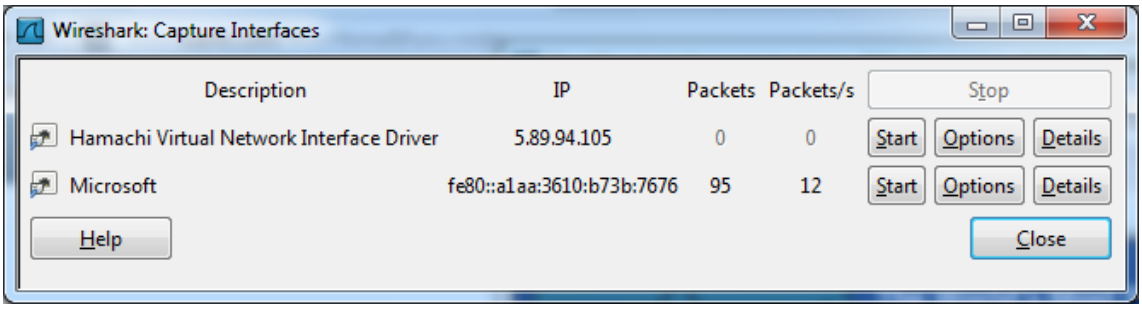
7. MONITORIZACIÓN DEL TRÁFICO EN REDES: HERRAMIENTAS

a) Descarga e instala Wireshark y realiza filtrado de servicios de red para monitorizar sólo el tráfico deseado.

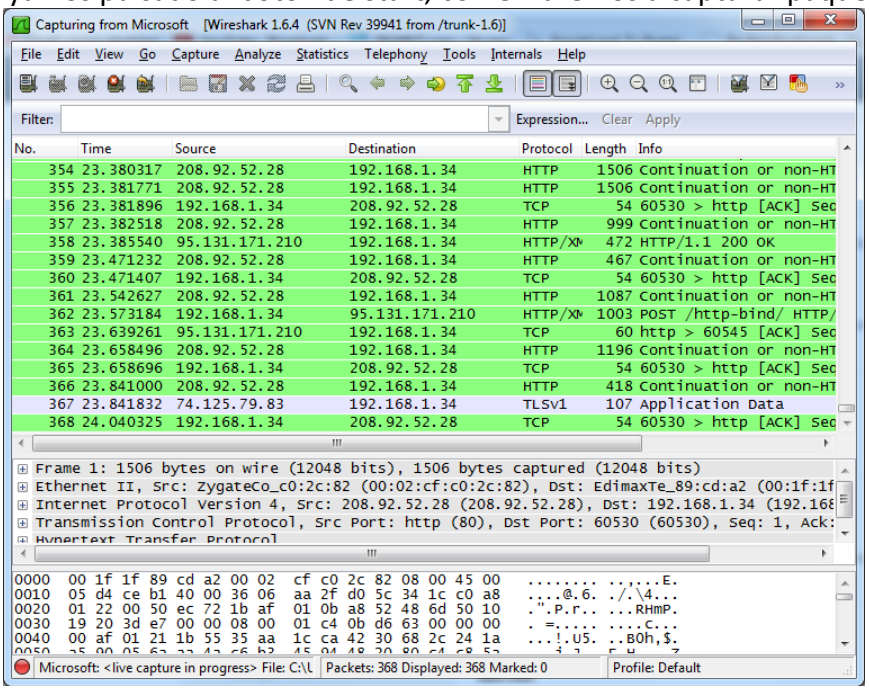
Instalamos la aplicación Wireshark que es una herramienta para monitorizar los paquetes de la red. Una vez instalado lo ejecutamos.



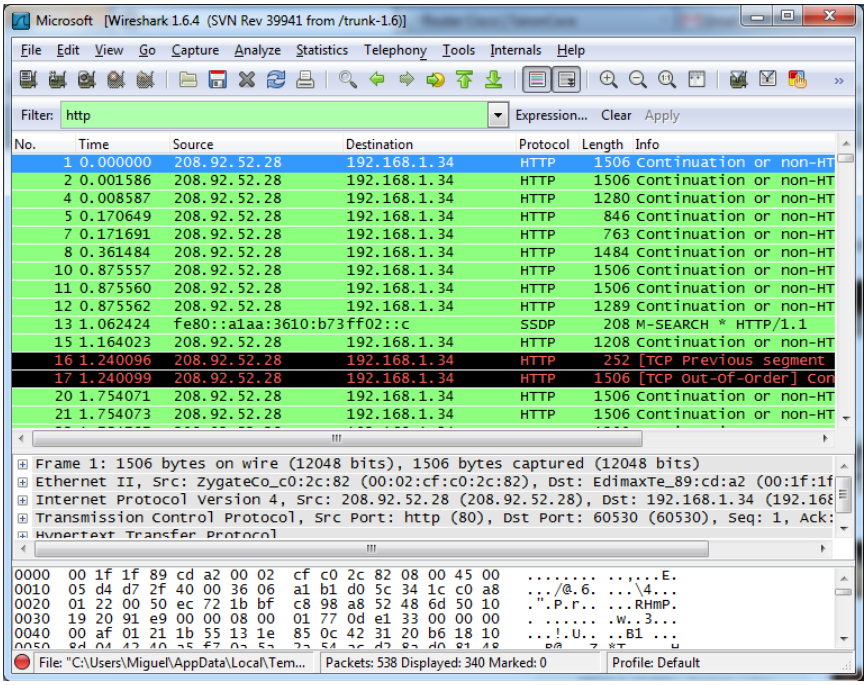
Seleccionamos la interfaz que deseamos monitorizar, pulsamos start.



Una vez hayamos pulsado al botón de start, comenzaremos a capturar paquetes.

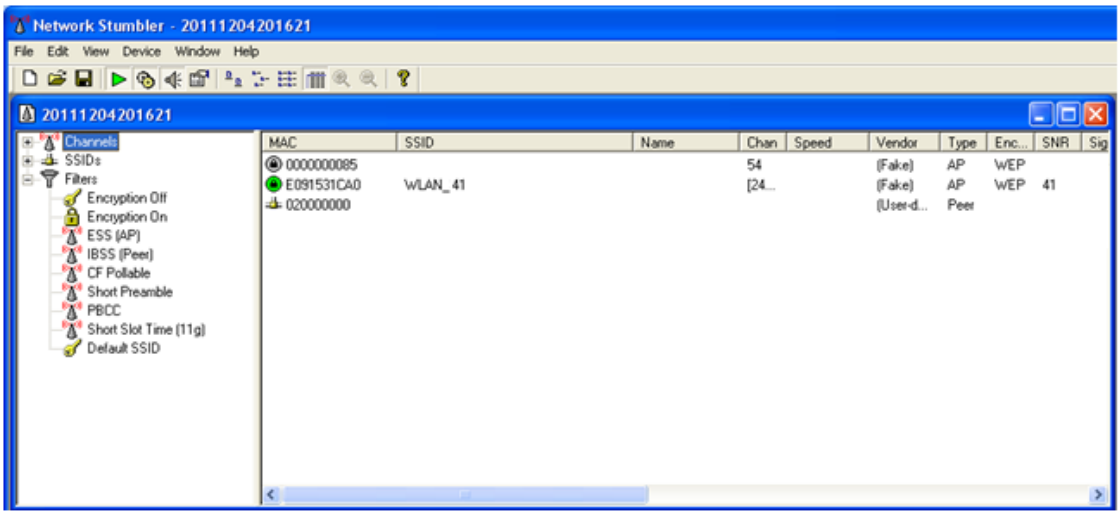


Usaremos un filtro para monitorizar sólo los paquetes deseados, utilizamos por ejemplo un filtro para ver solo los paquetes de “**http**”.

