"Gregorio Prieto"	**Practicas Tema 1 SIAD**		
		Antonio Quevedo Bueno	SIAD

1. Estar al día: Visitar los sitios web www.inteco.es ó www.securitybydefault.com y presentar una guía o artículo al resto de compañeros.

2. Confidencialidad:

2.1- Utilizar en Windows EFS (Encryted File System).

2.2- Utilizar PGP en Linux.

3. Integridad:

3.1- Utilizar en Windows SFC (System File Checker).

3.2- Utilizar en GNU/LINUX Rootkit Hunter.

4. Disponibilidad:

4.1.-Utilizar NMAP, ZNMAP o ZENMAP (www.nmap.org)

4.2-Utilizar NESSUS (www.nessus.org)

4.3-Microsoft Baseline Security Analyzer (MBSA)

4.4-Trabajo: Análisis de vulnerabilidades con: NMAP,

5. Amenazas:

5.1-Visitar el enlace :

http://openmultimedia.ie.edu/OpenProducts/securityxperts/securityxperts/portada.html

para:

5.1.1-*Jugar al Juego de Seguridad:* Elabore un resumen de los ataques que se proponen en el juego y el sistema de seguridad empleado.

5.1.2-*Elaborar un resumen del ataque sufrido a IRC Hispano* (Caso Ronnie).

5.2-Busca en Internet al menos una noticia relacionada con amenazas físicas a sistemas informáticos respecto a:

5.2.1-Robos, sabotajes, destrucción de sistemas.

5.2.2-Catástrofes, Incendios, Cortes de suministro eléctrico

5.3-Busca en Internet al menos una noticia relacionada con amenazas lógicas respecto a:

5.3.1-Ataques a un sistema informático - Ciberdelitos.

5.3.2- Ciberfraudes - Vulnerabilidades y Amenazas .

5.4-Busca al menos dos antivirus on line y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación:

(Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y virus encontrados y desinfectados)

5.5-Instala al menos dos antivirus en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación:
(Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y virus encontrados y desinfectados).
5.6-Instala al menos dos aplicaciones antimalware en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación:
(Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y *malware* encontrado y desinfectados).
6. Seguridad física y ambiental:
6.1-Se necesita realizar **un estudio de la ubicación y protección física de los equipos y servidores del aula,** desde el punto de vista de:
6.1.1-Acondicionamiento físico (Extintores, Sistema de aire acondicionado, Generadores eléctricos autónomos, racks)

6.1.2- Robo o sabotaje: Control de acceso físico y vigilancia mediante personal y circuitos cerrados de televisión (CCTV).

6.1.3- Condiciones atmosféricas y naturales adversas (Ubicación de sistemas, centros de respaldo en ubicación diferente al centro de producción, mecanismos de control y regulación de temperatura, humedad, etc.)

Para elaborar dicho estudio recogido en un documento se sugiere visitar entre otros los enlaces:
http://www.accesor.com http://www.copiadeseguridadcpd.com/
http://www.unitel-tc.com/index.php?m=15 http://www.biometriaaplicada.com/
http://www.abast.es/cs_condis_cpd.shtml http://www.senfor.com http://www.dabs.com/
6.2- Busca un único SAI para todos los sistemas informáticos del aula. Justifica tu respuesta y compara la misma con una solución de diferentes SAIs a repartir en el aula. Analiza aspectos como tipos de SAI y cálculo energético necesario.
Se sugiere visitar entre otros los enlaces: http://www.newsai.com
http://www.apc.com/es/ http://www.mgeups.co.uk/
http://www.riello-ups.com/?es/configuratore http://www.emersonnetworkpower.com/
6.3-Instalación de una cámara IP y transmisión de la imagen por una red LAN.
Descarga este manual del proceso de instalación de esta cámara IP OVILINK OC-600 y su gestión mediante software.
http://www.ovislink-espana.com/index.php?sec=99

Busca otros manuales de otras cámaras IPS y compara los procesos de instalación.
Elabora un documento con dicha comparación (al menos dos cámaras IPs).

6.4-Instalación de un SAI o UPS en un rack y su posterior uso.

Descarga estos manuales y analiza el proceso de instalación del SAI en un rack y su gestión mediante software.
http://tools.mgeops.net/download/intl/products/evolution/Evol_Ins_and_User_Man.pdf
http://powerquality.eaton.com/Products-services/legacy/patriot-info.asp
Busca otros manuales de otros SAIs y compara las características de este software de SAI .
Elabora un documento con dicha comparación (al menos dos SAIs).

6.5-Ampliar el estudio realizado del apartado a) del aula con la implantación de sistemas biométricos

Se sugiere visitar los enlaces:
http://www.zksoftware.es/ http://www.biometriaaplicada.com/
http://www.kimaldi.com/productos/sistemas_biometricos/
http://www.agedum.com/BioCloser/tabid/110/Default.aspx
http://www.biopassword.com/

2. Confidencialidad:

2.1- Utilizar en Windows EFS (Encryted File System).

Cifrar o descifrar una carpeta o un archivo

El cifrado de carpetas y archivos es una forma de protegerlos frente a un acceso no deseado. El sistema de cifrado de archivos (EFS) es una característica de Windows que permite almacenar información en el disco duro en formato cifrado. El cifrado es la protección de mayor nivel que proporciona Windows para ayudarle a mantener la información a salvo.

Para cifrar una carpeta o un archivo

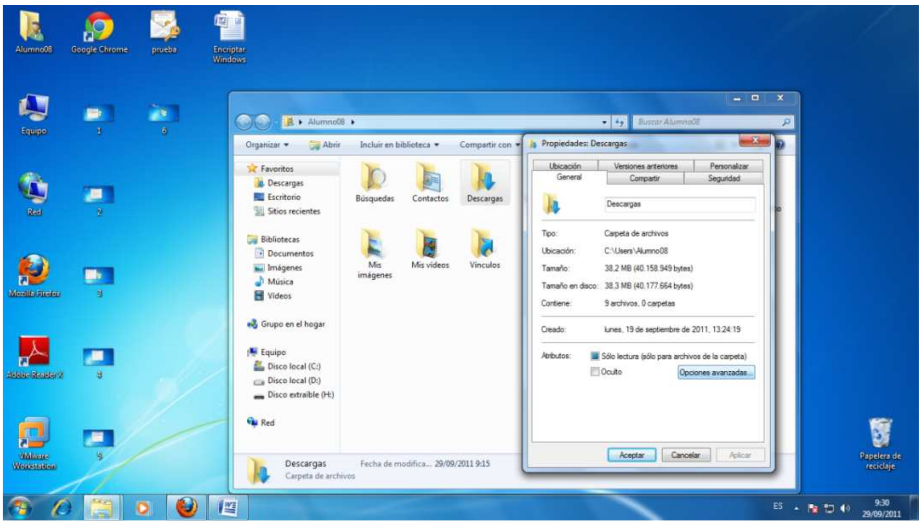
1. Haga clic con el botón secundario en la carpeta o el archivo que desee cifrar, y, a continuación, haga clic en Propiedades.
2. Haga clic en la pestaña General y, después, en Avanzadas.
3. Active la casilla Cifrar contenido para proteger datos y, a continuación, haga clic en Aceptar.

La primera vez que cifre una carpeta o un archivo, debe hacer una copia de seguridad del certificado de cifrado. Si el certificado y la clave se pierden o se dañan y no hizo una copia de seguridad, no podrá usar los archivos que haya cifrado.

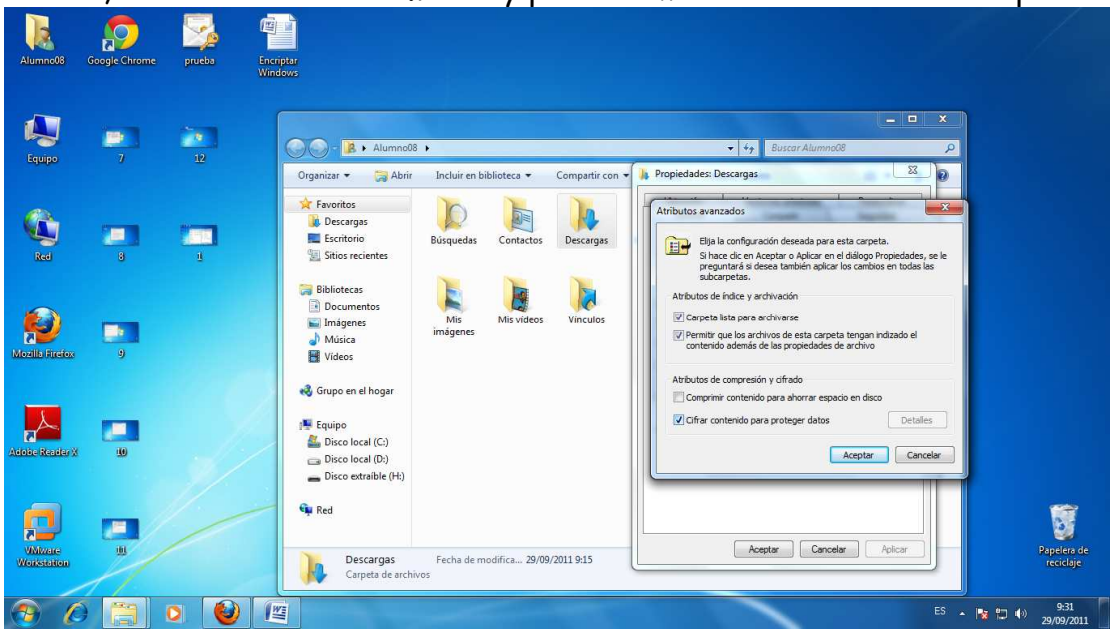
Para descifrar una carpeta o un archivo

1. Haga clic con el botón secundario en la carpeta o el archivo que desee descifrar, y, a continuación, haga clic en Propiedades.
2. Haga clic en la pestaña General y, después, en Avanzadas.
3. Desactive la casilla Cifrar contenido para proteger datos y, a continuación, haga clic en Aceptar.

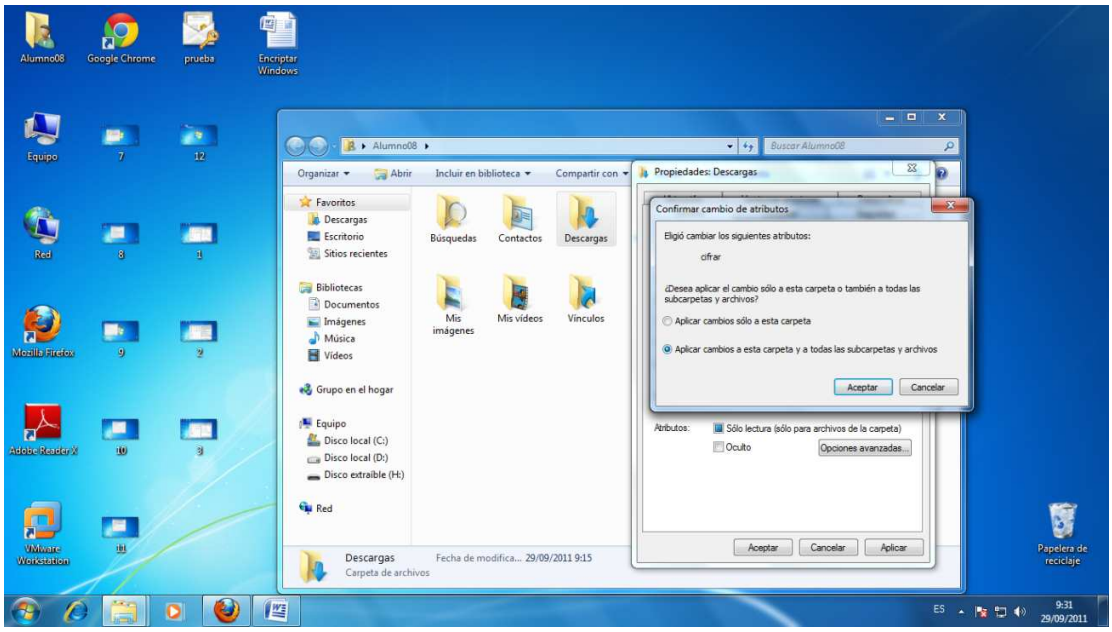
Ejemplo: Vamos a encriptar la carpeta descargas para que otros usuarios no puedan acceder a ella.



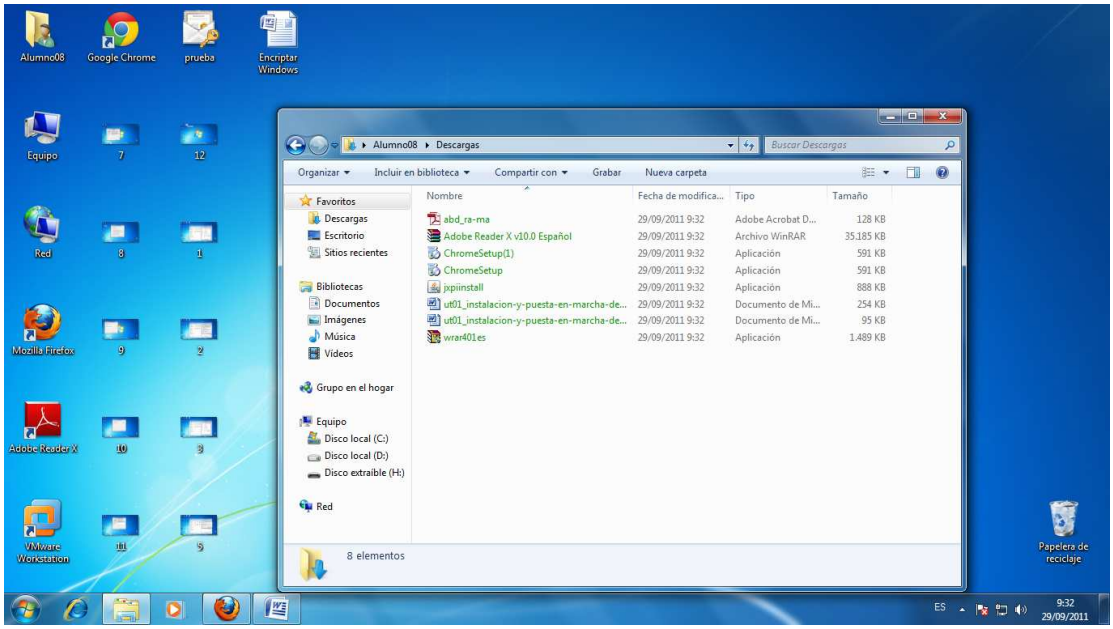
En primer lugar iremos a la carpeta descargar que esta dentro de la carpeta del usuario creada, en nuestro caso **alumno08** y presionamos boton derecho -> Propiedades



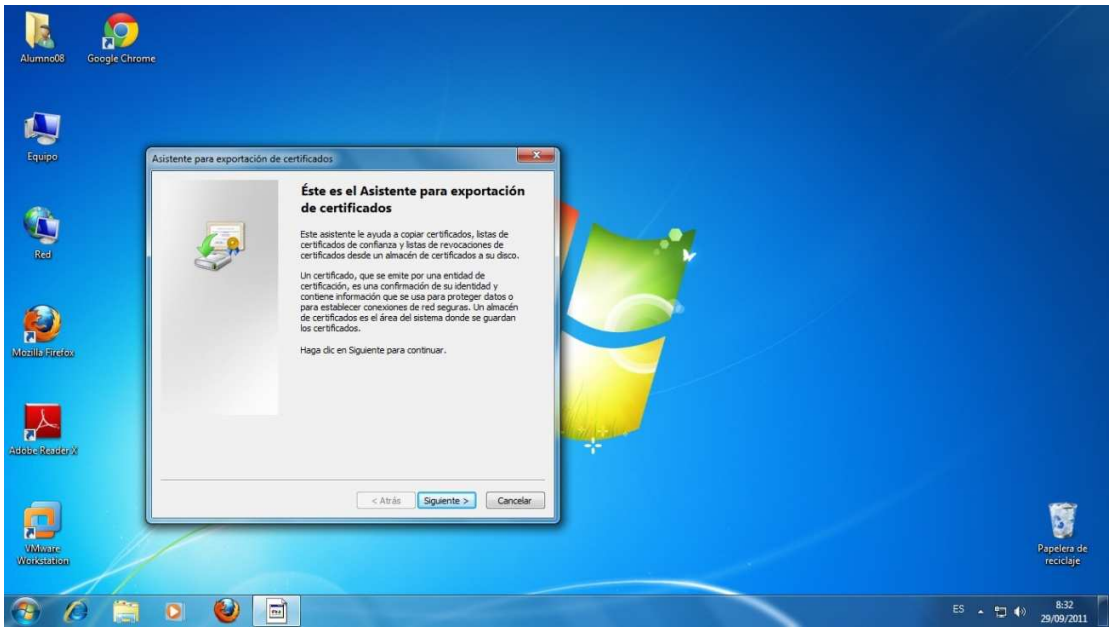
En la pestaña General seleccionamos “Opciones Avanzadas”



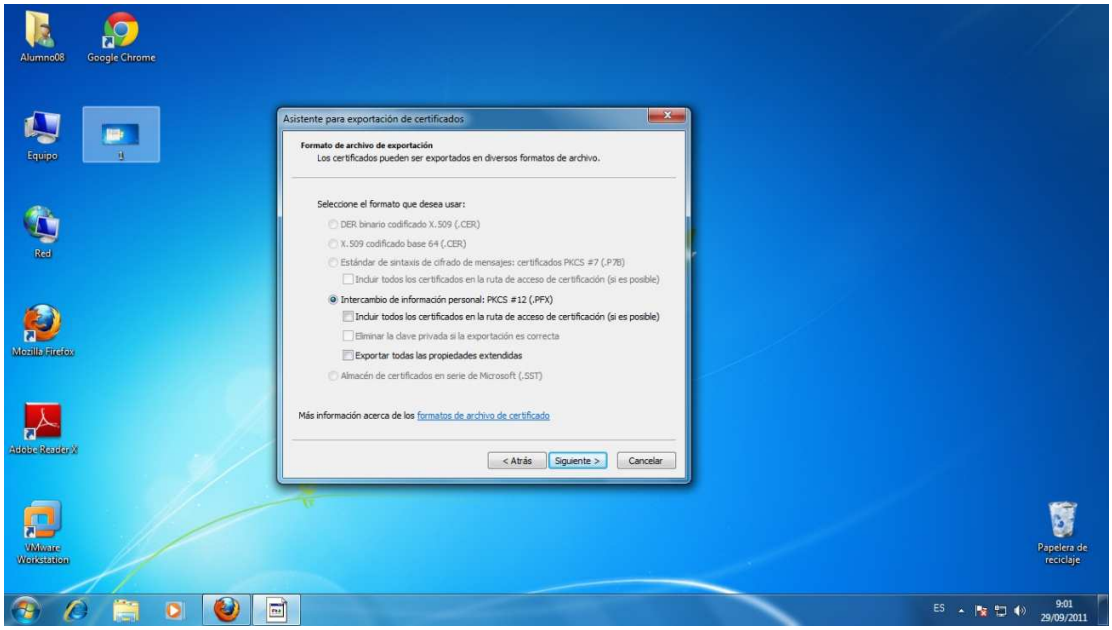
-Seleccionamos el atributo cifrar y Aplicar.

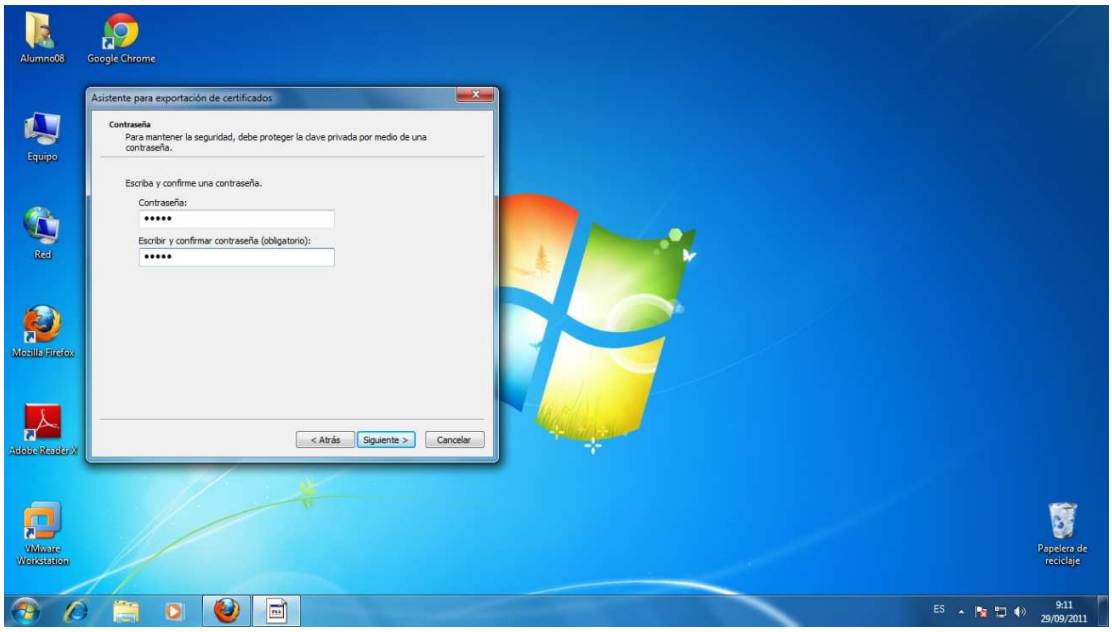


Como se puede ver ahora el contenido de la carpeta “Descargas” estas cifrada y solo el usuario administrador puede acceder a ella.

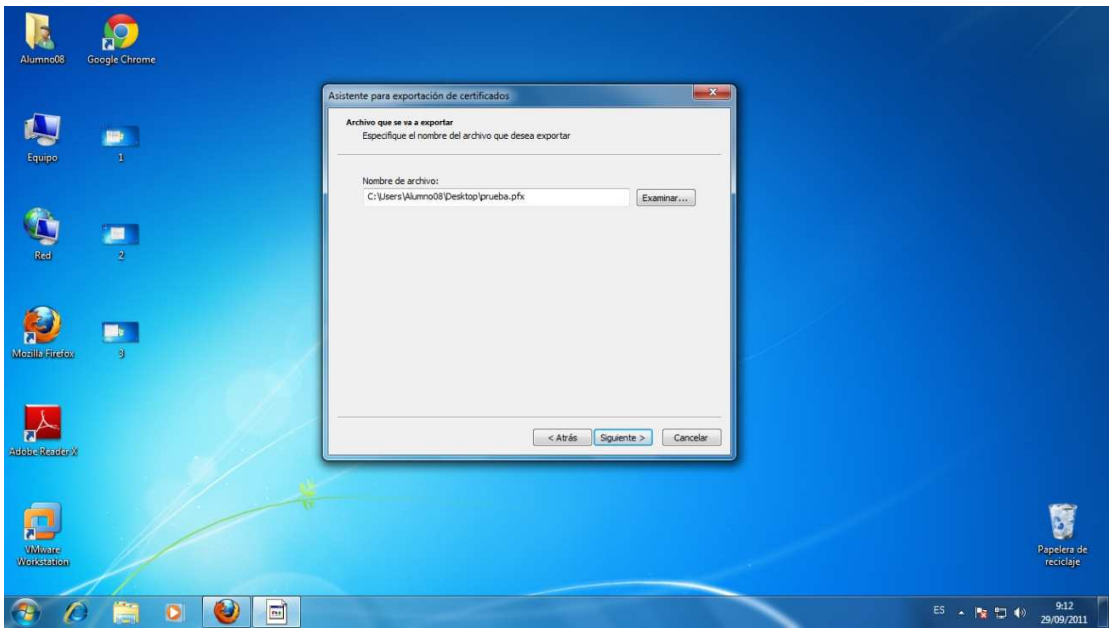


La 1º Vez que realizamos un cifrado, nos soltada un asistente para que podamos crear un certificado para la exportacion de cifrados.



