Parte V

Apéndices

Apéndice A

Comandos básicos

Para más información sobre los comandos podemos ejecutar: `$man <comando>`

Comandos de sistema

Comando	Descripción
`man`	Páginas del manual
`ls`	Listar (múltiples opciones)
`rm`	Borrar
`cp`	Copiar
`mv`	Mover o renombrar
`ln -s <fichero> <enlace>`	Enlace debil a fichero
`pwd`	Directorio actual
`cd <directorio>`	Entra en directorio
`cd ..`	Sale del directorio actual
`chown, chgrp y chmod`	Sobre atributos de ficheros
`touch <fichero>`	Crear ficheros vacíos
`find y locate`	Buscar ficheros
`grep`	Buscar texto en ficheros (muy potente)
`find / | grep 'cadena'`	Busca un fichero que contenga esa cadena por el sistema
`df`	Ver espacio libre en disco
`du -sh`	Ver espacio usado en el directorio actual
`cat, more y less`	Lista ficheros
`<comando>|more` y `<comando>|less`	Salida de comando filtrada por páginas
`vim` y `emacs`	Editores de texto, modo texto
`nedit`, `kedit` y `kwrite`	Editores de texto, modo gráfico
`split`	Partir ficheros
`which`	Devuelve el Path de un ejecutable, que se encuentre en la variable $PATH

Entorno gráfico X-Windows

Comando	Descripción
`startx`	Iniciar sesion X
`startx -- :2, :3, etc.`	Abrir nuevas sesiones
`xf86config`	Configurar X, modo texto
`xf86cfg`	Configurar X, modo gráfico
`CTRL+ALT+BACKSPACE`	Salir de las X

Comandos para comunicaciones y redes

Comando	Descripción
`who`	Lista los usuarios conectados
`finger`	Información sobre los usuarios
`mail`	Sencillo programa de correo
`write`	Manda un mensaje a la pantalla de un usuario
`wall`	Manda un mensaje a todos los usuarios
`mesg`	Activa/Desactiva la recepción de mensajes *write* y *wall*
`talk`	Establece una conversación con otro usuario
`baner`	Saca un letrero en pantalla con el texto que se le pase al comando
`cal`	Saca un calendario en pantalla
`clear`	Limpia la pantalla
`date`	Saca fecha y hora actuales
`passwd`	Cambia contraseña de un usuario

Comprimir y descomprimir

Comando	Descripción
`tar zxvf`	Descomprimir un *.tar.gz*
`tar jxvf`	Descomprimir un *.tar.bz2*
`tar cxvf <archivo>.tar.gz <archivo>`	Comprimir un archivo o directorio
`gzip -d`	Descomprimir un *.gz*
`tar`	Empaquetar sin comprimir (múltiples opciones)
`gzip`	Comprimir ficheros (despues de empaquetar)

Montaje de unidades

Comando	Descripción
`mount -t msdos /dev/floppy /mnt`	Montar diskette
`mount -t iso9660 /dev/cdrom /mnt`	Montar cdrom
`mount -t <tipo> /dev/<dispositivo> <punto_de_montaje>`	Montar un dispositivo
`umount <punto_de_montaje>`	Desmontar unidad

Uso del sistema

Comando	Descripción
`ps`	Procesos en ejecución del teminal
`ps -u<usuario>`	Procesos en ejecución del usuario
`lspci`	Dispositivos PCI del sistema
`lsmod`	Módulos cargados en el kernel
`modconf`	Cargar módulos en el kernel
`uname -a`	Información del sistema
`ldconfig -p`	Librerías instaladas
`ldd <ruta>/<programa>`	Librerías que usa el programa
`shutdown -r 0`	Reinizializa el sistema (`#reboot`)
`shutdown -h 0`	Apaga el sistema (`#halt`)
`shutdown <opcion> <n_segundos>`	Realiza ópcion despues de *n_segundos* segundos
`logout`	Cierra la sesión del usuario
`su <usuario>`	Cambia sesión a otro usuario (switch user)
`fdisk /mbr`	Borra el gestor de arranque del disco (arranques del sistema)

Apéndice B

Debian en castellano

Para tener las aplicaciones en nuestro idioma lo primero que necesitamos es instalar los siguientes paquetes:

```
#apt-get install user-euro-es language-env euro-support
```

Una vez hayamos realizado el apt-get, para ver "los locales" (idiomas locales) que tiene el usuario que se encuentra actualmente conectado, hay que ejecutar el siguiente comando:

```
$locale
```

Si además queremos saber que traducciones locales tenemos disponibles en el sistema, ejecutaremos la siguiente instrucción:

```
$locale -a
```

Si el idioma castellano, no se encuentra disponible entre las locales del sistema las podemos incluir en el archivo de configuración de locales, */etc/locale.gen*. Para ello añadiremos al final de ese archivo las siguientes líneas:

```
es_ES@euro ISO-8859-15
es_ES ISO-8859-1
```

Una vez añadidas al archivo necesitamos que las ejecute y reconfigure nuestro sistema, mediante el comando:

```
#/usr/sbin/locale-gen
```

Además en unos de los ficheros que carga las variables de usuario añadiremos las siguientes variables de entorno. Por ejemplo en el archivo *˜/.bash_profile*:

```
export LANG=es_ES.ISO-8859-15
export LC_ALL=es_ES@euro
```

La próxima vez que hagamos *login* con el usuario cargará el nuevo perfil. Podemos comprobamos que "los locales" son los correctos, con el mismo comando que antes: `$locale`

Una vez tengamos disponible el idioma castellano, podemos habilitar también el soporte para el euro en la consola. Pasa eso tenemos que añadir las siguientes líneas al fichero */etc/console-tools/config*, fichero de configuración de la consola:

```
SCREEN_FONT=lat0-sun16
APP_CHARSET_MAP=iso15
APP_CHARSET_MAP_vc2=iso15
APP_CHARSET_MAP_vc3=iso15
```

Si además también queremos colocar las páginas de manuales en castellano hay que instalar los siguientes paquetes:

```
#apt-get install user-es manpages-es manpages-es-extra
```