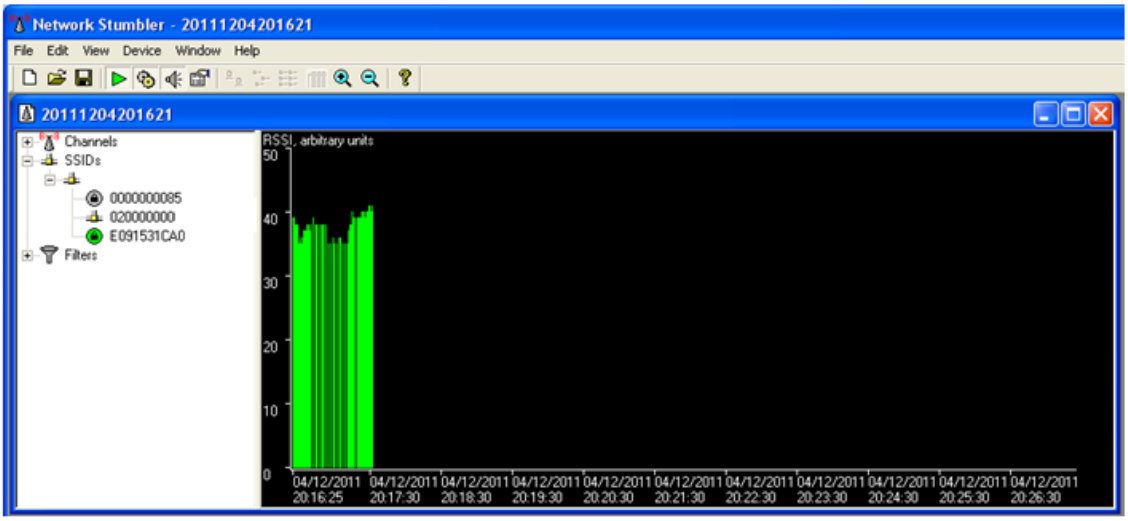


b) Descarga e instala Kismet o Network Stumbler para redes inalámbricas y realiza filtrados de red para monitorizar sólo el tráfico deseado.

Descargamos la aplicación NetWork Stumbler, que la utilizamos para monitorizar redes inalámbricas. Elegimos el punto de acceso de nuestra casa, en mi caso WLAN_41 y procedemos a observar la captura.



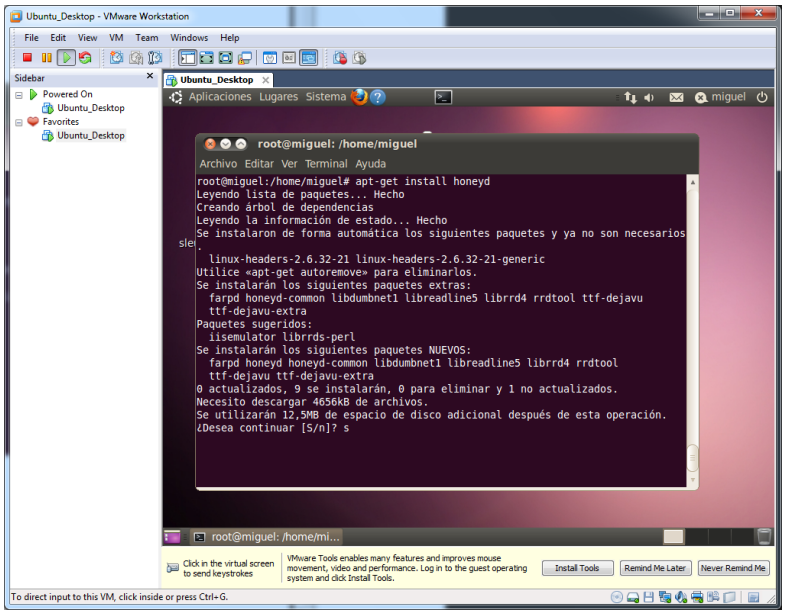
En este gráfico podemos monitorizar gráficamente la información de nuestro punto de acceso.



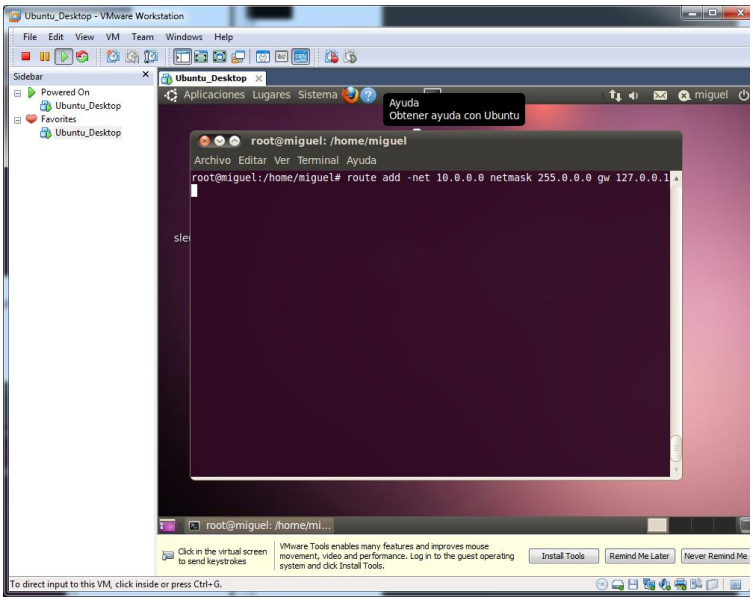
8. INTENTOS DE PENETRACIÓN:

a) **Honeypot**. Instalación, configuración, ejecución y prueba en Windows o GNU/Linux de **honeyd**

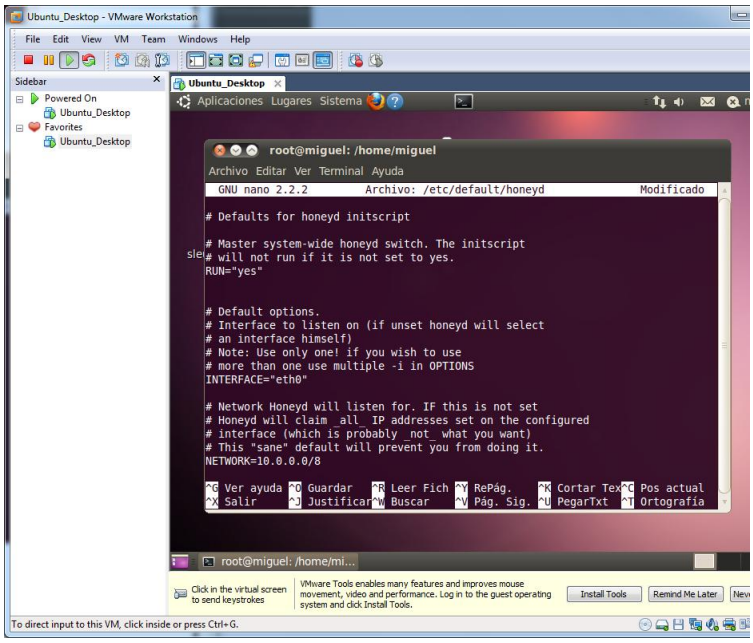
Honeypot es una aplicación que nos permite detectar intrusos, para instalarlo introducimos el comando **“apt-get install honeyd”.**



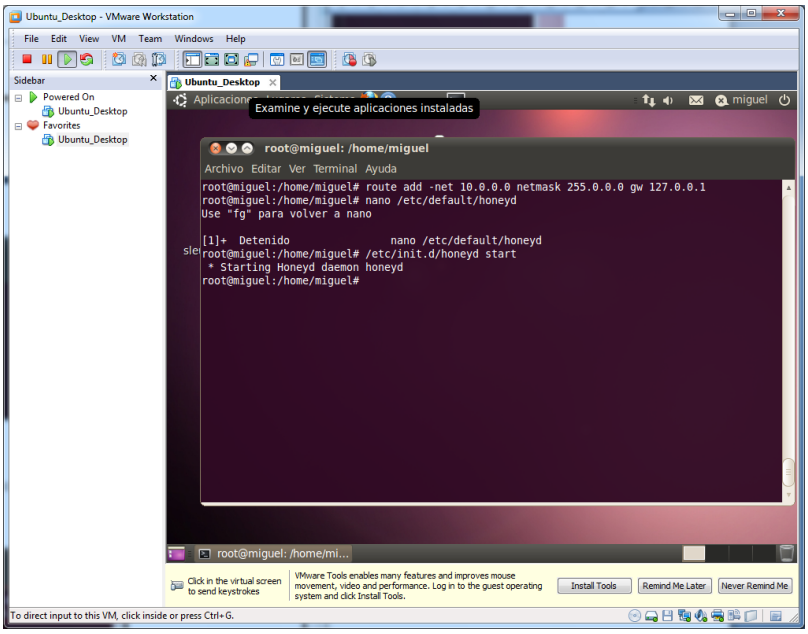
Una vez instalado tenemos que especificar una ruta para la tabla de enrutamiento. Con el siguiente comando.



