

Servicios

Introducción

Una regla básica de seguridad es mantener solamente los servicios que vayamos a utilizar, cada servicio conlleva una lista de vulnerabilidades y exploits mas o menos parcheadas y es por ello que es muy recomendable mantener solamente aquellos servicios necesarios.

Runlevels

Antes de configurar los servicios del sistema, debemos conocer los niveles de ejecución *runlevels* de cualquier sistema Linux. Un *runlevel* es un estado o modo de ejecución, con determinadas características que agura un número de servicios definido.

Los servicios que se ejecutan a cada *runlevel* se pueden consultar en el directorio correspondiente:

```
/etc/rc.d/rc<n>.d
```

Cambiando '<n>' por el número correspondiente

Los niveles de ejecución o *runlevels* existentes son

```
.0 . Halt  
.1 . Single-user mode  
.2 . Not used (user-de_nable)  
.3 . Full multi-user mode  
.4 . Not used (user-de_nable)  
.5 . Full multi-user mode (with an X-based login screen)  
.6 . Reboot
```

Cuando el sistema se encuentra en modo texto, estamos ejecutando el modo 3. Si por el contrario estamos usando un sistema de ventanas, ejecutamos el modo 5. Parece lógico que los servicios de un entorno texto serán muy distintos de los servicios que un sistema de ventanas.

Actuaciones

Se procede a listar y justificar los servicios prestados, aquellos que se consideres superfluos son desactivados.

ACAPI

El servicio ACPAPI (Advanced Configuration and Power Interface) es el encargado de manejar las funciones de ahorro de energía del sistema. Es recomendado mantenerlo activo para portátiles y la mayoría de equipos de sobremesa, aunque algunos servidores no lo necesitan.

De entre otros se encarga de las siguientes funcionalidades: *"Battery Monitor"*, *"Laptop Lid Switch"*, *"Laptop Display Brightness"*, *"Hibernate"*, *"Suspend"*, etc.

Activamos el servicio.

```
chkconfig --level 345 acpid on
```

ANACRON, ATD y CROND

Estos servicios son usados para ejecutar tareas, cada uno de ellos con un fin distinto. Es recomendado mantener el servicio crond activo, ya que su uso es muy frecuente y desactivamos los servicios atd y anacron.

Algunas tareas, como la limpieza de los directorios /tmp o /var requieren del servicio anacron. Debemos profundizar si se requiere o no el servicio atd

Activamos el servicio.

```
chkconfig --level 345 anacron on  
chkconfig --level 345 atd on  
chkconfig --level 345 crond on
```

AUTOFS

Es el servicio de montar en el sistema de archivos aquellos dispositivos removibles (CR-ROMs, Memorias USB, etc.).

Desactivamos este servicio.

```
chkconfig --level 345 autofs off
```

CAPI

Para aquellos usuarios con equipos ISDN (Integrated Services Digital Network).

Desactivamos el servicio

```
chkconfig --level 345 capi off
```

CPUSPEED

Este servicio monitoriza el uso de la CPU para economizar energis. Muchos equipos portátiles y los ordenadores actuales soportan estas funciones. Este resvicio debe activarse para *Pentium-M*, *Centrino*, *AMD PowerNow*, *Transmeta*, *Intel SpeedStep*, *Athlon-64*, *Athlon-X2*, *Intel Core 2*

Activamos el servicio

```
chkconfig --level 345 cpuspeed on
```

DC_CLIENT, DC_SERVER

Distcache (<http://distcache.sourceforge.net/>). El uso principal de este servicio res para las gestión de clusters con servidores SSL/TLS.

Desactivamos estos servicios

```
chkconfig --level 345 dc_client off  
chkconfig --level 345 dc_server off
```

DISKDUMP, NETDUMP

Diskdump es un servicio qua ayuda a realizar un debug de los fallos del kernel. Almacena un volcado de memoria o estado que luego puede ser analizado. Netdump tiene un funcionamiento similar pero a través de la red.

Es recomendado activarlo solo si estamor diagnosticando un problema

```
chkconfig --level 345 netdump off  
chkconfig --level 345 diskdump off
```

GPM

Este servicio se encarga de controlar el puntero del ratón fuera de el entorno de ventanas.

Es recomendado activarlo solo en modo texto.

```
chkconfig --level 3 gpm on  
chkconfig --level 45 gpm off
```

HALDAEMON

Activamos este servicio

```
chkconfig --level 345 haldaemon on
```

IP6TABLES

A no ser que se esté usando el protocolo IP6 para las conexiones de la web.

Deshabilitamos el servicio

```
chkconfig --level 2345 ip6tables off
```

IRDA

IrDA soporta comunicaciones infrarrojas entre dispositivos (laptops, PDA's, Teléfonos móviles, calculadoras, etc.).

