

**Seguridad
Y alta
Disponibilidad
Teoría
y
Ejercicios
(2012-2013)**



Seguridad y Alta disponibilidad

Capítulo 1 Principios de Seguridad y alta disponibilidad.

Principales objetivos de la seguridad informática:

- Detectar los problemas y amenazas a la seguridad (minimizar y gestionar los riesgos)
- Garantizar la adecuada utilización de recursos y aplicaciones
- Limitar perdidas y conseguir la recuperación del sistema en caso de incidente de seguridad
- Cumplir con el marco legal y requisitos a nivel organizativo.

Es necesario estar al día en esta materia.

Webs de interés en Seguridad:

http://www.inteco.es/blogs/inteco/Seguridad/BlogSeguridad/ultimos_articulos/

<http://www.securitybydefault.com/>

<http://www.hispasec.com/>

<http://www.elladodelmal.com/>

la **Seguridad absoluta** no es posible, por seguridad se entiende las Técnicas encaminadas a obtener altos niveles de seguridad, por ello se habla de **Fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de él), consiste básicamente en garantizar tres aspectos:

- **Confidencialidad:** Cualidad de un mensaje, comunicación o datos por la que solo pueda ser entendido por la persona a la que es enviado.
- **Integridad:** Cualidad de un mensaje, comunicación o datos que permite comprobar que no ha sido alterado.
- **Disponibilidad:** capacidad de un servicio, sistema o datos para ser accesibles y utilizable por los usuarios o procesos cuando se requiera.

Tienen que existir estos tres aspectos para que haya seguridad

Estos tres conceptos se estudian junto con:

- **Autenticacion:** Verificar que un mensaje pertenece a quien el documento dice (usuario, login, contraseña).
- **No repudio o irrenunciabilidad:** Permite probar la participación de las partes en una comunicación.
 - No repudio en origen: El emisor no puede negar el envío, la prueba la crea el emisor y la recibe el destinatario.
 - No repudio en destino: El receptor no puede negar la recepción ya que el emisor tiene pruebas de la recepción, creadas por el receptor y recibidas por el emisor.

Autenticacion:

- Algo que se sabe por ejemplo una contraseña de acceso
- Algo que se tiene por ejemplo una tarjeta de acceso
- Algo que se es por ejemplo la huella dactilar

Orden requisitos seguridad: Disponibilidad → Confidencialidad → Integridad → Autenticacion → No repudio

Confidencialidad, La confidencialidad se puede conseguir encriptando archivos y programas.

- En windows es posible encriptar carpetas y archivos mediante **EFS** (Encrypted File System), tras seleccionar un archivo o carpeta en propiedades y opciones avanzadas está la opción “Cifrar contenido para proteger datos”
- Existe un programa llamado **LockNote** que es una especie de bloc de notas que al guardar encripta la información con contraseña, el archivo resultante es un ejecutable .exe que contiene el programa y el texto contenido (como puede ser datos de usuarios y contraseñas, datos bancarios, etc.).

Integridad: Existe un malware denominado **rootkit**, que es un programa que sustituye los ejecutables binarios del sistema para ocultarse mejor, pudiendo servir de puerta trasera o backdoor para la ejecución remota, en windows la utilidad **System File Checker (SFC)** comprueba la integridad de los archivos de sistema.

- En Windows, en una terminal (cmd) ejecutamos **sfc /scannow** y se comprobaran todos los archivos de sistema (requiere que este insertado el CD de instalación para la comparación).
- En Linux se puede comprobar el Cheksum de un archivo con el comando **md5sum "fichero"** y comparar el resultado con el checksum original.
- **Rootkit hunter** es una herramienta mas completa bajo GNU/Linux para revisar permisos de los ejecutables, buscar rootkits conocidos y comprobación de la integridad de archivos de sistema.

Disponibilidad, Identificar y analizar la disponibilidad de servicios o servidores, puertos abiertos y versiones de sistemas operativos que lo soportan. Nmap se utiliza en auditorias de seguridad (y también se puede utilizar en un primer ataque). Búsqueda de posibles vulnerabilidades por medio de:

- www.securityfocus.com Facilita informes sobre vulnerabilidades en aplicaciones y sistemas operativos.
- Nessus4 (www.nessus.org) Aplicación que detecta vulnerabilidades, para windows y Linux.
- MBSA (Microsoft Baseline Security analyzer), herramienta diseñada para analizar el estado de seguridad según recomendaciones de Microsoft.
- Nmap (www.insecure.org/nmap/) aplicación en modo comando o gráfico (znmap) que proporciona, versiones de sistemas operativos instalados, direcciones MAC e IP, puertos abiertos o cerrados y versiones de aplicaciones.

Del estudio y análisis de las **vulnerabilidades** (agujeros de seguridad de un sistema) se aprovechan los desarrolladores de exploits. El fin del **exploit** puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio (introduciendo **payload**, que es como un malware que mete el exploit) o como origen de otros ataques a terceros, hay aplicaciones que poseen un conjunto de exploits para aprovecharse de las vulnerabilidades conocidas como “**metasploits**”

Recomendación

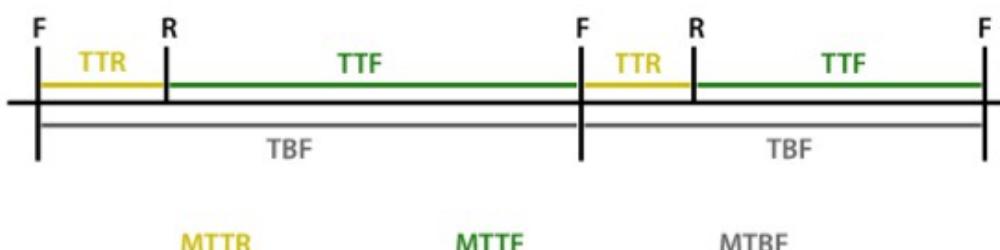
- ✓ Actualizar los sistemas.
- ✓ Aplicaciones configuradas con actualización automática.
- ✓ Activar la notificación de actualizaciones automáticas.
- ✓ Controlar la veracidad antes de instalar actualizaciones.

Actualmente existe software malicioso (malware) que sobrescribe las actualizaciones de aplicaciones conocidas.

Alta Disponibilidad, que es la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones, debido principalmente a su carácter critico, hay dos tipos de interrupciones:

- **Interrupciones previstas**, por ejemplo para realizar cambios o mejoras de hardware o software.
- **Interrupciones imprevistas**, son acontecimientos imprevistos (virus, desastres naturales, fallos hardware, etc.)

Las **métricas** utilizadas para medir la disponibilidad y fiabilidad de un sistema son **MTTF**, **MTTR** y **MTBF**. Si F indica el momento en el que el dispositivo falla y R el momento en que está de nuevo disponible, gráficamente tenemos:



TTR (Time to repair), tiempo que se necesita para volver a poner en marcha el sistema

TTF (Time to failure), tiempo que pasa hasta que falla

TBF (Time between failures), tiempo entre fallos

- **MTTF** (Mean time to failure) Tiempo medio hasta que se produce un fallo.
 - $MTTF = (\text{Tiempo total de funcionamiento correcto}) / (\text{no fallos})$
- **MTTR** (Mean time to repair) Tiempo medio que se tarda en poner de nuevo en marcha el sistema.
 - $MTTR = (\text{Tiempo total de inactividad}) / (\text{no fallos})$
- **MTBF** (Mean time between failures) Tiempo medio entre fallos.
 - $MTBF = (\text{Tiempo total}) / (\text{no fallos})$

Existen distintos niveles de disponibilidad, el mayor **nivel de exigencia** se obtiene **con los 5 nueves**: 99,999%, que acepta 5 minutos de inactividad al año.

Ejercicio de ejemplo:

1. Calcular el MTTR, MTTF y MTBF de un servidor que ha tenido 5 caídas en los últimos 3 meses. Las tres primeras se solucionaron en 5 minutos, pero las dos últimas supusieron un tiempo de inactividad de 30 y 40 minutos respectivamente.

5 fallos en 3 meses

3 meses -> $24 \times 60 \times 90 = 129600$ minutos

5 fallos -> $5 + 5 + 5 + 30 + 40 = 85$ minutos

$129600 - 85 = 129515$ minutos de funcionamiento correcto

$MTTR = 85 \text{ m} / 5 = 17 \text{ m}$

$MTTF = 129515 / 5 = 25903 \text{ m}$

$MTBF = 129600 / 5 = 25920 \text{ m}$

2. ¿Qué porcentaje de disponibilidad ha tenido el servidor del caso anterior?

$25903 / 25920 = 0,9993 \rightarrow 99,93\%$

Otra forma quizás más intuitiva:

$\text{Tiempo funcionamiento/Tiempo total} = 129515 / 129600 = 0,9993 > 99,93\%$

3. ¿Cuánto tiempo puede estar inactivo al mes un equipo para conseguir la disponibilidad de 5 nueves?

$1 \text{ mes} \times 30 \text{ días/mes} \times 24 \text{ horas/mes} \times 60 \text{ min/hora} = 43200 \text{ minutos tiene un mes}$

$100 \rightarrow 43200 \text{ m}$

$99,999 \rightarrow x$

$x = 43200 \times 99,999 / 100 = 43199,568 \text{ m}$ que tiene que estar funcionando

$43200 - 43199,568 = 0,432$ minutos (o sea, 25,92 s) de inactividad al mes, como máximo

Nota: si se deja instalando algo en Linux, se puede programar el apagado automático, ejecutando en otra terminal otro comando al de un tiempo, con: **sudo shutdown -h +60** en este caso 60 indica al de 60 minutos se apagara.

Elementos vulnerables en el sistema informático y **que hay que proteger**:

- El software
- El hardware
- Los **Datos** es el elemento principal a proteger y el mas difícil de recuperar.

Las medidas de seguridad se contemplan a diferentes niveles: locales, personales/individuales y globales.

La seguridad informática desde diferentes perspectivas:

- | | |
|---|---|
| ➤ Seguridad pasiva | Seguridad física, ambiental y copias de seguridad. |
| ➤ Seguridad lógica | Control, usuarios, privilegios, contraseñas, software de seguridad antimalware y cifrado de la información. |
| ➤ Seguridad en redes corporativas | Protocolos/aplicaciones seguras, SSH, TLS/SSL y VPN |
| ➤ Configuraciones de alta disponibilidad | Redundancia RAID, balanceo de carga, virtualización. |
| ➤ Normativa legal en materia de seguridad | LOPD y LSSICE |

Las **amenazas** pueden ser provocadas por personas, condiciones físico-ambientales y software o lógicas.

- **Amenazas provocadas por personas**
 - ➔ Dentro de una organización **el propio personal**.
 - ➔ **Hacker**, que es un experto o guru en aspectos técnicos relacionados con la informática (White hat o Hacker y Black hat o Crackers)
 - **Newbie** Hacker novato
 - **Wannabe** Le interesa el hacking pero al estar empezando no es reconocido por la elite.
 - **Lammer** o Script-Kiddies Hacen hacking utilizando programas que buscan y descargan.
 - **Luser** (looser + user) termino para referirse a los usuarios comunes despectivamente.
 - ➔ **Pirata informático**, ciberdelincuente, personas dedicadas a realizar actos delictivos y perseguidos legalmente.
 - **Amenazas físicas y lógicas**
 - ➔ Las amenazas físicas y ambientales afectan a las instalaciones y/o el hardware que contienen.
 - Robos, sabotajes, destrucción de sistemas
 - Cortes, subidas y bajadas bruscas de suministro eléctrico.
 - Condiciones atmosféricas adversas, humedad, temperatura extrema.
 - Catástrofes naturales.
 - Interferencias electromagnéticas.
 - ➔ **Amenazas lógicas** (software o código que de una u otra forma afecta al sistema).
 - **Herramientas de seguridad**, que detectan y solucionan fallos en los sistemas pero que también sirven para atacarlos.
 - **Falsos programas de seguridad** (Rogueware), falsos antivirus y antiespias.
 - **Puertas traseras** (backdoors), atajos que insertan los programadores en los programas.
 - **Virus**, código que se adhiere o pega en un fichero ejecutable y lo infecta.
 - **Gusanos** (Worm), programa que se ejecuta y propaga por si mismo generalmente en las redes.
 - **Troyanos**, aplicaciones con instrucciones escondidas que parece que hace una cosa, pero realmente ejecuta otras funciones ocultas sin conocimiento del usuario.
 - **Programas conejo** o bacterias, programas que no hacen nada útil, solo se reproducen y dejan sin recursos el sistema.
 - **Canales cubiertos**,

Técnicas de ataque, clasificación de las amenazas en función a la técnica empleada.

- **Malware** Se llama así a los programas malintencionados en general como virus, espías, gusanos, troyanos, etc.
- **Ingeniería social** Obtener información a través de la manipulación y confianza de usuarios legítimos, con el fin de obtener beneficios.
- **Scam** Estafa electrónica por medio del engaño como donaciones, transferencias, puede ser scam si hay perdida monetaria y hoax (bulo) si solo es engaño.
- **Spam** Correos o mensajes basura no solicitados.
- **Sniffing** Monitorar el tráfico de una red para hacerse con información confidencial.
- **Spoofing** Suplantación de identidad o falsificación.
- **Pharming** Redirección de un nombre de dominio a otra máquina falsificada y distinta.
- **Phishing** Estafa por suplantación de identidad e ingeniería social (acceso a cuentas bancarias)
- **Password cracking** Descifrar contraseñas de sistemas y comunicaciones.
- **Botnet** Permite controlar los ordenadores infectados de forma remota.
- **Denegación de servicio** (DoS) Causar que un servicio o recurso sea inaccesible al usuario.
- **Tabnabbing** similar al **Phishing** se aprovecha del hábito de tener varias pestañas abiertas a la vez en el navegador, entonces cuando entramos a un sitio web aparentemente normal (pero que es parte de esta estafa), el mismo esperará a que cambiemos de pestaña para modificar su ícono, título y contenido, y hacerse pasar por alguno de los sitios que usamos habitualmente (como nuestro correo, redes sociales, bancos, etc). Al volver a esta pestaña, veremos una pantalla para ingresar los datos de acceso y creeremos que es porque nuestra sesión expiró, aunque obviamente se trata del sitio hostil que tomó la forma de uno conocido para nosotros.

Auditoria de seguridad de sistemas de información

Es el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades.

Objetivos de una auditoria:

- Revisar la seguridad de los entornos y sistemas.
- Verificar el cumplimiento de la normativa y legislación vigente (Ley de protección de datos).
- Elaborar un informe independiente

Estándares:

- ISO 27001 Define los requisitos de auditoria y sistemas de gestión de seguridad.
- ISO 27002 Código internacional de buenas prácticas de seguridad de la información.

*Servicios de auditoria, fases:

- Enumeración de sistemas operativos, servicios, aplicaciones, topologias y protocolos de red.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas específicas de corrección.
- Recomendaciones sobre implantación de medidas preventivas.

Tipos de auditoria

- Auditoria de seguridad interna Nivel de seguridad de las redes locales y de carácter interno.
- Auditoria de seguridad perimetral Perímetro de la red local, conectado a redes publicas.
- Test de intrusión Se intenta acceder a los sistemas para comprobar el nivel de resistencia a la intrusión.
- Análisis forense Análisis posterior de incidentes, mediante el cual se trata de reconstruir como se ha penetrado en el sistema.
- Auditoria de código de aplicaciones Análisis del código independientemente del lenguaje empleado.

Las auditorias hay que realizarlas con cierta frecuencia.

Medidas de seguridad

- Según el sistema a proteger
 - Seguridad **física** Trata de proteger el hardware.
 - Seguridad **lógica** Protege el software.
- Según el momento en el que se pone en marcha las medidas de seguridad
 - Seguridad **activa** son preventivas, de este tipo son las medidas de seguridad lógica.
 - Seguridad **pasiva** son correctivas, posteriores a un ataque o incidente, de este tipo son las medidas de seguridad física y copias de seguridad.

Capítulo 2 Seguridad pasiva

Principios de la seguridad pasiva

La seguridad pasiva son las acciones o medidas posteriores a un ataque o incidente.

Amenazas	Medidas paliativas
Suministro eléctrico: cortes, variaciones del nivel medio de tensión (subidas y bajadas), distorsión y ruido añadido.	<ul style="list-style-type: none">- Sistema de alimentación ininterrumpida (SAI o UPS).- Generadores eléctricos autónomos.- Fuentes de alimentación redundantes.
Robos o sabotajes: acceso físico no autorizado al hardware, software y copias de seguridad	<ul style="list-style-type: none">- Control de acceso físico: armarios, llaves, blindaje, biometría.- Vigilancia mediante personal y circuitos cerrados de televisión (CCTV).
Condiciones atmosféricas y naturales adversas: temperaturas extremas, humedad excesiva, incendios, inundaciones, terremotos.	<ul style="list-style-type: none">- Elegir la correcta ubicación de sistemas, teniendo en cuenta en la construcción la probabilidad de catástrofes naturales y ambientales.- Centro de respaldo en ubicación diferente al centro de producción.- Proporcionar mecanismos de control y regulación de temperatura, humedad, etc.

Las **consecuencias de las amenazas** son:

- Perdida o mal funcionamiento del hardware.
- Falta de disponibilidad de servicios.
- Perdida de información.

Copias de seguridad

Las copias de seguridad o backup son replicas de datos que nos permiten recuperar la información original en caso de ser necesario.

Modelos de almacenamiento:

- **DAS** (Direct Attached Storage) Método tradicional, el propio disco duro del ordenador.
- **NAS** (Network Attached Storage) Almacenamiento conectado en Red.
- **SAN** (Storage Area Network) Dispositivos de almacenamiento conectados a una red de alta velocidad.

Modelos de almacén de datos

- Desestructurados DVD, memorias USB, discos duros con una mínima información de que ha sido copiado y cuando.
- Estructurados Se dividen en tres tipos de copias
 - ✓ Completa, total o integra Copia total de todos los datos.
 - ✓ Incremental Copia de los archivos que han cambiado desde la ultima copia.
 - ✓ Diferencial Copia de los archivos que han cambiado desde la ultima copia total.

Recomendación sobre el tipo de copia a efectuar

- Si el volumen de datos de nuestra copia de seguridad no es muy elevado, lo mas practico es realizar **siempre copias totales**.
- Si el volumen de datos de nuestra copia de seguridad es muy elevado, pero el volumen de datos que se modifican no lo es, se hace copia total y posteriormente realizar **siempre copias diferenciales**.
- Si el volumen de datos de nuestra copia de seguridad es muy elevado y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparan mucho espacio y lo mas practico es realizar una primera copia total y posteriormente realizar **siempre copias incrementales**.

Método de copia	Espacio de almacenamiento	Velocidad de copia	Restauración	Copia recomendada
Completo	Máximo	Muy lento	Muy simple	Pocos datos a copiar
Completo + Incremental	Mínimo	Rápido	Compleja	Muchos datos que cambian frecuentemente
Completo + diferencial	Intermedio	Lento	Sencilla	Datos cuya velocidad de cambio es moderada

Tipo de copia	Lee atributo de archivo (A)	Modifica atributo del archivo (A)
Total	NO	SI
Diferencial	SI	NO
Incremental	SI	SI
Diaria	NO	NO
Copia	NO	NO

Ejemplo de planificación de copia de seguridad:

- Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total.
- Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia del día 1.
- Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior.

Regla 3 2 1 de copias de seguridad:

- ✓ Tener 3 copias de seguridad diferentes (original y 2 copias).
- ✓ Tener 2 soportes diferentes
- ✓ Tener 1 copia fuera de la empresa.

Copias de seguridad con Herramientas del sistema (opciones):

- **Compresión** disminuye el espacio ocupado.
- **Duplicación** copias de seguridad duplicadas en un segundo soporte.
- **Cifrado**
- **Nombre del archivo** suele incluir el tipo de copia y la fecha, ejemplos:
 - copiatotal_01En11.tar.bz2
 - copiadiferencial_2012Enero15.tar.bz2

GNU/Linux

Bajo Linux se usa el comando **tar** que es un empaquetador de archivos junto con **cron** para automatizar las tareas.

➤ TAR

- ◆ empaquetado, opciones mas comunes:
 - tar -vcf nombre_archivo.tar nombre_carpeta_a_empaquetar
 - v: (verbose) permite obtener una descripción de los archivos empaquetados/desempaquetados
 - c: (create/vrear) crea un archivo tar
 - f: (file/archivo) indica que se dara un nombre al archivo tar
 - --newer=fecha: realiza un empaquetado incremental teniendo en cuenta que archivos han sido modificados, desde la fecha que se le indique.
- ◆ Desempaquetado, opciones mas comunes:
 - tar -tvxf mi_archivo.tar
 - t: ver el contenido (sin extraer)
 - x: (extract/extraer) extrae los archivos en la carpeta que contiene el tar

➤ CRONTAB

- ◆ La sintaxis es crontab [-e] -l [-r] [usuario]
 - el parámetro -e indica la edición del cron
 - el parámetro -l ver las tareas programadas en el archivo cron
 - el parámetro -r borrar un archivo cron
 - si no se especifica el usuario, el comando se ejecutara para el usuario en sesión.
crontab -e y dentro estas las líneas de texto con las programaciones:
*** * * * * comando_o_programa_a_ejecutar**
Cada asterisco en orden significa:
Minuto (0 -59) Hora (0 – 23) Día del mes (1 – 31) Mes (1 – 12) Día de la semana (0 – 6) 0 domingo
0 3 * * 5 /usr/bin/backup ejecuta el programa backup todos los días viernes a las 3 de la mañana

Ejemplo script para realizar una copia total de una carpeta determinada:

```
#!/bin/bash
#Script de copia total
#variable con los directorios que se copian
directorio="/home/juan/carpeta"
#variable con el directorio donde se guarda la fecha del ultimo backup
fechacopia="/home/juan/copia"
#variable con el directorio donde se guarda la copia
backup="/home/juan/copia"
fecha=`date +"%y%b%d"` #fecha de la copia con formato año mes dia
#El comando tar empaqueta los archivos de directorios contenidos en $directorio
#Con 2> redirigimos los mensajes de error al fichero errores_$fecha.txt
tar -vcf $backup/copiatotal_$fecha.tar $directorio 2> $backup/errores_$fecha.txt
#escribo en el fichero logscopias.txt las fechas de las copias totales hechas
echo Copia total realizada_$fecha >> $backup/logscopias.txt
#Se da permisos de ejecucion con: chmod u+x copiatotal.sh
#
#Se ejecuta en terminal con: sh copiatotal.sh
#
#Si en errores sale Removin leading '/' from member names indica que al
#descomprimir quita la primera / de tal manera que se descomprime a partir de
#donde este el fichero copia
#ahora se realiza una copia del backup en otro sitio remoto con scp
scp $backup/copiatotal_$fecha.tar usuario@IP:/home/usuario
#donde usuario es el nombre asignado y IP la dirección IP del servidor
```

Windows

En windows existe una utilidad para las copias de seguridad, bajo comando en terminal con: ntbackup o gráficamente en Inicio – Todos los programas – accesorios – Herramientas del sistema – 'Copia de seguridad'

Las opciones de copia de seguridad son:

- Total Copia todos los datos seleccionados y marca el archivo como copiado, no tiene en cuenta el atributo A, pero si lo modifica una vez copiados.
- Diferencial Copia todos los archivos modificados desde la ultima copia Tota o Incremental, no modifica el atributo A, pero si hace uso de el.
- Incremental Copia todos los archivos que han cambiado desde la ultima copia total o incremental realizada, hace uso del atributo A y lo modifica una vez copiados.
- Diaria Hace una copia de los archivos modificados en el día indicado.
- Copia Copia los datos de un lugar a otro, no tiene en cuenta el atributo A ni lo modifica,

Ejemplo de script batch de copia de seguridad:

@ECHO OFF

REM Hace copia de seguridad total del contenido de la carpeta Mis documentos y lo guarda en el escritorio
ntbackup backup "C:\Documents and Settings\rat\Mis documentos" /m copy /f "C:\Documents and Settings\rat\Escritorio\total_1.bkf" /j "CopiasSAD total"

REM Hace copia de seguridad diferencial del contenido de la carpeta Mis documentos y lo guarda en el escritorio

ntbackup backup "C:\Documents and Settings\rat\Mis documentos" /m differential /f "C:\Documents and Settings\rat\Escritorio\diferencial_1.bkf" /j "CopiasSAD diferencial"

Ejemplo de script batch para subir un fichero por ejemplo de copia de seguridad a un servidor ftp.

ftp -s:Envio_a_FTP.txt 192.168.7.111

El archivo txt al que se hace referencia contiene lo siguiente:

sad
contraseña
bin
put Backup_completo.bkf
bye

Tanto el archivo txt como el archivo a subir (Backup_completo.bkf) han de estar en el mismo directorio desde el que se ejecuta el script.

Copias de seguridad mediante aplicaciones

- En windows tenemos:
 - Cobian Backup (<http://www.cobiansoft.com/cobianbackup.htm>). Aplicación de Backup para windows, con muchas opciones, incluida la compresión y encriptacion, tambien poder subir el archivo de copia a un servidor.
- En Linux
 - fwbackups (<http://www.diffingo.com/oss/>)

Recuperación de datos, es posible recuperar archivos borrados mediante una serie de aplicaciones:

- Windows
 - Recuva. (<http://www.piriform.com/recuva>) Aplicación de recuperación de archivos borrados.
- GNU/Linux
 - Testdisk
 - Foresight
 - Scalpel
 - SpinRite (de pago)

Centros de procesado de datos (CPD)

Se denomina procesamiento de datos o CPD a aquella ubicación donde se encuentran todos los recursos necesarios para el procesamiento de la información de una organización. Se conoce también como Centro de computo o Centro de calculo, en inglés **Data center**. Estos recursos consisten en unas dependencias acondicionadas, servidores y redes de comunicaciones.

El factor mas importante para la creación de los CPD es **garantizar la continuidad y alta disponibilidad**, los requisitos generales son:

- **Disponibilidad y monitorización** “24x 7x 365”, disponibilidad, confianza y accesibilidad los 365 días del año.
- **Fiabilidad infalible** (5 nueves), 99,999% de disponibilidad.
- **Seguridad, redundancia y diversificación**. Almacenaje exterior de datos, tomas de alimentación independientes, SAIs y servicios de telecomunicaciones
- **Control ambiental/prevención de incendios**, Control de la calidad del aire, temperatura, humedad, electricidad, fuego, etc.

Según las recomendaciones la temperatura debe ser de 22'3°C o en el margen de 15 a 23°C y una humedad de entre 40% a 60%. Es necesario disponer de un **Plan de contingencia** corporativo con las actuaciones en caso de incidente.

Control de acceso físico, a las personas se las puede identificar por:

- **Algo que se posee** como una tarjeta de acceso, una llave, etc.
- **Algo que se sabe** como una contraseña, numero de identificación que se solicitar a su ingreso.
- **Algo que se es** como las huellas digitales, firma escrita, ojos, voz, etc.

Un rack normalizado para equipamiento informático tiene un ancho normalizado de 19 pulgadas.

Sistemas biometricos, son sistemas muy seguros:

- **Huella** digital
- Verificación de **voz**
- Verificación de patrones **oculares**
- Verificación Automática de **Firmas** (VAF)

Circuito cerrado de televisión (CCTV) y Cámaras IP.

Sistemas de alimentación ininterrumpida (SAI)

Un SAI o UPS es un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica tras un corte de suministro eléctrico.

Otra función de un SAI es mejorar la calidad de la energía eléctrica, filtrando subidas y bajadas de tensión así como eliminando armónicos de la red eléctrica.

Tipos de SAI:

- **SAI OffLine**, No estabilizan la corriente y solo generan la tensión cuando se produce un corte eléctrico
- **SAI InLine o Interactive**, Estabilizan la corriente incorporando un estabilizador de salida y solo generan la tensión de salida cuando se produce un corte eléctrico.
- **SAI OnLine**, Generan siempre la tensión de salida nueva independientemente de la entrada.

Los SAI disponen de funciones de conexión para monitorización y consulta del estado remoto, mediante puerto serie o USB y un software específico.

Algunos de los eventos que muestra el software de un SAI son: Estado de la Batería, sobrecarga de salida, Fallo Red, Tiempo restante en caso de fallo, etc.

La potencia de los SAI o UPS viene definida en VA (Voltiamperio) que es la potencia aparente o efectiva consumida por el sistema.

En continua la potencia se mide en vatios (W) y es el resultado de multiplicar la tensión en voltios (V) por la intensidad en amperios (A), sin embargo en alterna para equiparar los vatios (w) a voltiamperios hay que multiplicar los vatios por 1,4 y así tener en cuenta el pico máximo de potencia que puede alcanzar el equipo, de esta manera se obtiene la potencia aparente (VA), así **W*1,4=VA**.

Así mismo se recomienda dejar un margen de potencia sin usar en el SAI, por lo que se recomienda que el consumo de todos los equipos conectados no sobrepase el **70% de la capacidad total del SAI**.

Ejercicio de ejemplo calculo SAI:

Calcular los VA de una SAI que debe tener conectados a tomas de batería los siguientes equipos:

- 3 torres de 180 w c/u
- 2 monitores LED de 10 w c/u
- 1 router de 0,2 A
- 2 switches de 0,1 A
- 1 impresora de 200 VA

Solución:

- | | |
|-------------------------------|--|
| • 3 torres de 180 w c/u | $\rightarrow 3 \times 180 \times 1,4 = 756 \text{ VA}$ ($\text{VA} = \text{w} \times 1,4$) |
| • 2 monitores LED de 10 w c/u | $\rightarrow 2 \times 10 \times 1,4 = 28 \text{ VA}$ |
| • 1 router de 0,2 A | $\rightarrow P = V \times I$ |
| | $0,2 \times 220 = 44 \text{ w}$ |
| | $44 \times 1,4 = 61,6 \text{ VA}$ |
| • 2 switches de 0,1 A | \rightarrow Todo lo anterior, pero en un paso |
| | $2 \times 0,1 \times 220 \times 1,4 = 61,6 \text{ VA}$ |
| • 1 impresora de 200 VA | $\rightarrow 200 \text{ VA}$ |

Suma Consumos calculados en VA: $756 + 28 + 61,6 + 61,6 + 200 = 1107,2 \text{ VA}$ en total

Necesitamos una SAI que al 70% (p. ej) de capacidad nos de los 1107,2 VA calculados.

$$\begin{array}{rcl} 1107,2 & - & 70\% \\ x & - & 100\% \end{array}$$

$x = 1107,2 \times 100 / 70 = 1581,71 \text{ VA}$ deberá tener, como mínimo, la SAI que buscamos.

Seguridad y Alta disponibilidad

Capítulo 3 Seguridad lógica.

Principios de la seguridad lógica:

- ***La seguridad lógica** consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo accedan personas autorizadas (seguridad en el acceso lógico a sistemas, software antimalware y criptografía).
- Como principio básico de seguridad lógica en la configuración de sistemas: todo lo que no este permitido debe estar prohibido.

***Control de acceso lógico.**

El control de acceso lógico es la principal defensa para la mayoría de sistemas.

- ***Identificación** es cuando el usuario se da a conocer en el sistema (Nombre usuario).
- ***Autenticacion** es la verificación que realiza el sistema sobre esta identificación (Password).
 - ✓ Algo que se sabe por ejemplo una contraseña de acceso
 - ✓ Algo que se tiene por ejemplo una tarjeta de acceso
 - ✓ Algo que se es por ejemplo la huella dactilar

***Tipos de ataques** que sufren los sistemas de control de acceso:

- **Ataque de fuerza bruta.** Se intenta recuperar una clave probando todas las combinaciones posibles.
- **Ataque de diccionario.** Se intenta averiguar la clave probando las palabras de un diccionario o mas usadas.
- **Ataque según** análisis estadístico por **patrones** de contraseña típicos.

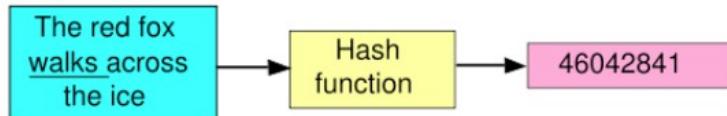
Se puede establecer un **numero máximo de tentativas** para que el sistema se bloquee automáticamente.

Política de contraseñas

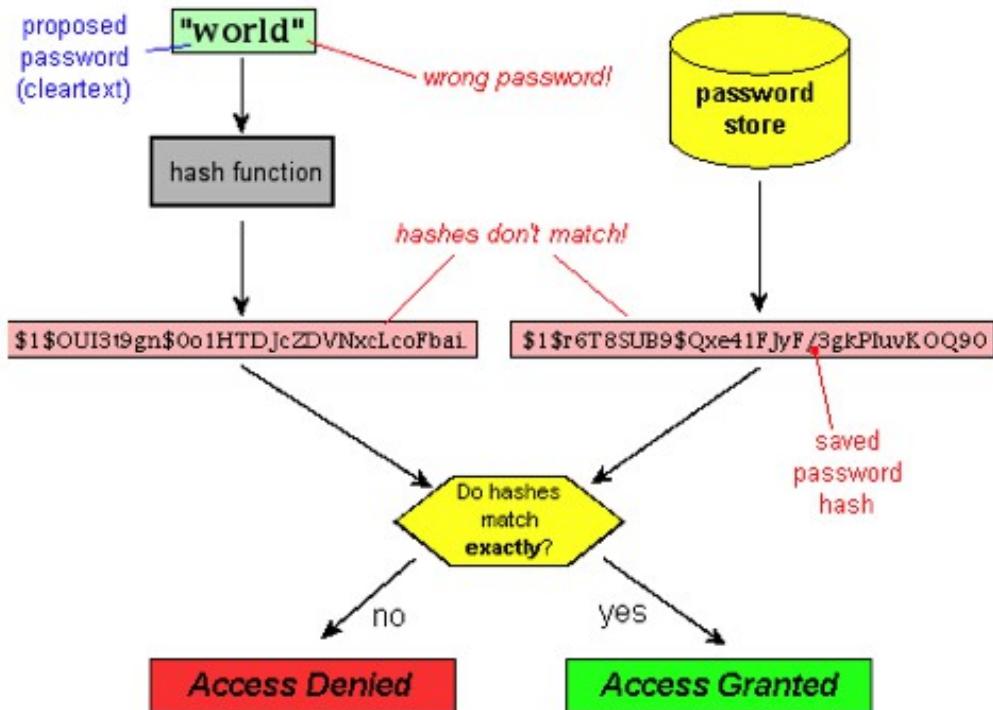
- **Longitud mínima.** Cada carácter añadido en una contraseña aumenta la seguridad, se recomienda un mínimo de 8 caracteres y lo ideal es al menos 14 caracteres.
- **Combinación de caracteres.** Combinar mayúsculas, minúsculas, números y símbolos, cuanto mas diverso mas segura.
- Se recomienda:
 - No repetir caracteres
 - No utilizar el nombre de inicio de sesión
 - No utilizar palabras de diccionario de cualquier idioma
 - Contraseñas diferentes para diferentes entornos.
 - No usar contraseñas en blanco.
 - Cambiar contraseñas con regularidad
 - No decir las contraseñas a nadie.

*Una **función hash** (MD4, MD5, SHA1, LM y NTLM) es un algoritmo matemático que nos da un resultado B al aplicarlo a un valor inicial A.

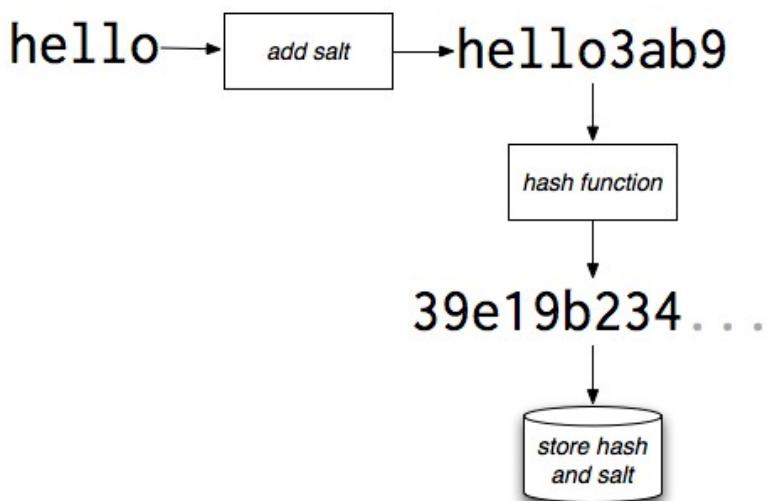
- Sea cual sea la longitud del texto base A, la longitud de su hash resultante B siempre va a ser la misma.
- Para cada entrada A, la función generará una salida B única.
- Dado un texto base, es fácil y rápido (para un ordenador) calcular su número resumen.
- Es imposible reconstruir el texto base a partir del número resumen.
- No puede presentar Colisiones o son muy pocas.



Un uso es para guardar el hash de una contraseña y compararlo luego con la introducción de la contraseña para el acceso a un determinado sistema.



*En criptografía, la **salt** (sal) comprende bits aleatorios que son usados como una de las entradas en una función derivadora de claves. La otra entrada es habitualmente una contraseña. La salida de la función derivadora de claves se almacena como la versión cifrada de la contraseña. La sal puede también ser usada como parte de una clave en un cifrado u otro algoritmo criptográfico. La función de derivación de claves generalmente usa una función hash, en conclusión la **salt** lo que hace al añadir mas caracteres, números ... aleatorios a la propia contraseña es dificultar los ataques de diccionario.



Para mayor seguridad la **salt** correspondiente a una contraseña se guarda independientemente del valor resultante de hash.

La **tablas Rainbow** son tablas de consulta que ofrecen un compromiso entre tiempo y espacio para obtener claves en texto simple a partir del resultado de una función de **hash**. proveen información acerca de la recuperación de contraseñas en texto plano generadas con ciertas funciones hash conocidas. Es importante saber que las tablas rainbow son creadas a partir de una función de hash específica, por ejemplo, para romper los hashes de MD5 necesitaremos unas tablas rainbow basadas en hashes de MD5 y para SHA, tablas rainbow SHA.

Hash of IMEI	IMEI
39f808b4d3b1b253f99d1bf1e3bb63b8aa530727	01124500 000000 8
205af15cb4ca8d542c6f0d964f965b2888115a9	01124500 000001 6
affd7a0fa4d837a41bf09ca06f11247ae457427b	01124500 000002 4
45c0d46a91a3b312511c8fa93d128cbac0270fc9	01124500 000003 2
33d2620bf9c59f387dc08498b76839a09f19a455	01124500 000004 0
...	...

Directivas de cuentas en Windows:

- Directivas de contraseñas
 - ◆ Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio.
 - ◆ Forzar el historial de contraseñas, Establece el numero de contraseñas a recordar, los usuarios no pueden usar la misma contraseña cuando caduca (el mínimo es 1).
 - ◆ Las contraseñas deben cumplir los requerimientos de complejidad:
 - ✓ 6 caracteres como mínimo
 - ✓ Contener caracteres de las siguientes clases: Mayúsculas, minúsculas, números, caracteres especiales, etc.
 - ✓ No contener 3 o mas caracteres del nombre de usuario.
 - ◆ Longitud mínima de la contraseña.
 - ◆ Vigencia máxima de la contraseñas.
 - ◆ Vigencia mínima de la contraseña.
- Directiva de bloqueo de cuentas
 - ◆ Duración del bloqueo de cuentas, en minutos cuanto tiempo esta bloqueada una cuenta.
 - ◆ Restablecer la cuenta de bloquesos después de: cuanto ha de pasar en minutos para restablecer la cuenta.
 - ◆ Umbral de bloquesos de la cuenta: Numero de intentos fallidos para que se bloquee la cuenta.
- Recomendaciones:
 - ◆ Contraseña mínima de 14 caracteres.
 - ◆ Que se modifique cada mes.
 - ◆ Que con tres intentos fallidos se bloquee 15'

GNU/Linux

El control sobre complejidad y cifrado de contraseñas en Linux se hace mediante el servicio **PAM** (Pluggable Authentication Module).

En **/var/log/auth.log** se registran los login en el sistema, los intentos fallidos se registran en líneas con información del tipo invalid password o authentication failure.

***Distintos niveles de control de acceso a los sistemas mediante contraseña:**

- **1º nivel:** Control con contraseña del arranque y la configuración de la BIOS.
- **2º nivel:** Control mediante contraseña del arranque y de la edición de las opciones de los cargadores de arranque.
- **3º nivel:** Control mediante usuario y contraseña para el acceso al sistema operativo.
- **4º nivel:** Contraseña y cifrado de acceso a datos y aplicaciones.

***Peligros de distribuciones Live**

Permiten arrancar sistemas operativos en modo live desde por ejemplo un CD o pendrive USB y contienen gran cantidad de herramientas de recuperación de datos y contraseña, ***algunas distribuciones son:**

- | | |
|----------------------|--|
| • Ultimate Boot CD | Entorno simulado de windows |
| • Backtrack | Con herramientas de auditoria de seguridad. |
| • Ophcrack | Con capacidad de extraer contraseñas de usuarios en windows. |
| • Siax | Montaje y acceso a los ficheros del disco. |
| • Wifiway y Wifislax | Con herramientas de auditoria wireless. |

***Control de acceso en la BIOS y Gestor de arranque**

- **Seguridad del sistema.** En cada arranque del sistema pedirá una contraseña que si se introduce incorrectamente el sistema no arrancará.
- **Seguridad de configuración de la BIOS.** Contraseña para acceder a la configuración de la propia BIOS.

Con las contraseñas de la **BIOS** cabe destacar que la seguridad de la BIOS es vulnerable ya que existen formas de resetear la BIOS y volver a sus valores iniciales y por tanto perder dichas contraseñas de acceso.

En relación al **Gestor de arranque** de GNU/Linux como GRUB, permite poner una contraseña de acceso a cada opción de arranque de los sistemas operativos gestionados y también una contraseña de arranque a las propias opciones del GRUB.

***Recuperación de contraseñas**

- **Ophcrack** es una aplicación que permite recuperar contraseñas de windows, se basa en el conocimiento de como windows almacena sus contraseñas de usuario (normalmente en **\windows\system32\config\SAM**, solo accesible sin arrancar el sistema operativo, desde por ejemplo una distribución live), emplea una comprobación de fuerza bruta y diccionarios (**tablas Rainbow**) que habrá que descargar dependiendo de la versión utilizada.
- **John the Ripper** (John) es otra aplicación con la que se pueden extraer las contraseñas de los usuarios, tanto en sistemas Windows como Linux.

Modificación de contraseñas

- **ERD commander** es una distribución live CD con la que se puede cambiar las contraseñas de los usuarios de un sistema Windows.
- Una vulnerabilidad que presentan los sistemas windows es por medio de herramientas que pueden modificarse o sustituirse por una consola de comandos ([cmd.exe](#) con privilegios de administrador), como por ejemplo la utilidad **StickyKeys**. (software de ayuda que se activa pulsando 5 veces seguidas la tecla SHIFT).
- En GNU/Linux las contraseñas encriptadas se encuentran en [/etc/shadow](#) y si podemos acceder al sistema de fichero y cambiar la contraseña de cualquier usuario por una conocida podremos acceder con la nueva contraseña.
 - ✓ En [/etc/pam.d/common.password](#) se indica el el algoritmo de cifrado empleado en [/etc/shadow](#), en la linea correspondiente al modulo pam_unix.so .

*Política de Usuarios y Grupos

- Definición de puestos
- Determinación de la sensibilidad del puesto
- Elección de la persona para cada puesto.
- Formación inicial y continua de los usuarios.
- Definición de los permisos de acceso.

GNU/Linux

- | | |
|------------------|---|
| • chmod | especificación de los permisos de un archivo |
| • chown | tomar posesión de un archivo |
| • chgrp | para cambiar de grupo |
| • getfacl | permite ver la información de permisos sobre un archivo |
| • setfacl | permite asignar permisos sobre un archivo |

Capítulo 4 Software antimalware.

Software malicioso o malware agrupa a los virus, gusanos, troyanos y en general a todos los programas que se han desarrollado para acceder a los ordenadores sin autorización y producir efectos no deseados.

- En los comienzos la motivación principal de los creadores de virus era el reconocimiento publico.
- Con la evolución de las tecnologías de comunicación y su implantación en todos los aspectos de la vida diaria, los ciberdelincuentes han visto en ello un negocio muy lucrativo, han pasado a tener una motivación económica.

***Formas de obtener un beneficio económico** por parte del creador de un programa malicioso:

- ◆ **Robar información sensible** del ordenador infectado como contraseñas, mail, datos personales, credenciales de acceso a diferentes entidades, banca online, etc.
- ◆ Crear una **red de ordenadores infectados** llamados Botnet o red Zombi, de tal manera que el atacante manipula todos simultáneamente por ejemplo para realizar ataques de denegación de servicio, envío de spam, etc.
- ◆ Venta de **falsas soluciones de seguridad** (rogueware) que no realizan lo que afirman, como por ejemplo falsos antivirus.
- ◆ Cifrar el contenido de los ficheros del ordenador y solicitar un **rescate** económico al usuario del equipo para recuperar la información.

****Clasificación del Malware**

- ◆ **Virus**: Infectan archivos y solo pueden existir dentro de otro fichero, generalmente son ejecutables (.exe, .src, .com, .bat).
- ◆ **Gusano**: Su característica principal es hacer el máximo numero de copias posible de si mismo para propagarse, los medios de propagación son correo electrónico, archivos falsos descargados de redes p2p, mensajería instantánea.
- ◆ **Troyano**: Es un código malicioso con capacidad de crear una puerta trasera o **backdoor**, que permita la administración remota a un usuario no autorizado, las formas de acceder al sistema son descargado por otro otro programa malicioso, visita a una pagina maliciosa, venir dentro de otro programa que parece inofensivo, etc.
- ◆ **Clasificaciones genéricas**:
 - Ladrones de información (**infostealers**). Códigos maliciosos que roban información como los **Keyloggers**.
 - Código delictivo (**crimeware**). Programas que realizan una acción delictiva en el equipo.
 - Greyware (o **grayware**). Aplicaciones que realizan alguna acción que no es dañina pero si molesta.

*Métodos de infección

- ◆ **Explotando una vulnerabilidad:** Los sistemas operativos o programas no siempre se comportan como se espera en determinadas situaciones y esto es aprovechado para ejecutar comandos no deseados o introducir programas maliciosos.
- ◆ **Ingeniería social:** Mediante técnicas de abuso de confianza para apremiar a un usuario a que realice determinada acción.
- ◆ **Por un archivo malicioso:** Es la forma en que gran cantidad de malware llega al ordenador, en archivos adjuntos, por medio del correo no deseado o spam, por la ejecución de aplicaciones web, archivos descargados de redes p2p, cracks, etc.
- ◆ **Dispositivos extraibles:** Muchos gusanos dejan copias de si mismos en dispositivos extraibles y por medio de la ejecución automática al conectarlo o reproducirse.
- ◆ **Cookies maliciosas:** Pequeños ficheros que monitorizan y registran las actividades del usuario en internet con fines maliciosos, por ejemplo tener hábitos de navegación para empresas de publicidad.

Keylogger es un software de recuperación de pulsaciones de teclado (denominado **Revealer Keylogger**) que luego envía la información recopilada remotamente por ftp o mail.

**Protección y desinfección, recomendaciones:

- ✓ Mantenerse informado de novedades y alertas de seguridad.
- ✓ Mantener actualizado el equipo.
- ✓ Hacer copias de seguridad.
- ✓ Utilizar software legal.
- ✓ Utilizar contraseñas fuertes.
- ✓ Crear usuarios con pocos privilegios para el uso cotidiano.
- ✓ Utilizar herramientas de seguridad (antimalware).
- ✓ Analizar el sistema de ficheros con varias herramientas.
- ✓ Realizar periódicamente escaneo de puertos, test de velocidad y conexiones de red.
- ✓ No fiarse de todas las herramientas antimalware, alguna no son lo que dicen (son maliciosas).

Clasificación de software antimalware:

- ◆ Antivirus es un programa informático diseñado para detectar, bloquear y eliminar códigos maliciosos.
 - **Antivirus de escritorio.** Se instala como una aplicación mas, control antivirus en tiempo real.
 - **Antivirus en linea.** Análisis vía web mediante la instalación de un plugin.
 - **Análisis de ficheros en linea.** Análisis de ficheros gratuito mediante múltiples antivirus.
 - **Antivirus portable.** Antivirus que no requiere instalación y consume unos pocos recursos.
 - **Antivirus live.** Arrancable y ejecutable desde la unidad de CD en modo live.
- ◆ **Antispyware.** El spyware o programa espía es una aplicación que recopila información del sistema para luego enviarla por internet.
- ◆ **Herramientas de bloqueo web.** Estas nos informan de la peligrosidad de los sitios web que se visitan, las que analizan en linea se instalan como un plugin en el navegador web.

Diferencia entre Antivirus y Antimalware/Antispyware:

- ✓ Los **antivirus** son programas cuyo objetivo es detectar y/o eliminar virus informáticos.
- ✓ Los **antimalware** son programas que detectan y eliminan programas maliciosos (virus, troyanos, gusanos ...).

Programas antimalware:

- **Malwarebytes** para uso con Windows
- **Spybotsd** también para uso con Windows.

Programas antivirus:

- **ClamAv** tiene versión GNU/Linux, Windows y OS X (este es ClamXav)
- **Antivirus live Kaspersky**

****Pasos para limpieza de malware (Análisis antimalware a fondo):**

1. Desconectar de la Red (internet)
2. Identificar procesos y driver maliciosos
3. Finalizar (o suspender) los procesos maliciosos localizados
4. Identificar y borrar los “autostarts maliciosos
5. Borrar ficheros maliciosos
6. Reiniciar el equipo y repetir
7. Analizadores de procesos de sistema:
 - **Process Explorer** de Sysinternals.
 - **HiJackThis**

Seguridad y Alta disponibilidad

Capítulo 5 Criptografía.

Principios de criptografía

La criptografía (del griego 'escritura oculta') es la ciencia de cifrar y descifrar información con técnicas especiales, usado frecuentemente en mensajes que solo puedan ser leídos por las personas a las que van dirigidos.

Al hablar de este área se debería hablar de criptología que a su vez engloba las técnicas de cifrado (criptografía) y sus técnicas complementarias donde se incluye el ***criptoanálisis** (*técnica que estudia los métodos para romper textos cifrados con objeto de recuperar la información original en ausencia de claves*).

Aspectos de la terminología de criptografía:

- ◆ La **información original** a proteger se denomina texto en claro o texto plano.
- ◆ El **cifrado** es el proceso de convertir texto plano en texto ilegible, se le llama texto cifrado o criptograma.
- ◆ Los algoritmos de cifrado se clasifican en dos grupos:
 - ✓ **Cifrado en bloque.** Se divide el texto original en bloques de bits de tamaño fijo y estos se cifran de manera independiente.
 - ✓ **Cifrado de flujo.** El cifrado es bit a bit, byte a byte o carácter a carácter.
- ◆ ***Las dos técnicas mas sencillas de cifrado son:**
 - ✓ La **sustitución:** consiste en cambiar el significado de los elementos básicos del mensaje, los dígitos, símbolos o caracteres. HOLA => H014
 - ✓ La **transposición:** consiste en re-ordenar los elementos del mensaje pero sin modificarlos. HOLA => OHAL
- ◆ El **descifrado** es el proceso inverso que recupera el texto plano a partir del criptograma y la clave.

*Tipos de algoritmo de cifrado

- **Simétricos o de clave simétrica o privada:** son los algoritmos que usan una clave única tanto para cifrar como para descifrar.
- **Asimétricos o de clave asimétrica o pública:** son los algoritmos que utilizan una clave para cifrar y otra clave distinta para descifrar.

El principio de **Kerchohoff** dice que la fortaleza de un sistema o algoritmo de cifrado debe recaer en la clave y no en el algoritmo que si es conocido, si no hay clave no se podrá descifrar el mensaje.

Scripts de cifrado

Como ejemplo de sustitución se puede utilizar el comando **tr** que realiza una sustitución carácter a carácter.

*Criptografía simétrica

La criptografía simétrica usa la misma clave para cifrar y descifrar mensajes. Dado que toda la seguridad recae en la clave, esta debe ser muy difícil de adivinar, para ello se usa la longitud y el conjunto de caracteres que use, algunos ejemplos de ***algoritmos de cifrado simétrico** son:

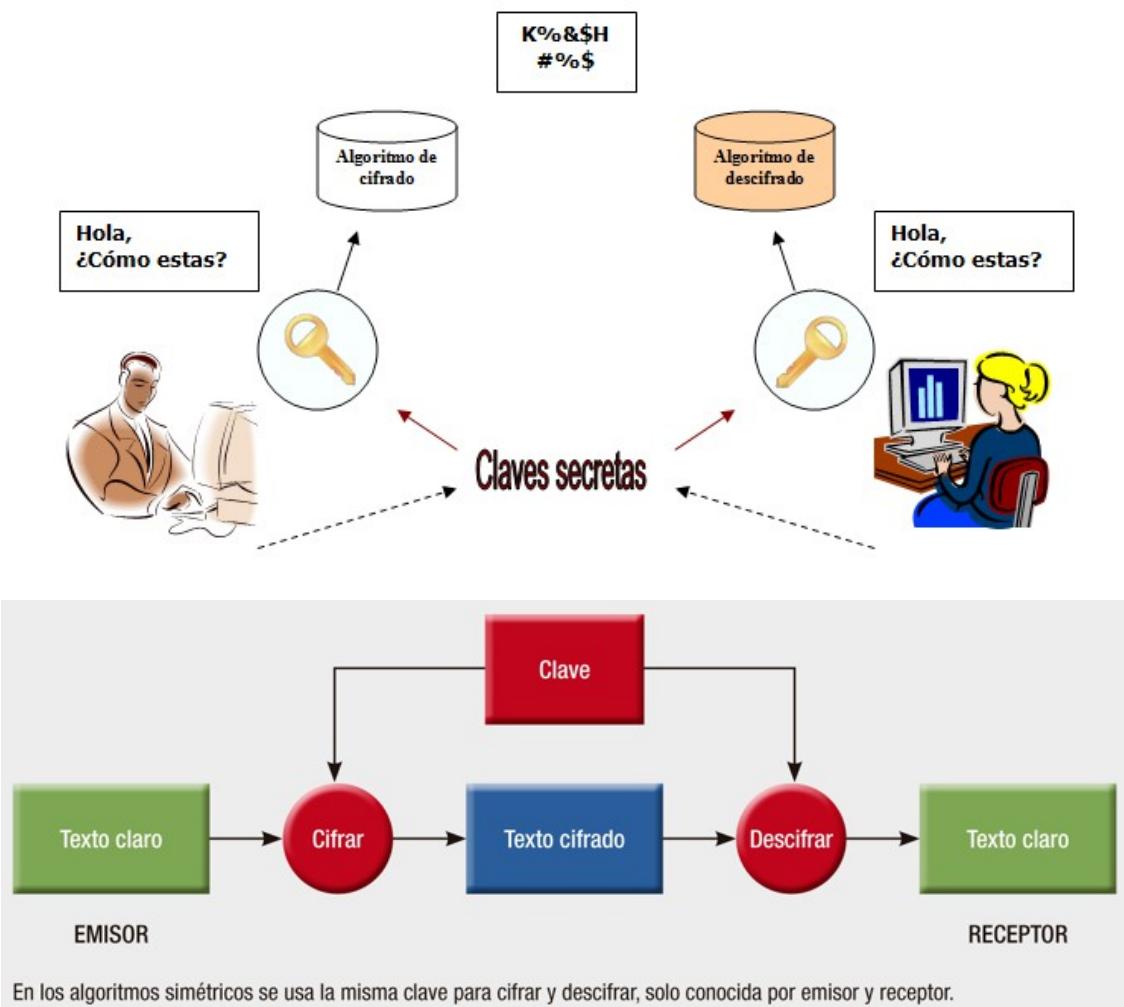
- Algoritmo de cifrado **DES** que usa una clave de 56 bits (son 2^{56} claves posibles), pero que es fácilmente descifrable por un ordenador moderno en cuestión de días.
- Algoritmo de cifrado **3DES, Blowfish, Twofish e IDEA** que usan claves de 128 bits o lo que es lo mismo 2^{128} claves posibles (aunque admiten entre 32 a 448bits dependiendo del algoritmo).
- Otros algoritmos usados son **RC5 y AES** (Advanced Encryption Standard) también conocido como **Rijndael**.

Los ***principales problemas de los algoritmos** de cifrado no están relacionados con su seguridad, sino con:

- ✓ **El intercambio de claves.** Una vez que remitente y destinatario han intercambiado las claves ya se pueden comunicar con seguridad, pero ¿que **canal de comunicación seguro** se ha usado?, esto hace que sea mas fácil para el atacante interceptar una clave que probar las posibles combinaciones para descubrirla.
- ✓ **El numero de claves que se necesitan:** si hay un numero 'n' de personas que se tienen que comunicar entre si, se necesitan $n/2$ claves diferentes para cada par de personas que se quieran comunicar en privado, con un grupo reducido de personas es posible, pero con un grupo grande es imposible llevarlo a cabo, son **muchas claves a custodiar** (sin embargo con la asimétrica solo hay que custodiar la clave privada propia).
- ✓ La **solución** a esto es la **criptografía asimétrica** y la **criptografía híbrida**.