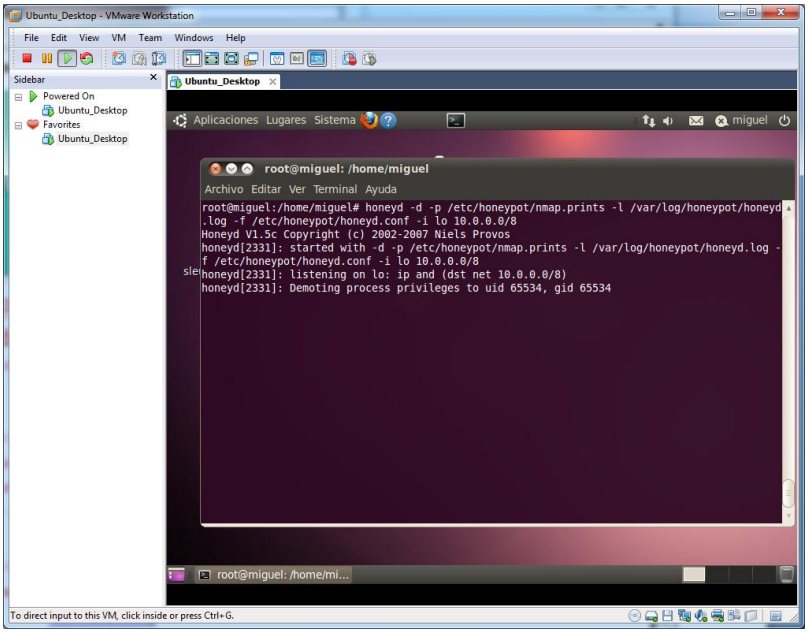
Editamos el fichero honeyd, dentro de "**/etc/default**", y configuramos los parámetros RUN como "**Yes**" y INTERFACE como "**eth0**".



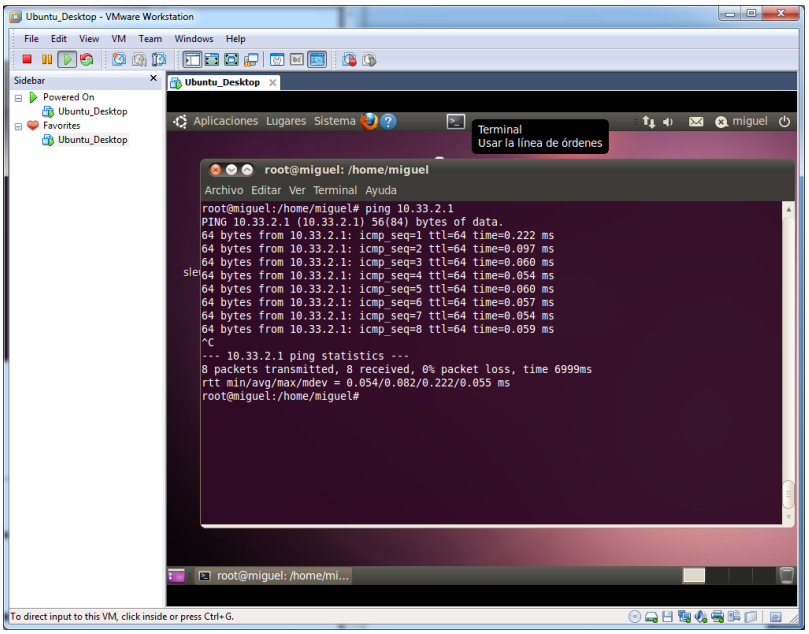
Comprobamos que funciona correctamente el servicio.



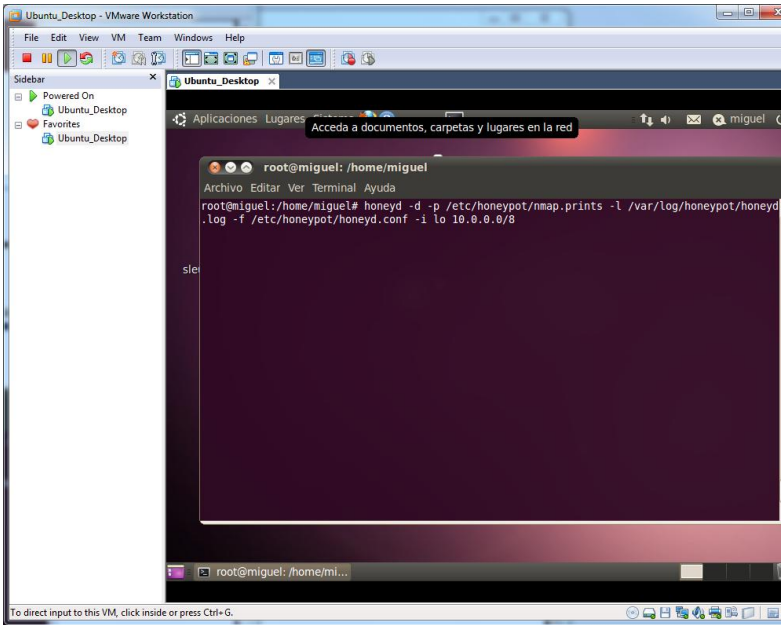
Finalmente comprobamos que la aplicación funciona.



Comprobamos con un ping a la dirección 10.33.2.1



Y ejecutamos de nuevo este comando, para detectar al intruso.

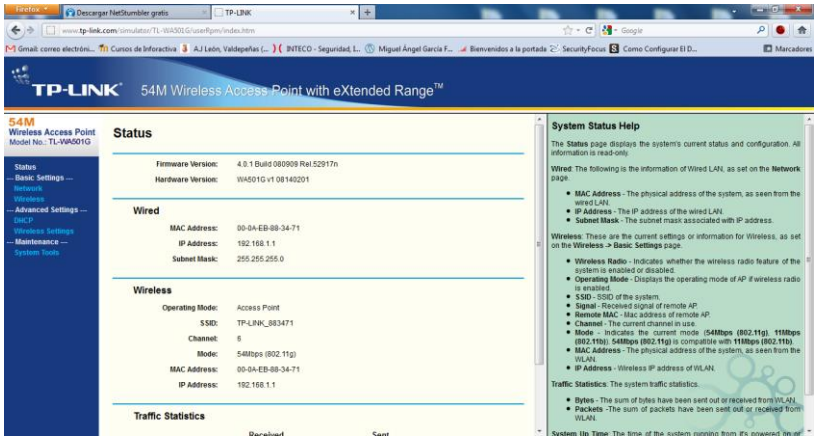


9. SEGURIDAD EN LAS COMUNICACIONES INALÁMBRICAS.

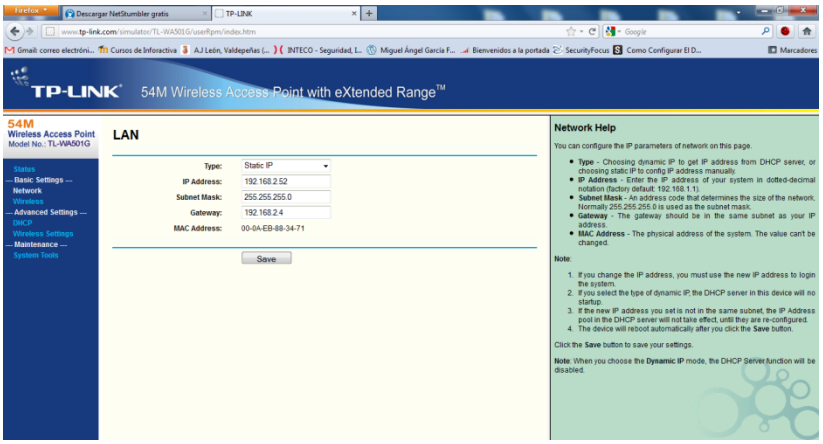
a) Configuración de un punto de acceso inalámbrico seguro.

Vamos a configurar los elementos básicos de un punto de acceso inalámbrico.

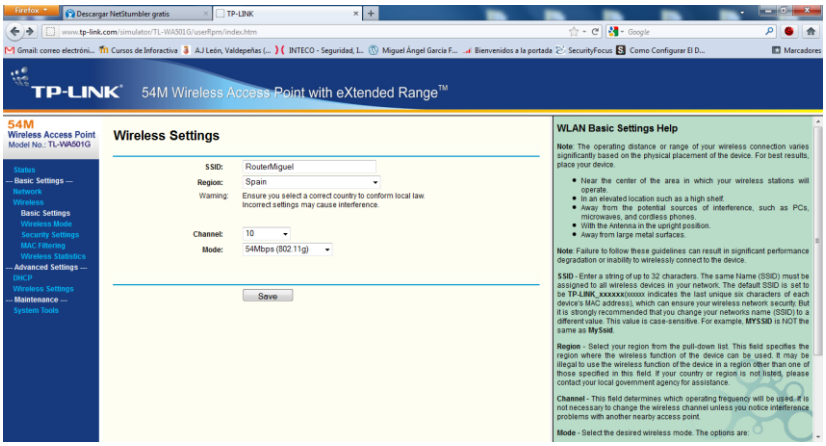
Accedemos al Router, y nos situamos en la siguiente pantalla, con algunos de los parámetros iniciales.



