

Seguridad en GNU/Linux



Matias Katz

Mail: matias@matiaskatz.com

Blog: www.matiaskatz.com

Twitter: [@matiaskatz](https://twitter.com/matiaskatz)



Contenido :



Seguridad en Usuarios y Control de Acceso



Encriptación e integridad de datos



Mantenimiento y lectura de Logs



Backup

Qué tan seguro es esto???

```
debian login: _
```



Problemáticas



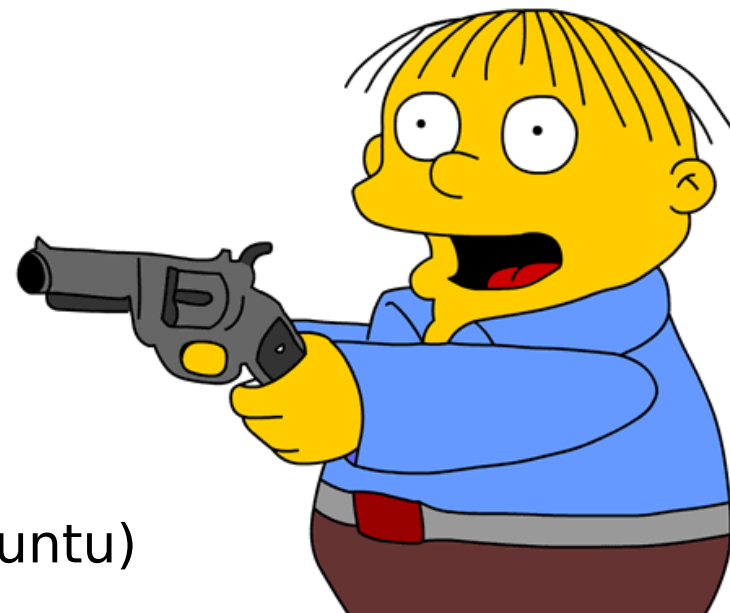
Root habilitado (salvo en Ubuntu)



Múltiples consolas habilitadas



“Recuperación de PWD” fácilmente realizable





“Root” es más fuerte que “Administrador”



Puede modificar el core del sistema



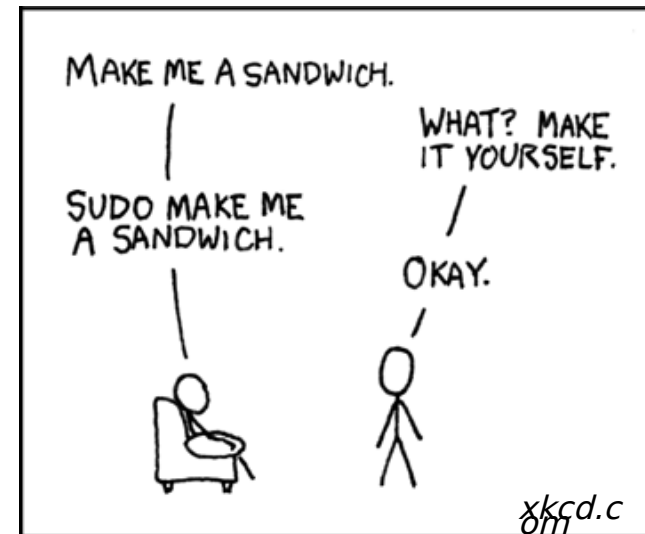
No debería usarse como login principal



Aún así, está habilitado por default (salvo en Ubuntu)



Contramedidas



- Ponerle un PWD fuerte (passwd root)
- Deshabilitar la cuenta (usermod -p '!' root)
- Habilitar SUDO (apt-get install sudo y editar /etc/sudoers)
- Superusuario secundario (adduser root2 | cambiar a 0:0)



Linux permite múltiples consolas de login





- Por default, existen 6 consolas paralelas (tty)
- El usuario común utiliza sólo el login gráfico, o 1 tty más
- Permitiría un login secundario no autorizado
- Root puede hacer login desde cualquiera



Contramedidas

- Limitar las consolas al mínimo necesario
 - (editar `/etc/default/console-setup` y `/etc/inittab`)
- Limitar las consolas con root login (editar `/etc/securetty`)

“*Recovery Console*”... “*Hacking Console*” 😊

-  Por default instalado y habilitado en el boot
-  Permite acceder al 100% del filesystem
-  Permite ingresar con privilegios de Root
-  El login es muy fácilmente bypassable



Contramedidas



Eliminar la Recovery Console



Encriptar el acceso al boot loader:



En Grub (grub-md5-crypt)



En Lilo (/etc/lilo.conf)

Tu información está realmente protegida???