Solo queda castellanizar las aplicaciones del sistema, si es que tienen los archivos del idioma. Hay que ejecutar el siguiente comando, seleccionando las opciones que nos interesen:

```
#dpkg-reconfigure locales,
```

Este documento esta basado en la documentación disponible en Debian, se puede consultar mediante:

```
$man castellanizar
```

Apéndice C

Archivos de configuración

Archivo	**Descripción**
/etc/lilo	Configuración del gestor de arranque Lilo
/etc/inetd.conf	Superservidor de Internet y envoltorio de demonios TCP/IP
/etc/xinetd.conf	Configuración del superservidor, mediante entorno gráfico
/etc/init.d/*	Scrips de inicio del sistema que ejecutara initd
/etc/rc#.d	Scripts *runlevels* que ejecuta *init* al arrancar el equipo
/etc/passwd	Usuarios del sistema
/etc/group	Contraseñas encriptadas de los usuarios del sistema
/etc/skel/*	El contenido de este directorio se copiará al home de cada usuario nuevo del sistema
/etc/fstab	Montaje de particiones en el sistema
/etc/X11/XF86Config-4	Configuracion de las X-Windows
~/.xinitrc	Archivo de arranque de usuario para las X-Windows
~/.vimrc	Archivo de configuración del Vim
/etc/profile	Preferencias de todos los usuarios del sistema
~/.profile	Preferencias del usuario
~/.bash_profile	Preferencias del shell bash
~/.bash_login	Configuración de inicio del shell bash
~/.bash_logout	Configuración de finalización del shell bash
~/.bashrc	Si se ejecuta un shell interactivo bash sin entrada por consola
/etc/ssh/ssh_config	Configuración del cliente para las conexiones seguras SSH
/etc/ssh/sshd_config	Configuración del servidor de conexiones seguras SSH
~/.gnupg/	Directorio que contiene los archivos de usuario de GnuPG
/etc/at.allow	Usuarios a los que les esta permitido programar tareas at
/etc/at.deny	Usuarios a los que les esta denegado programar tareas at
/etc/crontab	Taréas programadas del sistema
/var/spool/cron/crontabs/<usuario>	Tareas programadas por cada usuario
/etc/anacrontab	Tareas programadas que se pueden ejecutar con retraso
/etc/locale.gen	Archivo de locales
/etc/console-tools/config	Archivo de configuración de la consola
/etc/webmin/miniserv.conf	Archivo de configuración de Webmin
/etc/squid/squid.conf	Configuración del proxy Squid
/etc/squid/*	Archivos de configuración del Proxy Squid

Archivo	Descripción
/etc/kismet/kismet_ui.conf	Configuración de la interfaz del sniffer wifi Kismet
/etc/kismet/kismet.conf	Configuración del sniffer wifi Kismet
/etc/freeradius/radiusd.conf	Opciones de FreeRadius
/etc/freeradius/eap.conf	Opciones para EAP en FreeRadius
/etc/freeradius/clients.conf	IPs clientes de FreeRadius
/etc/freeradius/users.conf	Usuarios clientes de FreeRadius
/etc/modules.conf	Módulos que se cargarán al inicio
/etc/modules	Configuración de los módulos
/etc/network/interfaces	Configuración de interfaces de red
/etc/network/options	Configuración de las opciones de red
/etc/host.conf	Dice al sistema cómo resolver los nombres de los hosts
/etc/hostname	Nombre.dominio del host local
/etc/hosts	Nombre y dirección IP de hosts del sistema
/etc/hosts.allow	Hosts a los que se le permite el acceso al sistema
/etc/hosts.deny	Hosts a los que se le deniega el acceso al sistema
/etc/hotplug/*	Scrips de configuración de dispositivos hotplug (inst. dinámica)
/etc/hotplug.d/*	Archivos de agentes de dispositivos
/etc/cvs-cron.conf	Sistema de versiones concurrentes (cvs)
/etc/cvs-pserver.conf	Opciones del servidor de versiones (cvs)
/etc/dhcpd.conf	Archivo de configuración estandar DHCPD
/etc/default/dhcpd	Opciones del DHCPD
/var/lib/dhcp/dhcpd.leases	Base de datos *lease* para el servidor DHCPD
/var/lib/dhcp/dhclient.leases	Base de datos *lease* para el cliente DHCP
/etc/default/dhcp3-relay	Archivo de configuración DHCP-relay
/etc/dhpc3/dhclient.conf	DHCP del cliente dhcp3
/etc/dhcp3/dhcpd.conf	DHCP del servidor dhcp3
/etc/snort/snort.conf	Archivo de configuración de Snort
/etc/snort/rules/*.rules	Archivos de reglas para Snort
/etc/tripwire/twpol.txt	Archivo de políticas
/etc/acidlab/acid_conf.php	Archivo de configuración de ACID
/etc/portsentry/portsentry.conf	Archivo de configuración de PortSentry
/var/log/*	Registro de logs del sistema
/etc/nessus/nessusd.conf	Archivo de configuración de Nessus
/etc/proftpd.conf	Configuración del servidor ProFTPD
/etc/ftpusers	Usuarios del sistema que tienen permitido el acceso FTP
/etc/ypserv.conf	Configuración del servidor NIS
/etc/ypserv.securenets	Configura las IP que tienen permiso para usar el servidor NIS
/var/yp/Makefile	Configuración opciones servidor NIS y archivos a exportar
/var/yp/yp-servers	Listado de los servidores NIS secundarios de nuestro sistema
/etc/yp.conf	Configuración del cliente NIS
/etc/nsswitch	Archivos a importar del servidor NIS
/etc/resolv.conf	Contiene el nombre y la dirección IP de los servidores DNS
/etc/bind/db.lan	Añadir para los equipos de una LAN
/etc/bind/db.192.168.0	Añadir para el DNS inverso de una LAN
/etc/bind/named.conf	Configuración del servidor DNS BIND
/etc/bind/named.conf.local	Define zonas locales en el servidor DNS BIND
/etc/bind/named.conf.options	Define las opciones del servidor DNS BIND
/etc/samba/smb.conf	Configuración del servidor Samba
/etc/smbpasswd	Contiene los passwords de los usuarios Samba
/etc/smbusers	Contiene una lista de los usuarios del sistema y su correspondencia con su usuario Samba
/etc/lmhosts	Interfaz entre los nombres de maquinas NetBIOS y las direcciones IP numericas