Algunos **programas** o herramientas **de cifrado** simétrico son:

- ◆ PGP (Pretty Good Privacy) es el programa mas popular de encriptacion y creación de llaves publicas y privadas, su pega es que es un algoritmo propietario.
- ◆ ***GPG** (GNU Privacy Guard) es una herramienta para el cifrado similar al PGP pero de software libre bajo licencia GPL, utiliza **algoritmos** no patentados como **ElGamal, CAST5, Triple DES (3DES), AES y Blowfish**, viene pre-instalada en distribuciones Linux, ***algunas opciones del comando:**
 - ✓ **gpg --version** muestra la versión y algoritmos soportados.
 - ✓ **gpg -c archivo.txt** encripta el archivo con cifrado simétrico, da **archivo.gpg**
 - ✓ **gpg -c -a archivo.txt** encripta en formato legible (ASCII), da **archivo.asc**
 - ✓ **gpg -d archivo.asc** desencripta el archivo.
 - ✓ **gpg -c -a --cipher-algo AES192 archivo** **--cipher-algo** determino que algoritmo usar.
- ◆ ***TrueCrypt** para el cifrado de datos y particiones, en entorno gráfico.



*Criptografía de clave Asimétrica

Cada usuario del sistema criptográfico ha de poseer una pareja de claves:

- ✓ **Clave privada:** sera custodiada por su propietario y no se dará a conocer a ningún otro.
- ✓ **Clave pública:** sera conocida por todos los usuarios.

Esta pareja de claves es complementaria: lo que cifra una solo lo puede descifrar la otra y viceversa, los sistemas de cifrado de clave pública se basan en funciones resumen o **funciones hash** de un solo sentido, que aprovechan propiedades particulares de los números primos.

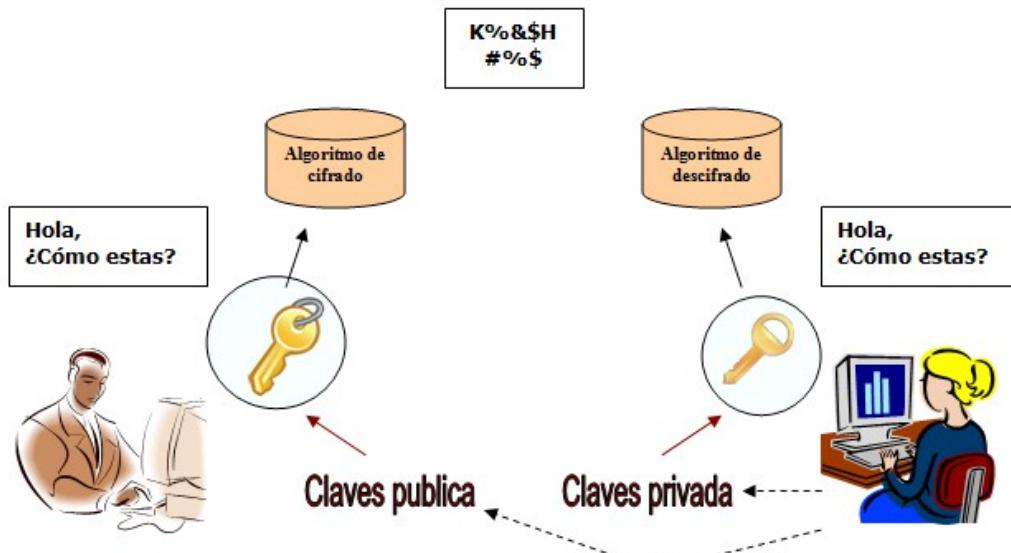
- Los ***hash o funciones de resumen** son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que *solo* puede volverse a crear con esos mismos datos).



*En cifrado simétrico es suficiente con 128bits, pero para criptografía asimétrica se recomiendan **claves públicas de 1024 bits**.

La ventaja de la **criptografía asimétrica** es que se puede cifrar con una clave y descifrar con la otra, pero este sistema **tiene bastantes desventajas**:

- ✓ Para una misma longitud de clave y mensaje se necesita **mayor tiempo de proceso**.
- ✓ Las **claves deben ser de mayor tamaño** que las simétricas.
- ✓ El mensaje cifrado **ocupa mas espacio** que el original.



En cada sentido del envío y recepción de información, se cifra el mensaje con la clave pública de la persona a la que se envía y esta lo descifra con su clave privada que solo el conoce, cada interlocutor tiene que tener la clave pública del otro.

- ◆ *algunas opciones del comando GPG en criptografía asimétrica:
 - ✓ **gpg --gen-key** genera un par de claves (privada y pública).
 - ✓ **gpg --list-keys** lista las claves públicas que tenemos, propia y ajenas.
 - ✓ **gpg --import clave.asc** importo la clave pública de un interlocutor.
 - ✓ **gpg --armor --output miclave_publica.asc --export ClaveID** exporto mi clave pública a un fichero (armor es para que se vea en caracteres ASCII).
 - ✓ **gpg --armor --output claveprivada --export-secret-key ClaveID** exporto mi clave privada a un fichero como backup.
 - ✓ **gpg --armor --recipient ClaveID_destinatario --encrypt fichero** encripto un fichero con la clave pública del destinatario (para desencriptar se usa **gpg -d fichero.gpg > fichero.xxx**).

Aplicaciones como PGP, comunicaciones TCP, protocolos SSH o la capa de seguridad TLS/SSL utilizan un **cifrado Híbrido**, que esta formado por criptografía asimétrica para el intercambio de claves de criptografía simétrica y criptografía simétrica para transmitir la información.

- *Algoritmos de técnicas de clave asimétrica:
 - ✓ Diffie-Hellman, RSA, DSA, ElGamal, criptografía de curva elíptica.

- Protocolos y software que usan los algoritmos citados:

- ✓ DSS (Digital Signature Standard) con el algoritmo DSA (Digital Signature Algorithm).
- ✓ PGP y CPG, una implementación de OpenPGP.
- ✓ SSH, SSL y TLS (por debajo de HTTPS esta SSL y TLS).

*Criptografía Híbrida

Usar claves asimétricas ralentiza el proceso de cifrado, para solucionar este inconveniente se utiliza un algoritmo de clave pública para cifrar el envío de una pequeña cantidad de información como puede ser una clave simétrica y posteriormente se usa un algoritmo de clave simétrica para el cifrado del mensaje, de esta forma se reduce el coste computacional. El proceso sería el siguiente:

- ✓ Ana escribe un mensaje con destino Bernardo, primeramente lo cifra con clave simétrica, esta clave se genera aleatoriamente y se llama clave de sesión, para enviar esta clave de sesión de forma segura se cifra de forma asimétrica con la clave pública de Bernardo.
- ✓ Bernardo recibe el mensaje cifrado con la clave de sesión y la clave de sesión cifrada con su clave pública, entonces utiliza su clave privada para descifrar la clave de sesión y una vez descifrada la utiliza para descifrar el propio mensaje.

Con el sistema de criptografía híbrida se consigue:

- ✓ **Confidencialidad:** Solo podrá leer el mensaje el destinatario del mismo.
- ✓ **Integridad:** El mensaje no podrá ser modificado (si se modifica no se podrá descifrar)
- ✗ Aunque quedan unos problemas sin resolver, **Autenticación** y **No repudio**.

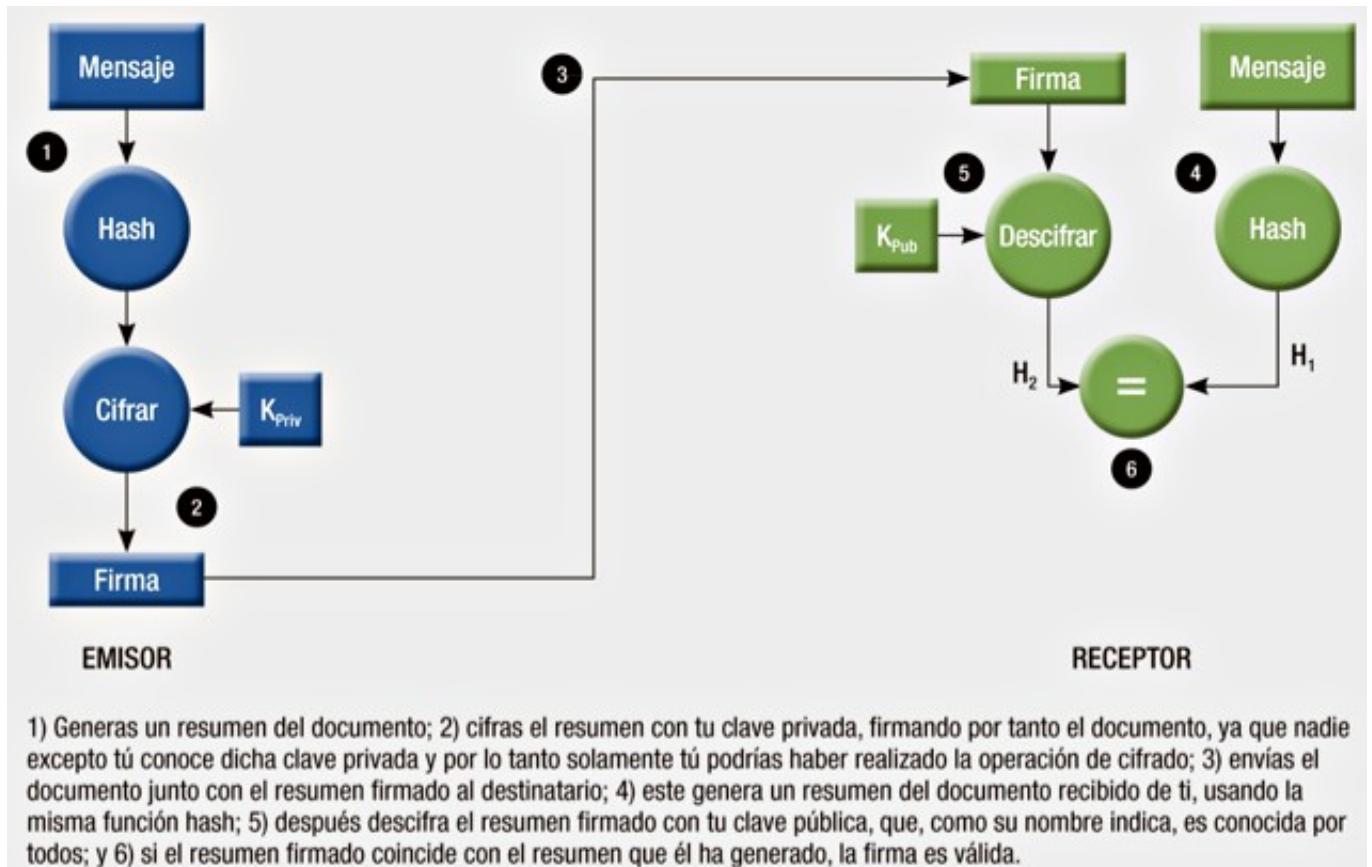


*Firma digital

Una de las ventajas de la criptografía de clave pública es que ofrece un método de firmas digitales, esto permite al receptor de un mensaje verificar la autenticidad del origen del mismo y que ademas no ha sido modificado. Por lo tanto con este sistema conseguimos:

- ✓ **Autenticación:** La firma digital es equivalente a la firma física de un documento.
- ✓ **Integridad:** El mensaje no podrá ser modificado.
- ✓ **No repudio en origen:** El emisor no puede negar haber enviado el mensaje.

La firma digital cifra con clave privada el resumen de los datos a firmar haciendo uso de funciones de resumen o hash.



- 1) Generas un resumen del documento; 2) cifras el resumen con tu clave privada, firmando por tanto el documento, ya que nadie excepto tú conoce dicha clave privada y por lo tanto solamente tú podrías haber realizado la operación de cifrado; 3) envías el documento junto con el resumen firmado al destinatario; 4) este genera un resumen del documento recibido de ti, usando la misma función hash; 5) después descifra el resumen firmado con tu clave pública, que, como su nombre indica, es conocida por todos; y 6) si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

Vídeos relacionados con la criptografía:

<http://www.intypedia.com/>

*Certificados digitales

Los certificados digitales asocian una clave publica con la identidad de su propietario.

El formato estándar de certificados digitales es **X.509** y su distribución es posible realizarla:

- ✓ Con clave privada (suele tener extensión *.pfx o *.p12) mas seguro y destinado a un uso privado de exportación e importación posterior como método de copia de seguridad.
- ✓ Solo con clave publica (suele ser de extensión *.cer o *.crt), destinado a la distribución no segura, para que otras entidades o usuarios tan solo puedan verificar la identidad, en los archivos o mensajes firmados.

Certificado

Nombre: Luis
Clave Publica: XF34....

=>

HASH

=>

XT64YZ78...

=>

Se cifra el HASH con la clave privada de la Autoridad de Certificación

*Terceras partes de Confianza

Dos usuarios pueden confiar directamente entre si, si ambos tienen relación con una tercera parte y esta da fe de la fiabilidad de los dos.

La forma en que esa tercera parte avalara que el certificado es de fiar es mediante su firma digital sobre el certificado.



Las **infraestructuras de Clave Pública** (ICP o PKI, Public Key Infrastructure) esta formado por:

- ◆ Autoridad de certificación (CA): emite y elimina los certificados digitales.
- ◆ Autoridad de registro (RA): controla la generación de los certificados, procesa las peticiones y comprueba la identidad de los usuarios, mediante el requerimiento de documentación de identificación personal.
- ◆ Autoridades de repositorio: almacenan los certificados emitidos y eliminados.
- ◆ Software para el empleo de certificados.
- ◆ Política de seguridad en las comunicaciones relacionadas con gestiones de certificados.

Documento nacional de identidad electrónico (DNIe)

Emitido por la Dirección General de la Policía acredita la identidad, los datos personales que en él aparecen y la nacionalidad y con respecto al mundo digital:

- ✓ Acreditar electronicamente y sin posibilidad de duda, la identidad de la persona.
- ✓ Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a las que le proporciona la firma manuscrita.

Incorpora un pequeño chip (circuito integrado) capaz de guardar de forma segura información en formato digital como:

- ✓ Un certificado electrónico para autenticar la personalidad del ciudadano.
- ✓ Un certificado electrónico para firmar electronicamente, con la misma validez que la firma manuscrita.
- ✓ Certificado de la autoridad de Certificación emisora.
- ✓ Claves para su utilización.
- ✓ La plantilla biométrica de la impresión dactilar.

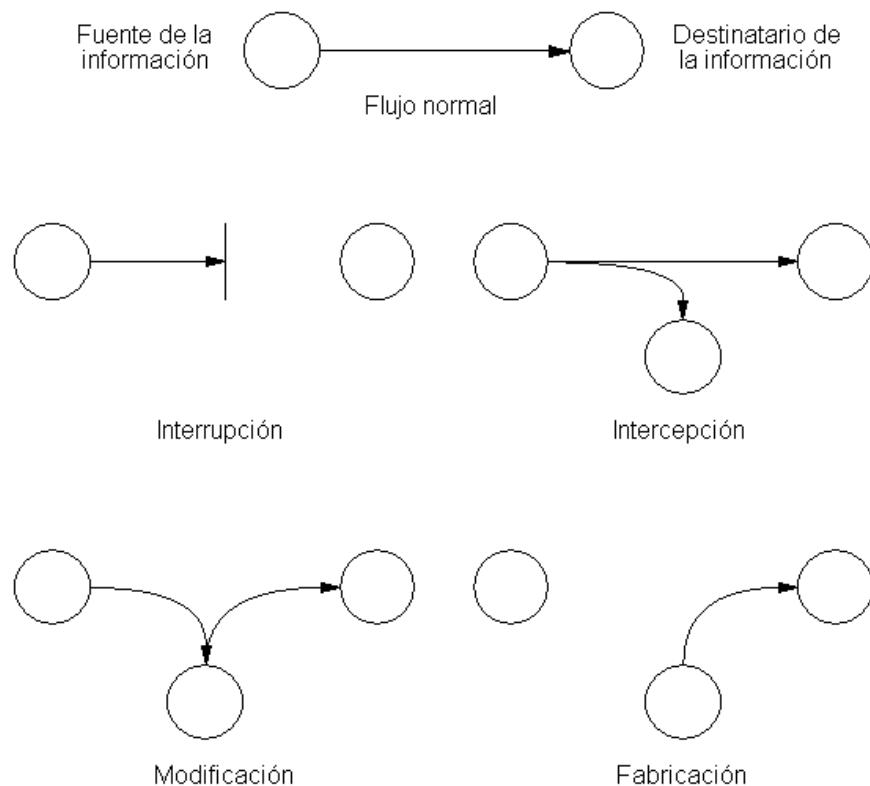
Para la utilización del DNI electrónico se necesita:

- ✓ Hardware específico: como un lector de tarjetas inteligente que cumpla el estandard ISO-7816.
- ✓ Software específico: Controladores o módulos criptográficos para el acceso al chip y su contenido.

Capítulo 6 Seguridad en redes corporativas.

***Amenazas y Ataques**, de forma genérica las amenazas en comunicaciones se dividen en 4 grandes grupos:

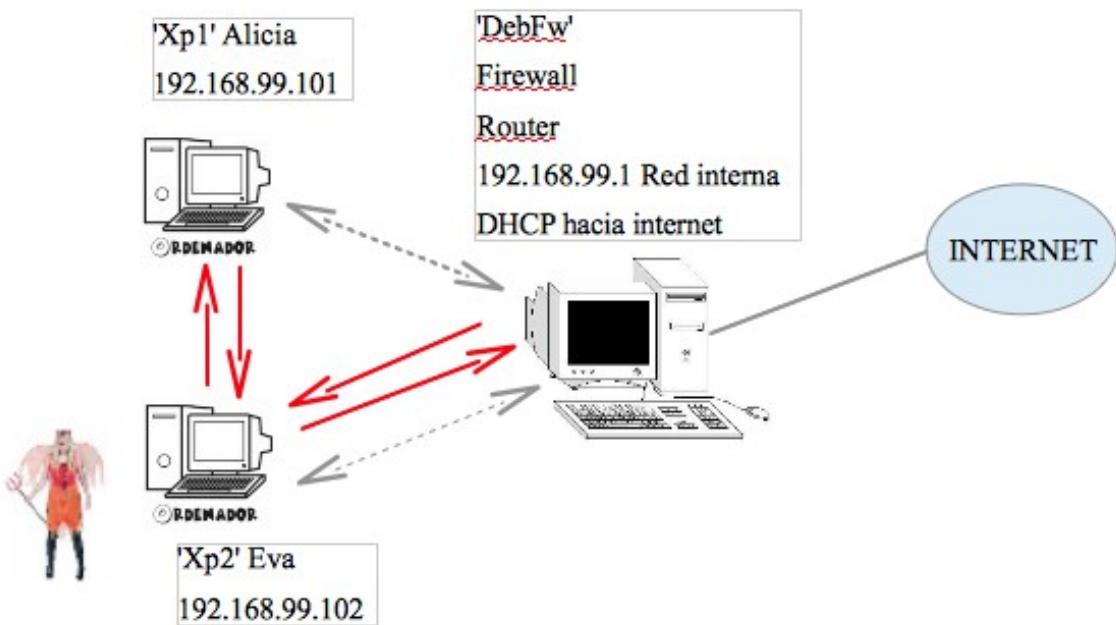
- ◆ **Interrupción**: Un objeto, servicio del sistema o datos en una comunicación se pierden, quedan inutilizables o no disponibles.
- ◆ **Interceptación**: Un elemento no autorizado consigue un acceso a un determinado objeto.
- ◆ **Modificación**: Ademas de conseguir el acceso consigue modificar el objeto, es posible incluso la destrucción, una modificación que inutiliza al objeto afectado.
- ◆ **Fabricación**: Modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el 'fabricado'.



*Técnicas de ataques informáticos en redes:

- ◆ **Ataque de denegación de servicio**. Llamado también ataque DoS, es un caso específico de **interrupción** de servicio, implica que un recurso o servicio no sea accesible a los usuarios legítimos, normalmente por la perdida de conectividad en la red por un consumo excesivo del ancho de banda o sobrecarga de los recursos del sistema atacado (mediante **botnet** o redes zombi se pueden controlar cientos de ordenadores con los que realizar este tipo de ataque).
- ◆ **Sniffing**. Es una técnica de **interceptación**: consiste en rastrear monitorizando el tráfico de una Red.
- ◆ **Man in the middle**: abreviado MitM es un caso específico de **interceptación y modificación de identidad**, el atacante supervisa la comunicación entre dos partes, falsifica las identidades de los extremos y recibe el tráfico de los dos sentidos.
- ◆ **Spoofing**: Es una técnica de **fabricación**, suplanta la identidad o realiza una copia o falsificación, por ejemplo de IP, MAC, web, mail.
- ◆ **Pharming**: Es una técnica de **modificación**, consiste en explotar una vulnerabilidad en el software de los servidores DNS o equipos de los usuarios, permitiendo modificar las tablas DNS redirigiendo un nombre de dominio conocido a otra maquina (IP) distinta, falsificada y seguramente fraudulenta.

Un programa capaz de realizar un envenenamiento de ARP es Cain&Abel, supongamos la situación que representa el esquema siguiente:



El ordenador Xp2 ejecuta el programa Cain&Abel y una vez realizado el envenenamiento ARP al Router y ordenador Xp1, queda interpuesto entre los dos, de tal manera que Xp1 toma a Xp2 como si fuera el router y el Router toma a Xp2 como si fuera Xp1, de esta manera todas las comunicaciones pasan por Xp1 y es el encargado de enviarlas luego tanto al router como a Xp1, a esto se llama el ***ARP Spoofing***, también conocido como ***ARP Poisoning o ARP Poison Routing**, ahora ya tenemos el control para hacer lo que queramos con las comunicaciones, como por ejemplo suplantar una dirección web (**Pharming**), monitorizar el tráfico (**Sniffing**) y por ejemplo extraer contraseñas, realizar ataques, etc.

*Protección contra el envenenamiento ARP:

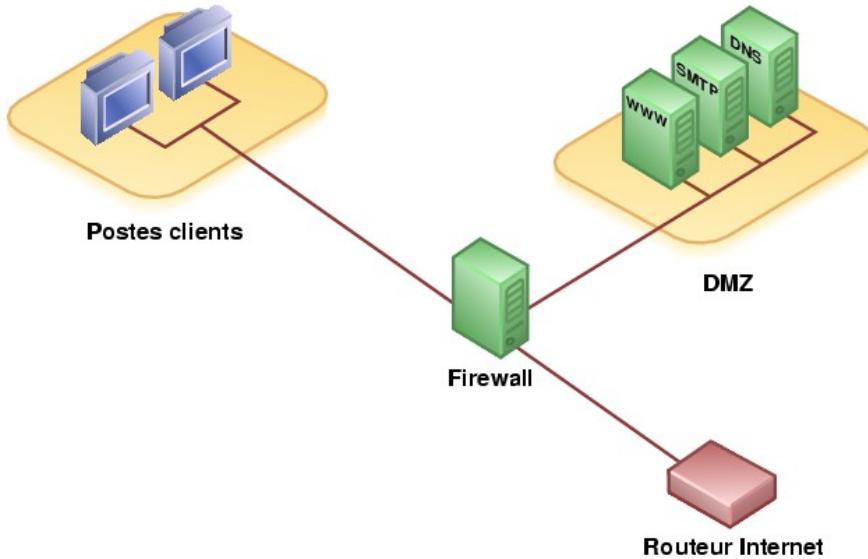
- ✗ PORT-SECURITY en el switch. Se trata de asignar una dirección MAC fija de un dispositivo al puerto donde se conecta, de tal manera que si se conecta otro equipo con otra Mac este puerto se bloquea..
- ✗ Entradas ARP estáticas. Es decir añadir entradas estáticas ARP, de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP.

Amenazas externas e internas

- ◆ **Amenaza externa** o de acceso remoto: Los atacantes están fuera de la red privada de una organización, se introducen desde redes públicas, tienen como objetivos los Servidores y Routers que son accesibles desde el exterior y sirven de puerta de acceso.
- ◆ **Amenaza interna** o corporativa: Los atacantes pertenecen a la red privada de la organización y de esta manera pueden comprometer la seguridad, servicios e información de la organización.

Como protegerse de las amenazas internas:

- ✓ Buen diseño de direccionamiento, parcelación y servicio de subredes dentro de la Red corporativa, por ejemplo con el uso de VLAN y zonas desmilitarizadas o DMZ.
- ✓ VLAN es crear redes lógicamente independientes dentro de una misma red física.
- ✓ ***Zonas desmilitarizadas o DMZ** tienen como objetivo que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, los equipos (*hosts*) en la DMZ no pueden conectar con la red interna. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.



- ✓ Políticas de administración de direccionamiento estático para servidores y routers.
- ✓ Monitorización del tráfico de red, asignaciones de direccionamiento dinámico y tablas ARP.
- ✓ Modificación de configuraciones de seguridad y contraseñas por defecto de la administración de servicios.
- ✓ En redes inalámbricas emplear el máximo nivel de seguridad.

*Sistemas de detección de intrusos (IDS)

Un sistema de detección de intrusos o IDS es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

Este sistema busca patrones previamente definidos que impliquen actividades sospechosas sobre la red, no detienen el ataque pero nos previenen. Hay varios tipos de IDS:

- HIDS (Host IDS). Protege a un único servidor, PC o host.
- NIDS (Net IDS). Protege un sistema basado en red. Un ejemplo de este sistema es:
 - ✓ ***Snort**, es un sistema de detección de intrusión basado en NIDS, implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques.

Comunicaciones seguras

La mayoría de comunicaciones que empleamos en la red como HTTP, FTP o SMTP/POP no emplean cifrado, las alternativas para realizar comunicaciones seguras son:

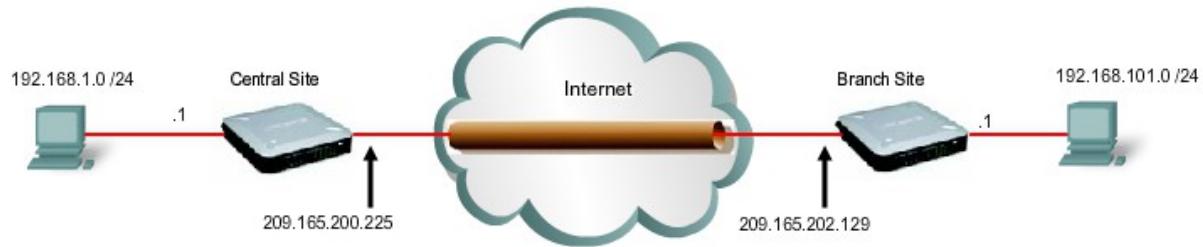
- ✓ SSL (Protocolo de capa de conexión segura) y TLS (Seguridad de la capa de transporte), se ejecuta sobre el protocolo TCP.
- ✓ IPSEC (Internet protocol security), asegura las comunicaciones sobre el protocolo IP autenticando o cifrando cada paquete IP.

La variante segura para HTTP es HTTPS.

La variante segura para FTP es **FTP seguro (SFTP)**.

*VPN

Una red privada virtual o VPN permite una extensión de una red local de forma segura sobre una red pública como internet.

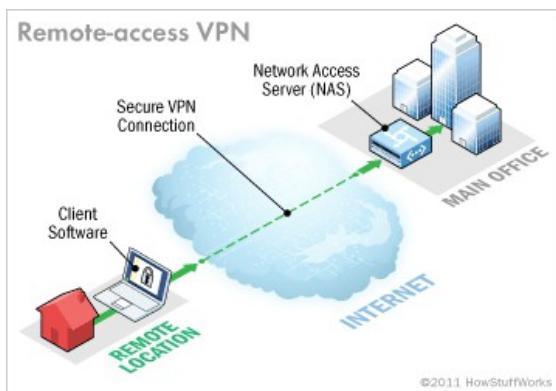


Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticidad, integridad y confidencialidad de la comunicación:

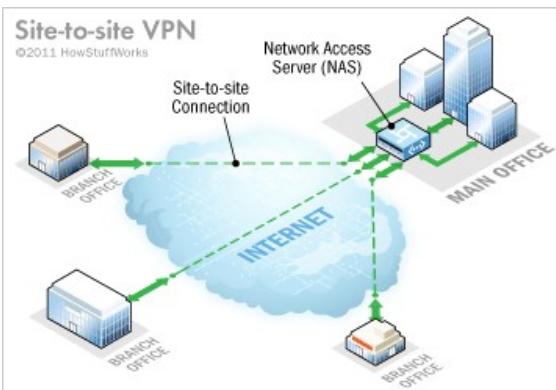
- ◆ **Autenticación y autorización.** Se controlan los usuarios y/o equipos y su nivel de acceso.
- ◆ **Integridad.** Los datos no han sido alterados, para lo que se usan funciones hash como MD5 y SHA.
- ◆ **Confidencialidad.** La información solo puede ser entendida por los destinatarios de la misma.
- ◆ **No repudio.** Los mensajes van firmados.

Existen 3 arquitecturas de conexión VPN:

- **VPN de acceso remoto.** El usuario se conecta con la empresa usando internet como acceso.



- **VPN punto a punto.** Conecta ubicaciones remotas (oficinas) con una sede central.



- **VPN over LAN.** Se emplea la red local (LAN) de la empresa para crear zonas a las que se añade cifrado y autenticación adicional mediante VPN.

El **protocolo** estándar que usa **VPN** es **IPSEC**, dos de las tecnologías mas utilizadas para crear VPNs son:

- ✓ **PPTP** o Point to Point Tunneling Protocol, fue desarrollado por Microsoft, es sencillo y fácil de implementar pero tiene menos seguridad que L2TP (este sistema esta ya roto y no es seguro).
- ✓ **L2TP** o Layer Two Tunneling Protocol. Es un estándar abierto y disponible en la mayoría de plataformas, se implementa sobre IPsec y tiene altos niveles de seguridad.

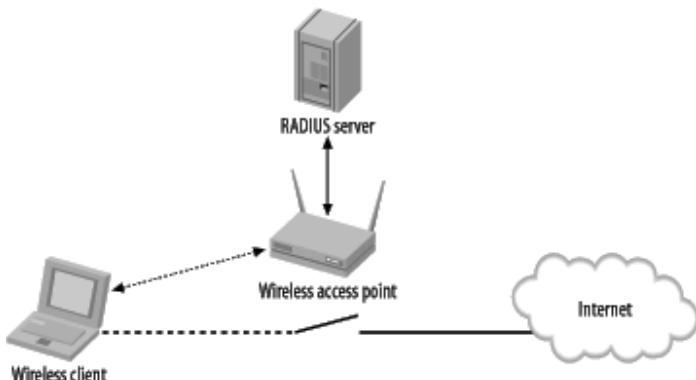
Sistemas de seguridad en VLAN

Los sistemas de cifrado empleados son:

- ◆ Sistema abierto u Open system. Sin autenticación, las comunicaciones no están cifradas.
- ◆ WEP o Wired Equivalent Privacy (Privacidad equivalente a cableado). Con autenticación que emplea para la encriptación claves de 13 caracteres (104 bits) o 5 caracteres (40 bits), llamado también WEP 128 o WEP 64 y tiene 2 métodos de autenticación:
 - Sistema abierto u Open system donde el cliente no se tiene que identificar en el pto de acceso durante la autenticación, después de la autenticación y asociación a la red tendrá que tener la clave WEP correcta.
 - Claves precompartidas o PSK. En la autenticación se envía la misma clave de cifrado WEP para la autenticación, verificación y controlando de este modo el punto de acceso.
 - De entre estas dos es mas segura la de Sistema abierto ya que con la precompartida es posible averiguar la clave en la fase de autenticación.
- ◆ *WPA o WI-FI Protected Access (Acceso de Wifi protegido). Se creó para corregir las deficiencias del sistema WEP fácilmente crakeable y consta de 2 estándares.
 - WPA empresarial o WPE Enterprise (grandes empresas). Donde la autenticación es usando un servidor Radius donde están almacenadas las credenciales y contraseñas de los usuarios.
 - WPA Personal (pequeñas empresas y hogar). La autenticación se realiza mediante clave precompartida de un modo similar al WEP.
 - Una de las mejoras sobre WEP es el uso del protocolo de integridad de clave temporal (TKIP) que cambia las claves dinámicamente a medida que el sistema es utilizado.

*Servidor autenticación RADIUS

Es un servidor (Radius) que se encarga de realizar la autenticación en vez de hacerla el punto de acceso wifi.



*Recomendaciones de seguridad en WLAN

- Cambiar contraseña por defecto → importantísimo!
- Actualizar firmware → importantísimo cuando la actualización soluciona problemas de seguridad.
- WEP → no usar, protección muy débil
- WPA → segura si usamos contraseñas largas y raras
- WPA2 → segura a día de hoy
- Cambiar SSID por defecto → como protección es débil, pero a la vez es importante para que no sepan con qué compañía tenemos la conexión
- Desactivar el broadcast SSID → protección muy débil. El SSID se emite cuando la red está funcionando aunque desactivemos el broadcast
- Desactivar DHCP → protección débil
- Filtrado MAC → protección débil, porque cambiar la MAC es sencillo
- Número máximo de dispositivos que pueden conectarse → protección débil
- Revisar periódicamente qué usuarios hay conectados → protección débil
- Desconexión del AP cuando no se use → Ok

Seguridad y Alta disponibilidad

Capítulo 7 Seguridad perimetral.

Las medidas de seguridad perimetral son la primera linea de defensa entre las redes publicas y redes corporativas o privadas, entre otras medidas están:

- ◆ Cortafuegos o firewall que bloquea las conexiones no autorizadas.
- ◆ Servidores proxy que hacen de intermediario entre clientes y servidores finales permitiendo el filtrado y Monitorización de servicios.

Un **cortafuegos o firewall** es una aplicación o dispositivo que esta diseñado para bloquear comunicaciones no autorizadas, permitiendo al mismo tiempo las que si lo están. La configuración para permitir o denegar el trafico entre diferentes redes se efectúa en base a un conjunto de normas y reglas. Las **características de los cortafuegos** son:

- ✓ Filtrado de paquetes de red en función a las direcciones de red (MAC, IP, Puerto origen y puerto destino).
- ✓ Filtrado por aplicación.
- ✓ Las reglas de filtrado se aplican sobre el trafico de salida o de entrada de una determinada interfaz.
- ✓ Registro o logs de filtrado de paquetes.

En el sistema Linux, **Iptables** es una de las herramientas cortafuegos mas empleadas, permite el filtrado de paquetes y funciones NAT, contiene una serie de reglas de filtrado, el orden de las reglas es importante, ya que se leen de manera secuencial.

- ✓ una orden de iptables tiene la siguiente estructura:
 - `iptables -t filter -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 80 -j ACCEPT`

tabla	Tipo de operación	Cadena	Regla con parámetros	Acción
<code>-t filter</code>	<code>-A</code>	<code>FORWARD</code>	<code>-i eth0 -s 192.168.2.100 -p tcp --dport 80</code>	<code>-j ACCEPT</code>

- ✓ Las opciones mas usadas son: `iptables -A`
 - `-A`: añadir cadena de regla a una determinada tabla
 - `-F`: elimina y reinicia a los valores por defecto todas las cadenas de una determinada tabla.
 - `-L`: listar las cadenas de reglas de una determinada tabla (por defecto filter)
 - `-P`: añadir regla por defecto, en caso de que no se cumpla ninguna de las cadenas de reglas definidas.
- ✓ Hay tres tipos de tablas incorporadas:
 - Filter table (Tabla de filtros), es la responsable del filtrado y contiene las siguientes cadenas:
 - ✓ INPUT – Todos los paquetes destinados a este sistema atraviesan esta cadena.
 - ✓ OUTPUT – Todos los paquetes creados por este sistema atraviesan esta cadena.
 - ✓ FORWARD – Todos los paquetes que pasan por este sistema para ser encaminados a su destino recorren esta cadena.
 - Nat table (tabla de traducción de direcciones de red), es la responsable de configurar las reglas de traducción de direcciones o de puertos de los paquetes, contiene las siguientes cadenas:
 - ✓ PREROUTING – Los paquetes entrantes pasan a través de esta cadena antes de que se consulte la tabla de enrute.
 - ✓ POSTROUTING – Los paquetes salientes pasan por esta cadena después de haberse tomado la decisión de enrute.
 - ✓ OUTPUT
 - Mangle table (Tabla de destrozo), es la responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad de servicio.

- ✓ Los modificadores y parámetros mas usuales son:
 - -t 'tabla' Hace que el comando se aplique a la tabla especificada (nat, mangle, filter)
 - -i interfaz de entrada (eth0, eth1, eth2).
 - -o interfaz de salida (eth0, eth1, eth2).
 - -s dirección de origen, puede ser la IP de un equipo
 - --sport Puerto origen (se indica el nombre o numero de puerto del protocolo, http o 80)
 - --dport Puerto destino (se indica el nombre o numero de puerto del protocolo, http o 80)
 - -p El protocolo del paquete a comprobar, tcp, udp, icmp o all, por defecto es all.
 - -j Especifica el objetivo de la cadena de reglas, osea una acción.
 - -m define que se aplica la regla si hay una coincidencia específica.
 - --state define una lista separada por comas de distintos tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).
 - --line-numbers Cuando listamos las reglas, agrega el numero que ocupa cada regla dentro de la cadena.

- ✓ Las acciones, que estarán siempre al final de cada regla (después de -j) y que determina que se hace con el paquete afectado por la regla.
 - ACCEPT Paquete aceptado
 - REJECT Paquete rechazado, se envía notificación por medio del protocolo ICMP.
 - DROP Paquete rechazado, sin notificación.
 - MASQUERADE Enmascaramiento de la dirección IP origen de forma dinámica, solo valida en la tabla NAT de la cadena postrouting.
 - DNAT Enmascaramiento de la dirección destino, muy conveniente para re-enrutado de paquetes.
 - SNAT Enmascaramiento de la dirección IP origen de forma similar a MASQUERADE pero con IP fija.

- ✓ Seguimiento de conexiones.
 - NEW Intentando crear una conexión nueva.
 - ESTABLISHED Parte de una conexión ya existente.
 - RELATED Relacionada, aunque no realmente parte de una conexión existente.
 - INVALID No es parte de una conexión existente e incapaz de crear una nueva conexión.

Se pueden configurar registros de LOG en iptables con la acción -j log en las reglas, se puede añadir un prefijo a cada entrada en el log para identificar los paquetes de forma mas sencilla con --log-prefix

- **iptables -t filter -A INPUT -i \$STARJ_EXT -p TCP -dport 22 -j LOG --log-prefix**

Tipos de cortafuegos:

- ✓ **Firewalls basados en servidores:** consta de una aplicación de firewall que se instala y ejecuta en un sistema operativo de red (NOS), que normalmente ofrece otra serie de servicios como enrutamiento, DNS, DHCP, proxy, etc.

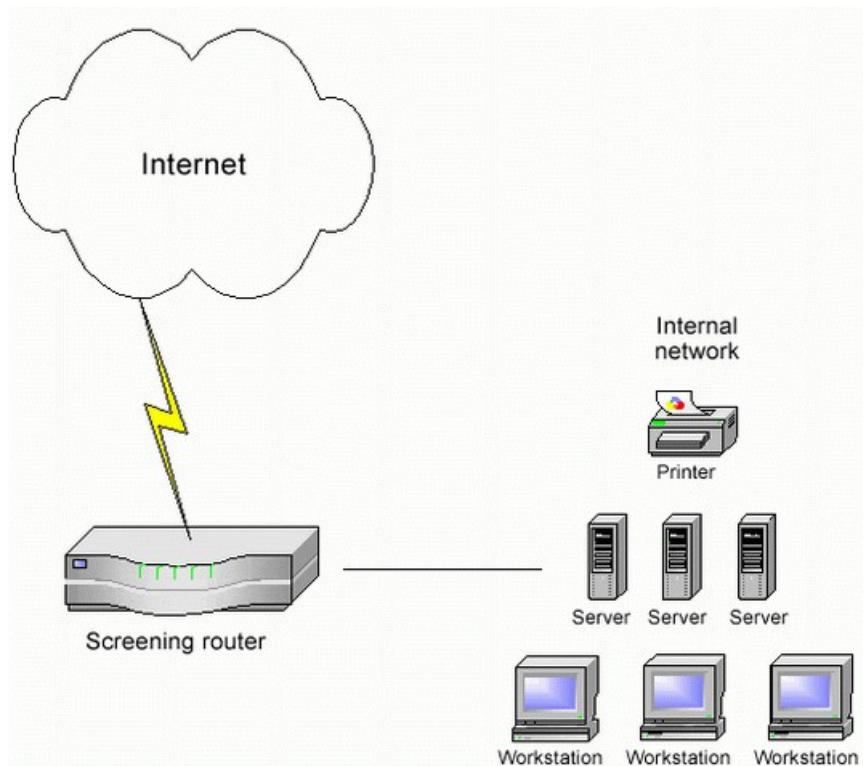
- ✓ **Firewalls dedicados:** son equipos que tienen instalada una aplicación específica de cortafuegos y trabajan de forma autónoma como cortafuegos.

- ✓ **Firewalls integrados:** se integran en un dispositivo hardware para ofrecer la funcionalidad de firewall (switches, routers que integran funciones de cortafuegos).

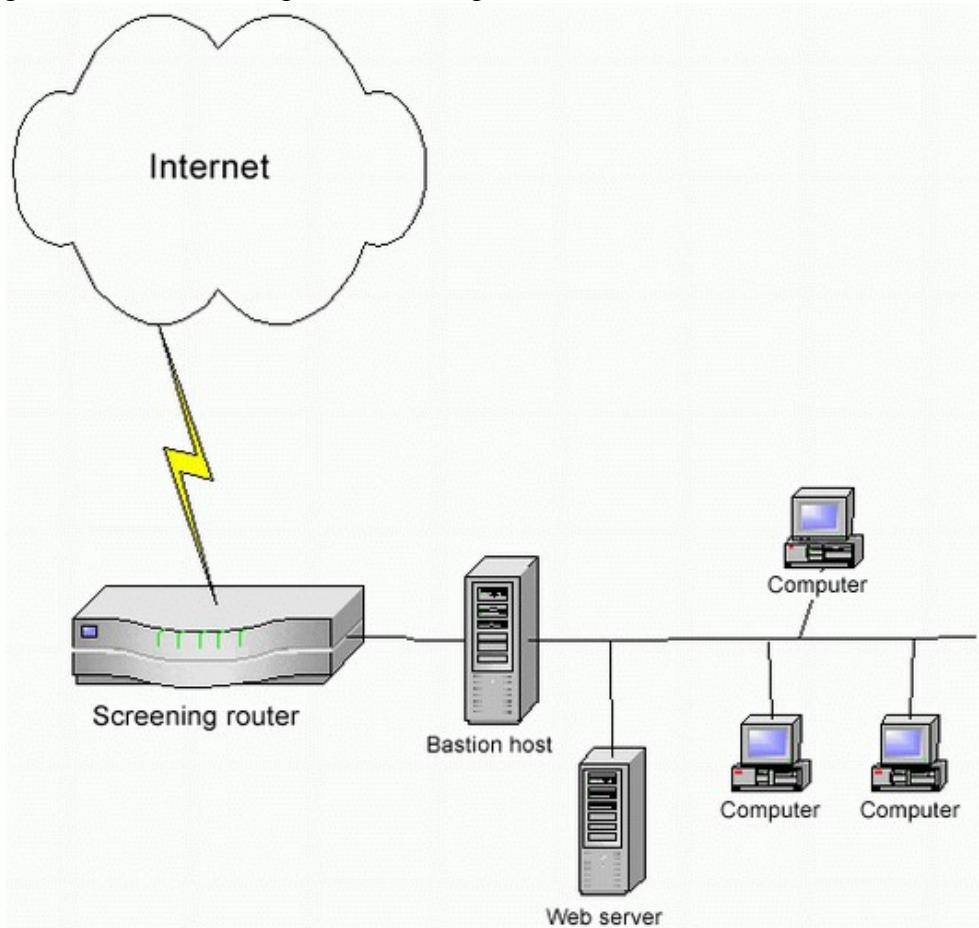
- ✓ **Firewalls personales:** se instalan en distintos equipos de la red de forma que lo protege individualmente de amenazas externas (por ejemplo el firewall de windows).

Arquitecturas de cortafuegos:

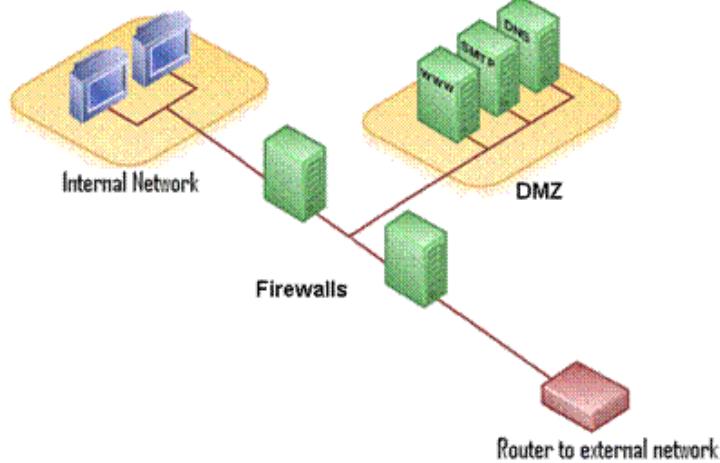
- ✓ **Screening router:** Router que realiza tareas de filtrado como frontera entre la red pública y la privada.



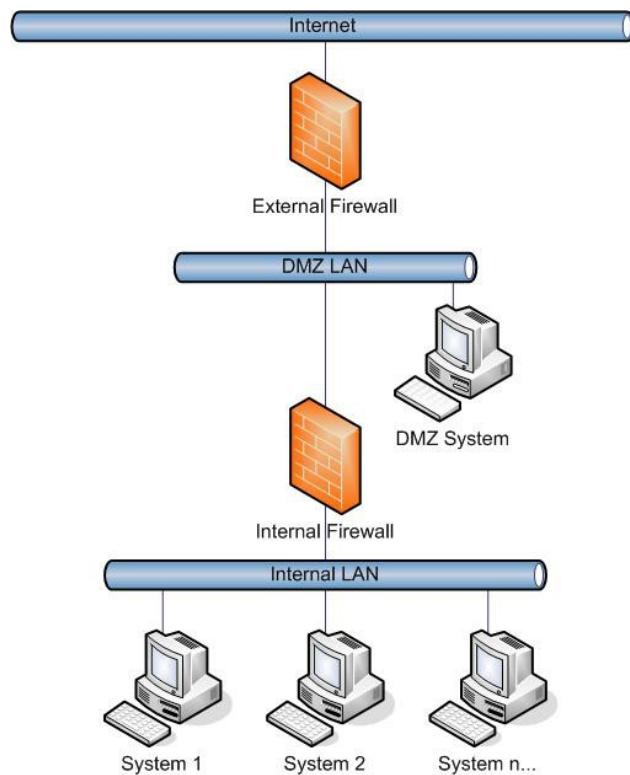
- ✓ **Screened Host:** Combina un ruter fronterizo exterior y un servidor proxy que filtrara y permitirá añadir reglas de filtrado a las aplicaciones empleadas.



- ✓ **Screened-subnet**: mediante la creación de una subred intermedia denominada DMZ o zona desmilitarizada entre la red externa y la red privada interna, permite tener 2 niveles de seguridad, uno algo menor en el cortafuegos mas externo y uno de mayor nivel en el cortafuegos de acceso a la red interna.



DMZ o zona desmilitarizada es una red local que se ubica entre la red interna de una organización y una red externa, generalmente internet, donde se ubican los servidores HTTP, DNS, FTP y otros de carácter publico. Habitualmente usa dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos.



La **política de seguridad** para la **DMZ** es la siguiente:

- ✓ El tráfico de la red externa a la DMZ está autorizado y a la red interna está prohibido.
- ✓ El tráfico de la red interna a la DMZ está autorizado y a la red externa está autorizado.

Proxy es una aplicación o sistema que gestiona las conexiones de red, sirviendo de intermediario entre las peticiones de servicios que requieren los clientes (HTTP, FTP, etc.), creando así una memoria cache de las peticiones y respuestas por parte de los servidores externos. También añaden funciones de control y autenticación de usuarios y reglas de filtrado de contenidos.

Capítulo 8 Configuraciones de Alta disponibilidad.

Alta disponibilidad se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento, debido a su carácter critico, las **soluciones** adoptadas son:

- ◆ **Redundancia en dispositivos hardware**, de tal manera que ante un fallo continúe el servicio, por ejemplo duplicados de equipos, servidores, fuentes de alimentación redundantes o dispositivos de red redundantes.
- ◆ **Redundancia, distribución y fiabilidad en la gestión de la información**, por ejemplo:
 - ✓ Sistemas RAID de almacenamiento.
 - ✓ Centros de procesamiento de datos de respaldo, garantizando copias de seguridad en distintas ubicaciones.
- ◆ **Redundancia en las comunicaciones**, por ejemplo dos salidas a internet con dos proveedores distintos de tal manera que si falla uno se mantenga la conexión con el otro (Balanceo de carga).
- ◆ Independencia en la administración y configuración de aplicaciones y servicios. Por ejemplo con la **virtualización** que ofrece servidores dedicados independientes bajo una misma maquina.

RAID (Redundant Array of Independent Disks), es un conjunto de discos independientes entre los que se distribuye o replica la información y que puede ser gestionado por:

- ✓ **Hardware**: el control se realiza por medio de tarjetas controladoras RAID dedicadas que gestionan el control de los diferentes discos.
- ✓ **Software**: Es el sistema operativo el que gestiona los discos mediante una controladora de discos tipo IDE, SATA, SCSI, etc.
- ✓ **Híbridos**: son los que están basados en software y hardware, con controladoras RAID baratas.

Las configuraciones RAID estándar son:

- ✓ **RAID 0** o data striping: conjunto dividido, distribuye los datos equitativamente entre dos o mas discos sin información de paridad que proporcione redundancia, incrementa el rendimiento pero si falla un disco se pierden los datos.
- ✓ **RAID 1** o data mirroring: conjunto espejo, crea una copia exacta de los datos en dos o mas discos, si falla uno de los discos la información no se pierde al estar replicada en otro disco.
- ✓ **RAID 5**: conjunto dividido con paridad distribuida, requiere un mínimo de tres discos, consiste en una división a nivel de bloques distribuyendo la información de paridad entre los discos miembros del conjunto, gracias a la información de paridad si falla un disco la información no se pierde.

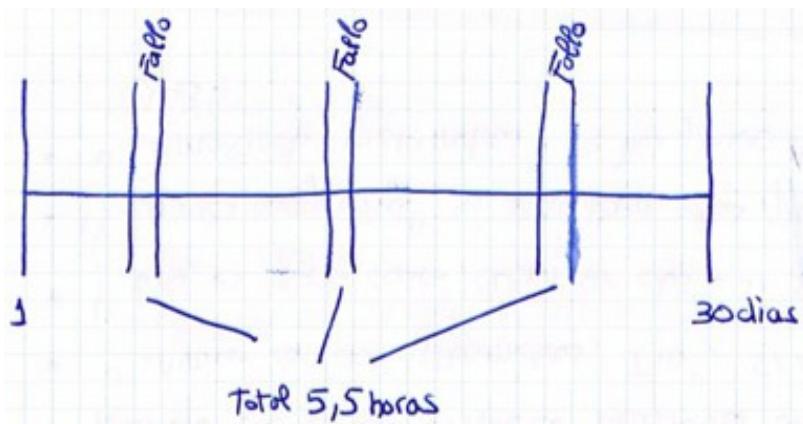
Balanceo de carga, consiste en un dispositivo hardware o software que reparte las peticiones de los clientes entre los diferentes servidores a los que se conecta dicho dispositivo, un ejemplo es cuando tenemos dos router distintos y cada un con un proveedor de internet diferente y hacemos que las peticiones que se hacen hacia internet por parte de los usuarios de la red salgan repartidas entre dichos router.

Virtualización, permite la ejecución simultanea de distintos sistemas operativos sobre una aplicación ejecutada y soportada bajo un equipo y sistema operativo determinado.

Capítulo 1 Principios de seguridad y alta disponibilidad

Ejercicio Alta disponibilidad:

Si durante un mes un equipo se ha caído 3 veces con un tiempo total de inactividad de 5,5 horas.
calcular el MTTR, MTTF y MTBF.



$$\text{Tiempo medio reparación} \parallel \text{MTTR} = 5,5 \text{ horas} / 3 = 1,83 \text{ horas}$$

$$\text{Tiempo medio hasta que se produce un fallo} \parallel \text{MTTF} = (30 \times 24) - 5,5 / 3 = 714,5 / 3 = 238,16 \text{ horas}$$

$$\text{Tiempo entre fallos} \parallel \text{MTBF} = 30 \times 24 / 3 = 240 \text{ horas}$$

Mayor nivel de disponibilidad, los 5 nueves (99,999%) ¿a que equivale en tiempo al año?
Porcentaje de funcionamiento sin fallos = 99.999% al año.

$$1 \text{ año} = 365 \times 24 \times 60 = 525.600 \text{ minutos}$$

$$\begin{aligned} 100\% & - 525.600 \\ 99,999\% - X & = 525.594,74 \end{aligned}$$

$$525.600 - 525.594,74 = 5,25 \text{ minutos de tiempo fuera de servicio al año, máximo.}$$

Test de conocimientos (pag.32)

1 La primera característica a garantizar en un sistema seguro es:

- a) Confidencialidad.
- b) Integridad.
- c) Disponibilidad.
- d) No repudio.

2 Indica qué sentencia es falsa:

- a) La integridad permite asegurar que los datos no se han falseado.
- b) Confidencialidad es desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- c) Disponibilidad es que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

3 Una de las siguientes medidas no pertenece a la seguridad lógica:

- a) Contraseñas.
- b) SAI.
- c) Copia de seguridad.
- d) SW antimalware.

4 ¿Qué elemento de un sistema informático se considera más crítico a la hora de protegerlo?

- a) Comunicaciones.
- b) Software.
- c) Hardware.
- d) Datos.

5 Un hacker:

- a) Siempre tiene una finalidad maliciosa.
- b) La mayoría de las veces tiene una finalidad maliciosa.
- c) A veces posee una finalidad maliciosa, entonces se denomina *cracker*.
- d) Es un curioso con una finalidad conocida.

6 El *phishing*:

- a) Es un tipo de fraude bancario.
- b) Es un tipo de *malware* o virus.
- c) Se contrarresta con un *spyware*.
- d) Se propaga mediante correo electrónico siempre.

7 ¿Cuál es el estándar ISO en materia de auditoría de sistemas de información?

- a) ISO 9001.
- b) ISO 27000.
- c) ISO 27002.
- d) ISO 27001.
- e) COBIT.

8 ¿Y el estándar de buenas prácticas en materia de seguridad informática?

- a) ISO 9001.
- b) ISO 27000.
- c) ISO 27002.
- d) ISO 27001.
- e) COBIT.

9 Con respecto a un análisis forense:

- a) Se realiza siempre *a posteriori* de detectar vulnerabilidades.
- b) Se debe realizar semanalmente.
- c) Se realiza tan solo cuando el sistema de información "ha muerto".
- d) Se realiza siempre *a priori* de detectar vulnerabilidades.

10 Una vez se realiza una auditoría:

- a) Si todo se encuentra correcto no es necesario volver a realizar auditorías.
- b) Es recomendable volver a realizarlas periódicamente.
- c) Es poco probable que todo esté perfecto.
- d) Es recomendable volver a realizarlas periódicamente, pero ya no tan exhaustivas.

Ejercicios propuestos (pag. 30)

Cinco nuevas estafas en Facebook y twitter (Articulo en <http://www.csospain.es/Cinco-nuevas-estafas-en-Facebook-y-Twitter/seccion-alertas/articulo-196360>)

- ¿Que tipos de ataques son los mas comunes que se producen en las redes sociales?
Infecciones de malware (47%) y Phishing (55%)
- ¿Crees que los Ciberdelitos y ciberfraudes proliferan con el uso de las redes sociales?
Si, ya que hay mucha mas gente a la que se puede llegar.
- ¿Que es un Blacklist?
Se trata de una lista donde se registran las direcciones IP que generan Spam.
- Indica alguna web con comprobación de direcciones web o URL, IP, direcciones de mail, etc, que sea potencialmente maliciosas.
<https://www.virustotal.com/#url>
- Indica que precauciones tomarías o como identificarías un fraude a través de una red social.
Ganar dinero fácil por medio de internet.
Reclamos sexuales
- Busca algún nuevo tipo de estafa que se produzca a través de las redes sociales.
La estafa 'caminandoalpasado' (<http://mexico.cnn.com/tecnologia/2012/07/11/la-estafa-caminandoalpasado-esta-circulando-en-redes-sociales>)

Web Hispasec, multitud de noticias y estudios de actualidad, analiza las noticias de la ultima semana.

- ¿Que vulnerabilidades y amenazas se describen?.
 1. Vulnerabilidad de USSD en Android neutraliza la SIM y resetea teléfonos de algunas marcas
 2. Google Chrome corrige 24 vulnerabilidades
 3. PhpMyAdmin distribuido temporalmente con una puerta trasera
- ¿Que tipo de precauciones se recomiendan?
 1. Para mitigar el error, Collin Mulliner ha desarrollado una pequeña aplicación para Android llamada 'TelStop' que permite que estos USSD deban ser aceptados por parte del usuario antes de ser ejecutados.
 2. Actualizar aplicación
 3. PhpMyAdmin ha recomendado la descarga y reinstalación completa del software si contiene el fichero 'server_sync.php'

Según recomendaciones de microsoft una contraseña segura debe tener 14 caracteres.

- ¿Tus contraseñas de acceso a sistemas operativos, mail, etc. son seguras?
Son seguras y con todo tipo de caracteres.
- ¿Cada cuanto tiempo cambias las contraseñas?
Cuando me parece.