Fuente: @SCavanna



Problemáticas



Filesystems sin encriptación



Violaciones de Confidencialidad



Violaciones de Integridad



Un sistema es tan fuerte como su eslabón más debil



La protección del sistema operativo es escasa



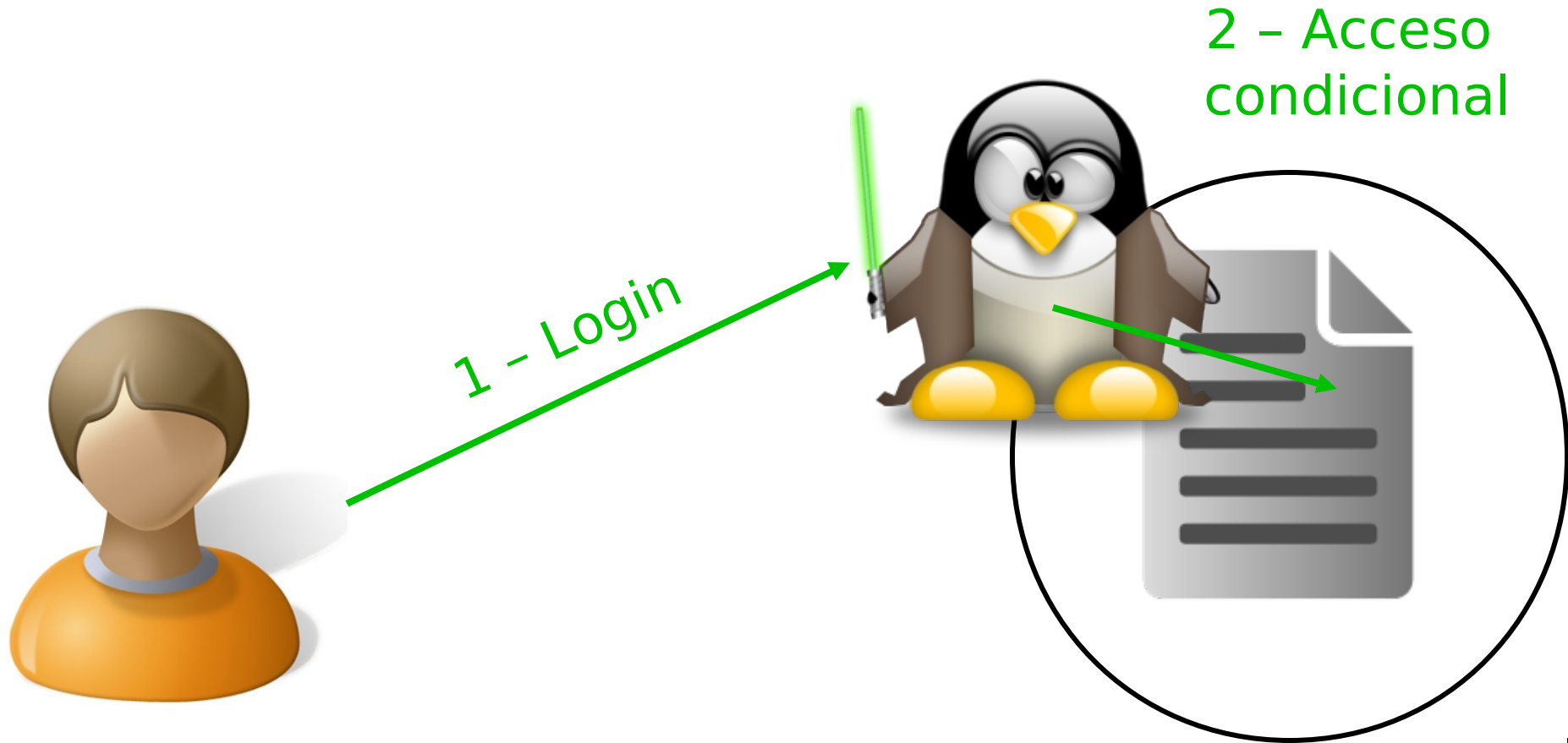
Se limita a los dominios de control del OS