Archivo	Descripción
/etc/printcap	Impresoras del sistema
/var/spool/samba	Cola de impresión, por defecto, en Samba
/var/spool/mail	Correo de los usuarios
/etc/dumpdates	Información de las copias de seguridad realizadas
/<particion>/quota.group	Archivos de configuración de quotas de grupo
/<particion>/quota.user	Archivos de configuración de quotas de usuario
/etc/exports	Archivo de configuración de NFS
/etc/jabber/jabber.xml	Archivo de configuración del servidor Jabber
/etc/printcap	Archivo de configuración de impresoras LPD
/etc/cups/cupsd.conf	Configuración del servidor Cups
/var/run/cups/printcap	Archivo de configuración de impresoras Cups
/var/spool/cups	Directorio donde se almacenan los archivos que se van a imprimir
/etc/apache/httpd.conf	Archivos de configuración de Apache
/etc/apache/modules.conf	
/etc/apache/access.conf	
/etc/apache/srm.conf	
/etc/apache/mime.types	
/etc/apache/conf.d/	Directorio de configuración de los módulos Apache
/etc/apache-ssl/*	Los mismos archivos de configuración, para Apache-SSL
/var/log/apache/*	Directorio donde se almacenan los logs, generados por Apache
/etc/webalizer.conf	Archivo de configuración de Webalizer
/var/www/webalizer	Reportes de estadisticas web
/etc/exim4/exim4.conf.template	Archivo de configuración de Exim4
/var/mail/<usuario>	Archivo de correo de los usuarios del sistema
/etc/mailname	Direcciones de correo locales
/etc/aliases	Alias de nombres de usuario
/etc/email-addresses	Direccion de correo del servidor
/etc/fetchmailrc	Archivo de configuración del servidor Fetchmail
~/.fetchmailrc	Archivo de configuración de usuario Fetchmail
/etc/courier/imapd	Archivo de configuración de courier-imap
/etc/courier/imapd.cnf	Opciones de courier-imap
/etc/courier/imapd-ssl	Opciones de courier-imap-ssl
~/.mailfilter	Configuración de usuario Maildrop
/etc/procmailrc	Archivo de configuración del servidor Procmail
~/.procmailrc	Archivo de configuración de usuario Procmail
/etc/clamav/clamd.conf	Archivo de configuración de ClamAV
/etc/default/spamassassin	Configuración del SpamAssassin
/etc/default/spampd	Configuración del demonio de SpamAssassin

Apéndice D

¿Por qué Debian no tiene *rc.local*?

A diferencia de otras distribuciones Linux, parece que Debian no usa *rc.local* (el archivo de configuración local) para el proceso de inicialización. Entonces, ¿qué facilidades suministra Debian para esta tarea?

Runlevels

Tradicionalmente en los sistemas UNIX/LINUX, cuando se inicia la máquina, el proceso "init" (que es ejecutado por el kernel cuando termina su arranque) ejecuta una serie de scripts de inicio, los cuales suelen encargarse de "setear" valores de configuración y ejecutar diversos programas.

Dicho proceso de arranque se separa en *runlevels*, que son simplemente números que identifican cada etapa, y en general van del 0 al 6, los números del 7 al 9 también están definidos pero no se suelen usar.

Hay una excepción, el *runlevel* **s**, que es el "single user mode", y se suele usar para tareas especiales de rescate y/o mantenimiento inesperado.

Hoy en día, las distribuciones manejan cada una sus scripts de arranque de forma particular, y muchas veces se manejan de forma alternativa sin tener *runlevels* claramente definidos como hasta hace unos años.

En algunas, se pueden encontrar los directorios */etc/rc#.d/*, donde # representa al número de *runlevel*; en otras están todos los scripts contenidos en */etc/rc.d* o en */etc/init.d*. Lo mas aconsejable en cada caso es consultar la documentación de cada distribución.

Podemos cofigurar gráficamente los scrips de RunLevel con la herramienta: `#ksysv`

Insertar un script en el arranque

Supongamos que un sistema necesita ejecutar el script *exemple* al inicializar, o al entrar en un *runlevel* en particular. Entonces el administrador del sistema debería:

- Colocar el script *exemple* en el directorio */etc/init.d/*
- Ejecutar la orden *update-rc.d* con los argumentos apropiados para preparar enlaces entre los directorios *rc?.d* (especificados desde la línea de comandos) y */etc/init.d/exemple*. Aquí, '?' es un número que corresponde a un *runlevel* estilo System V

La orden *update-rc.d*[1] creará enlaces entre ficheros en los directorios *rc?.d* y el script en */etc/init.d/*. Cada enlace comenzará con una 'S' o una 'K', seguida de un número, seguido por el nombre del script. Los scripts que comiencen con 'S' en */etc/rcN.d/* serán ejecutados al entrar al *runlevel N*. Los que lo hagan con con una 'K' serán ejecutados al dejar el *runlevel N*.

[1] Para tener disponible el comando *update-rc.d* hay que realizar un apt: #apt-get install rcconf

Uno podría, por ejemplo, obligar al script *exemple* a ejecutarse en el arranque, poniéndolo en */etc/init.d/* e instalando los enlaces con `#update-rc.d exemple defaults 19`. El argumento 'defaults' se refiere a los *runlevels* predeterminados, que son los que van del 2 al 5. El argumento '19' se asegura de que *exemple* sea llamado antes que cualquier otro script que contenga el número 20 o un número mayor.

Si necesitamos administra este tipo de archivos de runlevel podemos instalar con apt, el siguiente paquete: `#apt-get install rcconf`

Para ejecutarlo intruduciremos el comando: `#rcconf`

Mostrará un menú gráfico desde donde podremos habilitar o deshabilitar servicios en la carga inicial del sistema.