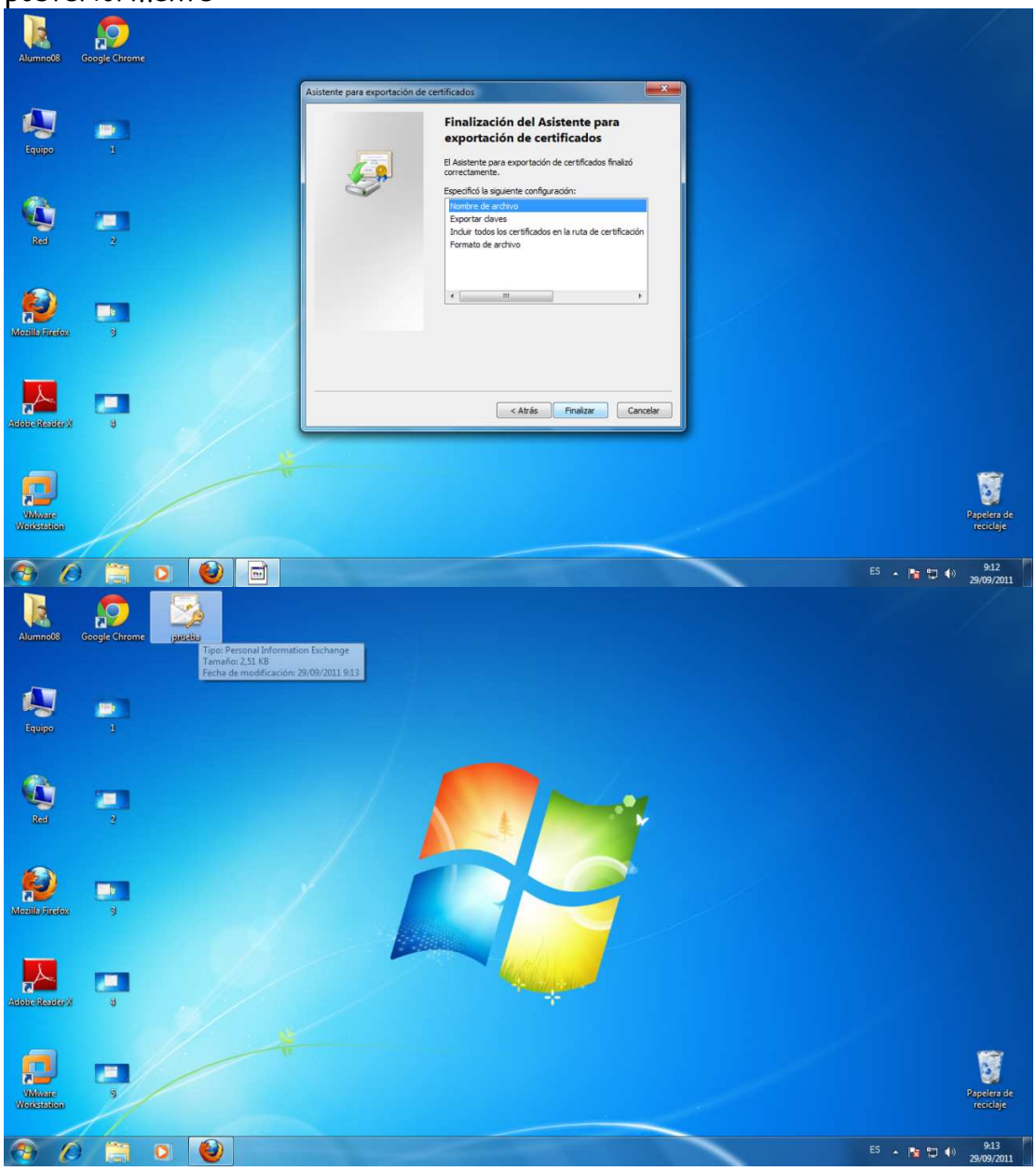


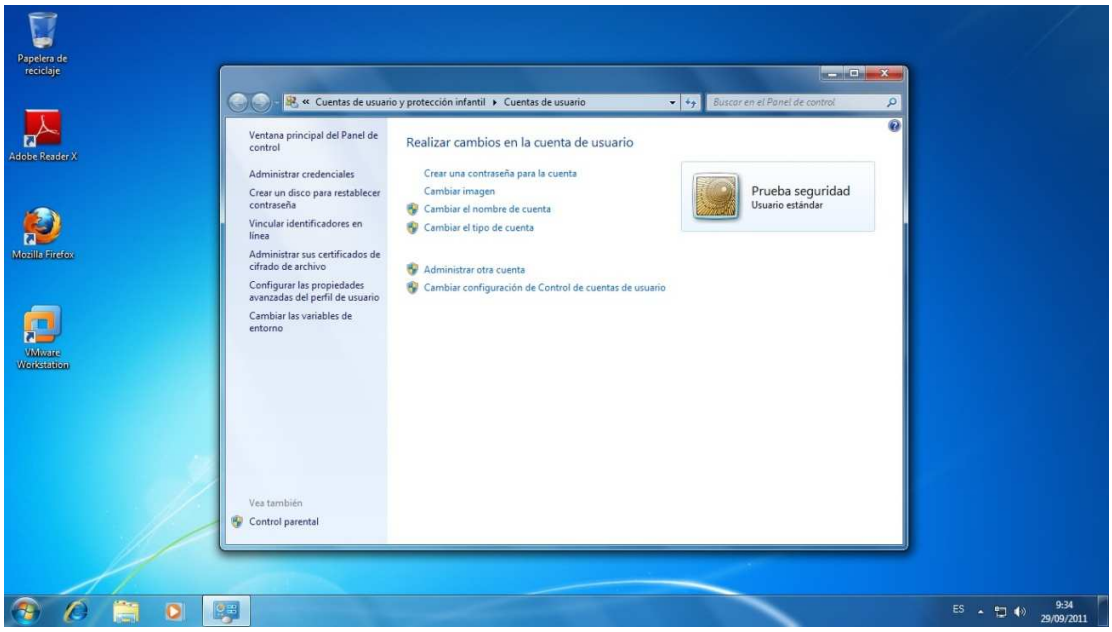
Aquí nos pide una contraseña para el certificado de modo que nadie vea que tipo de cifrado hemos realizado



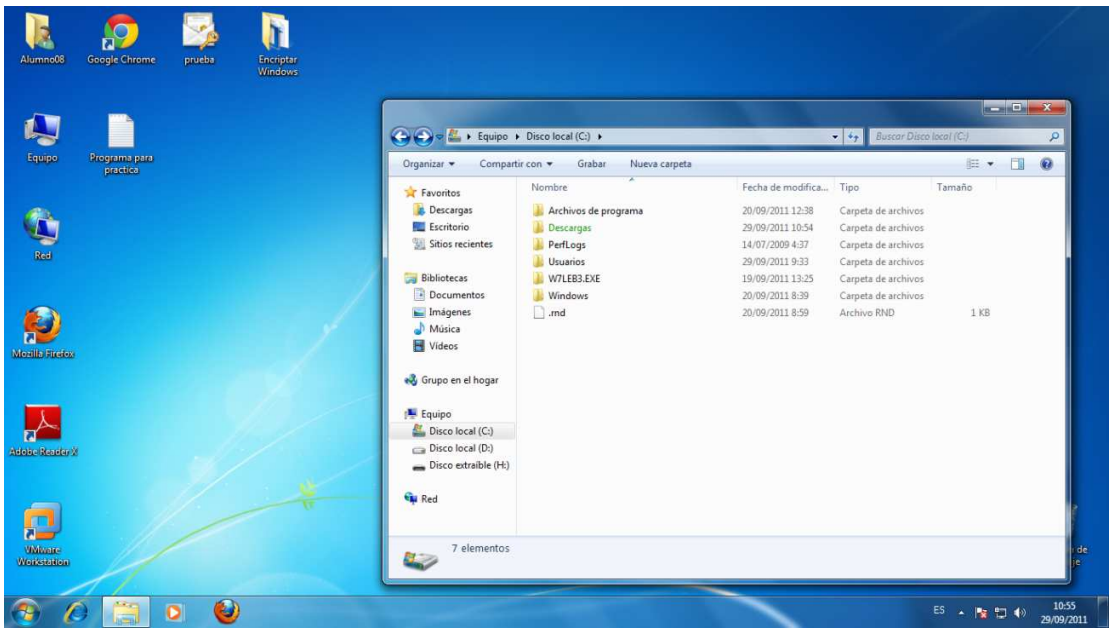
Aquí se guarda el directorio donde quedara guardado el certifcado para poder usarlo

posteriormente



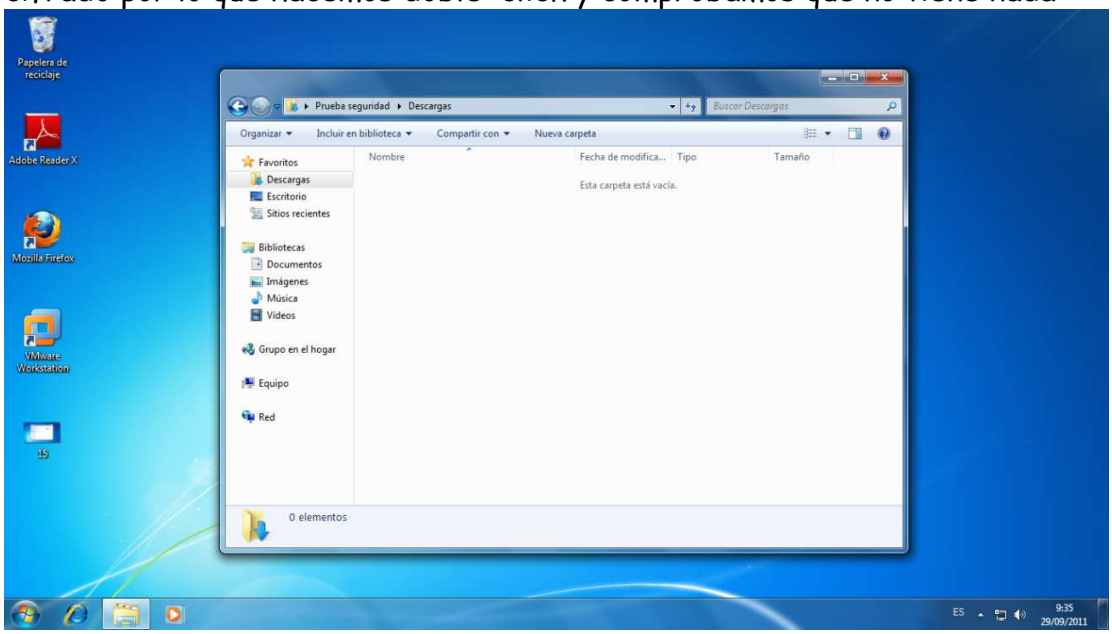


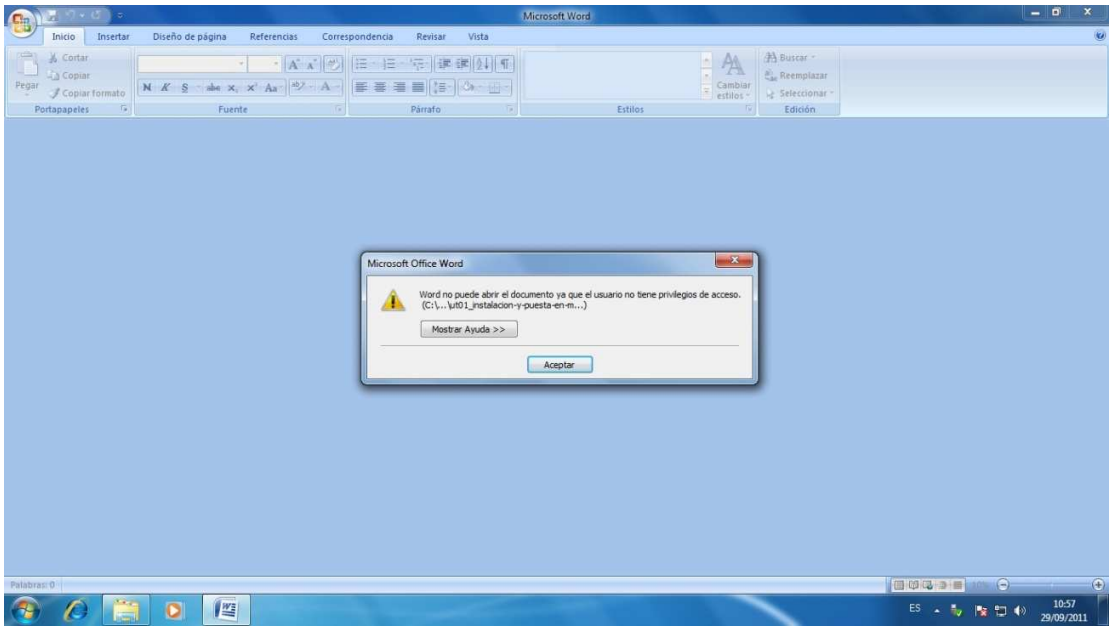
El siguiente paso sera crear un usuario no administrador. En nuestro caso se llamara “Prueba Seguridad”



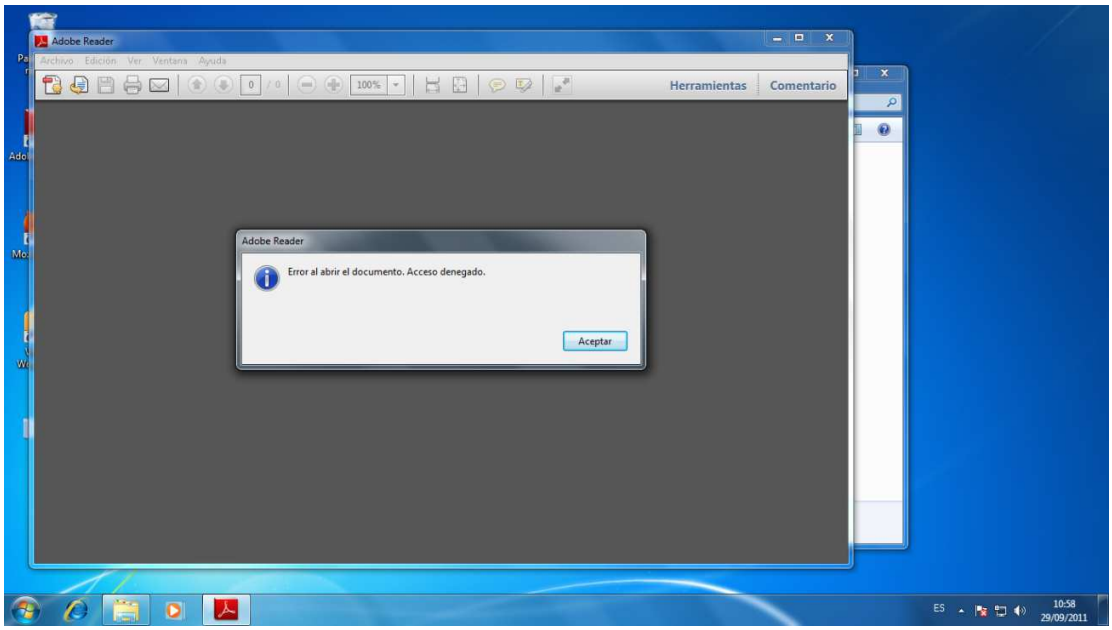
Como se puede ver la carpeta “Descargas ” aparece en verde eso quiere decir que esta

cifrado por lo que hacemos doble click y comprobamos que no tiene nada





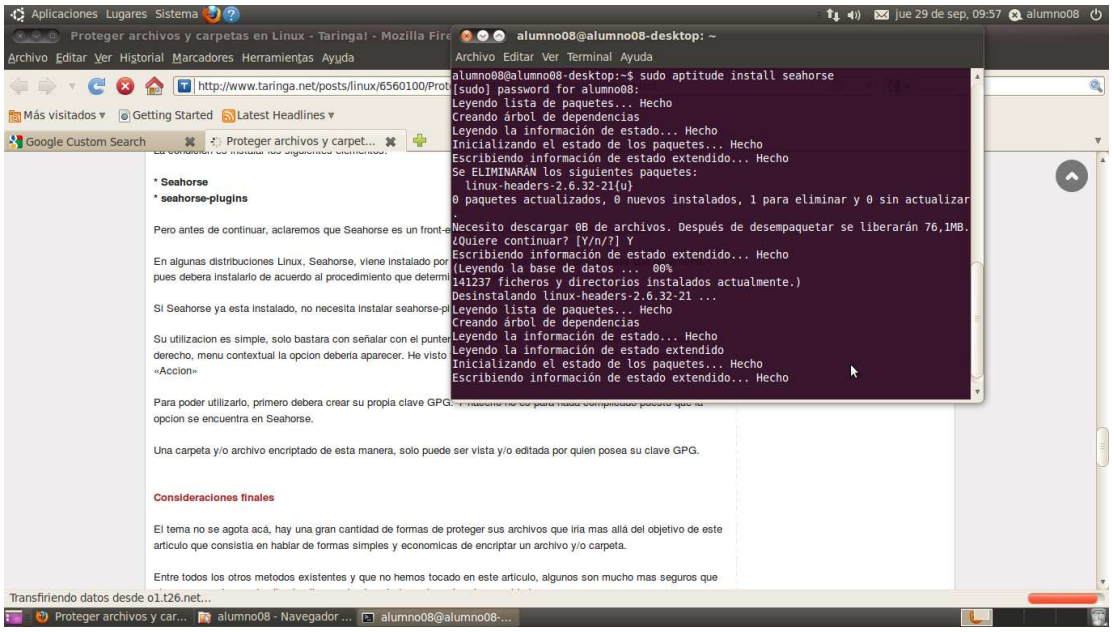
Por otro lado podemos ver ahora un fichero word y un fichero pdf cifrados denegandonos el acceso a su contenido



2.2- Utilizar PGP en Linux.

Encriptar en Ubuntu: SeaHorse

Vamos a instalar el programa SeaHorse para realizar un cifrado en Linux/Unix. Lo 1º que haremos será instalarlo con la siguiente sentencia:



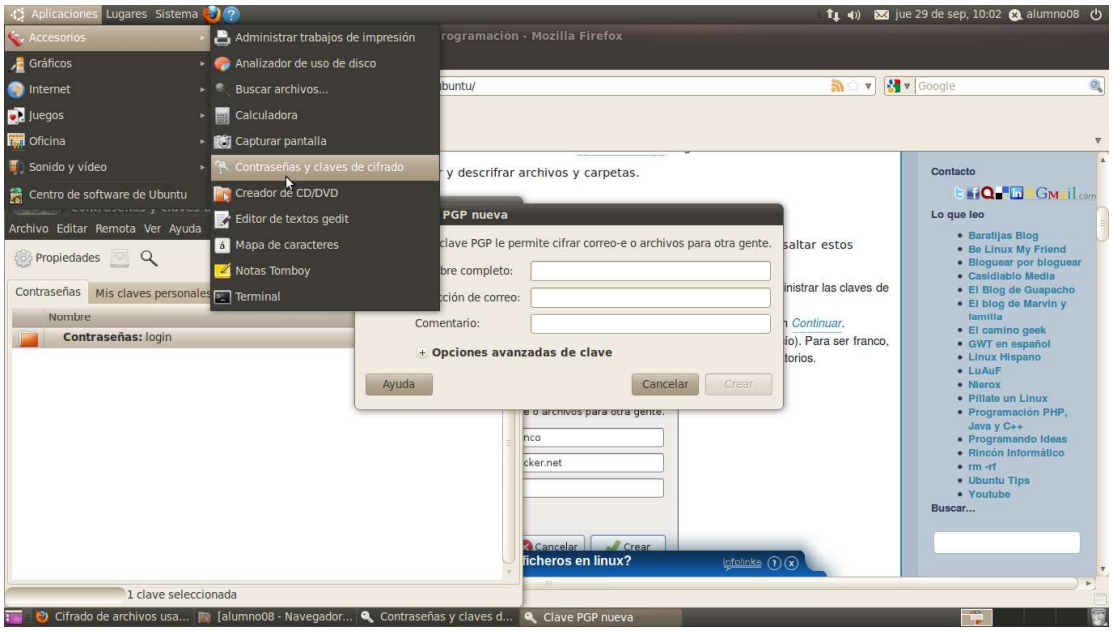
-Sudo aptitude install Seahorse
-Sudo ape-get install Seahorse

Nota: Si entras en la consola Unix como administrador no es necesario utilizar la sentencia “Sudo”.

Crear las claves

Para crear claves con sea Horse seguiremos los siguientes pasos:

1. Haz clic en *Aplicaciones —> Accesorios —> Contraseñas y claves de cifrado* para iniciar la aplicación **Seahorse**, que es usada para administrar las claves de cifrado en Ubuntu.

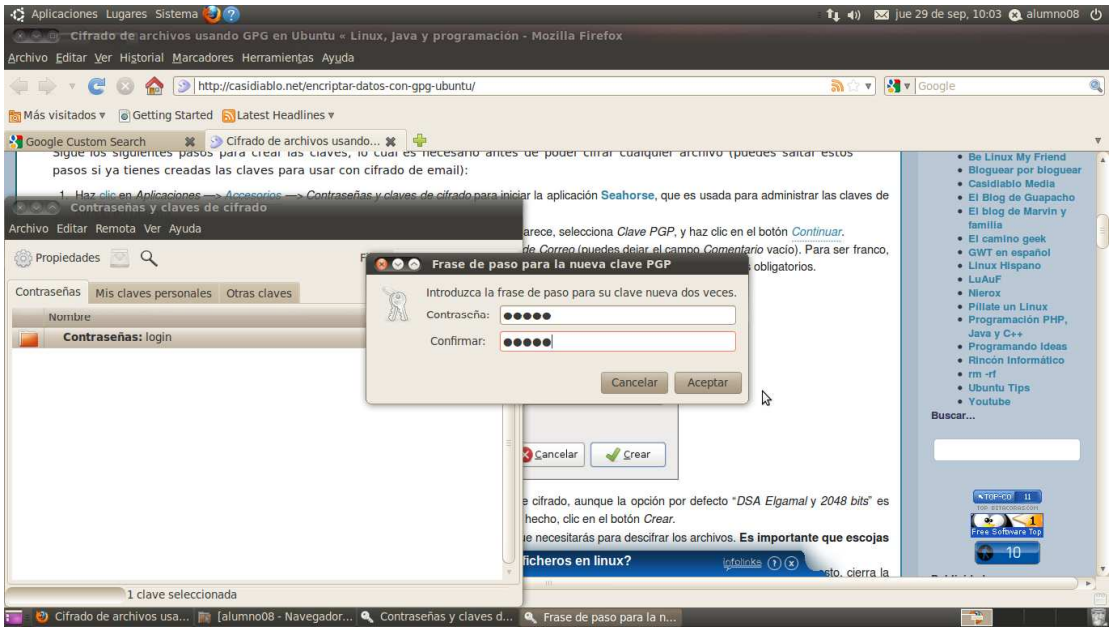


2. En la ventana que aparece, haz clic en el botón *Nuevo*. En el cuadro de diálogo que aparece, selecciona *Clave PGP*, y haz clic en el botón *Continuar*.

3. En el cuadro de diálogo que aparece, llena los campos *Nombre Completo* y *Dirección de Correo* (puedes dejar el campo *Comentario* vacío). Para ser franco, el campo email es solamente usado cuando usamos las claves con propósitos de envío de correo cifrado; sin embargo son campos obligatorios.

4. En el apartado *Opciones avanzados de clave*, puedes seleccionar un tipo diferente de cifrado, aunque la opción por defecto “*DSA Elgamal* y *2048 bits*” es considerada bastante segura a la vez que flexible para todas las necesidades. Una vez hecho, clic en el botón *Crear*.

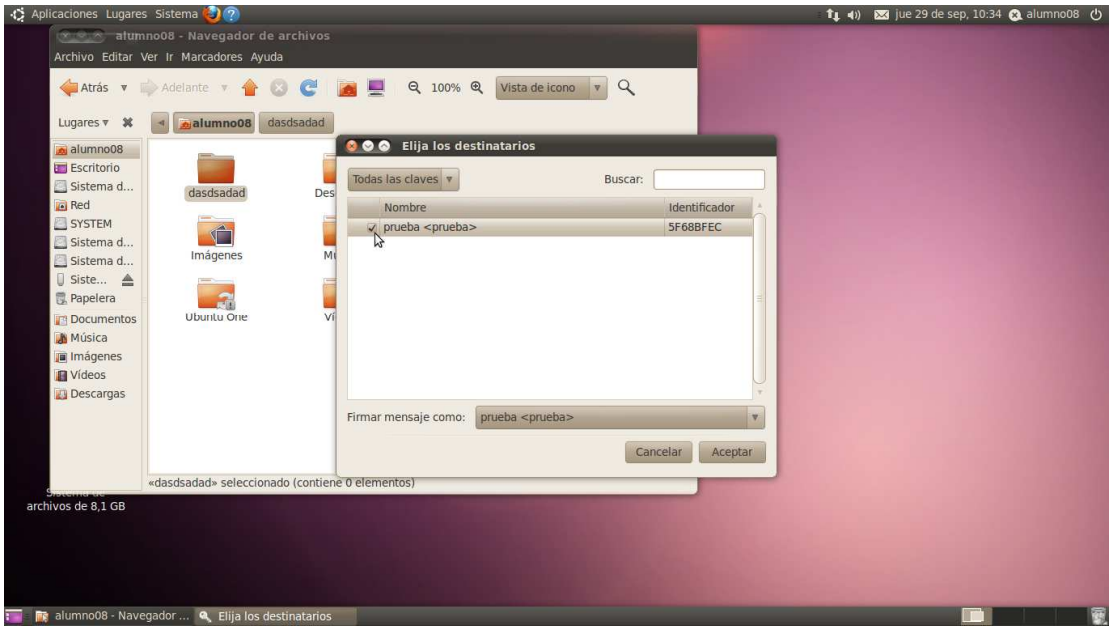
5. Después de esto, te solicitará una contraseña. Esencialmente, esta es la contraseña que necesitarás para descifrar los archivos. **Es importante que escojas una contraseña difícil de adivinar, pero a la vez fácil de recordar**. La contraseña puede incluir letras, números, símbolos, y espacios. En nuestro caso será “inves”



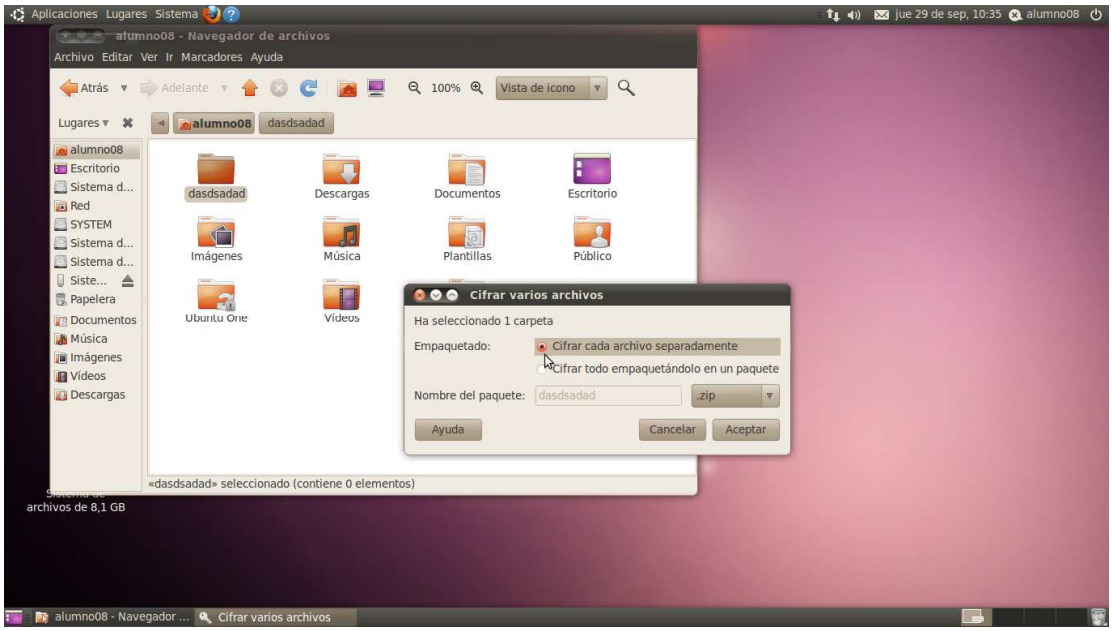
6. Después de esto, la clave será generada. Dependiendo en la velocidad de tu computador, esto puede tomar algunos minutos. Una vez hecho esto, cierra la aplicación *Seahorse*.

Cifrando/Descifrando archivos y carpetas

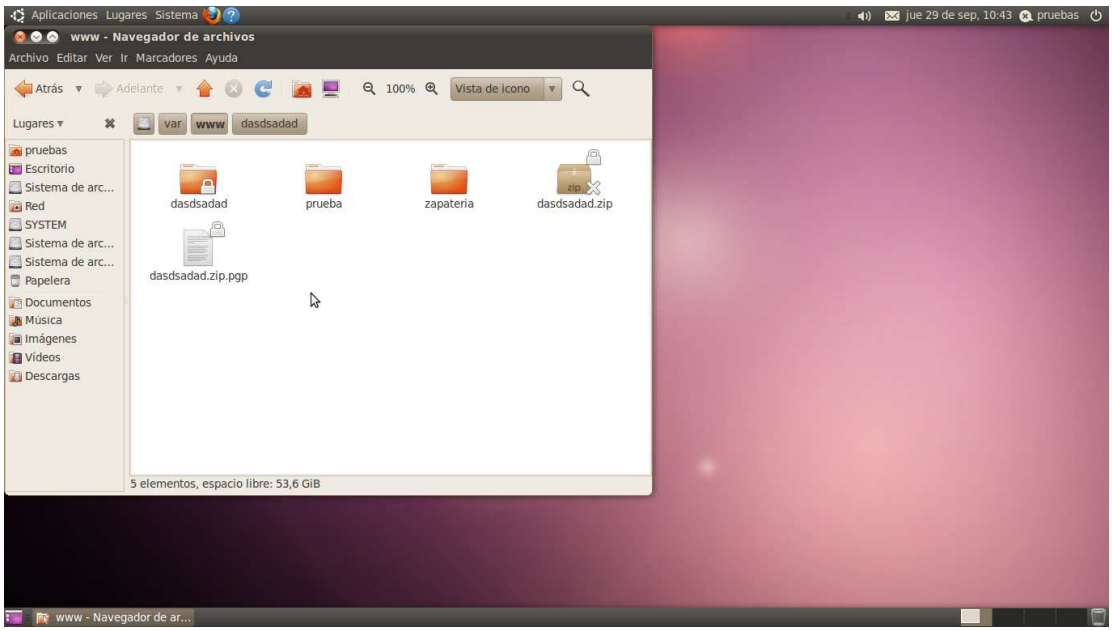
Una vez que el par de claves ha sido generado, cifrar y descifrar archivos es bastante simple. Solo tienes que **seleccionar un archivo, hacer clic derecho y seleccionar *Cifrar***.



Si has seleccionado una carpeta para cifrar, te preguntará si deseas cifrar cada archivo dentro de la carpeta por separado o si deseas que se cree un archivo ZIP que luego será cifrado. **La segunda opción es la mejor en la mayoría de los casos**.