Comprueba el estado de actualización de tus aplicaciones, realiza el análisis desde la web de Secunia con su inspector online.

- ¿Que aplicaciones disponían posibles vulnerabilidades al no encontrarse totalmente actualizadas?
No funciona con OS X
- ¿Cual es la solución propuesta?

Respecto a los navegadores web.

- ¿Que opciones de seguridad o privacidad permiten configurar tus navegadores web?
 Decir a los sitios web que no quiero ser rastreado
 Advertir cuando algún sitio intente instalar complementos
 Bloquear sitios reportados como atacantes
 Bloquear sitios reportados como falsificados
- ¿Se aceptan cookies?
 Si
- ¿Recuerdan contraseñas?, ¿cuales?
 Si, de acceso a los sitios, se puede desactivar.
- ¿Bloquean ventanas emergentes?
 Si
- ¿Disponen de restricciones de acceso a determinados sitios web?
 ???

Busca al menos dos antivirus en linea y realiza análisis de tu sistema, realiza una comparativa entre las soluciones empleadas.

<http://www.pandasecurity.com/spain/homeusers/solutions/activescan/>

<http://www.bitdefender.es/scanner/online/free.html>

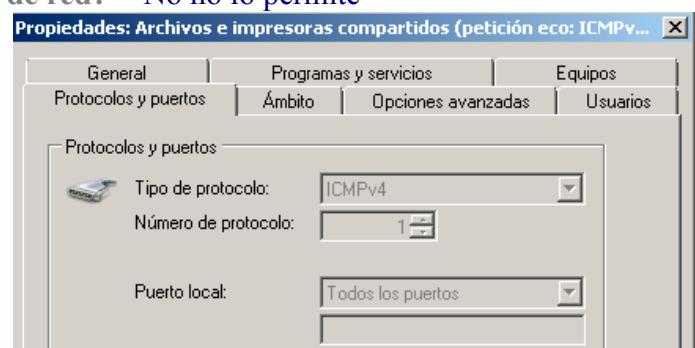
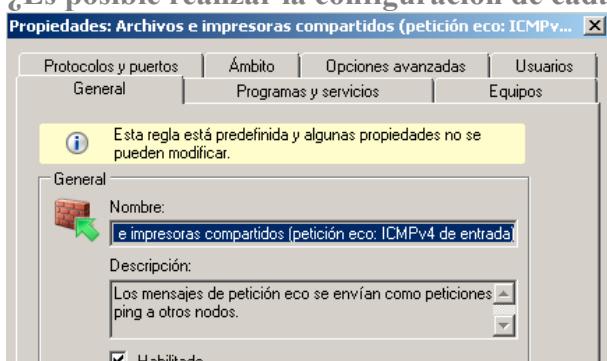
Mi sistema no es compatible con estos análisis (OS X)

¿Crees que los sistemas GNU/Linux al no disponer de tantas opciones de herramientas antivirus son mas seguros que los sistemas windows?, ¿porque?

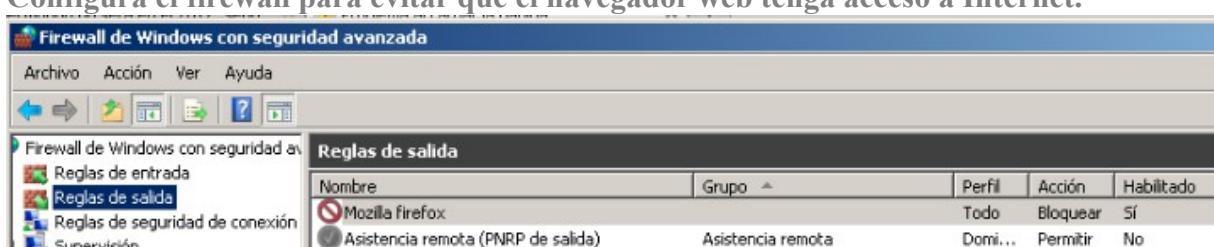
¿En caso de tener un servidor FTP bajo Linux, alojando archivos potencialmente maliciosos, seria recomendable tener alguna herramienta que rastree posibles archivos infectados?
 Si, para que estos no se transfieran a los usuarios.

Configura el el firewall de windows para evitar contestar a peticiones de red de eco entrante.

¿Es posible realizar la configuración de cada puerto de red? No no lo permite



Configura el firewall para evitar que el navegador web tenga acceso a Internet.



Test sobre malware

1. ¿Cuál de los siguientes programas maliciosos es más probable que haga que tu ordenador deje de funcionar?

- a. Troyano
- b. Gusano
- c. **Virus**
- d. Spyware
- e. Adware

2. ¿Cuál de los siguientes no es un programa en sí mismo, sino que se “pega” a otro?

- a. Troyano
- b. Gusano
- c. **Virus**
- d. Spyware
- e. Adware

3. ¿Cuál de los siguientes es más dado a enviar correos spam desde tu ordenador?

- a. Troyano
- b. **Gusano**
- c. Virus
- d. Spyware
- e. Adware

4. ¿Cuál de los siguientes es menos probable que sea detectado con software antivirus estándar?

- a. Troyano
- b. Gusano
- c. Virus
- d. Spyware
- e. **Adware**

5. ¿Cuál de los siguientes es más probable que venga con otro “malware”?

- a. **Troyano**
- b. Gusano
- c. Virus
- d. Spyware
- e. Adware

6. ¿Cuál de los siguientes es más probable que instale una “puerta trasera” que se conecta a Internet en nuestro equipo?

- a. **Troyano**
- b. **Gusano**
- c. Virus
- d. Spyware
- e. Adware

7. ¿Cuál de los siguientes es más probable que esté implicado en un ataque de denegación de servicio?

- a. Troyano
- b. **Gusano**
- c. Virus
- d. Spyware
- e. Adware

8. ¿Cuál de los siguientes es más probable que sea usado para robar tu identidad?

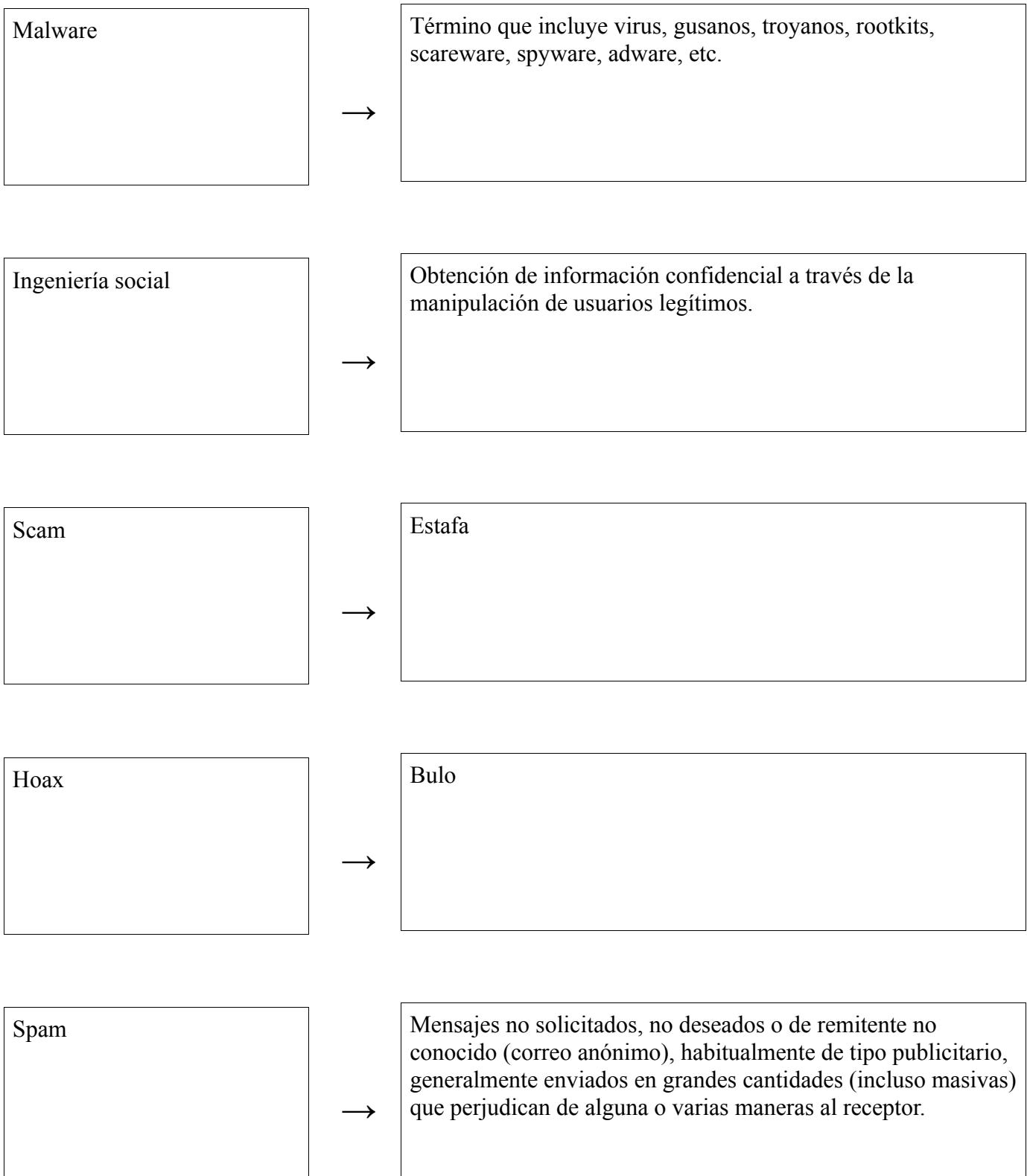
- a. Troyano
- b. Gusano
- c. Virus
- d. **Spyware**
- e. Adware

Respuestas:

1. c. virus. Trojans, worms, spyware, and adware all depend on your computer staying up and running. They use your computer's resources to accomplish whatever their designer intended, such as sending emails, displaying advertising, or stealing information from your computer. Viruses, however, are usually created by vandals who just want to damage as many computers as possible.
2. c. virus. Viruses are not stand-alone programs. Just as biological viruses must take over the cells of their host in order to function and reproduce; computer viruses must take over one or more files of the computer on which they are stored. Trojans, worms, spyware, and adware are all stand-alone programs that can run without the help of another application, though they often come bundled with other applications as a decoy, or with other malware.
3. b. worm. Worms are stand-alone programs that are often used to send spam emails, or emails containing viruses. Trojans often contain worms which are then installed for the purpose of sending spam emails, but the worms are what actually send the emails.
4. e. adware. In the strictest sense, adware is rarely patently illegal or destructive, and so antivirus software makers have traditionally avoided treating it as malware. Adware designers are usually large advertising companies with hundreds of millions of dollars, and they take care to insert end-user licensing agreements (EULA) that supposedly mean that the software is installed with permission. Also, adware will not usually do anything more destructive than show advertising. Nonetheless, adware can quickly multiply on a computer, hogging system resources and causing a computer to slow down or even malfunction. That's why most anti-spyware software makers target adware as well.
5. a. Trojan. By definition, Trojans bear other malware within them, just as the mythical wooden horse bore Greek warriors. The malware can be viruses, worms, spyware, or adware.
6. b. worm. Worms most commonly install a "backdoor" internet connection in order to send out data (for instance, spam emails or requests to remote servers) undetected.
7. b. worm. Worms, which most commonly install a "backdoor" internet connection on the host computer, are perfect for sending out the millions of server requests needed to achieve a denial-of-service attack. A denial-of-service attack is when a server is maliciously sent so many hits that it is overwhelmed and cannot continue to operate.
8. e. Spyware. Spyware is malware that collects information from your computer and sends it to another remote machine, so by definition any software that steals your identity is spyware. However, spyware is often installed on your computer by a Trojan, or sent to you by another computer infected with a worm, so other kinds of malware pose an indirect threat of identity theft as well.

Técnicas de ataque

Pon el recuadro en su posición correcta (resuelto).



Sniffing	→	Monitorización del tráfico de una red para hacerse con información confidencial.
Spoofing	→	Falsificación o suplantación de identidad.
Phishing	→	Normalmente usa la ingeniería social para intentar adquirir información confidencial (contraseñas, números de tarjetas de crédito, etc) de forma fraudulenta. A menudo el estafador, phisher, se hace pasar por una empresa de confianza en un correo electrónico, intentando que la víctima visite una página falsa donde debe dar sus datos.
Password cracking	→	Descifrar la contraseña de sistemas o aplicaciones.
Botnet	→	Conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El operador de la botnet puede controlar los equipos infectados de forma remota, a través del IRC o, más recientemente, HTTP.
Denegación de servicio (DoS)	→	Ataque a un sistema que deja un servicio inaccesible para los usuarios legítimos. Utiliza métodos como obligar a la víctima a utilizar todo su ancho de banda para responder a los atacantes o ir sobrecargando otros recursos de la víctima (la memoria, por ejemplo), de forma que acaban agotándose.

Capítulo 2 Seguridad pasiva

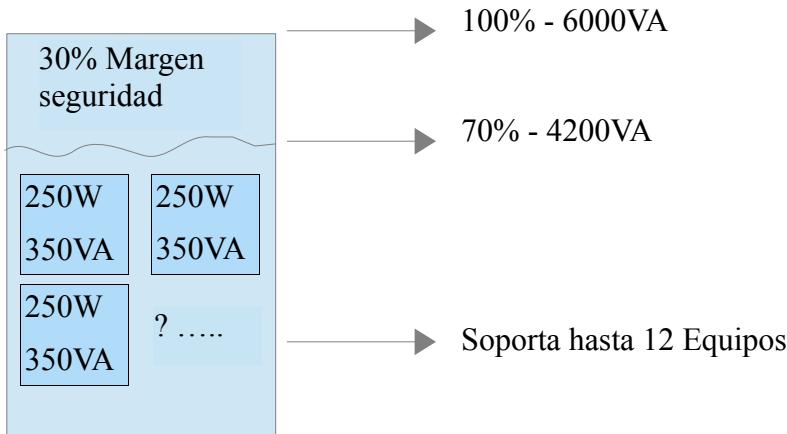
Ejercicio Calculo SAI:

A cuantos equipos de 250W cada uno podría dar servicio de forma adecuada una SAI de 6000VA

Cada equipo son $250 * 1,4 = 350\text{VA}$

El 70% de 6000VA es $= 6000\text{VA} * 70/100 = 4200\text{VA}$ (es una regla de 3)

Calculo de cuantos equipos para 4200VA $= 4200/350 = 12$ Equipos



Test de conocimientos (pag.64)

- 1** Las medidas de seguridad biométricas:
- a) Permiten el acceso a un sistema mediante contraseña asimétrica.
 - b)** Emplean la biología para medir parámetros de seguridad.
 - c) Emplean características biológicas para identificar usuarios.
 - d) Son el fundamento de la identificación mediante certificado digital.

- 2** Las SAIs:
- a) Permiten conectarse ininterrumpidamente a la red eléctrica.
 - b)** Suministran corriente eléctrica frente a cortes de luz.
 - c) Son dispositivos de almacenamiento de alta disponibilidad.
 - d) Son programas que permiten mantener confidencialidad.

- 3** Los armarios o bastidores para albergar sistemas no poseen:
- a) Profundidad variable.
 - b)** Ancho fijo.
 - c) Altura múltiplo de 1 U.
 - d)** Profundidad fija.

- 4** El sistema biométrico más fiable y seguro es:
- a) Reconocimiento de voz.
 - b)** Huella dactilar.
 - c)** Iris.
 - d) Escritura y firma.

- 5** La pinza ampermétrica sirve para realizar medidas de:
- e) Voltaje (V).
 - f) Potencia aparente (VA).
 - g)** Corriente eléctrica (A).
 - h) Potencia real (W).

- 6** En caso de tener una instalación CPD crítico con un suministro eléctrico muy fluctuante, el tipo de SAI a utilizar es:
- a)** Online o doble conversión.
 - b) Offline.
 - c) Inline.
 - d) Línea interactiva.

- 7** Si el espacio que disponemos para realizar copias de seguridad es limitado éstas deben ser:
- a) Completas.
 - b)** Incrementales.
 - c) Diferenciales.
 - d) Completas + Diferenciales.

- 8** El sistema biométrico mas empleado por su relación fiabilidad/coste es:
- a) Reconocimiento de voz.
 - b)** Huella dactilar.
 - c) Iris.
 - d) Escritura y firma.

- 9** En los sistemas GNU/Linux para realizar copias de seguridad automatizadas no se emplea el comando:
- a)** Bkp.
 - b) Crontab.
 - c) Tar.
 - d) Gzip.

Ejercicios propuestos (pag. 62)

1. Realiza una tabla comparativa en la que compares el tamaño en Gigabytes (GB), precio del dispositivo y divide el precio/capacidad o tamaño en GB para obtener el precio por cada GB de distintas memorias comerciales: memoria RAM, disco duro a 5400 y 7200rpm, CD, DVD, cinta de Backup, memorias y discos duros USB.

Dispositivo	Precio	Capacidad	Precio por GB
HD 5400rpm	158,24 €	3000,0GB	0,05 €
Cinta Backup Dell LTO 4 Worm	52,00 €	800GB	0,07 €
DVD	0,37 €	4,7GB	0,08 €
HD 7200rpm	57,79 €	500,0GB	0,12 €
CD	0,28 €	0,7GB	0,40 €
Pendrive	6,23 €	8,0GB	0,78 €
MemoriaSD	6,35 €	8,0GB	0,79 €
SSD	112,76 €	128,0GB	0,88 €
Modulo RAM DDR3	40,47 €	8,0GB	5,06 €

¿Cual es la memoria mas barata?

En precio por GB el disco duro de 5200rpm y 3TB

¿Cual es la mas rápida?

La memoria RAM DDR3

¿Crees que las memorias de estado sólido o flash sustituirán a los discos magnéticos como el disco duro?
A medida que su precio disminuya, aumente la capacidad y se equipare al de los discos duros si.

2. Busca información comercial en HP o Dell sobre sistemas de almacenamiento en cinta.

Unidad de almacenamiento en cinta modelo PowerVault LTO-3-080 con un precio de 1.229€ (sin IVA)

Cinta LTO-3 WORM de 400GB a un precio de 35,99 (sin IVA), 43,54€ IVA incluido

<http://www.dell.com/es/empresas/p/powervault-tape-drives>

Paquete de 1 cartuchos de cinta LTO4-WORM de Dell a 52€

¿Crees que hoy en día se siguen utilizando?

No sabría decir, pero observando que hay fabricantes que lo ofrecen será porque en las empresas se seguirá usando este sistema.

¿Cuáles suelen ser sus aplicaciones?

Yo creo que las aplicaciones son como medio de backup, copias de seguridad de datos.

¿Porque crees que se siguen empleando?

Según la tabla comparativa de más arriba es uno de los medios más baratos por GB de almacenamiento, además de que es posible que haya muchas empresas que vengan usando ese sistema desde hace tiempo y les suponga más caro el cambio de sistema.

¿Cual es el coste por MB?

0,07€ para el cartucho de 800GB

0,10€ para el cartucho de 400GB

3. Busca una empresa que se dedique a recuperar los datos de fallos físicos de discos e indica sus precios y servicios ofertados.

<http://www.recuperadata.com>

¿Te parecen caros los servicios de recuperación de datos?

Para un usuario normal son altos los precios.

Discos Duros

Recuperar disco duro con daños **LÓGICOS**. Precio por cada disco duro

SERVICIO	DIAGNÓSTICO	PRECIO
Estándar	Gratis*	450€+IVA
Express	150€+IVA	650€+IVA
Urgente	200€+IVA	750€+IVA

Discos Duros

Recuperar disco duro con daños **FÍSICOS**. Precio por cada disco duro

SERVICIO	DIAGNÓSTICO	PRECIO
Estándar	Gratis*	1.300€+IVA
Express	Gratis*	1.977€+IVA
Urgente	200€+IVA	2.623€+IVA

Discos de Estado Sólido (SSD)

Recuperación De Datos de daños **LÓGICOS**. Precio por cada disco de estado sólido (SSD)

SERVICIO	DIAGNÓSTICO	PRECIO
Estándar	100€+IVA	450€+IVA
Express	150€+IVA	650€+IVA
Urgente	200€+IVA	750€+IVA

Discos de Estado Sólido (SSD)

Recuperación De Datos de daños **FÍSICOS**. Precio por cada disco de estado sólido (SSD)

SERVICIO	DIAGNÓSTICO	PRECIO
Estándar	150€+IVA	1.500€+IVA
Express	200€+IVA	2.277€+IVA
Urgente	300€+IVA	2.923€+IVA

¿Cuales son los principales fallos, recomendaciones y precauciones que se deben tener con los discos duros?
Bloqueos del sistema, Averías mecánicas, Borrados involuntarios, Golpes y caídas, Virus, etc.
Sistema RAID, copias de seguridad, evitar golpes y vibraciones,

4. Para realizar copias de seguridad en internet hemos visto que existen sitios FTP gratuitos como Dropbox, Idrive o mozy, existen otras empresas especializadas en Backup remoto de pago. Analiza que servicios ofrecen y a que precios las empresas:

www.copiadaseguridad.com

Espacio contratado	Cuota de alta	Cuota mensual*
0,5 GB = 500 MB	Gratis	7,25€
1 GB = 1.000 MB	Gratis	14,90€
2 GB = 2.000 MB	Gratis	21,66€
4 GB = 5.000 MB	Gratis	34,25€
10 GB = 10.000 MB	Gratis	64,80€
20 GB = 10.000 MB	Gratis	99,72€
100 GB = 50.000 MB	Gratis	348,00€
Otros Servicios		Consultar

*IVA no incluido

Servicio de copia de seguridad remota

Servicio de copia de seguridad personalizado adaptable a cualquier presupuesto

Excelente servicio de atención al cliente

Server Backup Copia de seguridad para las PYME.

PC / Mac Backup Posibilidad de backup remote sobre un solo PC o Mac.

Pack de prueba durante 90 días gratis y sin ninguna obligación.

a partir de € 35,- al mes.

a partir de € 20,- al mes.

5. Para garantizar un espacio seguro de nuestras copias de seguridad podemos optar por contratar los servicios de empresas que realicen la recogida y custodia de copias de seguridad.

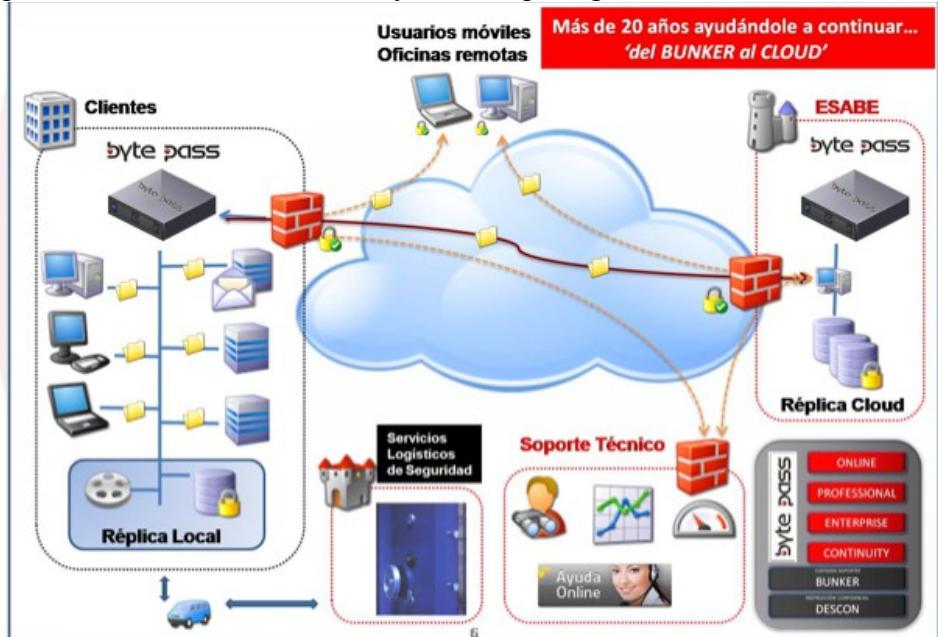
¿Que servicios y precios ofrecen empresas como www.esabe.com y www.copiassegura.com?

Servicios Tecnológicos (byte pass)

- **ONLINE.** Copias de Backup a través de Internet, mediante cifrado seguro.
- **PROFESSIONAL.** Servicio que combina el backup local con un backup remoto para pymes.
- **ENTERPRISE.** Servicio orientado a proteger entornos multiplataforma con backup local y remoto usando tecnología de deduplicación.
- **CONTINUITY.** Servicio que garantiza la continuidad tras un incidente. Levantamos el servicio en minutos con una imagen reciente. SIN RESTAURACIONES.

Servicios Logísticos

- **BUNKER.** Guarda y Custodia de copias de seguridad en soportes físicos (cintas, discos y media en general), en centros seguros.
- **DESCON.** Destrucción confidencial y certificada de cintas, discos, media en general y documentos.



No pone precios en la web.

¿Que normativa deben cumplir con respecto a seguridad informática?

<http://cert.inteco.es/Formacion/Legislacion/>

Legislación Nacional

En materia de seguridad informática existen siete normativas legales relevantes:

1. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD). [\[Documento disponible en HTML \(BOE 298 de 14-12-1999\)\]](#)
2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. [\[Documento disponible en HTML \(BOE 298 de 19-01-2008\)\]](#)
3. Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE). [\[Documento disponible en HTML \(BOE 166 de 12-07-2002\)\]](#)
4. Ley 59/2003, de 19 de diciembre, de Firma Electrónica. [\[Documento disponible en HTML \(BOE 304 de 20-12-2003\)\]](#)
5. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (LPI), regularizando, aclarando y armonizando las disposiciones vigentes en la materia. [\[Documento disponible en HTML \(BOE 97 de 22-04-1996\)\]](#)
6. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. [\[Documento disponible en HTML \(BOE 25 de 29-01-2010 páginas 8089 a 8138\)\]](#)
7. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. [\[Documento disponible en HTML \(BOE 25 de 29-01-2010 páginas 8139 a 8156\)\]](#)

Legislación Europea

En materia de seguridad informática existen dos normativas legales relevantes:

1. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre.[[Documento disponible en PDF \(Directiva 2009/136/CE\)](#) ].
2. Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre.[[Documento disponible en PDF \(Directiva 2009/140/CE\)](#) ].

7. Dentro de las herramientas de copia de seguridad encontramos herramientas específicas de realización de copia exacta, clonado o imágenes de disco, que permiten la restauración exacta de una determinada partición de disco. Indica algunos ejemplos de software de clonado de discos.

Clonezilla	http://clonezilla.org/
ImageDrive	http://www.runtime.org/data-recovery-products.htm
HD clone	http://www.miray.de/products/sat.hdclone.html#versions
Macrium reflect	http://www.macrium.com/

¿Como se guardara la copia de seguridad por ejemplo para una partición que ocupe 40Gb?

Por ejemplo con clonezilla solo se copian los bloques de la partición que están ocupados y ademas comprime la copia, por lo que la copia solo ocupara como máximo lo que este realmente ocupado si no se comprime.

¿Se realiza en un único soporte?

Para mayor seguridad es mejor tener al menos un duplicado

8. En ocasiones para poder restaurar la configuración de un equipo es interesante tener una copia de seguridad de nuestros controladores. Realiza una copia de seguridad de los controladores o drivers de tu equipo mediante alguna aplicación específica como DriverMax o similar. Valora ventajas e inconvenientes de este tipo de software en función de las opciones que permite realizar.

<http://www.innovative-sol.com/drivermax/>

¿Que utilidad puede tener una copia de seguridad de tus drivers?

Tenerlos a mano en caso de restauración o reinstalacion del SO

¿Es posible siempre recuperarlos, incluso teniendo el listado de dispositivos?

??? pide crearse una cuenta para poder probarlo

¿Y en caso de no tener dicho listado?

9. Análisis de mejoras de un CPD en una solución real. Lee y analiza el siguiente caso real “Solución integral de CPD altamente seguro para supermercados Condis”, en la fuente web:

http://www.abast.es/cs_condis_cpd.shtml

¿Que se considera un “traslado en caliente”?

Un traslado en caliente consiste en mover el CPD de lugar sin que eso signifique una interrupción del sistema cuando deveria de seguir funcionando.

¿Cuales eran los riesgos que corrían y que podrían poner en peligro su anterior CPD?

Que estaba en una entorno de oficina normal, donde casi todo es madera y papel, lo que significa que hay riesgo de incendio, ademas tambien tenían riesgo de inundaciones que ya se habían producido goteras en otras partes del edificio, la auditoria sobre el cumplimiento de la LOPD les alerto de protege mejor el acceso a los datos y sistemas, por ejemplo de intrusiones internas (aunque no habían tenido problemas de este tipo).

¿Que es una auditoria?

Un procedimiento que sirve para ver si cumple los requisitos el CPD

¿Quien tomo la decisión de cambio?

El Consejo de Administración y la Dirección General de Condis como respuesta a las inquietudes del departamento de IT.

¿Como se podrían resumir las soluciones adoptadas por la empresa en los distintos ámbitos?

Escoger un tipo de cerramiento totalmente estanco e ignífugo que proporcionase total protección frente a los riesgos de agua y fuego.

¿Las SAIs y el resto de sistemas se encuentran en la misma sala?

Si estaban ya instalados aunque se dividió en dos zonas.

¿Porque?

SEGURIDAD Y ALTA DISPONIBILIDAD

Ejercicios a entregar del tema 2

1 - Linux - Copia de seguridad completa

- * de la carpeta /home/tu_usuario/carpeta , donde el tamaño de la carpeta no debe exceder los 100 Mb
- * a la carpeta /home/tu_usuario/copia
- * que guarde en un fichero de texto de la misma carpeta /home/tu_usuario/copia la fecha en que se realiza
- * Incluir, tanto en este script como en los siguientes, comentarios aclaratorios a cada instrucción
- * Subir el script a una carpeta de nombre 'para_profesor' de tu cuenta en el equipo 'IP servidor'

Contenido archivo **copiatotal.sh** :

```
#!/bin/bash
#Script de copia total
#variable con los directorios que se copian
directorio="/home/juan/carpeta"
#variable con el directorio donde se guarda la fecha del ultimo backup
fechacopia="/home/juan/copia"
#variable con el directorio donde se guarda la copia
backup="/home/juan/copia"
fecha=`date +"%y%b%d"` #fecha de la copia con formato año mes dia
#El comando tar empaqueta los archivos de directorios contenidos en $directorio
#Con 2> redirigimos los mensajes de error al fichero errores_$fecha.txt
tar -vcf $backup/copiatotal_$fecha.tar $directorio 2> $backup/errores_$fecha.txt
#escribo en el fichero logscopias.txt las fechas de las copias totales hechas
echo Copia total realizada_$fecha >> $backup/logscopias.txt
#Se da permisos de ejecucion con: chmod u+x copiatotal.sh
#Se ejecuta en terminal con: sh copiatotal.sh
#Si en errores sale: Removin leading '/' from member names
#indica que al descomprimir quita la primera / de tal manera que se descomprime
#a partir de donde este el fichero copia
```

Las opciones de tar utilizadas son:

- v: (verbose) permite obtener una descripción de los archivos empaquetados/desempaquetados
- c: (create/vrear) crea un archivo tar
- f: (file/archivo) indica que se dara un nombre al archivo tar

2 - Linux - Copia de seguridad anterior programada todas las semanas a determinada hora

- * utilizando cron de forma similar a como configuramos el apagado automático de Linux Mint
- * Sube lo que has puesto en el cron a 'para_profesor'

Contenido File: /tmp/crontab.V15w0k/crontab

```
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# m h dom mon dow command
38 10 * * 2 sh /home/juan/copiatotal.sh
```

3 - Linux - Copia de seguridad completa que se envía a servidor SSH, FTP o similar

- * Añade al primer script una orden de copia remota (scp) para que la copia se envíe a tu cuenta en el equipo 'IP servidor'
- * Subir el script a 'para_profesor'

Contenido archivo **copiatotalscp.sh** :

```
#!/bin/bash
#Script de copia total
#variable con los directorios que se copian
directorio="/home/juan/carpeta"
#variable con el directorio donde se guarda la fecha del ultimo backup
fechacopia="/home/juan/copia"
#variable con el directorio donde se guarda la copia
backup="/home/juan/copia"
fecha=`date +"%y%b%d"` #fecha de la copia con formato año mes dia
#El comando tar empaqueta los archivos de directorios contenidos en $directorio
tar -vcf $backup/copiatotal_$fecha.tar $directorio 2> $backup/errores_$fecha.txt
#escribo en el fichero logscopias.txt las fechas de las copias totales hechas
echo Copia total realizada_$fecha >> $backup/logscopias.txt
#Se da permisos de ejecucion con: chmod u+x copiatotal.sh
#Se ejecuta en terminal con: sh copiatotal.sh
#Si en errores sale: Removin leading '/' from member names
#indica que al descomprimir quita la primera / de tal manera que se descomprime
#a partir de donde este el fichero copia
#ahora se realiza una copia del backup en otro sitio remoto con scp
scp $backup/copiatotal_$fecha.tar usuario@IP:/home/usuario
#donde usuario es el nombre usuario asignado y IP la direccion IP del servidor donde se sube
```

4 - (Opcional) Linux - Que scp no nos pida contraseña

Que pasa cuando hacemos un script para mandar un archivo via scp y que lo haga un cron, obviamente pues lo hacemos para no interrumpirnos en el proceso y entonces tenemos un problema, “¿cómo meter la contraseña?”

Pues no es tan complicado, chequense esto:

En la PC cliente realizamos lo siguiente:

```
# ssh-keygen -d
```

nos va a pedir algunos datos, solo confirmamos, nos va a pedir un passphrase lo dejamos en blanco, luego procedemos con lo siguiente para que la llave pública se encuentre en el servidor a donde queremos accesar.

```
# cat ~/.ssh/id_dsa.pub | ssh usuario@ip-server 'cat >> ~/.ssh/authorized_keys2'
```

Recuerden sustituir usuario e ip-server por los correspondientes en su servidor y listo, con esto estamos agregando la llave generada en id_dsa.pub a las llaves de confianza del servidor y listo ahora hagan un ssh o un scp para que vean que ya no les pide una contraseña.

5 - Linux - Entender y comentar el siguiente script de copias de seguridad

* Subir el script comentado a 'para_profesor'

```
#!/bin/bash
#variable a la que se le asigna el valor “datos” que es una carpeta que contiene los datos a guardar
DIR_A_GUARDAR=datos
#variable a la que se le asigna el valor “copia” que es la carpeta donde se guardan
DIR_DESTINO=copia
#Elimina (rm) backup.3 y todo su contenido (-r), ignorando ficheros no existentes (f)
rm -rf $DIR_DESTINO/backup.3
#Cambia el nombre de backup.2 por backup.3
mv $DIR_DESTINO/backup.2 $DIR_DESTINO/backup.3
#Cambia el nombre de backup.1 por backup.2
mv $DIR_DESTINO/backup.1 $DIR_DESTINO/backup.2
#Crea un enlace duro (-l) con el nombre backup.1 del backup.0
cp -al $DIR_DESTINO/backup.0 $DIR_DESTINO/backup.1
#Copia gracias a comando rsync en backup.0
#solo los cambios entre el directorio datos y lo contenido en backup.0
rsync -a --progress --delete $DIR_A_GUARDAR/ $DIR_DESTINO/backup.0/
```

Seguridad y alta disponibilidad (Capítulo 1 y 2)

Preguntas teóricas:

1. Explica la idea de confidencialidad en el contexto de la seguridad informática.

Es cuando un archivo, mensaje o comunicación solo pueda ser leído y entendido por la persona o sistema que este autorizado.

2. ¿Qué es el no repudio en origen?

Es cuando la prueba de que se ha enviado el mensaje la envía el emisor y la recibe el receptor.

3. ¿A qué se refieren las siglas MTTF? Explícalo brevemente.

Es el tiempo que pasa hasta que falla un dispositivo.

4. ¿Qué es un “script kiddie”?

Son los que se dedican a hackear los sistemas mediante programas ya realizados pero no tienen conocimientos informáticos

5. Diferencia seguridad activa de seguridad pasiva.

La seguridad pasiva tiene que ver con la seguridad física (protección del hardware), ambiental y las copias de seguridad y la seguridad activa con el control de acceso, gestión de sistemas operativos, usuarios y contraseñas.

6. Cita dos medidas que podemos tomar para que un posible corte de suministro eléctrico no suponga la caída de nuestros equipos.

Alimentar los equipos por medio de un SAI

Que el equipo informático disponga de dos sistemas de alimentación (Fuentes) independientes.

7. Explica la diferencia entre hacer copias de seguridad completa+incrementales y completa+diferenciales.

La completa es una copia de todos los archivos y la incremental de los archivos que van cambiando en cada fecha, cada incremental copia solo los archivos que cambian después de la última incremental, mientras que la diferencia es una copia de todos los archivos que han cambiado a partir de una copia total.

8. ¿Qué forma de trabajar de los sistemas operativos es aprovechada por las utilidades de recuperación de datos para llevar a cabo su cometido?

Pues que cuando se borra un archivo marca las posiciones como no ocupadas pero no borra la información que se mantiene hasta que se sobrescriba encima.

9. En el campo de la autenticación, pon un ejemplo de “algo que se sabe”, otro de “algo que se posee” y un tercero de “algo que se es”.

Algo que se sabe una contraseña.

Algo que se posee Una tarjeta de acceso.

Algo que se es Huella dactilar, iris, voz, la firma.

10. ¿Qué sentido tiene conectar una SAI a un ordenador a través del puerto USB?

Por medio de la conexión USB se puede monitorizar la SAI y esta ante un fallo puede dar órdenes al ordenador para que realice un apagado ordenado.

11. ¿Qué es el phishing?

Estafa basada en la suplantación de identidad y la ingeniería social para adquirir acceso a cuentas bancarias o comercio electrónico ilícito.

12. El día 1 de este mes realizamos una copia completa. Posteriormente hemos hecho copias diferenciales los días 5, 15 y 25. Acabamos de perder los datos del disco y tenemos que recuperarlos desde las copias de seguridad. ¿Qué copias y en qué orden debemos restaurar?

Copia total día 1 → diferencial día 5 → diferencial día 15 → diferencial día 25 → Perdida de datos
Primero se recupera la copia total del día 1 y luego la copia diferencial del día 25, solo se perderán los datos a partir del día 25 hasta el momento de la perdida de los datos

13. ¿Qué tres aspectos básicos debe garantizar un sistema seguro?

Confidencialidad: Cualidad de un mensaje, comunicación o datos de que solo podrá ser leído por la persona autorizada.

Integridad: Cualidad de un mensaje, comunicación o datos de que no ha sido alterado.

Disponibilidad: Cualidad de un mensaje, comunicación o datos de que será accesible por los usuarios o procesos autorizados cuando estos lo requieran.

14. ¿Qué es un keylogger?

Programa que captura las pulsaciones de teclas en un teclado por ejemplo para capturar contraseñas.

15. ¿Con qué término inglés nos solemos referir a la suplantación de identidad o falsificación de elementos como la IP, la MAC, la tabla ARP, etc.?

Spoofing

16. Explica cuatro tipos de copias de seguridad implementadas en los sistemas operativos de Microsoft.

Copia total: copia todos los archivos, no tiene en cuenta el atributo A, pero si lo modifica como copiado.

Copia incremental: copia los archivos modificados desde la ultima copia incremental o total, tiene en cuenta el atributo A y lo modifica como copiado.

Copia diferencial: copia los archivos modificados desde la ultima copia incremental o total, tiene en cuenta el atributo A y pero no lo modifica como copiado.

Diaría: Hace copia de los archivos que han cambiado en el dia.

17. Cita 4 amenazas lógicas que pueden afectar a la seguridad de nuestro sistema.

Virus, Gusanos, Troyanos, Falsos programas de seguridad, Puertas traseras, Herramientas de seguridad.

18. ¿Qué tipos de SAI existen y cómo funciona cada uno de ellos?

SAI offline: No estabilizan la corriente y solo generan la tensión de salida cuando se produce un corte de red.

SAI inline: Estabilizan la corriente y solo generan la tensión de salida cuando se produce un corte de red.

SAI online: Generan siempre la tensión de salida independientemente de la entrada.

19. ¿Qué es el malware? Pon 3 ejemplos.

Programas malintencionados que afectan a los sistemas con pretensiones de controlarlos, realizar acciones remotas, inutilizarlo o reenvío de spam.

Como virus, espías, gusanos, troyanos)

Preguntas prácticas:

1. Comparando empresas de hosting, has localizado una que ofrece una disponibilidad mensual de 3 nueves y otra que te garantiza que tu web no estará offline más de 2 días al año. ¿Cuál te ofrece mejor servicio en el apartado de disponibilidad? Justifica tu respuesta con cálculos.

Si el 100% es 365 días al año

$$x = 363 \text{ días} \quad x = 363 * 100 / 365 = 99,452\%$$

Como la segunda tiene una disponibilidad de dos 9, es mejor la primera con 3 nueves.

En el primer caso cada mes o 30'416 días ($365/12$) son 99,9% entonces

100% 30,416dias

$$99,9\% \times X = 99,9 * 30,416 / 100 = 30,386 \text{ dias} \text{ falla } 30,416 - 30,386 = 0,030 \text{ días al mes}$$

$$0,030 * 12 = 0,36 \text{ días al año si sacamos porcentaje es } (365 - 0,36) * 100 / 365 = 99,9\% \text{ superior al } 99,4\%$$

2. ¿Cuántos VA debe ofrecer, como mínimo, una SAI que dará servicio a un almacén en el que hay 2 servidores (250 W cada uno), 2 PCs (100 W c/u), 3 monitores (30 W c/u), 1 switch (0,2 A) y 1 router (0,1 A), si queremos conectar todos los equipos nombrados a la SAI?

$$2 \text{ servidores de } 250 \text{ W} * 1,4 = 700 \text{ VA}$$

$$2 \text{ Pcs de } 100 \text{ W} * 1,4 = 280 \text{ VA}$$

$$3 \text{ Monitores de } 30 \text{ W} * 1,4 = 126 \text{ VA}$$

$$1 \text{ switch de } 0,2 \text{ A} * 220 \text{ V} * 1,4 = 61,6 \text{ VA}$$

$$1 \text{ Router de } 0,1 \text{ A} * 220 \text{ V} * 1,4 = 30,8 \text{ VA}$$

Da un total de = 1198,4VA si estimamos no sobreponer el 70% de la capacidad entonces:

$$70\% \text{ es a } 1198,4 \text{ VA}$$

$$100\% \text{ es a } X \quad X = 1198,4 * 100 / 70 = 1712 \text{ VA} \text{ es lo que tiene que dar el SAI}$$

3. Calcula el MTTR de un servidor que en el último año ha estado 5 veces fuera de servicio, totalizando un tiempo de 17 horas de caída.

MTTR es el tiempo medio de reparación por lo que 17 horas / 5 fallos = **3,4 horas** de media por fallo.

4. Un servidor ha sufrido 6 caídas en los últimos 4 meses. Las 5 primeras se solucionaron en 6 minutos cada una y la 6^a en 40 minutos. Calcula el MTTR, MTTF y MTBF para dicho servidor

$$6 \text{ caídas en 4 meses} \rightarrow 6 \times 5 + 40 = 70 \text{ minutos caídos}$$

$$4 \text{ meses} \rightarrow 4 \times 30 \text{ días/mes} \times 24 \text{ h/día} \times 60 \text{ min/h} = 172800 \text{ minutos en 4 meses}$$

$$\text{MTTR} = \text{Tiempo offline/nº caídas} \rightarrow 70 / 6 = 11,66 \text{ minutos}$$

$$\text{MTTF} = \text{Tiempo funcionando/nº caídas} \rightarrow 172730 / 6 = 28788,33 \text{ minutos}$$

$$\text{Tiempo funcionamiento} \rightarrow \text{Tiempo total} - \text{Tiempo offline} \rightarrow 172800 - 70 = 172730 \text{ minutos}$$

$$\text{MTBF} = \text{Tiempo total/nº caídas} \rightarrow 172800 / 6 = 28800 \text{ minutos}$$

5. ¿Cuántos VA deberá tener como mínimo una SAI adecuada para dar servicio a 17 PCs (70w cada uno), 15 monitores (30w cada uno) y 2 routers (0,30A cada uno)?

$$17 \text{ PCs} \rightarrow 17 \times 70 \text{ W} \times 1,4 \text{ VA/W} = 1666 \text{ VA}$$

$$15 \text{ Monitores} \rightarrow 15 \times 30 \text{ W} \times 1,4 \text{ VA/W} = 630 \text{ VA}$$

$$2 \text{ routers} \rightarrow 2 \times 220 \times 0,30 \times 1,4 \text{ VA/W} = 184,8 \text{ VA}$$

$$\text{Total consumo equipos en VA} = 2480,4 \text{ VA} \text{ es el } 70\% \text{ del total del SAI}$$

Queremos poner una SAI con un margen de capacidad, por lo que escogeremos una para la que 2480,4VA sea el 70% de su capacidad aproximadamente.

$$2480,8 - 70\%$$

$$x - 100\% \quad x = 2480,8 \times 100 / 70 = 3544 \text{ VA}$$

Capítulo 3 Seguridad lógica

Test de conocimientos (pag.87)

1 ¿Qué tipo de cuenta se recomienda para un uso cotidiano en sistemas Windows?

- a) Administrador.
- b) Invitado.
- c) Limitada.
- d) Mínimos privilegios.

2 Una contraseña segura no debe tener:

- a) Más de 10 caracteres.
- b) El propio nombre de usuario contenido.
- c) Caracteres mayúsculas, minúsculas y símbolos.
- d) Frases fáciles de recordar por ti.

3 ¿Qué es la identificación?

- a) Momento en que el usuario se da a conocer en el sistema.
- b) Verificación que realiza el sistema sobre el intento de *login*.
- c) Un número de intentos de *login*.
- d) Un proceso de creación de contraseñas.

4 Para un usuario experimentado como tú, las actualizaciones deben ser:

- a) Automáticas, descargar e instalar actualizaciones automáticamente.
- b) Descargar actualizaciones y notificar si deseas instalarlas.
- c) Notificar, pero no descargar ni instalar.
- d) Desactivar actualizaciones automáticas.

5 Las contraseñas de sistemas GNU/Linux se encuentran encriptadas en el archivo:

- a) */etc/groups*.
- b) */etc/passwd*.
- c) */etc/shadow*.
- d) */etc/sha-pass*.

6 En caso de tener configurada con contraseña el SETUP de la BIOS, y querer prohibir el arranque en modo Live, el primer dispositivo de arranque debe ser:

- a) LAN.
- b) HD.
- c) USB.
- d) CD.

7 El comando `john --wordlist=password.lst passwords`, realiza un ataque:

- a) Diccionario.
- b) Fuerza bruta.
- c) Simple.
- d) PWstealer.

8 Activando la directiva local de seguridad en sistemas Windows “las contraseñas deben cumplir los requisitos de complejidad”, las contraseñas nuevas o renovadas no pueden tener:

- a) 5 caracteres.
- b) Números.
- c) Mayúsculas.
- d) Minúsculas.
- e) Caracteres especiales.

9 Una de las vulnerabilidades en la instalación de Windows XP es:

- a) Crea un conjunto de usuarios administrador.
- b) Crea un usuario Administrador con una contraseña débil.
- c) Crea un usuario Administrador sin contraseña.
- d) Crear 2 usuarios al menos sin contraseña.

10 Desde la utilidad de usuarios y *password* de Windows de Ultimate Boot Recovery no podemos:

- a) Resetear contraseñas.
- b) Recuperar contraseñas.
- c) Modificar contraseñas seguras.
- d) Dejar contraseñas en blanco.

Practica auditoria contraseñas con ophcrack

Se arranca una maquina virtual que tiene un Linux Mint (usuario sad contraseña 12345) y un XP, se arranca bajo linux para usar el programa que crackea las contraseñas 'ophcrack'.

1. Usar Ophcrack

- a) Se ejecuta el programa en terminal con: ophcrack
- b) una vez arrancado el programa se va a Load y se selecciona Encrypted SAM
 - ✓ Se selecciona en la partición de windows la carpeta \WINDOWS\system32\config
 - ✓ Abre el archivo de contraseñas y pinchamos en Crak para que saque contraseñas:

The screenshot shows the ophcrack application window. At the top is a menu bar with 'ophcrack' and icons for Load, Delete, Save, Tables, Crack, Help, and Exit. Below the menu is a toolbar with similar icons. The main area has tabs for 'Progress' (selected), 'Statistics', and 'Preferences'. A large table displays password cracking results for various users. The columns are: User, LM Hash, NT Hash, LM Pwd 1, LM Pwd 2, and NT Pwd. The 'Progress' tab at the bottom shows the status of the attack: Preload done, Brute force done, Pwd found: 3/9, and Time elapsed: 0h 0m 22s.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrador	a0df5b0aaac10037...	e09122aa01a519610...	not found	empty	not found
Invitado		31d6cfe0d16ae931b...			empty
Asistente de ayuda	4317d6de67b65db6...	4ba92e338485c9118...	not found	not found	not found
SUPPORT_388945a0		482bae364a168bb0c...			not found
ral		31d6cfe0d16ae931b...			empty
usuario1	aebd4de384c7ec43...	7a21990fc3d75994...	not found	empty	not found
usuario2	9a5760252b7455de...	0d7f1f2bdeac6e574d...	HOLA	empty	hola
usuario3	fda95fbeca288d44...	066ddfd4ef0e9cd7c2...	not found	empty	not found
usuario4	3c731e26899b5187...	c3c15b7c1b6e194e1...	not found	empty	not found

- ✓ Se ve como ha sacado una contraseña del usuario3 que es **hola**.
- ✓ LM Hash es la primera versión de Hash y NT Hash es una versión mejorada.

2. Usar Ophcrack + tablas

- a) Se ejecuta el programa en terminal con: ophcrack
- b) Se cargan las tablas, para ello se va pincha en Tables y se selecciona XP free small (que la tiene ya en su directorio), abre una carpeta y se pincha en install y OK.
 - ✓ Se pueden cargar mas tablas de la siguiente dirección (algunas son de pago):
 - <http://ophcrack.sourceforge.net/tables.php>
- c) Se va a Load y se se selecciona Encrypted SAM
 - ✓ Se selecciona en la partición de windows la carpeta \WINDOWS\system32\config
 - ✓ Abre el archivo de contraseñas y pinchamos en crak para que saque contraseñas:

ophcrack

The screenshot shows the ophcrack application window. At the top is a menu bar with 'Load', 'Delete', 'Save', 'Tables', 'Crack', 'Help', and 'Exit'. A 'About' button is also present. Below the menu is a tab bar with 'Progress' (selected), 'Statistics', and 'Preferences'. The main area contains a table with columns: User, LM Hash, NT Hash, LM Pwd 1, LM Pwd 2, and NT Pwd. The table lists several users and their corresponding hash values and password attempts. A progress bar at the bottom indicates '10% in RAM'.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrador	a0df5b0aaac10037...	e09122aa01a519610...	RETES	empty	retes
Invitado		31d6cfe0d16ae931b...			empty
Asistente de ayuda	4317d6de67b65db6...	4ba92e338485c9118...	not found	USRDDF5	not found
SUPPORT_388945a0		482bae364a168bb0c...			not found
ral		31d6cfe0d16ae931b...			empty
usuario1	aebd4de384c7ec43...	7a21990fc3d375994...	12345	empty	12345
usuario2	9a5760252b7455de...	0d7f1f2bdeac6e574d...	HOLA	empty	hola
usuario3	fda95fbeca288d44...	066ddfd4ef0e9cd7c2...	HELLO	empty	hello
usuario4	3c731e26899b5187...	c3c15b7c1b6e194e1...	ZNSGE1H	empty	Znsge1h

Table | Directory | Status | Progress

Preload: done Brute force: done Pwd found: 7/9 Time elapsed: 0h 3m 54s

- ✓ Se observa como ha desencriptado mas contraseñas, entre ellas la del usuario administrador, cuya contraseña es **retes**.

The screenshot shows a desktop environment with multiple windows. In the foreground, there is a LibreOffice Writer properties dialog for a document named 'SAD Cap3 01Practica ophcrack.odt'. The 'General' tab is selected, showing details like type (Text en formato OpenDocument), location (/media/ASIR2JUAN/2ASIR/1 Evaluacion Ejercicios), and creation date (30/10/2012, 09:20:07). In the background, an Oracle VM VirtualBox window titled 'ELO modificado [Corriendo]' is open, displaying the ophcrack application. The ophcrack interface shows a password cracking progress table and a progress bar indicating '10% in RAM'. A note in the ophcrack window states: '✓ Se observa como ha desencriptado mas contraseñas, entre ellas la del usuario administrador, cuya contraseña es retes'.

Comprobación de fortaleza de contraseñas con John de Ripper

1º Se instala 'bkhive' y 'John de Ripper' (en este caso en un Linux de una maquina virtual que también tiene una partición con windows, en un ordenador con windows se arrancaría un Linux en live CD), es necesario tener conexión a internet.

- Se instala bkhive sudo apt-get install bkhive
- Se instala John sudo apt-get install john

2º Para recuperar la 'clave del sistema', necesaria para luego descifrar las passwords

- bkhive /media/nombre-particion-XP/WINDOWS/system32/config/system paso1.txt

```
sad@sadpruoph ~ $ ls -l /media/
total 8
drwx----- 1 sad  sad  4096 2012-01-04 21:55 EAB8C2D1B8C29C07
lrwxrwxrwx 1 root root    7 2011-11-01 15:07 floppy -> floppy0
drwxr-xr-x 2 root root 4096 2011-11-01 15:07 floppy0
sad@sadpruoph ~ $ bkhive /media/EAB8C2D1B8C29C07/WINDOWS/system32/config/system
  pas01.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: b53df8ace607115ea66047b5bf879cb6
```

3º Utilizamos la clave anterior para recuperar los hashes de las contraseñas de la SAM

- samdump2 /media/nombre-particion-XP/WINDOWS/system32/config/SAM paso1.txt > paso2.txt

```
sad@sadpruoph ~ $ samdump2 /media/EAB8C2D1B8C29C07/WINDOWS/system32/config/SAM
paso1.txt > paso2.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : SAM
```

4º Ejecutamos 'John de Ripper', quien realiza realmente el 'ataque', Nota: tarda bastante rato.

- john paso2.txt

```
sad@sadpruoph ~ $ john paso2.txt
Created directory: /home/sad/.john
Loaded 10 password hashes with no different salts (LM DES [64/64 BS MMX])
  HELLO          (usuario3)
  12345          [usuario1]
                 (ral)
                 (SUPPORT_388945a0)
                 (Invitado)
  HOLA           (usuario2)
  RETES          (Administrador)
  USRDDF5        (Asistente:2)
  ZNSGE1H        (usuario4)
guesses: 9  time: 0:02:22:07 (3)  c/s: 21967K  trying: 1Q3LTFJ - 1Q3LMB.
Session aborted
```

- Tras mas de 2 horas ha detectado lo mostrado en la imagen superior y aun no ha terminado de ejecutarse por completo, así que se cancela.

En el caso de un sistema Linux los ataques se realizan contra el archivo que contiene las contraseñas encriptadas, esto es /etc/shadow.

- John - -single archivo_shadow este comando permite realizar una búsqueda con combinaciones simples, mediante palabras habituales, incluido el nombre de usuario.
- john - - wordlist=password.lst archivo_shadow Este comando realiza la búsqueda empleando como diccionario el archivo.
- john - - incremental= all archivo_shadow Realiza un ataque de fuerza bruta probando con combinaciones de números, caracteres, mayúsculas y minúsculas.