Insertar un script, mediante el asistente gráfico

Se pueden agregar scrips de forma gráfica, mediante nuestra herramienta de configuración web: Webmail. En la figura D.1 podemos observar el método para agregar un scrip nuevo.

Figura D.1: Interfaz gráfica Webmin para agregar Runlevels

Apéndice E

Puertos por defecto

El n.º de puertos a los que podemos acceder en cada hosts es de 65.536 (2^{16}). Estos puertos están divididos en tres secciones:

- *Los puertos IANA*: Son los 1024 primeros puertos del PC. La organización IANA (Internet Assigned Numbers Authority) adjudicó a cada uno de estos puertos una utilidad, protocolo,... para estandarizar la comunicación.
- *Los puertos Registrados*: Son aquellos comprendidos entre el 1.024 y el 49.151 asignados a protocolos, programas, ... Pero no se encuentran estandarizados.
- *Los puertos privados*: Son los que van del 49.152 y el 65.535. Sobre ellos no recae ningún uso particular y son utilizados para uso privado de los hosts y programas locales.

Si necesitamos más información, sobre la asignación de puertos la podemos consultar en la RFC1700 que data de Octubre de 1994, disponible en la dirección: *http://www.ietf.org/rfc/rfc1700.txt*.

También existe otro "malicioso" grupo de puertos, son los puertos por defecto de los troyanos. Se utilizan para establecer la comunicación servidor-cliente entre los ordenadores implicados en la misma. Al existir troyanos que permiten utilizar utilizar otros puertos , la identificación de los mismos puede no ser infalible, si bien la mayoría de los usuarios de troyanos no se molestan en cambiar los puertos y utilizan los puertos por defecto. Si necesitamos más información, en la siguiente página web podemos encontrar la mayoría de puertos de troyanos: *http://webs.ono.com/usr026/Agika2/2troyanos/puertos_troya.htm*

Y para terminar con esta sección, podemos observar los puertos que hemos utilizado en este proyecto:

Servicio	**Puerto**	**Servicio**	**Puerto**
FTP	21	SAMBA	901
SSH	22	NESSUS	1241
TELNET	23	RADIUS SERVER	1812
DNS	53 (UDP)	HORDE	2095
DHCP SERVIDOR	67 (UDP)	HORDE (SSL)	2096
DHCP CLIENTE	68 (UDP)	SQUID	3128
TFTP	69	JABBER CLIENTE	5222
WEB (HTTPS)	80	JABBER SERVIDOR	5269
HTTPS	443	WEBMIN	10000
CUPS	631		

Apéndice F

Manual del editor Vim (Vi mejorado)

Personalmente utilizo el editor Vim frente al editor Emacs, este último es más completo y tiene más opciones, pero no me son útiles. Prefiero un editor potente y a la vez simple (Vim es muy simple, una vez conocidos los comandos básicos).

Tiene dos modos de trabajo, el modo comando y el modo inserción. Me voy a centrar, principalmente en el modo comando debido al gran número de opciones disponibles.

Edición de ficheros

Para editar un fichero simplemente hay que hacer:

`$vi <archivo>`, ...en caso de que no exista se creará.

Modo inserción

Al editar un fichero entramos en el modo comando por defecto, si lo que queremos es entrar en el modo inserción, tenemos varias opciones:

- a: Añadir a partir del siguiente carácter
- i: Insertar a partir del carácter actual
- o: Insertar una línea debajo de la actual y comenzar allí la inserción

El modo inserción no tiene muchos secretos, se puede escribir lo que se quiera y luego volver al modo comando, pulsando la tecla *Esc*.

Modo comando

El modo comando del vim tiene multitud de opciones, pasemos a detallar las más utilizadas:

- u: Deshacer la última acción. Cabe destacar que en Vim, a diferencia de otros editores se pueden deshacer infinitos cambios, ya que esta opción no tiene límite
- CTRL+r: Rehace la última acción deshecha con "u"
- w: Guardar
- w!: Fuerza a guardar (es recomendable usar esta opción)

- q: Salir, si no se ha guardado bloquea la salida
- q!: Fuerza a salir sin guardar
- x: Guardar y salir
- x!: Guardar y salir, forzando la escritura.
- e fichero: Abre el fichero
- dd: Elimina la línea sobre la que está el cursor
- x: Suprime el carácter siguiente a donde esta el cursor
- <numero>yy: Copia una cantidad de líneas igual a número
- p: Pegar líneas
- /cadena: Busca 'cadena' en el texto sobre el que trabajamos
- n: nueva búsqueda sobre la última cadena especificada
- :<numero> : Va a la línea identificada por el número
- %s/cadena/nueva_cadena: Se usa para sustituir 'cadena' por 'nueva_cadena' en el texto, esta opción es especialmente útil
- r fichero: Vuelca el contenido de fichero sobre la posición actual del cursor
- !comando: Inserta la salida de un comando ejecutado. Por ejemplo si hacemos *!ls* inserta la salida de *ls* en nuestro fichero.
- . (punto): Repite el último comando

Personalización del Vim

Se puede personalizar Vim mediante un archivo de configuración, el *~/.vimrc*. En dicho fichero tenemos una serie de opciones que podemos activar o desactivar según lo que prefiramos, las principales son:

- syntax on: Activa el coloreado de sintaxis, muy útil para programadores
- set nobackup: Evita que se creén copias de seguridad cada vez que editemos un fichero
- set showmode: Muestra siempre en que modo estamos trabajando (comando o inserción)
- set ruler: Muestra una regla con información en la parte inferior de la consola
- set vb: Desactiva el molesto "pitido" y lo sustituye por un parpadeo de pantalla
- set ignorecase: No diferencia entre mayúsculas y minúsculas
- set showmatch: Es útil para realizar búsquedas, resaltará los resultados coincidentes con el patrón.
- `au BufReadPost * if line ("""")lexecute(normal'"")`|endif: Posiciona el cursor en donde se encontraba la última vez que editamos el fichero

Basado en un manual publicado en Todo-Linux, puede ser consultado en la siguiente dirección:

http://www.todo-linux.com/modules.php?name=News&file=article&sid=2162

Apéndice G

Guía rápida de IPTables

IPTables es una herramienta para filtrar paquetes del kernel (2.4x o posterior).