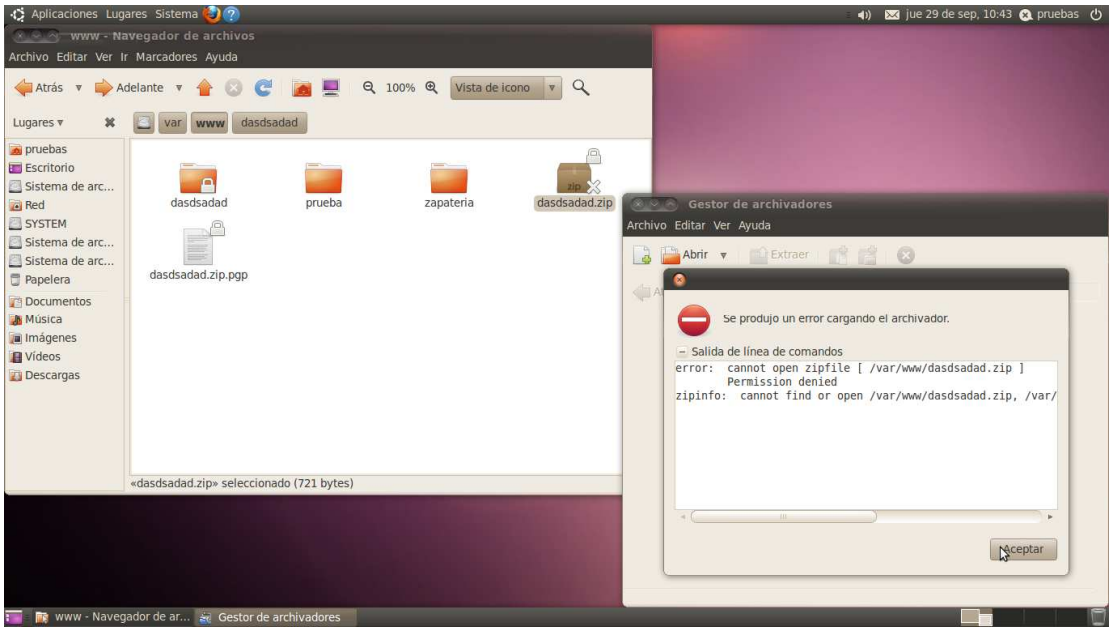


Si estás cifrando un archivo, una vez que el cifrado esté completo, deberías encontrarte con una nueva versión con la extensión *.pgp*. **Puedes/debes entonces borrar el archivo viejo**. Si cifraste una carpeta, deberías encontrar dos nuevos archivos—la versión cifrada con la extensión *.pgp* y un archivo *.zip* con la versión original del folder. Tanto el ZIP como la carpeta original, pueden ser borrados después del cifrado.



Por razones de seguridad, **las versiones no cifradas de los archivos deben ser eliminados permanentemente**, en vez de simplemente enviarlos a la papelera de reciclaje. Pero antes asegúrate de probar descifrando el archivo cifrado, para ver que todo va bien.

Para ello, debes hacer doble clic en el archivo *.pgp*, y entonces digitar la contraseña cuando te la pida. El archivo original reaparecerá entonces. En caso de ser una carpeta, el archivo *.zip* aparecerá, y deberás entonces extraer el contenido del mismo.



Guía: Como Utilizar El “System File Checker” Para Reparar Tu PC Que No Arranca

Un fichero llamado “System File Checker” (sfc.exe) es una utilidad cual se activa via una linea de comando utilizando el Command Prompt en Windows. Esta te ayuda a reparar archivos corruptos en el sistema operativo que hacen que el mismo mal funcione. Si tu maquina no arranca por completo, este comando lo puedes utilizar desde el disco de instalación.

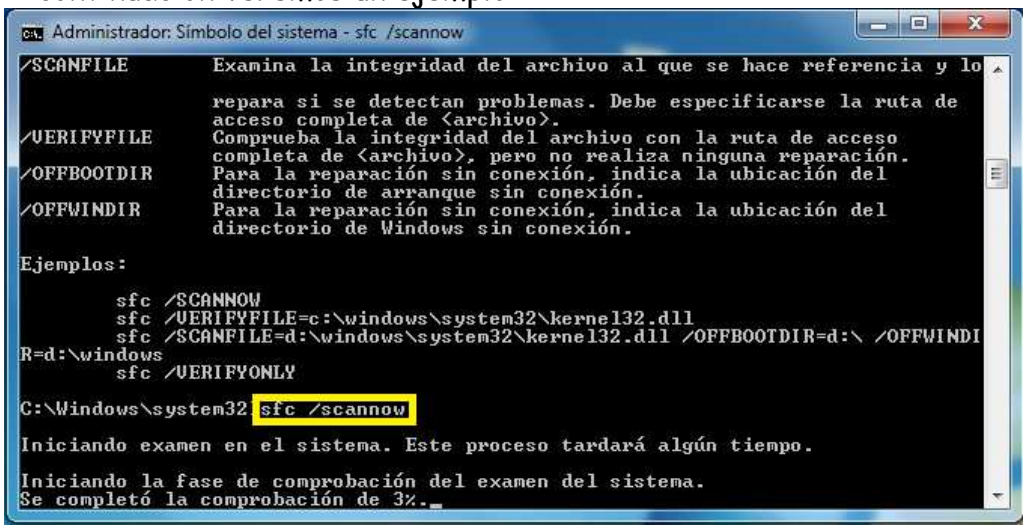
Normalmente tu abres el Command Prompt como administrador y escribes sfc /scannow para escanear los archivos del sistema y el procede a reparar los que estén rotos o simplemente termina si no encuentra nada, pero cuando lo haces desde un CD/DVD de instalación no es así de sencillo. De esta forma tendrás que arrancar tu maquina desde el CD/DVD de instalación y escoger la opción de “Repair Your Computer” luego escoges el disco donde esta el sistema operativo (Normalmente es el C), abres el Command Prompt y escribes el siguiente comando:

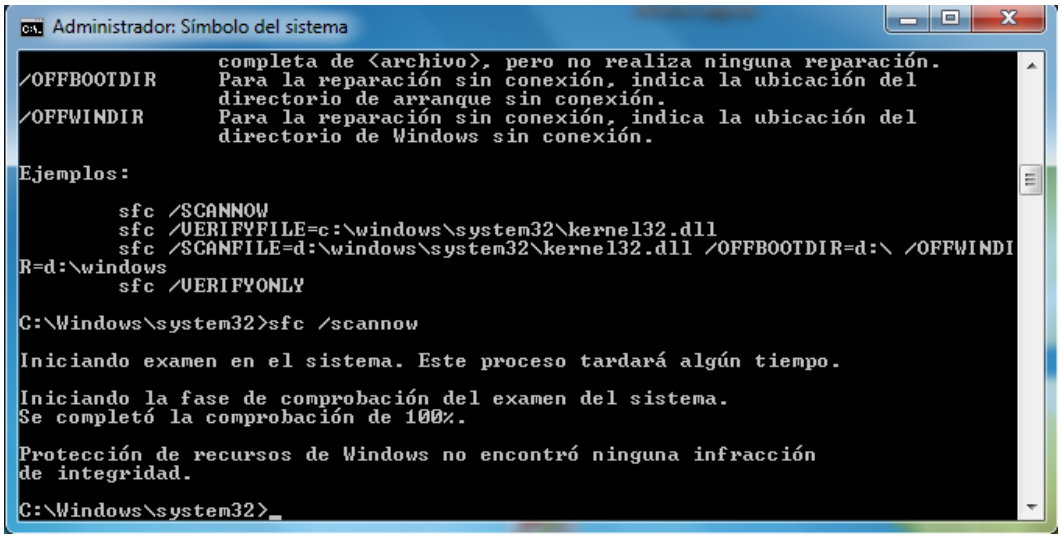
-sfc /scannow /offbootdir=d: /offwindir=d:windows

El comando de arriba muestra la letra d: como disco de instalación del sistema pero puede ser que tu letra sea diferente así que debes de prestarle atención a esa parte en particular.

De todos modos esto te puede salvar la vida y evitar que tengas que reformatear la maquina en caso de que falle el arranque. En Windows Vista y Windows 7 puedes hacer esto también pero estos sistemas operativos cuentan ya con un método de reparación automática que detecta los errores y trata de corregirlos por si.

A continuación veremos un ejemplo:

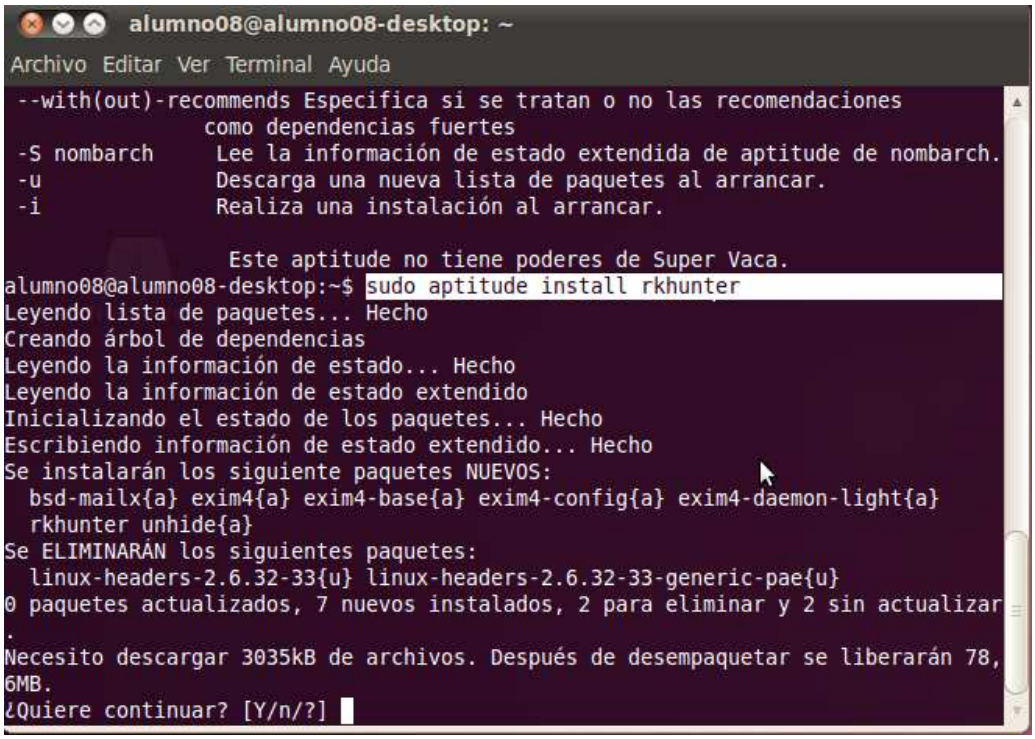




Aquí podemos comprobar que tras usar el “System File Checker” no ha habido ningún problema con los ficheros del sistema operativo. Si se hubiera dado el caso, dicho programa intentaría actualizarlo

INTEGRIDAD UBUNTU: RKHUNTER

Rkhunter (o **Rootkit Hunter**) es una herramienta de Unix que detecta los rootkits, los backdoors y los exploit locales, buscando los directorios por defecto (de rootkits), los permisos incorrectos, los archivos ocultos, las cadenas sospechosas en los módulos del kernel, y las pruebas especiales para Linux y FreeBSD. En general dicho programa vale para chequear con seguridad los ficheros del sistema y comprobar si alguno está dañado o defectuoso. Esta aplicación esta para todos los sistemas operativos, pero en esta práctica la instalaremos y usaremos en Ubuntu.



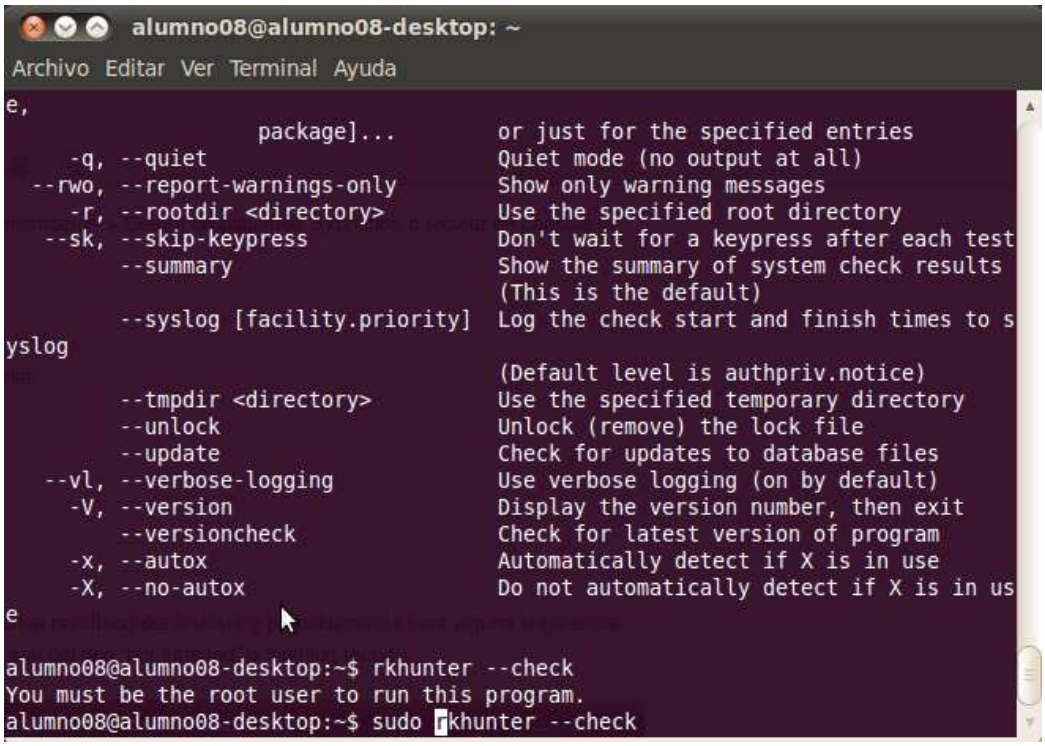
-Lo primero de todo será instalarla mediante la siguiente sentencia:

-Sudo aptitude install rkhunter

-Sudo apg-get install rkhunter

Nota: Si entras a la consola como administrador, no es necesario utilizar la sentencia “sudo”

Una vez que lo hemos instalado lo haremos funcionar de la siguiente forma:



-Sudo rkhunter --check
-Sudo rkhunter –checkall

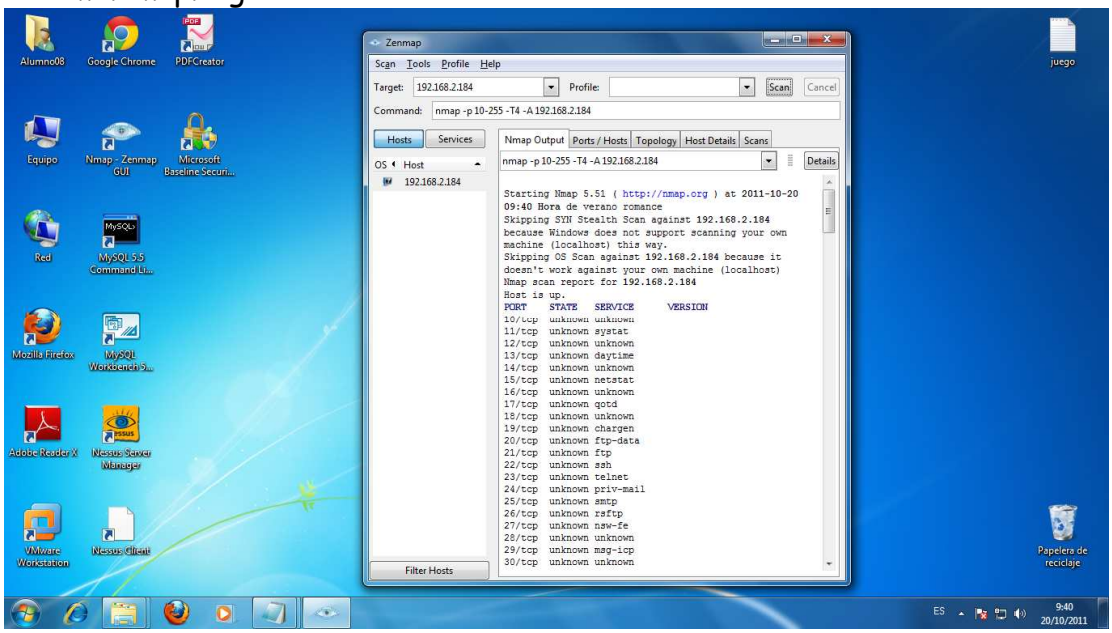
Con ambas sentencias, empezara a checkear las particiones del disco duro para comprobar si ahí algún fichero corrompido. Se diferencian que la 1º solo lo hace en la partición que esta almacenara el SO y la 2º lo hace en todos los volúmenes conectados.

4. Disponibilidad:

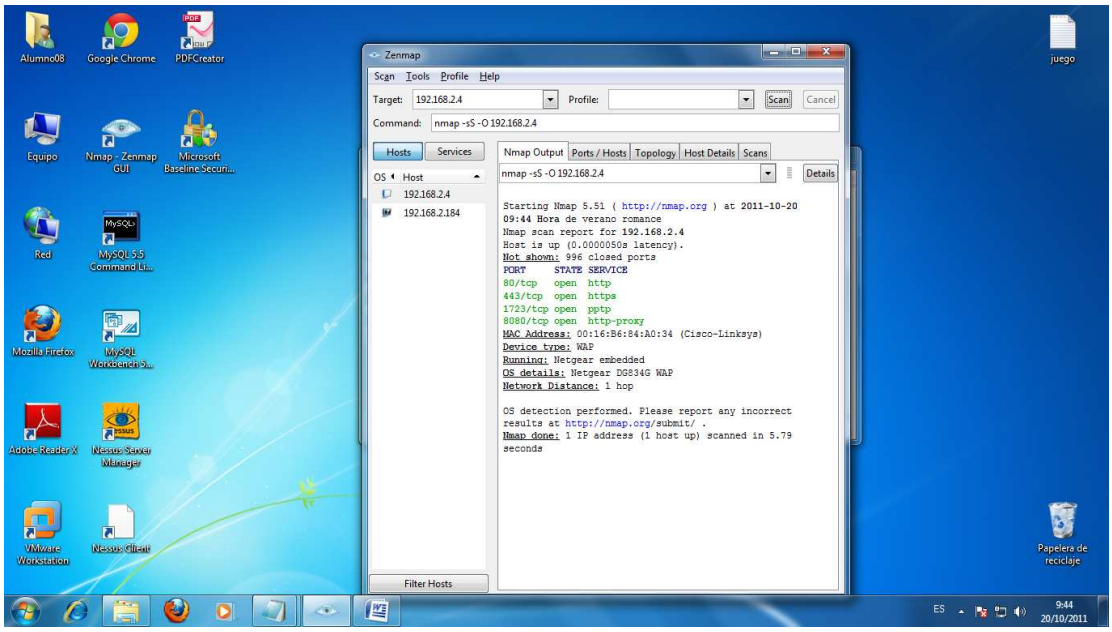
4.1.-Utilizar NMAP, ZNMAP o ZENMAP (www.nmap.org)

nmap -p 10-255 -T4 -A -v scanme.nmap.org

muestra todos los puertos abiertos de la pagina web scanme.nmap.org

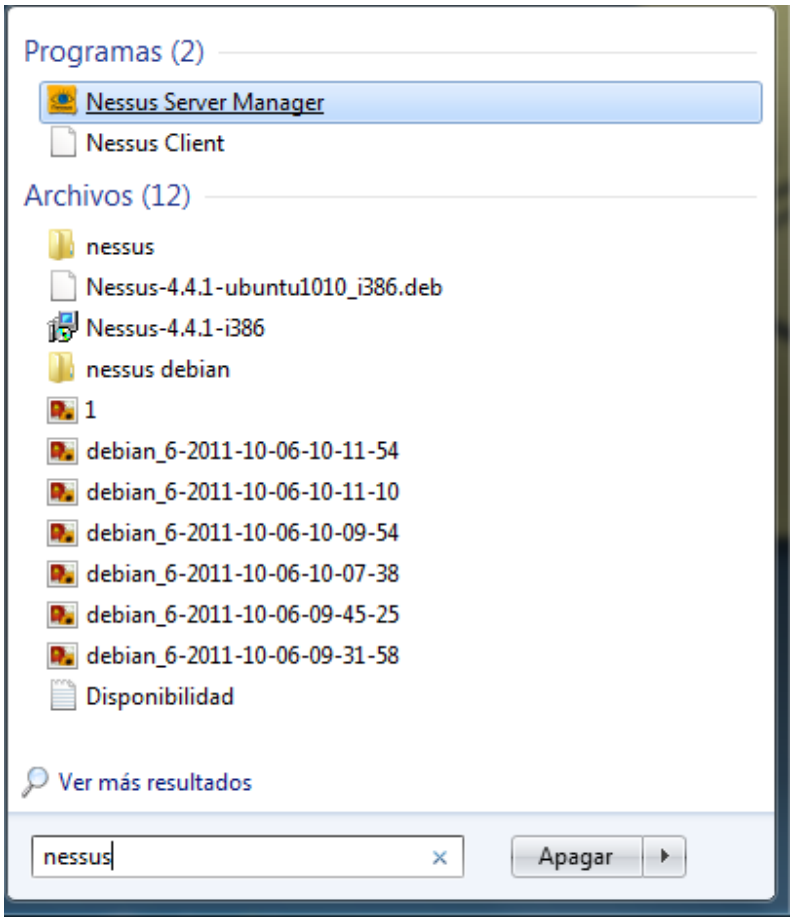


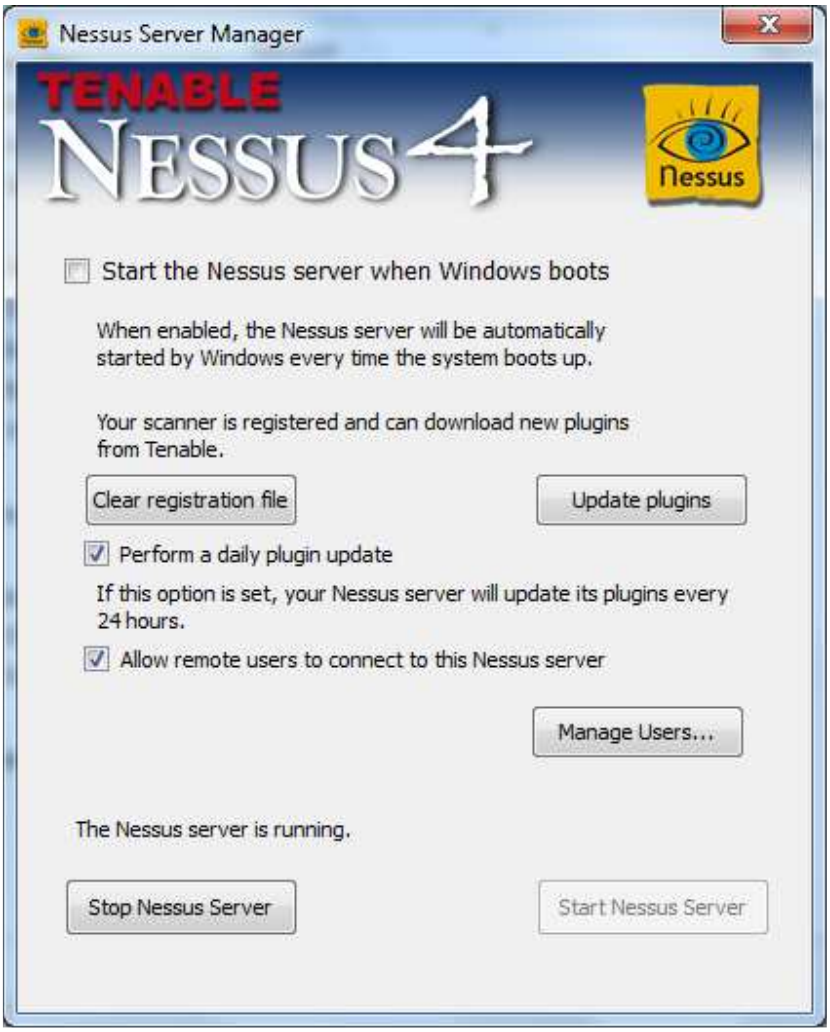
nmap -sS -O 192.168.2.4



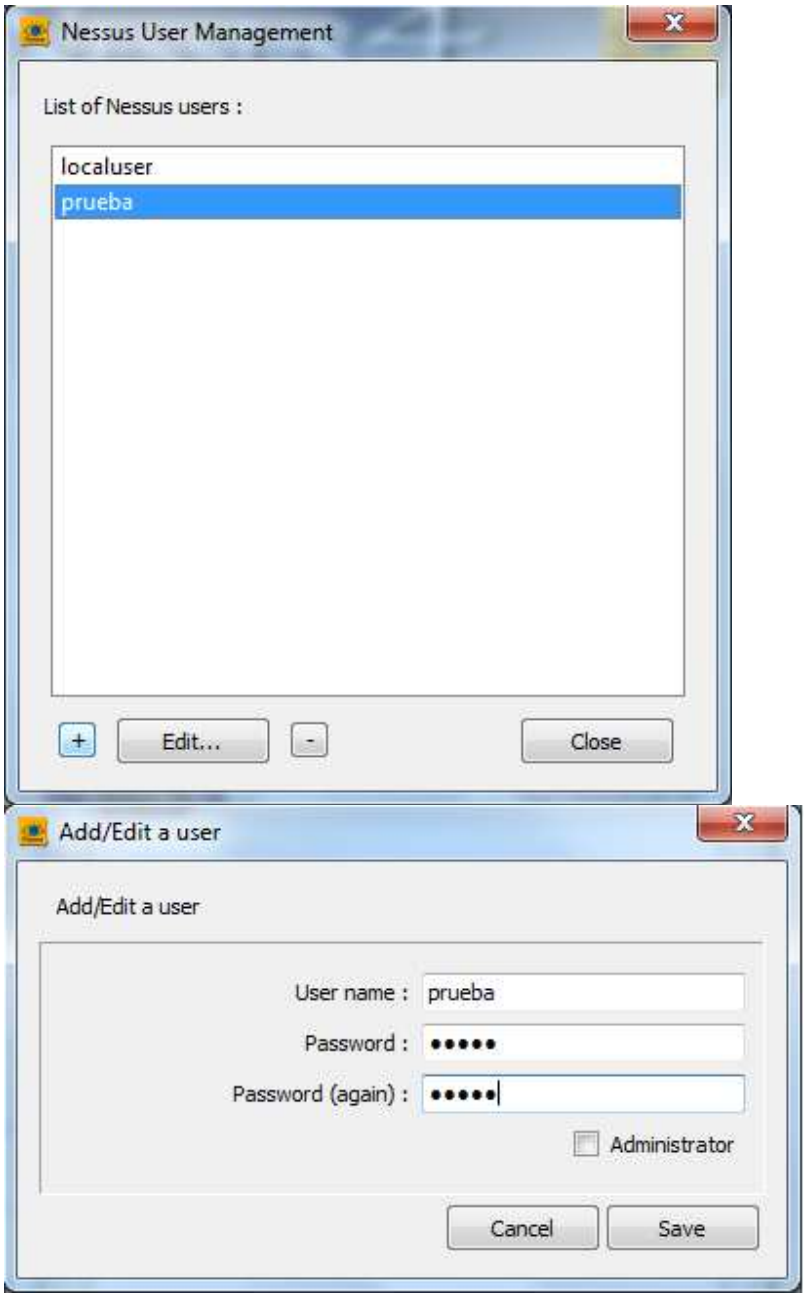
4.2-Utilizar NESSUS (www.nessus.org)

Este programa está dividido en 2 partes: la manager y el cliente. Primero debemos ejecutar el servidor para poder utilizar el cliente