Utilizando otro OS, se elimina la protección



Dominio de protección del OS





Bypass de la protección del OS



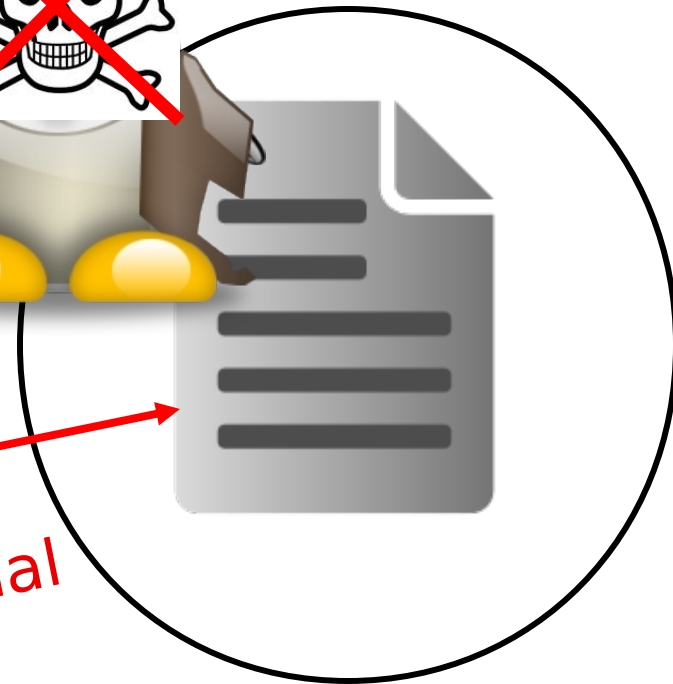
1 - Login



2 - Acceso incondicional



3 - Control Anulado





Violaciones de confidencialidad



Acceso a información privada dentro del disco



Adquisición de valores hash de passwords de sistema



El atacante tendrá acceso autorizado al sistema



Indetectable y eterno si no cambian los PWDs



Violaciones de integridad



Alteración directa del contenido del disco



Modificación de información importante



Inyección de malware



Creación de nuevos superusuarios escondidos



Contramedidas

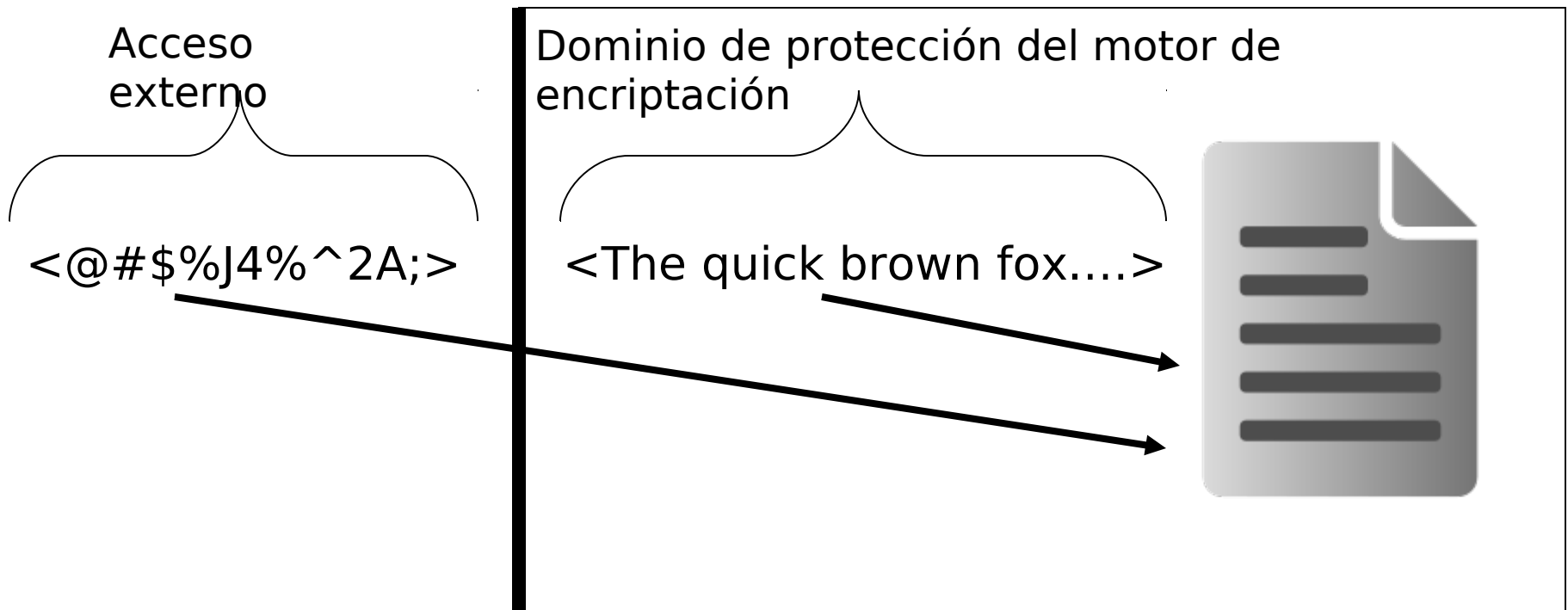


Encriptación de información (o del disco entero)