Comandos básicos

IPTables es la evolución de *ipchains* y *ipfwadm* y básicamente permite o rechaza los paquetes que llegan al host desde una red.

- Cadenas (chains) predefinidas:
  - INPUT: Los paquetes que llegan a nuestra máquina
  - OUTPUT: Los paquetes que salen de nuestra máquina
  - FORWARD: Los paquetes que atraviesan nuestra máquina
- Las opciones básicas:
  - -s: Especifica una dirección de origen
  - -d: Especifica una dirección de destino
  - --sport: Puerto de origen
  - --dport: Puerto de destino
  - --tcp-flags mascara activos: Flags permitidos (máscara) y flags activos
  - -m: Módulo de opciones (Vease `$man iptables`)
  - -f: Paquetes fragmentados
  - -t: Especifica la tabla (filter, nat o mangle)
  - -p: Especifica un protocolo
  - -i: Especifica un interface de entrada
  - -o: Especifica un interface de salida
  - -j: Especifica la acción a ejecutar sobre el paquete
- Acciones:
  - DROP: Elimina el paquete
  - LOG: Registra el paquete
  - REJECT: Rechaza el paquete
  - ACCEPT: Acepta el paquete

- Comandos fundamentales:
  - `iptables -L`, ... ver las reglas introducidas
  - `iptables -F`, ... borrar todas las reglas

Con `#man iptables` tenemos todas las opciones.

Ejemplos

- Eliminamos todas los paquetes de entrada y salida:

```
iptables -A INPUT -j DROP
iptables -A OUPUT -j DROP
```

- Aceptamos que se conecten a nuestro servidor Web(80) y FTP(21):

```
iptables -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -A INPUT -p TCP --dport 21 -j ACCEPT
```

- Permitimos la comunicación con el servidor DNS:

```
iptables -A INPUT -p udp --dport 53 -j ACCEPT
```

- Script muy básico de IPTables para dar acceso al 80 y al 22:

```
#!/bin/bash
# Permitimos que se conecten a nuestro servidor web y al ssh
iptables -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -A INPUT -p TCP --dport 22 -j ACCEPT
# Permitimos la comunicacion con el servidor dns
iptables -A INPUT -p udp --dport 53 -j ACCEPT
# Reglas basicas. Denegamos todas las entradas permitimos todas las salidas
iptables -A INPUT -j DROP
iptables -A OUTPUT -j ACCEPT
```

- Si queremos poner la máquina como firewall con dos interfaces de red, eth0 y eth1:
  - Activamos el ip_forward:
    `echo 1 > /proc/sys/net/ipv4/ip_forward`
  - Hacemos el NAT de las direcciones de fuera y permitimos la salida:

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
iptables -A FORWARD -o eth1 -i eth0 -j ACCEPT
```

  - Sólo permitimos que la red interna acceda a los puertos 25 y 80 de la red externa:

```
iptables -A FORWARD -s 192.168.0.0/24 -p TCP -j DROP
iptables -A FORWARD -s 192.168.0.0/24 -p TCP --dport 25 -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/24 -p TCP --dport 80 -j ACCEPT
```

- Si queremos hacer un proxy transparente para la salida de la red interna, es decir abrir un puerto de salida en el router:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport [puerto_externo]
         -j DNAT --to [IP_maquina]:[puerto_maquina]
```

- Si queremos denegar un rango concreto de IPs:

```
iptables -A INPUT -s 195.76.238.0/24 -j DROP
iptables -A INPUT -s 217.116.8.112/29 -j DROP
iptables -A INPUT -s 217.116.0.144 -j DROP
iptables -A INPUT -s 195.76.172.0/24 -j DROP
iptables -A INPUT -s 155.201.0.0/16 -j DROP
```

Debian Sarge, nueva versión estable

En el proyecto Debian, Sarge ha sido congelada y en breve será la nueva versión 'stable' de Debian. La versión testing pasara a llamarse Etch y será una versión real "en pruebas" ya que Sarge llevaba mucho tiempo entre los usuarios y ya esta muy probada.

Para tener nuestro servidor es necesario tener una versión estable y no en pruebas, hemos de modificar nuestro */etc/apt/sources.list* para que no nos cambie de versión automáticamente.

En estos momentos mi archivo /etc/apt/sources.list contiene las siguientes entradas:

```
deb http://ftp.rediris.es/debian testing main contrib non-free
deb-src http://ftp.rediris.es/debian/ testing main non-free contrib
deb http://ftp.rediris.es/debian-non-US testing/non-US main contrib non-free
deb-src http://ftp.rediris.es/debian-non-US testing/non-US main contrib non-free
deb http://security.debian.org/ testing/updates main contrib non-free
```

Para que mi sistema siga siendo Sarge, aunque dentro de unos días lo hará en la nueva etapa como estable, deberemos cambiarlo por este otro:

```
deb http://ftp.rediris.es/debian sarge main contrib non-free
deb-src http://ftp.rediris.es/debian/ sarge main non-free contrib
deb http://ftp.rediris.es/debian-non-US sarge/non-US main contrib non-free
deb-src http://ftp.rediris.es/debian-non-US sarge/non-US main contrib non-free
deb http://security.debian.org/ sarge/updates main contrib non-free
```

Y realizar un: `#apt-get update`

Si dejamos el archivo */etc/apt/sources.list* como "testing", nuestro sistema dejará de ser Sarge, y pasará a ser Etch.

También quería recordar que existe una tercera versión de Debian: *Debian Sid* o "unstable", que es la versin inestable. Esta versión siempre se llamará así: "Sid" y no es adecuada para el uso de servidores, ya que esta destinada a desarrollar el software que luego pasará al resto de versiones.