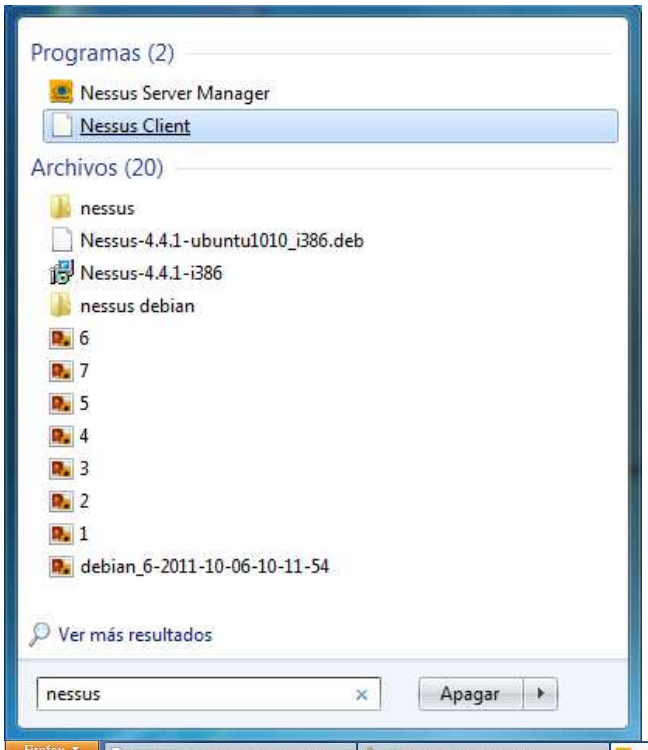

Programas (2)
Nessus Server Manager
Nessus Client
Archivos (12)
nessus
Nessus-4.4.1-ubuntu1010_i386.deb
Nessus-4.4.1-i386
nessus debian
1
debian_6-2011-10-06-10-11-54
debian_6-2011-10-06-10-11-10
debian_6-2011-10-06-10-09-54
debian_6-2011-10-06-10-07-38
debian_6-2011-10-06-09-45-25
debian_6-2011-10-06-09-31-58
Disponibilidad
Ver más resultados
nessus
Apagar

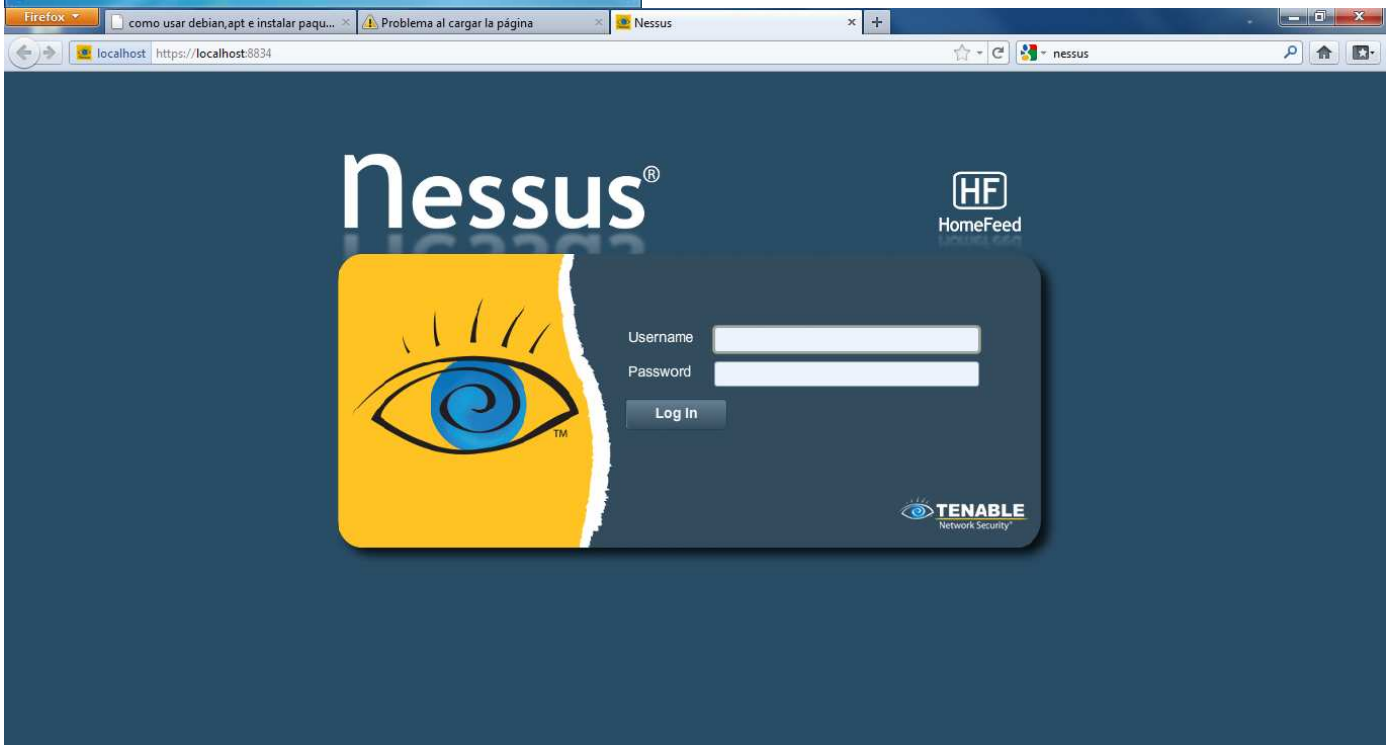


Lo primero que haremos será abrir la opción “**Manage Users**” y crear un usuario prueba para accede al sistema

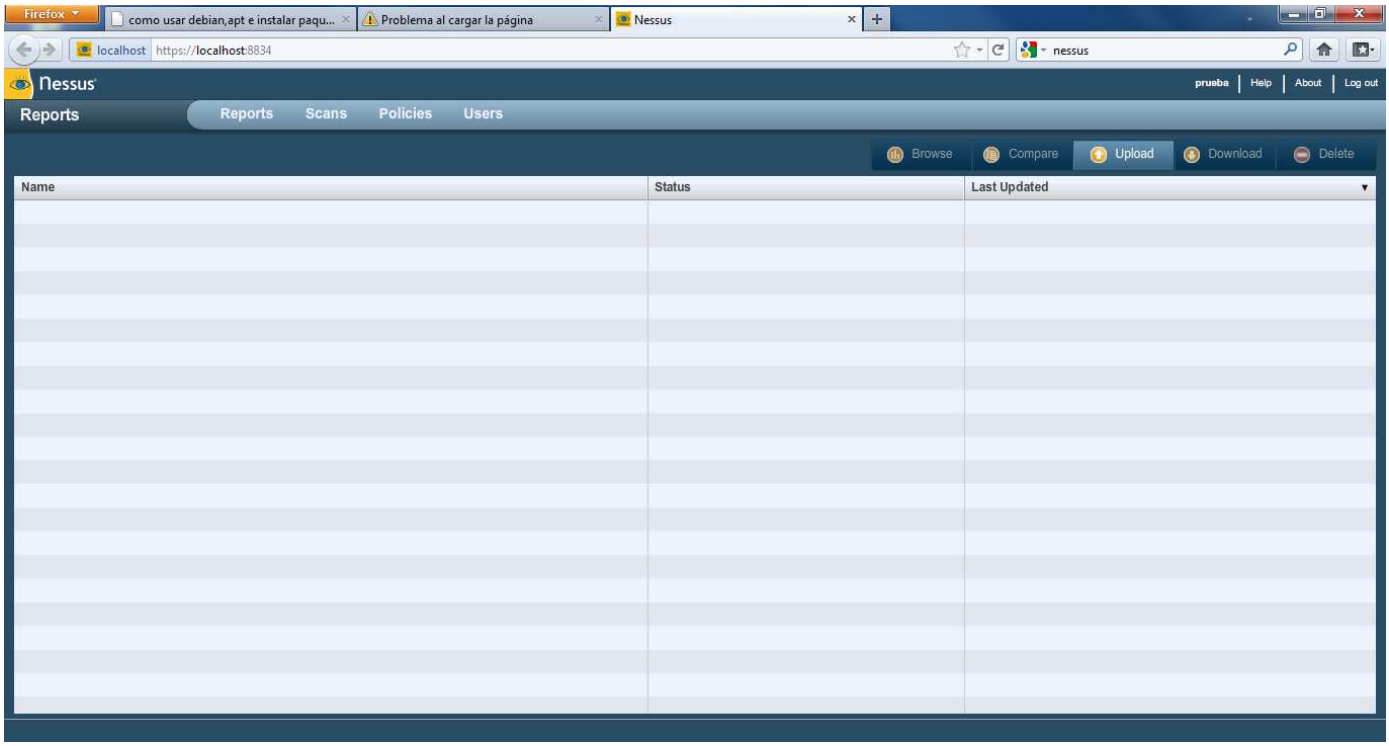


Después ejecutaremos el programa cliente que ejecutara el puerto 8834 un cliente del nesus. Ingresaremos con la cuenta prueba


Programas (2)
Nessus Server Manager
Nessus Client
Archivos (20)
nessus
Nessus-4.4.1-ubuntu1010_i386.deb
Nessus-4.4.1-i386
nessus debian
6
7
5
4
3
2
1
debian_6-2011-10-06-10-11-54
Ver más resultados
nessus
Apagar


Firefox
como usar debian,apt e instalar paqu...
Problema al cargar la página
Nessus
localhost
https://localhost:8834
nessus
Nessus®
HF
HomeFeed
Username
Password
Log In
TENABLE
Network Security

Aquí vemos el interfaz del programa una vez ejecutado correctamente tanto el cliente como el servidor

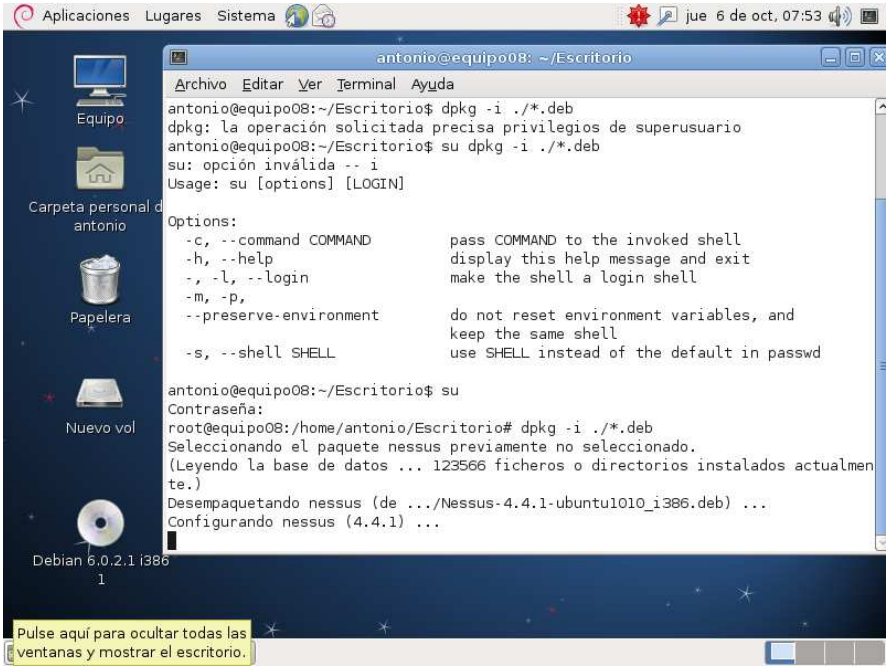


NESUS EN DEBIAN

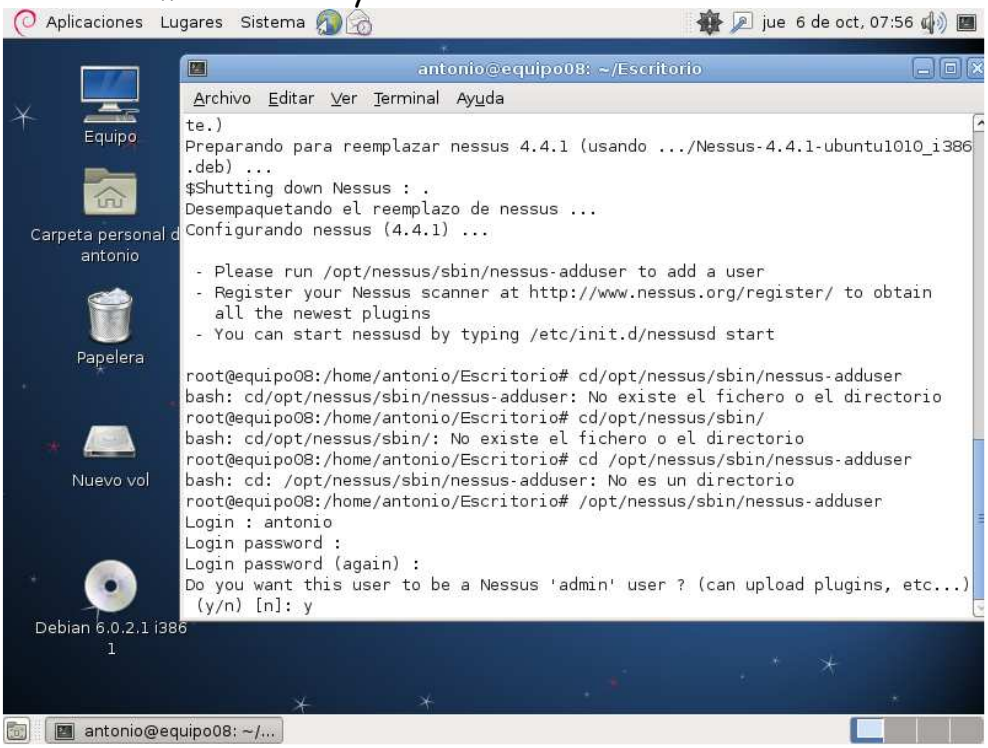
Ahora vamos a realizar la instalación de Nessus en un SO UNIX/LINUX, en este caso debian.

En primer lugar lo que haremos sera actualizar los repositorios con la sentencia:

-su dpkg –i ./*.deb

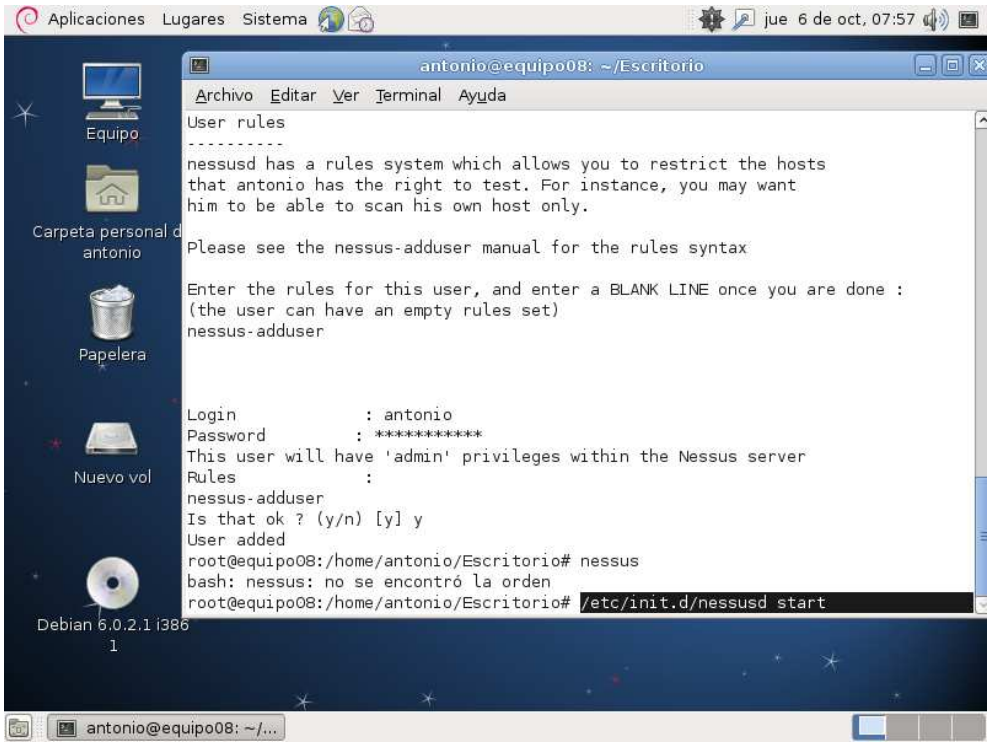


Después nos pedirá que creemos un usuario y que si quiere sea administrador. En nuestro caso se llamara Antonio y lo será

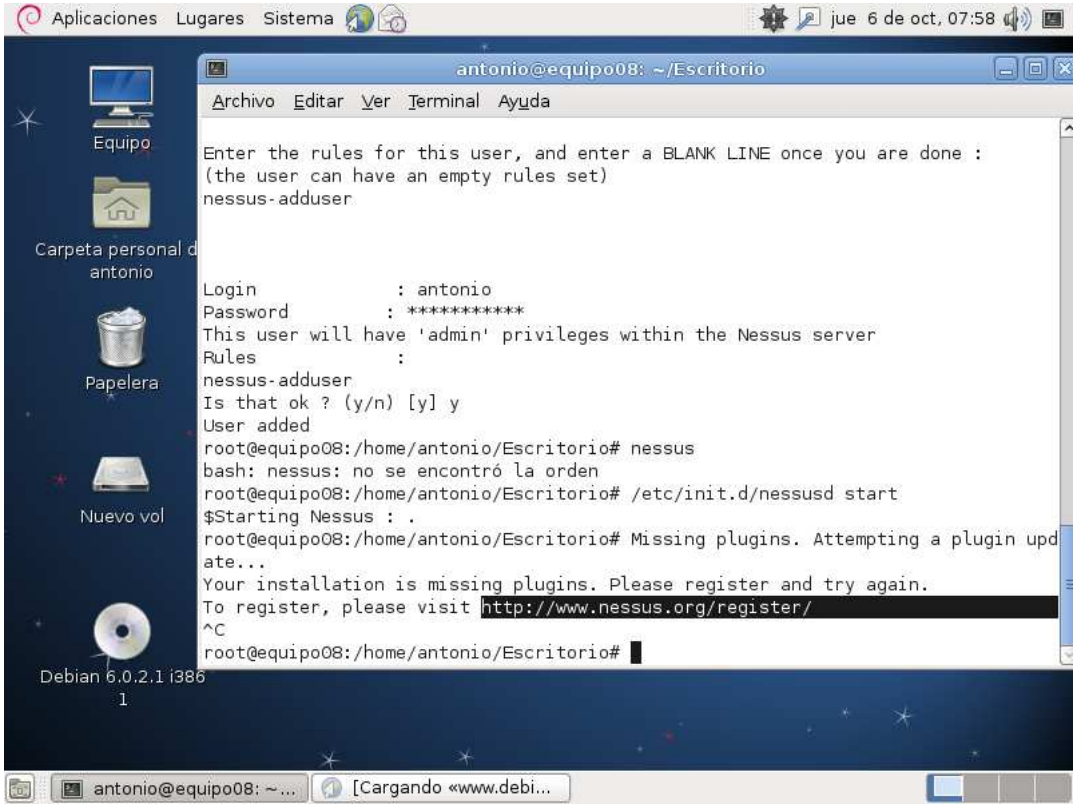


Nessus esta sin ejecutar por lo que lo haremos hacienda la siguiente sentencia:

-/etc/init.d/nessusd start

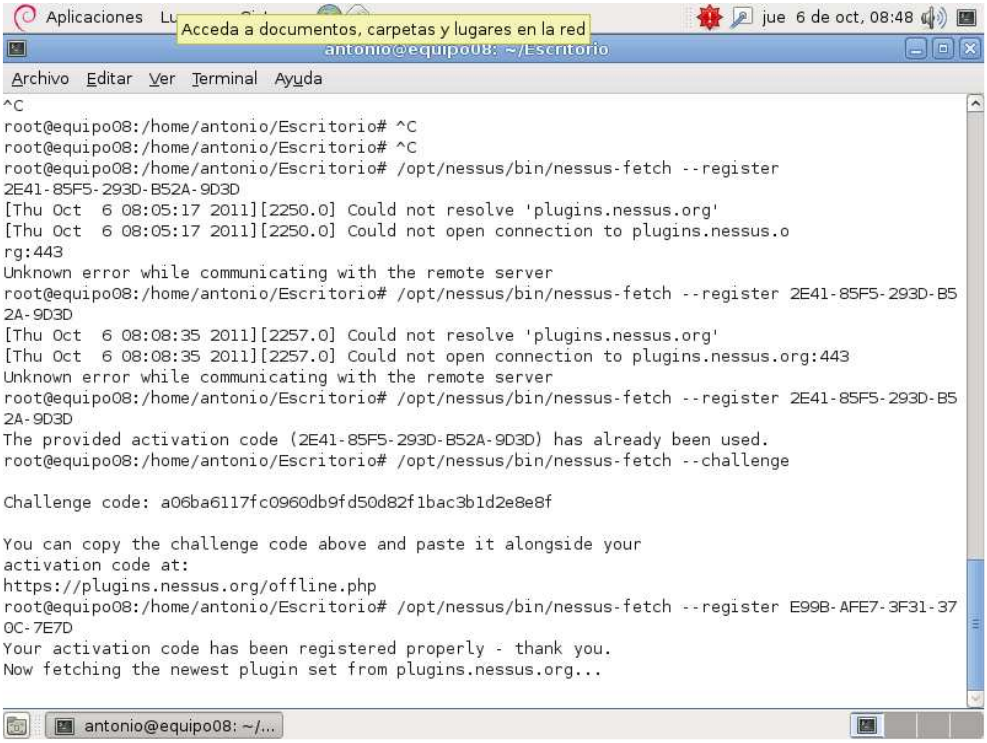


Ahora aparecera un mensaje que nos muestra que no tenemos instalado los plugins del programa. Por lo que debemos de bajarlo de la página http://www.nessus.org/register



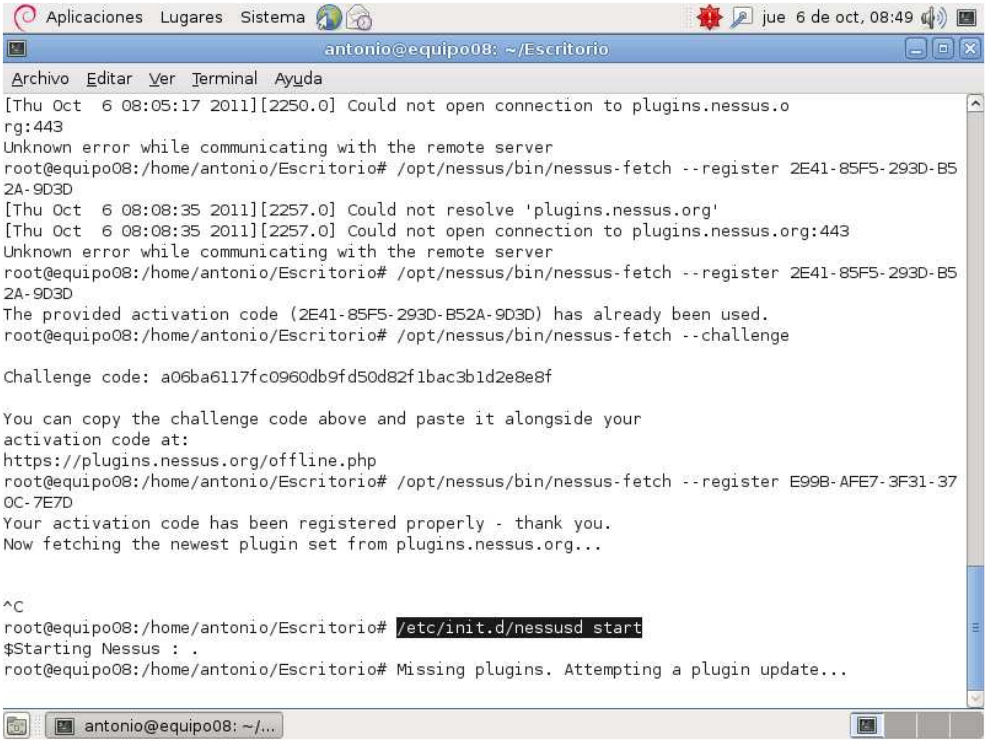
Cuando lo hagamos nos dara un codigo que debemos de ponerlo con la siguiente sentencia:

-opt/nessus/bin/nessus-fetch –register codigo!!



Después de bajar los plugins iniciaremos el programa con:

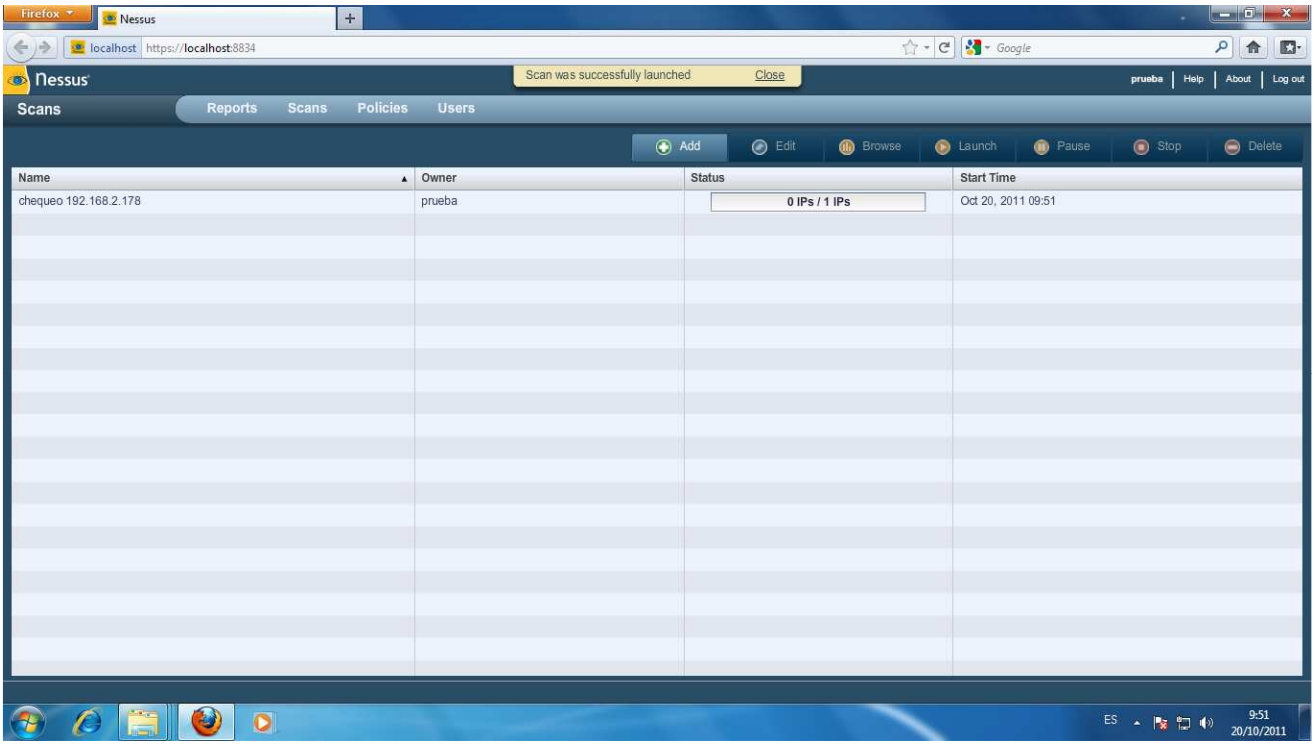
/etc/init.d/nessusd start



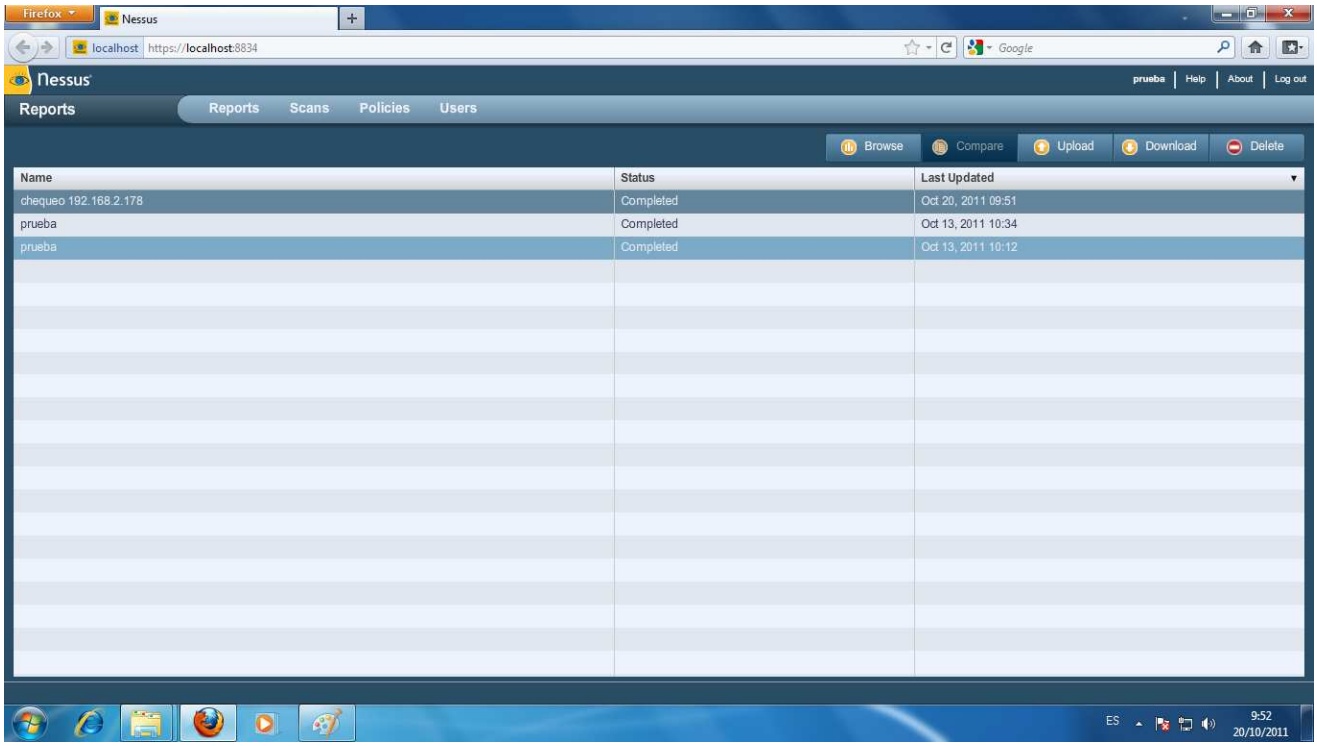
Despues de eso solo tenemos que poner que esperar que lance el menú grafico de Nessus server.
EJEMPLOS!!!