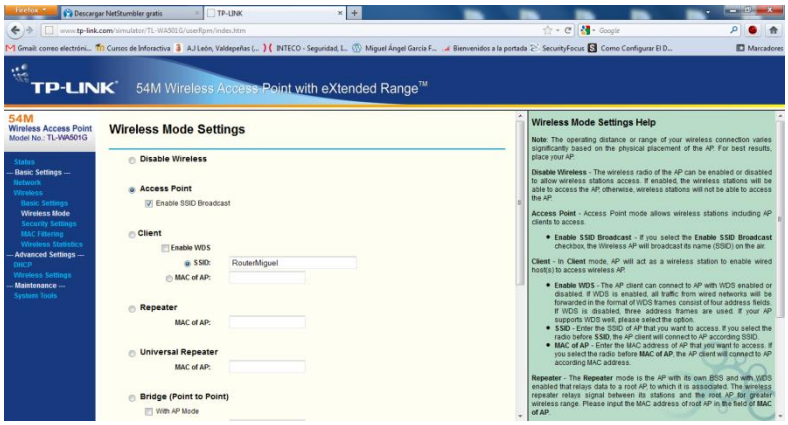
Configuramos las IPs del punto de acceso inalámbrico. En la opción Network de “Basic Settings”.



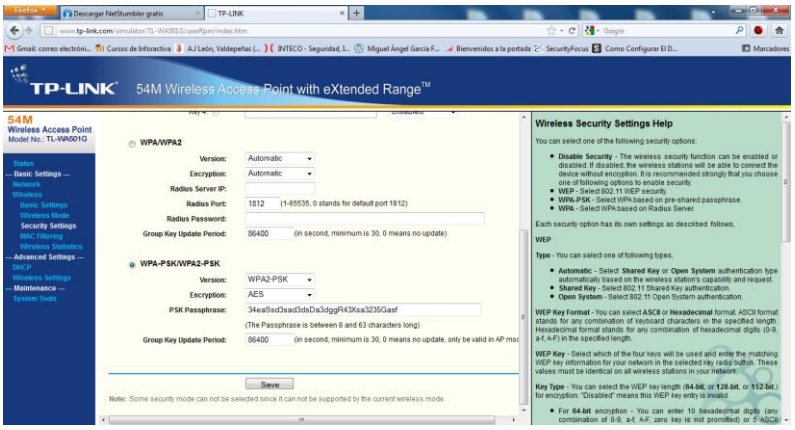
En la opción Wireless Settings, cambiamos el SSID del router, la región, canal y modo de transmisión.



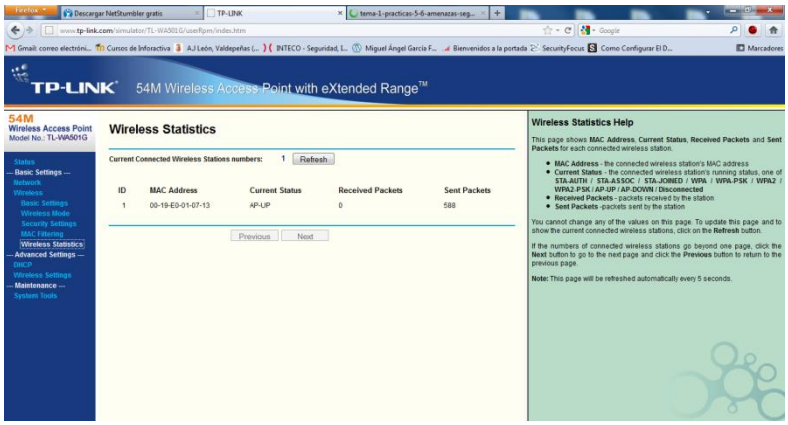
En la siguiente pantalla podemos realizar diferentes configuraciones.



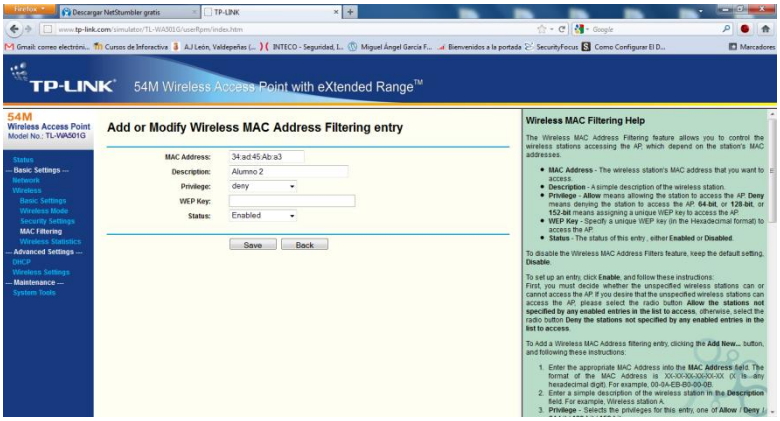
En el modo Security Setting asignaremos una clave del tipo VPA2-PSK, del tipo AES. Para el acceso al medio inalámbrico.



Si nos vamos a las estadísticas inalámbricas, podemos comprobar los equipos o sus direcciones MAC que están conectados.

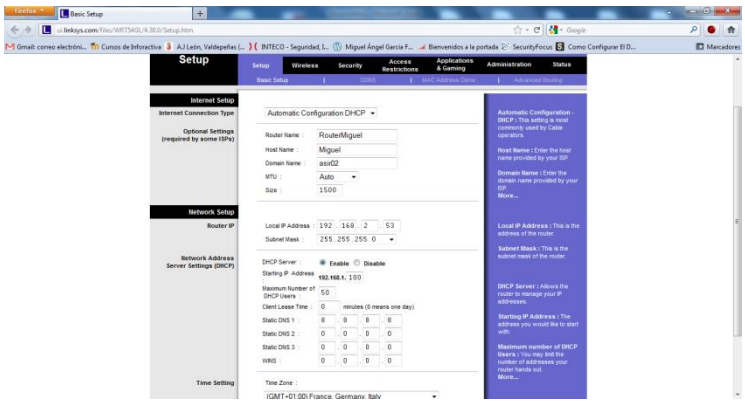


Podemos hacer un filtro de las direcciones Mac que queramos y denegar su acceso.

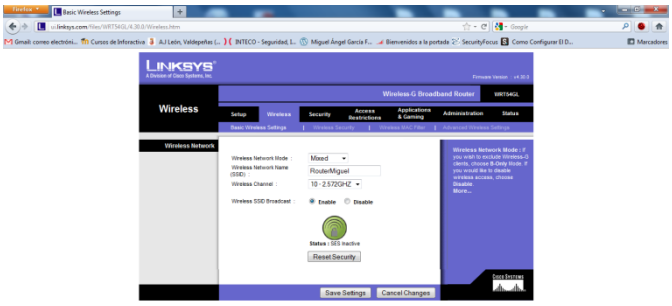


b) Configuración de un router de acceso inalámbrico CISCO LINKSYS WRT54GL, utilizando un simulador.

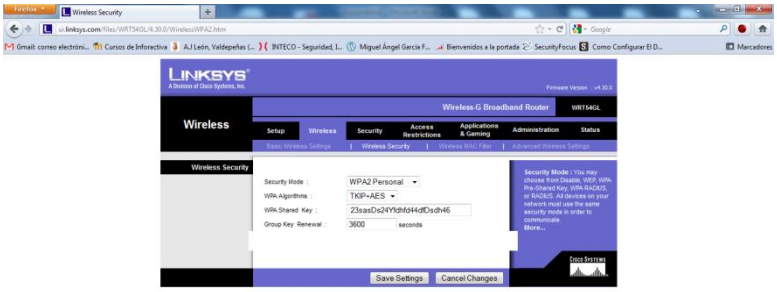
Nos situamos en las configuraciones básicas del router o “Basic Setup”, en esta opción configuramos el nombre del router, dominio, Dirección Ip, Submáscara, dhcp, rango de direcciones etc.