Practica Modificación contraseñas en windows con ERD Commander

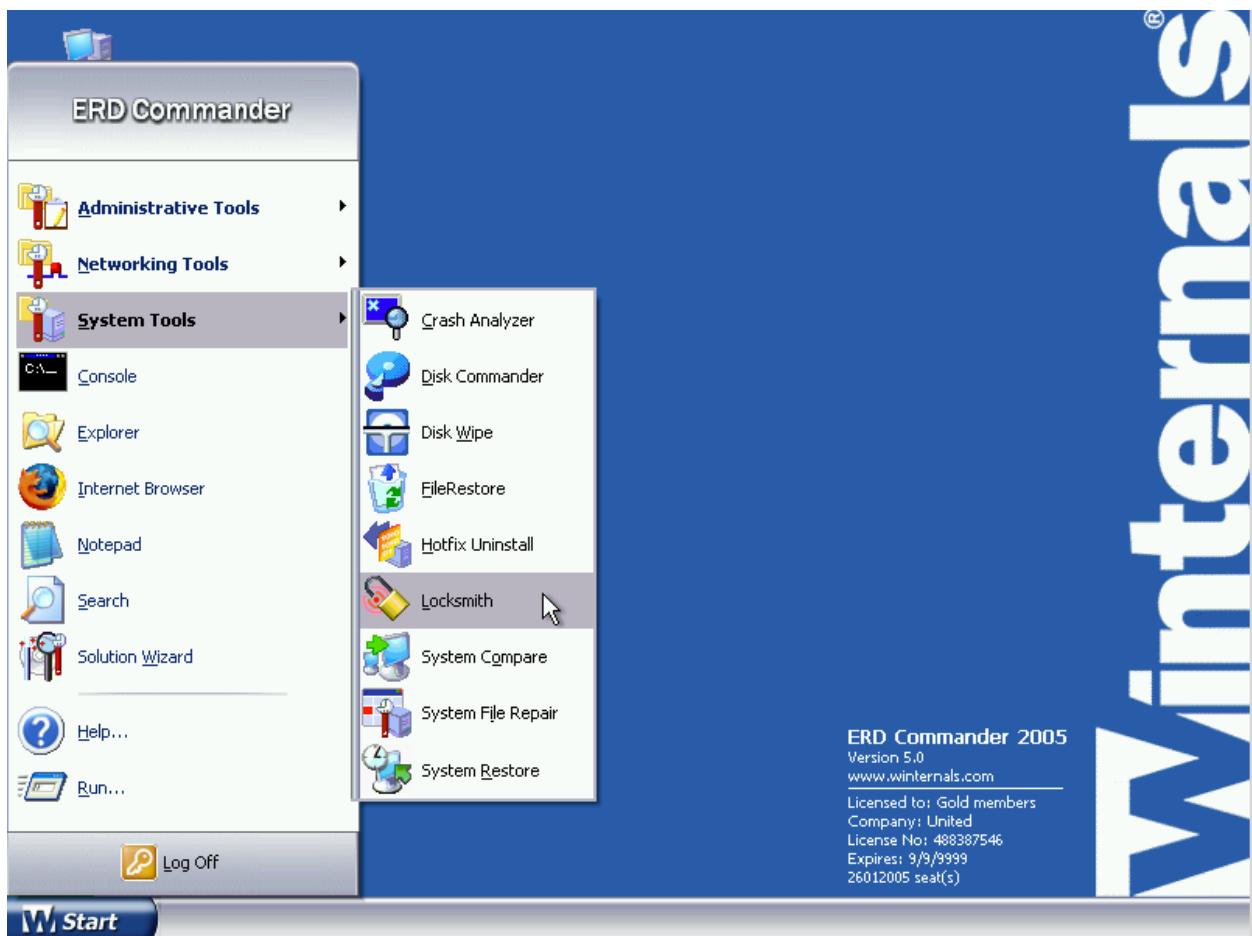
- En una virtual que tenga instalado un windows se arranca con una ISO que contiene **ERD commander** en live CD.
- Se selecciona las opción por defecto 'Run ERD Commander'.



- Y escogemos el tipo de teclado mas adecuado a nuestro sistema y la instalación de windows a modificar, en este caso solo hay una en C:\ y OK



- Una vez se abre el sistema arrancamos la utilidad locksmith que esta en start \System tools.



- Y cuando arranca la utilidad ya podemos seleccionar el usuario o usuarios de windows a los que les queremos cambiar la contraseña.



- Escogemos el usuario al que le queremos cambiar la contraseña, ponemos las contraseña que queramos y pinchamos en Next y Finish, ya podemos arrancar con el usuario en windows con la nueva contraseña que le hemos dado.



Capítulo 4 Software antimalware

Test de conocimientos (pag.104)

1 Malware que toma el control remoto del usuario administrador:

- a) Hoax.
- b) Joke.
- c) Rootkit. *malware que se ejecuta antes del sistema*
1 la máquina como quien
- d) Gusano.

2 Malware que envía mensajes electrónicos con noticias falsas o bulos:

- a) Hoax.
- b) Joke.
- c) Rootkit.
- d) Gusano.

3 Malware que permite capturar lo que se pulsa por teclado para capturar posibles usuarios y contraseñas:

- a) Clicker.
- b) Spyware.
- c) Exploit.
- d) Keylogger.

4 Diferencia entre el *scam* y el *spam*:

- a) Fraude bancario y correo basura.
- b) Fraude electrónico y correo basura.
- c) Correo basura y fraude *malware*.
- d) Troyano y gusano.

5 La finalidad actual de crear *malware* es:

- a) Lucrarse.
- b) Hacer el mal.
- c) Divertirse.
- d) Buscar errores en las aplicaciones.
- e) Crear parches de seguridad posteriores.

Distribuidor	Categoría	Elementos
Extension.Mismatch	File	c:\documents and settings\networkservice\configuración local\archivos temporales
Extension.Mismatch	File	c:\documents and settings\networkservice\configuración local\archivos temporales
Extension.Mismatch	File	c:\documents and settings\networkservice\configuración local\archivos temporales
Worm.Conficker	File	c:\Windows\system32\gqygon.dll
Worm.Conficker	File	e:\RECYCLER\w-5-3-42-2813952290-8240758988-879315005-3665\vgkvsq.vmx
Dont.Steal.Our.Software.A	File	e:\aflo 2010-2011\\$1\malwarebytes 1.46\patrick.exe
Worm.Palevo	Registry Value	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Wi
Worm.Palevo	Registry Value	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Wi
Hijack.Shell	Registry Data	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Wi
PUM.Hijack.StartMenu	Registry Data	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explor

Para la figura mostrada, contesta a las preguntas 6, 7 y 8.

6 Despues de realizar un análisis *antimalware*, ¿qué tipo de *malware* es la 4^a entrada?

- a) Gusano.
- b) Troyano.
- c) Virus.
- d) PWstealer.

7 ¿Qué ha modificado la 7^a entrada?

- a) Consola de comandos.
- b) Administrador de tareas.
- c) Registro.
- d) Archivo ejecutable.

8 ¿Qué inhabilita la 9^a entrada?

- a) Consola de comandos.
- b) Administrador de tareas.
- c) Registro.
- d) Archivo ejecutable.

9 ¿Bajo qué término se engloban acciones maliciosas no demasiado perjudiciales?

- a) Hoax.
- b) Greyware.
- c) Joke.
- d) Infostealer.

Herramienta antimalware MalwareBytes

- Se descarga MalwareBytes de la pagina oficial (mbam-setup-1.65.1.1000.exe, esta es la versión utilizada)
 - ✓ <http://es.malwarebytes.org/mwb-download>
- En la instalación se desmarca la casilla “Activar la version de prueba de Malwarebytes Anti-malware PRO” y tras finalizar la instalacion se ejecuta el programa.



- Se selecciona análisis completo, las unidades a escanear y se pincha en Analizar.



- Tras el análisis da el siguiente resultado (se ha probado en un XP dentro de una maquina virtual).



- Y tras pinchar en 'Mostrar los resultados' da la siguiente información:

Distribuidor	Categoría	Elementos	Otros
<input checked="" type="checkbox"/> PUM.Disabled.Secu...	Registry Data	HKLM\SOFTWARE\Microsoft\Security Center\AntiVirusDisableNotify	Bad: (1) Good: (0)
<input checked="" type="checkbox"/> PUM.Disabled.Secu...	Registry Data	HKLM\SOFTWARE\Microsoft\Security Center\FirewallDisableNotify	Bad: (1) Good: (0)
<input checked="" type="checkbox"/> PUM.Disabled.Secu...	Registry Data	HKLM\SOFTWARE\Microsoft\Security Center\UpdatesDisableNotify	Bad: (1) Good: (0)

- Da unos problemas de seguridad de avisos que estan desactivados, para activar estos avisos se va a **Panel de control – Centro de seguridad**, se selecciona '**Cambiar la forma en que el centro de seguridad me alerta**' y se activan las casillas, para voler a analizar y ver si ya no salen estar alertas detectadas.

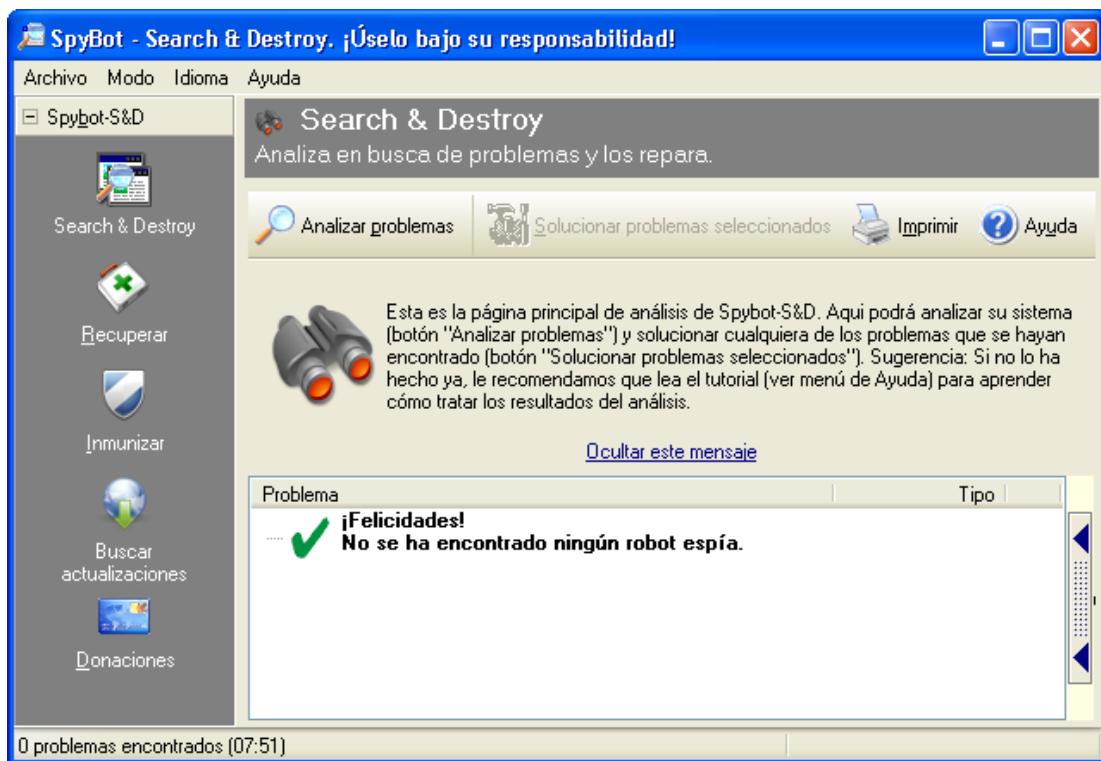
- Tras el análisis ya no salen estos avisos y no detecta elementos maliciosos:

Programa Spybotsd

- Tras instalar el programa (Spybotsd162.exe) se ejecuta y se escanea , el programa permite realizar una copia de seguridad del registro y actualizar el programa al iniciarse.



- Se pincha en 'Analizar problemas' para ver si encuentra amenazas en un XP de pruebas virtualizado.



- Hay un boton de 'Inmunizar' que una de las acciones que realiza es actualizar el fichero host que esta en \Windows\System32\drivers\etc y le añade las paginas maliciosas, la imagen solo muestra las primeras (justo después de la entrada 127.0.0.1 localhost), pero ha metido infinidad de ellas:

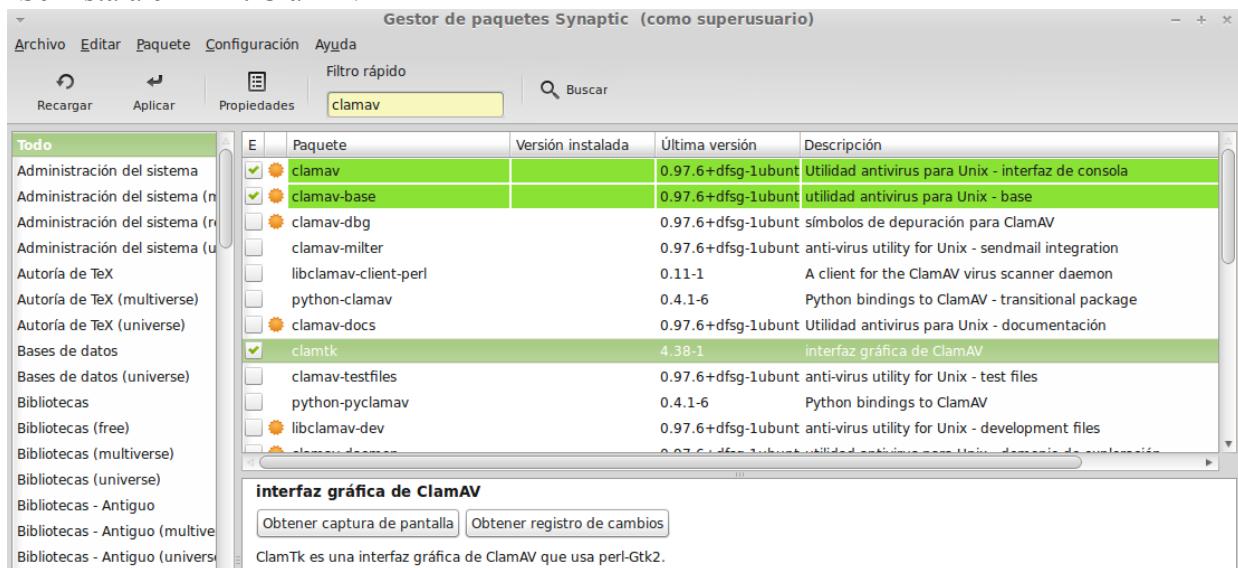
```
# debe ponerse en la primera columna, seguida del nombre de host correspondiente.
# La dirección IP y el nombre de host deben separarse con al menos un espacio.
#
#
# También pueden insertarse comentarios (como éste) en líneas individuales
# o a continuación del nombre de equipo indicándolos con el símbolo "#"
#
# Por ejemplo:
#
#      102.54.94.97      rhino.acme.com      # servidor origen
#      38.25.63.10      x.acme.com          # host cliente x

127.0.0.1      localhost
# Start of entries inserted by Spybot - Search & Destroy
127.0.0.1      www.007guard.com
127.0.0.1      007guard.com
127.0.0.1      0081.com
127.0.0.1      www.008k.com
127.0.0.1      008k.com
127.0.0.1      www.00hq.com
127.0.0.1      00hq.com
127.0.0.1      010402.com
127.0.0.1      www.032439.com
127.0.0.1      032439.com
127.0.0.1      www.Oscan.com
127.0.0.1      Oscan.com
127.0.0.1      www.1000gratisproben.com
127.0.0.1      1000gratisproben.com
127.0.0.1      1001namen.com
127.0.0.1      www.1001namen.com
127.0.0.1      100888290cs.com
127.0.0.1      www.100888290cs.com
127.0.0.1      www.100sexlinks.com
127.0.0.1      100sexlinks.com
127.0.0.1      www.10sek.com
127.0.0.1      10sek.com
127.0.0.1      www.1-2005-search.com
127.0.0.1      1-2005-search.com
127.0.0.1      www.123fporn.info
127.0.0.1      123fporn.info
127.0.0.1      123haustiereundmehr.com
127.0.0.1      www.123haustiereundmehr.com
127.0.0.1      123moviedownload.com
127.0.0.1      www.123moviedownload.com
127.0.0.1      www.123simsen.com
127.0.0.1      123simsen.com
127.0.0.1      www.123topsearch.com
127.0.0.1      123topsearch.com
127.0.0.1      125sms.co.uk
127.0.0.1      www.125sms.co.uk
127.0.0.1      125sms.com
```

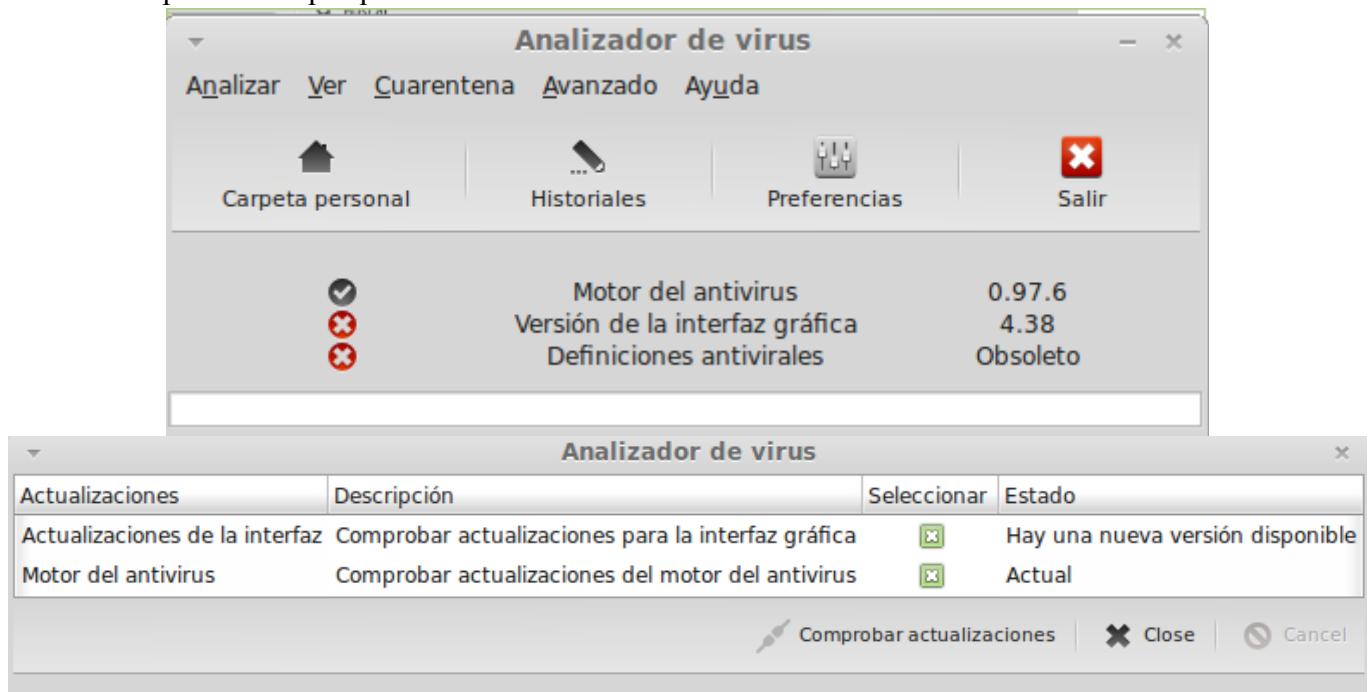
El programa lo que hace al meter estas entradas, es que al ponerlas en el navegador se redirigirá a si mismo y así NO entres en las páginas maliciosas.

Utilización de clamAv en Linux mint real para buscar virus en particiones Windows.

- Se instala en Mint ClamAv



- No se puede usar porque cuando arranca no funciona.



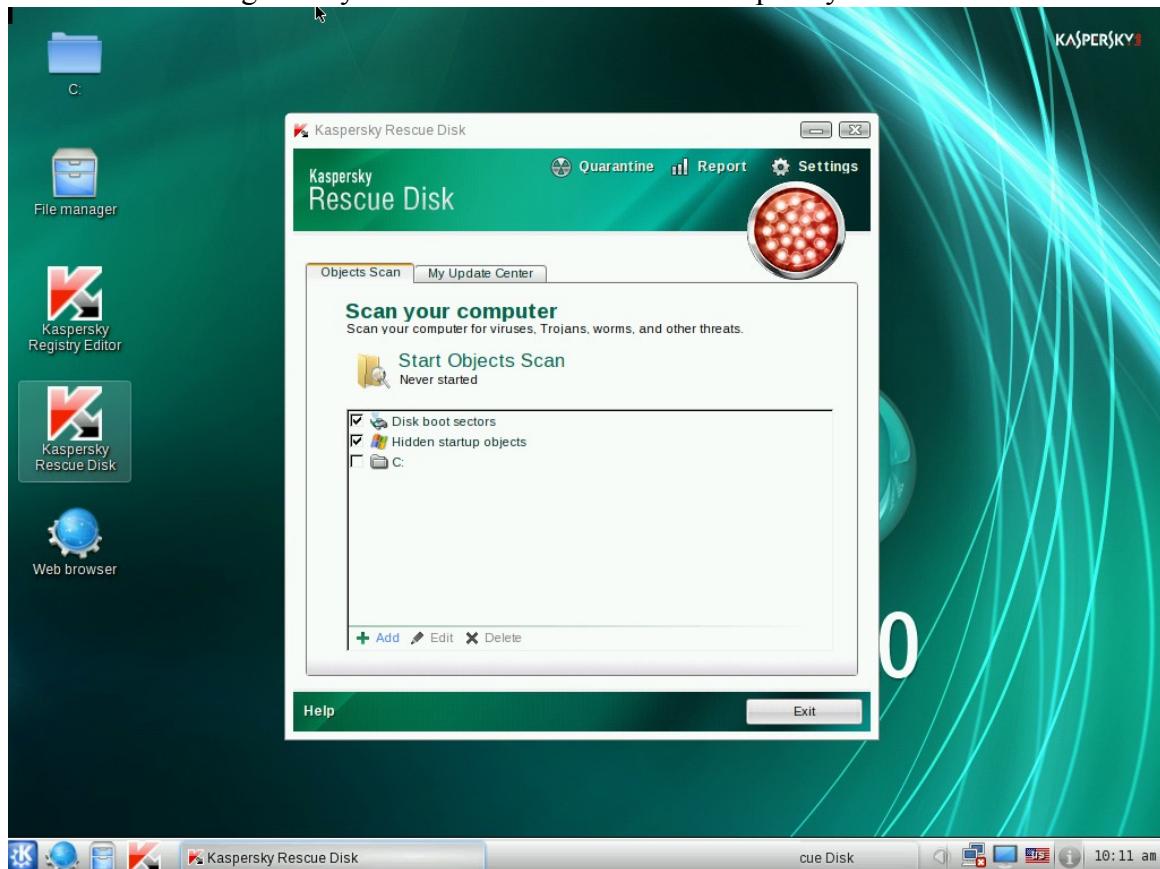
- Sale la pantalla de actualización pero no actualiza ni hace nada, esta practica no se puede hacer.

Análisis de la maquina virtual XP con un antivirus Live CD

- Se pone como unidad de CD la iso del antivirus Kaspersky (kav_rescue_10.iso) y se inicia la maquina virtual seleccionando arranque desde el CD.



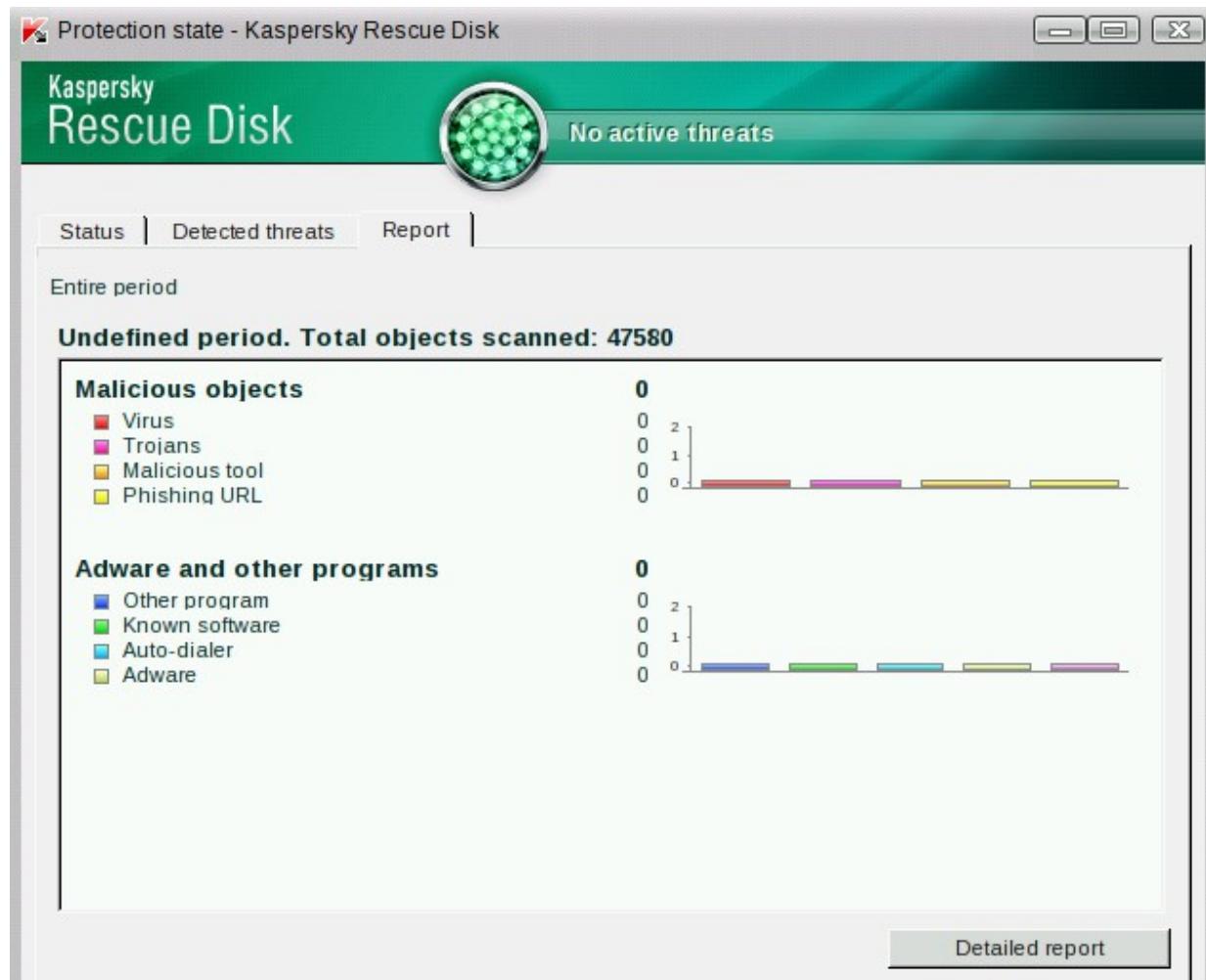
- Se selecciona modo grafico y tras arrancar se selecciona Kaspersky Rescue Disk.



- Se selecciona la unidad C que ah montado (donde esta windows) y se pincha en 'Start Objects scan', primero se actualiza y luego hace el escaneo (hay que configurar la red para que se pueda actualizar).



- No ha encontrado amenazas:



Preguntas tipo de los capítulos 3 y 4

1. ¿Medidas de seguridad al almacenar las contraseñas? y ¿porque?
No guardar la contraseña, solo el Hash y añadir la sal a las contraseñas antes de pasarlas por el hash.
Es porque si se produce un fallo de seguridad se evita el filtrado de la contraseña en claro y con la salt se dificulta que los hashes sean atacados, ademas habría que guardar la salt que se aplica a la contraseña en un lugar diferente a donde se guarda el hash.
2. ¿Que nuevo ataque a la contraseña ha surgido en los últimos años?
Ataque según análisis estadístico **por patrones** de contraseña típicos.
3. ¿Tiene sentido la longitud máxima en una contraseña? Explica porque si, porque no
En principio no, porque las contraseñas deben pasar por el hash y como el hash tiene longitud fija, no es necesario que la contraseña tenga límite de longitud.
4. Cita tres niveles de acceso a un sistema que puedan protegerse con contraseña
Acceso la Bios
Acceso al gestor de arranque
Acceso al sistema operativo
Acceso a aplicaciones y datos cifrados
5. ¿Porque no son recomendables las actualizaciones automáticas en sistemas críticos?
Porque las actualizaciones pueden romper o desestabilizar el sistema.
Porque generalmente alguna o muchas de las actualizaciones requieren el reinicio del sistema y esto afectaría al servicio.
6. ¿Que es un ataque de día cero o 'cero day'?
Es un problema de seguridad que se ha detectado cuando ya se está utilizando para infectar o atacar sistemas.
7. Cita 4 tipos de antivirus
Antivirus de escritorio.
Antivirus portable.
Antivirus online.
Live CD.
Análisis de ficheros online.
8. ¿Que son las tablas Rainbow? ¿para que se utilizan?
Son bases de datos o ficheros que contienen, de forma muy comprimida, las contraseñas a las que corresponden los hashes. Dependiendo de la tabla, cubre todas las posibles contraseñas hasta 5 caracteres, o 6 o 7.....
9. ¿Que es rogueware? ¿y hoax?
Rogueware: Falsas soluciones antivirus.
Hoax: Bulo que circula por internet.

10. Si hablamos de contraseñas ¿que es la sal?

Es una secuencia de bits aleatorias que se añaden a todas las contraseñas de un sistema.

11. Cita 6 recomendaciones de seguridad que ayuden a mantener el ordenador sin malware o a minimizar sus efectos negativos.

Mantenerse informado de novedades y alertas de seguridad.

Mantener actualizado el equipo.

Hacer copias de seguridad.

Utilizar software legal.

Utilizar contraseñas fuertes.

Crear usuarios con pocos privilegios para el uso cotidiano.

Utilizar herramientas de seguridad (antimalware).

Analizar el sistema de ficheros con varias herramientas.

Realizar periódicamente escaneo de puertos, test de velocidad y conexiones de red.

No fiarse de las herramientas antimalware, algunas no son lo que dicen (son maliciosas).

12. Define los términos exploit y payload

Exploit son programas que se aprovechan de los agujeros de seguridad.

Payload es como un malware que mete el exploit.

13. Cuales son los dos ataques clásicos para intentar romper una contraseña?

Por fuerza bruta.

Por ataque de diccionario.

14. Explica la directiva “forzar el historial de contraseñas” de Windows.

El objetivo es evitar la reutilización de contraseñas, permite guardar las X ultimas contraseñas que ha puesto el usuario.

15. Explica como se realiza un análisis antimalware manual.

Desconectar de la Red (internet).

Identificar procesos y driver maliciosos (con un analizador de procesos de sistema).

Finalizar (o suspender) los procesos maliciosos localizados.

Identificar y borrar los “autostarts maliciosos.

Borrar ficheros maliciosos.

Reiniciar el equipo y repetir.

16. ¿Quien encuentra normalmente mas problemas de seguridad en un ordenador, un programa antivirus o un programa malware?

El antimalware ya que comprende todo tipo de programas maliciosos como virus, troyanos, gusanos etc. y el antivirus por definición es mas específico para virus.

17. ¿Que es un hoax? ¿y un greyware?

Greyware: Es un programa molesto, pero que no daña el equipo.

Hoax: Bulo que circula por internet.

Test de conocimientos (Cap.5 pag. 129)

- 1** Indica qué sentencia es falsa con respecto al DNIe:
- a) Posee la misma utilidad en Internet que el DNI anterior.
 - b) Posee mucho más nivel de seguridad que el anterior.
 - c) Lo poseen actualmente muchas menos personas que el anterior.
 - d) Exige un hardware bastante económico para emplearlo.

- 2** Con el certificado digital y el DNIe todavía no puedo realizar trámites como:
- a) Acceder a la declaración de la renta.
 - b) Realizar devoluciones *online* de un producto.
 - c) Averiguar mis datos de la Seguridad Social.
 - d) Pedir una cita para el médico.

- 3** En un sistema criptográfico el aspecto más importante es:
- a) Longitud de la clave.
 - b) La asimetría.
 - c) La clave.
 - d) Tiempo de cifrado.

- 4** ¿Cuál de estos tipos de mecanismos de identificación no poseen validez alguna todavía?
- a) DNIe.
 - b) Firma digitalizada.
 - c) Firma digital.
 - d) Certificado digital.

- 5** La codificación RSA-3, es un método:
- a) Asimétrico.
 - b) Simétrico.
 - c) Hash.
 - d) Híbrido.
- 6** ¿Qué tipo de cifrado se emplea en este comando gpg -c?
- a) Asimétrico.
 - b) Simétrico.
 - c) Hash.
 - d) Firma digital.
 - e) Híbrido.

- 7** ¿Para qué se emplea este comando gpg -b?
- a) Cifrado Asimétrico.
 - b) Cifrado Simétrico.
 - c) Publicación de clave pública.
 - d) Firma digital.
 - e) Cifrado Híbrido.

- 8** ¿Para qué se emplea este comando gpg --send-keys?
- a) Cifrado Asimétrico.
 - b) Cifrado Simétrico.
 - c) Publicación de clave pública.
 - d) Firma digital.
 - e) Híbrido.

Programa Steghide

sudo apt-get install steghide

para sacar datos ocultos de una imagen con sudo steghide --extract -sf imagen.jpg

```
juan@HZ061512 ~ $ sudo steghide --extract -sf gaztelugatxe.jpg
```

Anotar salvoconducto:

anotó los datos extraídos e/"mensaje_oculto.txt".

```
juan@HZ061512 ~ $ cat mensaje_oculto.txt
```

N0 0LV1D35 357UD14R DUR0 P4R4 3L 3X4M3N D3L LUN35. H4Y MUCH0 3N JU3G0.

Sustituciones vía terminal

se crea un fichero con echo "texto a meter" > doc1.txt

lo cambio con cat doc1.txt | tr [aobesg] [408356]

```
juan@HZ061512 ~ $ cat mensaje_oculto.txt
```

N0 0LV1D35 357UD14R DUR0 P4R4 3L 3X4M3N D3L LUN35. H4Y MUCH0 3N JU3G0.

```
juan@HZ061512 ~ $ echo "esto es un mensaje de prueba de criptografia" > doc1.txt
```

```
juan@HZ061512 ~ $ cat doc1.txt | tr [aobesg] [408356]
```

35t0 35 un m3n54j3 d3 pru384 d3 cript06r4fi4

```
juan@HZ061512 ~ $ cat doc1.txt | tr [408356] [aobesg]
```

esto es un mensaje de prueba de criptografia

```
juan@HZ061512 ~ $ echo "esto es un mensaje de prueba de criptografia" > doc1.txt
```

```
juan@HZ061512 ~ $ cat doc1.txt | tr [aobesg] [408356]
```

35t0 35 un m3n54j3 d3 pru384 d3 cript06r4fi4

```
juan@HZ061512 ~ $ cat doc1.txt | tr [408356] [aobesg]
```

esto es un mensaje de prueba de criptografia

```
juan@HZ061512 ~ $ cat doc1.txt
```

esto es un mensaje de prueba de criptografia

```
juan@HZ061512 ~ $ cat doc1.txt | tr [aobesg] [408356] > doc2.txt
```

```
juan@HZ061512 ~ $ cat doc2.txt
```

35t0 35 un m3n54j3 d3 pru384 d3 cript06r4fi4

```
juan@HZ061512 ~ $ cat doc2.txt | tr [408356] [aobesg] > doc3.txt
```

```
juan@HZ061512 ~ $ cat doc3.txt
```

esto es un mensaje de prueba de criptografia

Cifrado simétrico con GPG (alternativa libre a PGP)

Se comprueba la versión de la herramienta de cifrado gpg en Linux mint 13 y los algoritmos (Cipher) soportados.

```
juan@HZ061512 ~ $ gpg --version
gpg (GnuPG) 1.4.11
Copyright (C) 2010 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later
<http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: ~/.gnupg
Supported algorithms:
Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
CAMELLIA128,
      CAMELLIA192, CAMELLIA256
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

Se crea un archivo de texto de prueba y se encrypta con la herramienta de encryptacion (la opción es -c y pide meter la contraseña con la que se encriptara).

```
juan@HZ061512 ~ $ nano archivo_prueba_cifrado_juan.txt
juan@HZ061512 ~ $ cat archivo_prueba_cifrado_juan.txt
Este es una archivo de prueba de juan
Es para probar el cifrado con GPG
Si lo consigues descifrar enhorabuena
juan@HZ061512 ~ $ gpg -c archivo_prueba_cifrado_juan.txt
juan@HZ061512 ~ $ ls -l archivo_prueba_cifrado_juan.*
-rw-r--r-- 1 juan juan 110 nov 27 09:37 archivo_prueba_cifrado_juan.txt
-rw-r--r-- 1 juan juan 149 nov 27 09:39 archivo_prueba_cifrado_juan.txt.gpg
```

Si hago un cat sobre el archivo cifrado sale un galimatias.

```
juan@HZ061512 ~ $ cat archivo_prueba_cifrado_juan.txt.gpg
#####/7?*?N?U?>?r?5????k?"??uT?/?V?-
#W?]?$?0+??^?G##?_??<2#?5?3??~??xRj?{#&?C?u
V?rE#X?<??#q$$HU??#?#?-?#? ?F_F?9ID??0??_?!"?
```

Si al cifrar añado -a al comando el cifrado aunque encriptado sale legible.

```
juan@HZ061512 ~ $ gpg -c -a archivo_prueba_cifrado_juan.txt
juan@HZ061512 ~ $ ls -l archivo_prueba_cifrado_juan.*
-rw-r--r-- 1 juan juan 110 nov 27 09:37 archivo_prueba_cifrado_juan.txt
-rw-r--r-- 1 juan juan 300 nov 27 09:47 archivo_prueba_cifrado_juan.txt.asc
-rw-r--r-- 1 juan juan 149 nov 27 09:39 archivo_prueba_cifrado_juan.txt.gpg
juan@HZ061512 ~ $ cat archivo_prueba_cifrado_juan.txt.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAwMCTJDc4deKX1xgyYTy5dTJwnwCsRq0IBRCCeDPvlZryRwsjN3Mk6gNcsMx
b3VvvCagB8MWjknMPY8VmXUx33EhmvtS6j6gfz5w200C/SfXOqamAQA1LM1XXa9o
fCW174U8NtMwTzLej446dYIOsBT7syIfWjbu6SU02Zk2OmmzYSs74DFpNaa/bHk9
o83Q8co=
=fACy
-----END PGP MESSAGE-----
```

Se hace la prueba de desencriptar el mensaje con la opción -d (pide la contraseña utilizada para encriptar que es: 12345678Aa).

```
juan@HZ061512 ~ $ gpg -d archivo_prueba_cifrado_juan.txt.gpg
gpg: CAST5 encrypted data
gpg: encrypted with 1 passphrase
Este es una archivo de prueba de juan
Es para probar el cifrado con GPG
Si lo consigues descifrar enhorabuena
gpg: WARNING: message was not integrity protected
```

gpg: WARNING: message was not integrity protected

Este mensaje quiere decir que ha desencriptado el mensaje pero no puede asegurar que el mensaje no haya sido modificado.

Se prueba a encriptar con otro algoritmo de los soportados (ver pantallazo de versión).

```
juan@HZ061512 ~ $ gpg -c -a --cipher-algo AES192 archivo_prueba_cifrado_juan.txt
File `archivo_prueba_cifrado_juan.txt.asc' exists. Overwrite? (y/N) N
Enter new filename: archivo_prueba_cifrado_juan.txt.AES192
juan@HZ061512 ~ $ ls -l archivo_prueba_cifrado_juan.*
-rw-r--r-- 1 juan juan 110 nov 27 09:37 archivo_prueba_cifrado_juan.txt
-rw-r--r-- 1 juan juan 340 nov 27 10:21 archivo_prueba_cifrado_juan.txt.AES192
-rw-r--r-- 1 juan juan 300 nov 27 09:47 archivo_prueba_cifrado_juan.txt.asc
-rw-r--r-- 1 juan juan 149 nov 27 09:39 archivo_prueba_cifrado_juan.txt.gpg
juan@HZ061512 ~ $ cat archivo_prueba_cifrado_juan.txt.AES192
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0ECAMCcmX7MEySPz5g0qMBIDyGnDh5pZYkJ2u/VkoPh5rSmOYIuPW/xNzq45ES
DzPm4nQAm5bBNQHPM8yxiOf4ggendcASKgqRwQ3RaVZadRF9YCW5qPNO6ZxuJkm
a
o1RUVKXxXK0G+wB4p1gCkFmWjpFRwjh+73/A7hM/wGXRaSIItsbLsaCmquGRPTik
MnfQvIzNHild8l7P/EwQv50SxS8D9PGnWkTRVz6K92bUoaXO
=ic64
-----END PGP MESSAGE-----
```

Opciones de uso de gpg:

- **gpg --version** muestra la versión y algoritmos soportados
- **gpg -c 'archivo'** encripta el archivo especificado
- **gpg -c -a 'archivo'** encripta el archivo especificado en formato legible
- **gpg -d 'archivo'** des-encripta el archivo especificado
- **gpg -c -a --cipher-algo 'algoritmo' 'archivo'** encripta el archivo especificado en formato legible, con el algoritmo especificado y soportado.

Cifrado simétrico con TrueCrypt (<http://www.truecrypt.org/>)

Permite encriptar un disco duro o partición.

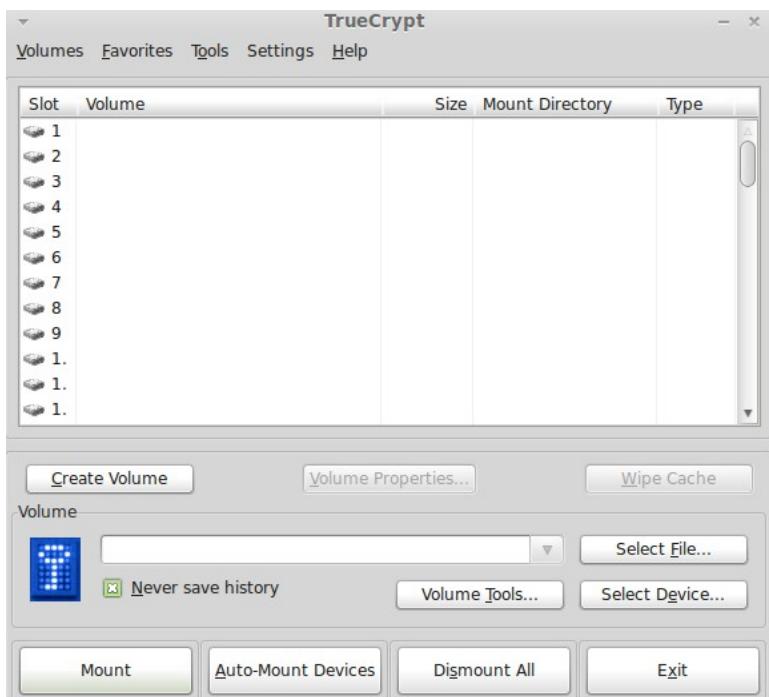
Tiene la posibilidad de crear un contenedor virtual encriptado dentro de otro y ademas oculto.

Se comprueba la versión gráfica de la herramienta de cifrado TrueCrypt en Linux mint 13.

- Una vez descargado el paquete de la pagina web y extraído su contenido, se ejecuta desde una terminal invocando al ejecutable con (hay que estar en la carpeta que contiene el ejecutable):
 - ✓ `sh truecrypt-7.1a-setup-x86`
 - ✓ Elegimos la opción: 1) Install truecrypt_7.1a_i386.tar.gz para instalarlo
 - ✓ Tras aceptar la licencia y meter contraseña root se instala.

```
Uninstalling TrueCrypt:  
-----  
To uninstall TrueCrypt, please run 'truecrypt-uninstall.sh'.  
  
Installing package...  
[sudo] password for juan:  
usr/bin/truecrypt  
usr/bin/truecrypt-uninstall.sh  
usr/share/applications/truecrypt.desktop  
usr/share/pixmaps/truecrypt.xpm  
usr/share/truecrypt/doc/License.txt  
usr/share/truecrypt/doc/TrueCrypt User Guide.pdf  
  
Press Enter to exit...
```

- Para abrir la aplicación se va a Aplicaciones => Accesorios => TrueCrypt
 - ✓ Una vez se abre se pincha en 'Create volume'



- ✓ Se selecciona la opción por defecto 'Create an encrypted file container' , con esta opcion se crea un contenedor virtual a modo de fichero.
- ✓ Con la otra opción 'Create a Volume within a partition/drive' encriptariamos un disco o partición enteros.



- ✓ Se selecciona 'Standar TrueCrypt volume', con lo que crea un contenedor virtual encriptado normal.
 - ✗ Si seleccionamos 'Hidden TrueCrypt volume' crea primero un contenedor virtual encriptado y dentro de el otro contenedor virtual encriptado que quedaría oculto, en este caso daremos contraseñas diferentes a ambos contenedores y a la hora de abrirlo según que contraseña le demos al programa abrirá uno u otro contenedor.
- Esta opción puede ser útil si por ejemplo queremos que nadie acceda al volumen oculto, por ejemplo si tenemos que dar la contraseña del volumen encriptado a 'alguien' (le daríamos la contraseña del primer volumen y ya no verían el otro volumen que queda oculto).



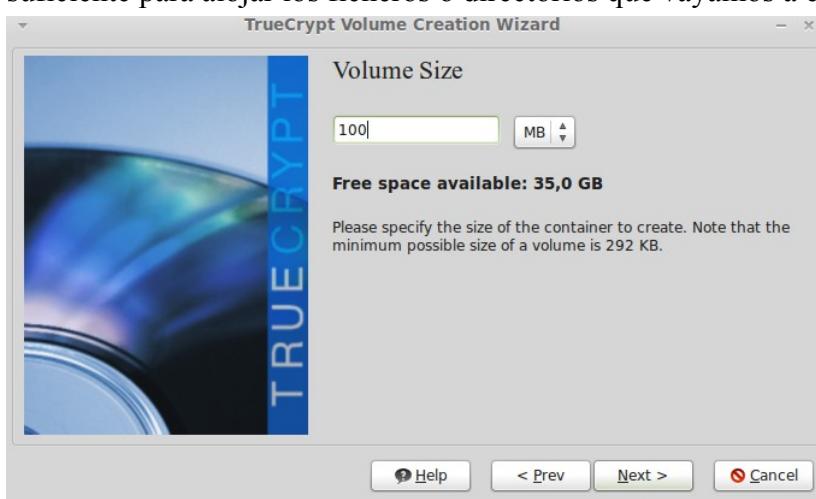
- ✓ Se selecciona el nombre y la localización donde se guardara el disco virtual encriptado.



- ✓ Se selecciona el tipo de algoritmo de encriptacion, se pueden escoger varios.



- ✓ Se selecciona el tamaño del volumen (este tamaño lo elegiremos de tal manera que tenga espacio suficiente para alojar los ficheros o directorios que vayamos a encriptar).



- ✓ Establecemos una contraseña (deberá ser segura y larga).



- ✓ Si considera que la contraseña es corta y no es segura te avisa.



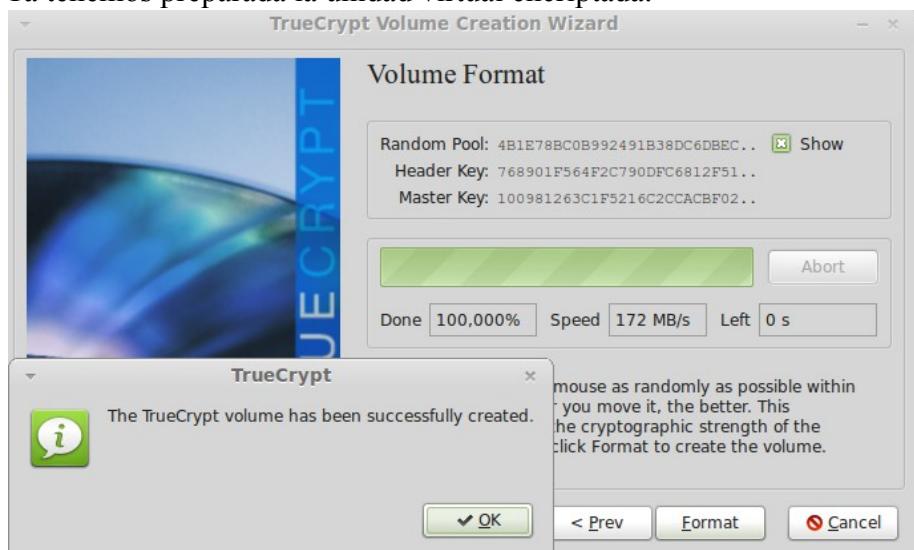
- ✓ Se selecciona el formato del volumen (se puede elegir entre FAT y los formatos EXT de Linux).



- ✓ En la siguiente pantalla damos a 'Format'.

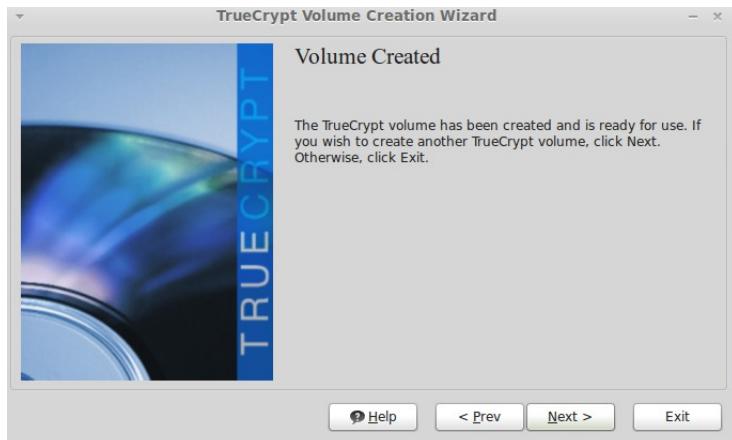


- ✓ Ya tenemos preparada la unidad virtual encriptada.

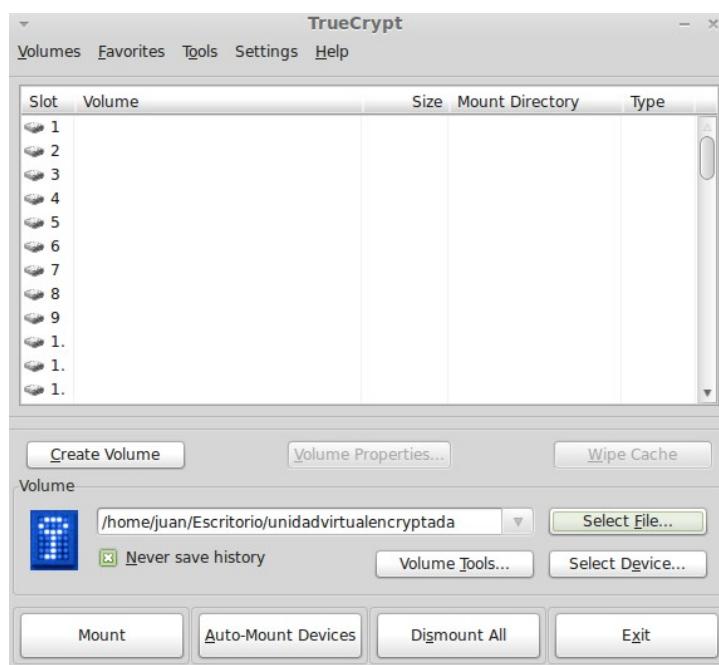


- ✓ Tras pinchar en 'OK' confirma que ha creado el volumen.

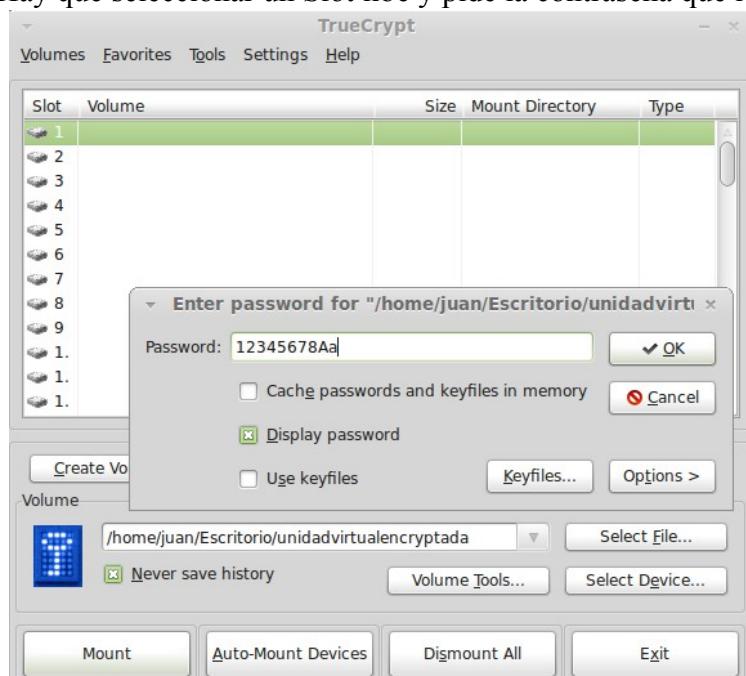
- ✓ Con 'Exit' salimos del asistente, si queremos crear otra unidad virtual pincharíamos en 'Next'.



- ✓ Volvemos al programa y hay que montar la unidad creada pinchando en 'Select file' y 'Mount'.

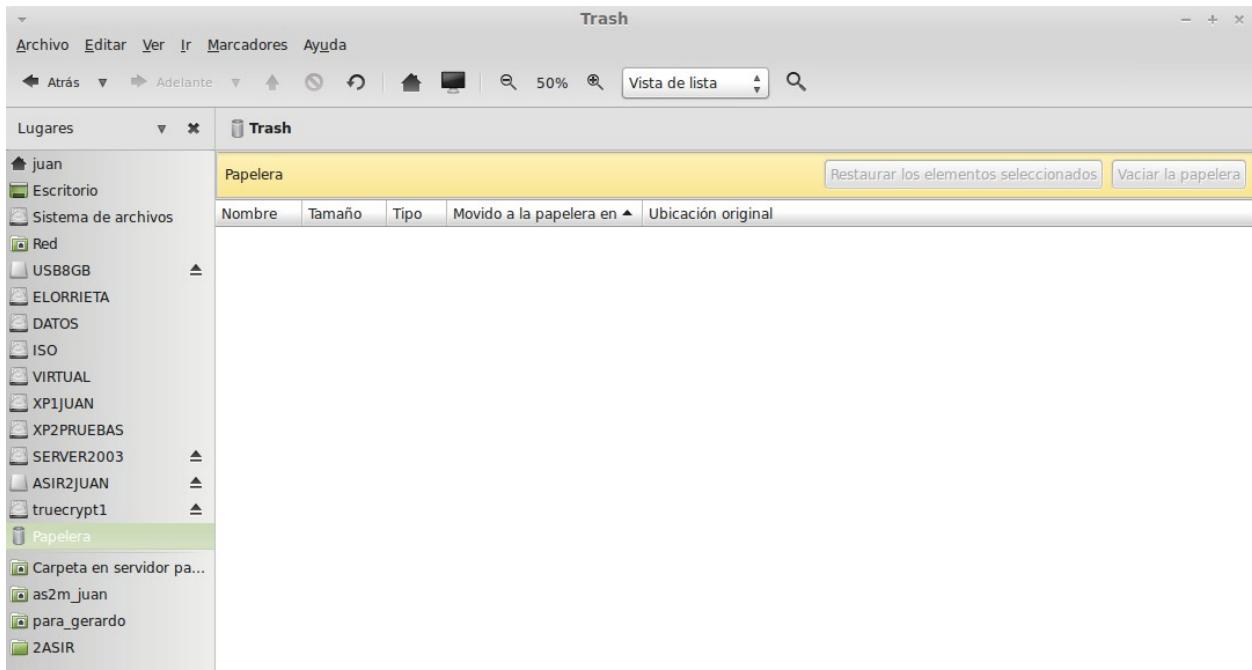


- ✓ Hay que seleccionar un Slot libre y pide la contraseña que le asignamos al crearlo.



Nota: Pide también la contraseña de administrador para terminar de montar la unidad virtual.

- ✓ Una vez hecho ya aparece en el Explorador de archivos como una unidad mas y podemos meter los archivos y carpetas que queramos.



- ✓ Un sistema interesante para aplicar por ejemplo a un pendrive y llevar el contenido protegido en caso de perdida, eso si deberemos tener instalado el programa en el ordenador donde pinchemos el pendrive para poder acceder a la información.
- ✓ En la pagina de descargas (<http://www.truecrypt.org/downloads>) podemos descargar el programa para las siguientes plataformas:
 - ✗ Windows 7/Vista/XP/2000
 - ✗ Mac OS X
 - ✗ Linux

Practica 5.5 (pagina 118) Cifrado asimétrico

- Generamos un par de claves con gpg
✓ `juan@HZ061512 ~ $ gpg --gen-key` y se siguen los pasos:

```
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.
```

Please select what kind of key you want:

- (1) RSA and RSA (default)
- (2) DSA and Elgamal
- (3) DSA (sign only)
- (4) RSA (sign only)

Your selection? 1

RSA keys may be between 1024 and 4096 bits long.

What keysize do you want? (2048) 4096

Requested keysize is 4096 bits

Please specify how long the key should be valid.

- 0 = key does not expire
- <n> = key expires in n days
- <n>w = key expires in n weeks
- <n>m = key expires in n months
- <n>y = key expires in n years

Key is valid for? (0) **12345678Aa**)

Key does not expire at all

Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID from the Real Name, Comment and Email Address in this form:

"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: juan

Name must be at least 5 characters long

Real name: alberto

Email address: alberto@miccorreo.com

Comment: prueba encriptado asimetrico

You selected this USER-ID:

"alberto (prueba encriptado asimetrico) <alberto@miccorreo.com>"

Change (N)ame, (C)omment, (E)mail or (O)key/(Q)uit? O

You need a Passphrase to protect your secret key.

Aqui pide que metamos una contraseña (le pongo 12345678Aa)

We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy.

Not enough random bytes available. Please do some other work to give the OS a chance to collect more entropy! (Need 238 more bytes)

- ✓ Ahora se introducen con el teclado todos los caracteres necesarios al azar (incluso moviendo el ratón o reproduciendo un fichero mp3) hasta alcanzar los 238bytes que pide.
- ✓ Una vez ha terminado de recolectar caracteres genera la clave, para verla con:
 - ✗ `juan@HZ061512 ~ $ gpg --list-keys`

```
/home/juan/.gnupg/pubring.gpg
-----
pub 4096R/60993E7F 2012-12-04
uid          alberto (prueba encriptado asimetrico) <alberto@miccorreo.com>
sub 4096R/BEA9FD63 2012-12-04
```

- Ahora hay que enviar la clave publica generada a las personas con las que queremos comunicarnos para lo que generamos un archivo .asc y coger la cable publica del otro interlocutor de la siguiente manera:
 - ✓ `juan@HZ061512 ~ $ gpg --armor --output Clave_publica_juan.asc --export 60993E7F`
 - ✗ Al final ponemos la **ClaveID** que puede ser '60993E7F' o 'alberto@miccorreo.com'
 - ✗ la opción --armor es para que se vea en caracteres ASCII.
 - ✓ Se envía la cable publica generada al otro interlocutor (fichero `Clave_publica_juan.asc`)
 - ✗ Se puede enviar por correo o en soporte tipo pendrive USB
 - ✗ Se puede subir a un servidor de claves publicas como el servidor pgp de iris:
 - `gpg --send-keys --keyserver pgp.rediris.es ClaveID`.
 - ✗ Para hacer una búsqueda de claves publicas seria:
 - `gpg --keyserver NombreDelServidor --search-keys ClaveID`.
 - ✗ Para bajar la clave:
 - `gpg --keyserver NombreDelServidor --recv-keys ClaveID`
 - ✓ Se coge la clave del interlocutor, en este caso `Clave_publica_Gerardo.asc` y se importa.
 - ✗ `juan@HZ061512 ~ $ gpg --import Clave_publica_Gerardo.asc`

```
gpg: key 2516C5B8: public key "Gerardo (La dirección no existe)
<gerardo@nowinchess.com>" imported
gpg: Total number processed: 1
gpg:           imported: 1 (RSA: 1)
```

- Vemos el listado de claves que tenemos y que ahora incorpora la clave de Gerardo:
 - ✓ `juan@HZ061512 ~ $ gpg --list-keys`

```
/home/juan/.gnupg/pubring.gpg
-----
pub 4096R/60993E7F 2012-12-04
uid          alberto (prueba encriptado asimetrico) <alberto@miccorreo.com>
sub 4096R/BEA9FD63 2012-12-04

pub 2048R/2516C5B8 2012-12-04
uid          Gerardo (La dirección no existe) <gerardo@nowinchess.com>
sub 2048R/E1B76F46 2012-12-04
```

A medida que importemos claves publicas de otros interlocutores, irán añadiéndose al fichero.

- Para tener una copia aparte de nuestra clave privada se hace con el siguiente comando:
 - ✓ **gpg --armor --output ficheroclave --export-secret-key ClaveID**
- Ahora enviamos un fichero a Gerardo encriptandolo de la siguiente manera:
 - ✓ **juan@HZ061512 ~ \$ gpg --armor --recipient gerardo@nowinchess.com --encrypt pruebajuan.pdf**

```
gpg: E1B76F46: There is no assurance this key belongs to the named user
pub 2048R/E1B76F46 2012-12-04 Gerardo (La dirección no existe)
<gerardo@nowinchess.com>
Primary key fingerprint: 0FFD 42BB C1A7 45B2 5A97 B7B2 9251 2693 2516 C5B8
Subkey fingerprint: 28DC 3C10 FC51 B5CC 78A2 6529 B433 0807 E1B7 6F46

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

Nos indica que no puede autentificar al interlocutor y que seamos nosotros los que asumamos que es quien dice ser, ponemos 'y'. y crea el fichero encriptado:

- ✗ **pruebajuan.pdf.asc**
- ✗ Este fichero se lo enviamos a Gerardo y el puede desencriptarlo haciendo uso de su clave.
- ✓ Para desencriptar el fichero en este caso el que envía Gerardo se hace:
 - ✗ **juan@HZ061512 ~ \$ gpg -d Archivo_secreto_Gerardo.txt.asc > Archivo_secreto_Gerardo.txt**

```
gpg: encrypted with RSA key, ID E302D5E6
gpg: decryption failed: secret key not available
```

En este caso da error, es porque Gerardo ha encriptado el fichero en vez de con mi clave publica con la clave publica de otro alumno y lógicamente solo el podría desencriptarlo.