Desde la página oficial de Debian podemos obtener los siguientes datos:

- Desde el 3 de mayo de 2005, las actualizaciones de seguridad de la distribución "en pruebas" las gestiona el equipo de seguridad. Por tanto, esta distribución dispone de oportunas actualizaciones de seguridad. Esta situación es temporal, ya que la distribución en pruebas está congelada.
- La fecha de publicación, inicialmente prevista para el 30 Mayo, se ha pospuesto una semana, y pasa a ser el 6 de junio de 2005.
- Como es usual, las metas de la versin y la fecha en la que se hará pública no se determinan con antelación. En otras palabras, "Debian publica la nueva versión cuando es el momento de hacerlo".
- Los mayores cambios para Sarge incluyen reemplazar el antiguo sistema de instalación con discos flexibles, por el nuevo instalador de Debian, y usar GCC 3.3 como el nuevo compilador predeterminado en arquitecturas que hasta ahora usaban la versión 2.95. También se ha llevando a cabo la introducción de nuevas versiones de programas como son Perl 5.8 y XFree86 4.3.

Como despedida solo cabe decir, que acerte de pleno en la planificación y la elección de Debian Sarge fue primordial para que este documento sirva como ayuda durante un largo tiempo a los nuevos "administradores junior", sitio en el cual humildemente me ubico.

Licencia Creative Commons: Reconocimiento-CompartirIgual

Gracias a la Universidad de Barcelona y en particular a Ignasi Labastida i Juan y a la colaboración de un grupo de abogados de reconocido prestigio disponemos hoy por hoy de las licencias creative commons, no meramente traducidas al castellano y al catalán, sino también y sobre todo, adaptadas a la legislación española.

Con demasiada frecuencia, la visión sobre la protección de de obras creativas tiende a los extremos. Por una lado tenemos la concepción en la cual cualquier posible uso de una obra debe estar regulado al milímetro; cuyo máximo exponente en nuestro país quizá sea la cada vez menos querida SGAE

Por otro lado tenemos la anarquía total. Una visión en la que los creadores tienen total libertad para hacer lo que les dé la gana, pero en la que no tienen absolutamente ninguna protección.

Creative commons surge como una solución de compromiso entre ambas posturas. De esta forma, los creadores pueden elegir qué derechos quieren reservarse y qué usos de su obra quieren permitir. Así se construye una capa de protección que ofrece una alternativa razonable y flexible a la cada vez más restrictiva normativa en cuestión de propiedad intelectual.

En diciembre de 2002, Creative Commons lanza el primer conjunto de licencias, que cualquier a puede utilizar de forma completamente gratuita para proteger sus creaciones.

Las licencias de Creative Commons se inspiran en la licencia a GPL de la Fundación para el Software Libre; pero, al contrario ésta, las licencias Creative Commons no están pensadas para software, sino para otros tipos de trabajos creativos: páginas web, tesis doctorales, música, películas, fotografías, literatura, cursos ...

Como escoger una licencia

Para que la selección de licencias resulte fácil para todo el que quiera proteger sus obras sin necesidad de saber nada de Derecho, han creado una herramienta online, diponible en Castellano y Catalán que te permite ir eligiendo el tipo de protección que quieres para tu trabajo y en función de las opciones que escojas, te ofrece la licencia más adecuada.

- http://creativecommons.org/license/?lang=es, ... herramienta en castellano.
- http://creativecommons.org/license/?lang=ca, ... herramienta en catalán.

[0]Estos datos han sido obtenidos de la web http://www.elcuaderno.info, acogida a la licencia http://creativecommons.org//licenses/by-sa/2.0/, "Reconocimiento-CompartirIgual" la misma bajo la que se encuentra este proyecto, el autor no se cita al no figurar en el articulo.

Creative commons no supone renunciar a proteger tu trabajo, sino que implica que puedes escoger qué derechos prefieres reservarte y qué derechos quieres ceder a los demás.

Tú decides en qué condiciones estás dispuesto a permitir la utilización de tu trabajo, combinando las distintas condiciones que puedes imponer, hay hasta once tipos de licencias distintas de las que escoger (adaptadas a nuestra legislación, en este momento hay 6).

Estas son las condiciones que se pueden escoger:

- ***Attribution/Reconocimiento***: Permites que otras personas puedan copiar, distribuir y comunicar púlicamente la obra así como hacer obras derivadas, incluyendo el hacer un uso comercial de tu obra. Siempre que:
  - Te citen y te reconozcan como el autor original de la obra.
  - Al reutilizar o distribuir la obra, tienen que dejar bien claro los términos de la licencia la obra
- ***Noncommercial/No comercial***: Permites que otras personas puedan copiar, distribuir y comunicar púlicamente la obra así como hacer obras derivadas. Siempre que:
  - Te citen y te reconozcan como el autor original de la obra.
  - Al reutilizar o distribuir la obra, tienen que dejar bien claro los términos de la licencia la obra
  - No utilicen tu obra con fines comerciales
- ***No Derivative Works/Sin obra derivada***: Permites que otras personas puedan copiar, distribuir y comunicar púlicamente la obra, incluidos los posibles usos comerciales de la obra. Siempre qué:
  - Te citen y te reconozcan como el autor original de la obra.
  - Al reutilizar o distribuir la obra, tienen que dejar bien claro los términos de la licencia la obra
  - No se alterare, transforme o genere una obra derivada a partir de tu obra.
- ***Share Alike/Compartir igual***: Permites copiar, distribuir y comunicar púlicamente la obra, hacer obras derivadas y hacer un uso comercial de esta obra. La distribución de las obras derivadas se permite única y exclusivamente cuando la obra derivada utilice una licencia idéntica que la que tiene el trabajo original.

  No se pueden combinar las condiciones “compartir igual” y “sin obra derivada”, puesto que la condición “compartir igual” sólo es aplicable a las obras derivadas.