Deshabilitamos este servicio

```
chkconfig --level 345 irda off
```

IRQBALANCE

Este servicio es para incrementar el rendimiento dentro de un sistema multiproceso. Sin embargo no se como afecta a los CPU's multinucleo (Intel Dual Core o Core 2 Duo)

Activamos para procesadores multinucleo

```
chkconfig --level 2345 irqbalance on
```

ISDN

Esta es otra forma de hardware/servicio de conexión a Internet.

A menos que el equipo disponga un módem ISDN, deshabilitamos el servicio

```
chkconfig --level 2345 isdn off
```

KUDZU

Este servicio se encarga de detectar y configurar el nuevo hardware conectado al equipo. Es recomendado desactivar este servicio y ejecutarlo únicamente cuando sea necesario.

```
chkconfig --level 345 kudzu off
```

MESSAGEBUS

Servicio para el manejo de las comunicaciones internas IPC (Interprocess Communication) Linux . Se encarga de el envío de mensajes entre aplicaciones del sistema.

Activamos este servicio

```
chkconfig --level 345 messagebus on
```

MCSTRANS

Este servicio es necesario para el funcionamiento de *SELinux*. Por defecto *SELinux* estará activo y por lo tanto es necesario.

Activamos este servicio

```
chkconfig --level 345 mcstrans on
```

MDMONITOR

Servicio para la monitorización del *Software RAID* o *LVM*. En nuestro caso, los servidores hacen uso del *Software RAID* para la redundancia de información, por lo que lo dejamos operativo.

Activamos este servicio.

```
chkconfig --level 345 mdmonitor on
```

MDMPD

Servicio para la monitorización de dispositivos *MultiPath*, de almacenamiento accesibles por más de un controlador

Desactivamos este servicio

```
chkconfig --level 345 mdmopd off
```

NETPLUGD

Este servicio monitoriza las tarjetas ethernet y ejecuta comandos cuando su estado varia

Desactivamos este servicio.

```
chkconfig --level 345 network off
```

NETFS

Servicio que monca cualquier sistema de archivos en red (NFS, Snmba, etc) en el momento de carga del sistema.

Desactivamos este servicio

```
chkconfig --level 345 netfs off
```

NETWORK

Activamos este servicio

```
chkconfig --level 345 network on
```

PCSCD

Da soporte sobre *Smart Cards* y lectores. Este tipo de tarjetas sirven para la autenticación y firma digital y están en los chips de atarjetas de crédito, tarjetas de identificación, etc.

Desactivamos este servicio

```
chkconfig --level 2345 pcscd off
```

PORTMAP

Servicio complementario al NFS (Network File System) y NIS (Autenticación). Si no hacemos uso de NFS, el servicio debe estar desactivado

Desactivamos este servicio

```
chkconfig --level 345 portmap off
```

READHEAD_EARLY, READHEAD_LATER

Mejoran la velocidad de carga del sistema manteniendo ciertas aplicaciones en memoria.

Activamos este servicio

```
chkconfig --level 2345 readhear_early on  
chkconfig --level 5 readhear_later on
```

RESTODECOND

Usado para monitorizar y restaurar file context para SELinux. No se requiere pero es muy recomendado tener este servicio activo si hacemos uso de SELinux.

Activamos este servicio

```
chkconfig --level 345 restorecond on
```

SENDMAIL

Servicio de MTA (Mail Transport Agent) por excelencia para la gestión del correo. Es útil para el envío de correo de root o notificaciones vía email del sistema.

Activamos este servicio

```
chkconfig --level 345 sendmail on
```

SYSLOG

Servicio para el registro de eventos del sistema a través de logs de sistemas. E

Activamos este servicio

```
chkconfig --level 345 syslog on
```

SMART

El servicio SMART para la monitorización del disco es útil para prever fallos de hardware.

Activamos este servicio

```
chkconfig --level 345 sendmail on
```

Verificación

Verificamos cuáles servicios están activos

Tras haber resuelto aquellos servicios indispensables para el sistema comprobamos la tabla de servicios en los niveles de carga del sistema runlevels.

```
chkconfig --list
```