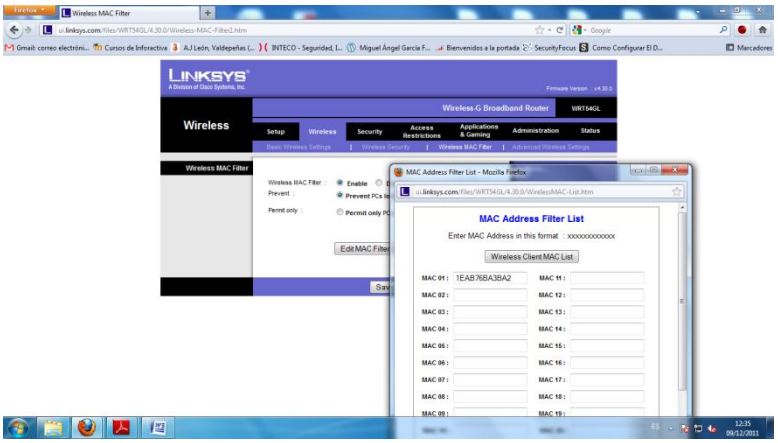
En la pestaña wireless, en la configuración básica de wireless, escribimos el nombre de SSID de nuestro router y el canal de transmisión.



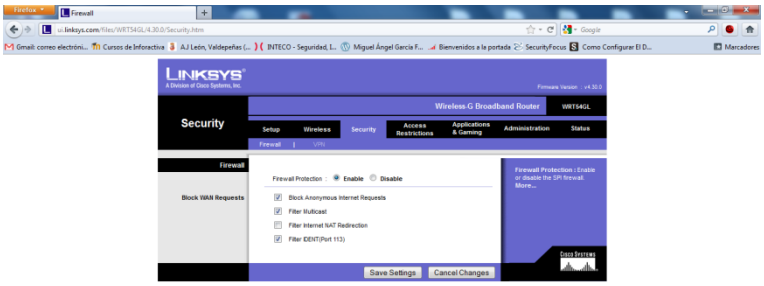
En la opción seguridad de la inalámbrica o wireless, elegimos el tipo de clave o password que vamos a usar, en nuestro caso escogemos WPA2, del tipo TKIP-AES.



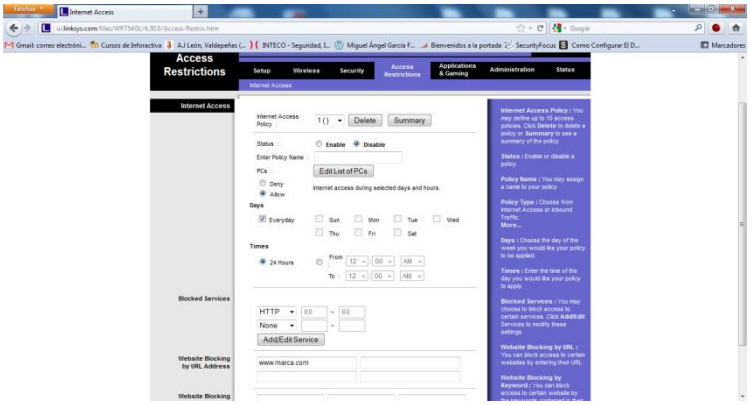
Podemos utilizar un filtro de direcciones MAC, para permitir o denegar alguna máquina.



En la pestaña seguridad, podemos configurar parámetros relacionados con cortafuegos.



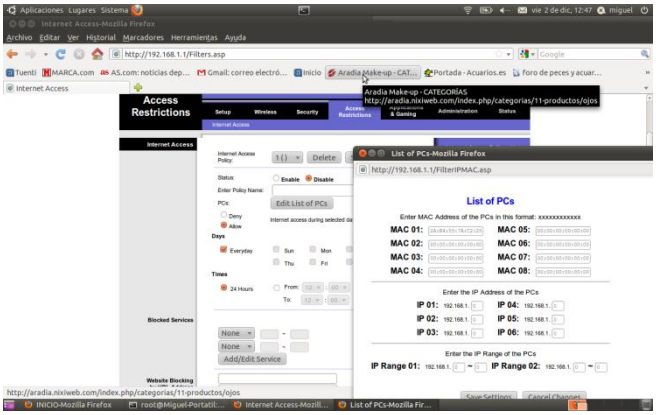
Finalmente, en las restricciones de acceso, podemos restringir puertos o incluso direcciones de páginas web.



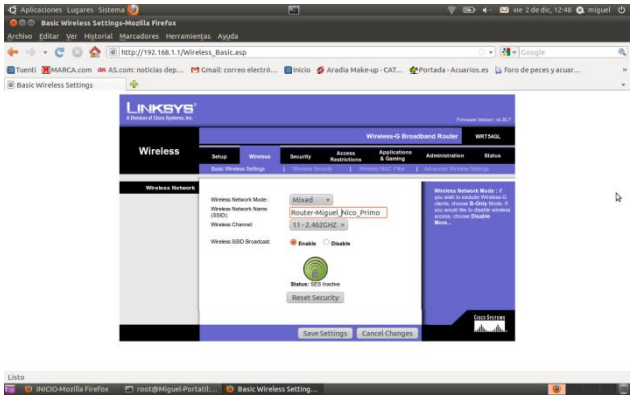
c) Configuración de un router de acceso inalámbrico CISCO Linksys seguro y un cliente de acceso inalámbrico en Windows y GNU/Linux.

- Filtro MAC, WPA, Control parental.

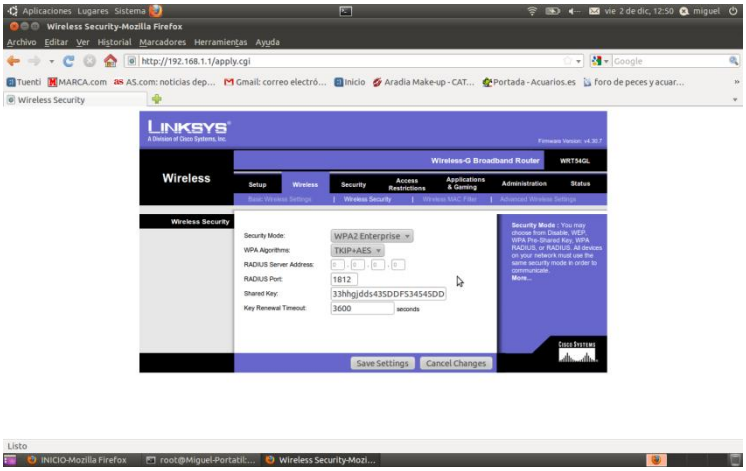
Configuramos el router inalámbrico de clase. En la pestaña restricciones de acceso podemos filtrar direcciones MAC, para evitar el acceso a los equipos de dichas direcciones.



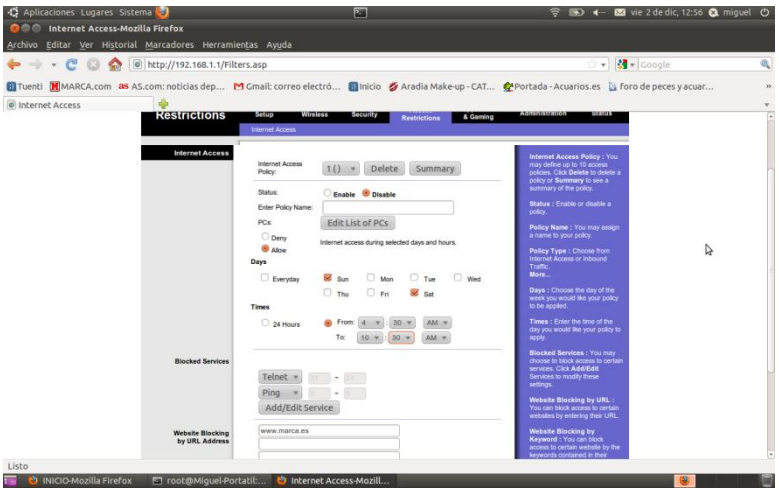
Configuramos el nombre de nuestro Router inalámbrico de clase. Elegimos el canal.



En la pestaña Wireless, configuramos nuestra clave del router, con seguridad WPA2 y modo TKIP-AES introduciendo la clave. Además podemos configurar un servidor Radius.

