

## EJERCICIOS - HARDENING

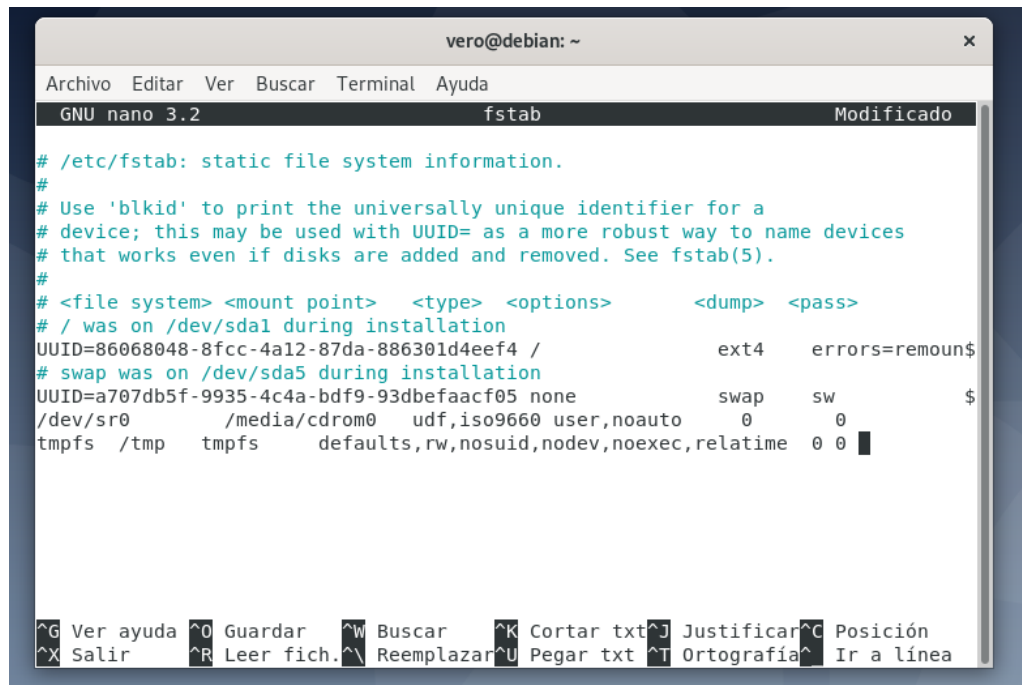
### Prerrequisitos

- Instala la máquina virtual virtual Debian 10 o Debian 11 en VirtualBox

### Ejercicios

Realiza las siguientes tareas de hardening o bastionado sobre la máquina Debian, siguiendo las instrucciones de la guía CIS Benchmark:

#### 1.1.2 Ensure /tmp is configured (Scored)



The screenshot shows a terminal window titled 'vero@debian: ~' with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda) and a status bar (GNU nano 3.2, fstab, Modificado). The main content is the /etc/fstab file, which contains static file system information. The file is being edited in nano, and the cursor is at the end of the line for the /tmp directory. The file content is as follows:

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options>      <dump> <pass>
# / was on /dev/sdal during installation
UUID=86068048-8fcc-4a12-87da-886301d4eef4 /      ext4      errors=remoun$
# swap was on /dev/sda5 during installation
UUID=a707db5f-9935-4c4a-bdf9-93dbefaacf05 none    swap      sw         $
/dev/sr0      /media/cdrom0  udf,iso9660 user,noauto 0      0
tmpfs /tmp      tmpfs      defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

The status bar at the bottom shows various keyboard shortcuts for nano, such as ^G Ver ayuda, ^O Guardar, ^W Buscar, ^K Cortar txt, ^J Justificar, ^C Posición, ^X Salir, ^R Leer fich., ^\ Reemplazar, ^U Pegar txt, ^T Ortografía, and ^\_ Ir a línea.

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=86068048-8fcc-4a12-87da-886301d4eef4 / ext4 errors=remount
-ro 0 1
# swap was on /dev/sda5 during installation
UUID=a707db5f-9935-4c4a-bdf9-93dbefaacf05 none swap sw
0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
root@debian:/etc# mount -a
root@debian:/etc# dr -Th
bash: dr: orden no encontrada
root@debian:/etc# df -Th
S.ficheros Tipo Tamaño Usados Disp Uso% Montado en
udev devtmpfs 1,5G 0 1,5G 0% /dev
tmpfs tmpfs 301M 4,9M 296M 2% /run
/dev/sda1 ext4 37G 4,2G 31G 13% /
tmpfs tmpfs 1,5G 0 1,5G 0% /dev/shm
tmpfs tmpfs 5,0M 4,0K 5,0M 1% /run/lock
tmpfs tmpfs 1,5G 0 1,5G 0% /sys/fs/cgroup
tmpfs tmpfs 301M 4,6M 296M 2% /run/user/1000
tmpfs tmpfs 1,5G 0 1,5G 0% /tmp
root@debian:/etc#
```

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/# cd /etc
root@debian:/etc# cat fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=86068048-8fcc-4a12-87da-886301d4eef4 / ext4 errors=remount
-ro 0 1
# swap was on /dev/sda5 during installation
UUID=a707db5f-9935-4c4a-bdf9-93dbefaacf05 none swap sw
0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
root@debian:/etc# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
root@debian:/etc# mount | grep -E '\s/tmp\s'
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
root@debian:/etc# grep -E '\s/tmp\s' /etc/fstab | grep -E -v '^#\s*'
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
root@debian:/etc#
```