Deberíamos obtener una lista como la siguiente:

acpid	0:off	1:off	2:off	3:on	4:on	5:on	6:off
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off
atd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
autofs	0:off	1:off	2:off	3:off	4:off	5:off	6:off
capi	0:off	1:off	2:off	3:off	4:off	5:off	6:off
cpuspeed	0:off	1:on	2:on	3:on	4:on	5:on	6:off
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
dc_client	0:off	1:off	2:off	3:off	4:off	5:off	6:off
dc_server	0:off	1:off	2:off	3:off	4:off	5:off	6:off
diskdump	0:off	1:off	2:off	3:off	4:off	5:off	6:off
gpm	0:off	1:off	2:on	3:on	4:off	5:off	6:off
haldaemon	0:off	1:off	2:off	3:on	4:on	5:on	6:off
httpd	0:off	1:off	2:off	3:on	4:off	5:off	6:off
ip6tables	0:off	1:off	2:off	3:off	4:off	5:off	6:off
irda	0:off	1:off	2:off	3:off	4:off	5:off	6:off
irqbalance	0:off	1:off	2:on	3:on	4:on	5:on	6:off
isdn	0:off	1:off	2:off	3:off	4:off	5:off	6:off
kudzu	0:off	1:off	2:off	3:off	4:off	5:off	6:off
mcstrans	0:off	1:off	2:on	3:on	4:on	5:on	6:off
mdmonitor	0:off	1:off	2:on	3:on	4:on	5:on	6:off
mdmpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
messagebus	0:off	1:off	2:off	3:on	4:on	5:on	6:off
microcode_ctl	0:off	1:off	2:off	3:off	4:off	5:off	6:off
multipathd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
netdump	0:off	1:off	2:off	3:off	4:off	5:off	6:off
netfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off
netplugd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
network	0:off	1:off	2:on	3:on	4:on	5:on	6:off
nscd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
pcscd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
portmap	0:off	1:off	2:off	3:off	4:off	5:off	6:off
psacct	0:off	1:off	2:off	3:off	4:off	5:off	6:off
rdisc	0:off	1:off	2:off	3:off	4:off	5:off	6:off
readahead_early	0:off	1:off	2:on	3:on	4:on	5:on	6:off
readahead_later	0:off	1:off	2:off	3:off	4:off	5:on	6:off
restorecond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
saslauthd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off
smartd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
sshd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
syslog	0:off	1:off	2:on	3:on	4:on	5:on	6:off
vsftpd	0:off	1:off	2:off	3:on	4:off	5:off	6:off

webmin	0:off	1:off	2:on	3:on	4:off	5:on	6:off
wpa_supplicant	0:off	1:off	2:off	3:off	4:off	5:off	6:off
ypbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off
yum-updatesd	0:off	1:off	2:off	3:on	4:on	5:on	6:off

Como referencia indicamos también en este pequeño manual los servicios asignados por defecto

acpid	0:off	1:off	2:off	3:on	4:on	5:on	6:off
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off
atd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
autofs	0:off	1:off	2:off	3:on	4:on	5:on	6:off
capi	0:off	1:off	2:off	3:off	4:off	5:off	6:off
cpuspeed	0:off	1:on	2:on	3:on	4:on	5:on	6:off
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
dc_client	0:off	1:off	2:off	3:off	4:off	5:off	6:off
dc_server	0:off	1:off	2:off	3:off	4:off	5:off	6:off
diskdump	0:off	1:off	2:off	3:off	4:off	5:off	6:off
gpm	0:off	1:off	2:on	3:on	4:on	5:on	6:off
haldaemon	0:off	1:off	2:off	3:on	4:on	5:on	6:off
httpd	0:off	1:off	2:off	3:on	4:off	5:off	6:off
ip6tables	0:off	1:off	2:on	3:on	4:on	5:on	6:off
iptables	0:off	1:off	2:on	3:on	4:on	5:on	6:off
irda	0:off	1:off	2:off	3:off	4:off	5:off	6:off
irqbalance	0:off	1:off	2:on	3:on	4:on	5:on	6:off
isdn	0:off	1:off	2:on	3:on	4:on	5:on	6:off
kudzu	0:off	1:off	2:off	3:on	4:on	5:on	6:off
mcstrans	0:off	1:off	2:on	3:on	4:on	5:on	6:off
mdmonitor	0:off	1:off	2:on	3:on	4:on	5:on	6:off
mdmpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
messagebus	0:off	1:off	2:off	3:on	4:on	5:on	6:off
microcode_ctl	0:off	1:off	2:off	3:off	4:off	5:off	6:off
multipathd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
netdump	0:off	1:off	2:off	3:off	4:off	5:off	6:off
netfs	0:off	1:off	2:off	3:on	4:on	5:on	6:off
netplugd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
network	0:off	1:off	2:on	3:on	4:on	5:on	6:off
nscd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
pcscd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
portmap	0:off	1:off	2:off	3:on	4:on	5:on	6:off
psacct	0:off	1:off	2:off	3:off	4:off	5:off	6:off
rdisc	0:off	1:off	2:off	3:off	4:off	5:off	6:off
readahead_early	0:off	1:off	2:on	3:on	4:on	5:on	6:off
readahead_later	0:off	1:off	2:off	3:off	4:off	5:on	6:off
restorecond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
saslauthd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off
smartd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
sshd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
syslog	0:off	1:off	2:on	3:on	4:on	5:on	6:off
vsftpd	0:off	1:off	2:off	3:on	4:off	5:off	6:off
webmin	0:off	1:off	2:on	3:on	4:off	5:on	6:off
wpa_supplicant	0:off	1:off	2:off	3:off	4:off	5:off	6:off
ypbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off
yum-updatesd	0:off	1:off	2:off	3:on	4:on	5:on	6:off

Verificar puertos abiertos

Otra medida para verificar los servicios activos del sistema es comprobar que puertos están abiertos en realidad sobre las interfaces del sistema. Cualquier puerto abierto puede ser una evidencia de un servicio operativo o incluso de una intrusión.