- Por hardware (si está disponible)
- Vía el OS (LUKS, Linux Unified Key Setup)
- Truecrypt (www.truecrypt.org)



Encriptación - Modus Operandi



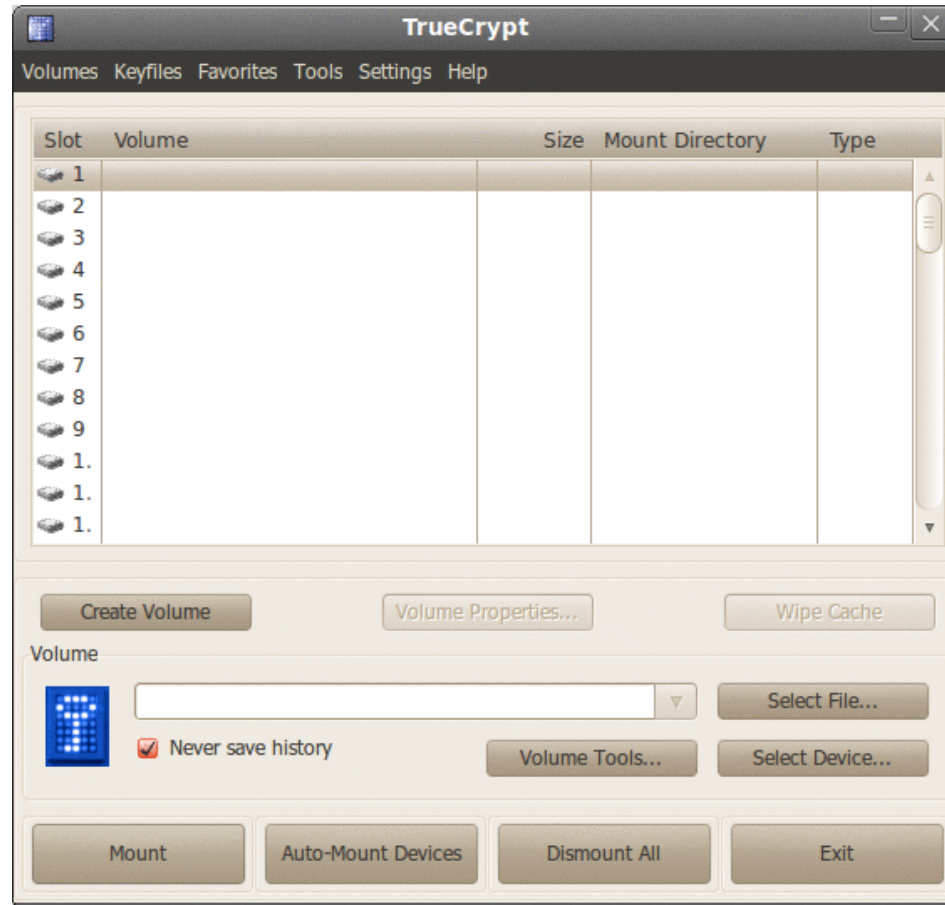


Encriptación vía OS (en la instalación)

```
Guided - use entire disk  
Guided - use entire disk and set up LVM  
Guided - use entire disk and set up encrypted LVM  
Manual
```



Encriptación vía Truecrypt



Sabes lo que pasa en tu equipo???



✓ Problemáticas



- NADIE NADIE NADIE LEE NUNCA LOS LOGS
- NADIE NADIE NADIE LEE NUNCA LOS LOGS
- NADIE NADIE NADIE LEE NUNCA LOS LOGS 😊



Lectura de Logs

- TODA la actividad en nuestro equipo se guarda en los logs
- Casi todas las intrusiones recién listadas se podrían identificar
- Como método detectivo son excelentes herramientas



Contramedidas

- Implementar auditorías críticas de sistema (auditd)
- Leer los últimos eventos (`tail /var/log/xxx`)
- Utilizar tools de OS (ps, Gnome Monitor, netstat, tcpdump)
- Utilizar herramientas de terceros (logwatch, logcheck)