- ✗ **juan@HZ061512 ~ \$ gpg -d Prueba_solo_para_Juan.txt.gpg > Prueba_solo_para_Juan.txt**

```
ou need a passphrase to unlock the secret key for
user: "alberto (prueba encriptado asimetrico) <alberto@miccorreo.com>"'
4096-bit RSA key, ID BEA9FD63, created 2012-12-04 (main key ID
60993E7F)
```

```
gpg: encrypted with 4096-bit RSA key, ID BEA9FD63, created 2012-12-04
"alberto (prueba encriptado asimetrico) <alberto@miccorreo.com>"
```

Ahora si es un fichero encriptado con mi clave publica, pide una contraseña, en este caso la que he metido mas arriba al generar las claves, que era **12345678Aa**

- ✗ Ahora puedo ver el fichero ya desencriptado y el mensaje que contiene, en este caso es un txt con el siguiente mensaje:

Hola, Juan,

take it easy!

- Ahora ya podemos comunicarnos de forma segura.
- Los pasos resumidos del proceso son:
 - ✓ Juan genera las claves y envía clave publica a Gerardo
 - ✓ Gerardo importa la clave publica de Juan
 - ✓ Gerardo cifra un fichero con la clave publica de Juan
 - ✓ Gerardo envía el fichero encriptado a Juan
 - ✓ Juan desencripta el fichero encriptado con su clave privada (la suya propia, la de Juan)
 - ✓ Nadie mas puede descifrar ese fichero, porque nadie mas debe conocer la clave privada de juan.
 - ✓ Gerardo genera las claves y envía clave publica a Juan
 - ✓ Juan importa la clave publica de Gerardo
 - ✓ Juan cifra un fichero con la clave publica de Gerardo
 - ✓ Juan envía el fichero encriptado a Gerardo
 - ✓ Gerardo desencripta el fichero encriptado con su clave privada (la suya propia, la de Gerardo)

Practica 5.6 (pagina 122) Firma digital de documentos

- Creo un documento, por ejemplo un archivo txt:
 - ✓ `juan@HZ061512 ~ $ echo firma digital juan > archivo_a_firmar_juan.txt`
- Firmo el documento que he creado:
 - ✓ `juan@HZ061512 ~ $ gpg --armor --sign archivo_a_firmar_juan.txt`
 - ✗ El fichero contiene una frase: 'firma digital juan' y una vez firmado (pide la contraseña que se uso al hacer las claves privada y publica), crea un documento llamado `archivo_a_firmar_juan.txt.asc` que contiene:

```
juan@HZ061512 ~ $ cat archivo_a_firmar_juan.txt.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

owEBYgKd/ZANAwACAVU7QORgmT5/AawyYhlhcmNoaXZvX2FfZmlybWFyX2p1YW4u
dHh0UMbdR2Zpcm1hIGRpZ2l0YWwganVhbqqJAhwEAAECAAYFAIDG3UcACgkQVTtA
5GCZPn+UEhAAwmXwPOce9ZOKZ+sIFhLVpjsmXJKh1K/1zi8ohSL6qZlQlZscoIic
V+cHi5NU739mxZPJsoy4nUZhFLm10sb1XTYklE9ds/4L6h/lh8LK/BEKgXZO2dZA
FdxEWBCkFHfaM4rRuktPPLRvvVhpJpRkYgs2xQZgeo4vEdTqT2Xv6iun8rxycGi9
SWEpVQkSWtJlmQK6k+WV0tmAGO4hxvzwiGvgddUj1qx1aAhiETqkd1W8hoNROwi6
UkZ1W9ITzcRBLi8V6daagOjfi75riL6a0DPBsl66S/pCo8taIJcBxwzNvjK+voXa
hC6SXWVkkkr3UO+oZFvrrbr47f4zxO9noVRscDX5WYVGbElP6Uz485f3NcqrZFFJW
5CFvt0H3+sNzeTF49DjZNE8mwDp7tiYxVXuCOUYBVMHCLRSiHHjsDNSNRpFqk4ui
5y8dxnxc/y3wGS8PLAQldl8hoge8/3+h8X/TnAbsnzf32nOvMTssyGEEJmKaaBBN
B1k8hEvIAs8BTb67wWp99djoq0aG7PQ6ccyVp/wmqKlprgP1HOAPJdIKtM6bfvLF
eHMruoqqGPLI16RJaBPbmwpf4Ws6WxCwd2DFHfheh4EwovfhWtMYVSJkrTxam/xr
7MsA0Q/q383vZhZQYhD+gXrFT+cshqutbtRHtypzvUiu193cY9uiWZ0=
=vJYA
-----END PGP MESSAGE-----
```

- ✗ En este caso el fichero esta cifrado tanto la firma como el contenido todo dentro del mismo fichero.
- ✗ Y si desencripto el fichero (que es lo que haria el receptor del mensaje, que tiene que tener mi clave publica) el resultado es:

```
juan@HZ061512 ~ $ gpg --decrypt archivo_a_firmar_juan.txt.asc
firma digital juan
gpg: Signature made mar 11 dic 2012 08:14:15 CET using RSA key ID 60993E7F
gpg: Good signature from "alberto (prueba encriptado asimetrico) <alberto@micorreo.com>"
```

- ✗ Si lo desencripta el destinatario usando mi clave publica le da un aviso de certificacion, esto se resuelve con los certificados:

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
```

- ✓ Firmo el documento pero solo cifro la firma
- ✗ `juan@HZ061512 ~ $ gpg --clearsign archivo_a_firmar_juan.txt`
- ✗ El fichero contiene una frase: 'firma digital juan' y una vez firmado crea un documento llamado archivo_a_firmar_juan.txt.asc que contiene:

```
juan@HZ061512 ~ $ cat archivo_a_firmar_juan.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

firma digital juan
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJQxuKzAAoJEFU7QORgmT5/L14QAMD9rDKQeERVgLn+pJmeuL65
zY7D3tH8Q/8CdV1drUQqBzhPl917I89XmQste1ajPPp/bB52XtEl2qhz2ObZEZMh
+/6S2ClVqQmcHOF6B8OMtl0pCuN7m63L/Gy3Lv71FZKX2yn2ID8nv4Y3aR6EqeDe
jRzA+FlN3LvFV85nih8Nu3CkcbOKNFoHuP8YTfjgAfYNAy/IhsySmRGzTwqvgwhB
CRpO7g9WdoBYHjydBmDU2MmtmHfdrK8mtIUDOG3I3/FBOr+OsD2KBAIHctHzwIey
G8V98IvHPc3hPYvgsrUUc/BGidzzdsFrmsq6/R7sRbLW1ExXmXhllt1KNKqBEzBH
fS3nCOJEvPnx7PL+aR4GApYDaRuCV7CJOxf9bUvS6aiNd7hgeCz3w1bBApkQwJL
QaYQhoyWsHeDd9x02kTh3ODCmvdhxPiTD/K2P1t+WhyXFvo8iQ4napSFl9pQAiya
EQA8P8TqZS8D/GgvsET8APtXhFQL/WO5yI0LZS72XLz5+ctqY975gxwJHN7qNnCv
9UvW9fC3Wbc9FVxzF46vXgUdkfRuLT+V96+cChx0AfXwSeNDsP5fLdTL7gSFrR5G
7nTvvGnMVGUwkivGZ/XIDZowN1ZOzJnJLd85Xp9t63LcxpUQeQBIWEcotDeUhkTP
P4tX2Zjuj/bcusu658XA
=SHbi
-----END PGP SIGNATURE-----
```

- ✗ En este caso el fichero esta cifrado solo la firma, el contenido del fichero, esto es la frase esta sin cifrar como se ve al hacer cat. Y si lo descifro me da:

```
juan@HZ061512 ~ $ gpg --decrypt archivo_a_firmar_juan.txt.asc
firma digital juan

gpg: Signature made mar 11 dic 2012 08:14:15 CET using RSA key ID 60993E7F
gpg: Good signature from "alberto (prueba encriptado asimetrico) <alberto@micorreo.com>"
```

- ✓ Creo un fichero aparte con la firma.
- ✗ `juan@HZ061512 ~ $ gpg --armor --detach-sign archivo_a_firmar_juan.txt`
- ✗ El fichero contiene una frase: 'firma digital juan' y una vez firmado crea un documento llamado archivo_a_firmar_juan.txt.asc que contiene la firma, para no confundirnos se le puede cambiar el nombre:
 - `juan@HZ061512 ~ $ mv archivo_a_firmar_juan.txt.asc firma.asc`

- ✗ Entonces lo que se envia es el archivo de texto, el archivo con la firma y la clave publica si no la tiene y para comprobar la autenticidad del documento se hace con:
- ✗ **juan@HZ061512 ~ \$ gpg --verify firma.asc archivo_a_firmar_juan.txt**
- ✗ En este caso solo te informa de la autenticidad de la firma, ya que el texto lo tienes ya en claro en su propio fichero.

```
juan@HZ061512 ~ $ gpg --verify firma.asc archivo_a_firmar_juan.txt
```

```
gpg: Signature made mar 11 dic 2012 08:45:28 CET using RSA key ID 60993E7F
```

```
gpg: Good signature from "alberto (prueba encriptado asimetrico) <alberto@micorreo.com>"
```

- ✗ Los pasos que tiene que hacer el emisor del emnsaje son:
 - Crear la firma del fichero con: **gpg --armor --detach-sign 'fichero'**
 - Enviar Fichero, Firma (fichero con extension .asc creado con gpg) y Clave publica.
- ✗ Los pasos que tiene que hacer el receptor son:
 - Importar la firma.
 - Importar el fichero y la firma del fichero
 - Comprobar la autenticidad con: **gpg --verify fichero firma**
 -

✓

Practica 5.7 (pagina 123) Certificados

- Se comprueba con un Navegador Web (Firefox) una pagina segura como puede ser la BBK
- ✓ En el navegador ya aparece como segura (candado en verde).



- ✓ Si pinchamos en el candado nos da informacion sobre la autenticidad de la pagina y la entidad que ha emitido el certificado.

Visor de certificados:"login.live.com"

General Detalles

Este certificado ha sido verificado para los siguientes usos:

Certificado del servidor SSL

Emitido para

Nombre común (CN)	login.live.com
Organización (O)	Microsoft Corporation
Unidad organizativa (OU)	Passport
Número de serie	6C:73:81:81:51:6E:7E:6C:4F:B5:7C:01:AA:BE:87:88

Emitido por

Nombre común (CN)	VeriSign Class 3 Extended Validation SSL SGC CA
Organización (O)	VeriSign, Inc.
Unidad organizativa (OU)	VeriSign Trust Network

Validez

Emitido el	18/09/12
Caduca el	20/09/14

Huellas digitales

Huella digital SHA1	02:C1:D2:C1:9C:11:F2:87:B4:A3:46:A4:20:D0:B2:42:AB:5F:33:68
Huella digital MD5	B4:8B:AC:2A:1D:4C:C0:7B:1E:22:B2:E7:E1:78:EF:57

- ✓ En Detalles tenemos informacion mas detallada del certificado.
- ✓ Si la pagina no es segura por no estar certificada, sale un mensaje de aviso.

https://bbk.es

Ás visitados v Linux Mint Community Forums Blog News v

Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **bbk.es**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intenta conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

▼ Detalles técnicos

bbk.es usa un certificado de seguridad no válido.

El certificado sólo es válido para www.bbk.es.
(Código de error: ssl_error_bad_cert_domain)

▶ Entiendo los riesgos

✓

Practica Correo seguro

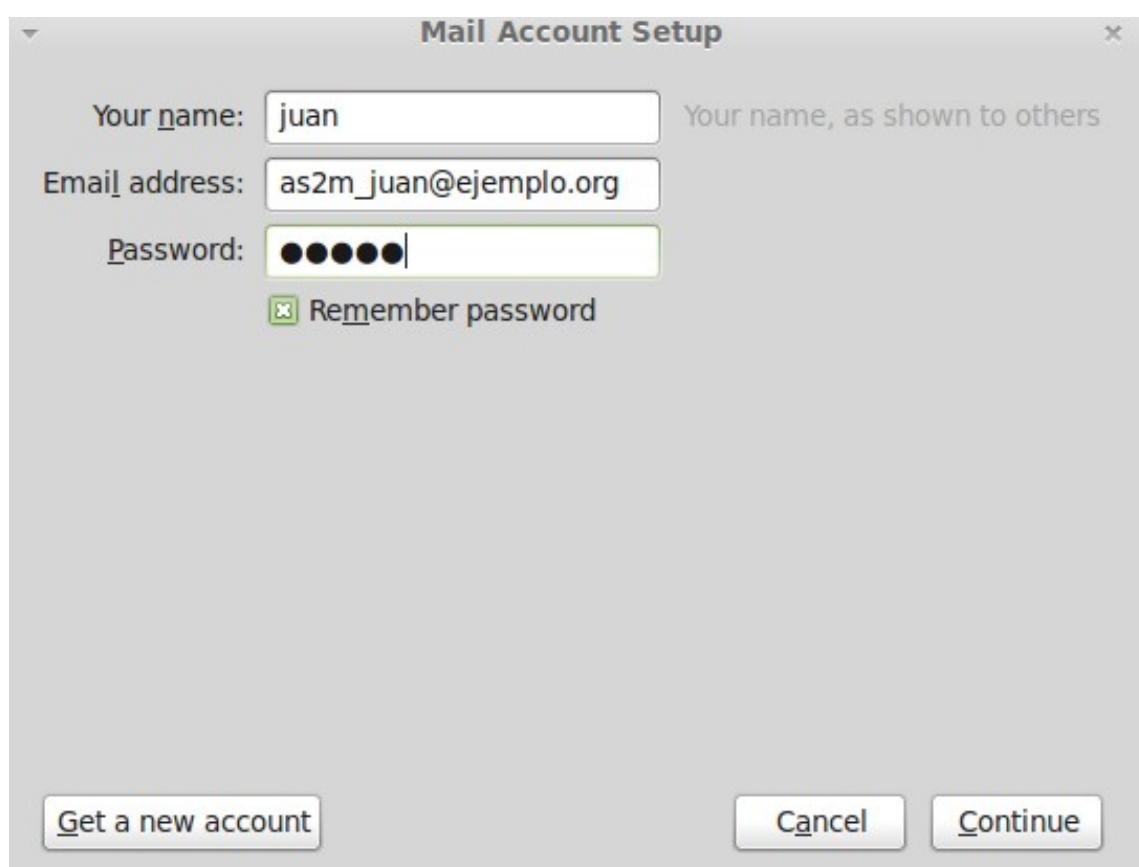
- Primero editamos el archivo de **hosts** para poder resolver el dominio que se ha creado para la practica (ejemplo.org) que corresponde a una maquina virtual con nombre: ubs1004 y IP: 192.168.7.222 donde esta instalado un Servidor de correo con POSTFIX

✓ juan@HZ061512 ~ \$ sudo nano /etc/hosts

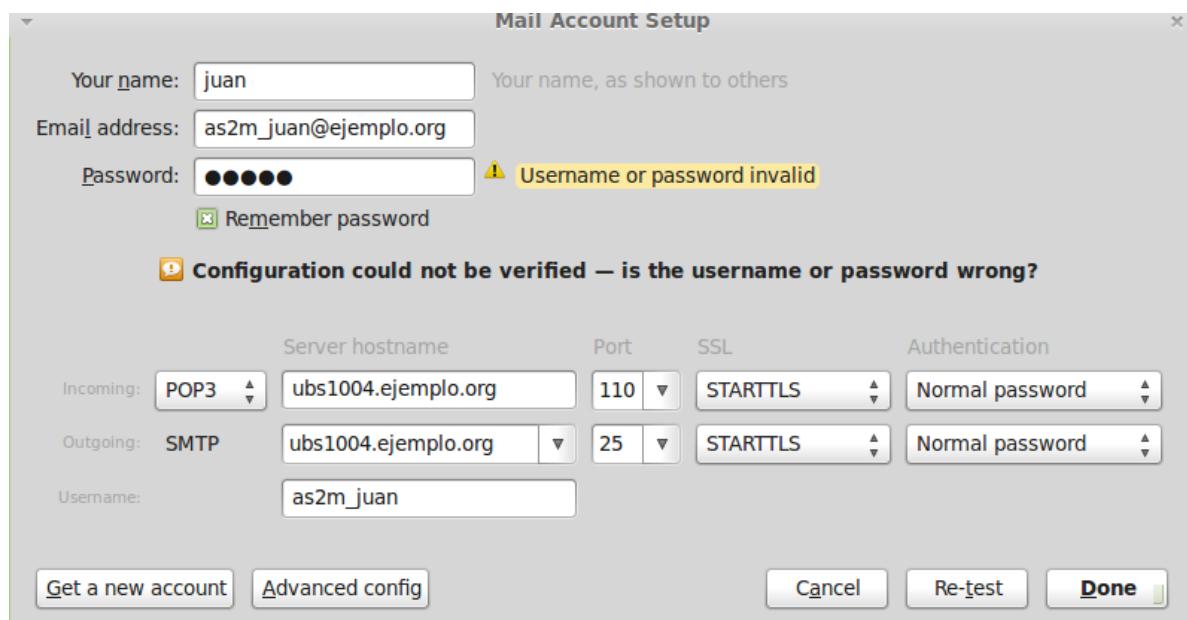
```
127.0.0.1      localhost
127.0.1.1      HZ061512
#linea que se pone para la practica de correo seguro
192.168.7.222  ubs1004.ejemplo.org ejemplo.org
```

```
# The following lines are desirable for IPv6 capable hosts
::1    ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

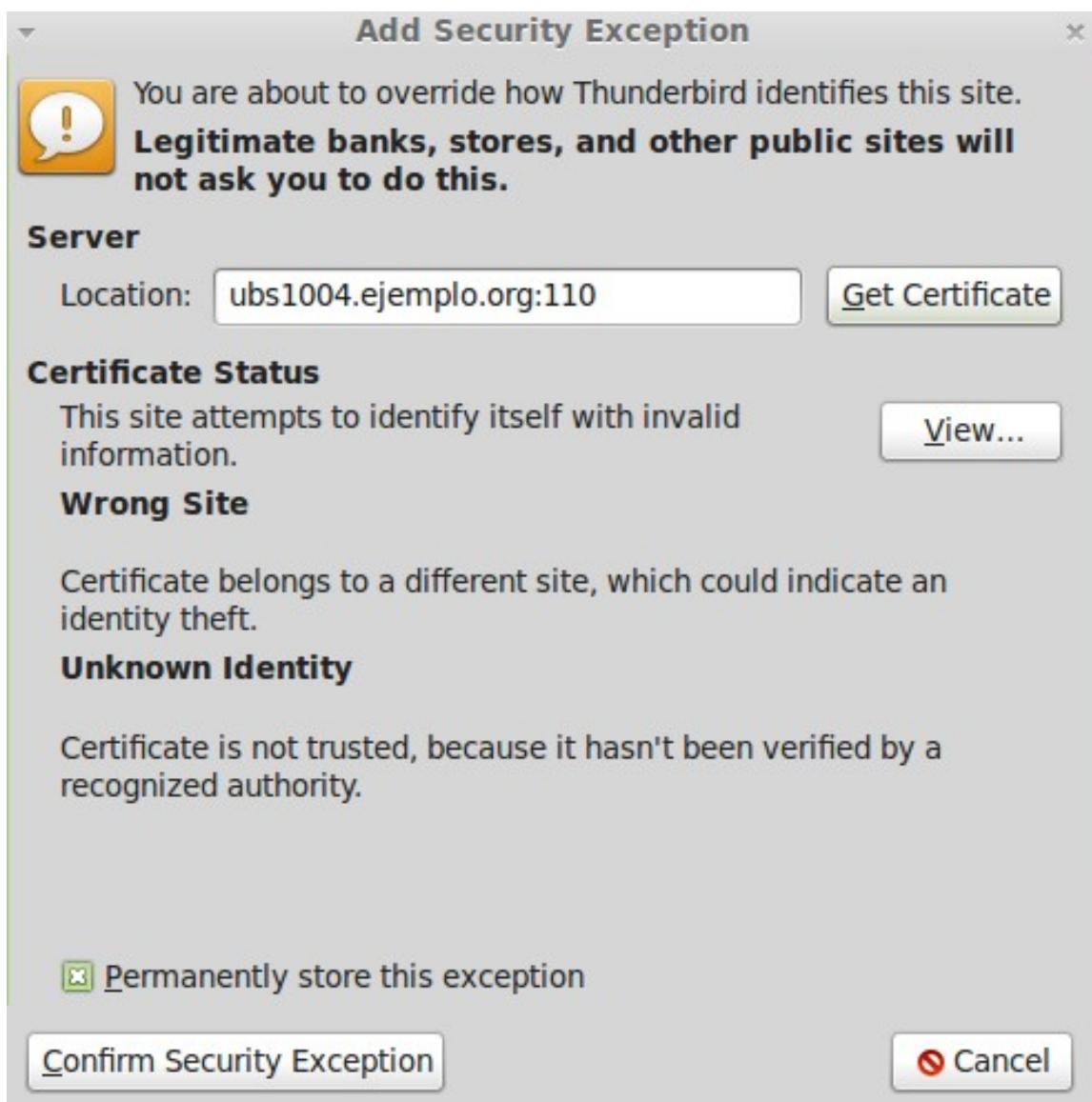
- El usuario creado en la maquina virtual para mi es: **as2m_juan** y su password: 12345
- Se arranca el cliente de correo Thunderbird y se configura la cuenta de correo para el usuario asignado.
- ✓ Se introduce el usuario y la contraseña



- ✓ Mientras se conecta se pincha en 'Configuración manual' y se configuran los parámetros



- ✓ Se acepta la excepción de seguridad



- ✓ Se comprueba la configuración en Thunderbird de la cuenta para que este igual que las imágenes:

as2m_juan@ejemplo.org

- Server Settings
- Copies & Folders
- Composition & Addressing
- Junk Settings
- Disk Space
- Return Receipts
- Security
- Local Folders
- Junk Settings
- Disk Space
- Outgoing Server (SMTP)

Account Settings - <as2m_juan@ejemplo.org>

Account Name:

Default Identity
Each account has an identity, which is the information that other people see when they read your messages.

Your Name:

Email Address:

Reply-to Address:

Organization:

Signature text: Use HTML (e.g., **bold**)

Attach the signature from a file instead (text, HTML, or image):

Attach my vCard to messages

Outgoing Server (SMTP):

Server Settings

Server Type: POP Mail Server

Server Name: Port: Default: 110

User Name:

Security Settings

Connection security:

Authentication method:

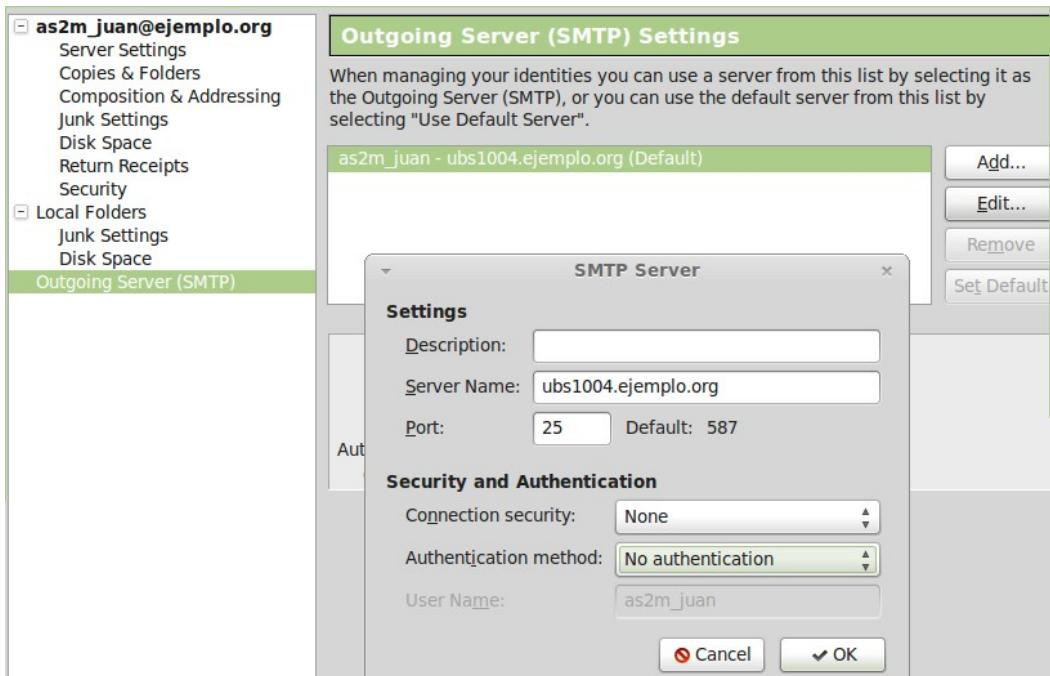
Server Settings

- Check for new messages at startup
- Check for new messages every minutes
- Automatically download new messages
- Fetch headers only
- Leave messages on server
 - For at most days
 - Until I delete them

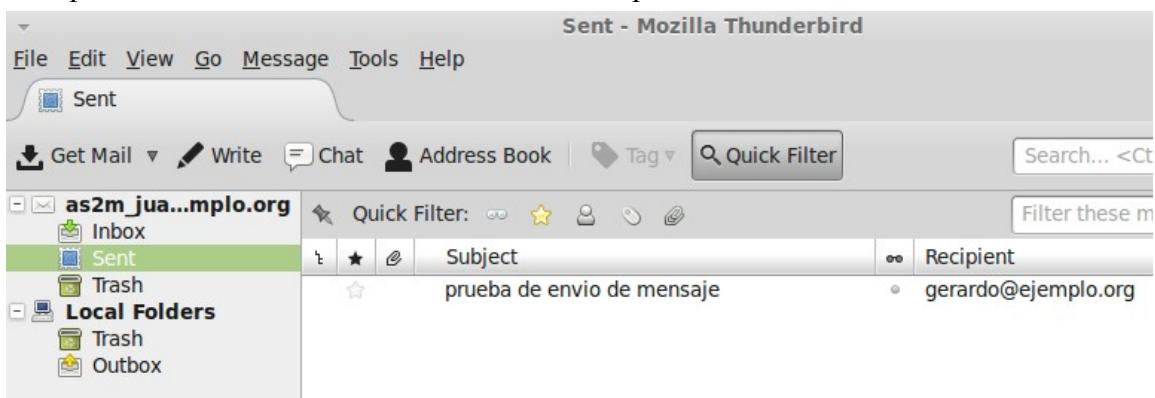
Message Storage

Empty Trash on Exit

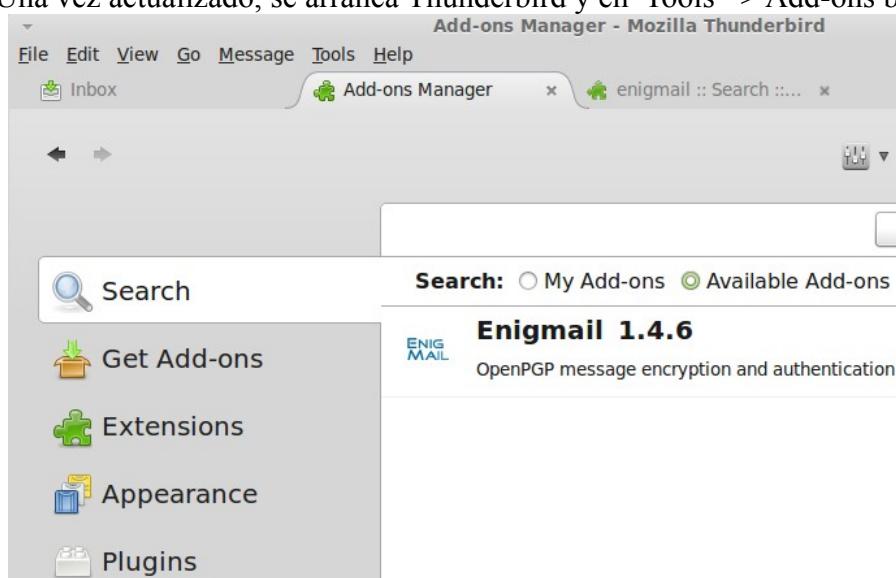
Local directory:



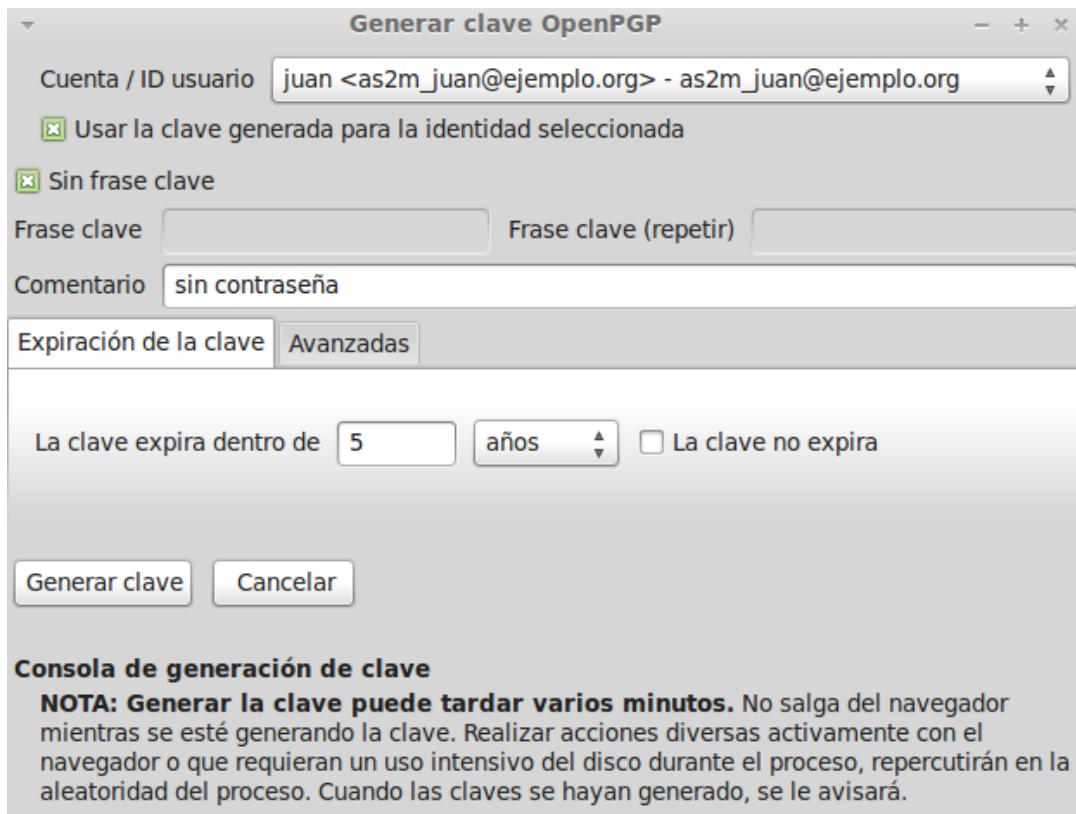
- Se prueba a enviar un correo a la dirección del profesor



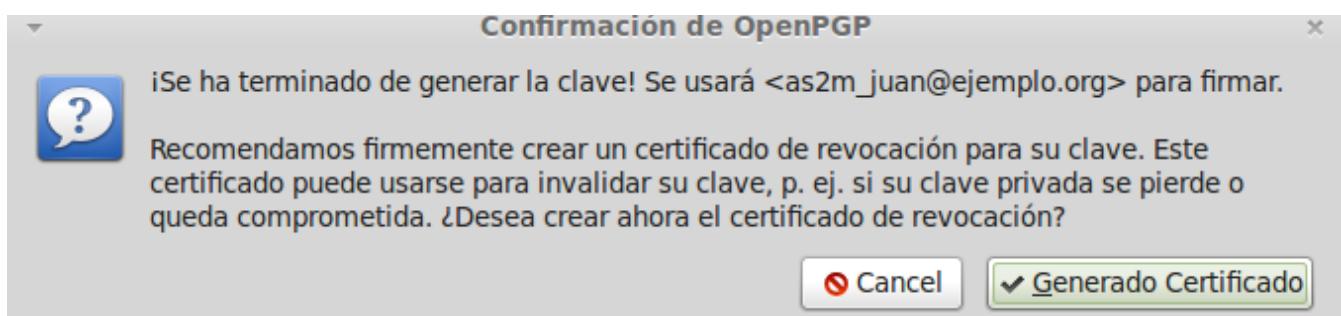
- Para poder tener la opción de cifrar los mensajes hay que instalar un complemento al Thunderbird, para ello tenemos que tener al menos la versión 16 de Thunderbird , actualizamos el sistema con sudo apt-get update y Sistema => Administración => Gestor de actualizaciones.
- Una vez actualizado, se arranca Thunderbird y en Tools => Add-ons buscamos **enigmail**



- Abrimos Administrar claves OpenPGP dentro de la pestaña OpenPGP de Thunderbird que aparece tras instalar el plugin.
- En la pestaña 'OpenPGP' se pincha en 'Administración de claves' y una vez dentro pinchamos en 'Generar' nuevo par de claves.



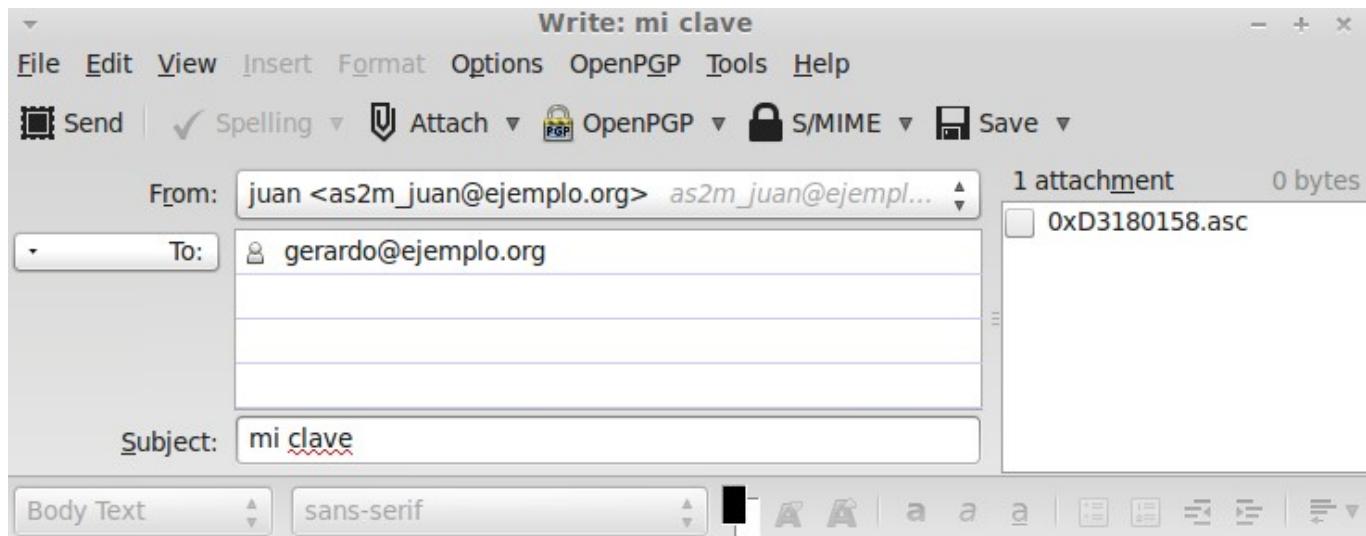
- Se crea el certificado de revocación y se guarda, este certificado se podrá usar para revocar la clave.



- Se busca la clave generada y picando sobre ella y con botón derecho del ratón se selecciona enviar por correo a la persona que queremos que pueda cifrar el mensaje cifrado que nos enviara.



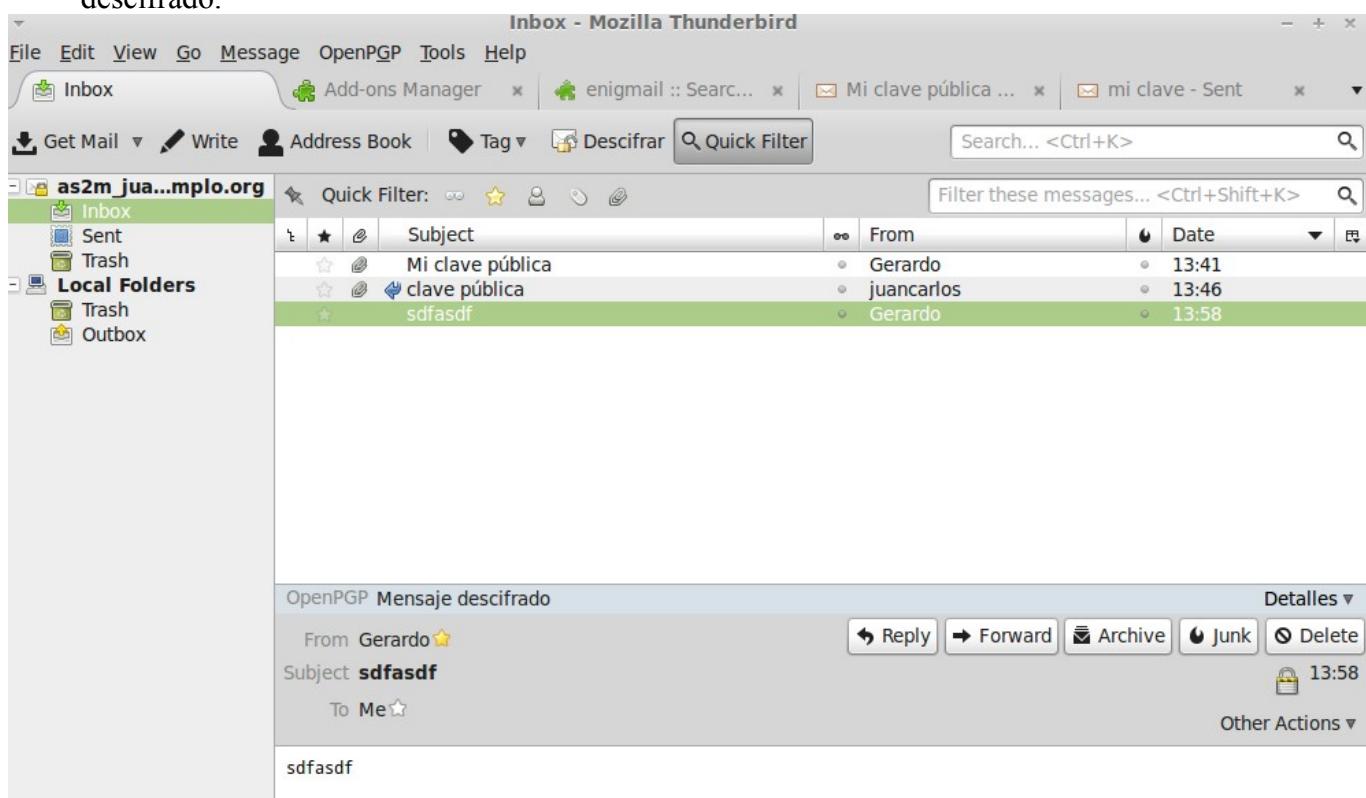
- La clave se enviará por correo a la persona seleccionada y ella tendrá que importar esa clave pública, lo mismo que haré yo también importando su clave pública (para poder enviarle mensajes cifrados con su clave pública), de tal manera que los mensajes cifrados que nos intercambiemos los podamos descifrar.



- A la hora de enviar un mensaje tenemos la opción de cifrarlo pinchando en al pestaña OpenPGP.

El proceso consiste en que Yo encripto el mensaje que le envío a Gerardo con su clave pública y él usando su clave privada lo descifra y Gerardo cifra el mensaje que me envía con mi clave pública y yo lo descifro con mi clave privada.

- En la siguiente pantalla se ve un mensaje que me ha enviado Gerardo cifrado pero que yo veo descifrado.



Test de conocimientos (Cap.6 pag. 160)

1 La configuración de clientes de red en WLAN es menos compleja si:

- a) No se habilita DHCP server en el AP.
- b) Se habilita el SSID broadcast.**
- c) Se habilita la seguridad WEP.
- d) Se habilita la seguridad WPA.

2 Indique qué sentencia es verdadera:

- a) Las redes inalámbricas son más o menos igual de seguras que las cableadas.
- b) Las redes inalámbricas nunca serán tan seguras como las cableadas.**
- c) Las redes cableadas UTP son más seguras que con STP.
- d) Las redes de fibra óptica son menos seguras que las inalámbricas.

3 El mecanismo de seguridad más robusto en redes inalámbricas es:

- a) Open system.
- b) WPA2.**
- c) WPA.
- d) WEP.

4 En redes inalámbricas no se recomienda:

- a) Cambiar el SSID de fábrica.
- b) Cambiar el *password* de administrador por defecto.
- c) Habilitar el DHCP.**
- d) Tener claves WEP complejas.

5 Con respecto a SSH:

- a) Es un servicio único de GNU/Linux.
- b) En Windows se puede emplear el cliente Putty.**
- c) Es un protocolo que emplea el puerto 23.
- d) Ninguna de las anteriores.

6 El puerto que no emplea TLS/SSL es:

- a) 22.**
- b) 990.
- c) 995.
- d) 443.

7 Frente a ataques MitM una posible solución es:

- a) Emplear entradas ARP dinámicas.
- b) Emplear direcciones IP dinámicas.
- c) Emplear direcciones IP estáticas.
- d) Emplear entradas ARP estáticas.**

8 ¿Cuál de estos programas no funciona como sniffer?

- a) Cain & Abel.
- b) Snort.
- c) Wireshark.
- d) LogmeIn.**

9 El protocolo estándar para conexiones VPN suele ser:

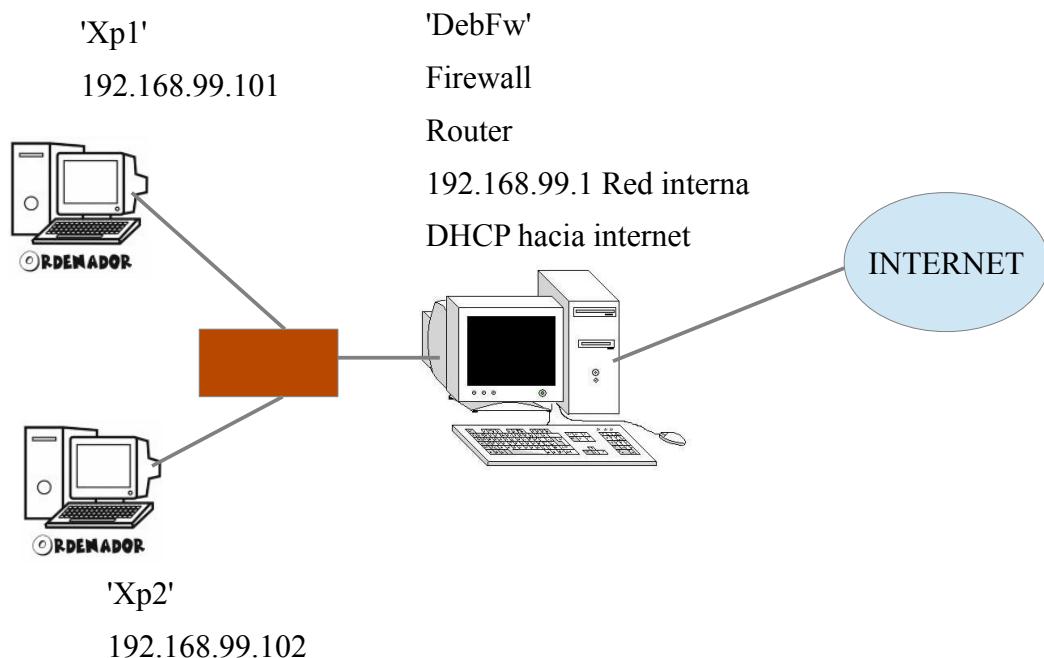
- a) PPTP.
- b) IPSEC.**
- c) L2TP.
- d) SSL/TLS.

Preparación Maquinas virtuales para las Practicas

(T6 – Práctica 6.1, pág. 133)

Se necesitan las siguientes maquinas virtuales:

- ✓ 2 Maquinas virtuales con XP
- ✓ 1 Maquina virtual con Debian



Procedimiento:

- ✓ Descargar DebFw.ova de 192.168.7.2
- ✓ Importarlo desde VirtualBox (Importar servicio virtualizado del menú)
- ✓ Antes de iniciarla, configurar la red que VirtualBox asigna a la máquina:
 - ✗ Tarjeta 1 -> NAT, eth0, PCnetFAST, MAC 080027000000
 - ✗ Tarjeta 2 -> **Red interna** (intnet), eth1, Intel PRO/1000 T, MAC 080027111111
- ✓ Este máquina virtual Debian tiene:
 - ✗ root/12345
 - ✗ La IP de la tarjeta interna es 192.168.99.1
 - ✗ Un script **enruta.sh** gracias al cual puede hacer de enrutador para el resto y que ejecutamos.
 - sh en ruta.sh
- ✓ En un XP virtual:
 - ✗ Configurar la red de VirtualBox como “**Red interna**” e “intnet”
 - ✗ La IP de la tarjeta será 192.168.99.x
 - ✗ Como puerta de enlace deberá tener 192.168.99.1
 - ✗ Tras todo lo anterior, deberá tener acceso a Internet (ping 8.8.8.8)
- ✓ En otro XP virtual configurar lo mismo pero con otra IP diferente (ver dibujo)

Contenido Script '**enruta.sh**'

```
#!/bin/sh
TARJINT=eth1
TARJEXT=eth0

# Vacío todas las reglas de IPtables
iptables -F
iptables -t nat -F

# Cadenas
iptables --delete-chain
iptables -t nat --delete-chain

# Política
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

# loopback interface
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# NAT
iptables -t nat -A POSTROUTING -o $TARJEXT -j MASQUERADE

# Permito reenvío
iptables -A FORWARD -i $TARJINT -o $TARJEXT -j ACCEPT
iptables -A FORWARD -i $TARJEXT -o $TARJINT -m state --state ESTABLISHED,RELATED -j
ACCEPT

echo 1 > /proc/sys/net/ipv4/ip_forward
```