Ahora veremos unos ejemplos:
-Vamos a realizar un chequeo de puertos a varios host para comprobar los niveles de seguridad

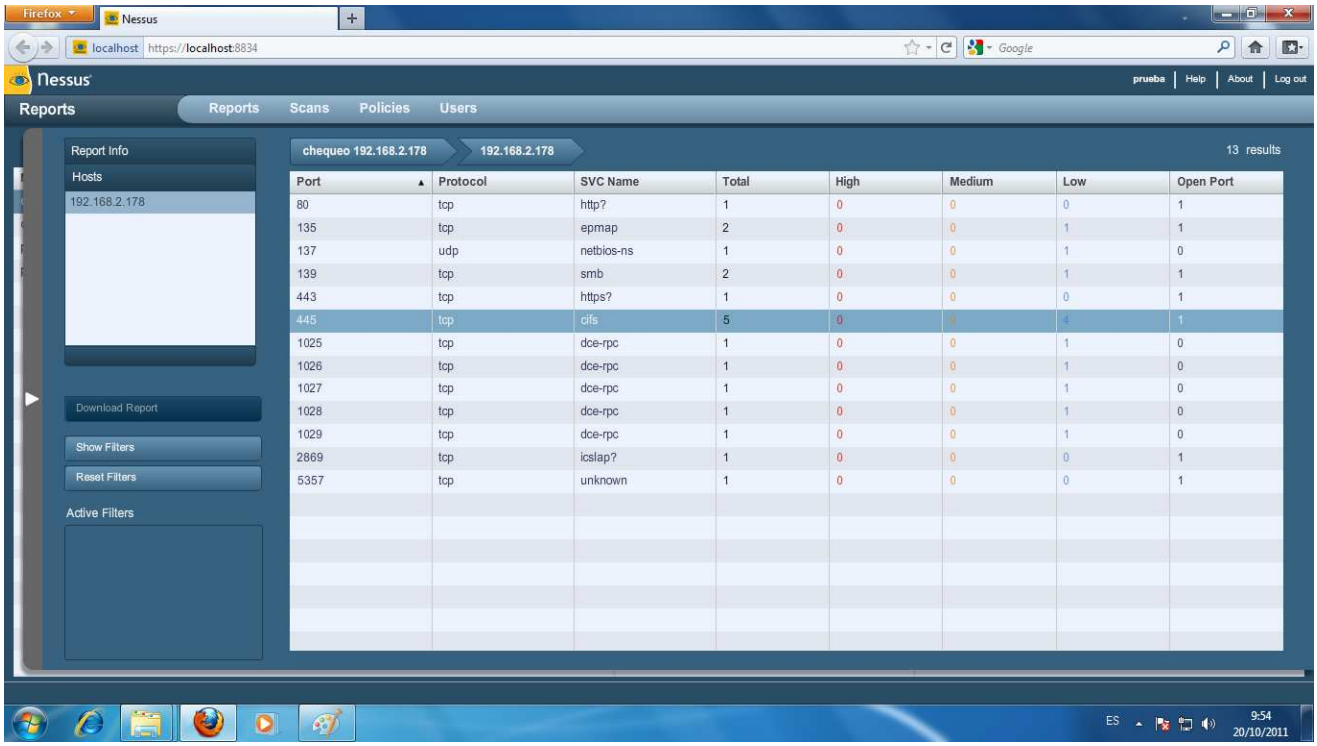
Para ello nos vamos a la pestaña “SCANS” y le damos a “ADD”
Una vez dentro le daremos a tipo de SCAN a “Internal SCAN”

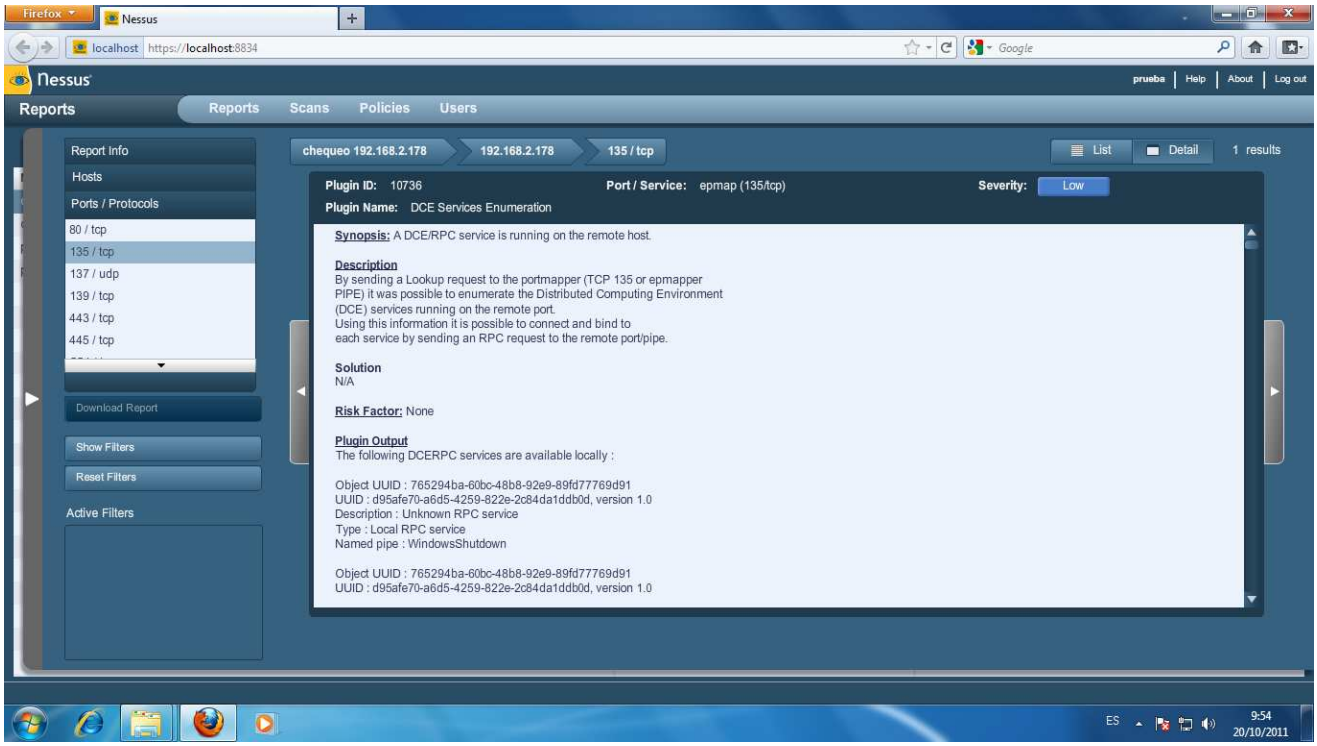


Una vez que se haya terminado, podemos comprobar en la seccion de reports los scans



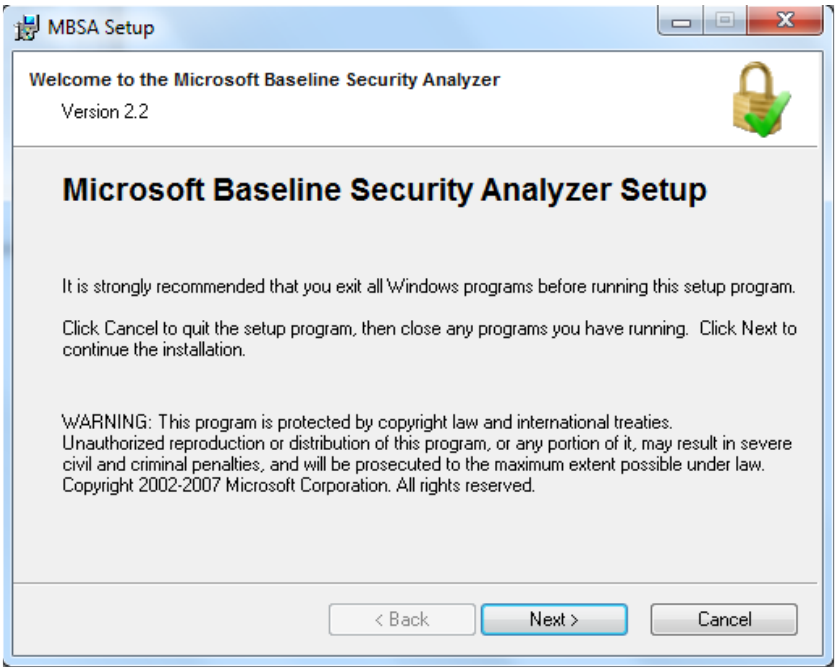
Aquí se puede comprobar que puertos de nuestro host tienen un nivel mas o menos seguro y un detallado informe de cada uno de ellos


Firefox
Nessus
localhost https://localhost:8834
Google
Nessus
prueba | Help | About | Log out
Reports
Reports Scans Policies Users
Report Info
Hosts
192.168.2.178
Download Report
Show Filters
Reset Filters
Active Filters
chequeo 192.168.2.178
192.168.2.178
13 results
Port | Protocol | SVC Name | Total | High | Medium | Low | Open Port
80 tcp http? 1 0 0 0 1
135 tcp epmap 2 0 0 1 1
137 udp netbios-ns 1 0 0 1 0
139 tcp smb 2 0 0 1 1
443 tcp https? 1 0 0 0 1
445 tcp cifs 5 0 0 4 1
1025 tcp dce-rpc 1 0 0 1 0
1026 tcp dce-rpc 1 0 0 1 0
1027 tcp dce-rpc 1 0 0 1 0
1028 tcp dce-rpc 1 0 0 1 0
1029 tcp dce-rpc 1 0 0 1 0
2869 tcp icslap? 1 0 0 0 1
5357 tcp unknown 1 0 0 0 1
ES
9:54
20/10/2011


Firefox
Nessus
localhost https://localhost:8834
Google
Nessus
prueba | Help | About | Log out
Reports
Reports Scans Policies Users
Report Info
Hosts
Ports / Protocols
80 / tcp
135 / tcp
137 / udp
139 / tcp
443 / tcp
445 / tcp
Download Report
Show Filters
Reset Filters
Active Filters
chequeo 192.168.2.178
192.168.2.178
135 / tcp
List
Detail
1 results
Plugin ID: 10736
Port / Service: epmap (135/tcp)
Severity: Low
Plugin Name: DCE Services Enumeration
Synopsis: A DCE/RPC service is running on the remote host.
Description
By sending a Lookup request to the portmapper (TCP 135 or epmapper
PIPE) it was possible to enumerate the Distributed Computing Environment
(DCE) services running on the remote port.
Using this information it is possible to connect and bind to
each service by sending an RPC request to the remote port/pipe.
Solution
N/A
Risk Factor: None
Plugin Output
The following DCERPC services are available locally :
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
ES
9:54
20/10/2011

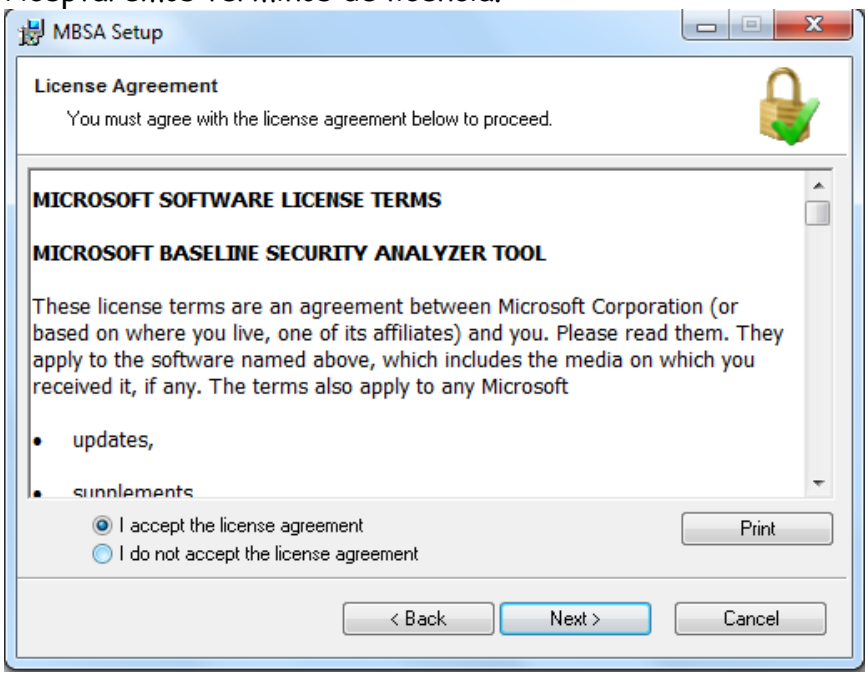
4.3-Microsoft Baseline Security Analyzer (MBSA)

A continuacion vamos a instalar el software Microsoft Baseline Security Analyze para realizar un chequeo a nuestro ordenador. Una vez que tengamos bajado el programa, comenzaremos la instalación.

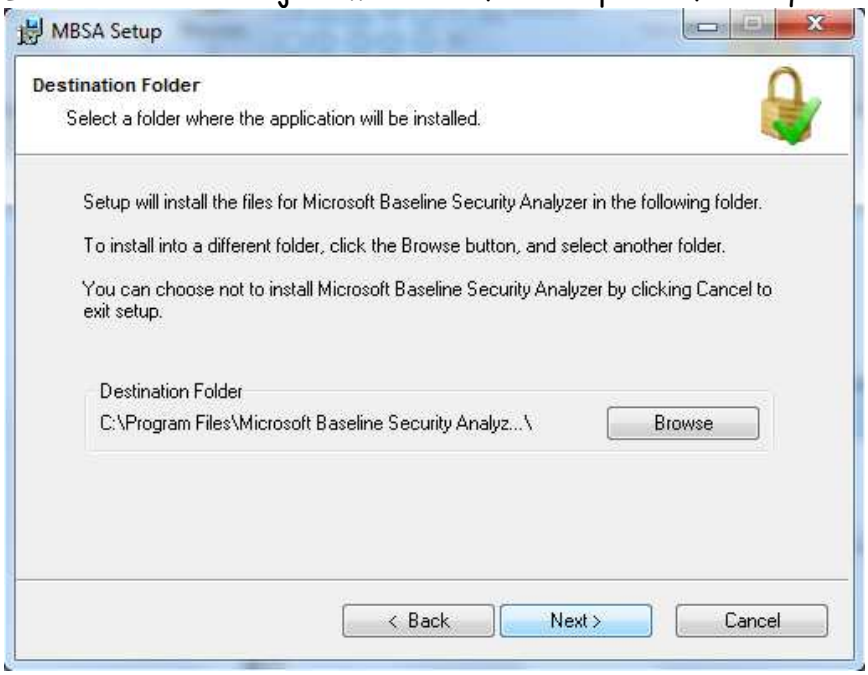


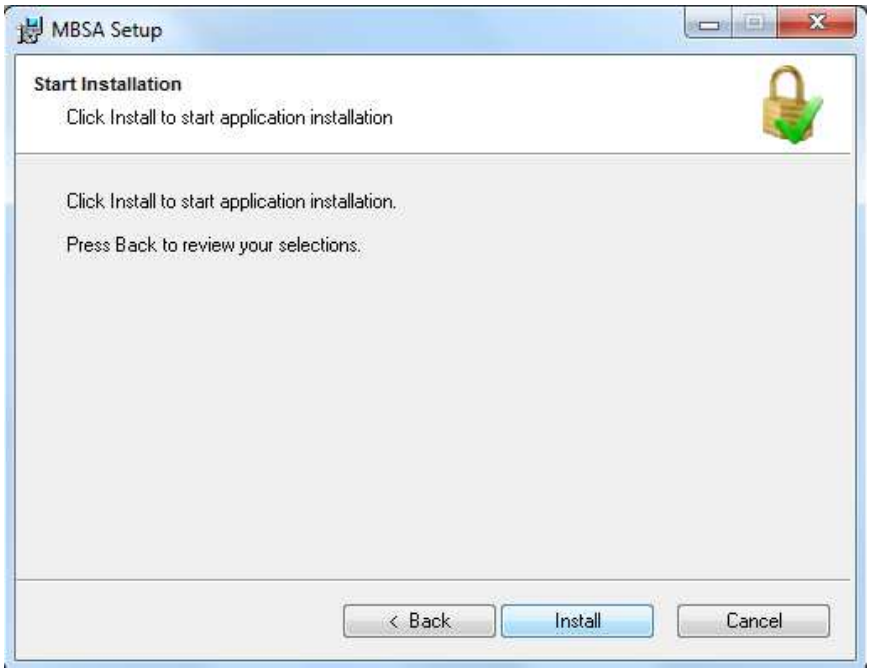
No deseamos instalar barras adicionales a nuestro navegador, por lo que desactivaremos todas las opciones

Aceptaremos términos de licencia.

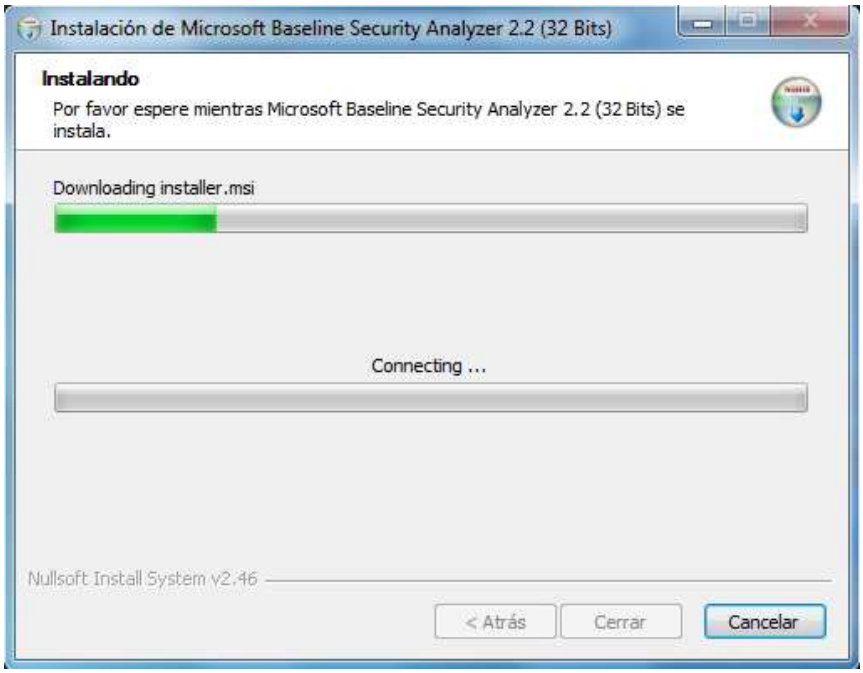


La instalación la dejaremos en el fichero por defecto que nos trae el programa



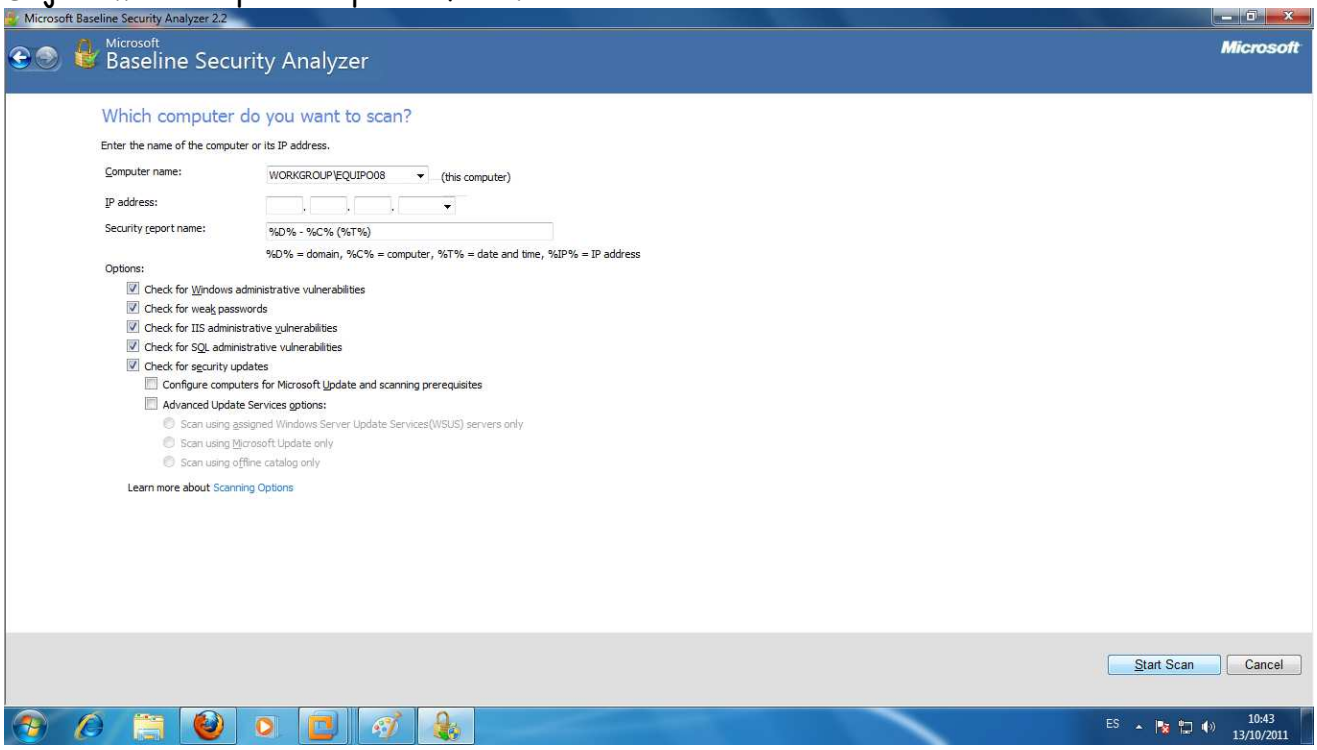


Y comenzara la instalacion



Una vez que acabe de instalarse podemos ver la parte grafica del programa. Ahora vamos a realizar 2 pruebas de chequeo: a nuestro host y a un dominio creado. En primer lugar

haremos el de nivel local.
Dejaremos las opciones por default.



5. Amenazas:

5.1-Visitar el enlace:

http://openmultimedia.ie.edu/OpenProducts/securityxperts/securityxperts/portada.html

para:

5.1.1-*Jugar al Juego de Seguridad:* Elabore un resumen de los ataques que se proponen en el juego y el sistema de seguridad empleado.

TROYANOS

Un troyano es un aplicación "disfrazada" de programa que se nos introduce en el sistema con la intención de abrir una puerta trasera por la que poder controlar remotamente nuestro ordenador.

DENEGACIÓN DE SERVICIOS

Ataque continuado por medio del uso de los servicios normales disponibles en una computadora o máquina servidor con el objeto de saturarla y obligarla a cesar sus funciones.

INGENIERÍA SOCIAL

La ingeniería social consiste en conseguir claves haciéndose pasar por gente relacionada con el entorno de la empresa atacada. Así se averigua, por ejemplo, la fecha de nacimiento (típica clave de seguridad para mucha gente), etc. Los grandes *hackers* siempre han usado esta técnica.

HACKER

Persona que dispone de conocimientos elevados en cuanto a seguridad informática y de la capacidad de violar los sistemas de seguridad de una computadora o una red, ya sea por placer o malicia (en este caso sería un *cracker*).

VIRUS

Programas autorreplicantes que intentan expandirse lo más posible camuflándose en aplicaciones o ficheros, generalmente con intenciones malignas o molestas.

LSSI/LOPD

La ley puede ser tan peligrosa para nuestra empresa como cualquier ataque. Incluso puede ser usada para causar pérdidas a una empresa. La protección de datos es imprescindible.

FIREWALL

Un cortafuego (FIREWALL) es el mecanismo de prevención contra amenazas por intrusión externa. Sus principales funciones son el control de acceso al sistema (tanto de entrada como de salida), la validación de usuarios, el registro de eventos, la auditoría y la generación de alarmas.

ANTIVIRUS

Es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

Conjunto de medidas y recomendaciones que se han de tomar para prevenir infecciones, salidas de códigos y exponer zonas vulnerables de la red.

NEWS

Boletines, grupos de *news*, listas de correo, etc. Todo aquello que de forma regular y periódica nos proporciona información y avisos.

ACTUALIZACIONES DE SOFTWARE

Muchos programas que diariamente usamos contienen errores o *bugs*. Las casas de software suelen sacar parches o actualizaciones que cierran estas brechas en la publicidad y optimizan el sistema. Un error puede convertirse en un *exploit*, es decir, un ataque que puede ser utilizado contra nosotros.

HUB

Un Hub es un concentrador y distribuidor de información y tráfico, que permite que dos o más ordenadores se comuniquen entre sí.

SERVIDOR

Una máquina servidor es un ordenador que tiene un servicio activo (en este caso, el chat) y que permite que los usuarios disfruten de él (un servidor típico del IRC Hispano puede soportar entre 200 y 8000 usuarios concurrentes).

ENLACES

Son las líneas de gran capacidad que permiten la comunicación entre usuarios. El color indica en segundos la calidad de la comunicación.

SPLIT ZONE

Cuando un servidor se deslinka de la red, se queda colgado en un espacio virtual denominado 'Split Zone'. Los usuarios que se encuentren en estos servidores no pueden contactar con el resto de la red.