Uso del auditd

```
7 14:52:59.985:55) : name=/etc/passwd flags=follow,open inode=23087346 dev=08:02 mode=
14:52:59.985:55) : cwd=/webroot/home/lighttpd
/2007 14:52:59.985:55) : inode=23087346 inode_uid=root inode_gid=root inode_dev=08:02
/2007 14:52:59.985:55) : watch_inode=23087346 watch=password filterkey=password-file per
2007 14:52:59.985:55) : arch=x86_64 syscall=open success=yes exit=3 a0=7fbffffcb4 a1=0
```




Uso del logwatch

```
##### Logwatch 7.3 (03/24/06) #####
Processing Initiated: Fri Oct 30 04:02:03 2009
Date Range Processed: yesterday
                    ( 2009-Oct-29 )
                    Period is day.
Detail Level of Output: 0
Type of Output: unformatted
Logfiles for Host: www-52.nixcraft.net.in
#####

----- Named Begin -----

**Unmatched Entries**
general: info: zone XXXXXX.com/IN: Transfer started.: 3 Time(s)
general: info: zone XXXXXX.com/IN: refresh: retry limit for master ttttttttttt
general: info: zone XXXXXX.com/IN: Transfer started.: 4 Time(s)
general: info: zone XXXXXX.com/IN: refresh: retry limit for master ttttttttttt

----- Named End -----

----- iptables firewall Begin -----

Logged 87 packets on interface eth0
From 58.y.xxx.ww - 1 packet to tcp(8080)
From 59.www.zzz.yyy - 1 packet to tcp(22)
From 60.32.nnn.yyy - 2 packets to tcp(45633)
From 222.xxx.ttt.zz - 5 packets to tcp(8000,8080,8800)

----- iptables firewall End -----
```

Nunca pasa nada.... hasta que pasa.





Problemáticas

- NADIE NADIE NADIE REALIZA BACKUPS NUNCA
- NADIE NADIE NADIE REALIZA BACKUPS NUNCA
- Creo que ya entendieron 😊





Realizar backups






- ✓ Nos salvan la vida en caso de catástrofe
- ✓ Nos salvan la vida en caso de error humano
- ✓ En fin, nos salvan la vida
- ✓ Lo mejor es que es muy fácil y rápido realizarlos
- ✓ Encima de todo, se pueden automatizar



Qué backupear?

- Tus archivos personales (~/.documents, ~/.desktop, etcétera)
- Archivos ocultos (~/.gnome, ~/.kde, ~/.profile, etcétera)
- Configuraciones de sistema (/etc completo, se necesita root)
- Archivos de booteo (/boot)
- No olvidarse de encriptar los backups también!

Cuándo backupearlo?

-  Todos los días
-  Cada 3 días
-  1 vez por semana
-  1 vez por quincena
-  Más no 😊