Configuración maquina virtual Debian con dos tarjetas de Red:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
    address 192.168.99.1
    netmask 255.255.255.0
```

Envenenamiento Tablas ARP - Práctica 6.1

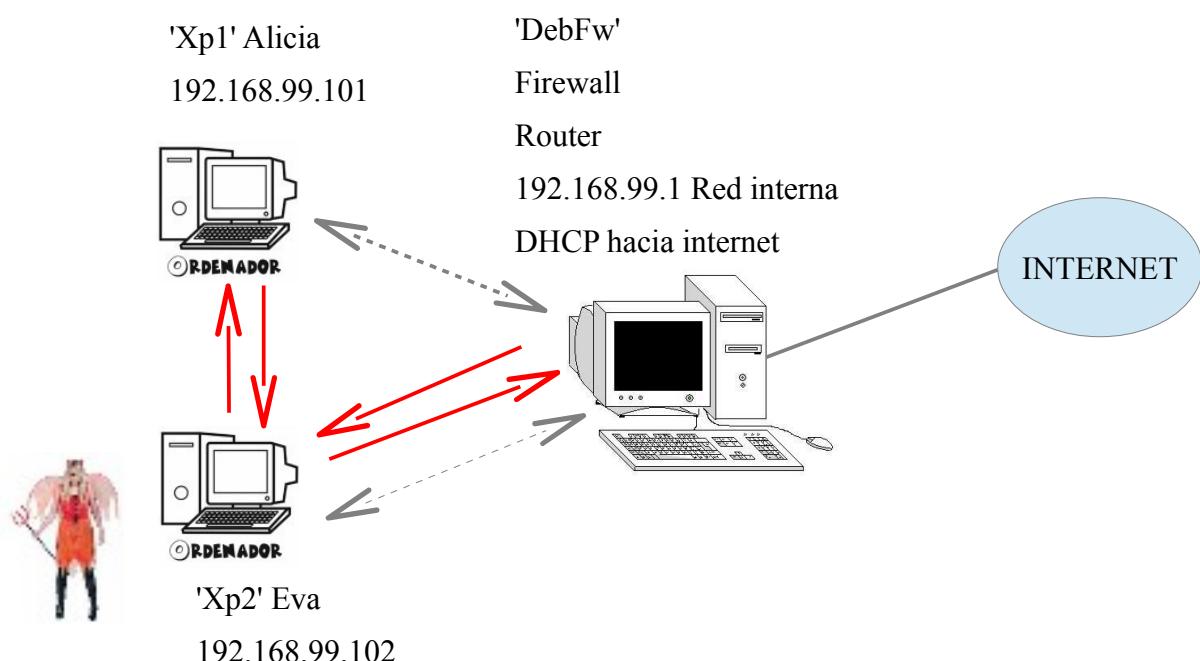
(T6 – Práctica 6.1, pág. 133)

Para la práctica hay que descargar el programa Cain&Abel

✓ www.oxid.it/cain.html

Situación:

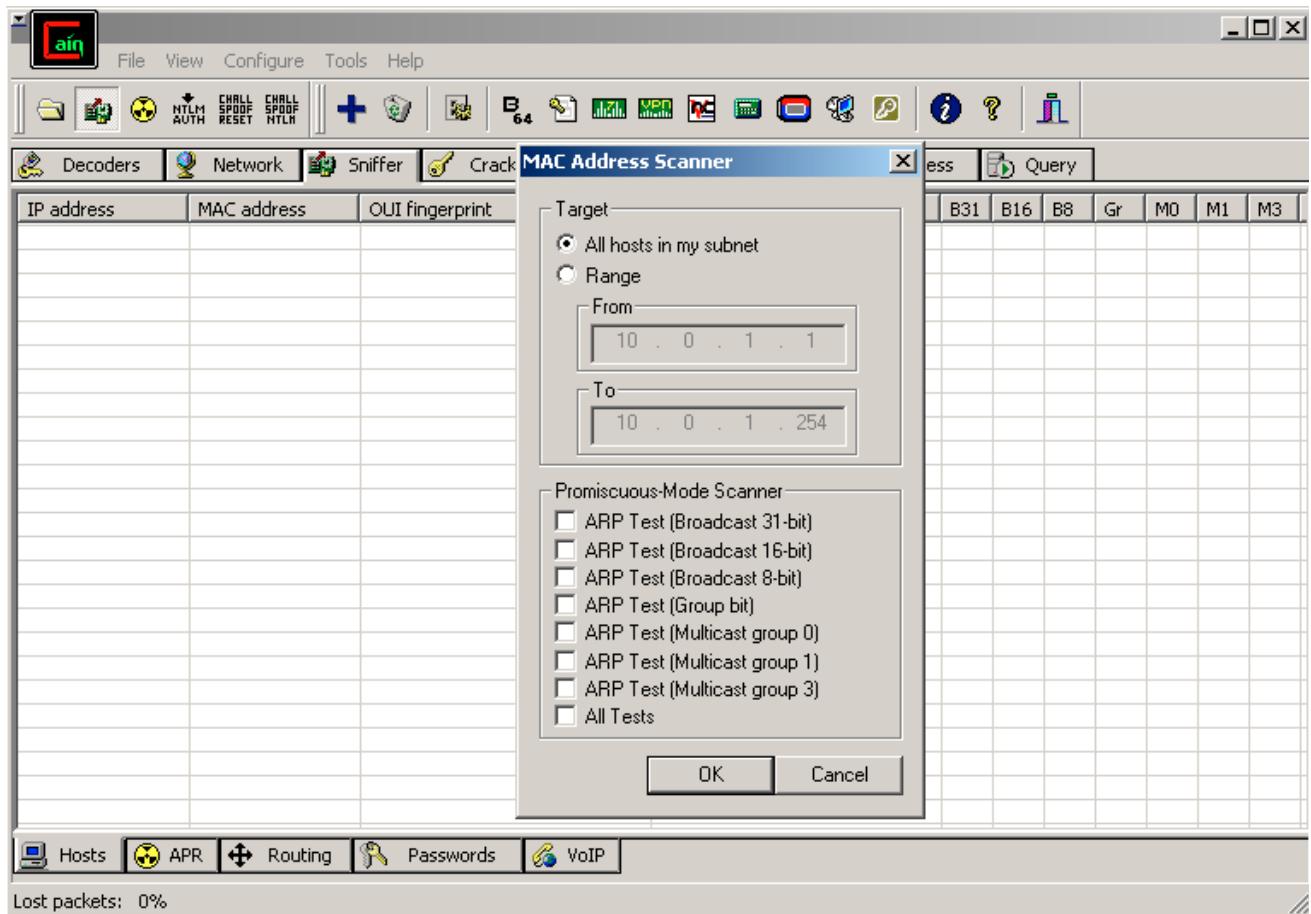
- XP1 sera Alicia Un inocente ordenador
- DebFw sera Bob Hace de router
- XP2 sera Eva El malo (La diablesa)



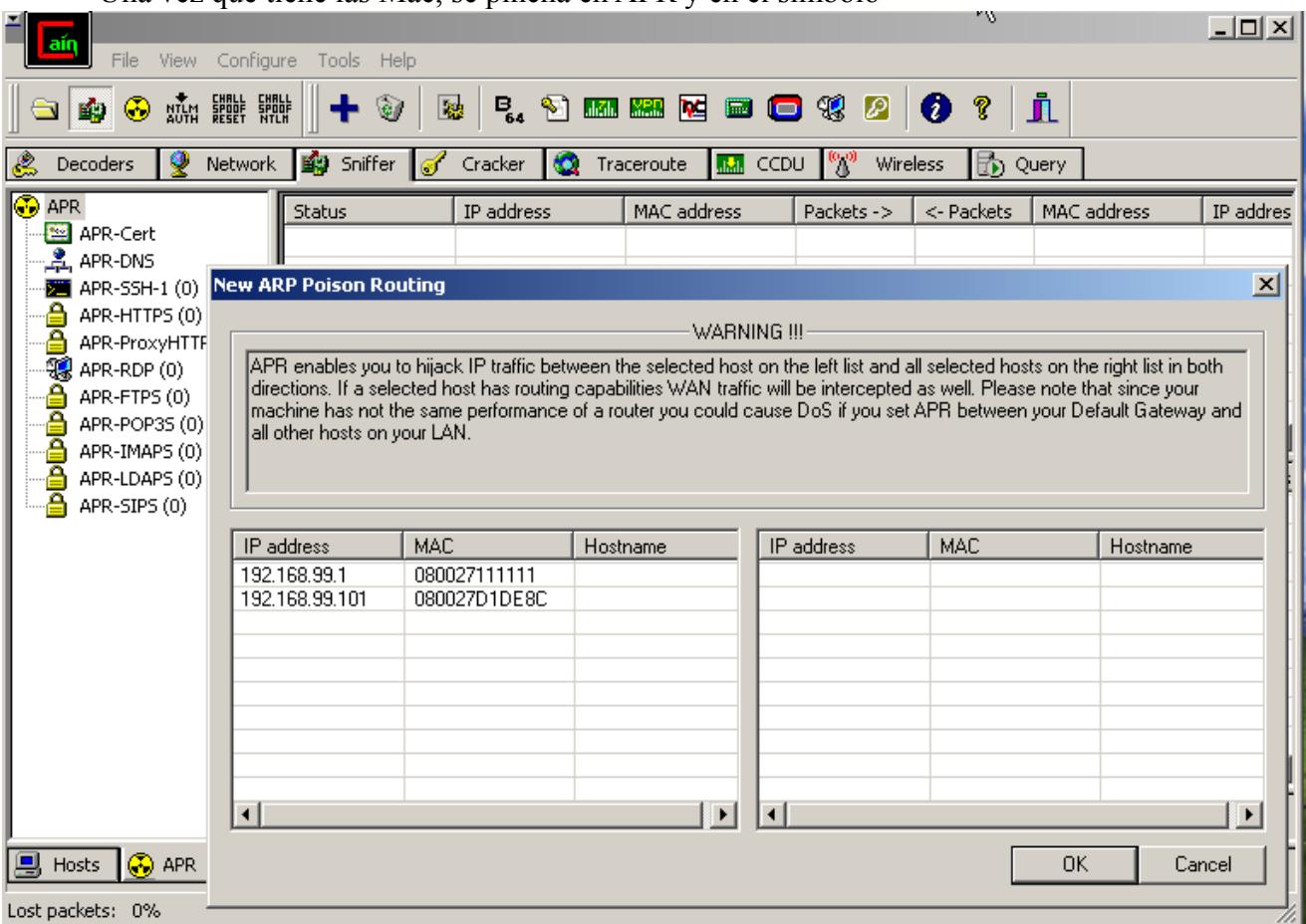
En gris el tráfico normal y en rojo como es el tráfico una vez que se arranca el programa Cain&Abel y envenena las tablas de ARP del equipo Debian y XP1 haciendo que el tráfico pase por él.

Desde Eva descargar Cain&Abel ([ca_setup.exe](#)) de la web: www.oxid.it/cain.html

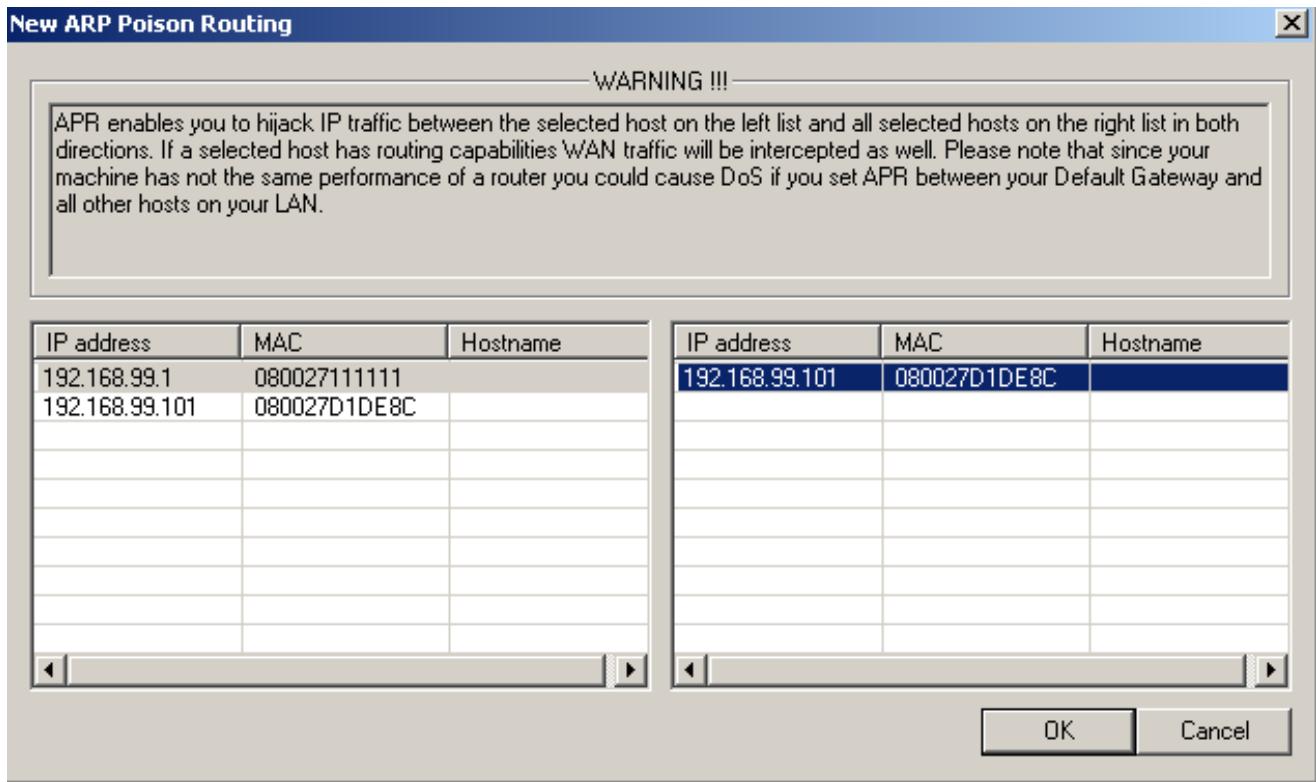
- Instalar Cain&Abel
- Tras la instalación pide instalar un paquete de driver, le decimos que si.
 - marcamos que NO arranque el WinPcap driver en el boot time.
- Se arranca el programa, que avisa que está activado el Firewall de windows y algunas funcionalidades no funcionaran.
 - Se desactiva el Firewall de windows
 - Se selecciona 'Sniffer' y el apartado 'Host', se pincha en el símbolo de la tarjeta para iniciar y a continuación en el símbolo '+', sale una pantalla de 'Mac Address Scanner' que por defecto marca 'All host in my subnet' y le damos a OK.



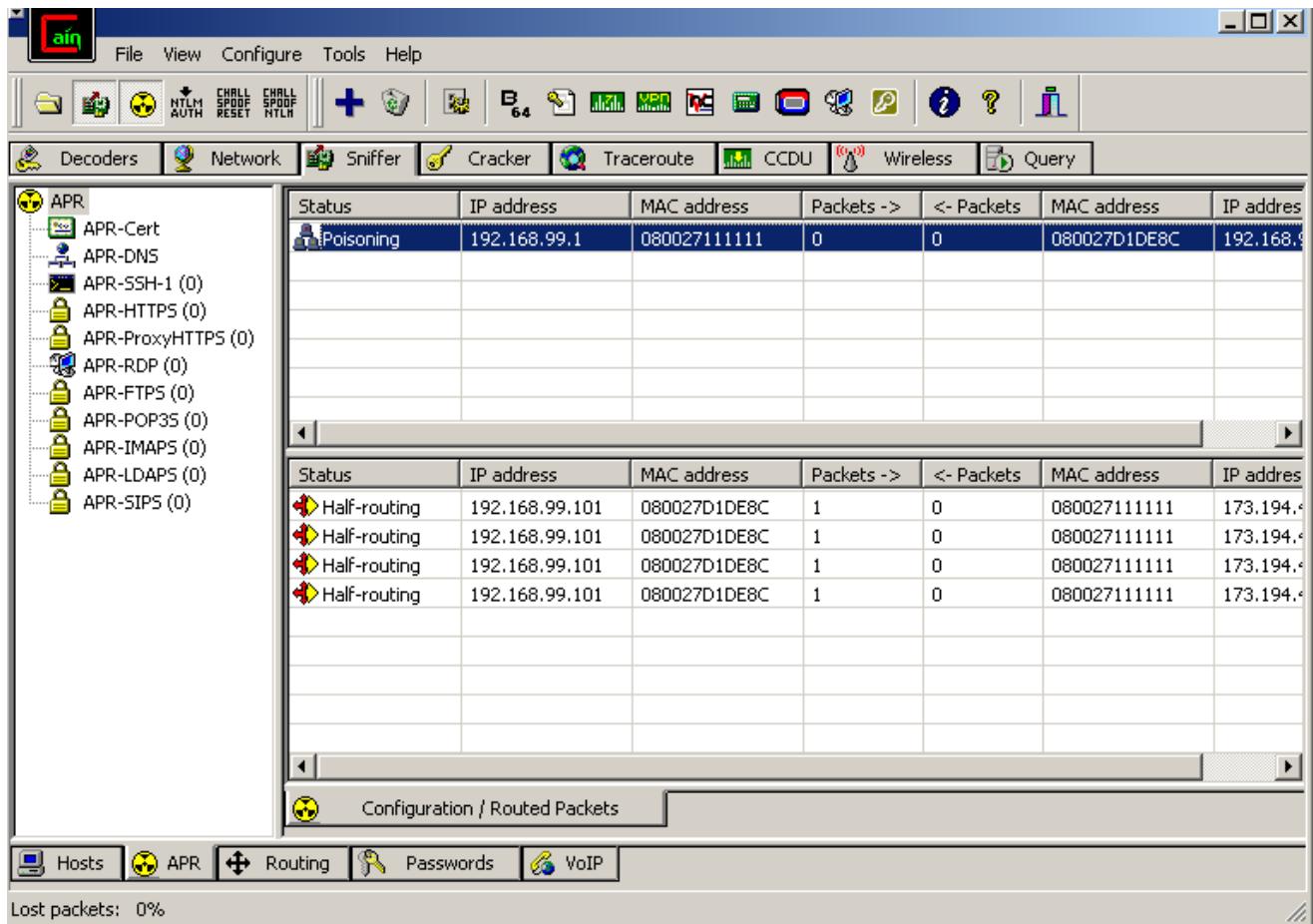
- Una vez que tiene las Mac, se pincha en APR y en el símbolo +



- Se seleccionan los equipos y OK.



- Se pincha en el símbolo de APR y start.



- Vamos al XP1 (Alicia) y en el Navegador web vamos a una pagina de correo y intentamos entrar con un usuario y contraseña (no importa que de error de usuario o contraseña al entrar).

[←](#) correoweb.euskaltel.es/login/login.jsp ★ ▾ C



Correo web

Identificador:

Clave:

entrar

Para solicitar una nueva cuenta de correo infórmese en nuestro teléfono gratuito de Atención al Cliente.

euskaltel

- Atención a Particulares: **1717**

- Atención a Empresas: **900 840 200**

© Euskaltel, S.A.

- Y en el programa si vamos a 'Contraseñas' y el apartado 'HTTP', veo que ha capturado el usuario y contraseña que había metido.

Sniffer

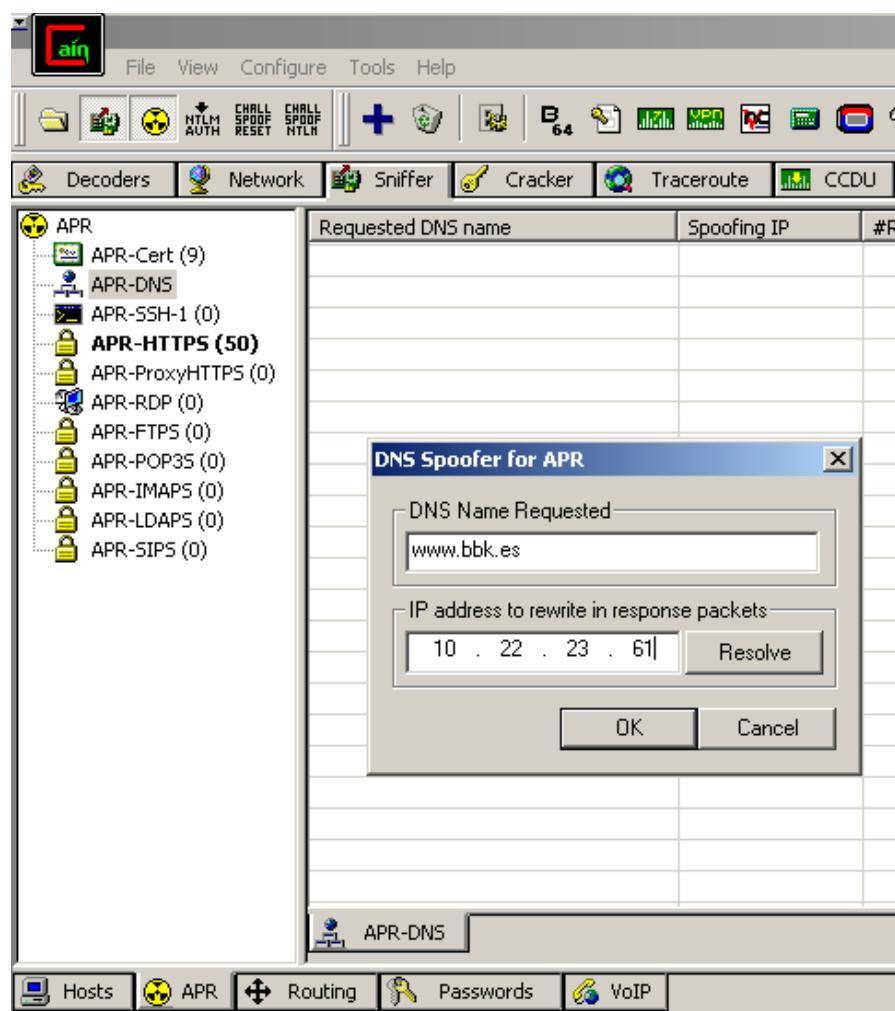
Decoders	Network	Sniffer	Cracker	Traceroute	CCDU	Wireless	Query
Passwords							
FTP (0)	Timestamp	HTTP server	Client	Username	Password	URL	
HTTP (21)	18/12/2012 - 0:10:52	173.194.41.8	192.168.99.101	682967434	925x620	http://www.euskaltel.com/CanalOnline/integracion/live/m	
IMAP (0)	18/12/2012 - 10:11:53	173.194.41.8	192.168.99.101	587010972	925x620	http://www.euskaltel.com/CanalOnline/integracion/live/m	
LDAP (0)	18/12/2012 - 10:15:36	173.194.41.2	192.168.99.101	1883997885	925x620	http://www.euskaltel.com/CanalOnline/homes/home_parl	
POP3 (0)	18/12/2012 - 10:15:36	173.194.41.2	192.168.99.101	1883997885	925x620	http://www.euskaltel.com/CanalOnline/homes/home_parl	
SMB (1938)	18/12/2012 - 10:15:36	173.194.41.2	192.168.99.101	1883997885	925x620	http://www.euskaltel.com/CanalOnline/homes/home_parl	
Telnet (0)	18/12/2012 - 10:15:36	173.194.41.2	192.168.99.101	1883997885	925x620	http://www.euskaltel.com/CanalOnline/homes/home_parl	
VNC (0)	18/12/2012 - 10:16:43	173.194.41.2	192.168.99.101	88365802	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
TDS (0)	18/12/2012 - 10:16:43	173.194.41.2	192.168.99.101	88365802	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
TNS (0)	18/12/2012 - 10:16:43	173.194.41.2	192.168.99.101	88365802	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
SMTP (0)	18/12/2012 - 10:16:43	173.194.41.2	192.168.99.101	88365802	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
NNTP (0)	18/12/2012 - 10:16:59	173.194.41.2	192.168.99.101	961118224	771x436	http://www.euskaltel.com/CanalOnline/integracion/live/m	
DCE/RPC (0)	18/12/2012 - 10:17:12	2.23.69.186	192.168.99.101	66055	SAPI_LONG	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11	
MSKerberos-PreAuth (0)	18/12/2012 - 10:17:13	2.23.69.186	192.168.99.101	66055	SAPI_LONG	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11	
Radius-Keys (0)	18/12/2012 - 10:17:20	173.194.41.2	192.168.99.101	1221438806	771x436	http://www.euskaltel.com/CanalOnline/integracion/live/m	
Radius-Users (0)	18/12/2012 - 10:17:53	173.194.41.2	192.168.99.101	1502362247	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
ICQ (0)	18/12/2012 - 10:17:53	173.194.41.2	192.168.99.101	1502362247	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
IKE-PSK (0)	18/12/2012 - 10:17:53	173.194.41.2	192.168.99.101	1502362247	771x436	http://www.euskaltel.com/CanalOnline/homes/home_parl	
MySQL (0)	18/12/2012 - 10:18:28	212.55.8.74	192.168.99.101	pepe@pepe.mail	pruebacontraseña	http://correoweb.euskaltel.es/login/login.jsp	
Hosts	APR	Routing	Passwords	VoIP			
Lost packets: 0%							

- Esta es otra prueba curiosa, se accede a hotmail desde Firefox y no recupera la contraseña va por https (pone MBA) hacemos lo mismo desde Internet Explorer de windows (versión 6) resulta que si captura la contraseña y usuario.

The screenshot shows the Cain & Abel interface with the 'Passwords' module selected. A tree view on the left lists various protocols and their counts: FTP (0), HTTP (39), IMAP (0), LDAP (0), POP3 (0), SMB (1938), Telnet (0), VNC (0), TDS (0), TNS (0), SMTP (0), NNTP (0), DCE/RPC (0), MSKerb5-PreAuth (0), Radius-Keys (0), Radius-Users (0), ICQ (0), IKE-PSK (0), MySQL (0), SNMP (0), SIP (0), GRE/PPP (0), PPPoE (0), and SAP Diag (1). The main pane displays a table of captured password entries:

	Timestamp	HTTP server	Client	Username	Password	URL
	18/12/2012 - 10:17:13	2.23.69.186	192.168.99.101	66055	SAPI_LONG	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:17:20	173.194.41.2	192.168.99.101	1221438806	771x436	http://www.euskaltel.com/CanalOnline/integraci
	18/12/2012 - 10:17:53	173.194.41.2	192.168.99.101	1502362247	771x436	http://www.euskaltel.com/CanalOnline/homes/h
	18/12/2012 - 10:17:53	173.194.41.2	192.168.99.101	1502362247	771x436	http://www.euskaltel.com/CanalOnline/homes/h
	18/12/2012 - 10:18:28	212.55.8.74	192.168.99.101	pepe@pepe.mail	pruebacontraseña	http://correoeweb.euskaltel.es/login/login.jsp
	18/12/2012 - 10:27:04	212.55.8.73	192.168.99.101	pk`pouipou	ijijoji` pojp	http://correoeweb.euskaltel.es/login/login.jsp?err
	18/12/2012 - 10:28:52	173.194.41...	192.168.99.101	2	1	http://www.google.es/
	18/12/2012 - 10:28:53	173.194.41...	192.168.99.101	5	2	http://www.google.es/
	18/12/2012 - 10:28:53	173.194.41...	192.168.99.101	8	3	http://www.google.es/
	18/12/2012 - 10:28:53	173.194.41...	192.168.99.101	b	4	http://www.google.es/
	18/12/2012 - 10:28:53	173.194.41...	192.168.99.101	e	5	http://www.google.es/
	18/12/2012 - 10:28:54	173.194.41...	192.168.99.101	h	6	http://www.google.es/
	18/12/2012 - 10:28:54	173.194.41...	192.168.99.101	k	7	http://www.google.es/
	18/12/2012 - 10:29:02	65.54.165....	192.168.99.101	64855	MBI	http://www.google.es/search?hl=es&source=hp
	18/12/2012 - 10:29:04	2.23.69.186	192.168.99.101	64855	MBI	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:29:04	65.54.165....	192.168.99.101	64855	MBI	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:29:27	65.54.165....	192.168.99.101	64855	MBI	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:29:28	65.54.165....	192.168.99.101	prueba@hotmail.com	contraseñaa	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:29:29	2.23.69.186	192.168.99.101	64855	MBI	https://login.live.com/psscure/post.srf?wa=w
	18/12/2012 - 10:31:50	212.55.8.74	192.168.99.101	prueba@hotmail.com	clavesegura	http://correoeweb.euskaltel.es/login/login.jsp?err
	18/12/2012 - 10:32:02	65.54.165....	192.168.99.101	64855	MBI	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:32:23	65.54.165....	192.168.99.101	64855	MBI	https://login.live.com/login.srf?wa=wsignin1.0&
	18/12/2012 - 10:32:28	65.54.165....	192.168.99.101	prueb@hotmail.com	clavesegura	https://login.live.com/login.srf?wa=wsignin1.0&

- Vamos a la opción ARP-DNS y le podemos decir que un Nombre de dominio lo redirija a una IP que especifiquemos.



- Vemos como al poner www.bbk.es sale la pagina que muestra la IP que le hemos puesto (la del colegio).

IEFPS Elorrieta-Erreka Mari GBLHI - Dpto. de Informática - Informatika Saila - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda

Dirección <http://www.bbk.es/> Ir Vínculos >

Elorrieta-Erreka Mari | Kibia | Programas |

Dpto. de informática - Informatika Saila

Páginas de l@s profesor@s - Irakasleen orrialdeak

- [C. Etxeandia](#)
- [J. González](#)
- [J.J. Orcasitas](#)
- [G. Fernández](#)
- [A. Ortega](#)
- [HOBETUZ](#)
- [1.ASI](#)

Cursos - Ikastaroak

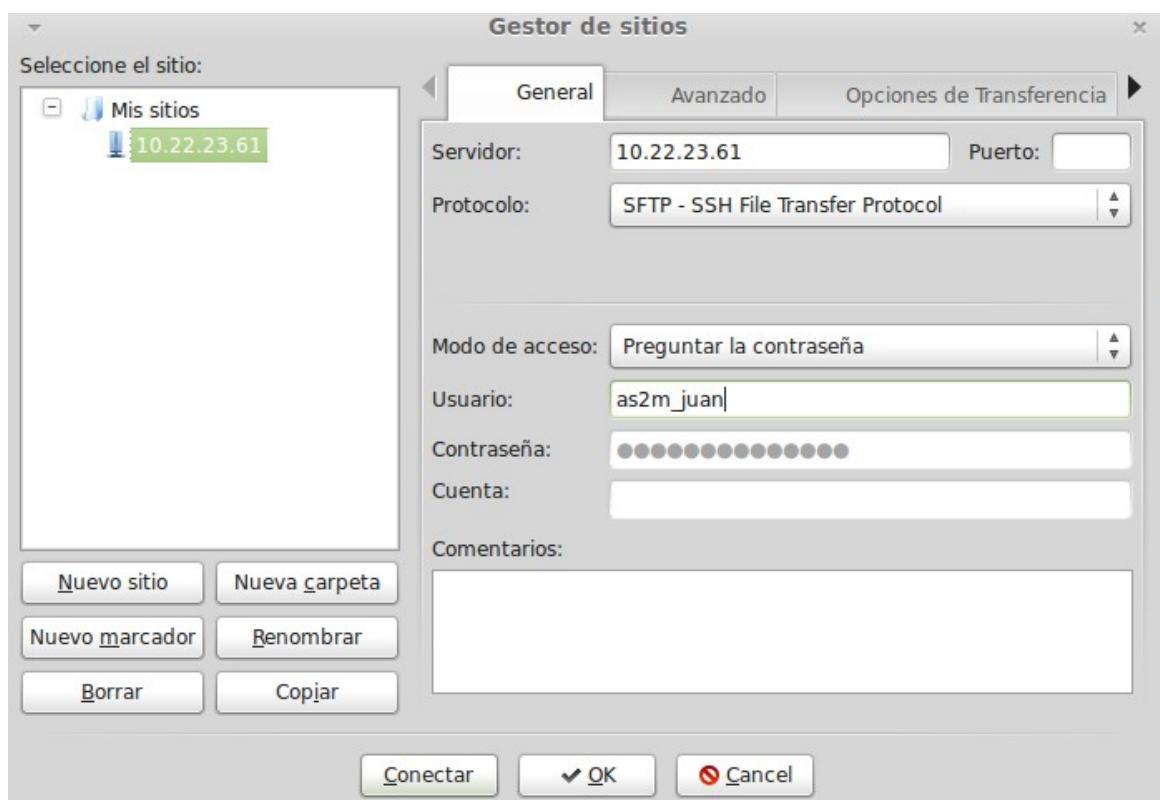
- [Cursos](#)

Internet

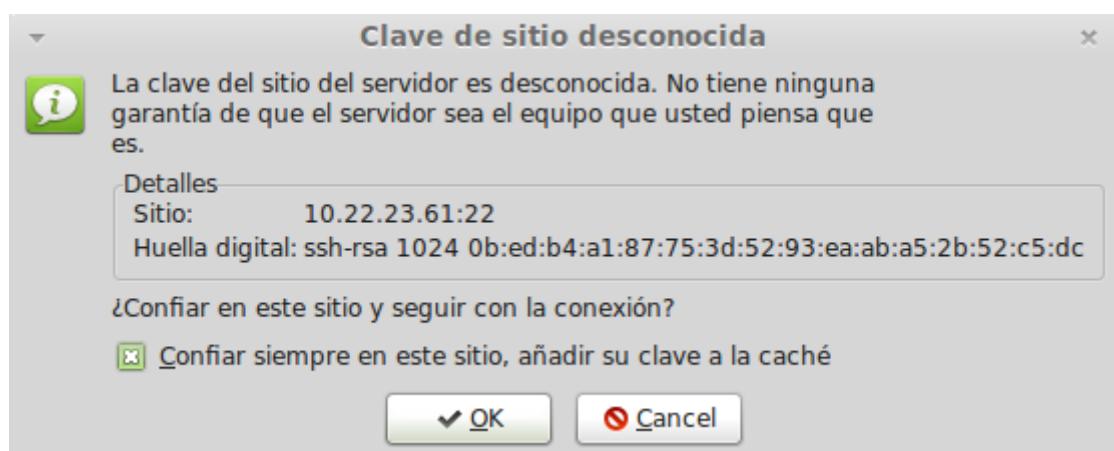
FTP seguro SFTP - Practica 6.5

(T6 – Práctica 6.5, pág. 144)

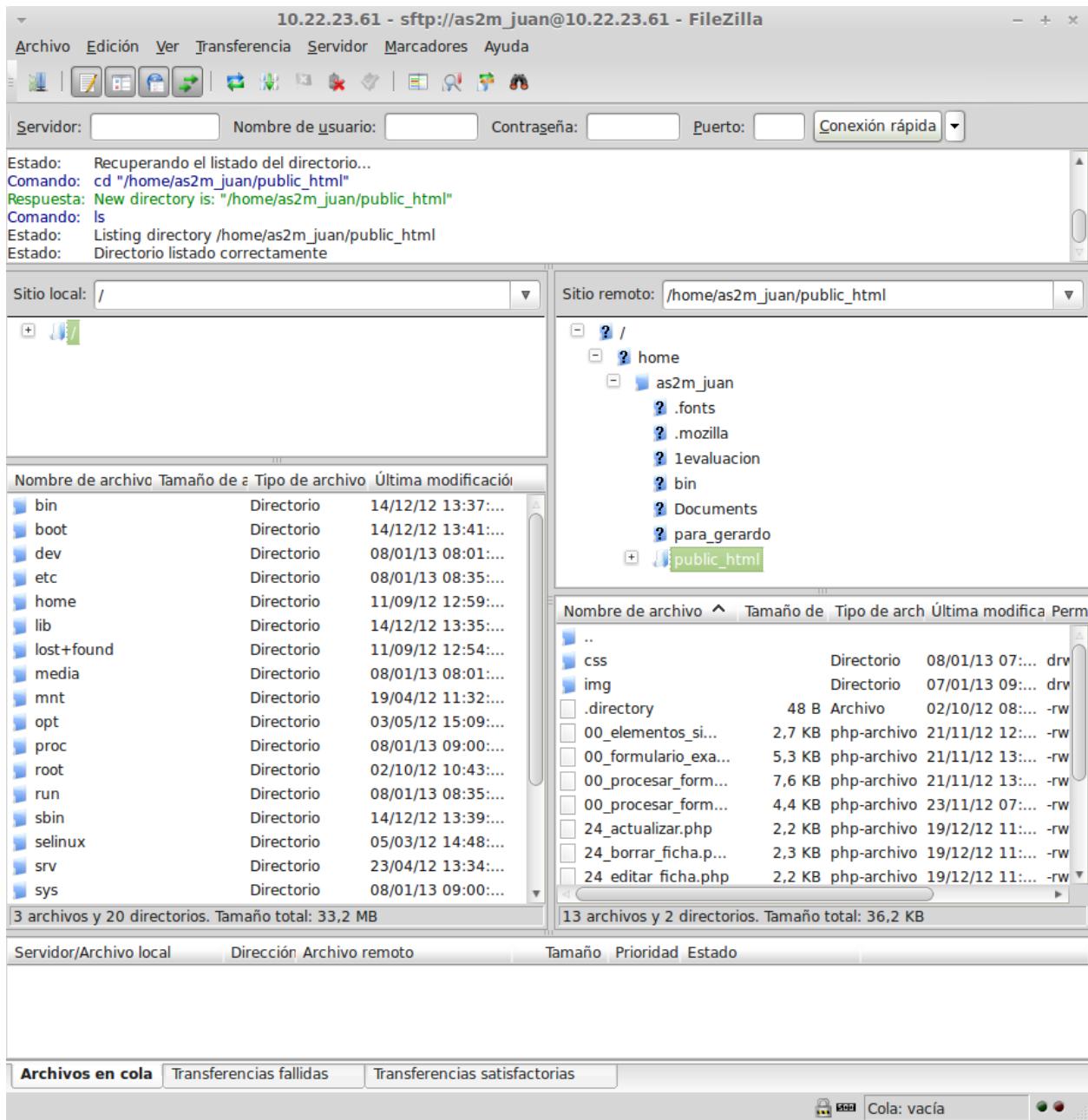
1. Para la practica hay que descargar el programa Filezilla
 - ✓ <http://filezilla-project.org/>
 - ✓ En Linux Mint se instala con el Gestor de software
2. Una vez arrancado el programa se pincha en 'Archivo', 'Gestor de sitios' y se configura para que use el protocolo FTP seguro (SFTP) así como los datos de acceso como usuario, contraseña y dirección IP del servidor.



- ✓ Al ser la primera vez que se conecta sale un aviso de clave desconocida, damos OK.



- ✓ Una vez dentro ya podemos acceder de forma segura a nuestro sitio.



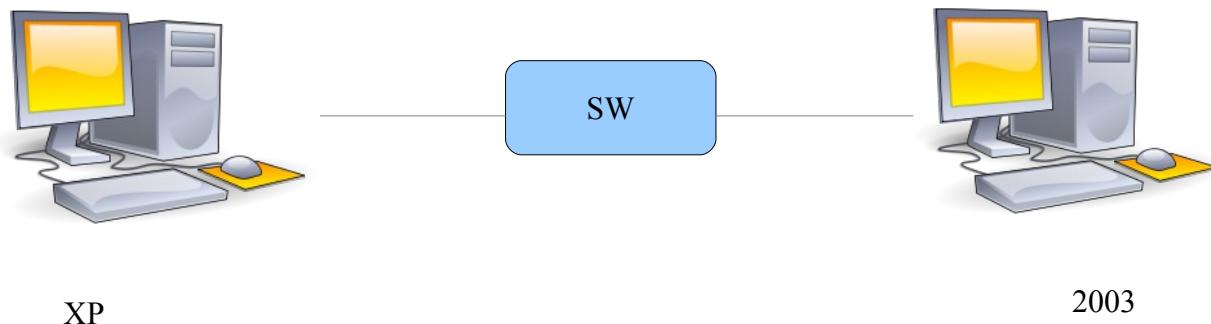
Simulación conexión VPN - Práctica 6.6

(T6 – Práctica 6.6, pág. 146)

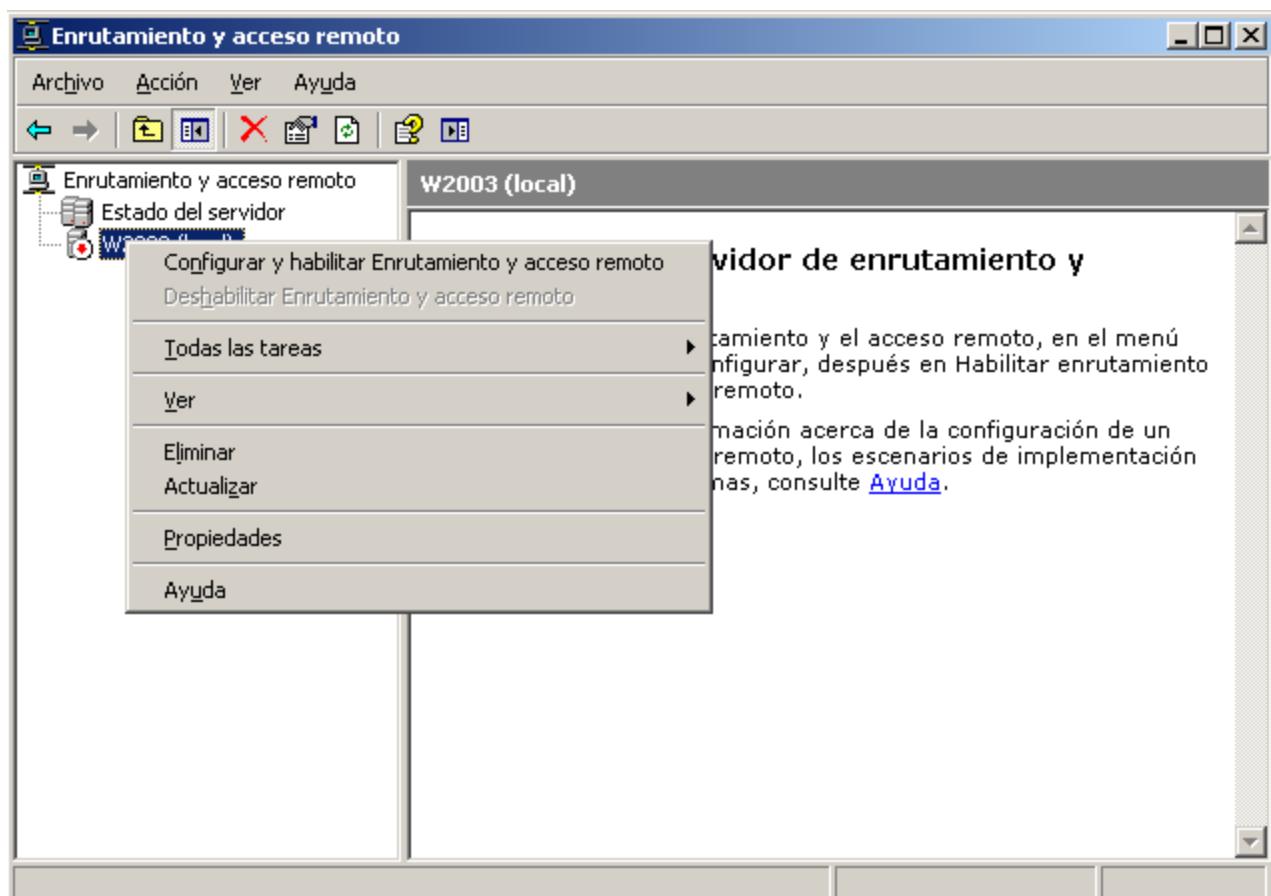
Nota: No se va a hacer exactamente la práctica del libro.

Se trata de hacer una práctica de VPN entre una máquina virtual con Windows 2003 server virtualizado y un XP también virtualizado.

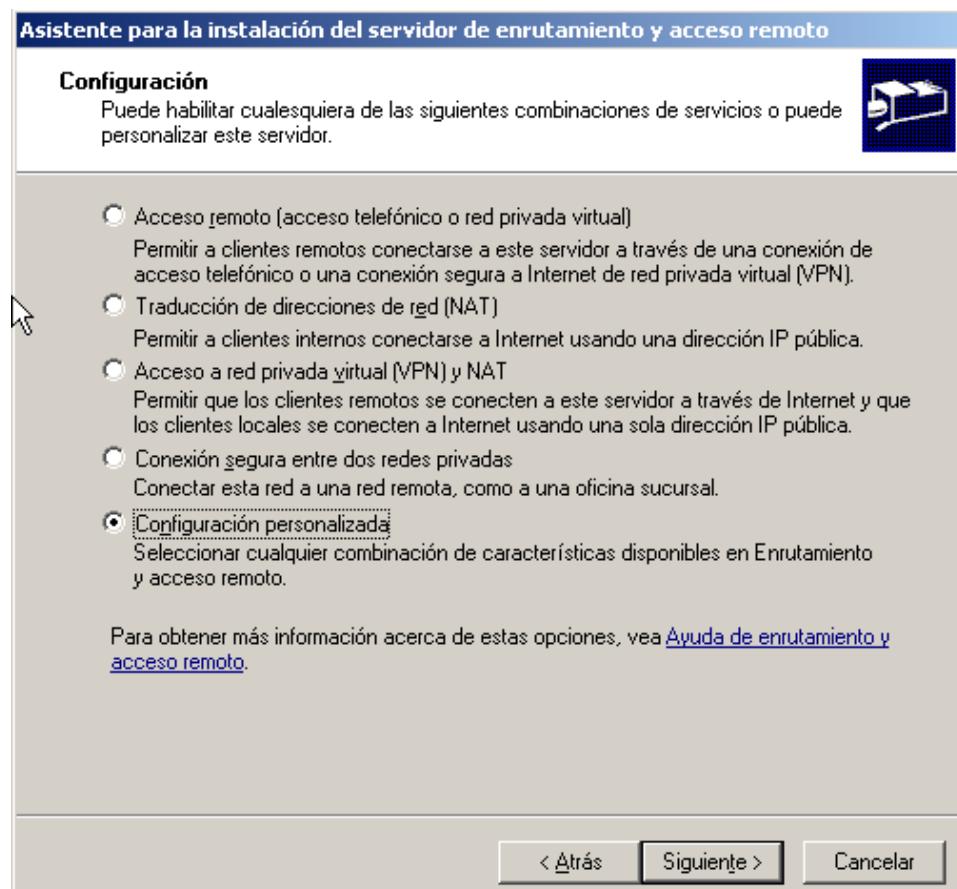
Para la práctica hay que descargar una máquina virtual de 2003



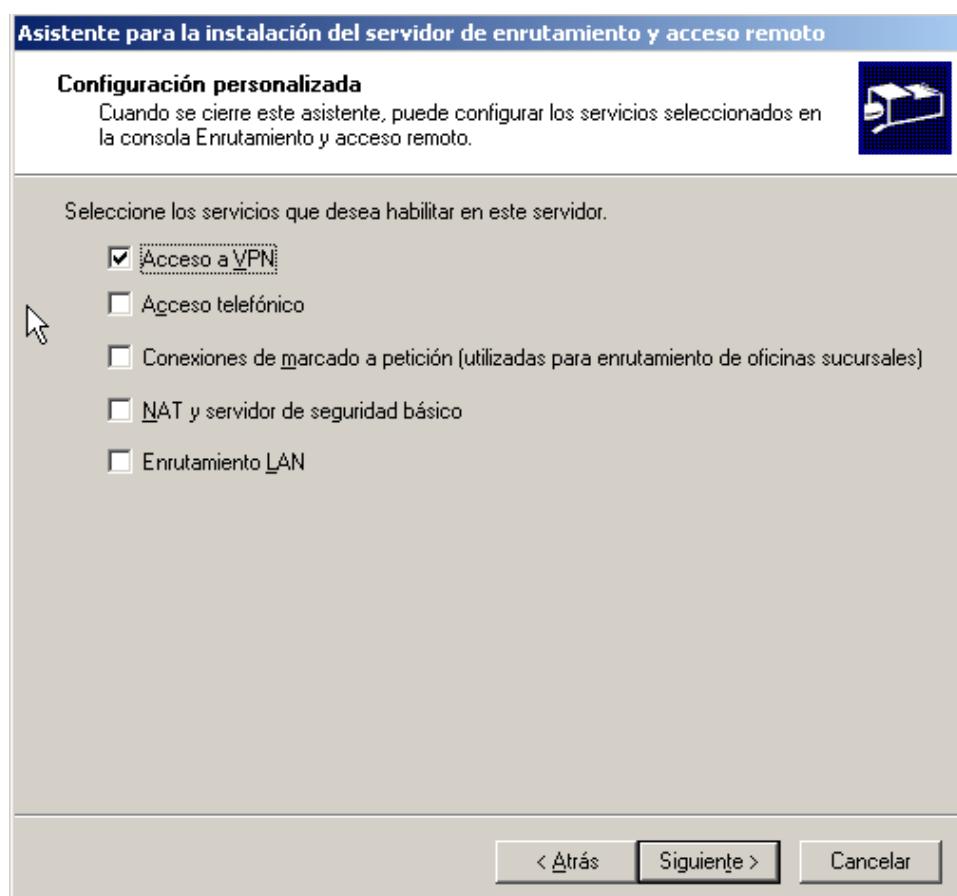
1. En el Server 2003 hay que configurar el acceso VPN y acceder como Administrador.
 - ✓ Entrar en Herramientas administrativas -> Enrutamiento y Acceso remoto y con botón derecho del ratón encima del servidor, elegir 'Configurar enrutamiento...'!



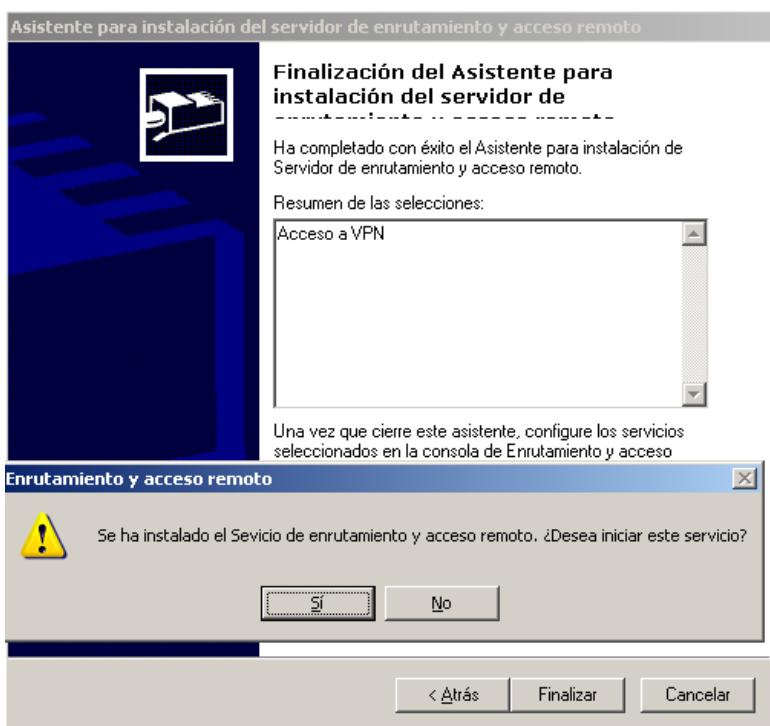
- ✓ Se selecciona 'Configuración personalizada' .



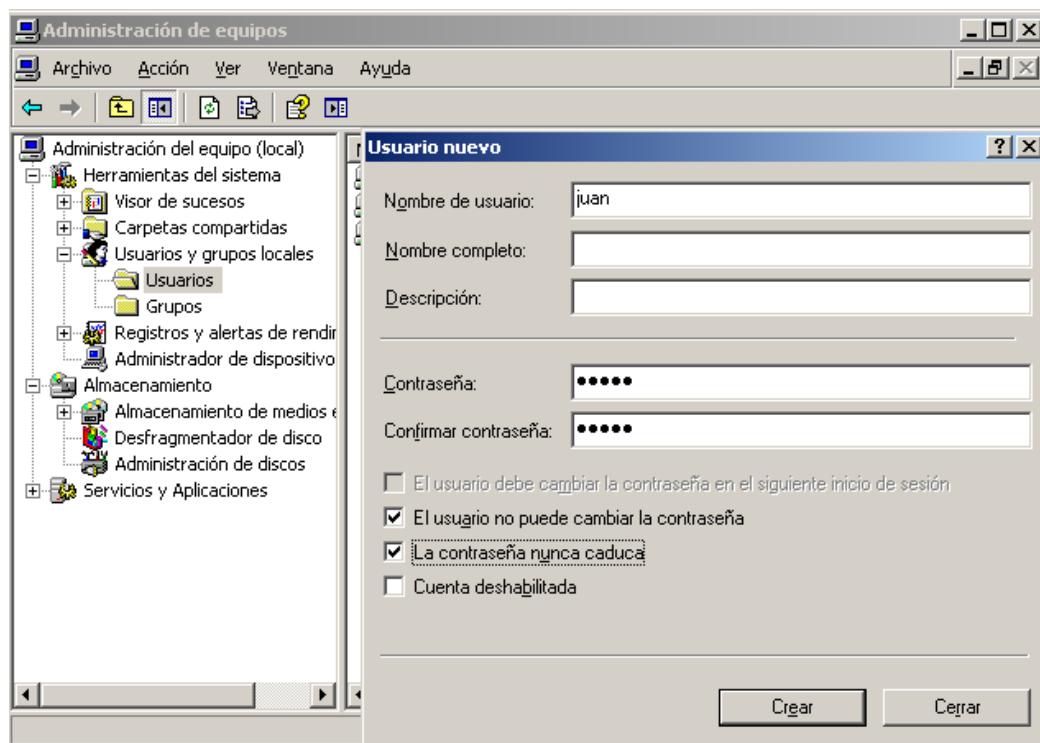
- ✓ Se selecciona 'VPN access' .



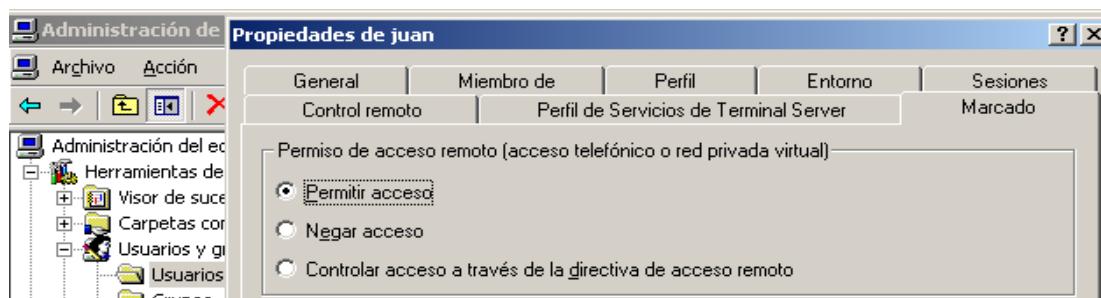
- ✓ Y se activa el servicio.



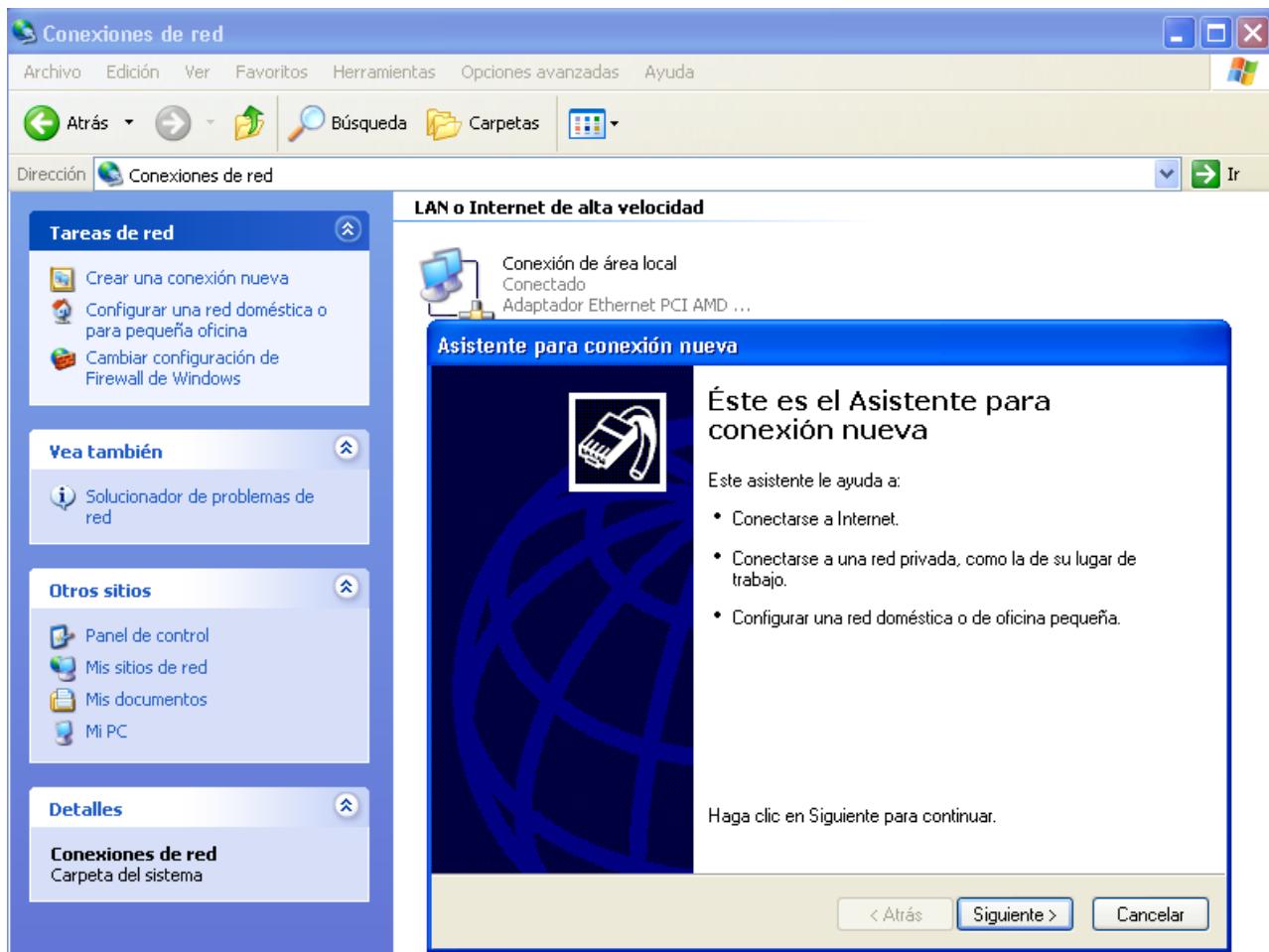
- ✓ Creo un usuario (que sera el mismo con el que acceda luego desde XP).



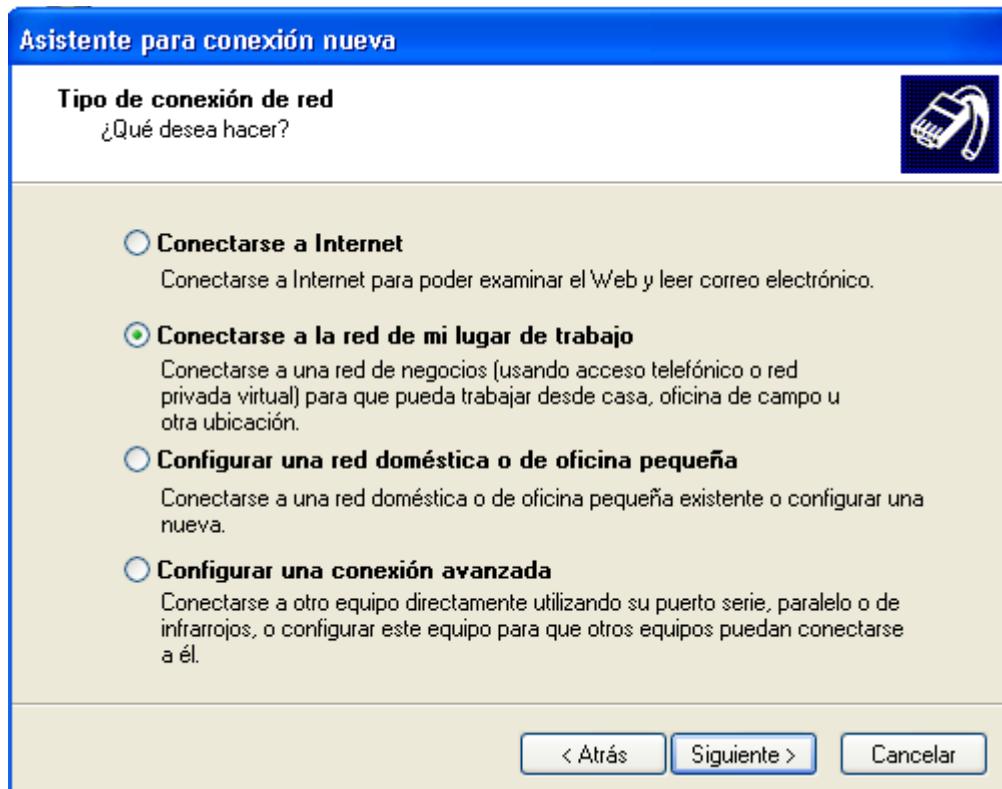
- ✓ Y en 'Propiedades' del usuario creado, le autorizo la conexión remota.



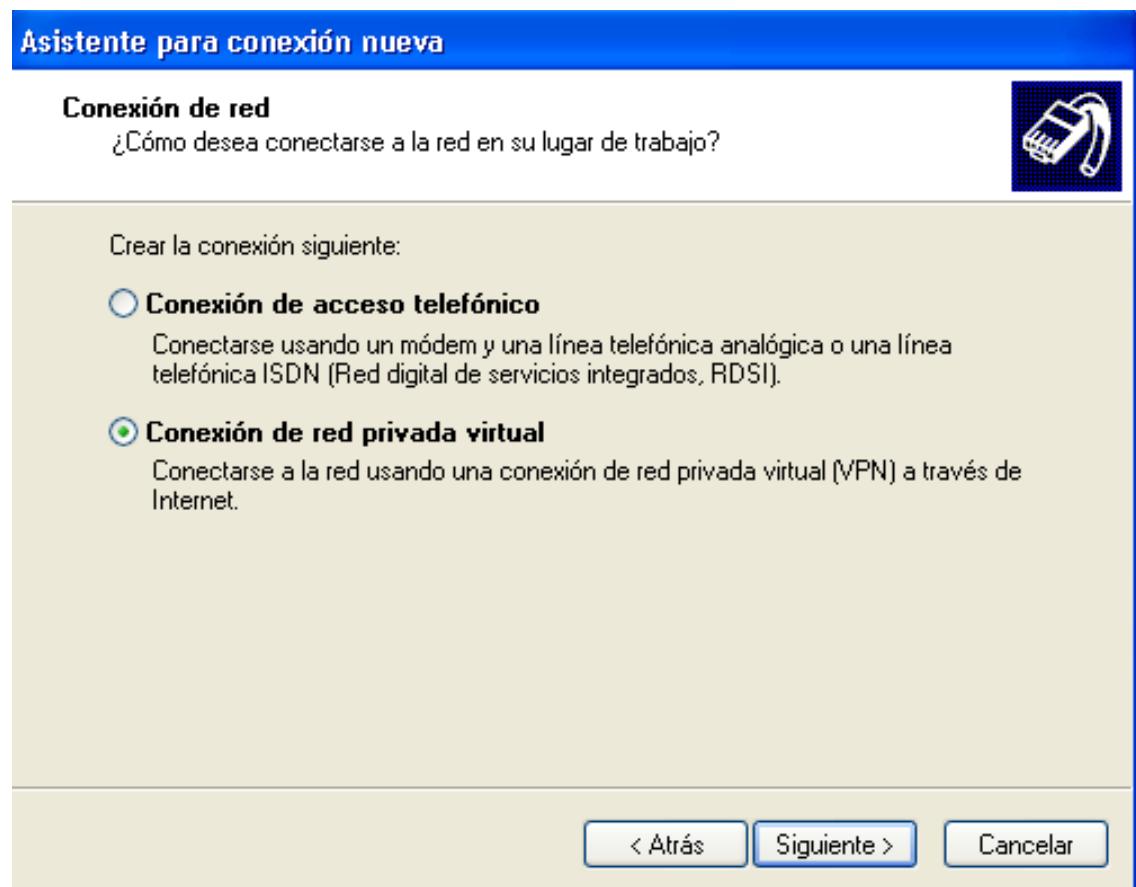
- ✓ En el ordenador con XP entro como el usuario que quiera, inicio el asistente de Conexiones de Red nuevas.



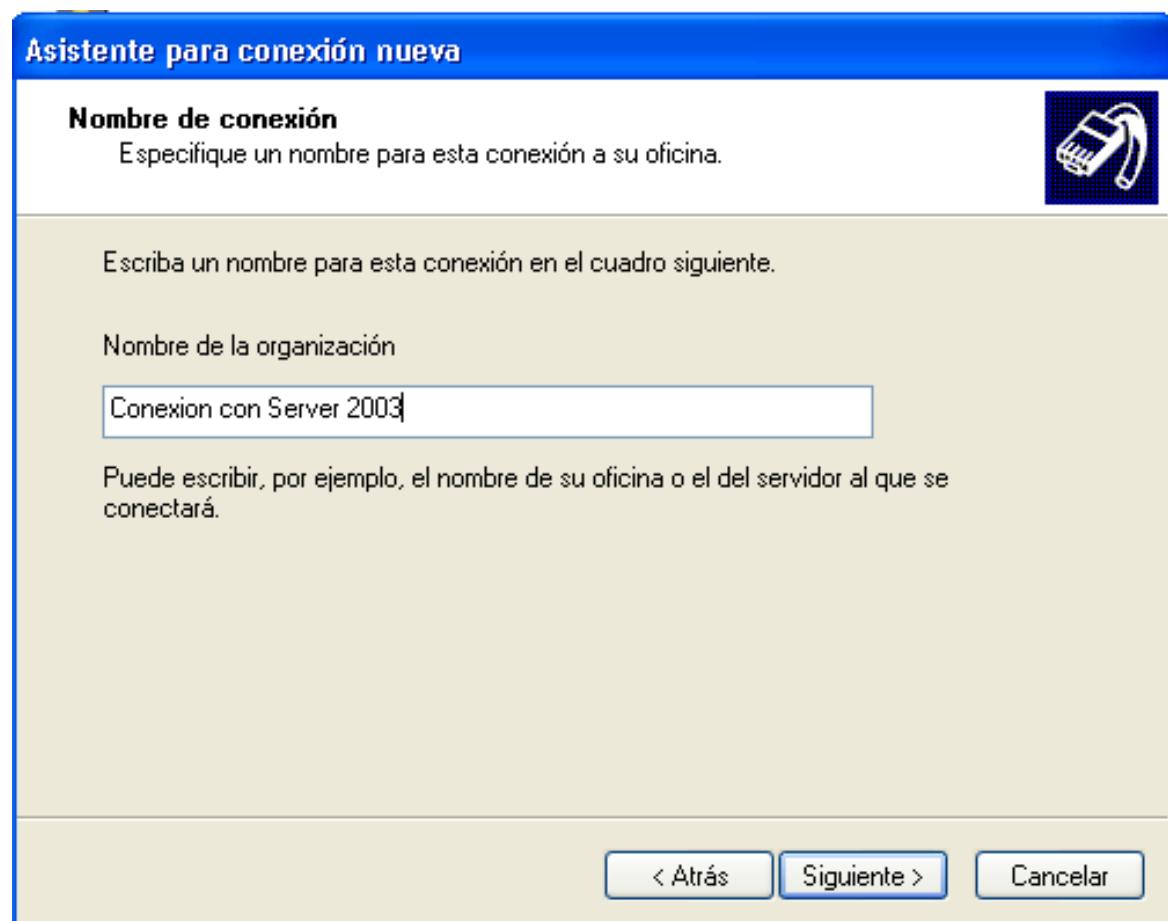
- ✓ Escojo 'Conectarse a la red de mi lugar de trabajo' .



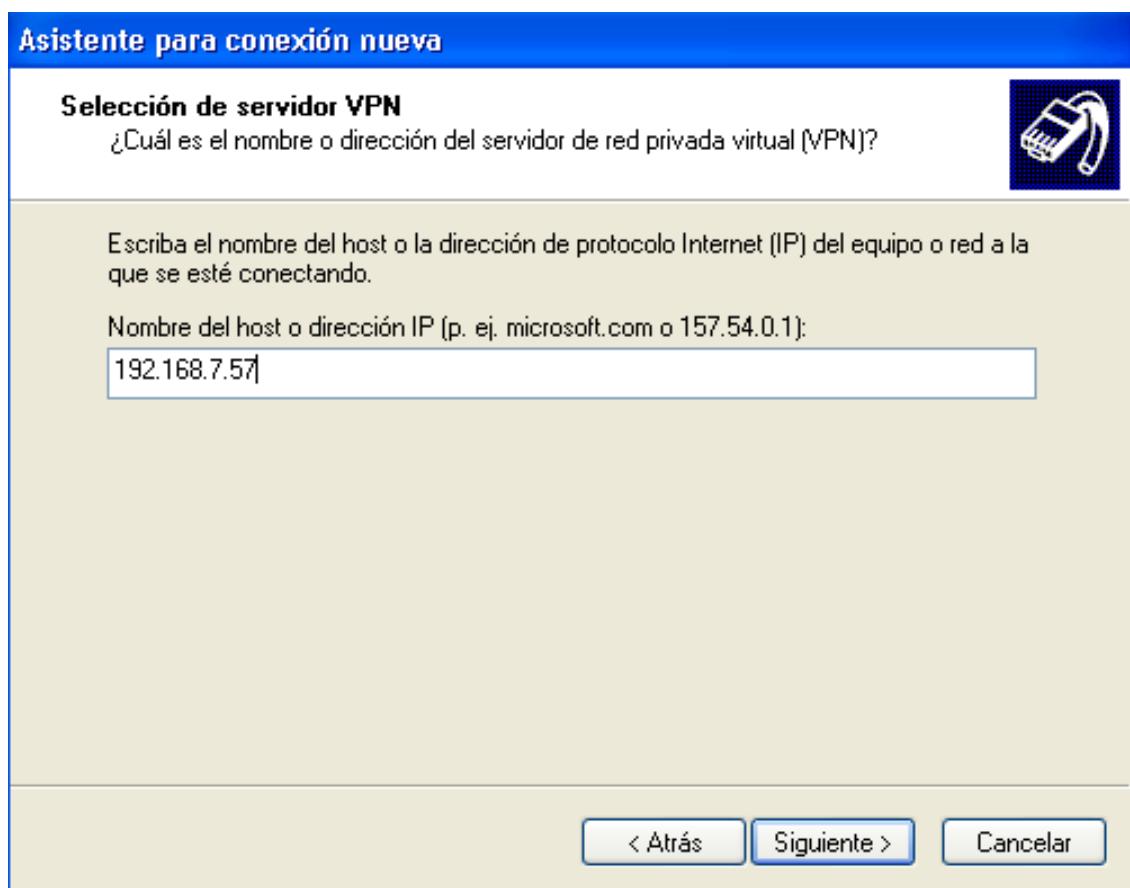
- ✓ Escojo conexión de red privada virtual.



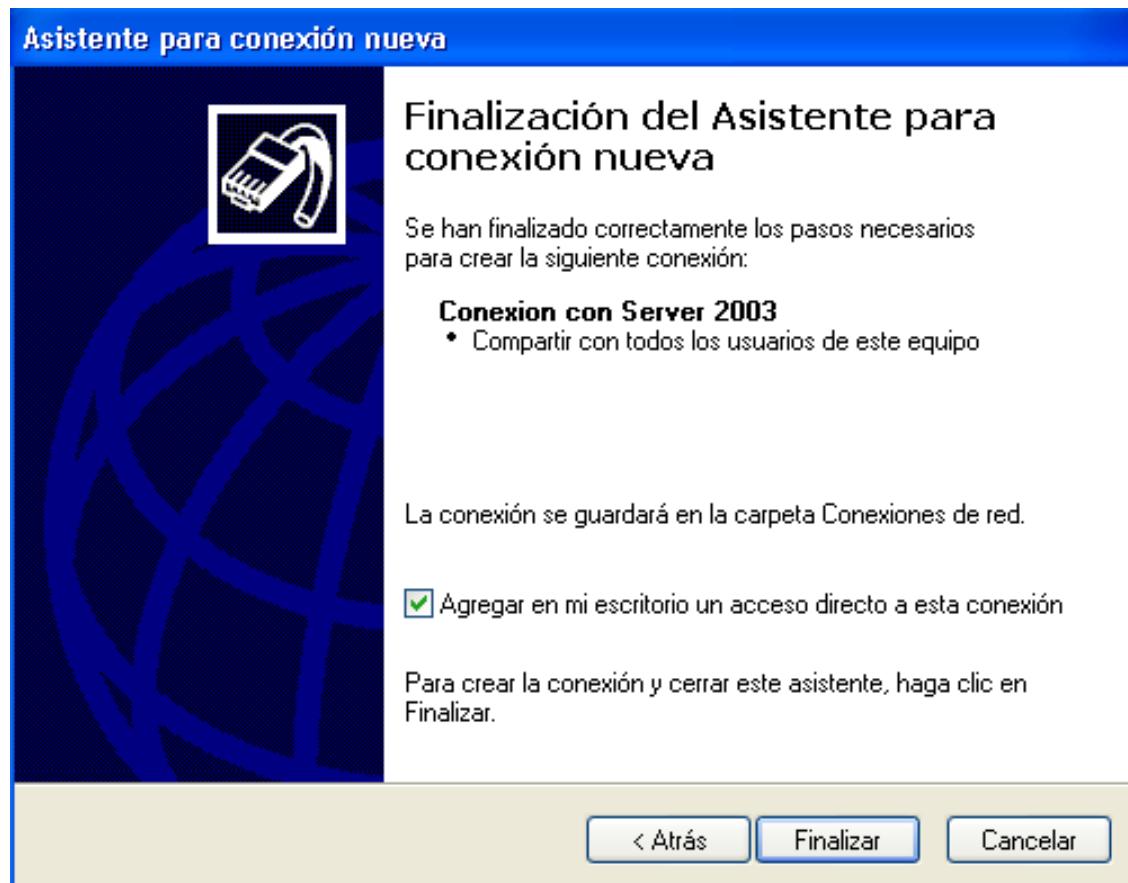
- ✓ Le doy un nombre a la conexión.



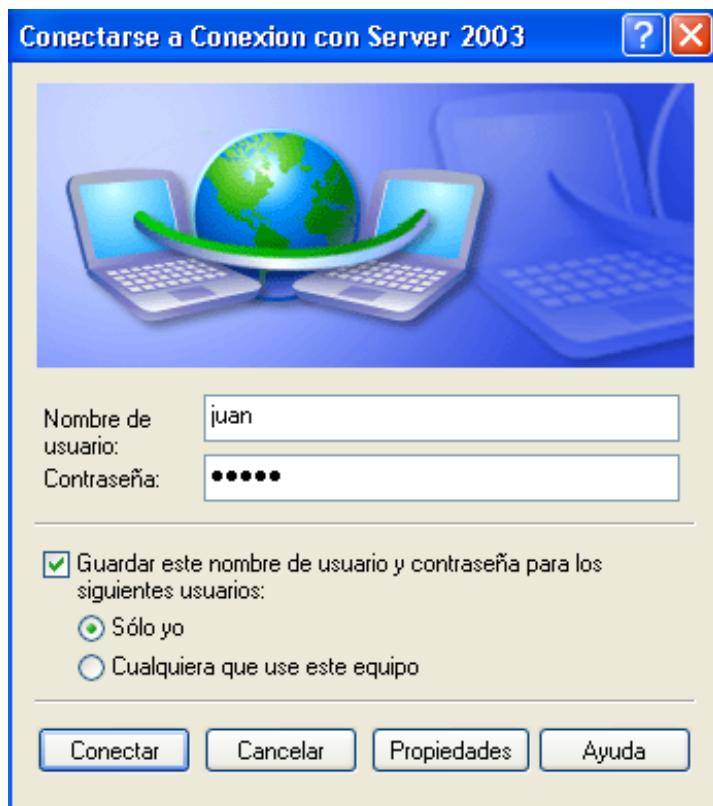
- ✓ Asigno la IP del servidor al que me voy a conectar (Server 2003).



- ✓ Agrego un acceso directo al escritorio si quiero.



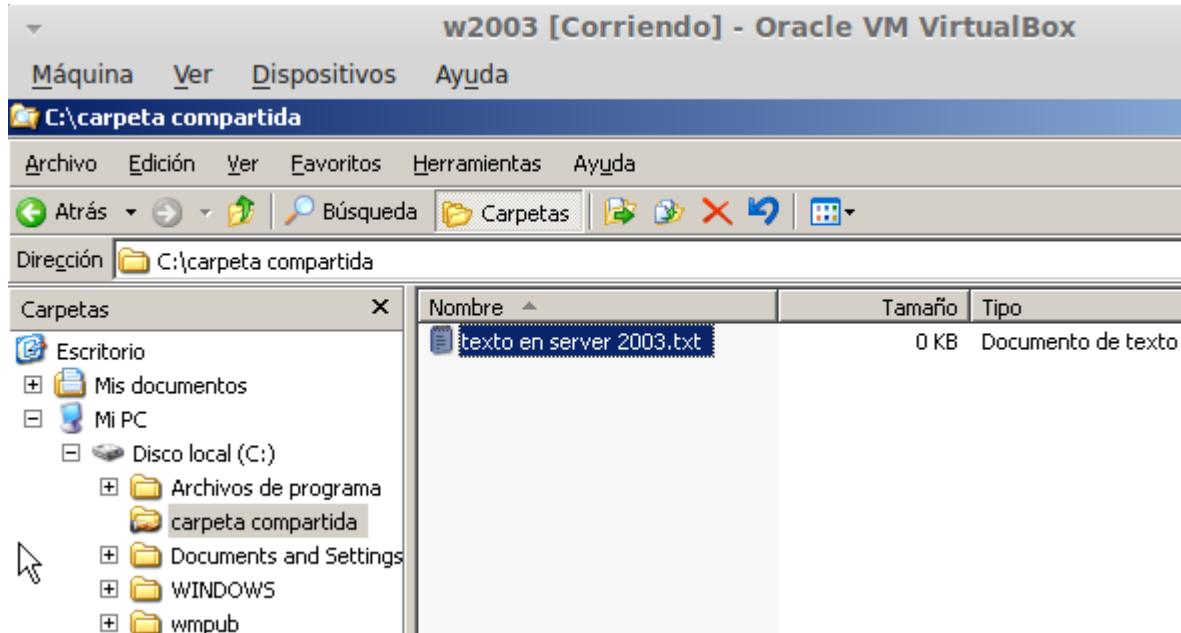
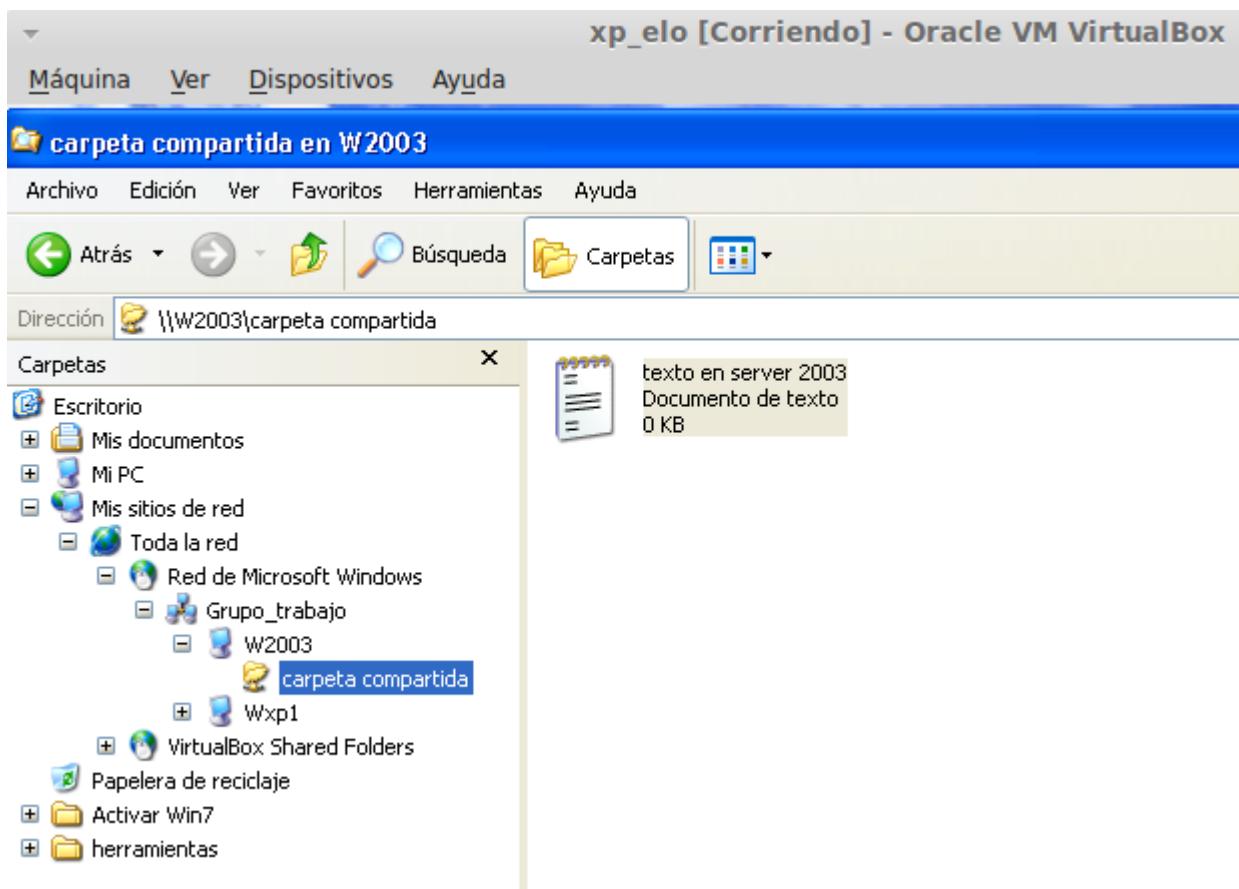
- ✓ Entró con el usuario que he creado en el server 2003 y al que le he dado autorización de conexión.



- ✓ Y ya tengo creada la conexión virtual segura VPN.



- ✓ Ahora podría acceder por ejemplo a una carpeta compartida del Server 2003 de forma segura a través de la conexión VPN.



Test de conocimientos (Cap. 7 pag. 183)

1

Iptables:

- a) Es un conjunto de reglas de routers.
- b) Es equivalente a las ACL en Windows.
- c) Emplea características de un *firewall* de Zone Alarm.
- d) Se trata de un cortafuegos basado en reglas de filtrado.

2

En un servidor con cortafuegos iptables que realiza funciones de enrutado únicamente, la opción habitual es:

- a) INPUT.
- b) FORWARD.
- c) OUTPUT.
- d) Ninguna de las anteriores.

3

El archivo donde se almacenan los logs de iptables es:

- a) /var/log/iptables.log.
- b) /etc/init.d/rsyslog.
- c) /var/log/squid/access.log.
- d) /var/log/squid/cache.log.

4

En Squid url_regex es una opción:

- a) De control de acceso a determinadas web listadas en un archivo.
- b) De control de acceso a determinadas palabras reservadas listadas en un archivo.
- c) Para registrar sucesos de intento de acceso al proxy.
- d) De control de acceso a los buscadores webs que incluyan palabras reservadas.

5

Los cortafuegos son elementos:

- a) Hardware.
- b) Software.
- c) Pueden ser software y hardware.
- d) Ninguna de las anteriores.

6

Squid como proxy transparente recibe peticiones normalmente en el puerto:

- a) 80.
- b) 53.
- c) 8080.
- d) 3128.

7

Un cliente que utiliza Squid como proxy transparente, envía peticiones normalmente al puerto:

- a) 80.
- b) 53.
- c) 8080.
- d) 3128.

8

La integración de un servidor proxy y cortafuegos se denomina:

- a) Screening router.
- b) Dual Homed-Host.
- c) Screened Host.
- d) Screened-subnet.

1

¿Qué sistema RAID controla paridad?

- a) RAID 0.
- b) RAID 1.
- c) RAID 5.
- d) RAID 10.

2

La configuración de red (bajo VMWare) que permite crear una red de máquinas virtuales privada, distinta e independiente de la red a la que pertenece la máquina física es:

- a) Host-only.
- b) Bridge.
- c) NAT.
- d) Ninguna de las anteriores.

3

La administración de los servicios de virtualización (bajo VMWare) se suele realizar mediante:

- a) Aplicación de escritorio.
- b) Correo electrónico.
- c) FTP.
- d) Servicio web.

4

El balanceo de carga no permite realizar:

- a) De 4 conexiones a Internet tener 2 conexiones de igual velocidad.
- b) De 1 conexión a Internet tener 2 conexiones de igual velocidad.
- c) De 2 conexiones a Internet tener 1 sola conexión de velocidades sumadas.
- d) Ninguna de las anteriores.

5

A los sistemas de máximo nivel de alta disponibilidad se les tolera una inactividad anual de:

- a) 5 minutos.
- b) 10 minutos.
- c) 15 minutos.
- d) no se les permite ningún minuto.

6

Bajo sistemas Windows podemos realizar balanceo de carga con la aplicación:

- a) VirtualBox.
- b) Kerio Winroute.
- c) Virtual PC.
- d) WinGate.

7

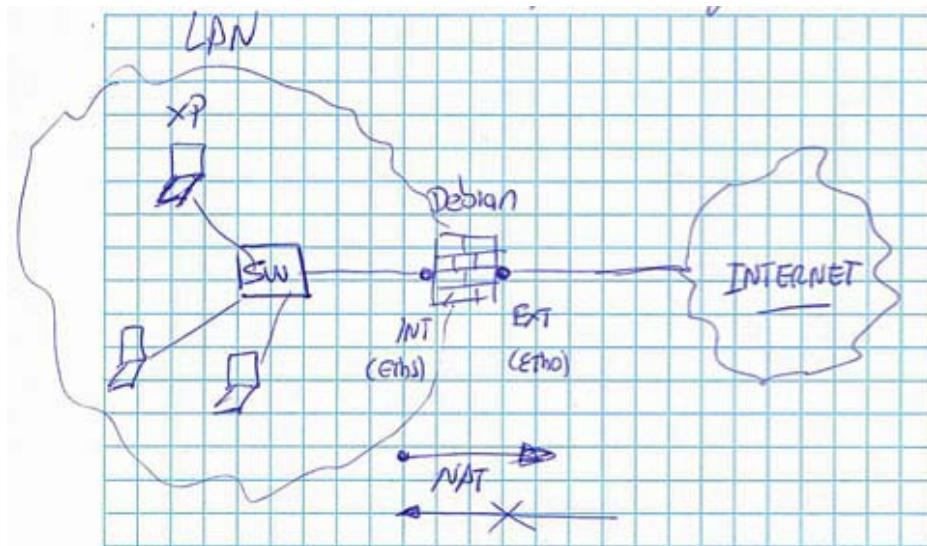
Bajo sistemas GNU/Linux qué aplicación nos permite monitorizar la actividad de las distintas tarjetas de red:

- a) Iptraf.
- b) Iproute.
- c) Iptables.
- d) Show_ip_route.

Configuración de cortafuegos, IPTables - Practica

(T7 – Práctica 7.1, pág. 163)

Para la practica se utiliza una maquina virtual con Linux (Debian) que hará de cortafuegos y una maquina virtual con XP, que hará de cliente en la red LAN.



Se preparan dos script para el equipo Debian, uno que permitirá todo tipo de comunicaciones (Todo abierto) y otro que no permitirá ninguna comunicación (Todo cerrado).

Script todo abierto (todoabierto.sh):