IRC (CHAT)

Internet Relay Chat, conversaciones que se mantienen en tiempo real entre varios usuarios que conectan a una misma red. Suelen ser por modo texto y a veces con el apoyo de videoconferencia. Un mismo usuario puede mantener múltiples conversaciones simultánes con otros usuarios, de múltiples puntos geográficos.

LAG

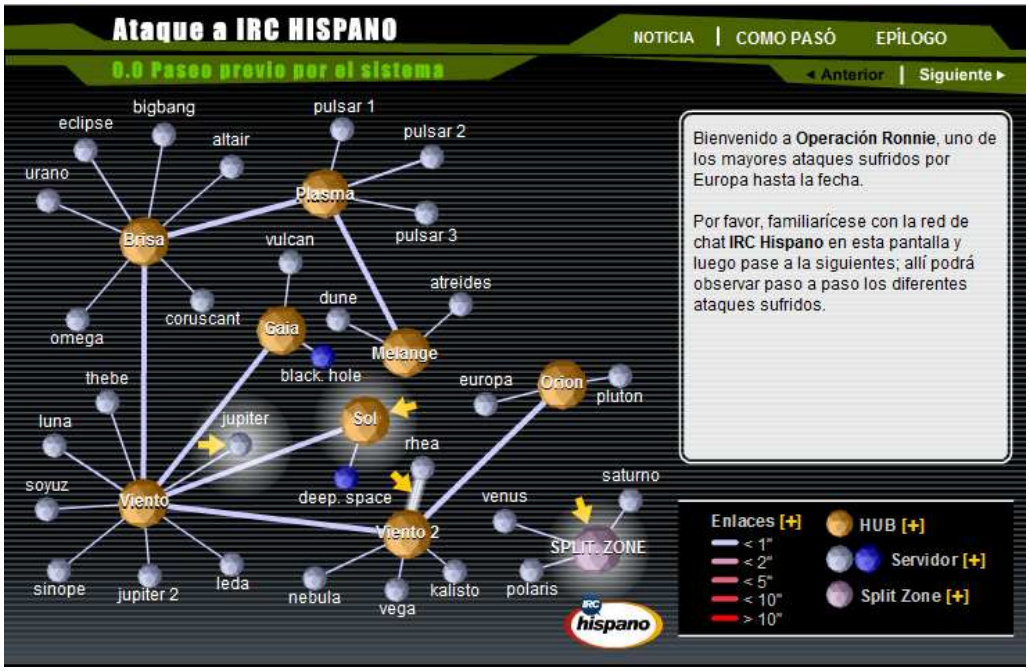
Es un término muy usado en Internet que refleja el retardo que hay entre que tú envías un mensaje de texto a través del chat a un usuario, y éste lo acaba recibiendo. El lag siempre existe aunque se mide en milésimas de segundos. Cuando hay un ataque, o una línea soporta un consumo de ancho de banda excesivo, el lag puede incrementarse hasta varios segundos, dificultando las comunicaciones en tiempo real.

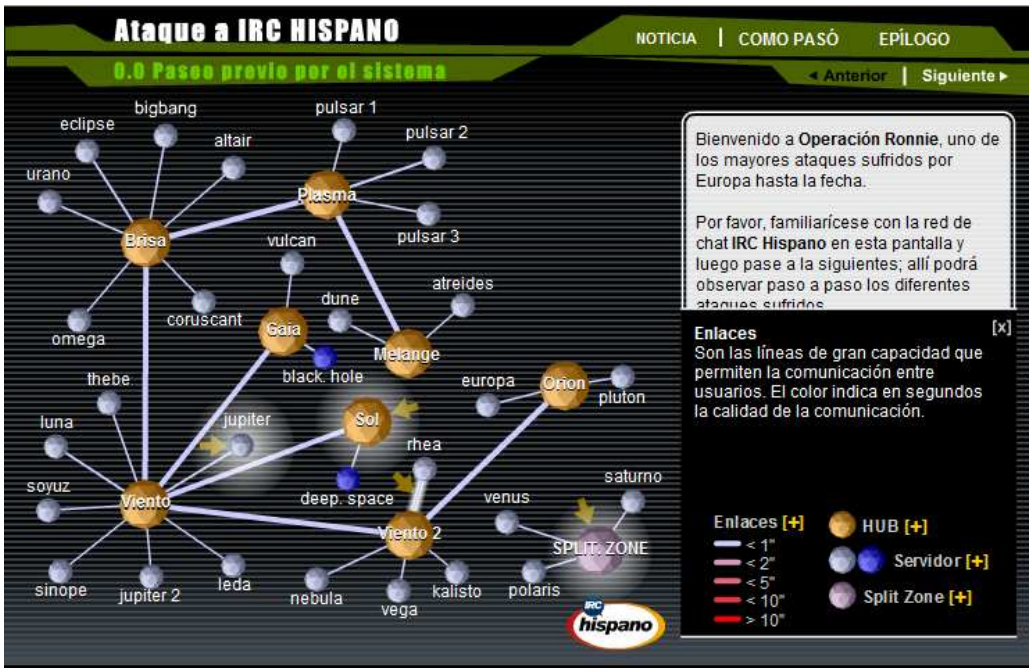
ORDENADOR ZOMBIE

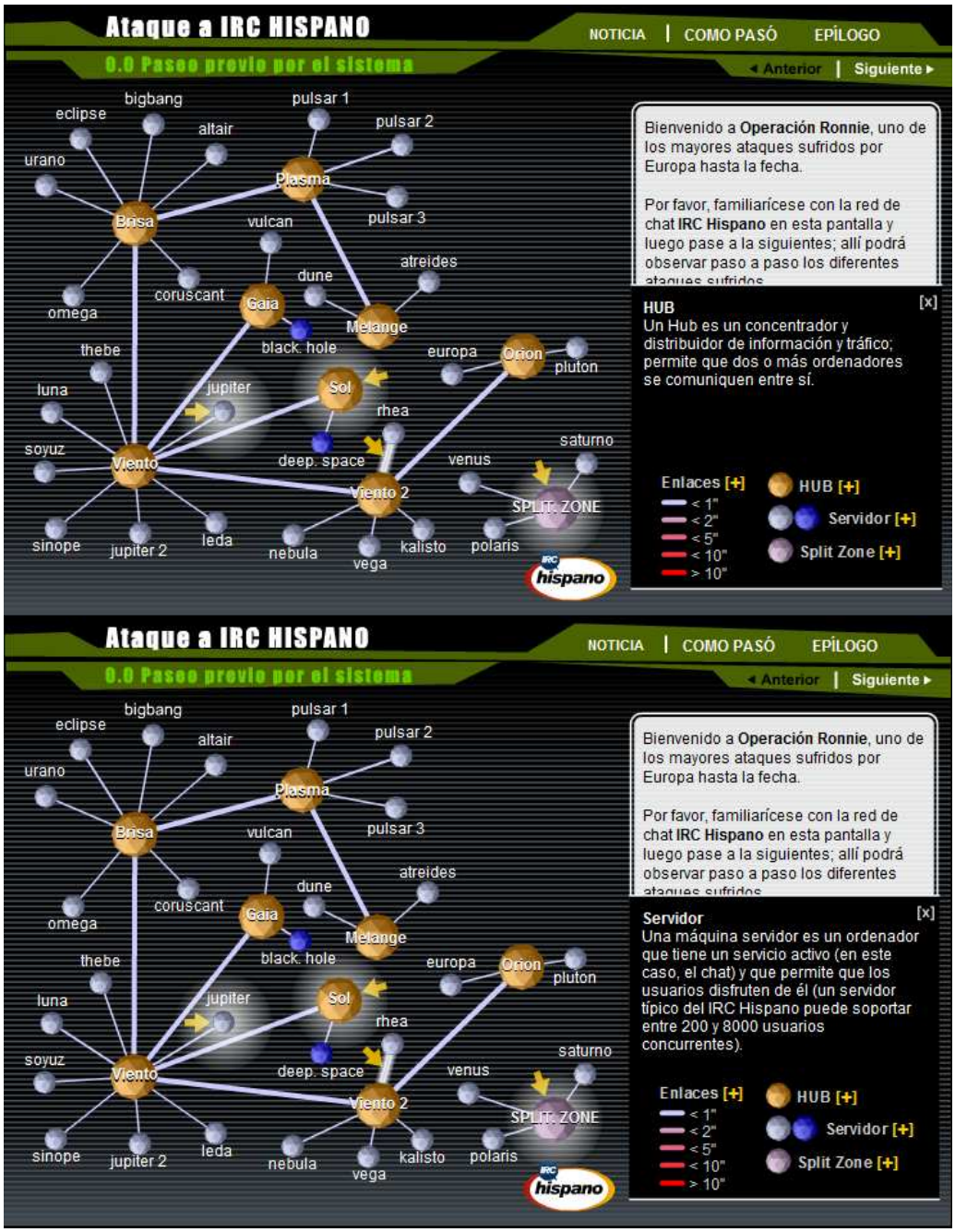
Ordenador infectado por un virus de tipo troyano. Es controlado de forma remota y se usan generalmente para lanzar ataques masivos. Obedecen las órdenes del hacker y se suelen agrupar (por medio de herramientas de hacking) en bloques de miles y a veces incluso cientos de miles de ordenadores

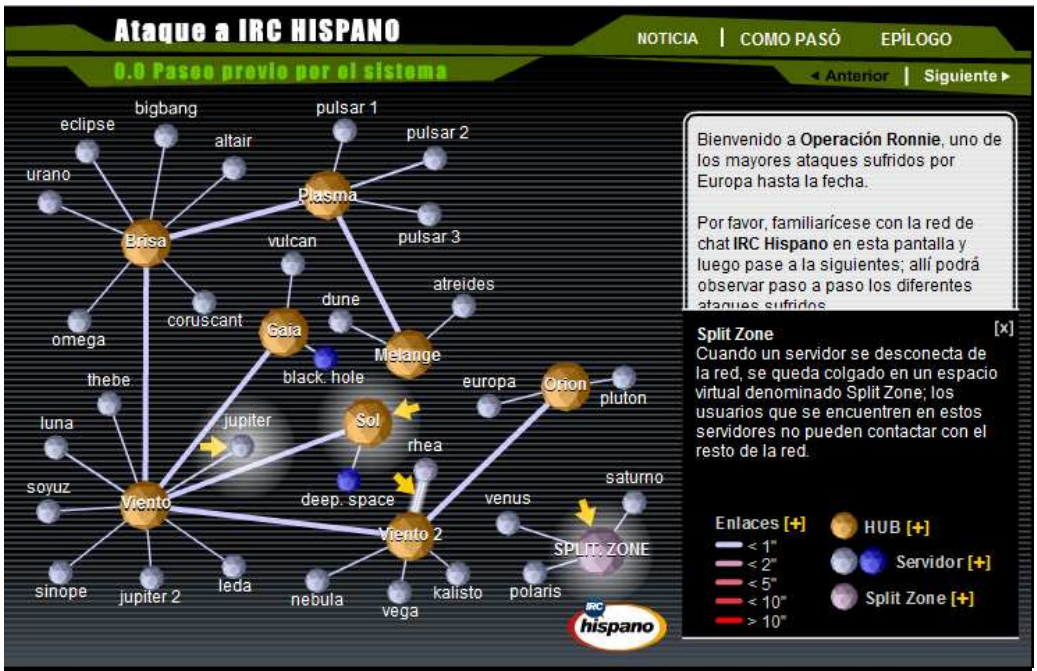
5.1.2-*Elaborar un resumen del ataque sufrido a IRC Hispano* (Caso Ronnie).

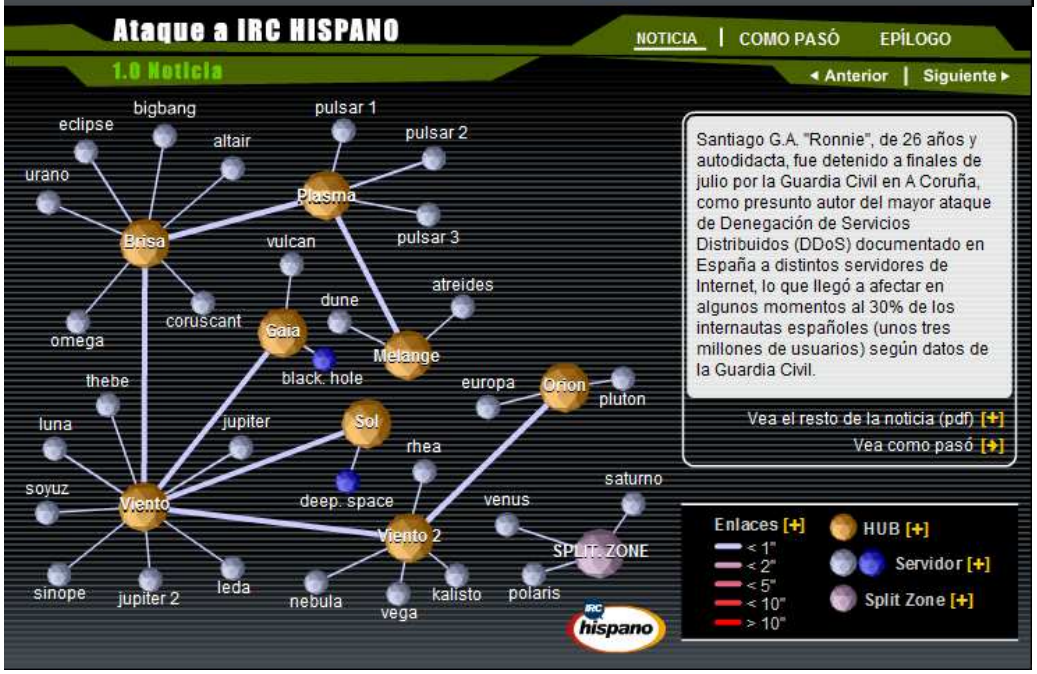
Vamos a ver un resumen del caso Ronnie.

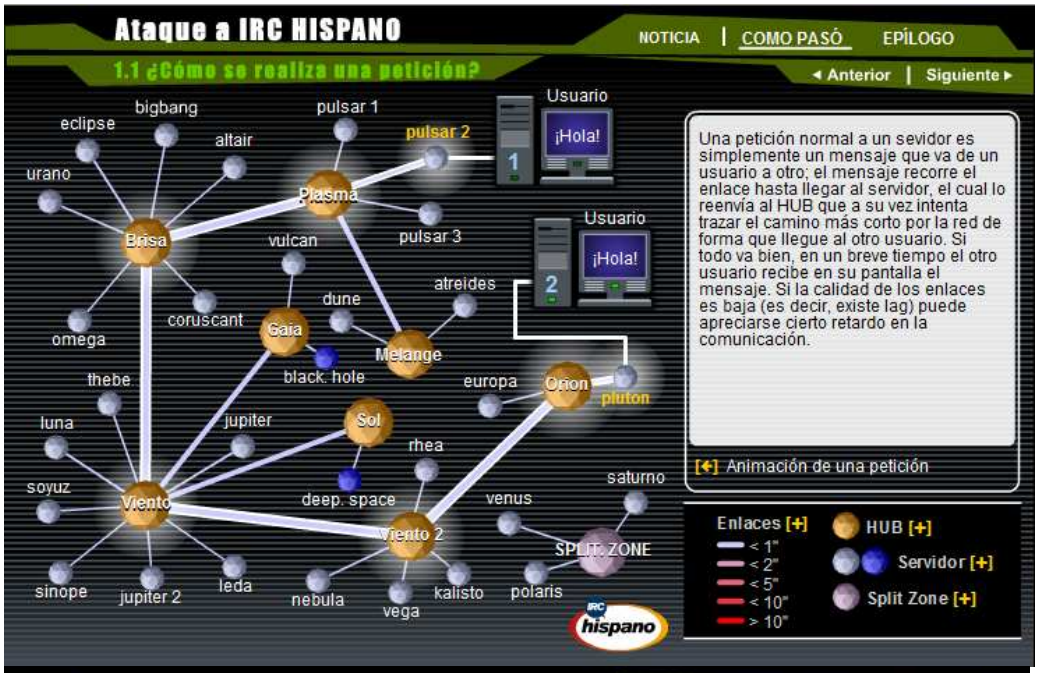


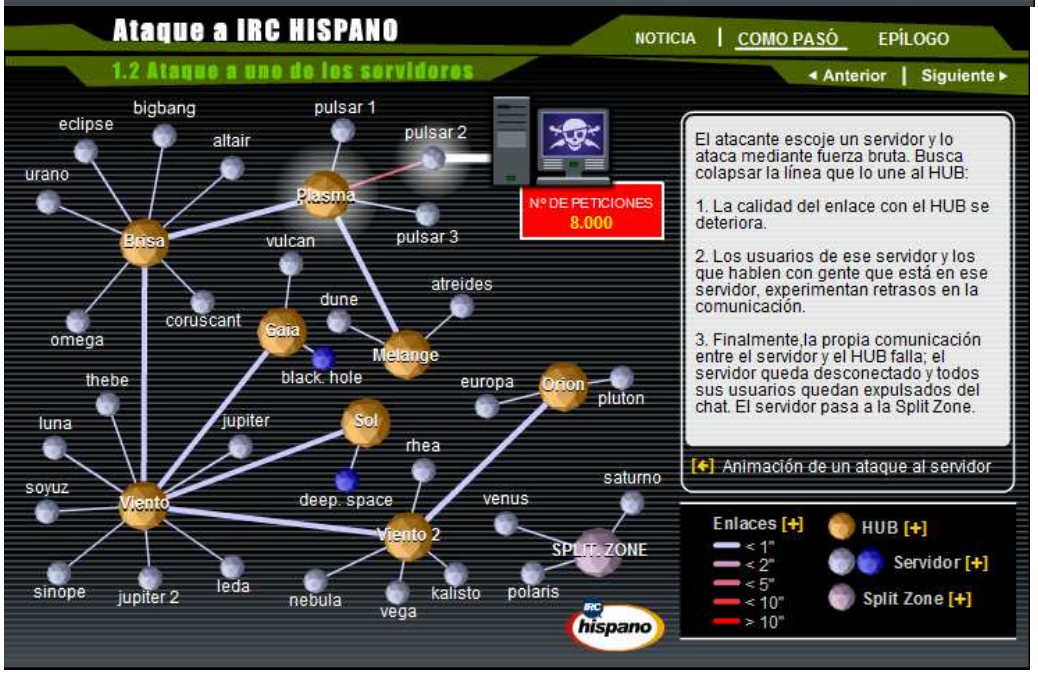

Ataque a IRC HISPANO
NOTICIA | COMO PASÓ EPÍLOGO
0.0 Paseo previo por el sistema
◂ Anterior | Siguiente ▸
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
thebe
black. hole
europa
Orion
pluton
luna
jupiter
Sol
rhea
saturno
soyuz
deep. space
venus
Viento
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano
Bienvenido a Operación Ronnie, uno de los mayores ataques sufridos por Europa hasta la fecha.
Por favor, familiarícese con la red de chat IRC Hispano en esta pantalla y luego pase a la siguientes; allí podrá observar paso a paso los diferentes ataques sufridos
Enlaces [x]
Son las líneas de gran capacidad que permiten la comunicación entre usuarios. El color indica en segundos la calidad de la comunicación.
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]

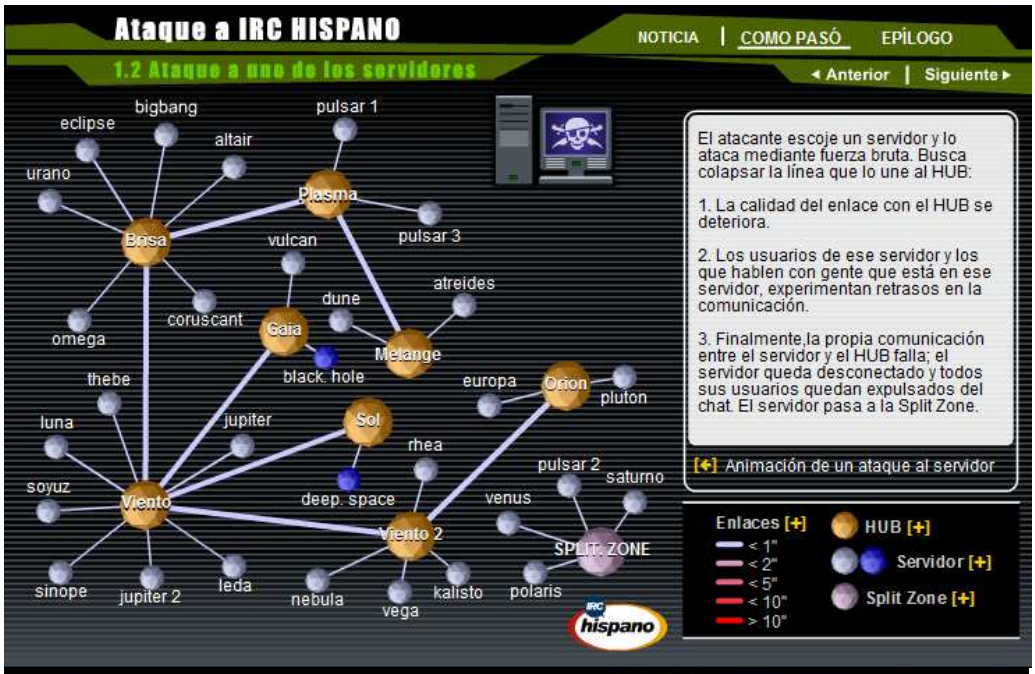

Ataque a IRC HISPANO
NOTICIA | COMO PASÓ | EPÍLOGO
0.0 Paseo previo por el sistema
◂ Anterior | Siguiente ▸
Bienvenido a Operación Ronnie, uno de los mayores ataques sufridos por Europa hasta la fecha.
Por favor, familiarícese con la red de chat IRC Hispano en esta pantalla y luego pase a la siguientes; allí podrá observar paso a paso los diferentes ataques sufridos.
HUB [x]
Un Hub es un concentrador y distribuidor de información y tráfico; permite que dos o más ordenadores se comuniquen entre sí.
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
soyuz
Viento
deep. space
saturno
venus
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano
Ataque a IRC HISPANO
NOTICIA | COMO PASÓ | EPÍLOGO
0.0 Paseo previo por el sistema
◂ Anterior | Siguiente ▸
Bienvenido a Operación Ronnie, uno de los mayores ataques sufridos por Europa hasta la fecha.
Por favor, familiarícese con la red de chat IRC Hispano en esta pantalla y luego pase a la siguientes; allí podrá observar paso a paso los diferentes ataques sufridos.
Servidor [x]
Una máquina servidor es un ordenador que tiene un servicio activo (en este caso, el chat) y que permite que los usuarios disfruten de él (un servidor típico del IRC Hispano puede soportar entre 200 y 8000 usuarios concurrentes).
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
soyuz
Viento
deep. space
saturno
venus
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano


Ataque a IRC HISPANO
NOTICIA | COMO PASÓ | EPÍLOGO
0.0 Paseo previo por el sistema
◂ Anterior | Siguiente ▸
Bienvenido a Operación Ronnie, uno de los mayores ataques sufridos por Europa hasta la fecha.
Por favor, familiarícese con la red de chat IRC Hispano en esta pantalla y luego pase a la siguientes; allí podrá observar paso a paso los diferentes ataques sufridos.
Split Zone [x]
Cuando un servidor se desconecta de la red, se queda colgado en un espacio virtual denominado Split Zone; los usuarios que se encuentren en estos servidores no pueden contactar con el resto de la red.
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
soyuz
Viento
deep. space
saturno
venus
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano


Ataque a IRC HISPANO
NOTICIA | COMO PASÓ | EPÍLOGO
1.0 Noticia
◂ Anterior | Siguiente ▸
Santiago G.A. "Ronnie", de 26 años y autodidacta, fue detenido a finales de julio por la Guardia Civil en A Coruña, como presunto autor del mayor ataque de Denegación de Servicios Distribuidos (DDoS) documentado en España a distintos servidores de Internet, lo que llegó a afectar en algunos momentos al 30% de los internautas españoles (unos tres millones de usuarios) según datos de la Guardia Civil.
Vea el resto de la noticia (pdf) [+]
Vea como pasó [+]
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
soyuz
Viento
deep. space
saturno
venus
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano


Ataque a IRC HISPANO
NOTICIA | COMO PASÓ EPÍLOGO
1.1 ¿Cómo se realiza una petición?
◂ Anterior | Siguiente ▸
Usuario
¡Hola!
Usuario
¡Hola!
Una petición normal a un sevidor es simplemente un mensaje que va de un usuario a otro; el mensaje recorre el enlace hasta llegar al servidor, el cual lo reenvía al HUB que a su vez intenta trazar el camino más corto por la red de forma que llegue al otro usuario. Si todo va bien, en un breve tiempo el otro usuario recibe en su pantalla el mensaje. Si la calidad de los enlaces es baja (es decir, existe lag) puede apreciarse cierto retardo en la comunicación.
[+] Animación de una petición
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
soyuz
Viento
deep. space
venus
saturno
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano


Ataque a IRC HISPANO
NOTICIA | COMO PASÓ EPÍLOGO
1.2 Ataque a uno de los servidores
◂ Anterior | Siguiente ▸
Nº DE PETICIONES
8.000
El atacante escoje un servidor y lo ataca mediante fuerza bruta. Busca colapsar la línea que lo une al HUB:
1. La calidad del enlace con el HUB se deteriora.
2. Los usuarios de ese servidor y los que hablen con gente que está en ese servidor, experimentan retrasos en la comunicación.
3. Finalmente,la propia comunicación entre el servidor y el HUB falla; el servidor queda desconectado y todos sus usuarios quedan expulsados del chat. El servidor pasa a la Split Zone.
[+] Animación de un ataque al servidor
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
bigbang
eclipse
altair
pulsar 1
pulsar 2
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
soyuz
Viento
deep. space
venus
saturno
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
hispano


Ataque a IRC HISPANO
NOTICIA | COMO PASÓ | EPÍLOGO
1.2 Ataque a uno de los servidores
◂ Anterior | Siguiente ▸
bigbang
eclipse
pulsar 1
altair
urano
Plasma
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
pulsar 2
saturno
soyuz
Viento
deep. space
venus
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
El atacante escoje un servidor y lo ataca mediante fuerza bruta. Busca colapsar la línea que lo une al HUB:
1. La calidad del enlace con el HUB se deteriora.
2. Los usuarios de ese servidor y los que hablen con gente que está en ese servidor, experimentan retrasos en la comunicación.
3. Finalmente,la propia comunicación entre el servidor y el HUB falla; el servidor queda desconectado y todos sus usuarios quedan expulsados del chat. El servidor pasa a la Split Zone.
[+] Animación de un ataque al servidor
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
hispano


Ataque a IRC HISPANO
NOTICIA | COMO PASÓ | EPÍLOGO
1.3 Ataque a un HUB
◂ Anterior | Siguiente ▸
bigbang
eclipse
pulsar 1
altair
urano
Plasma
N.º DE PETICIONES
1.000.000
Brisa
vulcan
pulsar 3
atreides
dune
coruscant
Gaia
omega
Melange
black. hole
thebe
europa
Orion
pluton
luna
jupiter
Sol
rhea
saturno
soyuz
Viento
deep. space
venus
Viento 2
SPLIT. ZONE
sinope
jupiter 2
leda
nebula
vega
kalisto
polaris
El atacante decide partir la red en pedazos. Por medio de sus ordenadores zombis lanza un ataque masivo contra el HUB:
1. Colapsa la línea.
2. Degrada el servicio que se da, y la comunicación servidor-HUB y cliente-cliente.
3. Desconecta el HUB.
Al caer el HUB la red entera se "splitea" (deshace en pedazos) quedando los servidores separados hasta que se trazan nuevos enlaces alternativos con los HUB que permanecen en pie.
[+] Animación de un ataque al HUB
Enlaces [+]
< 1"
< 2"
< 5"
< 10"
> 10"
HUB [+]
Servidor [+]
Split Zone [+]
hispano

En general, el caso ronnie fue un ataque de fuerza bruta a los servidores, de modo que colapsaran y dejaran de funcionar correctamente, una vez llegados a eso, los servidores se mandan a una zona muerta que no se detecta con facilidad, haciéndolos pasar por una red

zombi. A partir de este punto consiste en repetir el proceso hasta que todos los servidores estén caídos y comience el caos. Para defenderse de este ataque se recomienda tener un servidor muy potente, aunque a la larga con este método caera de todos modos. Otra idea sera varios proveedores, que en caso de que uno falle, utilizar el de recambio para mantener el orden de trabajo igual

5.2-Busca en Internet al menos una noticia relacionada con amenazas físicas a sistemas informáticos respecto a:
5.2.1-Robos, sabotajes, destrucción de sistemas.