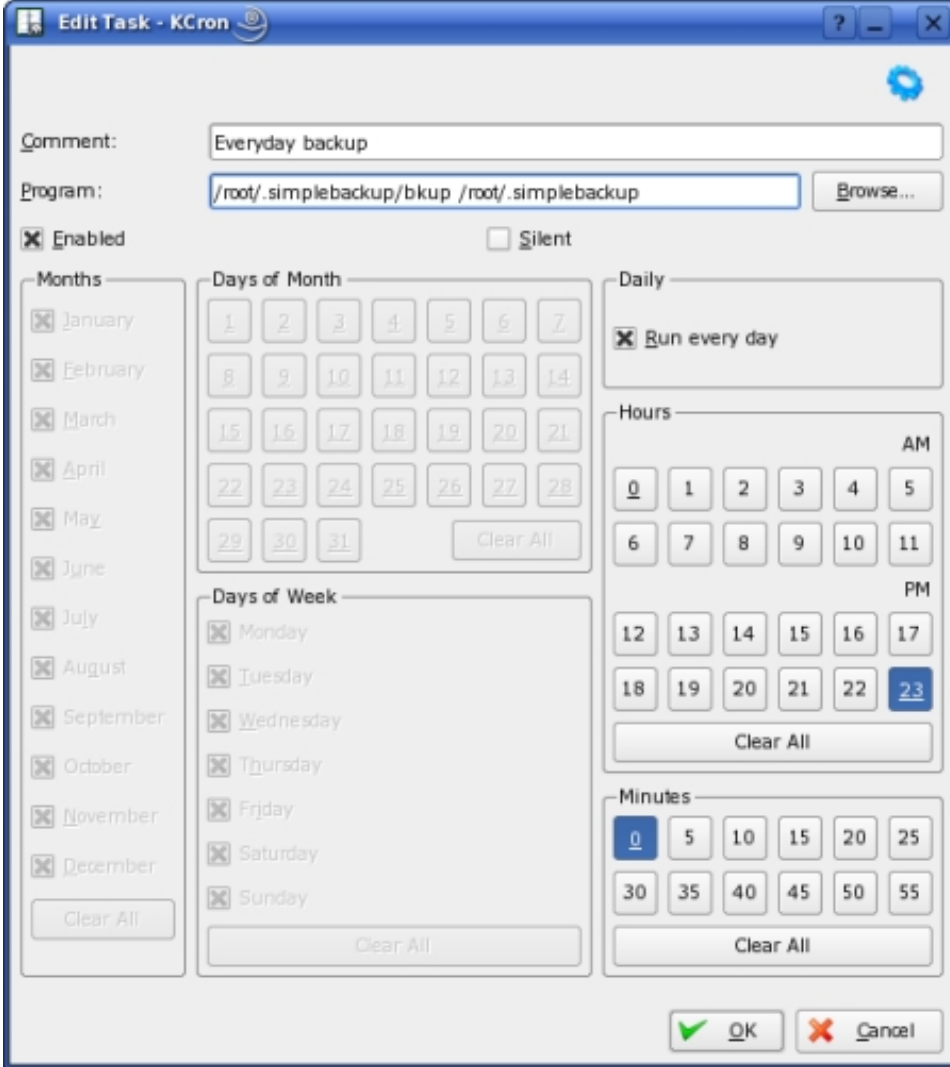


Cómo backupearlo?

- Copiar manualmente los directorios en cada ocasión
- Armar una tarea programada (cron, kcron, gnome-schedule)
- Utilizar herramientas avanzadas (AMANDA, afbackup, bacula)
- Realizar imágenes de disco en frío (PING)



Uso de KCron



Edit Task - KCron

Comment:

Program:

Enabled Silent

Months

- January
- February
- March
- April
- May
- June
- July
- August
- September
- October
- November
- December

Days of Month

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	<input type="button" value="Clear All"/>			

Days of Week

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

Daily

Run every day

Hours

0	1	2	3	4	5	AM
6	7	8	9	10	11	
12	13	14	15	16	17	PM
18	19	20	21	22	23	

Minutes

0	5	10	15	20	25
30	35	40	45	50	55



Uso de Bacula

The screenshot shows the 'bat - Bacula Admin Tool' window. On the left is a 'Select Page' sidebar with options like Console, Clients, FileSets, Jobs, JobList, JobPlot, Media, Storage, and Version Browser. The 'Media' page is selected. The main area displays a table of storage pools and their volumes.

Volume Name	Id	Status	Enabled	Bytes	Files	Jobs	Retention	Media Type	Slot	Use Dur
Pools										
TapePool										
TYV236L2	3	Full	1	239479467236	424	363	31536000	LTO-G2	9	0
TYV238L2	5	Append	1	100134236160	279	260	31536000	LTO-G2	0	0
TYV239L2	1	Append	1	1	0	0	31536000	LTO-G2	11	0
DiskPool										
File0003	4	Append	1	0	0	0	31536000	File	0	0
File002	2	Error	1	122001	0	305	31536000	File	0	0

At the bottom, there is a 'Console Command Line Entry' field with the text 'Command: ' and 'At main prompt waiting for input ...' below it.



Usos de PING (Partimage Is Not Ghost)

```

Partition Image 0.6.0-rc2
* Partition to save/restore
sda1                -extended-                #
sda5                jfs                150.98 MB
sda6                jfs                150.98 MB
sda7                xfs                149.98 MB
sda8                reiserfs-3.5      149.98 MB
hda1                ntfs                1.95 GB
hda2                -extended-

* Image file to create/use
/mnt/backup/linux-redhat-7.1.partimg.gz

Action to be done:
(*) Save partition into a new image file
( ) Restore partition from an image file
( ) Restore an MBR from the imagefile

[X] Connect to server
   IP/name of the server: 192.168.10.2 Port: 13000
   SSL disabled at compile time
  
```

Todo está a un *apt-get* de distancia.

(también se acepta *yum* 😊)

Seguridad en GNU/Linux



Matias Katz

Mail: matias@matiaskatz.com

Blog: www.matiaskatz.com

Twitter: [@matiaskatz](https://twitter.com/matiaskatz)

Preguntas ?