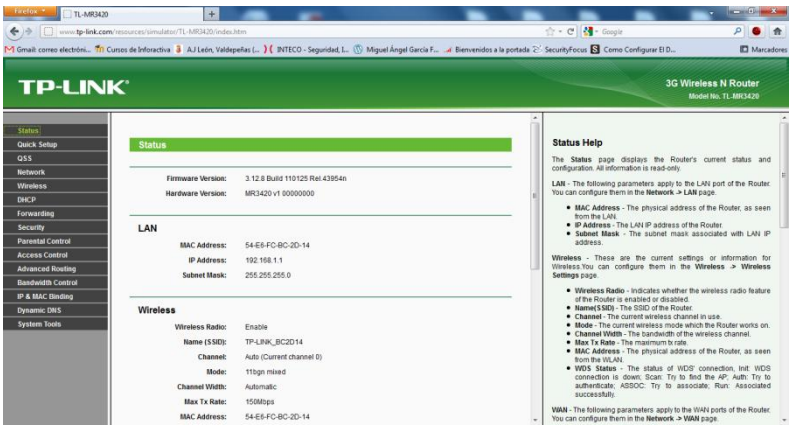


En la pestaña de restricciones y control parental, podemos elegir los días de acceso con sus respectivas horas y además podemos denegar puertos y páginas web.

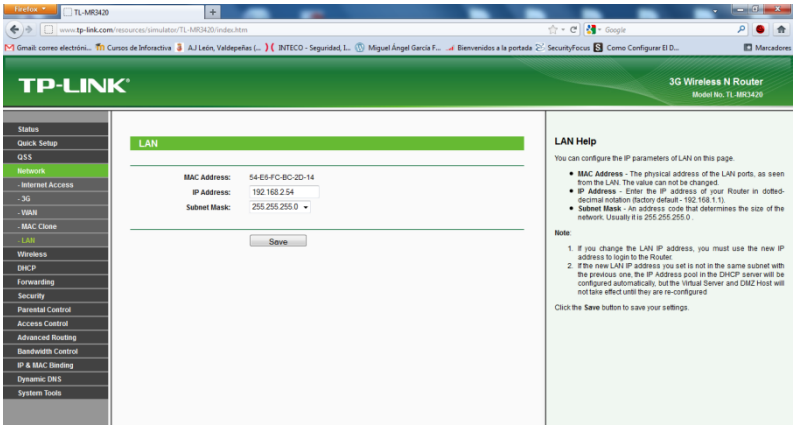


d) Configuración de un router de acceso inalámbrico TP-LINK, utilizando un simulador.

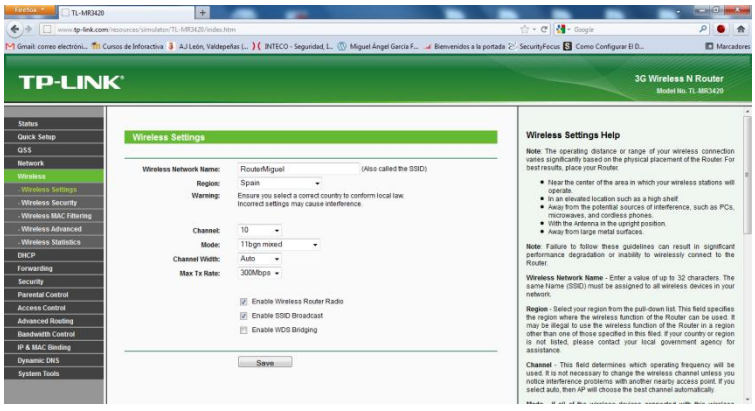
Accedemos al router de acceso inalámbrico TP-LINK, en la pantalla principal o Status, podemos observar distintos parámetros del router que nos vienen configurados por defecto.



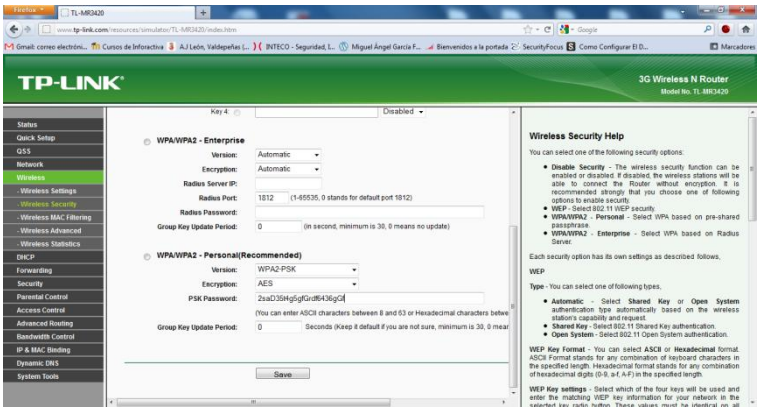
En la opción Network, LAN, Configuramos parámetros de nuestro router, como nuestra IP y la submáscara.



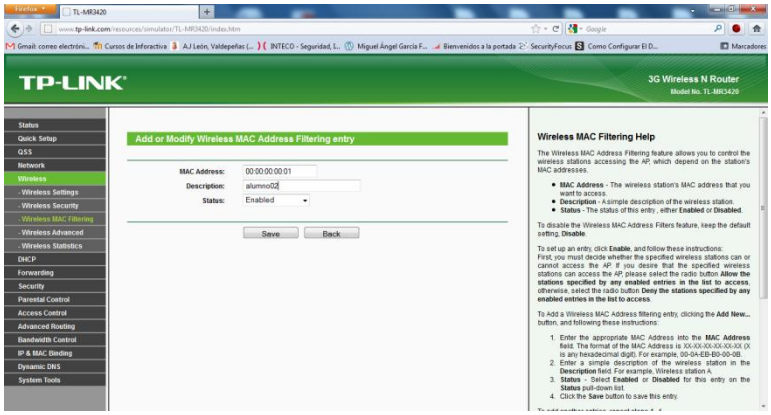
Nos situamos ahora en la configuración inalámbrica, elegimos el nombre de nuestro router, nuestra región, el canal, y el tipo y frecuencia de ancho de banda.



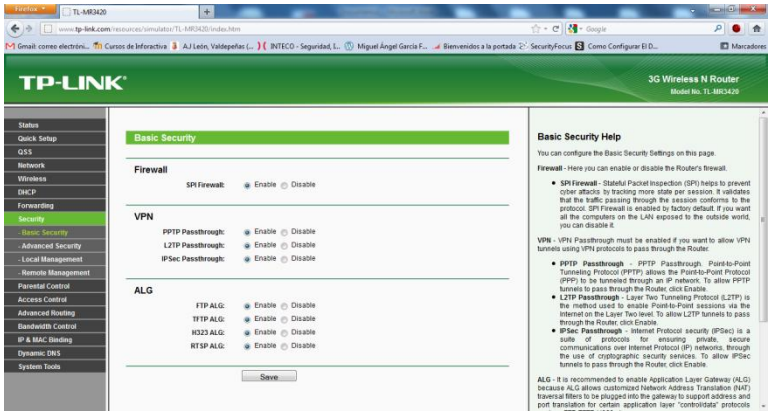
En las opciones de seguridad inalámbricas, elegimos el tipo de clave inalámbrica “**WPA2-PSK**”, modo de encriptación “**AES**”, posteriormente escribimos la clave.



Podemos configurar un filtro de direcciones MAC de algunos equipos.



Podemos además configurar parámetros relacionados con los firewalls o cortafuegos.

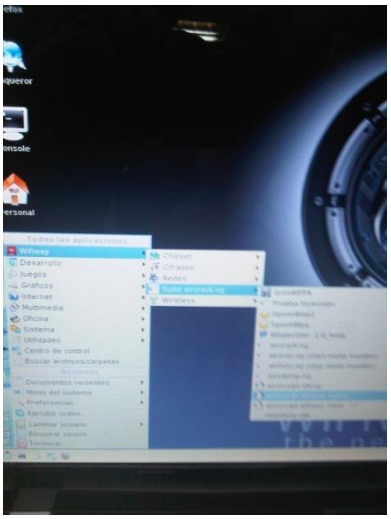


9. SEGURIDAD EN LAS COMUNICACIONES INALÁMBRICAS.

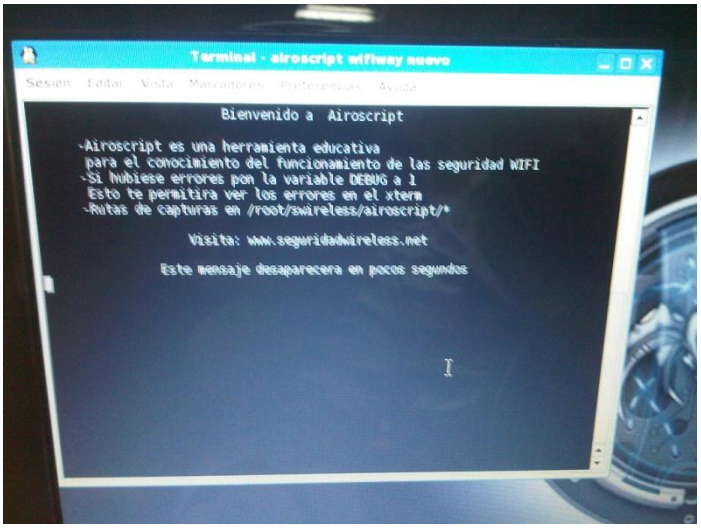
e) Realiza una auditoria wireless para medir el nivel de seguridad de una red inalámbrica, utilizando una aplicación para monitorizar y recuperar contraseñas inalámbricas WEP (airodump, aircrack, etc)

f) Realiza una auditoria wireless para medir el nivel de seguridad de una red inalámbrica, utilizando una distribución Live (Backtrack, Wifiway, Wifislax, etc) para monitorizar y recuperar contraseñas inalámbricas WEP.