Expertos de la universidad Ruhr de Bochum, en Alemania, han logrado “crackear” datos cifrados transmitidos en lenguaje XML, un estándar creado por el W3C que está presente en muchas páginas web.

Básicamente, el cifrado de XML se utiliza para los datos que se envían entre servidores online y es empleado en negocios que mueven importantes cantidades de dinero, como pueden ser las tiendas de comercio online o compañías del mundo financiero.

Afortunadamente, el agujero en el cifrado de XML solo puede ser explotado si el cifrado de los datos transmitidos se realiza con AES en modo CBC, y no afectaría si están protegidos mediante claves RSA o certificados X.509.

Entre las empresas que utilizan XML cifrado en sus servicios web se encuentran IBM, Microsoft o Red Hat Linux, lo que demuestra que su uso está muy extendido por internet.

Los autores del estudio creen que ya no se puede considerar el cifrado de XML como seguro y han recomendado que se realice una actualización completa del mismo para solucionar la vulnerabilidad.

Santa Brígida denuncia un sabotaje informático

Seguridad y Emergencias pone el caso en manos de la Guardia Civil - Las sospechas recaen en agentes por el conflicto laboral con el Ayuntamiento.

El Ayuntamiento de Santa Brígida ha denunciado un presunto sabotaje informático producido en las dependencias de la Jefatura de la Policía Local, el penúltimo fin de semana de julio.

El concejal de Seguridad y Emergencias de la Villa, Martín Sosa, se personó la semana pasada en el cuartel de la Guardia Civil de San Mateo para dejar constancia de la desaparición de un directorio informático de un ordenador ubicado en las oficinas de la Policía Local, durante el fin de semana del 22 al 24 de julio.

En la declaración del concejal *popular* satauteño se apunta como posibles autores del sabotaje informático a agentes de la Policía Local, debido al conflicto laboral que mantienen con el Consistorio presidido por Lucas Bravo de Laguna.

Martín Sosa explicó este miércoles a CANARIASAHORA que "como concejal responsable es mi obligación presentar esta denuncia para poner en conocimiento esos hechos, en base a los informes de un auxiliar administrativo adscrito a la Jefatura. Es mi responsabilidad para que se esclarezca, si ha sido un sabotaje o un fallo informático".

Los hechos denunciados fueron advertidos por personal del Ayuntamiento la mañana del lunes 25 de julio, cuando quedó constancia de la eliminación, en el intervalo de tiempo del fin de semana anterior, de un directorio con información necesaria para prestar el servicio policial, así como las labores administrativas de la Concejalía.

La información perdida incluía la base de control de los boletines de denuncias de Valora, la empresa recaudadora municipal. También se han extraviado documentos y plantillas de multas que han bloqueado, en parte, el trabajo del personal administrativo de la Jefatura de la Policía Local.

"Yo no sé lo que ha pasado o si puede haber sido un error informático. En ningún momento acuso de nada a la Policía, pero sí he tenido que dejar constancia que existe en el Cuerpo un conflicto laboral manifiesto", abundó sobre el caso el concejal de Seguridad satauteño.

"Debe ser la Guardia Civil quien determine si fue un acto intencionado o un fallo de la torre del ordenador", recalcó Martín Sosa.

5.2.2-Catástrofes, Incendios, Cortes de suministro eléctrico
Sony en busca de 1.6 millones de televisores Bravia por posibles problemas de incendio

Sony se ha puesto a detectar televisores vendidos a marchas forzadas, casi como lo que ocurre en el mercado del automóvil donde los grandes fabricantes hacen importantes llamadas a revisión de un automóvil por culpa de algún componente que puede terminar por dar problemas.

En el caso de la multinacional japonesa, está en busca y captura de 1.6 millones de televisores Bravia, que han sido vendidos a partir del año 2007. La razón: un componente defectuoso que podría causar incendios en el equipo. Se habla de un elemento que tiene que ver con la retroiluminación del LCD, que se sobrecalienta en exceso.

Se han detectado once incidentes por culpa del poco definido problema (en Japón), y Sony considera causa suficiente para detectar los 1.6 millones televisores que han sido vendidos principalmente en Japón, pero también en Estados Unidos y Europa.

Aunque no tenemos muy claro que Sony trabaje con las mismas denominaciones para todos los mercados, en un primer listado encontramos los siguientes modelos: DL-40D3400, KDL-40D3500, KDL-40D3550, KDL-40D3660, KDL-40V3000, KDL-40W3000, KDL-40X3000 and KDL-40X3500.

Intentamos informar de la situación teniendo en cuenta la fuente oficial en japonés, y las informaciones que he tenido lugar de leer en diferentes medios, esperamos que Sony España se pronuncie al respecto, antes de preocuparnos más de la cuenta sobre este asunto.
5.3-Busca en Internet al menos una noticia relacionada con amenazas lógicas respecto a: 5.3.1-Ataques a un sistema informático - Ciberdelitos.
5.3.2- Ciberfraudes - Vulnerabilidades y Amenazas.

Rompen “red” mundial de “ciber-fraude”

Detienen en EU a diez sujetos y buscan a otras 17 personas
Operaban en todo el mundo y pretendían robar 220 millones de dólares de cuentas de sus víctima. Los 17 restantes aparecen en la lista de los “más buscados” del FBI

Buscados por el FBI

TIJUANA BC 1 de octubre de 2010 (AFN).- El FBI de los Estados Unidos informó este viernes sobre el desmantelamiento de la mayor red mundial de “ciber-fraude” que ya era investigada y que según las acusaciones que pesan en contra de sus integrantes, utilizaron centenares de cuentas bancarias falsas buscando recibir más de 3 millones de dólares de sus victimas.

Mediante un comunicado de prensa, el Federal Bureau of Investigation del vecino país, hizo saber que el jueves previo, su oficina en Nueva York arrestó a diez sujetos relacionados con el caso, en tanto prosiguen en la búsqueda de otras 17 personas, cuyos rostros quedaron fichados dentro de la lista de los “más buscados”.

En total, este “anillo” criminal pretendía robar unos 220 millones de dólares y para esto utilizó de manera activa el virus conocido como “Zeus” para infectar más computadoras.

“Pero más allá de la pérdida monetaria real y potencial, este caso es importante porque se contó con un extraordinario nivel de cooperación entre las fuerzas del orden internacional para detener al grupo”, dijo Weysan Dun, agente especial a cargo de la oficina del FBI en

Omaha, donde la investigación comenzó en mayo de 2009, cuando los agentes descubrieron un patrón que era utilizado en transacciones bancarias sospechosas".

Dun dijo que hay muchos desafíos en un caso complicado a nivel mundial como era éste y explicó que en varios países involucrados "hay diferencias en zonas horarias, la geografía y la cultura, por no mencionar que todas nuestras leyes de ciber no son las mismas. Pero esas diferencias, sentenció, fueron superadas".

Afirmó que los resultados hablan por si mismos y dijo que además de enviarse un mensaje a los "piratas informáticos de todo el mundo", en el sentido de que hay menos lugares seguros de los que pueden operar, se hace notar asimismo que la tolerancia internacional para este tipo de actividad delictiva está disminuyendo.

Refirió que sus socios en el extranjero están tratando de manera más agresiva y efectiva los delitos cibernéticos y que el número de naciones que han colaborado y trabajado en conjunto en este caso, representa un paso adelante, muy significativo en la manera de investigar este tipo de asuntos.

El agente especial del FBI reveló que los ladrones cibernéticos fueron "inteligentes" en su manera de operar, ya que en lugar de apuntar hacia las corporaciones y los grandes bancos, tomaron como objetivo las cuentas de las empresas de tamaño medio, ciudades e inclusive Iglesias.

Antes de la captura de los diez delincuentes en Nueva York, los integrantes de este "anillo" lograron robar 70 millones de dólares y por lo tanto era una red de robo mayor, comentó por su parte Gordon Nieve, asistente del Director de Cyber del FBI Division.

"La actividad criminal global a esta escala, comentó Nieve, es una amenaza a nuestra infraestructura financiera y sólo se puede combatir eficazmente a través del tipo de cooperación que hemos visto en este caso".

Los "socios" de Estados Unidos en la aplicación de esta Ley, son, según refirieron: el Reino Unido, Ucrania y los países bajos, que han anunciado asimismo la ejecución de numerosas detenciones y órdenes de registro en varios países "en uno de los mayores casos de ciber criminales que han sido investigados.

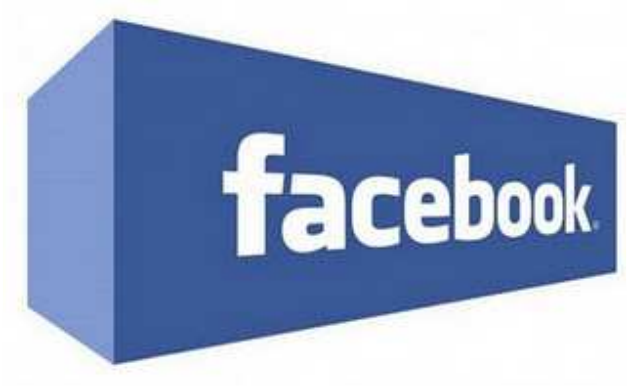
Por lo que respecta al uso del virus conocido como troyano Zeus, los "piratas informáticos" en el este de Europa infectaron varias computadoras en todo el mundo. Dicho virus fue "transportado" a través de un e-mail, que cuando los destinatarios abrían, el software malicioso se instalaba en su equipo y en secreto capturaba las contraseñas, números de cuenta y otros datos utilizados para acceder a las cuentas, a través de la "banca en línea".

Los hackers utilizan esta información para hacerse cargo de las cuentas de las víctimas bancarias y realizar transferencias no autorizadas, de miles de dólares a la vez, a menudo de "enrutamiento" de los fondos a otras cuentas controladas por una red de "mulas de dinero".

Muchos de esos "mulas" en Estados Unidos, fueron reclutados desde el extranjero y éstos crearon cuentas bancarias con documentos y nombres falsos.

Una vez que el dinero estaba en sus cuentas "las mulas" enviaban de vuelta lo obtenido, a sus jefes en el Este de Europa, a fin de que lo convirtieran en dinero en efectivo. Por este trabajo y el contrabando del dinero, fuera del país, se les pagaba una comisión.

Peligrosa ciber-estafa se expande vía Facebook



Alerta a todos los usuarios de Facebook, ya que una nueva estafa electrónica se está propagando a través de la red social, con objeto de robar los datos de cuentas bancarias.

El fraude funciona de la siguiente manera: Los usuarios reciben un mensaje en su buzón privado, donde se les indica que deben verificar sus cuentas si es que quieren seguir

utilizándolas y, para ello, deben entregar información personal para dar prueba de su identidad

Así, se les re-dirige a un sitio malicioso, donde se les piden datos como su respuesta a la pregunta secreta e incluso información sobre su cuenta bancaria. En algunos casos, también se incluye la petición de datos sobre su cuenta Paypal.

Obviamente, todo se trata de una estafa para robarles el dinero, ya que Facebook **NUNCA** pedirá ese tipo de información. Es importante jamás entregar datos personales y nunca proporcionar información bancaría o financiera a nadie, sin importar quien digan ser.

El mensaje fraudulento, se envía a todos los contactos que tengas en Facebook, por lo que si recibiste dicho correo dentro de tu cuenta de la red social, es importante que les adviertas para que no caigan en la trampa.

Si recibes el mensaje, sólo elimínalo y nunca hagas clic sobre ningún enlace que se te de. Si es que requieres entrar a una dirección donde vas a indicar algún dato, lo mejor es que la escribas directamente en el navegador

CIBER DELITO

Delitos informáticos

En lo que va de 2010, el robo a cuentas bancarias vía medios informáticos suma un perjuicio de más de $400 mil en el Guayas

El 5 de noviembre pasado, Liliana Buendía, una guayaquileña de 29 años, fue víctima de un delito informático. De acuerdo con la denuncia que presentó en la Policía Judicial del Guayas, la tarde de aquel día, el saldo de su cuenta de ahorros quedó reducido a $59, pues le habían robado $2 400 mediante una transacción fraudulenta. Irónicamente, Buendía se desempeña como jefa de Sistemas en su lugar de trabajo.

Según estadísticas del Observatorio de Seguridad Ciudadana de Guayaquil (OSC), desde el 1.° de enero hasta el 12 de diciembre de 2010, se han presentado 199 denuncias por transferencias bancarias ilícitas vía Internet en la urbe porteña, siendo septiembre el mes de mayor incidencia con el 24,62% de los casos. En tanto, diciembre registra el 1,51%.

Además, de las 23 384 denuncias en total que ha receptado ese organismo durante todo el año, dicha modalidad de delito informático representa el 0,85%. Esto significa que el promedio semanal de su cometimiento es cuatro veces a la semana, especialmente, los lunes y viernes con el 19,80% y el 21,29% del universo de los casos, respectivamente, según lo explicó Bernardo Ovalle, director del organismo.

Referente a la sanción que implica robar mediante vías electrónicas, el artículo 553 del Código Penal indica: "Serán reprimidos con prisión de seis meses a cinco años y multa de $500 a $1 000 de los Estados Unidos de Norteamérica (...) los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de esta o de un tercero, en beneficio suyo o de otra persona (...)".

Sin embargo, Patricia Morejón, jefa de la Unidad de Delitos Informáticos y Telecomunicaciones de la Fiscalía del Guayas, manifestó que en el artículo se debería sustituir la prisión por reclusión, ya que esta es la modalidad más cometida dentro de los delitos informáticos. "Como la sanción es de prisión, todo el mundo se lleva el dinero que le da la gana y simplemente van a una medida alternativa, y no pasa nada", acotó.

El argumento se sustenta sumando los perjuicios económicos que ha provocado el robo por Internet, los mismos que ascienden a $492 021,35 en lo que va del año, según datos del OSC.

De acuerdo con cifras del organismo, el robo a los clientes del Banco Pichincha en 2010 sumó $193 703,22, seguido por el Banco del Pacífico con $102 022,59, Produbanco con $73 931,87, Banco de Guayaquil con $45 922,23, IESS con $44 251,24, entre otros.

En ese sentido, Juan Carlos Parra, experto en programación, afirmó que los bancos y demás empresas deben "obligadamente encriptar sus datos y servidores", es decir, proteger la información para que no pueda ser leída sin una clave.

Entre otras recomendaciones, indicó que "no se deben habilitar todos los puertos USB de las computadoras, y las redes deben ser solamente internas con claves que se cambien constantemente".

En cuanto a las precauciones que debe adoptar la ciudadanía para evitar ser víctima de los delincuentes informáticos señaló que se "tiene que evitar colocar datos personales a como dé lugar". (DVQ)

Tipos de delitos informáticos

A partir de la creación de la Ley de Comercio Electrónico, Firmas Electrónicas, y Mensajes de Datos en abril de 2002, se reconoció la validez jurídica de los datos informáticos y archivos adjuntos, por lo que a su vez, también se reconocieron a los delitos informáticos, entre los que se encuentran varias modalidades que están tipificadas en el Código Penal. Una de ellas es el phishing, en el que el delincuente virtual se hace pasar por una persona o empresa de confianza a través de un correo electrónico o cualquier medio de mensajería

instantánea para obtener información como números de cuenta o de tarjetas de crédito. También están el "sabotaje informático" y el "daño informático", cuando un individuo daña dolosamente un programa o hardware. En cambio, la "falsificación electrónica" consiste en alterar cualquier tipo de mensaje o documento electrónico. Por otro lado, la "estafa informática" se refiere a los mensajes que llegan a los correos electrónicos o los que automáticamente se abren anunciando la obtención de un premio, e incluso ofertan empleos. En tanto, la denominada "violación a la intimidad y a la confidencialidad" se produce cuando se leen mensajes sin autorización, o cuando se divulga un secreto comercial. Finalmente, está la "apropiación ilícita", que se refiere a la transferencia de dinero vía Internet de manera ilegal.

Modalidad para profesionales

De acuerdo con Mario Acosta, comandante de la Policía Judicial del Guayas, el delincuente cibernético "no es un ladrón común", pues su perfil "es el de una persona con bastos conocimientos en programación y sistemas".

En este sentido, Patricia Morejón, jefa de la Unidad de Delitos Informáticos de la Fiscalía del Guayas, indicó que el alto grado de preparación de este tipo de delincuentes ha provocado que "este delito informático no tenga fronteras". Según explicó, no es novedad que a un ecuatoriano se le roben sus ahorros a través de una transferencia que fue ejecutada en Colombia, los EEUU o Perú.

Por esta razón, Morejón aseguró que es necesario que se empiecen a habilitar convenios internacionales para combatir los delitos cibernéticos. Además, indicó: "Hasta pedir una asistencia penal internacional para investigar una transferencia que se hizo en otro país, se me va el plazo de la instrucción fiscal, y no se tienen las pruebas". Por otro lado, Juan Carlos Parra, experto en programación, aseguró que "en el mundo todos los servidores son vulnerables", porque los piratas informáticos siempre están maquinando la forma de cómo acceder a ellos. Además, agregó que el término hacker está mal utilizado, pues explicó que "solo se trata de una persona que tiene elevados conocimientos informáticos". Los ladrones en red son los crackers, cuyo objetivo es hacer daño. El término proviene de la expresión anglosajona "criminal hacker", acotó.

Casi 22.000 españoles son víctimas de ciberdelitos al día

MADRID (Reuters) - Casi 22.000 españoles son víctimas cada día de ciberdelitos, lo que le supuso al país un coste neto total de más de 5.900 millones de euros el año pasado debido a la delincuencia online, según reveló el Informe sobre Cibercrimen de Norton para 2011 presentado el jueves en Madrid.

Un 69 por ciento de los usuarios ha sido víctima de ciberdelitos alguna vez en su vida, y un 44 por ciento de los encuestados en España no cuenta con un software de seguridad actualizado, según los datos de la empresa de seguridad en Internet.

"Existe una seria confusión en cuanto a cómo ve la gente la amenaza del cibercrimen", afirmó Adam Palmer, asesor de Norton Lead Cybersecurity.

"El cibercrimen es mucho más corriente de lo que la gente cree. Requiere que todos estemos más alerta y que invirtamos en nuestra seguridad online y nuestros smartphone", añadió.

En cuanto a los tipos más comunes de cibercrimen, sobresalen un año más los ataques de "malware" (software malicioso) y virus informáticos (58 por ciento), seguidos por los cada vez más comunes secuestros de perfiles en redes sociales (37 por ciento) y las estafas online, con un 9 por ciento.

Las víctimas más propensas a sufrir un ciberataque son los jóvenes y los que más tiempo pasan conectados a la semana.

"Los jóvenes son más propensos a sufrir ciberataques porque pasan más horas en Internet, lo que hace que uno se confíe más", señaló Javier Ildefonso, responsable de Comercio Electrónico de Norton para Europa, Oriente Próximo y África.

5.4-Busca al menos dos antivirus on line y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación: (Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y virus encontrados y desinfectados)

Comparativa de 2 antivirus online

QuickScan Beta 32-bit v0.9.9.99	Eset Online Scaner
Fecha de Análisis: Fri Oct 21 13:12:53 2011 ID de la Máquina: FC6B050B No se han encontrado infecciones Envío iniciado - 4 archivo(s) RdLang_Updater.ESP (14336) RdLang_SaveAsRTF.ESP (25088) RdLang_weblink.ESP (44032) RdLang_EScript.ESP (100352) Velocidad de envío - 11 KB/s Envío finalizado - 4 enviados, 0 fallidos El archivo(s) enviado se encuentra limpio. Scan finished - communication took 17 sec Total traffic - 0.19 MB enviados, 0.88 KB recibido Scanned 903 files and modules - 50 seconds	Versión de la base de firmas de virus: 6442 (20110906) Fecha: 25/10/2011 Hora: 9:30:16 Discos, carpetas y archivos analizados: Memoria operativa;C:\Sector de inicio;D:\Sector de inicio;F:\Sector de inicio;C:\;D:\;F:\ Cantidad de objetos analizados: 1912238 Cantidad de amenazas detectadas: 0 Hora de finalización: 11:39:45 Tiempo total de análisis: 7769 seg (02:09:29)

Los 2 antivirus muestran la información mostrada, el tiempo transcurrido, y en general muestra que nuestro ordenador no tiene ningún tipo de amenaza virus. Por otro lado en este informe se ha omitido los ficheros que han analizado. Destacar que Quick Scan muestra otros datos informativos, como la velocidad de envió y la ID de la maquina, pero el Eset Scan Online analiza los ficheros 1 a 1 permitiendo más precisión, aunque sea más lento.

5.5-Instala al menos dos antivirus en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación:
(Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y virus encontrados y desinfectados).

Panda Active Scan	Eset Online Scanner
ANALYSIS: 2011-10-26 19:33:52 PROTECTIONS: 1 MALWARE: 43 SUSPECTS: 0 PROTECTIONS Description ESET NOD32 Antivirus 4.2	Versión de la base de firmas de virus: 6442 (20110906) Fecha: 25/10/2011 Hora: 9:30:16 Discos, carpetas y archivos analizados: Memoria operativa;C:\Sector de inicio;D:\Sector de inicio;F:\Sector de inicio;C:\;D:\;F:\ Cantidad de objetos analizados: 1912238 Cantidad de amenazas detectadas: 0 Hora de finalización: 11:39:45 Tiempo total de análisis: 7769 seg (02:09:29)

Esta vez hemos usado la versión local de Eset Online Scanner que a diferencia del modo online, este escanea más a fondo los ficheros y muestra un registro mucho mas profundo y detallado.

5.6-Instala al menos dos aplicaciones antimalware en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación: (Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y *malware* encontrado y desinfectados).

Malwarebytes' Anti-Malware 1.51.2.1300
Versión de la Base de Datos: 7622 Windows 6.1.7601 Service Pack 1 Internet Explorer 9.0.8112.16421 25/10/2011 16:31:41 mbam-log-2011-10-25 (16-31-41).txt Tipos de Análisis: Análisis Rápido Objetos examinados: 173178 Tiempo transcurrido: 3 minuto(s), 24

segundo(s)

Procesos en Memoria Infectados: 0
Módulos de Memoria Infectados: 0
Claves del Registro Infectadas: 0
Valores del Registro Infectados: 0
Elementos de Datos del Registro Infectados: 0
Carpetas Infectadas: 0
Archivos Infectados: 0

Procesos en Memoria Infectados:
(No se han detectado elementos maliciosos)

Módulos de Memoria Infectados:
(No se han detectado elementos maliciosos)

Claves del Registro Infectadas:
(No se han detectado elementos maliciosos)

Valores del Registro Infectados:
(No se han detectado elementos maliciosos)

Elementos de Datos del Registro Infectados:
(No se han detectado elementos maliciosos)

Carpetas Infectadas:
(No se han detectado elementos maliciosos)

Archivos Infectados:
(No se han detectado elementos maliciosos)

6. Seguridad física y ambiental:

6.1-Se necesita realizar **un estudio de la ubicación y protección física de los equipos y servidores del aula,** desde el punto de vista de:

6.1.1-Acondicionamiento físico (Extintores, Sistema de aire acondicionado, Generadores eléctricos autónomos, racks)

Precauciones antiincendios

El CPD necesita un sistema propio de detección del fuego y de extinción. No se debe a que el CPD suponga en sí mismo una posible fuente de incendios, sino más bien al valor de la información almacenada y al considerable daño que supondría para el negocio una pérdida de la misma.

Los fuegos raramente comienzan en el CPD. Los CPDs resultan dañados más a menudo por los fuegos (o por el humo y gases) que comienzan en otras partes y se extienden a la sala de procesamiento de datos.

Los equipos pueden resultar seriamente dañados, por el humo y gases corrosivos (como el Cloruro de Hidrógeno producido en la combustión de los cables, salvo que se elija adecuadamente el cable). Estos equipos pueden también verse dañados por los materiales utilizados para la extinción del fuego incluyendo flurocarbono, agua y dióxido de carbono.

En muchos casos, el daño debido a los elementos de extinción del fuego es superior al

producido por el fuego propiamente.

Dentro del CPD, los riesgos se reducen al mínimo guardando las impresoras, una fuente común de ignición, lejos de los otros equipos.

Todos los cables tendidos bajo el suelo deberían ser LSZH (Low Smoke Zero Halogen).

Los principios apropiados para la protección contra incendios son: reducir la probabilidad de que un fuego comience, reducir la probabilidad de que un fuego se disperse y reducir el daño mínimo que un fuego puede causar.

El riesgo de que un fuego comience se reduce al mínimo si el CPD está situado lejos de cuartos de la planta y de almacenes de materiales inflamables, y no construido sobre áreas de estacionamiento de coches. Las paredes del CPD deben tener un grado mínimo de resistencia al fuego de una hora (RF-60) aunque se recomienda un grado RF-120, y deben proporcionar barrera frente al humo. Todas las puertas de acceso deben tener una ventana con cierre propio. Todos los materiales usados en la construcción de la sala de ordenadores deben ser incombustibles. Para controlar el daño por agua, todas las entradas del piso, de la pared y del techo deben estar selladas.

Los CPDs necesitan sistemas contra incendios así como preventivos. Mientras no haya un sistema ideal, los sistemas por aspersión que se activan por dos detectores son una buena elección. Si se instala este tipo de sistemas por aspersión, hay que evitar que en caso de incendio el agua caiga directamente sobre los equipos electrónicos y que los sistemas de circulación de energía y de aire en las áreas afectadas permanezcan abiertos. Deben proporcionarse extractores de gas y desagües.

Los extintores manuales contra el fuego deben ser de dióxido de carbono u otros gases con agentes de extinción. No debe haber componentes químicos de extinción por polvo seco en el área de ordenadores.

Exigencias de comportamiento al fuego

Hay que tener en cuenta que las condiciones de reacción al fuego aplicables a elementos constructivos se justificarán:

- Mediante la clase que figura en cada caso, en primer lugar, conforme a la nueva clasificación europea.
- Mediante la clase que figura en segundo lugar entre paréntesis, conforme a la clasificación que establece la norma UNE-23727.
- Los productos deberán acreditar su clase de reacción al fuego conforme a la normativa 23727:1990 mediante un sistema de evaluación de la conformidad equivalente al correspondiente al del marcado CE que les sea aplicable.

Control de inundaciones

Según norma:

Deben de existir detectores de inundación con alarmas en varios sitios instaladas en sitios visibles del edificio, ya que la falta de estos detectores supone la existencia de un riesgo muy elevado de pérdida de equipos en caso de producirse una inundación.

No siempre es posible evitar conducciones de agua dentro de las salas destinadas a ordenadores o centros técnicos o de telecomunicaciones, incluso la instalación de los sistemas específicos de estos locales, implican tener conductos de agua en su interior.

Las fugas de fluidos, si no se descubren a tiempo, pueden causar daños en los equipos o pérdidas de información.

Armarios ignífugos

Los equipos y soportes de datos que se encuentran en locales sin medidas especiales de seguridad, son especialmente vulnerables ante riesgos de manipulación indebida, incendios o radiaciones, que pueden alterar y destruir el contenido de los mismos.

Las copias de back-up o los servidores de respaldo, también han de contar con protección ante eventuales riesgos que puedan afectar al servicio que deben proporcionar.