```
#!/bin/bash

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Permito por defecto el acceso
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Script todo cerrado (todocerrado.sh):

```
#!/bin/bash

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Se comprueba con XP cada una de las situaciones.

Script que permite las comunicaciones desde el XP y hacia el XP (script1.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
iptables -t filter -A FORWARD -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $STARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $STARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Script que permite enviar datos hacia internet pero no la entrada de los datos de vuelta (script2.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $STARJETA_INT conseguimos que solo funcione en un sentido
iptables -t filter -A FORWARD -i $STARJETA_INT -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $STARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $STARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Script que permite enviar peticiones hacia internet y que entren la repuestas a estas peticiones, pero no las conexiones desde internet que no hayan tenido un origen en el XP de la red LAN (script3.sh):

```
#!/bin/bash
TARJETA_INT=eth1
TARJETA_EXT=eth0
#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F
#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $STARJETA_INT conseguimos que funcione solo en el sentido de salida
iptables -t filter -A FORWARD -i $STARJETA_INT -j ACCEPT
#instruccion que permite que solo entren respuestas a lo que ha salido permitido por la instruccion anterior
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $STARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $STARJETA_EXT -j MASQUERADE
#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Se modifica el Script para permitir solo comunicaciones con protocolo TCP y al puerto 80 (script4.sh):

```
#!/bin/bash
TARJETA_INT=eth1
TARJETA_EXT=eth0
#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F
#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $STARJETA_INT conseguimos que funcione solo en el sentido de salida
#con -p TCP --dport 80 solo permite protocolo TCP y a un puerto 80
iptables -t filter -A FORWARD -i $STARJETA_INT -p TCP --dport 80 -j ACCEPT
#instruccion que permite que solo entren respuestas a lo que ha salido permitido por la instruccion anterior
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $STARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $STARJETA_EXT -j MASQUERADE
#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Esta configuración no permite la resolución de nombres, por lo que en el navegador tenemos que poner la IP de la web ya que si se pone el nombre no lo resolverá.

Se modifica el Script para permitir ademas de las comunicaciones con protocolo TCP y al puerto 80, la resolución de nombres DNS con el puerto 53 (script5.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $TARJETA_INT conseguimos que funcione solo en el sentido de salida
#con -p TCP --dport 80 solo permite protocolo TCP y a un puerto 80
#iptables -t filter -A FORWARD -i $TARJETA_INT -p TCP --dport 80 -j ACCEPT

#otra linea para permitir protocolo de resolucion de nombres DNS y puerto 53
iptables -t filter -A FORWARD -i $TARJETA_INT -p UDP --dport 53 -j ACCEPT

#instruccion que permite que solo entren respuestas a las salidas permitidas por la instruccion anterior
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $TARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $TARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Con esta configuración ya podemos poner tanto la IP como el nombre de la web que el navegador web de la maquina virtual con XP, que se comunicara sin problemas, siempre que sea a una pagina web (HTTP) y al puerto 80.

Se modifica el Script para permitir ademas de todo lo anterior, las peticiones de ping realizadas desde la maquina virtual con XP hacia internet, por ejemplo a 8.8.8.8 (script6.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $TARJETA_INT conseguimos que funcione solo en el sentido de salida
#con -p TCP --dport 80 solo permite protocolo TCP y a un puerto 80
iptables -t filter -A FORWARD -i $TARJETA_INT -p TCP --dport 80 -j ACCEPT

#otra linea para permitir protocolo de resolucion de nombres DNS y puerto 53
iptables -t filter -A FORWARD -i $TARJETA_INT -p UDP --dport 53 -j ACCEPT

#otra linea para permitir que se pueda hacer ping
iptables -t filter -A FORWARD -i $TARJETA_INT -p ICMP --icmp-type 8 -j ACCEPT

#instruccion que permite que solo entren respuestas a las salidas permitidas por la instruccion anterior
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $TARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $TARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Si probamos este script, podemos hacer ping a la IP 8.8.8.8, pero sin embargo si hacemos ping a la dirección IP del eth1 del cortafuegos desde el XP no responderá, así que afinamos un poco mas la configuración del script para que se le pueda hacer ping al cortafuegos y este también pueda hacer ping.

Se modifica el Script para permitir ademas de todo lo anterior, las peticiones de ping realizadas y recibidas por el cortafuegos (script7.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $TARJETA_INT conseguimos que funcione solo en el sentido de salida
#con -p TCP --dport 80 solo permite protocolo TCP y a un puerto 80
iptables -t filter -A FORWARD -i $TARJETA_INT -p TCP --dport 80 -j ACCEPT

#otra linea para permitir protocolo de resolucion de nombres DNS y puerto 53
iptables -t filter -A FORWARD -i $TARJETA_INT -p UDP --dport 53 -j ACCEPT

#otra linea para permitir que se pueda hacer ping
iptables -t filter -A FORWARD -i $TARJETA_INT -p ICMP --icmp-type 8 -j ACCEPT

#permiso ping al cortafuegos
iptables -t filter -A INPUT -p ICMP --icmp-type 8 -j ACCEPT

#permiso ping desde el cortafuegos
iptables -t filter -A OUTPUT -p ICMP --icmp-type 8 -j ACCEPT

#instruccion que permite que solo entren respuestas a lo que ha salido
#permitido por las instrucciones anteriores, instruccion generica
#FORWARD para FORWARD, OUTPUT para las INPUT y INPUT para las OUTPUT
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $TARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $TARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Añado instrucción que permite el servicio Web desde el cortafuegos accesible desde internet (script8.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $TARJETA_INT conseguimos que funcione solo en el sentido de salida
#con -p TCP --dport 80 solo permite protocolo TCP y a un puerto 80
iptables -t filter -A FORWARD -i $TARJETA_INT -p TCP --dport 80 -j ACCEPT

#otra linea para permitir protocolo de resolucion de nombres DNS y puerto 53
iptables -t filter -A FORWARD -i $TARJETA_INT -p UDP --dport 53 -j ACCEPT

#otra linea para permitir que se pueda hacer ping
iptables -t filter -A FORWARD -i $TARJETA_INT -p ICMP --icmp-type 8 -j ACCEPT

#permiso ping al cortafuegos
iptables -t filter -A INPUT -p ICMP --icmp-type 8 -j ACCEPT

#permiso ping desde el cortafuegos
iptables -t filter -A OUTPUT -p ICMP --icmp-type 8 -j ACCEPT

#permiso acceso a un servidor web en el propio cortafuegos
iptables -t filter -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p TCP --dport 443 -j ACCEPT

#instruccion que solo se permite acceso desde la red LAN interna al servidor WEB
#iptables -t filter -A INPUT -i $TARJET_INT -p TCP --dport 80 -j ACCEPT

#instrucciones genericas, dejan entrar respuestas a salidas permitidas por instrucciones anteriores
#FORWARD para FORWARD, OUTPUT para las INPUT y INPUT para las OUTPUT)
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $TARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $TARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Se añade una linea comentada para que solo permita el acceso al servicio WEB desde la Red interna (**iptables -t filter -A INPUT -i \$TARJET_INT -p TCP --dport 80 -j ACCEPT**), para hacer uso de esta regla se des-comenta y se comentan las dos reglas anteriores que permiten el acceso desde internet a los puertos 80 y 443.

Y por ultimo añado instrucción que permite accesos al servidor SSH del cortafuegos desde un ordenador en concreto, (script9.sh):

```
#!/bin/bash

TARJETA_INT=eth1
TARJETA_EXT=eth0

#A continuacion borro todas las reglas de filtrado y nat
iptables -t filter -F
iptables -t nat -F

#Deniego por defecto el acceso
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#Para que acepte paquetes enviados desde un equipo externo a un equipo interno de la red y viceversa
#con -i $TARJETA_INT conseguimos que funcione solo en el sentido de salida
#con -p TCP --dport 80 solo permite protocolo TCP y a un puerto 80
#iptables -t filter -A FORWARD -i $TARJETA_INT -p TCP --dport 80 -j ACCEPT

#otra linea para permitir protocolo de resolucion de nombres DNS y puerto 53
iptables -t filter -A FORWARD -i $TARJETA_INT -p UDP --dport 53 -j ACCEPT

#otra linea para permitir que se pueda hacer ping
iptables -t filter -A FORWARD -i $TARJETA_INT -p ICMP --icmp-type 8 -j ACCEPT

#permiso ping al cortafuegos
iptables -t filter -A INPUT -p ICMP --icmp-type 8 -j ACCEPT

#permiso ping desde el cortafuegos
iptables -t filter -A OUTPUT -p ICMP --icmp-type 8 -j ACCEPT

#permiso acceso a un servidor web en el propio cortafuegos
iptables -t filter -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p TCP --dport 443 -j ACCEPT

#instruccion que solo se permite acceso desde la red LAN interna al servidor WEB
#iptables -t filter -A INPUT -i $TARJ_INT -p TCP --dport 80 -j ACCEPT

#permiso accesos al servidor SSH del cortafuegos solo desde un PC determinado
iptables -t filter -A INPUT -s 192.168.7.2 -i $STARJ_INT -p TCP --dport 22 -j ACCEPT

#instrucciones genericas, dejan entrar respuestas a salidas permitidas por instrucciones anteriores
#FORWARD para FORWARD, OUTPUT para las INPUT y INPUT para las OUTPUT)
iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#En la cadena POSTROUTING de la tabla nat hacemos "MASQUERADE"
#Hacemos NAT a los paquetes salientes, de forma que su IP de origen
#es sustituida por la IP publica del FW para la red del interfaz eth0
#la interfaz eth0 (variable $TARJETA_EXT) es la que esta conectada a internet
iptables -t nat -A POSTROUTING -o $TARJETA_EXT -j MASQUERADE

#Para que Linux reenvie paquetes
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Se puede añadir una regla para que cree un LOG y seria:

iptables -t filter -A INPUT -i \$STARJ_EXT -p TCP -dport 22 -j LOG --log-prefix

Con el XP probamos cada cambio en cada uno de los script y las consecuencias que tiene en las comunicaciones.

Como se ve cada script es igual al anterior y sobre el se van añadiendo o modificando reglas

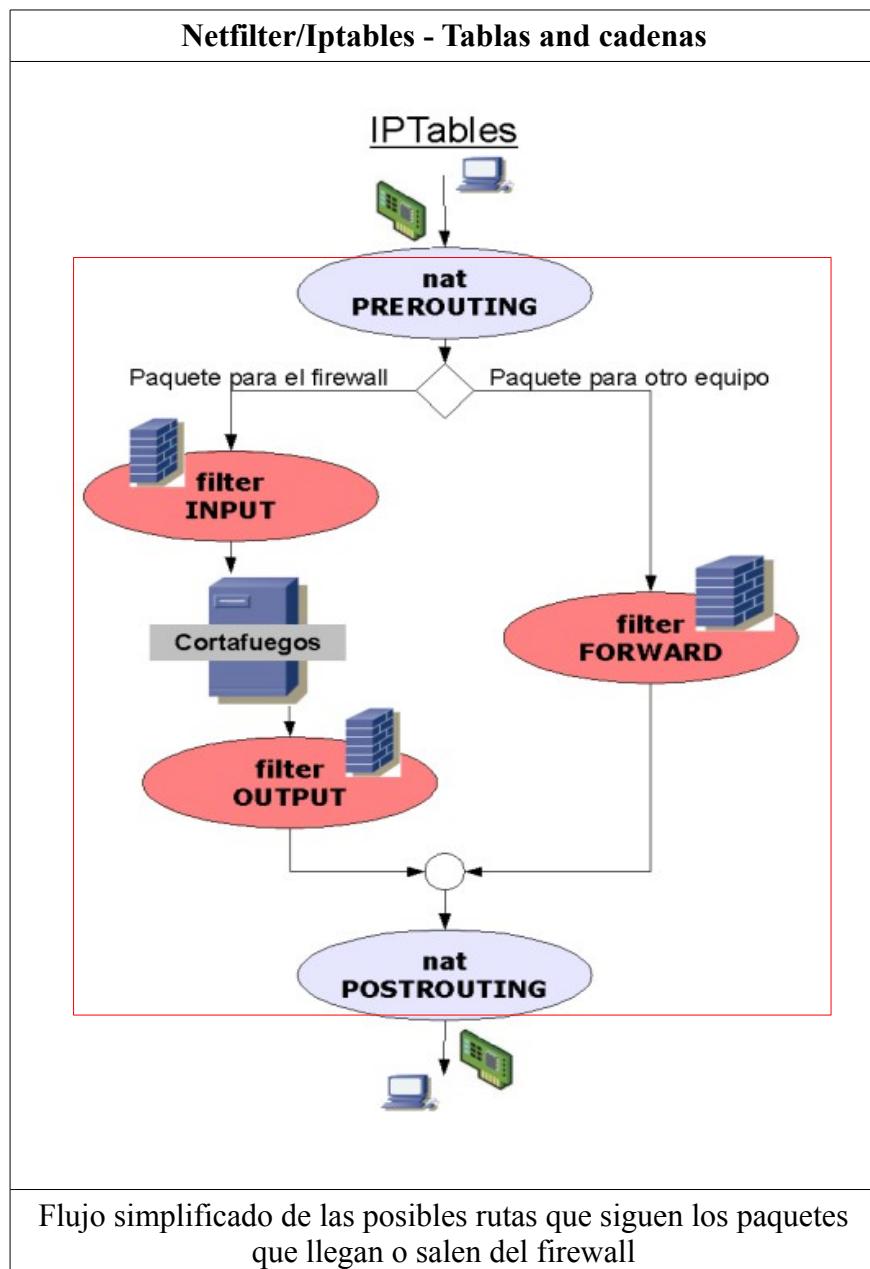
Aclaraciones:

INPUT es lo que le llega al Firewall sea de la tarjeta interna o externa (eth0 o eth1)

OUTPUT es lo que sale desde el Firewall por cualquiera de las tarjetas (eth0 y eth1)

FORWARD es lo que no es para el Firewall y lo deja pasar o se filtra según lo que se ponga en el script

En la siguiente imagen (Extraída de los apuntes de Gerardo), se ve la situación de INPUT, OUTPUT y FORWARD, se ha dibujado un recuadro en rojo para delimitar lo que esta dentro del firewall.



Resumen opciones instrucciones de la orden iptables:

- ✓ una orden de iptables tiene la siguiente estructura:

- iptables -t filter -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 80 -j ACCEPT

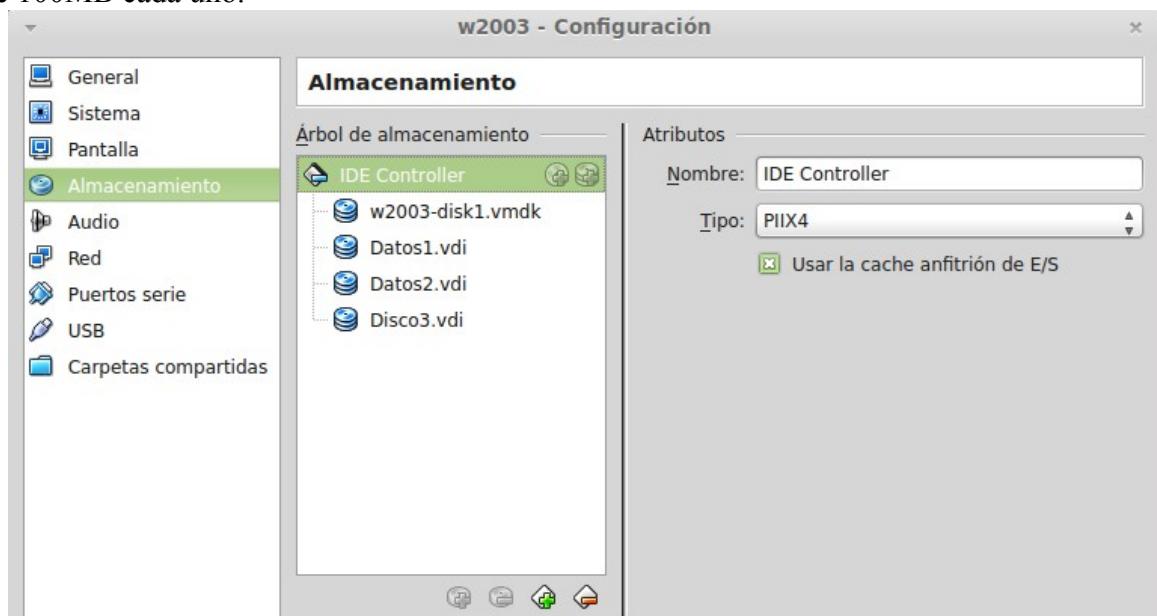
tabla	Tipo de operación	Cadena	Regla con parámetros	Acción
-t filter	-A	FORWARD	-i eth0 -s 192.168.2.100 -p tcp --dport 80	-j ACCEPT

- ✓ Las opciones mas usadas son: iptables -A
 - -A: añadir cadena de regla a una determinada tabla
 - -F: elimina y reinicia a los valores por defecto todas las cadenas de una determinada tabla.
 - -L: listar las cadenas de reglas de una determinada tabla (por defecto filter)
 - -P: añadir regla por defecto, en caso de que no se cumpla ninguna de las cadenas de reglas definidas.
- ✓ Hay tres tipos de tablas incorporadas:
 - Filter table (Tabla de filtros), es la responsable del filtrado y contiene las siguientes cadenas:
 - ✓ INPUT – Todos los paquetes destinados a este sistema atraviesan esta cadena.
 - ✓ OUTPUT – Todos los paquetes creados por este sistema atraviesan esta cadena.
 - ✓ FORWARD – Todos los paquetes que pasan por este sistema para ser encaminados a su destino recorren esta cadena.
 - Nat table (tabla de traducción de direcciones de red), es la responsable de configurar las reglas de traducción de direcciones o de puertos de los paquetes, contiene las siguientes cadenas:
 - ✓ PREROUTING – Los paquetes entrantes pasan a través de esta cadena antes de que se consulte la tabla de enrutado.
 - ✓ POSTROUTING – Los paquetes salientes pasan por esta cadena después de haberse tomado la decisión de enrutado.
 - ✓ OUTPUT
 - Mangle table (Tabla de destrozo), es la responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad de servicio.
- ✓ Los modificadores y parámetros mas usuales son:
 - -t 'tabla' Hace que el comando se aplique a la tabla especificada (nat, mangle, filter)
 - -i interfaz de entrada (eth0, eth1, eth2).
 - -o interfaz de salida (eth0, eth1, eth2).
 - -s dirección de origen, puede ser la IP de un equipo
 - --sport Puerto origen (se indica el nombre o numero de puerto del protocolo, http o 80)
 - --dport Puerto destino (se indica el nombre o numero de puerto del protocolo, http o 80)
 - -p El protocolo del paquete a comprobar, tcp, udp, icmp o all, por defecto es all.
 - -j Especifica el objetivo de la cadena de reglas, osea una acción.
 - -m define que se aplica la regla si hay una coincidencia específica.
 - --state define una lista separada por comas de distintos tipos de estados de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).
 - --line-numbers Al listar reglas, agrega el numero que ocupa cada regla dentro de la cadena.
- ✓ Las acciones, que estarán siempre al final de cada regla (después de -j) y que determina que se hace con el paquete afectado por la regla.
 - ACCEPT Paquete aceptado
 - REJECT Paquete rechazado, se envía notificación por medio del protocolo ICMP.
 - DROP Paquete rechazado, sin notificación.
 - MASQUERADE Enmascaramiento de la dirección IP origen de forma dinámica, solo valida en la tabla NAT de la cadena postrouting.
 - DNAT Enmascaramiento de la dirección destino, muy conveniente para re-enrutado de paquetes.
 - SNAT Enmascaramiento de la dirección IP origen de forma similar a MASQUERADE pero con IP fija.
- ✓ Seguimiento de conexiones.
 - NEW Intentando crear una conexión nueva.
 - ESTABLISHED Parte de una conexión ya existente.
 - RELATED Relacionada, aunque no realmente parte de una conexión existente.
 - INVALID No es parte de una conexión existente e incapaz de crear una nueva conexión.
- ✓ Se pueden configurar registros LOG en iptables con la acción -j log en las reglas, se puede añadir un prefijo a cada entrada en el log para identificar los paquetes de forma mas sencilla con --log-prefix.
 - **iptables -t filter -A INPUT -i \$STARJ_EXT -p TCP --dport 22 -j LOG --log-prefix**

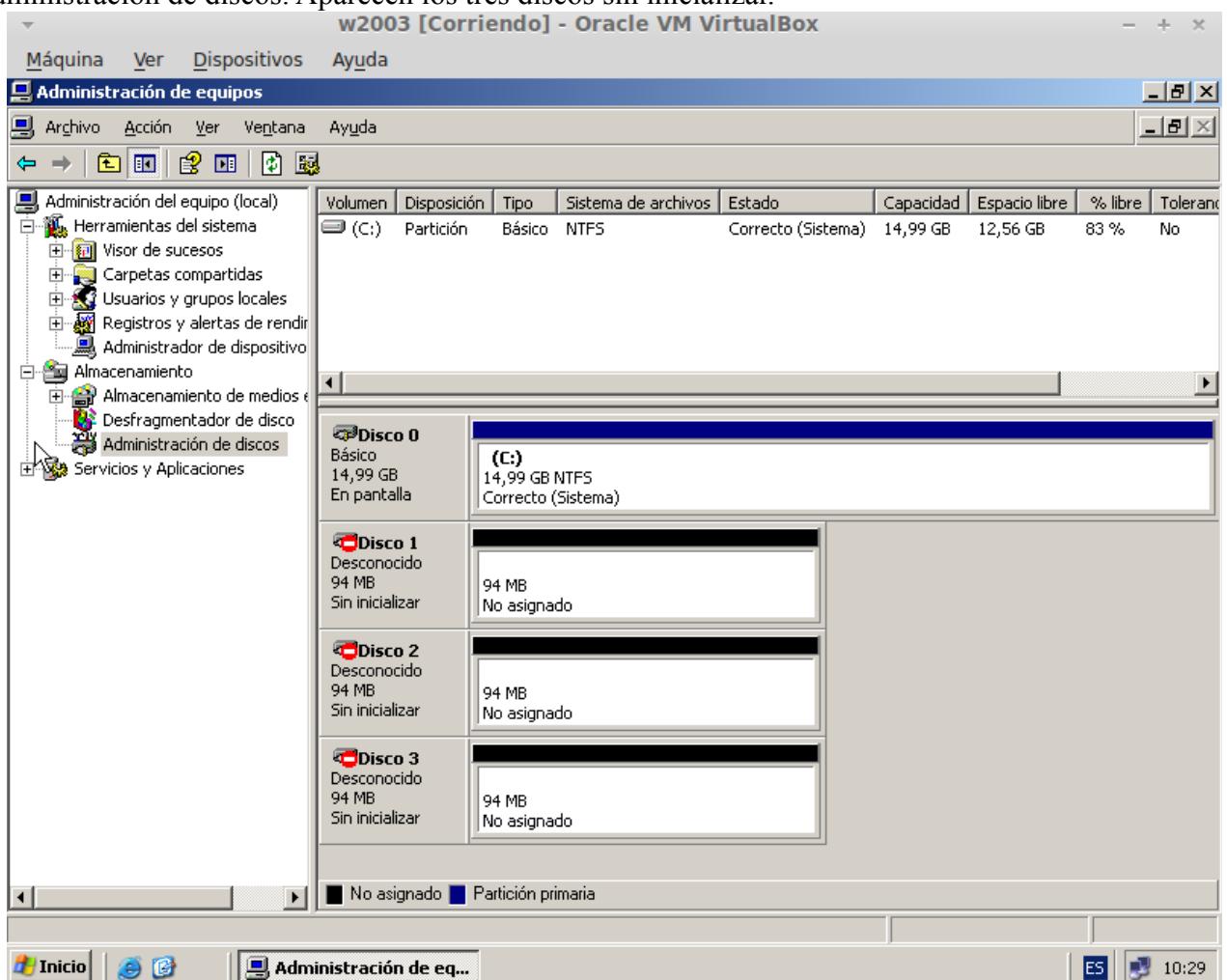
Practica RAID

(T8 – Práctica 8.1, pág. 189)

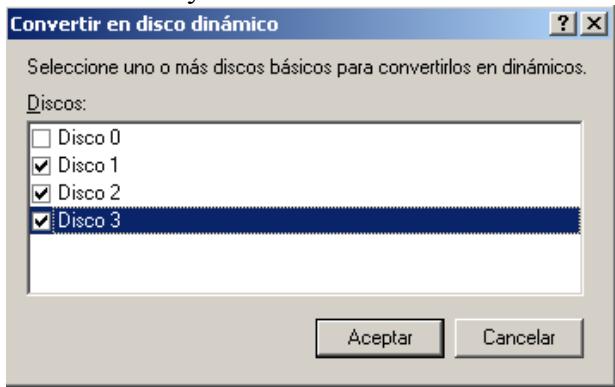
En una maquina virtual con Windows 2003 se le añaden 3 discos virtuales mas, que se llamaran Datos 1, 2 y 3 de 100MB cada uno.



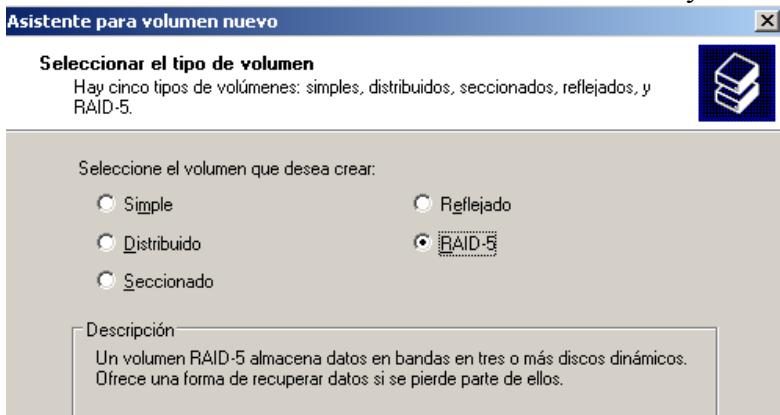
Se arranca Windows 2003 y en Herramientas Administrativas – Administrador de equipos
-Administración de discos. Aparecen los tres discos sin inicializar.



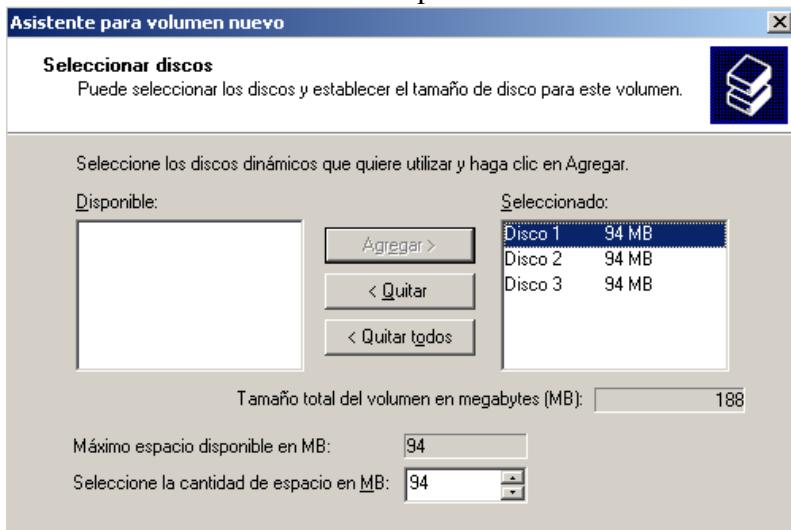
Se inicializan y Se convierten en dinámicos



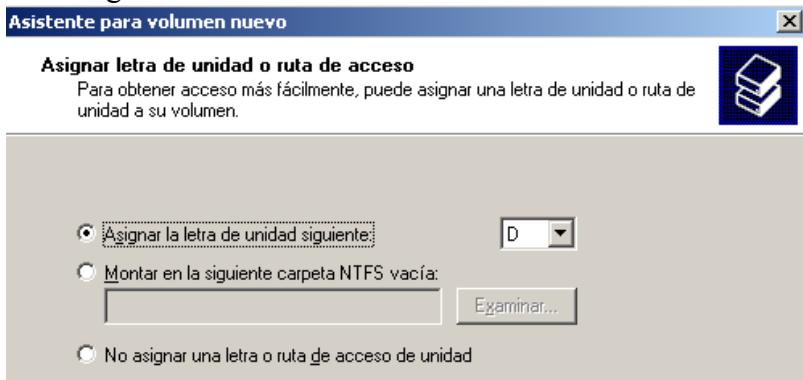
En cada uno de ellos seleccionamos Nuevo volumen y como opción RAID-5



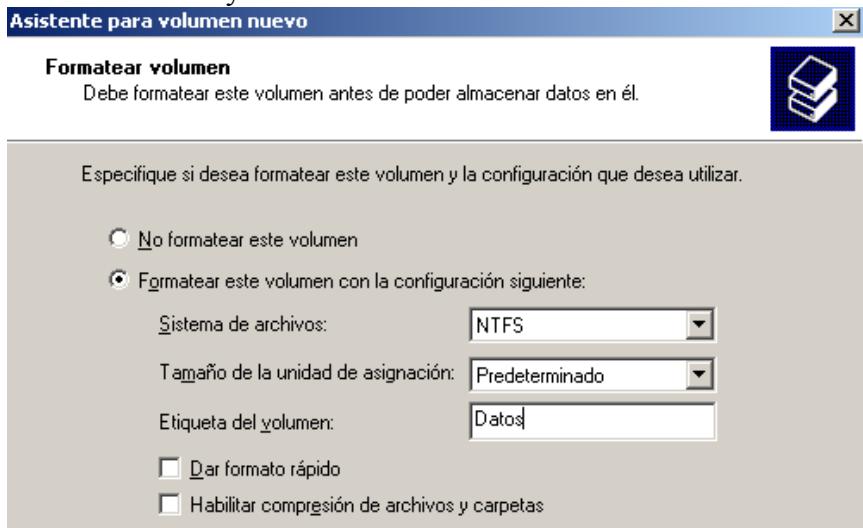
Se añaden el resto de los discos para formar el RAID-5



Y se asigna la letra de unidad



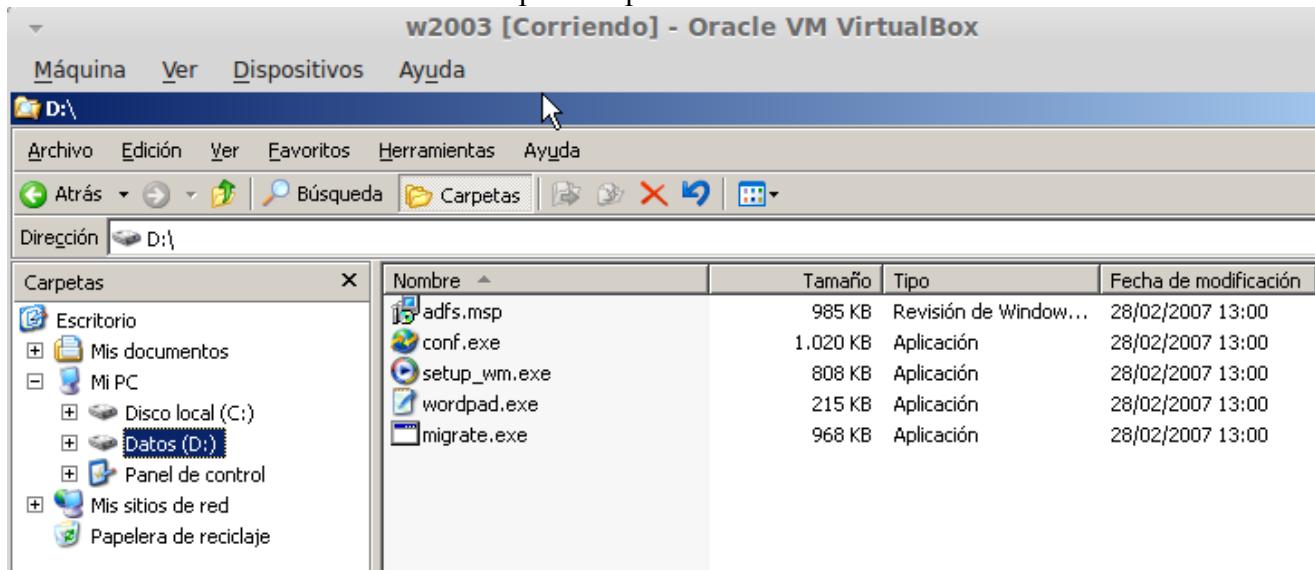
Se le da formato y nombre



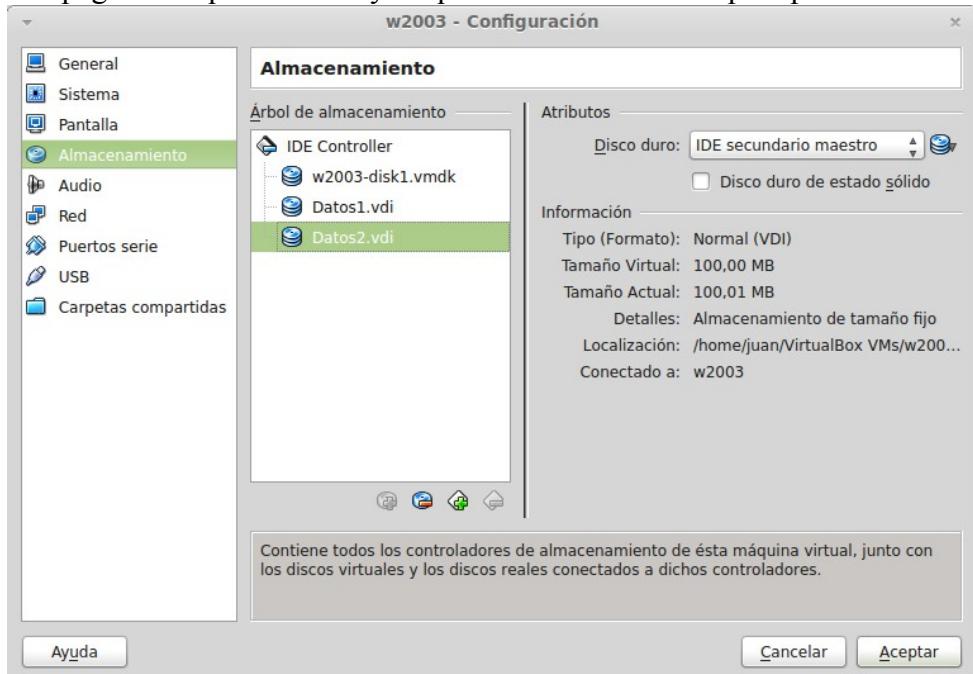
Aparece un resumen de la acciones y tras aceptar crea el sistema RAID-5



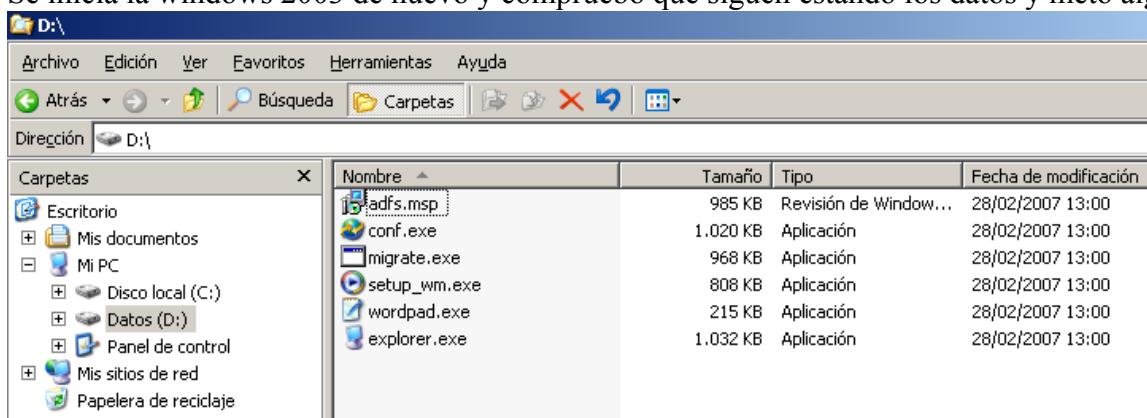
Se mete información en el disco creado para las pruebas.