La forma mas confiable de verificar que puertos están escuchando en la red es usar un escáner de puertos tal como *nmap*. La aplicación *nmap* puede usarse de forma remota pero es bueno complementar el resultado obtenido con una ejecución local ya que el servicio *iptables* puede distorsionar o ocultar los puertos abiertos reales.

Si el equipo no dispone de *nmap* , procedemos a su instalación

```
yum install nmap
```

Ejecutamos el comando siguiente para determinar que puertos están escuchando por conexiones TCP desde la red.

```
nmap -sT -O localhost
```

-sT <i>TCP connect</i>	Usa la llamada al sistema connect para intentar una conexión a un puerto, si no es posible, ese puerto no esta abierto.
-O	Intenta descubrir que sistema operativo se está ejecutando.

Es resultado debería ser parecido al siguiente:

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-04-17
15:04 CEST
Interesting ports on patagon.iddover.net (127.0.0.1):
Not shown: 1675 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
No exact OS matches for host (If you know what OS is running on it,
see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
...
Uptime 0.020 days (since Tue Apr 17 14:36:02 2007)
Nmap finished: 1 IP address (1 host up) scanned in 9.576 seconds
```

El resultado de escaneo es más que positivo ya que *nmap* no ha logrado detectar el sistema operativo que se está ejecutando y nos revela que

solamente existen 5 puertos (y servicios) que se están ejecutando. Sin embargo existe un puerto que nos podría parecer desconocido y que en un escaneo externo no saldría reflejado.

Para verificar si el puerto está asociado con la lista oficial de servicios conocidos, escribimos:

```
cat /etc/services | grep 25
```

La primera línea de la lista normalmente revelará el servicio al que se asocia, sin embargo también podría no tener ningún servicio conocido asociado.

En nuestro caso la salida es la siguiente:

```
smtp          25/tcp      mail
smtp          25/udp      mail
```

Por ahora conocemos que está relacionado con el servicio de correo, por lo que podríamos deducir que se trata del sendmail, pero para verificar la información sobre el proceso que tiene asignado el puerto usamos el comando *netstat*.

Tanto la aplicación *nmap* como *netstat* puede ser muy útil para la resolución ágil de problemas por la que si el servidor no dispone de ella deberíamos instalarlas.

```
netstat -anp | grep :25
```

-a	Muestra aquellos servicios que están simplemente a la escucha aunque no hayan establecido conexión
-n	Muestra las direcciones IP sin tratar de resolver el nombre de dominio (mediante un reverse dns)
-p	Revela el identificador de proceso (PID) del servicio que abrió el puerto.

El comando anterior nos devuelve lo siguiente

```
tcp 0 0 127.0.0.1:25 0.0.0.0:*          LISTEN          2489/sendmail: acce
```

Como ya habíamos deducido, netstat nos revela que es la aplicación sendmail la que está haciendo uso del puerto 25.

Para el mismo fin también se puede usar el comando *lsof*. Este comando muestra archivos del sistema que estén siendo utilizados por procesos activos.

```
sendmail 2489 root 4u IPv4 8285 TCP patagon.iddover.net:smtp (LISTEN)
```

No obstante hay algo que no es del todo correcto en esta salida y es que como vemos, el servicio está a la escucha de cualquier dirección IP y si el equipo no

es un servidor de correo debería limitar el acceso solamente a la interficie local 127.0.0.0. Esta medida se explica en el apartado referente al servicio sendmail.

Referencias

Para ampliar información consulta las siguientes referencias:

<http://www.redhat.com/docs/manuals>

<http://www.mjmwired.net/resources/mjm-services-fc6.html>

¿Que es iddover.net?

Iddover Hosting es una iniciativa española en el sector de servidores dedicados. Nace en contraposición de los servicios actuales de hosting . Pretende ofrecer un hosting de alta calidad gestionable a través de un potente panel propio que se adecua a los requisitos de seguridad y que proporciona al cliente potentes herramientas al alcance de un solo click

Desde 69€ dispondrás de un servidor dedicado administrado auditado con todas las medidas de seguridad ya aplicadas.

<http://www.iddover.net>