Los **armarios ignífugos** para para datos, rack y equipos, proporcionan la más alta protección ante todo tipo de agentes externos como incendios, explosivos, acceso, gases, radiaciones y daños criminales.

La combinación de acero, células de hormigón y materiales especiales que absorben el calor, aseguran el mayor nivel de seguridad.

La protección certificada con la norma VDMA24991, asegura unos niveles de seguridad S120DIS.

Todos los armarios ignífugos están equipados con un tipo de cierre hermético de autosellado ante agentes agresivos externos (gas, fuego, agua, etc.), con el que basta impulsar la puerta a su posición cerrada, sin necesidad de cerrar con la llave.

Sistema de cableado estructurado

Un Sistema de **Cableado Estructurado** (SCE) se define en el entorno de un CPD como el conjunto de elementos, incluyendo paneles de terminación, módulos, conectores, cable, y latiguillos, instalados y configurados para proporcionar conectividad principalmente de datos desde los repartidores designados hasta las rosetaso puntos de planta que dan

servicio al equipamiento ubicado en el CPD (Host, dispositivos de almacenamiento, etc).

Las aplicaciones estándar soportadas deben incluir, entre otras, IEEE 802.3, 1OBASE-T, lOOBase-TX, y 100BASE-FX, 1000BASE-SX, 1000BASE-LX. Además, los enlaces o canales deben ser capaces de soportar las aplicaciones emergentes de alta velocidad como 10 Gigabit Ethernet, 1OGBASE-SR , l000Base-T, 1000 Base-TX y ATM a 52/155/622/1000 Mbps, Fiber Channel, etc., pensando principalmente en los enlaces entre servidores y backbone.

Extinción mediante agua nebulizada

La rápida expansión de los negocios mundiales a través de internet ha creado la necesidad de instalaciones adecuadas para los ordenadores y equipos de telecomunicaciones. Estas intalaciones deben tener acceso a las redes de comunicaciones y a las fuentes de alimentación, por lo que deben gozar de un alto nivel de seguridad y protección contra incendios.

HI - FOG es el sistema cada vez más utilizado en estas instalaciones para proteger no sólo los equipos informáticos y de telecomunicaciones, sino las salas de generadores y conmutadores de emergencia. En principio, los clientes eran escépticos sobre la instalación de un sistema a base de agua para salas de ordenadores y telecomunicaciones. Pero mediante los rociadores HI - FOG de acción previa, cuyas tuberías sólo se llenan de agua cuando se produce el segundo nivel de alarma, el riesgo de descarga accidental es mínimo.

El uso de la innovadora bomba de gas GPU asegura que, en caso de incendio, la descarga de agua es muy baja y sólo se produce, naturalmente, en la zona del fuego. La misma unidad

ofrece grandes ventajas sobre los sistemas gaseosos, pues protege todas las zonas con riesgo de incendio en la instalación, incluso las salas de máquinas y generadores de emergencia. ! Y los costes de recarga son mínimo!

La tecnología HI-FOG para salas de datos

Además de proteger las salas de ordenadores, Marioff suministra normalmente una "solución total" con su sistema DAU (Double - cylinder Accumulator Unit), para proteger salas con equipos de alta tensión, como los generadores y fuentes de alimentación. La unidad MAU (Machinery space Accumulator Unit) se utiliza para proteger las salas de generadores de emergencia y otros servicios mecánicos. El sistema se complementa con componentes como subsistemas de detección y paneles de control, con todos los cuales se ofrece una solución llave en mano.

La GPU (Gas- driven Pump Unit) de Marioff es ideal para oficinas y centros de datos por dos razones: su innovador sistema de alimentación es totalmente independiente de cualquier red externa y por tanto puede funcionar durante un corte de corriente mediante nitrógeno o aire a presión.

Además, la GPU produce una mínima descarga de agua, reduciendo de forma significativa los daños sobre los equipos y sistemas críticos.

Sistemas HI-FOG para salas de ordenadores

Marioff suministra además sistemas especiales para pequeñas salas de ordenadores, basados en la detección rápida del humo en vez de los sistemas convecionales. El principal objetivo de estos sistemas es la absorción del humo, que es el componente que más daño causa a los equipos.

Sistema funcional y de fácil manejo

En cuanto a funcionalidades del sistema, PHENIXIA ha optado por la innovación:

- Interfaz de control con idioma seleccionable Número ilimitado de consolas de operador. Los puestos de operador no están sujetos a licencia.
- Posibilidad de transmisión de audio bidireccional con cámaras equipadas con micrófono/altavoz y codificación MPEG4.
- Cámaras alimentadas bajo el estándar poE (power over Ethernet), que utiliza un único cable de cuatro pares trenzados para transmitir las señales y alimentar la cámara, con el ahorro consiguiente en infraestructura eléctrica y en mantenimiento respecto a un sistema con cámaras analógicas. Gestión de permisos granular: por ejemplo, se puede denegar el permiso a mover cualquier cámara domo mientras se permite la activación de la ronda (captación secuencial de varias posiciones predefinidas).
- Velocidad de grabación variable, en función de la actividad detectada por las cámaras. El usuario puede definir varias ventanas con umbrales distintos. En situación de detección de movimiento, la grabación se realiza a la máxima velocidad (25 imágenes por segundo), mientras que en situaciones estáticas se reduce la velocidad de grabación a unas pocas imágenes por segundo.
- Modos de visualización: 1, 4, 16, 32 ó 64 cámaras.

- Formatos de imagen MJPEG y MPEG4.

Aplicaciones

Entre las aplicaciones de este nuevo sistema, se cuentan las siguientes:

- Vigilancia de instalaciones industriales.
- Vigilancia y control de vehículos en aparcamientos.
- Conteo de personas.
- Reconocimiento de defectos en cadenas de producción.
- Mapas de ocupación en establecimientos comerciales.
- Complemento en controles de acceso.
- Control de calidad: fichas visuales de acabado de producto.
- Vigilancia y control de disposición de producto en franquicias.
- Centralización del video vigilancia en empresas con multitud de ubicaciones geográficas.

6.1.2- Robo o sabotaje: Control de acceso físico y vigilancia mediante personal y circuitos cerrados de televisión (CCTV).

CCTV y Sistemas de Videovigilancia

Los sistemas de CCTV o videovigilancia permite la visualización remota de las cámaras en cualquier momento.

El **Circuito Cerrado de Televisión** o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de vídeovigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

Las cámaras pueden estar sostenidas por una persona, aunque normalmente se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden

estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes debe ser excelente, ya que se puede transformar de niveles oscuros a claros... Todas estas cualidades hacen que las soluciones CCTV de Accesor ofrezcan el máximo nivel de confianza.

La función de un **detector de movimiento** es la de detectar cualquier cosa o persona en movimiento. Se encuentran, generalmente, en sistemas de seguridad o en circuitos cerrados de televisión.

El sistema puede estar compuesto, simplemente, por una cámara de vigilancia conectada a un ordenador, que se encarga de generar una señal de alarma o poner el sistema en estado de alerta cuando algo se mueve delante de la cámara. Además, con el detector de movimiento se maximiza el espacio de grabación, grabando solamente cuando se detecta movimiento.

- **Cámaras** Las cámaras son el elemento central en cualquier tipo de solución de CCTV. Es por ello que desde ACCESOR trabajamos con los productos que nos ofrecen una mejor calidad, fiabilidad y durabilidad.

Proyectamos y configuramos la instalación de CCTV más acorde con sus necesidades:

- Cámaras fijas o domos con movimiento.

- Equipos con zoom óptico de hasta 22x y zoom electrónico de 10x

- Color o Monocromo, con conmutación automática.

- Equipos con visión nocturna e infrarrojos.

- Cámaras con autoenfoque y estabilizador automático de imagen.

- Sistemas conectados a internet para supervisión remota.

- **Grabadores** El videograbador es el núcleo del sistema de videovigilancia ya que en él se almacena toda la información recogida durante el tiempo de vigilancia. Actualmente, los mecanismos de compresión de imagen han hecho que estos dispositivos sean capaces de almacenar muchas horas de grabación.

Lector automático de Matriculas CLPR-W-ACR

La forma más económica y sencilla de instalar un Lecrtor de Matrículas en nuestro sistema de Control de Accesos.

El CLPR-W-ACR es un sistema de lectura automática de placas de matrículas, diseñado para que su instalación y gestión sean muy sencillas y fiables. Lectura de matriculas en negativo mediante los leds IR, asegura la autentificación de placas de matriculas y permite lecturas con cualquier tipo de luz, incluso a pleno sol. El sistema puede funcionar de dos formas: autónoma o controlada.

Forma autónoma:

Cada vez que la unidad CLPR reciba un contacto de presencia, envía una solicitud al PC donde comprueba si en su base de datos ese código es válido, en caso afirmativo, pasa un comando a la unidad CLPR, para que dé un contacto de apertura a la barrera o pilona.

Forma Controlada:

Cuando la unidad CLPR detecta la presencia de un vehículo, captura la imagen y transforma la descripción de la placa en un código que se envía mediante un protocolo wiegand a la central de control de accesos OPEN4, TPL4 o Mega. Si este código está autorizado, la central activa el pase.
La unidad CLPR, actúa como un lector más, por tanto, la unidad funciona sin necesidad de estar en conexión con el PC permitiendo conectar en una

misma central distintas tecnologías como proximidad, manos libres (Free), Radio (Mandos Go-Pro).... La gestión de usuarios se realiza en el Amadeus 5 con todas sus funciones y aplicaciones como si se tratara de un lector más.

Todas las soluciones de CCTV permiten su integración con los sistemas de Control de Accesos de Accesor. De este modo, podrá comprobar en cualquier momento si sus empleados hacen un uso adecuado de las acreditaciones que dan acceso a su empresa.

Además en ACCESOR le asesoraremos y ayudaremos en todos los pasos que se deben seguir para cumplir todos los requisitos indicados en la LEY ORGANICA 15/1999, DE PROTECCIÓN DE DATOS.

6.1.3- Condiciones atmosféricas y naturales adversas (Ubicación de sistemas, centros de respaldo en ubicación diferente al centro de producción, mecanismos de control y regulación de temperatura, humedad, etc.)

Ubicación del Centro de Proceso de Datos (CPD) y Características Generales del Edificio.

Cuando se escoge un lugar para ubicar el CPD, si el problema de los metros cuadrados no existiese en las zonas urbanas donde se concentran las instalaciones de sistemas informáticos, lo ideal sería construir locales que respondan perfectamente a las necesidades del servicio informático, pero a menudo la empresa dispone de locales vacíos o libera algunos locales previamente ocupados e implanta los de los servicios informáticos. Esta práctica que puede parecer económica, no lo es forzosamente en la medida en que la adecuación de esos locales imponen modificaciones importantes que gravan considerablemente el precio resultante final.

Por otra parte, los locales informáticos no se limitan únicamente a las salas que abrigan los materiales específicos, ya que son indispensables locales anejos, tales como los servicios de estudio y de programación. Su instalación debe regirse por reglas de seguridad que deberán

seguirse imperativamente. Estas reglas de seguridad conciernen tanto a los materiales y al personal como a la protección contra los riesgos de cualquier naturaleza.

En la construcción de un edificio para instalar un sistema informático, lo primero que se debe elegir es su emplazamiento. La elección del emplazamiento, aparte de las consideraciones de tipo estratégico o de tipo económico para la entidad, precisa ser seguro frente a los riesgos de naturaleza física.

La sala en la que va a albergarse la computadora es donde se centran los mayores cuidados de la instalación de un sistema informático.

Aparte de la infraestructura normal de un edificio, la sala de la computadora precisa cosas tales como falso piso, falso techo, insonorización, climatización y suministro eléctrico.

Falso Piso

Un falso piso está constituido por baldosas independientes y removibles en madera o metal, de dimensiones variables y recubiertas de un revestimiento plástico. Las baldosas reposan sobre soportes de altura regulable. Estos soportes se colocan sobre el pavimento de base que debe presentar una superficie lisa y estar provisto de un recubrimiento antipolvo.

La altura del falso piso está comprendida normalmente entre 0.05 y 0.075 m, pudiéndose conseguir alturas mayores, bajo encargo, en casos especiales en que se precise que sea visitable. Su resistencia a la carga debe ser equilibrada, variando según los materiales y los fabricantes entre 500 y 750 kg/m², calculándose la resistencia media a partir de la unidad central del sistema informático. La carga debida al falso piso varía entre 30 y 50 kg/m².

Debe ser robusto e indeformable; resistir a la humedad, a la corrosión y a las cargas mal repartidas, sin hundirse ni desplazarse. Las baldosas son totalmente intercambiables y permiten asegurar la estanqueidad para la circulación del aire, no transmitiendo las vibraciones.

Cada baldosa está revestida de un semiaislante, cuyas características eléctricas y resistividad asegura el aislamiento de cargas estáticas y la protección de las personas. La parte metálica que recubre la parte inferior de las baldosas, además de permitir un primer aislamiento en caso de incendio, junto con los soportes, deben unirse eléctricamente a tierra, cuya resistencia eléctrica debe ser tan baja como sea posible (2 a 3 ohmios),

constituyendo también de esta forma un blindaje antimagnético.

Para permitir los movimientos de material y/o los desplazamientos de carros, los accesos a las salas están equipados de una rampa de desnivel variable para una pendiente comprendida entre el 10 y el 12%. Esta rampa está generalmente recubierta de goma estriada, antiderrapante.

Ruido.

Debe considerarse también la posibilidad de altos niveles de ruido en el entorno de trabajo que perturban el mismo e incluso pueden llegar a producirse molestias en la salud de los trabajadores. En caso de ser el nivel de ruido muy alto, será preciso adoptar las medidas oportunas de insonoración; esta situación puede producirse en sistemas que utilicen gran número de impresoras o lectores de fichas.

La insonoración tiene por objeto el eliminar al máximo las vibraciones sonoras en el interior del local y evitar su propagación al exterior. El ruido se produce por la propagación de ondas emitidas por las vibraciones de una fuente que son transmitidas por el medio ambiente. Está compuesto de sonidos de frecuencias variables

INSTALACIONES ELÉCTRICAS Y TEMPERATURA AMBIENTAL.

Suministro de Energía Eléctrica.

Todas las computadoras dependen vitalmente del suministro de energía eléctrica. Si este suministro falla, el sistema queda totalmente fuera de juego inmediatamente y durante el tiempo que el fallo dure, pudiendo también verse afectados los sistemas de aire acondicionado y de protección de incendios. Los paros en el acondicionamiento del aire pueden originar pérdidas de información, que pueden llegar a ser parciales o totales, temporales o definitivas, en discos y cintas.

Por supuesto que la pérdida total de suministro no es la única fuente de problemas: variaciones de voltaje o frecuencia, por encima de los valores especificados por los fabricantes de la computadora, incluso si es sólo por breves intervalos de tiempo, pueden provocar un mal funcionamiento en los equipos.

Normalmente, las instalaciones reciben su alimentación de los suministros públicos de

electricidad, y debe considerarse la posibilidad de fallos de ese suministro debido a daños accidentales en las subestaciones, cables subterráneos, daños por tormentas en líneas aéreas, excesos de carga en casos de fuerte demanda o, incluso, acciones terroristas contra el sistema de alimentación.

Algunas perturbaciones pueden ser de tan corta duración que son muy difíciles de detectar y de relacionar con fallos en el funcionamiento de los equipos.

Si hay posibilidades de que el suministro sea de objeto de perturbaciones, puede ser necesario disponer de una fuente de alimentación no sujeta a la influencia de las perturbaciones, considerando incluso la posibilidad de instalar filtros o un motor-alternador que actúen como un amortiguador entre el suministro y la computadora que pueden vencer variaciones en la alimentación que tengan duraciones por debajo de aproximadamente 100 milisegundos.

Para variaciones de más larga duración, se deben tomar medidas especiales, tales como la incorporación de un volante en el juego motor-alternador.

Para perturbaciones más largas o incluso interrupciones, deben considerarse algunas formas de fuentes alternativas de energía.

El sistema más completo y más complejo es el que se denomina habitualmente SAI (Sistema de Alimentación Ininterrumpida), que es una unidad de conversión de energía eléctrica que proporciona corriente alterna de alta calidad. Acepta diversos suministros de energía de entrada, dentro de unos parámetros especificados, y los convierte en la energía de salida necesaria para el equipo de proceso de datos, dentro de los parámetros que éste precisa. Las entradas de energía aceptables por SAI incluyen los suministros de las compañías, generadores locales o baterías

Acondicionamiento de Aire.

Es recomendable que todas las computadoras tengan una atmósfera libre de polvo, dentro de unos límites especificados de temperatura y humedad relativa. Tal control es sólo posible mediante el uso de equipos de climatización, que realicen las funciones básicas de mantenimiento de la temperatura del aire dentro de los límites requeridos, bien mediante la extracción del calor, o bien suministrando o haciendo circular el aire y manteniendo la humedad relativa.

Es aconsejable recomendar que el equipo se utilice y almacene a una temperatura de 21 ± 1°C y una humedad relativa de 50% ± 5%

El aire acondicionado también impide la entrada de polvo mediante presurización de la sala de la computadora con aire fresco para crear un flujo hacia el exterior del aire procedente vía ventanas o cualquier filtración por otro lugar.

La seguridad puede verse comprometida por los daños que las partículas de polvo pueden producir en las cabezas y en las superficies de grabación. El polvo puede originarse o bien procedente del exterior de la sala de la computadora producido por actividades en habitaciones o edificios anejos, o por operaciones industriales cercanas, o bien en el interior de la misma, debido a manipulaciones de papel, desprendimientos de muros o paredes, o fibras procedentes del techo o de los aislamientos de la sala. Una vez que se ha identificado la procedencia del polvo, puede ser posible vencer el problema en sus fuentes. Las personas que acceden a la sala de la computadora pueden introducir también polvo en las ropas y en el calzado.

6.2- Busca un único SAI para todos los sistemas informáticos del aula. Justifica tu respuesta y compara la misma con una solución de diferentes SAIs a repartir en el aula. Analiza aspectos como tipos de SAI y cálculo energético necesario.
Se sugiere visitar entre otros los enlaces: http://www.newsai.com
http://www.apc.com/es/ http://www.mgeups.co.uk/
http://www.riello-ups.com/?es/configuratore http://www.emersonnetworkpower.com/

Liebert PSI-XR

Liebert PSI-XR is a compact, line-interactive UPS system designed especially for IT applications such as network closets and small data centers.

The flexible design of Liebert PSI-XR allows the unit to be configured as a self-standing tower or to be rack-mounted within a 2U space. It is available in four capacities, in both 230V or 120V models.

The UPS features an innovative line-interactive design incorporating buck/boost automatic voltage regulation technology. This protects against utility voltage fluctuation by raising and lowering utility power to the level needed by the connected equipment. It also allows the UPS to prolong battery life by maximizing its time on utility power before going to battery.

Ideally suited for

- PC's
- Network workstations
- Servers
- Network closets
- Large network peripherals
- VoIP

Liebert PSI-XR Standard Features:

Flexibility

- Six to seven battery-backed outlets
- Configurable input voltage window
- Rotatable Display Panel
- Automatic Frequency Sensing
- Multiple Communications Options (USB, SNMP and Contact Closure)

Higher Availability

- Data line surge protection
- Advance early warning of UPS system status
- Full sequenced battery testing
- Lightning and surge protection
- Remote emergency power off
- User replaceable hot swappable batteries
- Ample battery backup time at full load when utility fails, for an orderly shutdown of connected equipment

Lowest Total Cost of Ownership

- 0.9 Output Power Factor to provide more power for your protected load, and more energy efficient operation
- Wider input voltage window
- Reduced installation time and costs
- Two-Year Warranty Standard

6.3-Instalación de una cámara IP y transmisión de la imagen por una red LAN.
Descarga este manual del proceso de instalación de esta cámara IP OVILINK OC-600 y su gestión mediante software.
http://www.ovislink-espana.com/index.php?sec=99
Busca otros manuales de otras cámaras IPS y compara los procesos de instalación.
Elabora un documento con dicha comparación (al menos dos cámaras IPs).

6.4-Instalación de un SAI o UPS en un rack y su posterior uso.

Descarga estos manuales y analiza el proceso de instalación del SAI en un rack y su gestión mediante software.
http://tools.mgeops.net/download/intl/products/evolution/Evol_Ins_and_User_Man.pdf
http://powerquality.eaton.com/Products-services/legacy/patriot-info.asp

Busca otros manuales de otros SAIs y compara las características de este software de SAI .
Elabora un documento con dicha comparación (al menos dos SAIs).

6.5-Ampliar el estudio realizado del apartado a) del aula con la implantación de sistemas biométricos

Se sugiere visitar los enlaces:
http://www.zksoftware.es/ http://www.biometriaaplicada.com/
http://www.kimaldi.com/productos/sistemas_biometricos/
http://www.agedum.com/BioCloser/tabid/110/Default.aspx
http://www.biopassword.com/

Hemos decidido poner como defensa extra el siguiente hardware de sistemas biométricos:

- tecnologías de hardware y software para reconocimiento de huella digital en ambientes transaccionales, poblacionales y civiles (AFIS) modelo Verifier 300 LC 2.0

El Verifier 300 LC (Lexan Case) de Cross Match Technologies captura impresiones dactilares que aseguran resultados acertados y confiables en programas de identificación, verificación y registro de las personas.

Los Verifier de Cross Match han sido entregados en más de 5.000 aplicaciones alrededor del mundo en una gran variedad de proyectos que incluyen documento nacional de identidad, control fronterizo, licencias de conducir, seguridad en bancos y control de acceso físico.
El Verifier 300 LC tiene conectividad USB y por su tamaño compacto es fácilmente integrable en aplicaciones existentes. Existe también una versión kiosco que facilita la integración. El Verifier 300 LC produce imágenes de impresiones dactilares de alta calidad manteniendo una precisión geométrica de menos de un píxel. Construido con un liviano pero resistente policarbonato lexan, presenta alta durabilidad.

La línea de productos Verifier de Cross Match es conocida por su superior calidad de imagen, consistencia entre unidades, durabilidad y bajo mantenimiento. Los Verifier son ideales para control de fronteras, registros de las personas, control de acceso en correccionales, licencias de conducir, aplicaciones bancarias y de tiempo y asistencia. Estos lectores proveen imágenes de alta calidad forense y años de operación confiable. Verifier 300 LC versión Kiosco

Beneficios del Verifier 300 LC

- Cable USB integrado
- Bajo mantenimiento
- Resistente, durable y portátil (0,45 kg)
- Imágenes consistentes y de alta calidad forense
- Iluminación mejorada puede captar Imágenes de dedos oscuros, con manchas, o marcas

Características del Verifier 300 LC	Requerimientos del sistema	Especificaciones
• Área de captura amplia (30 mm x 30 mm) • Alto contraste cumple con el ANSI /NIST • La conexión USB elimina la necesidad de una tarjeta de video • Liviano (0,45 kg / 1 lb) • Lentes asféricas patentadas • Certificaciones FCC, UL, CE	Uno de los siguientes sistemas operativos: • Windows XP Profesional (SP1 y USB SDK 2.000 o posterior) • Windows 2000 Profesional • Windows ME • Windows 98 SE • Windows 98 • Windows 95 OSR 2.1 (4.03.1212 soporte técnico limitado) • Pentium compatible 133 Mhz o más • 32 MB RAM • 10 MB de espacio en disco disponible • Puerto USB 1.0 compatible (Puerto USB 2.0 compatible con USB SDK version 2.000 o más)	**Resolución** 500 DPI ± 1% **Función de Transferencia Modular (MTF)** 50% a 10 ciclos por milímetro en el platen **Linearidad y Rectilinearidad** Menos de un píxel (promedio) **Uniformidad de iluminación** Menos del 50% de variación del centro a los rincones **Área de Captura** 30.5 mm x 30.5 mm (1.2" x 1.2") **Salida (Digital)** Universal Serial Bus (USB) **Potencia requerida (Digital)** 5 V DC provisto por la PC vía puerto USB **Rango de Temperatura** 2° a 38°C (35° a 100°F) **Rango de Humedad** 10-95% no condensada; resistente al agua **Peso** 0.45 kg (1 lb) **Dimensiones (Alto x Largo x Ancho)** 62 mm x 162 mm x 83 mm (2.45" x 6.38" x 3.25")

El precio de dicho producto no es elevado permitiendo aumentar la seguridad de nuestros ordenadores. Se debe poner 1 en cada ordenador. Además incluye un sistema antirrobo, de modo que si alguien lo roba, este bloqueara el ordenador y sin un autentificado especial, no se podrá desbloquear

Biometría por voz

BioCloser es un sistema de control de acceso biométrico. Admite distintos niveles de seguridad en función de la aplicación y utiliza la voz como método de autenticación. Algunas de las cualidades más importantes de la voz son su naturalidad, versatilidad y escasa intrusividad, que hacen de ella un método biométrico agradable para el usuario y adecuado para un buen número de aplicaciones.

BioCloser dispone de 6 funcionalidades principales en orden creciente en cuanto al nivel de seguridad:

- Swing: Es la funcionalidad más sencilla de BioCloser. Utiliza el reconocimiento del mensaje para el acceso a un recinto. Supone una autenticación de usuario con un alto nivel de vulnerabilidad, cualquier otra persona podría averiguar el código y usarlo para su acceso.
- Open Up: Evolución de Swing que realiza el reconocimiento biométrico del usuario a través de su voz. Este sistema permite realizar un control de acceso de forma segura, certificando la identidad del usuario.
- SecureLogin: Utiliza un identificador para reconocer al usuario y dos números aleatorios para evitar grabaciones. El reconocimiento biométrico se realiza sobre la secuencia completa de dígitos.
- Alarm: Funcionalidad que puede utilizarse en combinación con cualquiera de las descritas con anterioridad. Incorpora la conexión a una central de alarmas a través de Internet. El usuario podrá recibir mensajes sobre los eventos de acceso que se den en el sistema.
- SecureData: Funcionalidad que puede utilizarse como complemento de cualquiera de las anteriores. Su objetivo es la protección de los datos biométricos de los usuarios mediante el soporte cifrado y acceso con smartcards.
- Además de las funcionalidades comentadas, BioCloser permite la incorporación de tecnologías biométricas adicionales tales como el reconocimiento facial o el reconocimiento de huellas dactilares.
  Otro aspecto a destacar es el control a múltiples accesos. Con esta funcionalidad se podrán incluir permisos para los distintos usuarios según el punto de entrada

El modelo elegido es este:

Equipo fiable, de fácil uso y grandes prestaciones para el control de horario y de personal entradas/salidas. Incluye software con completos listados. Fácil instalación y configuración. También disponemos de otros modelos para cualquier necesidad.

CARACTERÍSTICAS TÉCNICAS Y GENERALES:

Capacidad: Hasta 1.600 huellas dactilares.
Huellas dactilares por usuario: De 1 a 10 huellas.
Modo de verificación: 1: 1 y 1: N.
Fichajes almacenados: Hasta 50.000 sin descargar al PC.
Comunicación: USB, Ethernet y Pen Drive.
Tipo de lector: Óptico (sensor ZK).
Teclado: 16 teclas.
Display: 4 líneas y 20 columnas.
Tiempo de registro: - 2 seg.
Tiempo de verificación: - 1 seg.
Alimentación: 5 V.
Batería de Alimentación de 2 a 3 horas: Opcional
Dimensiones: 182 mm x 126 mm x 50 mm.

Permite la visualización de mensajes a usuarios y del Nombre (Alias) de la persona que está fichando.
Distintos modos de operación: Sólo huella, Código + Huella y Código + Password
Incorpora puerto USB para comunicación con el PC o para la descarga de fichajes a una unidad portátil (Pendrive o Flash Disk)
Cambio de hora automático verano-invierno.
Permite la respuesta del terminal al fichar a través de voz.
Admite la introducción de ilimitadas incidencias (Fumar, Comida, Asuntos, Médico, etc…)

Este modelo permitirá que en la sala solo puedan acceder los usuarios identificados en la voz, además su precio no es elevado y aun sigue en stock.