Una vez que has escogido las condiciones que quieres, accedes a la licencia apropiada de tres maneras:

- Resumen simple: Un resumen en un lenguaje simple que todo el mundo puede entender, junto con los iconos representativos de la licencia.
- Código legal: el texto completo de la licencia dirigido fundamentalmente a abogados.
- Código digital: Una versión de la licencia legible por máquinas que ayudará a las herramientas de búsqueda y otras aplicaciones a identificar tu trabajo en función de sus condiciones de uso.

Cómo se utiliza la licencia

Una vez elegida la licencia, obtendremos un código HTML, que una vez pegado en la página web generará un botón.

El botón "some rights reserved", indica que los contenidos del sitio web están protegidos por una licencia Creative commons. El botón enlaza con el resumen de la licencia que utilizas para proteger tus contenidos. De esta forma, comunicando públicamente los términos de tu licencia si alguien infringe los mismos, estás protegido jurídicamente y puedes interponer una demanda en defensa de tus derechos de propiedad intelectual.

Creative commons no es un bufete de abogados ni proporciona asesoramiento jurídico en caso de infringimiento de los términos de una licencia. Si se da el caso, tendrás que acudir a un abogado, los que yo conozco? Supongo que los mismos que todo el mundo: Javier Mestre y Carlos Sánchez Almeida del bufete Almeida (*http://www.bufetalmeida.com*). En la lista de correo sobre licencias creative commons en español, participan varios abogados, quizá allí puedes preguntar qué bufete hay cerca de dónde vives que esté especializado en estos temas.

Las seis posibles combinaciones adaptadas a la legislación española son:

1. Reconocimiento
2. Reconocimiento-SinObraDerivada
3. Reconocimiento-NoComercial-SinObraDerivada
4. Reconocimiento-NoComercial
5. Reconocimiento-NoComercial-CompartirIgual
6. Reconocimiento-CompartirIgual

Licencia escogida

Por el carácter abierto y libre de este proyecto, para elegir la licencia se voy a seguir el espíritu de GNU y sus licencias: GPL para software y GFDL (GNU Free Document) para documentación.

Por eso cedo el derecho de realizar una explotación económica de la obra, a condición de que, esa obra modificada o derivada este bajo la misma licencia que la primera y en ella se me cite como autor original.

Es decir, para el PFC: "Servidor Linux para conexiones seguras de una LAN a Internet", he escogido la licencia CC - "Reconocimiento-CompartirIgual".

La asignación de este tipo de licencia "Creative Common" respecto a GFDL, está justificada debido a que, en mi opinión, GFDL tiene un gran fallo, no permite realizar modificaciones de la obra y publicarlas bajo el mismo nombre y en mi caso, esta obra se deberá actualizar con el tiempo, ya sea por mí o por alguna otra persona que continúe el proyecto. No quiero que el PFC nazca y muera igual, prefiero donarlo a la comunidad y permitir que se pueda modificar y actualizar con el tiempo.

Creative Commons, me ha facilitado el siguiente párrafo para cualquier persona que necesite más información sobre la licencia:

"Esta obra está bajo la licencia de Atribución de Creative Commons: *Reconocimiento-CompartirIgual 2.1 España*. Para ver una copia de esta licencia, visite *http://creativecommons.org/licenses/by-sa/2.1/es/* o envie una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA."

Resumen simple de la licencia del PFC

Figura G.1: Licencia Reconocimiento-CompartirIgual

Esto es un resumen legible del texto legal, la licencia completa se encuentra disponible en la dirección: *http://creativecommons.org/licenses/by-sa/2.1/es/legalcode.es*

Páginas Web consultadas

http://acidlab.sourceforge.net/ - Consola de análisis de Bases de datos de intrusiones (ACID)
http://airsnort.shmoo.com/ - Web oficial de AirSnort
http://apostols.org/projectz/neped/ - Web oficial de NePED, detector de sniffers
http://barrapunto.com - Web de noticias sobre informática
http://bogofilter.sourceforge.net/ - Página web de Bogofilter
http://bulma.es - Comunidad de usuarios Linux, multitud de artículos
http://bulma.net/body.phtml?nIdNoticia=1334 - Manual de configuración DNS BIND 9.2.1
http://cauchy.bdat.net/dns/bind-9/DNS-HOWTO-9-es/ - DNS Como
http://certisign.com.br/servidores - Entidad de certificación
http://deim.etse.urv.es/ajuda/manuals/vi/ - Manual del vi
http://docs.kde.org/es/HEAD/kdegraphics/ksnapshot/ - Manual de KSnapshot
http://download.jabber.org/ - Pluggins para jabber
http://eia.udg.es/~atm/tcp-ip/index.html - Documentación sobre TCP/IP
http://enterprise.bidmc.harvard.edu/pub/nessus-php/ - Interfaz PHP para Nessus
http://es.tldp.org - Proyecto Lucas, documentación Linux en español
http://es.tldp.org/Tutoriales/NOVATO/novato-a-novato/novato-a-novato.html - Manual del novato
http://es.wikipedia.org - Wikipedia, la enciclopedia libre
http://gimp.hispalinux.es - Grupo de usuarios Españoles de GIMP
http://gsyc.escet.urjc.es/robotica/apuntes/captura_video_COMO.pdf - COMO capturar video
http://his.sourceforge.net/trad/honeynet/ - Proyecto HoneyNet en castellano
http://hostap.epitest.fi/wpa_supplicant/ - HowTo wpa_supplicant
http://httpd.apache.org/ - Apache HTTPD Server Project
http://kile.sourceforge.net/ - Web oficial Kile
http://latex2rtf.sourceforge.net/ - Convertidor de Latex a Rtf
http://laura.celdran.name/ - HowTos Laura Celdran
http://losinvisibles.net/como/como.html - Mini Como's de Simon
http://oriol.joor.net/article_fitxers/1574/WXP-WAP-EAPTLS.pdf - Conectar WinXP a Radius
http://packages.debian.org/testing/ - Guía completa de paquetes Debian Sarge
http://patux.glo.org.mx/imp-mini-como.html - HowTo sobre IMAP
http://prosper.sourceforge.net/ - Web oficial de Prosper
http://sourceforge.net/projects/airsnort - Proyecto SourceForge AirSnort
http://spamassassin.apache.org/ - Página web de SpamAssassin
http://tira.escomposlinux.org/ - Tira cómica Linux
http://tldp.org/HOWTO/html_single/8021X-HOWTO/ - HowTo 802.1x
http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/ - HowTo oficial de Samba
http://webadminmodules.sourceforge.net/ - Módulos para Webmin
http://webs.ono.com/usr026/Agika2/2troyanos/puertos_troya.htm - Puertos de Troyanos
http://www.apache.org/ - Página Web del Proyecto Apache
http://www.apache-ssl.org/ - Página Web del Proyecto Apache-SSL
http://www.bastille-linux.org - Web de Bastille Linux
http://www.bufetalmeida.com - Bufete Almeida, especializado en ciberderechos
http://www.canariaswardrive.org/ - 1.er campeonato de Wardriving en España
http://www.catb.org/ esr/fetchmail/ - Página web de Fetchmail