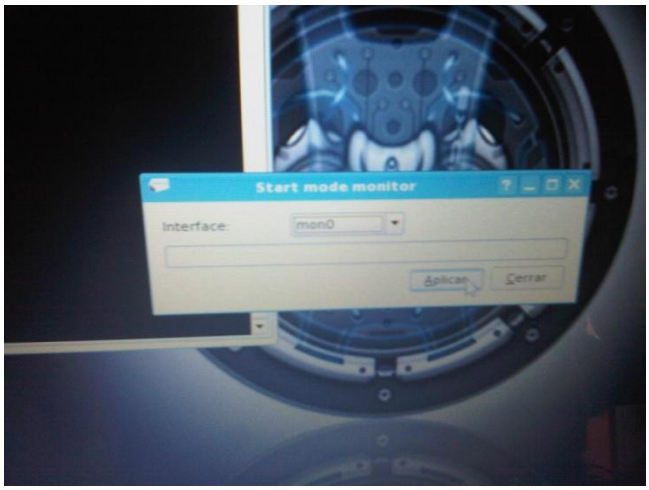
Vamos a sacar la clave de acceso, de nuestro router inalámbrico de clase, arrancamos en un disco el WifiWay.



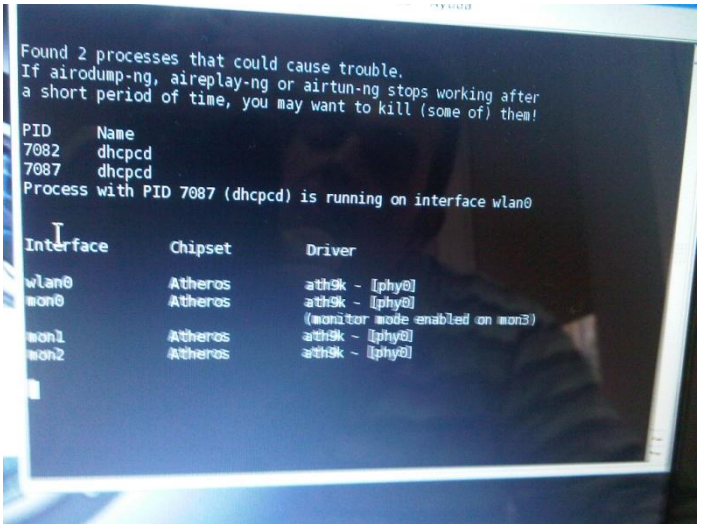
Arrancamos el airoscript, e iniciamos una nueva auditoría



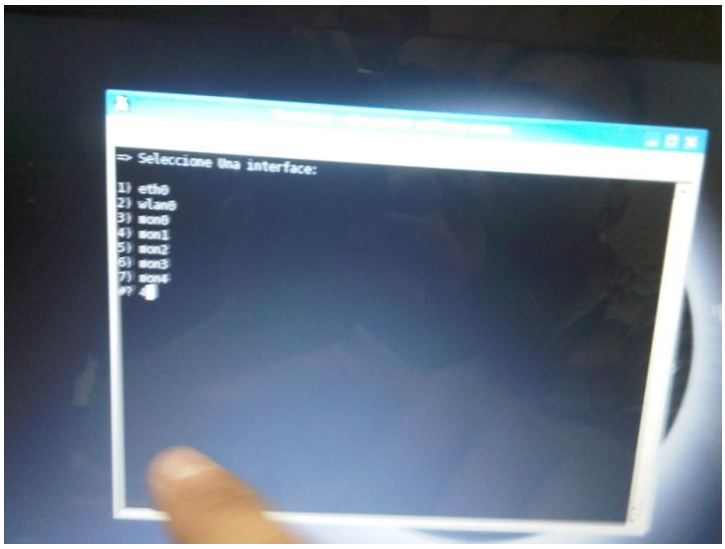
Como es lógico debemos elegir, la interfaz o tarjeta de red que usaremos para analizar el tráfico de la red.



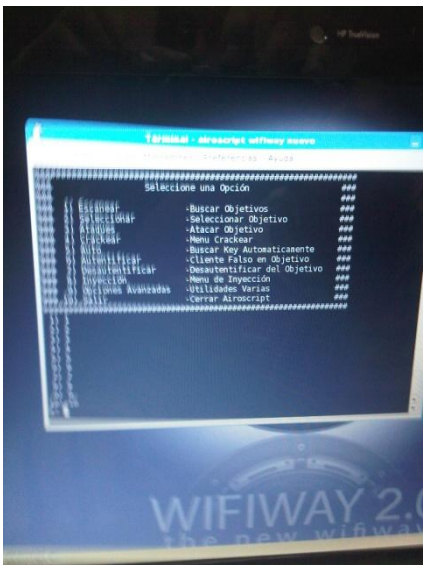
Elegimos la opción Wlan0, ya que vamos a capturar paquetes del entorno inalámbrico.



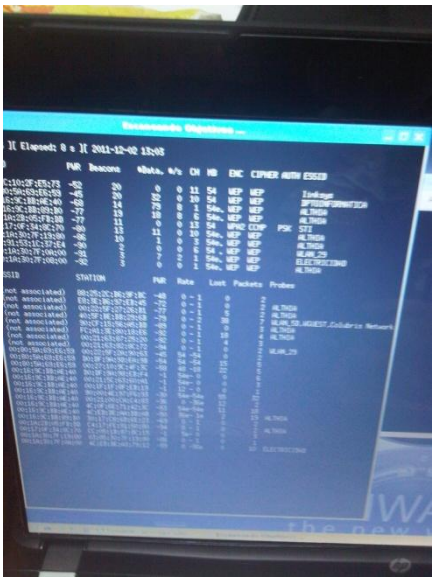
En el siguiente menú, escogemos el entorno de nuevo “Wlan0”.



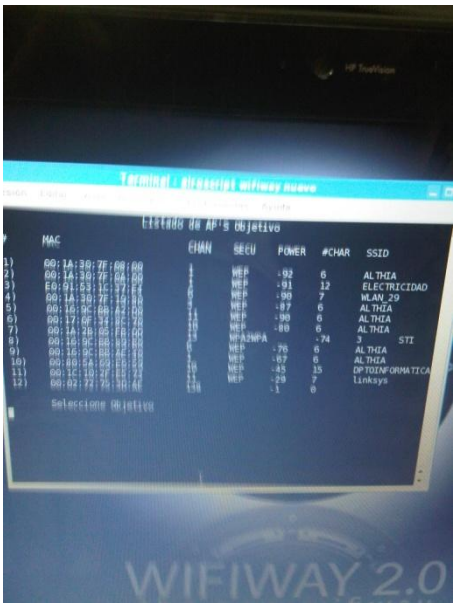
Seleccionamos del menú las opciones que queramos realizar, en nuestro wifiway, para empezar vamos a escanear los objetivos para escoger el punto de acceso al que vamos a capturar paquetes, para ello escogemos la opción 1.