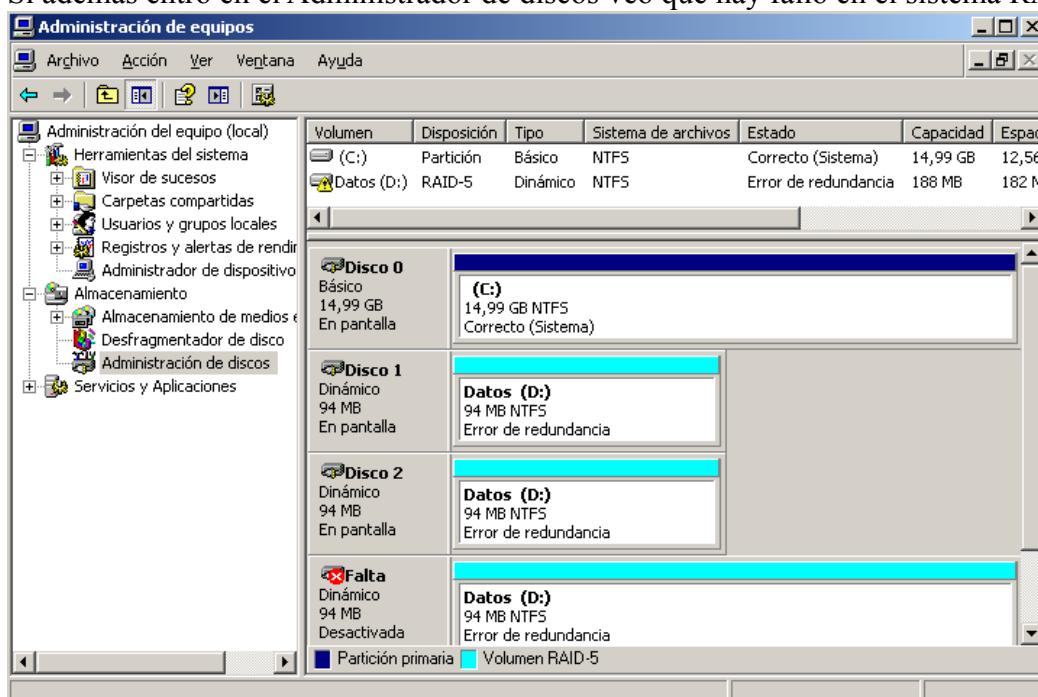
Se apaga la maquina virtual y se quita uno de los discos para provocar un fallo de un volumen.



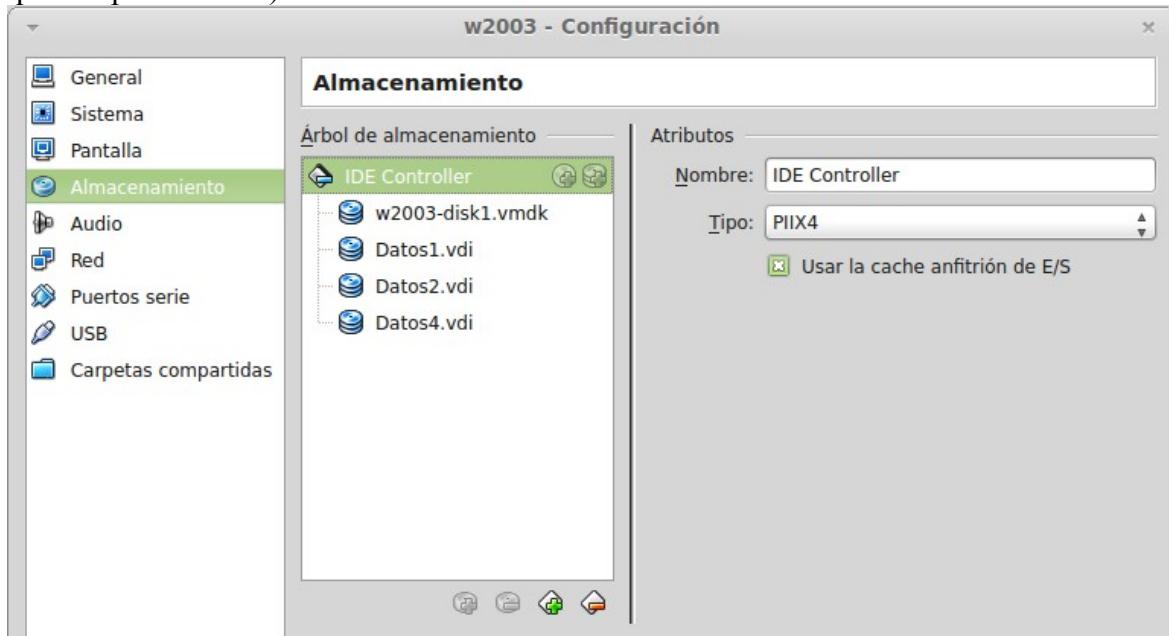
Se inicia la windows 2003 de nuevo y compruebo que siguen estando los datos y meto algún archivo mas.



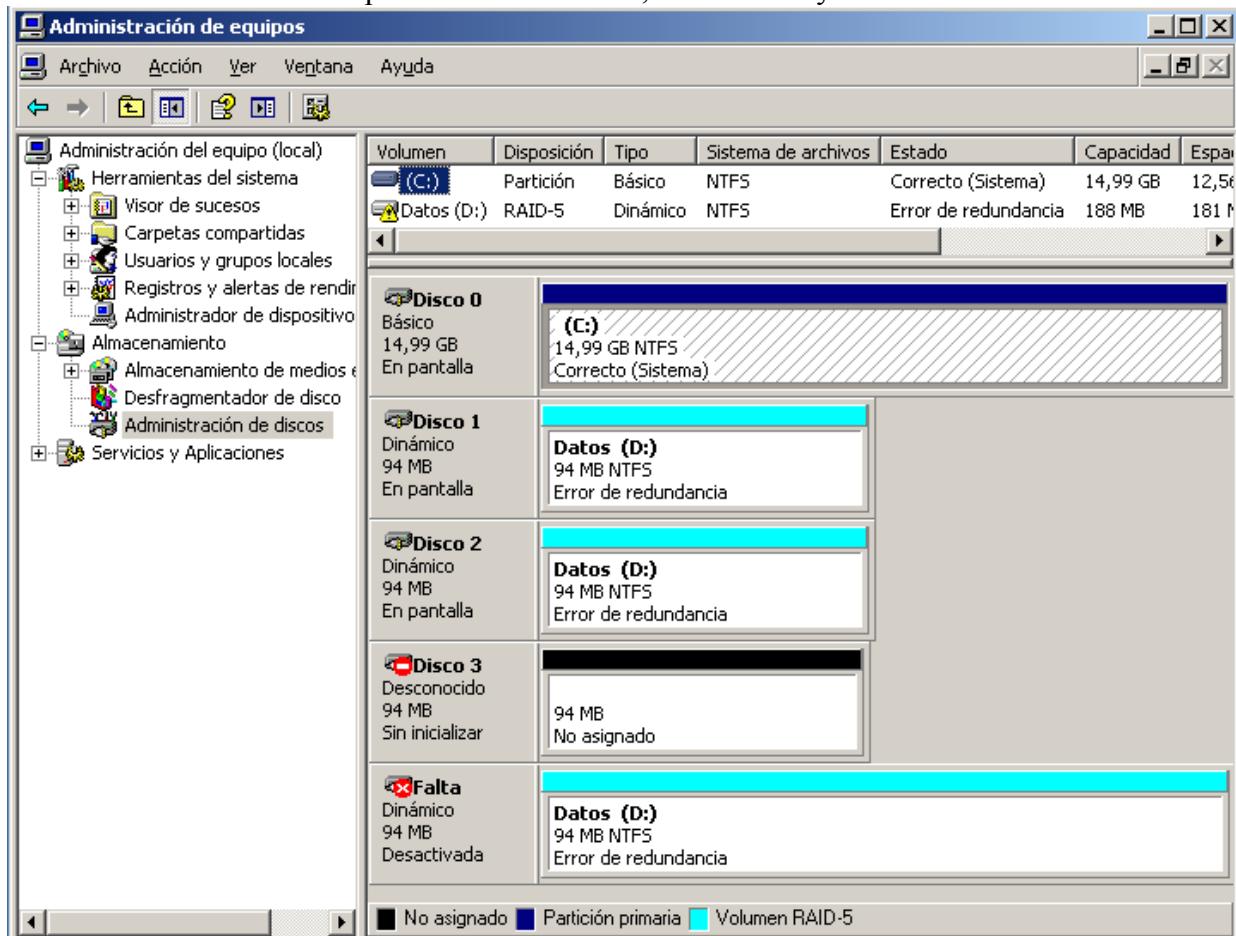
Si ademas entro en el Administrador de discos veo que hay fallo en el sistema RAID.



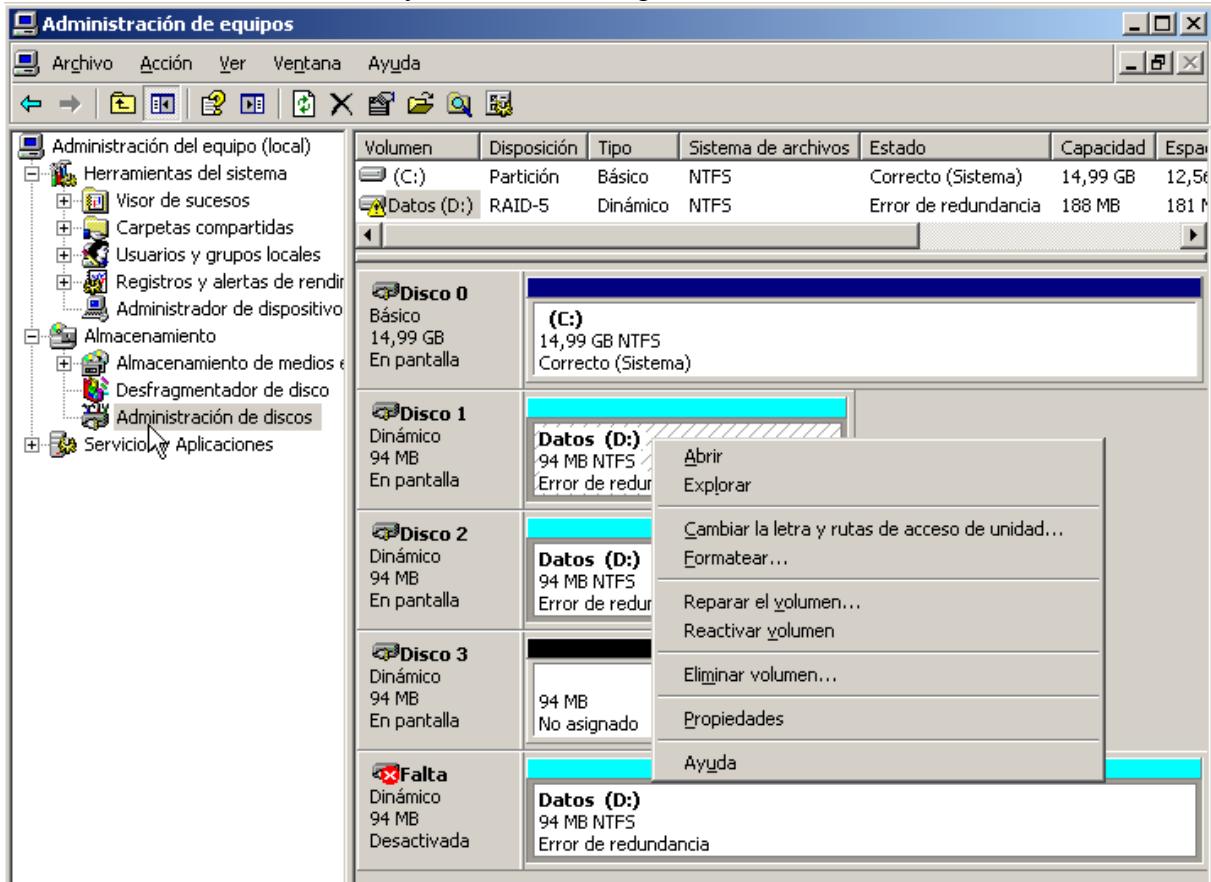
Se apaga la maquina virtual y se añade otro disco (Datos 4) en reposición del averiado (el que se ha quitado previamente).



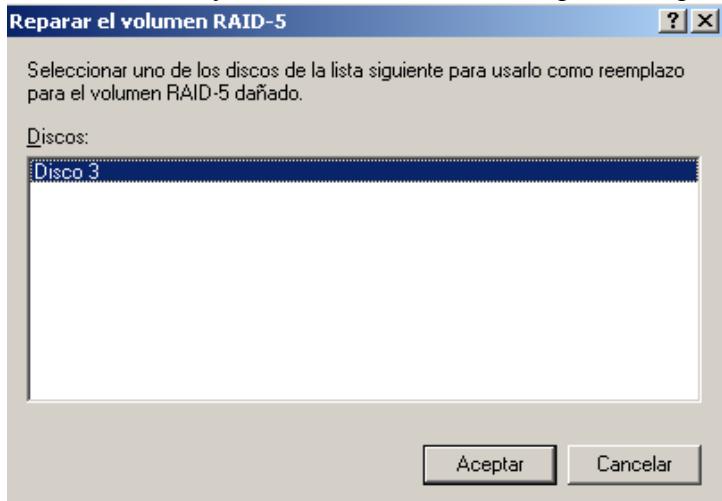
Se vuelve a arrancar windows y En Herramientas Administrativas – Administrador de equipos
-Administración de discos aparece el nuevo disco, se inicializa y se convierte en dinámico.



Una vez echo, se va al Disco 1 y se selecciona Reparar el volumen.



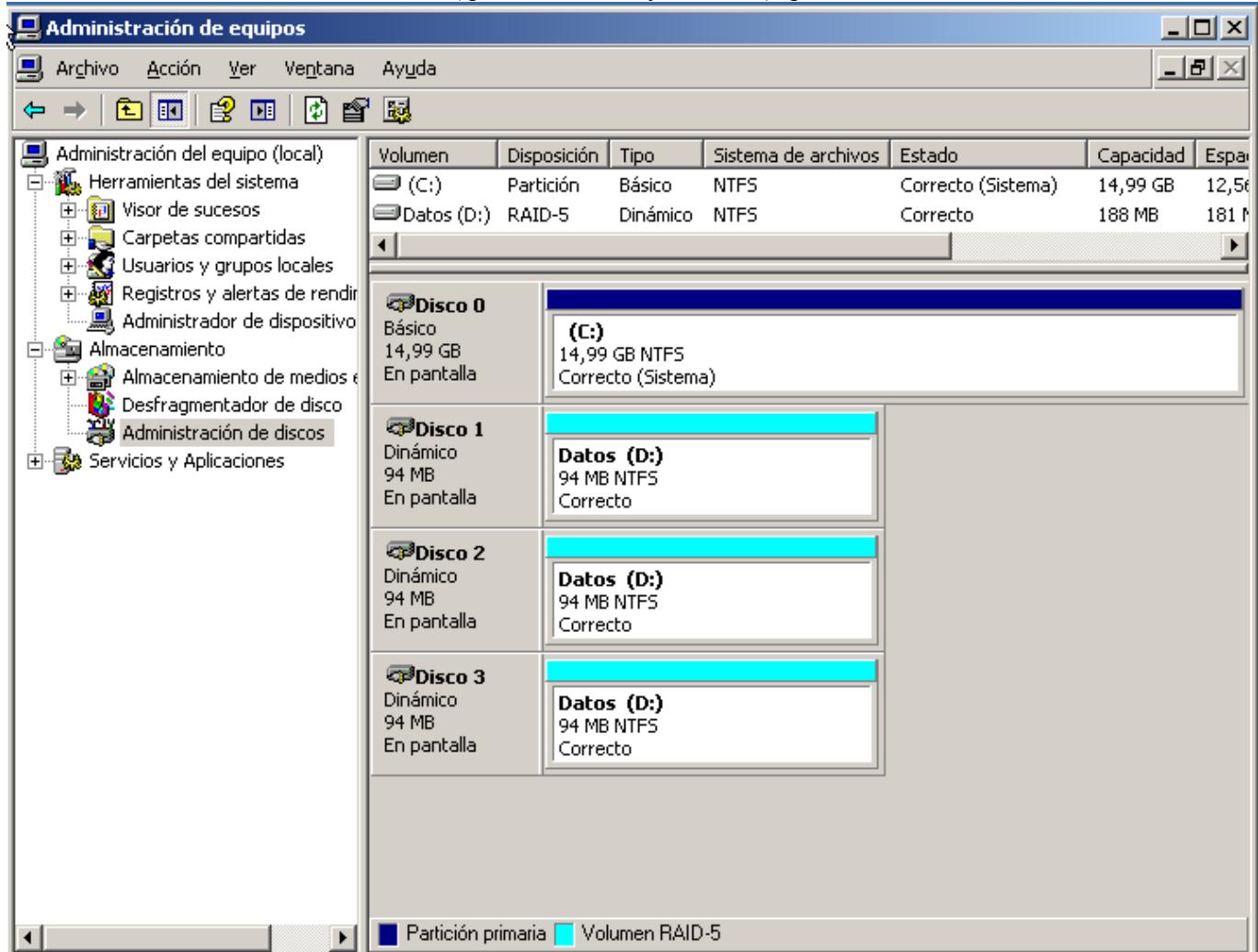
Pedirá un disco y se selecciona el Disco 3 que es el que se ha metido nuevo.



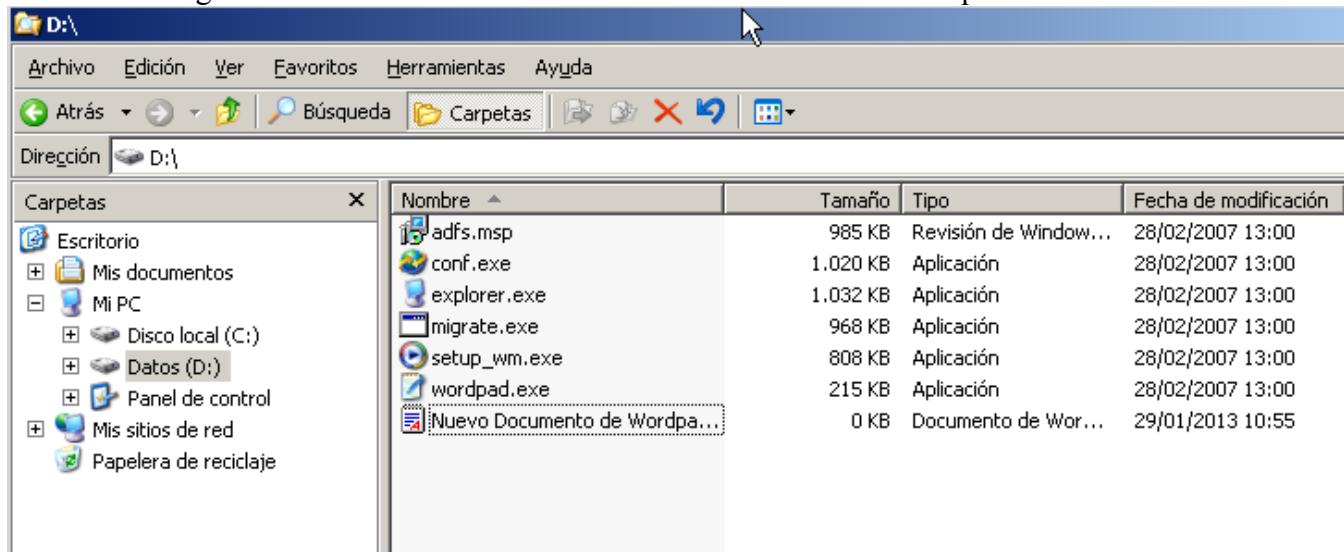
Luego en el que da error 'falta' se selecciona Extraer disco.



Un vez extraído el volumen con fallo (que en realidad ya no esta) queda OK el sistema RAID.



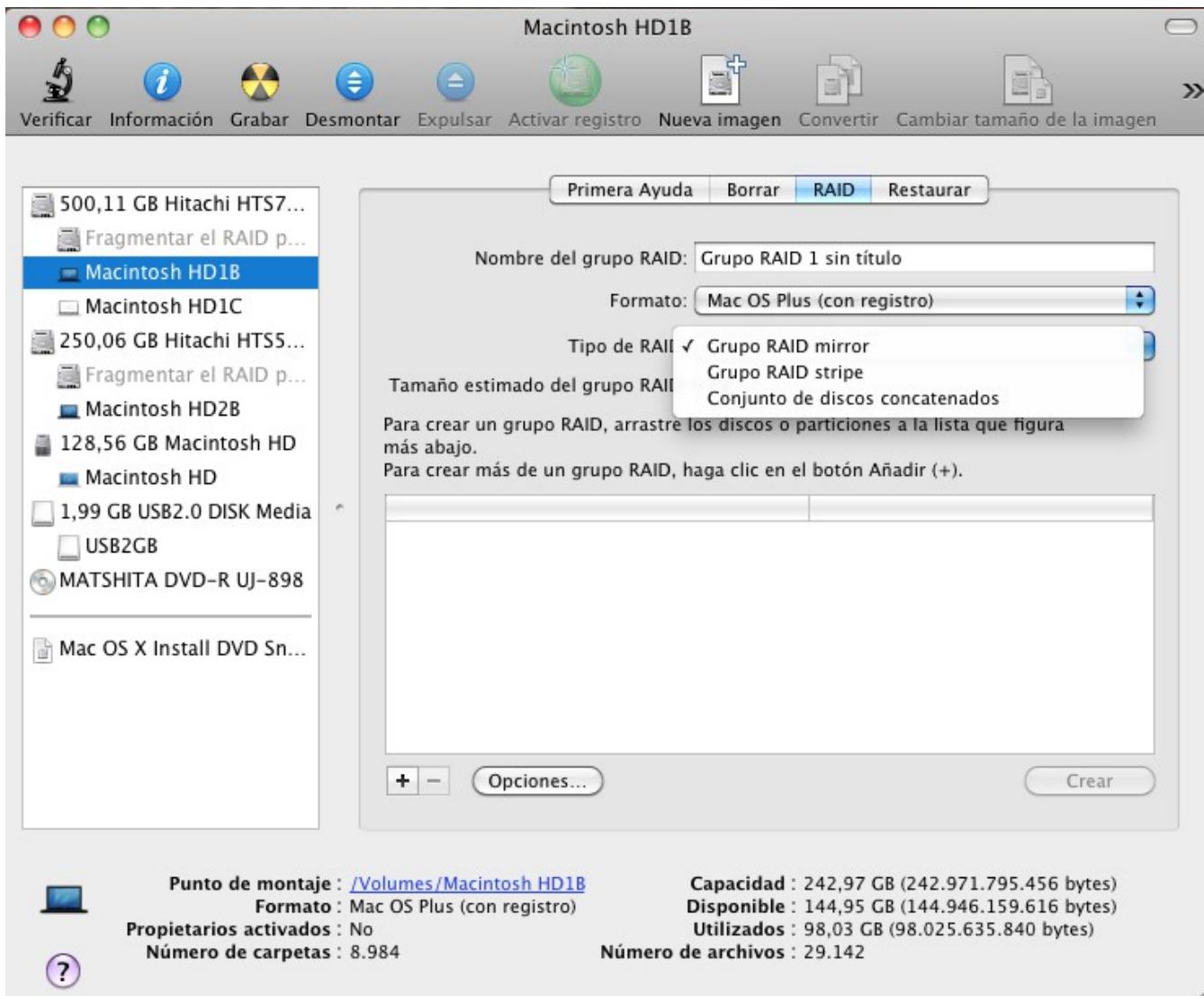
Los ficheros siguen estando en el volumen de Datos como si nada hubiera pasado.



RAID en OS X (Snow Leopard)

En equipos Apple con el sistema operativo Snow Leopard (actualmente sustituido por Lion) pero ampliamente utilizado, se puede realizar un sistema RAID por software y utilizando 2 o mas discos duros, particiones o dispositivos de almacenamiento externo.

Para configurar dos Discos como RAID necesitamos la aplicación 'Utilidad de Disco' que viene ya integrada con el sistema operativo y ubicada en la carpeta 'utilidades'.



Cuando seleccionamos un disco duro o partición con la que queremos hacer un RAID, tenemos una pestaña llamada 'RAID' donde tendremos todas las opciones disponibles:

- **Grupo RAID mirror:** Conocido también como RAID 1, proporciona seguridad al copiar en dos o mas discos simultáneamente la información, de tal manera que si uno de los discos del grupo mirror se desconecta o falla el ordenador tiene acceso a los datos contenidos en el resto de Discos del Grupo.
 - Ventaja: Conseguimos seguridad, los datos están duplicados en cada disco.
 - Desventaja: La velocidad de escritura disminuye (discos diferentes) o se mantiene prácticamente igual en el mejor de los casos (discos iguales).

- **Grupo RAID stripe:** Conocido también como RAID 0, proporciona velocidad de acceso a los datos, lo que se hace es guardar la información repartida entre los discos que forman el grupo stripe, de tal manera que el acceso es mucho más rápido al estar cada disco en canales diferentes, se pueden usar discos duros o particiones de igual o diferente tamaño (las mejores prestaciones se consiguen si son del mismo tamaño y características).
- Ventaja: Conseguimos velocidad de acceso (según discos se puede llegar al doble).
 - Desventaja: Los datos están repartidos, si falla un disco perderemos la información.

- **Conjunto de discos concatenados:** Sirve para crear un Disco de mayor tamaño, a partir de Discos más pequeños, similar en funcionamiento a RAID stripe pero la velocidad de acceso es menor, si los discos son de similar tamaño es mejor usar stripe.

También sirve para, a partir de un Raid 0 y un Raid 1 crear un Raid 10, con lo que conseguiríamos velocidad y seguridad (en este caso se necesitan 4 discos duros o particiones que estén en diferente puerto cada una para obtener todos los beneficios).

Para comprobar el funcionamiento del sistema RAID, he cogido una partición de cada Disco duro (de igual tamaño, 128GB) y le he aplicado RAID mirror, en mi caso al contener una de las particiones el sistema operativo ha tenido que realizar una copia de seguridad previamente.

A tener en cuenta:

- Si la partición o disco duro que va a formar parte de RAID es con el que hemos arrancado, no nos permitirá añadirlo, deberemos de iniciar el sistema desde el DVD de instalación (que también contiene 'Utilidad de discos') o una instalación que tengamos en otro disco duro que no participe en la formación de RAID.
- Las particiones o discos duros con los que se vaya a formar RAID serán formateados por lo que hay que hacer copia de seguridad si contienen datos que no queramos perder.

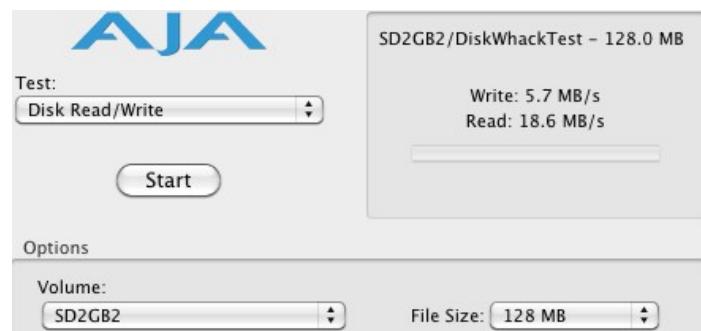
Apuntar que en este caso uno de los Discos duros es de 7200rpm y da velocidades de escritura/lectura sostenidas de alrededor de 80MB/s, sin embargo el otro Disco duro es de 5200rpm y las lecturas de escritura/lectura son de alrededor de 40MB/s. Tras la creación del RAID constato lo siguiente:

- La velocidad de escritura disminuye y es algo más rápida que el más lento.
- La velocidad de lectura es similar o un poco más rápida que el más rápido.

En otra prueba he utilizado 2 tarjetas SD de 2GB iguales, le he aplicado la opción mirror y después la opción stripe y he comparado resultados con un programa de test de discos duros.

Primero he medido la velocidad de cada tarjeta en modo normal:

Nos da una media de 5MB/s en escritura y 16MB/s en lectura.



Creo el Grupo RAID mirror (recordar que este proceso elimina los datos de los discos, como ya se ha comentado anteriormente)



Nota: A la hora de crear el Grupo RAID marcamos la opción "Reconstruir Grupos RAID mirror automáticamente" de tal manera que cuando falle uno y lo reemplazamos o se desconecte y lo volvamos a conectar , el sistema lo reconstruya con la información del existente y lo incorpore al conjunto, si no lo hacemos no pasa nada, porque con la utilidad de discos tenemos la opción también para hacerlo de forma manual.

A esta pantalla accedemos pinchando en 'opciones':



Tras el proceso se crea el conjunto RAID que aparecerá con el nombre que le hemos asignados (aparece de forma independiente cada disco y después el conjunto):



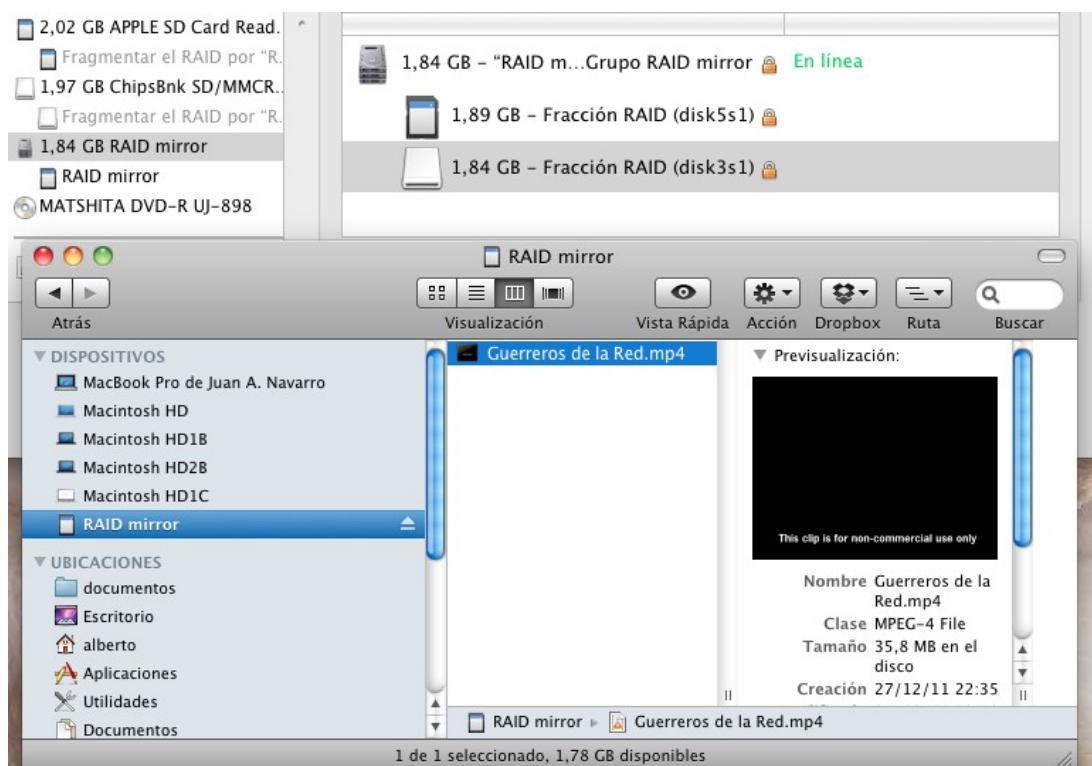
Se ejecuta el Test y se comprueban resultados:



Como se aprecia la velocidad de escritura es algo mas lenta que el mas lento y la velocidad de lectura se ha incrementado.

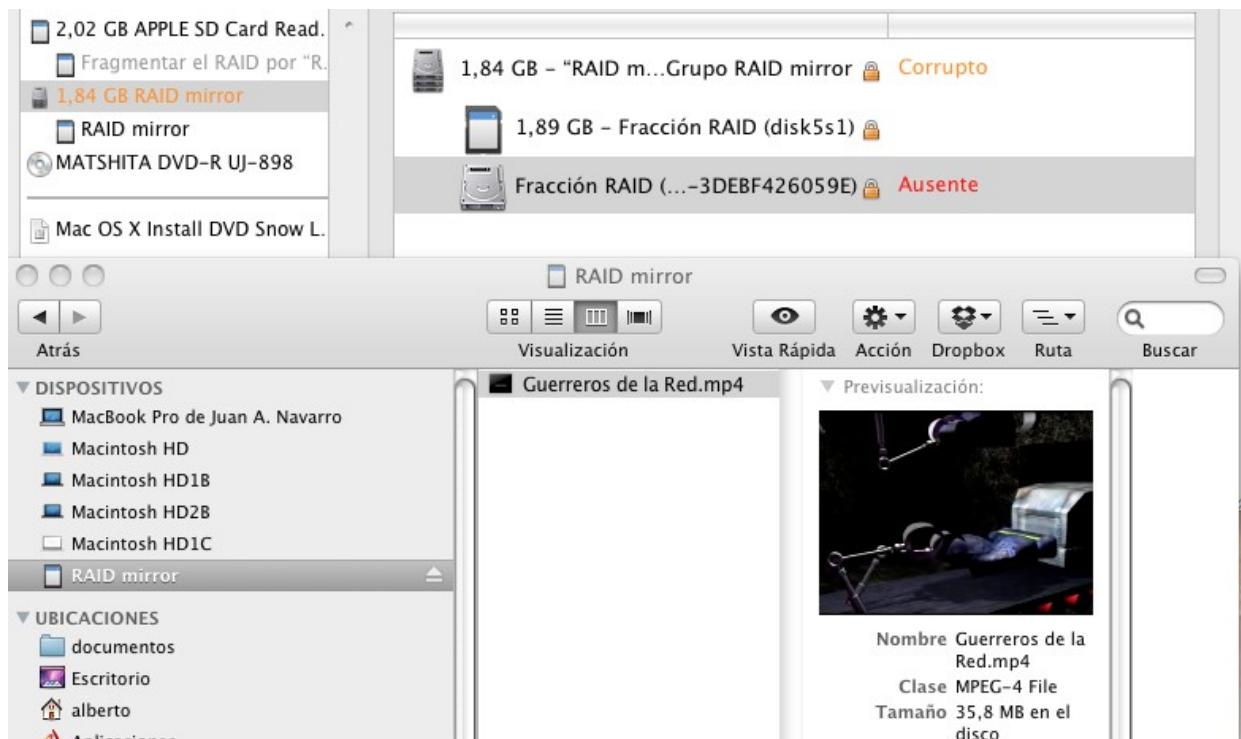
En RAID mirror se gana en seguridad al estar los datos duplicados en ambos discos, esto lo vamos a confirmar guardando un archivo y desconectando uno de los discos a ver que pasa:

- En esta imagen se puede ver el archivo copiado y como los discos están en linea:

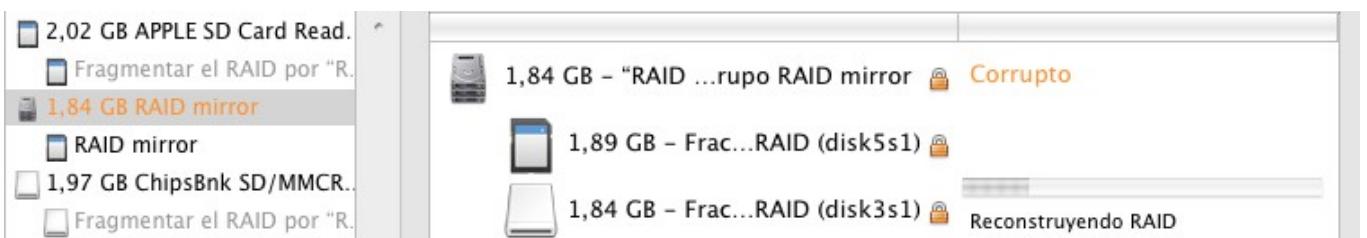


Si retiramos de forma intempestiva uno de los discos, aun sigue apareciendo el conjunto RAID en Utilidad de disco pero indicando un fallo.

En el explorador aparece el disco y el archivo sigue estando, en este caso contiene un video, que si lo ejecutamos se visualiza correctamente.



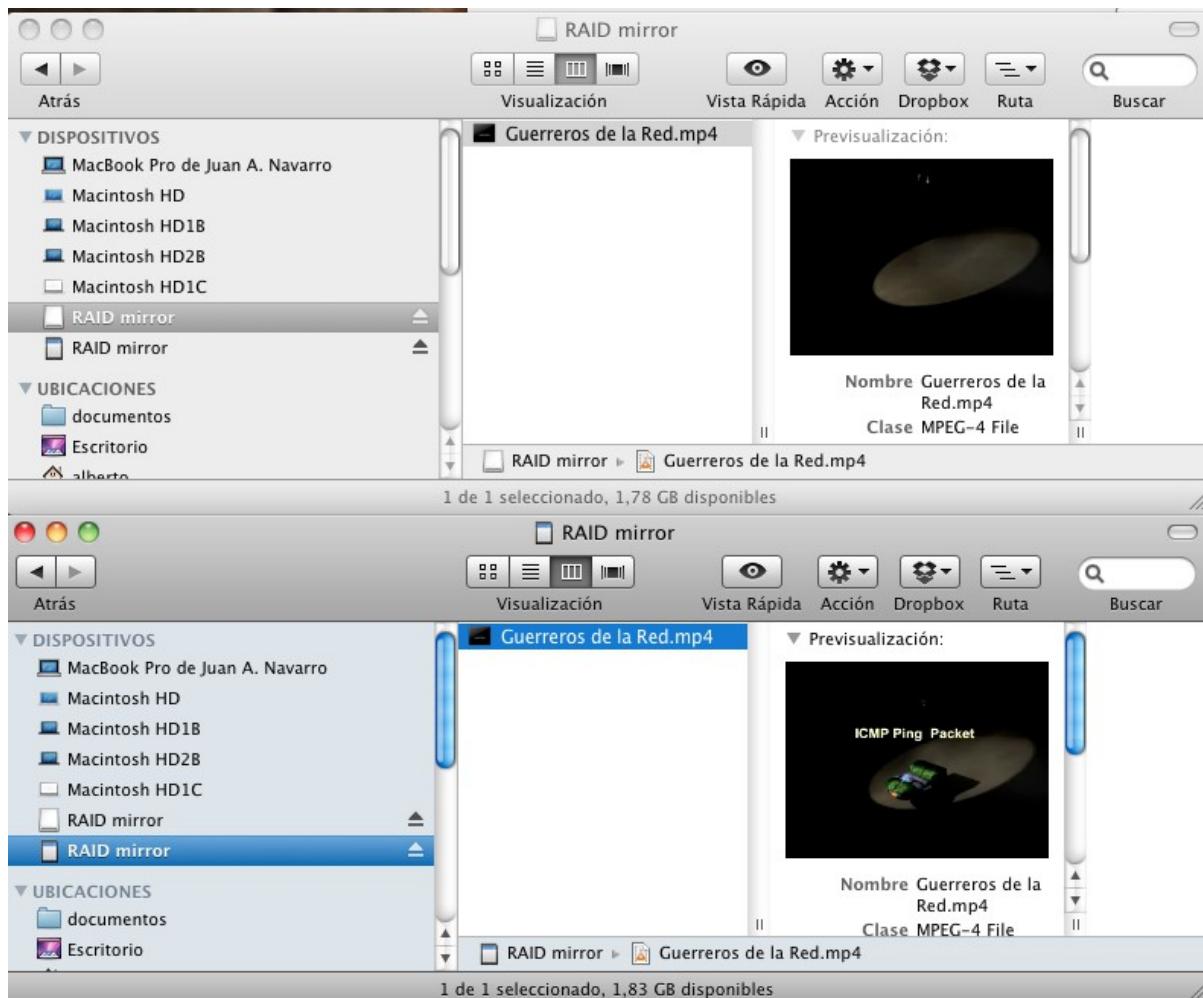
Si conectamos el Disco de nuevo el disco lo reconstruye automáticamente con la información del que esta operativo:



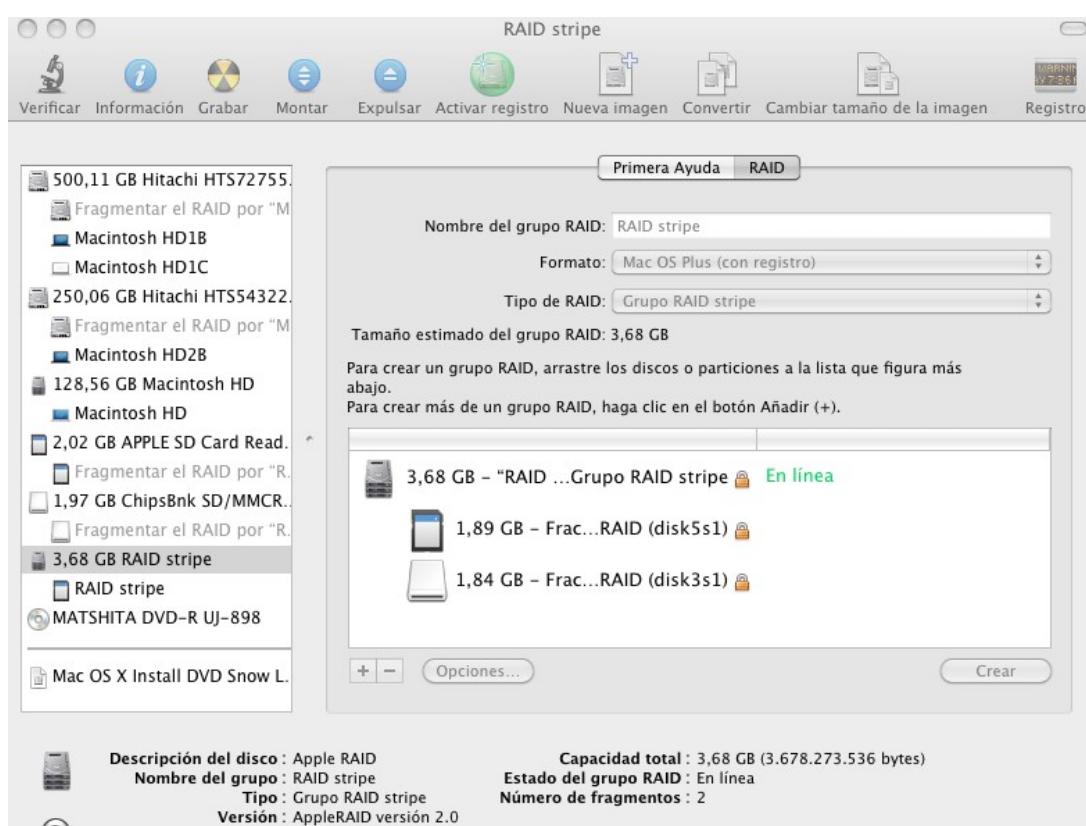
Ya sea automáticamente si se ha marcado al opción o manualmente con 'Utilidad de Discos', el proceso se realiza en segundo plano, por lo que podemos en nuestro caso seguir visualizando el video contenido en la unidad.

Nota: Si eliminamos el Grupo RAID mirror, lo que pasa es que el sistema vuelve a dejarnos las dos unidades separadas como al principio, pero con los datos intactos y duplicados en los dos discos.

Como se puede ver en la siguiente imagen:

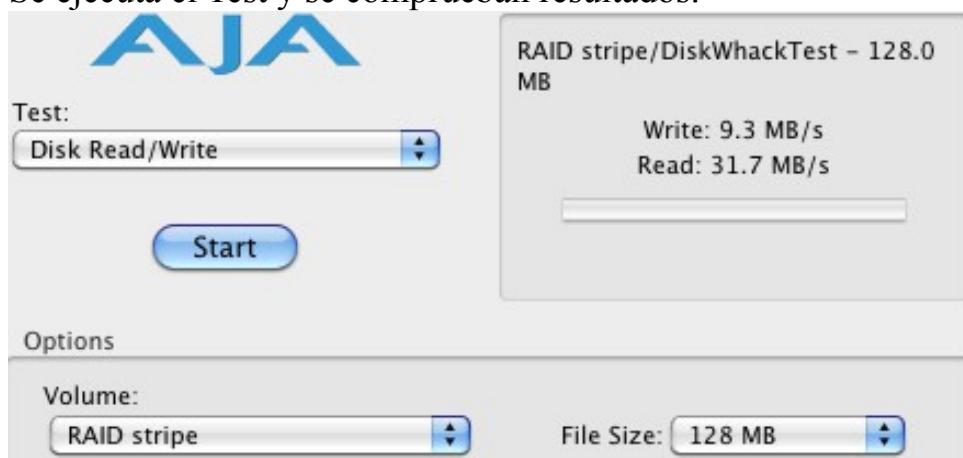


Creamos el Grupo RAID stripe: Mismo procedimiento que el caso anterior pero con la opción stripe (llamamos al conjunto 'RAID stripe', pero le podemos llamar como queramos):



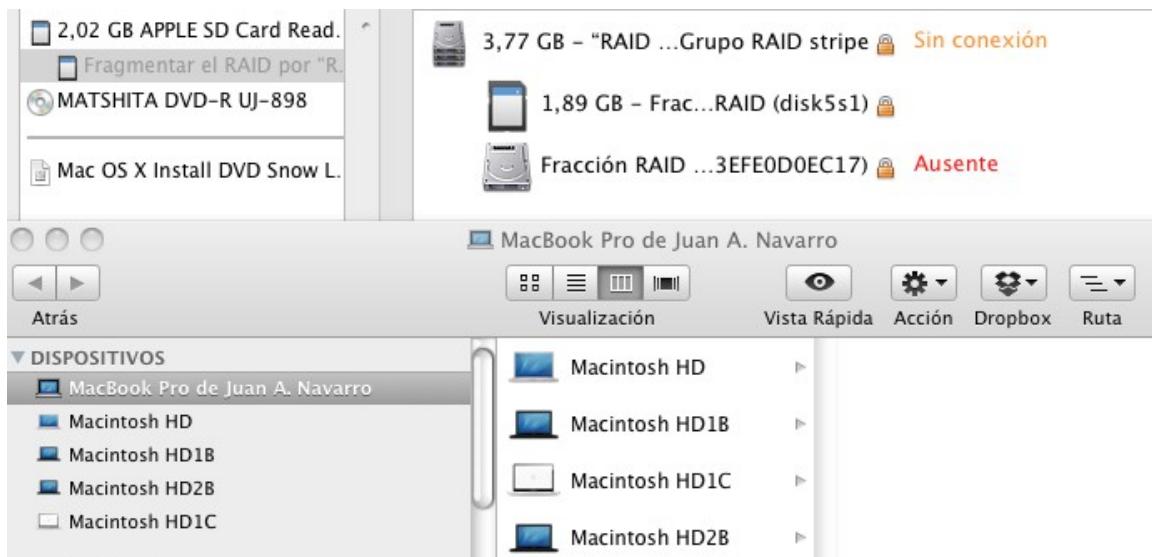
Nota: en este caso no tenemos la opción 'Reconstruir Grupos RAID mirror automáticamente', que como indica su nombre solo es valida para la opción mirror.

Se ejecuta el Test y se comprueban resultados:



Se puede apreciar como la velocidad de escritura prácticamente se duplica y la velocidad de lectura también mejora con respecto a la opción 'mirror' y por supuesto a si estuvieran como unidades normales.

Si retiramos de forma intempestiva uno de los discos, ya no aparece en el explorador de archivos (Finder en OS X) y en utilidad de Disco no avisa de la desconexión, esto es porque los datos están repartidos en ambos dispositivos y solo se puede reconstruir la información si ambos están presentes.



En este caso lo hemos desconectado cuando no estábamos realizando ninguna acción sobre el dispositivo y al volver a conectarlo todo vuelve a la normalidad.

Nota: Si eliminamos el Grupo RAID stripe perdemos todos los datos que contengan los dispositivos que lo formen y tendremos que volver a darles formato.

En función de las necesidades utilizaremos mirror o stripe, cada uno tiene ventajas e inconvenientes que deberemos valorar.

Práctica Alta Disponibilidad 1 – CARP

(Common Address Redundancy Protocol)

Servidor Web 1 (Apache) Maestro
192.168.7.55



Servidor Web 1 (Apache) Esclavo
192.168.7.56



El Protocolo de redundancia de Dirección Común, o **CARP** permite que varios sistemas comparten la misma dirección IP.

En algunas configuraciones, esto puede ser utilizado para la disponibilidad o el equilibrio de carga. Los anfitriones pueden utilizar direcciones IP separadas.

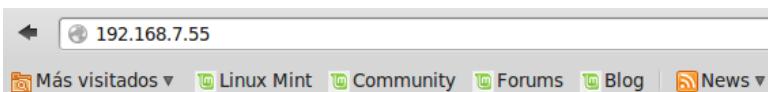
Su objetivo principal es proporcionar redundancia de comutación por error,

- Se necesitan 2 Maquinas virtuales con Linux Debian instalado.
- Dejar cada máquina con sólo una tarjeta de red (Des-habilitar el 2º adaptador si lo tiene)
- Reconfigurar la red teniendo en cuenta que puede haber cambiado de eth0 a ethx (comprobarlo con:
 - dmesg | grep eth
- Comprobar que la red funciona antes de seguir, cada maquina tendra su propia IP :

Configuracion Debian1
Interface principal
auto eth2
iface eth2 inet static
address 192.168.7.55
netmask 255.255.255.0
gateway 192.168.7.1

Configuracion Debian2
Interface principal
auto eth2
iface eth2 inet static
address 192.168.7.56
netmask 255.255.255.0
gateway 192.168.7.1

- Instalar apache2 en cada máquina y modificar el fichero /var/www/index.html para distinguir ambas máquinas (basta con la instalación por defecto para las pruebas).
 - apt-get install apache2



It works!

DEBIAN MASTER JUAN

This is the default web page for this server.

The web server software is running but no content has been added, yet.

This is the default web page for this server.

The web server software is running but no content has been added, yet.

- Instalar en cada máquina el paquete ucarp
 - apt-get install ucarp
- Poner en cada máquina la siguiente configuración de red en el fichero /etc/network/interfaces
 - nano /etc/network/interfaces

```
Configuracion Debian1
# Interface principal
auto eth0
iface eth0 inet static
    address 192.168.7.55      # la otra máquina tendrá la 192.168.7.56 p.ej.
    netmask 255.255.255.0
    gateway 192.168.7.1
    #####
    # Configuración ucarp
    #####
    ucarp-vid    1
    ucarp-vip    192.168.7.57  # esta es la IP que comparten
    ucarp-password 12345       # contraseña para comunicarse
    ucarp-advskew 1
    ucarp-advbase 1
    ucarp-master yes

# El interface carp, encima de eth0
iface eth0:ucarp inet static
    address 192.168.7.57    # de nuevo la IP que comparten
    netmask 255.255.255.255
```

```
Configuracion Debian2
# Interface principal
auto eth0
iface eth0 inet static
    address 192.168.7.56      # la otra máquina tendrá la 192.168.7.55 p.ej.
    netmask 255.255.255.0
    gateway 192.168.7.1
    #####
    # Configuración ucarp
    #####
    ucarp-vid    1
    ucarp-vip    192.168.7.57  # esta es la IP que comparten
    ucarp-password 12345       # contraseña para comunicarse
    ucarp-advskew 1
    ucarp-advbase 1
    ucarp-master no

# El interface carp, encima de eth0
iface eth0:ucarp inet static
    address 192.168.7.57    # de nuevo la IP que comparten
    netmask 255.255.255.255
```

- Se reinicia la red.
/etc/init.d/networking restart (o stop, start)
- Se comprueba el funcionamiento poniendo en el navegador la IP 192.168.7.57 .
- Aparecerá una de los dos Servidores en dicha dirección independientemente de que estén funcionando los dos (en principio sera el master por defecto) y en función a cual falle, aparecerá la Web correspondiente al que tiene la IP 192.168.7.55 o 192.168.7.56, para ello se tira abajo el puerto de red en uno de ellos con **ifdown ethx** y luego en el otro con /etc/init.d/networking stop (**ifup ethx** lo volvemos a levantar, donde x es el numero de puerto, para que este siempre uno de ellos levantado).
- Pantallazos de lo que debe de dar en cada caso:



DEBIAN MASTER JUAN

This is the default web page for this server.

The web server software is running but no content has been added, yet.



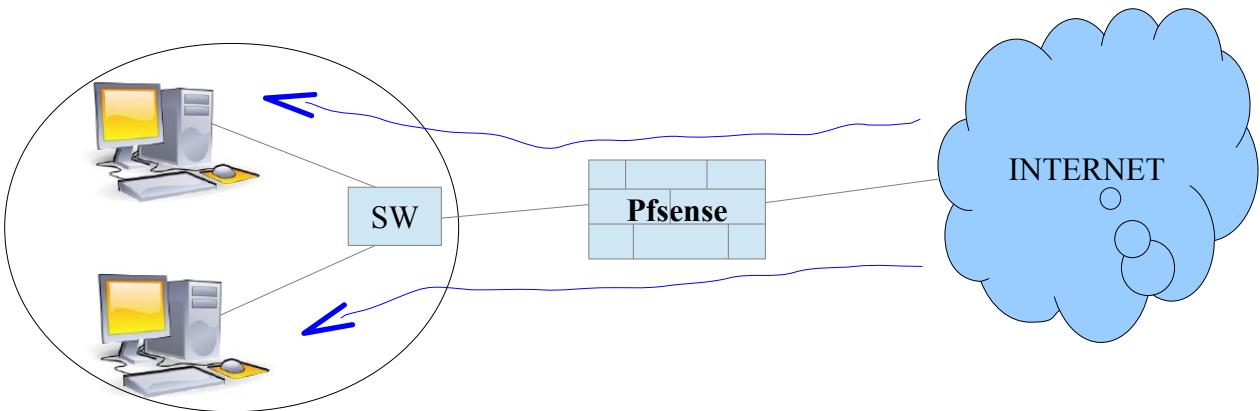
DEBIAN SLAVE JUAN

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Práctica Alta Disponibilidad – Pfsense

(Uso Balanceo de carga)



pfSense es una distribución personalizada de FreeBSD, adaptada para ser usada como Firewall y Router. cuenta con una interfaz web sencilla para su configuración.

<http://www.pfsense.org/>

The screenshot shows the pfSense web interface at the URL <http://192.168.7.3>. The main navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and pfSense.localdomain. The Status: Dashboard page is displayed, featuring two main sections: System Information and Interfaces.

System Information:

Name	Value
Name	pfsense.localdomain
Version	2.0.1-RELEASE (i386) built on Mon Dec 12 17:53:52 EST 2011 FreeBSD 8.1-RELEASE-p6
Unable to check for updates.	
Platform	pfSense
CPU Type	Intel(R) Core(TM)2 CPU 6400 @ 2.13GHz
Uptime	00:20
Current date/time	Fri Feb 8 12:57:41 UTC 2013
DNS server(s)	127.0.0.1 8.8.8.8
Last config change	Tue Jan 22 9:36:30 UTC 2013
State table size	9/22000 Show states
MBUF Usage	646/8512
CPU usage	36%
Memory usage	24%
Swap usage	0%
Disk usage	12%

Interfaces:

Interface	IP Address	Description
WAN	192.168.7.3	1000baseT <full-duplex>
LAN	192.168.99.100	1000baseT <full-duplex>

Algunas de las funcionalidades que incluye son:

- Firewall
- Nat
- VPN
- Servidor DNS
- **Balance de carga**
- Portal Cautivo
- Servidor DHCP
- Servidor PPPoE
- SNMP
- RIP
- Wake on LAN
- etc.

En clase se realiza una demostración del funcionamiento en el modo de Balance de carga, de tal manera que se tienen dos ordenadores que sirven la misma pagina web (aunque se las llama con nombre diferente) y el equipo con la distribución Pfsense en tres maquinas virtuales, la maquina virtual con Pfsense se encarga de repartir el trafico proveniente de internet (en la demostración en el lado de internet están los ordenadores del aula) entre los dos ordenadores. Así a unos les sale la pagina que sirve uno de los ordenadores Web y otros la pagina del otro PC.

Si falla uno de los ordenadores que sirve la pagina Web el trafico es enrutado en su totalidad al otro ordenador.