http://www.catcert.net/ - Agencia catalana de certificación
http://www.cert.org/ - Agencia seguridad en Internet CERT (Computer Emergency Response Team)
http://www.cervantex.org - Comunidad de usuarios españoles de TEX
http://www.chkrootkit.org/ - Web de chkrootkit
http://www.clamv.net - Web oficial del antivirus de correo ClamV
http://www.compuamersa.com/linux.htm - Sobre las distribuciones
http://www.courier-mta.org/ - Página web de Courier
http://www.cypherspace.org/openpgp/ - Implementaciones de OpenPGP
http://www.debian.org - Web oficial de Debian
http://www.debian.org/distrib/ - Métodos de la distribución Debian
http://www.debian.org/doc/ - Documentación rápida para Debian
http://www.debian.org/doc/manuals/apt-howto/index.es.html - APT HowTo, en español
http://www.debian.org/doc/manuals/securing-debian-howto/index.es.html - Manual de seguridad
http://www.digitalhermit.com/linux/Kernel-Build-HOWTO.html - Recompilación Kernel HowTo
http://www.distrowatch.com/index.php?language=ES - Todo sobre distribuciones
http://www.dslreports.com/forum/remark,9286052 mode=flat - Conectar WinXP a Radius (Ingles)
http://www.elcuaderno.info/ - Web de noticias
http://www.entrust.net - Entidad de certificación
http://www.escomposlinux.org/ - Grupos de noticias de Linux
http://www.exim.org/ - Página web de Exim
http://www.faqs.org/docs/iptables/index.html - Tutorial IPTables (Inglés)
http://www.freeradius.org/ - FreeRadius
http://www.gimp.org - Web oficial de The Gimp
http://www.gnome.org/ - Web de GNOME
http://www.gnupg.org - Web oficial de GnuPG
http://www.gwolf.org/seguridad/portsentry/ - Manual de uso PortSentry
http://www.gwolf.org/seguridad/logcheck/ - Manual de uso Logcheck
http://www.honeyd.org - Web oficial de Honeyd
http://www.horde.org/ - Página web de Horde
http://www.icewalkers.com/Linux/Howto/ - HowTos en español
http://www.ietf.org/rfc/rfc1700.txt - Puertos estandarizados por la IANA
http://www.iks-jena.de/produkte/ca - Entidad de certificación
http://www.imendio.com/projects/planner/ - Web oficial Planner
http://www.insecure.org/nmap/ - Escaner de puertos
http://www.isc.org/index.pl?/sw/bind/ - Página oficial de Bind
http://www.jabber.org/ - Página web oficial de Jabber
http://www.jabberes.org/ - Página de usuarios de Jabber españoles
http://www.kde.org/ - Web de KDE
http://www.kernel.org - Fuentes oficiales
http://www.kismetwireless.net - Web oficial Kismet Wireless
http://www.latex-project.org/ - Web oficial de LATEX
http://www.lids.org/ - Linux Intrusion Detection System
http://www.linux.cu/manual/basico-html/node120.html - Definición de tareas periódicas
http://www.linuxdocs.org - HowTos
http://www.linuxdocs.org/HOWTOs/Kernel-HOWTO.html - Kernel HowTo
http://www.linuxguruz.com/iptables/ - Manuales sobre IPTables
http://www.linuxlots.com/~barreiro/spain/cuota.html#toc1 - Cuotas de usuario
http://www.linuxzamora.org - Web de usuarios de Linux
http://www.llibreriaha.com/cas/index.asp - Librería técnica online de Barcelona
http://www.missl.cs.umd.edu/wireless/eaptls/ - HowTo EAP-TLS en WPA
http://www.nessus.org/ - Herramienta de búsqueda de vulnerabilidades
http://www.netfilter.org - Web oficial de IPTables
http://www.netsecuritysvcs.com/ncc/ - Herramienta gráfica para Nessus
http://www.nodedb.com/europe/es - Web de nodos wireless

http://www.openssh.org - Web de OpenSSH
http://www.packetfactory.net/Projects/sentinel/ - Web oficial de Sentinet, detector de sniffers
http://www.planetplanner.org/ - Comunidad de usuarios de Planner
http://www.procmail.org/ - Página web de Procmail
http://www.proftpd.org/ - Web oficial del proyecto ProFTPD
http://www.samba.org/samba/docs/ - Documentación sobre samba
http://www.snort.org - Web oficial de Snort
http://www.thawte.com - Entidad de certificación
http://www.tldp.org/HOWTO/BootPrompt-HOWTO.html - HowTo bootprompt en Debian Sarge
http://www.todo-linux.com/ - Manuales sobre linux
http://www.tripwire.org - Web oficial de Tripwire
http://www.verisign.com/site - Entidad de certificación VeriSign
http://www.webmin.com/ - Web de Webmin
http://www.wifimaps.com/ - Mapas de nodos wireless
http://www.xfree86.org/ - Web de XFree86
http://www.xombra.com - Articulos sobre Linux
http://www.zonagratuita.com/servicios/seguridad/snort.html - Snort + Acid en Windows
http://xvidcap.sourceforge.net - Proyecto Xvidcap