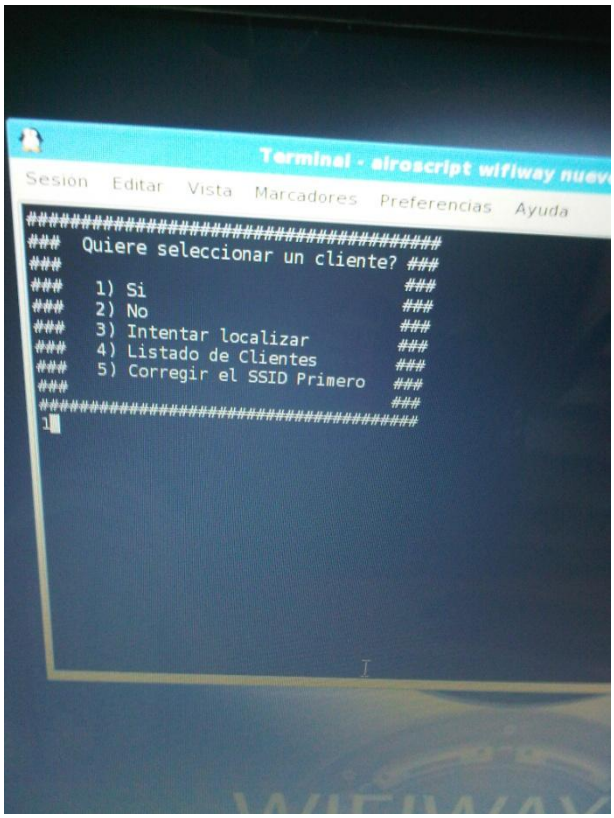
El airoscript comenzará, a capturar información del entorno inalámbrica, capturando los puntos de acceso visibles con sus respectivas direcciones MAC.



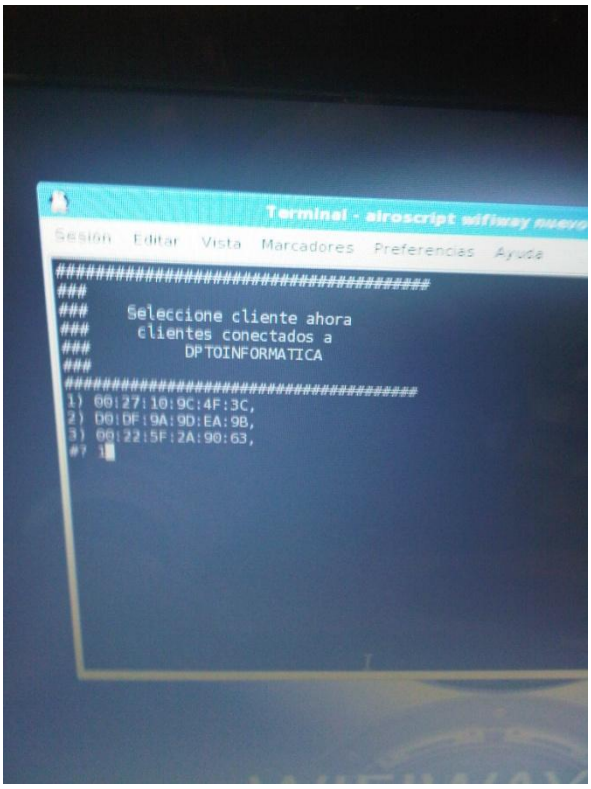
Una vez hayamos capturado los distintos puntos de acceso disponibles, los tendremos organizados en el siguiente menú, nosotros vamos a intentar sacar los paquetes y las claves de nuestro router de clase configurado por nosotros. Elegimos la opción 12 que corresponde a nuestro router Linksys.



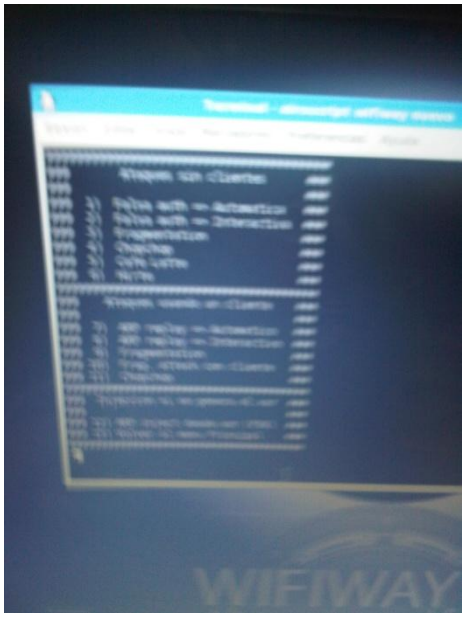
Elegimos la primera opción, para escoger un cliente, al cual vamos a capturar los paquetes con el “aircrack”.



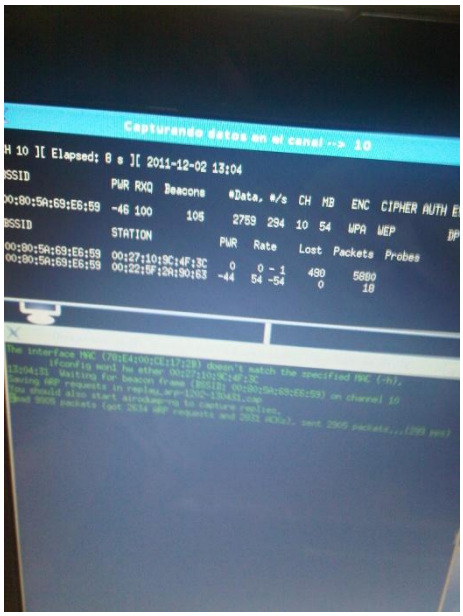
Elegimos una dirección MAC de cliente, para capturar los paquetes al router inalámbrico.



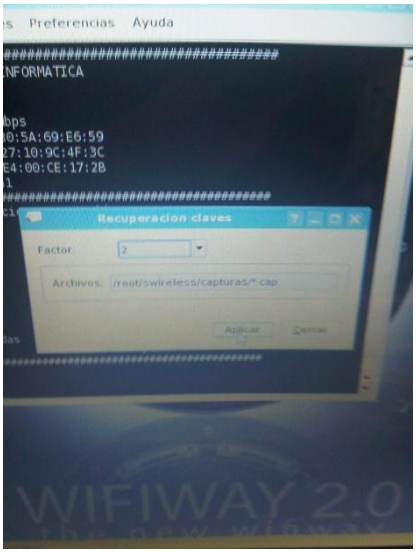
En el menú de ataque de clientes podemos elegir la opción de realizar ataque.



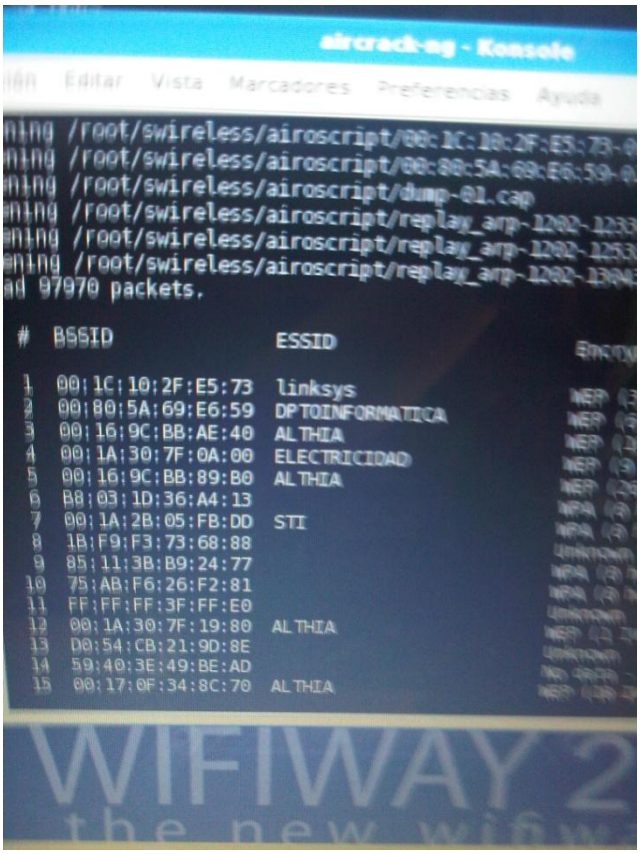
Inicializamos la captura de paquetes.



Una vez tengamos una cantidad de paquetes capturados adecuados, tenemos que crackear o recuperar la clave del router con el aircrack, elegimos el lugar donde tenemos guardada la información necesaria para desencriptar la clave.



Comenzamos el crackeo de la password del router.



Una vez crackeado y desencriptado, tenemos a nuestra disposición nuestra clave resuelta, que configuramos en nuestro punto de acceso anteriormente. Hemos sacado la clave con éxito.