No tengo exactamente en las mismas rutas pero demuestro que la configuracion esta bien

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
tk-3.0 polkit-1
oot@debian:/etc# cd systemd
oot@debian:/etc/systemd# ls
ournald.conf networkd.conf system user
ogind.conf resolved.conf system.conf user.conf
etwork sleep.conf timesyncd.conf
oot@debian:/etc/systemd# cd system
oot@debian:/etc/systemd/system# ls
luetooth.target.wants graphical.target.wants
bus-fi.wl.wpa_supplicant1.service multi-user.target.wants
bus-org.bluez.service network-online.target.wants
bus-org.freedesktop.Avahi.service printer.target.wants
bus-org.freedesktop.ModemManager1.service sockets.target.wants
bus-org.freedesktop.nm-dispatcher.service sysinit.target.wants
bus-org.freedesktop.timesync1.service syslog.service
isplay-manager.service timers.target.wants
etty.target.wants
oot@debian:/etc/systemd/system# cd /run/systemd/generator
oot@debian:/run/systemd/generator# ls
dev-disk-by\x2duuid-a707db5f\x2d9935\x2d4c4a\x2dbdf9\x2d93dbefaacf05.swap'
local-fs.target.requires
local-fs.target.wants
media-cdrom0.mount
-.mount
```

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/run/systemd/generator# ls
'dev-disk-by\x2duuid-a707db5f\x2d9935\x2d4c4a\x2dbdf9\x2d93dbefaacf05.swap'
local-fs.target.requires
local-fs.target.wants
media-cdrom0.mount
-.mount
swap.target.requires
tmp.mount
root@debian:/run/systemd/generator# ls -l
total 16
-rw-r--r-- 1 root root 274 feb 15 17:07 'dev-disk-by\x2duuid-a707db5f\x2d9935\x2d4c4a\x2dbdf9\x2d93dbefaacf05.swap'
drwxr-xr-x 2 root root 80 feb 15 17:07 local-fs.target.requires
drwxr-xr-x 2 root root 60 feb 15 17:07 local-fs.target.wants
-rw-r--r-- 1 root root 244 feb 15 17:07 media-cdrom0.mount
-rw-r--r-- 1 root root 277 feb 15 17:07 -.mount
drwxr-xr-x 2 root root 60 feb 15 17:07 swap.target.requires
-rw-r--r-- 1 root root 255 feb 15 17:07 tmp.mount
root@debian:/run/systemd/generator# cd local-fs.target.wants
root@debian:/run/systemd/generator/local-fs.target.wants# ls
systemd-fsck-root.service
root@debian:/run/systemd/generator/local-fs.target.wants# cd ..
root@debian:/run/systemd/generator# cat tmp.mount
```

vero@debian: ~

✕

Archivo Editar Ver Buscar Terminal Ayuda

```
drwxr-xr-x 2 root root 80 feb 15 17:07 local-fs.target.requires
drwxr-xr-x 2 root root 60 feb 15 17:07 local-fs.target.wants
-rw-r--r-- 1 root root 244 feb 15 17:07 media-cdrom0.mount
-rw-r--r-- 1 root root 277 feb 15 17:07 -.mount
drwxr-xr-x 2 root root 60 feb 15 17:07 swap.target.requires
-rw-r--r-- 1 root root 255 feb 15 17:07 tmp.mount
root@debian:/run/systemd/generator# cd local-fs.target.wants
root@debian:/run/systemd/generator/local-fs.target.wants# ls
systemd-fsck-root.service
root@debian:/run/systemd/generator/local-fs.target.wants# cd ..
root@debian:/run/systemd/generator# cat tmp.mount
# Automatically generated by systemd-fstab-generator
```

[Unit]

SourcePath=/etc/fstab

Documentation=man:fstab(5) man:systemd-fstab-generator(8)

Before=local-fs.target

[Mount]

Where=/tmp

What=tmpfs

Type=tmpfs

Options=defaults,rw,nosuid,nodev,noexec,relatime

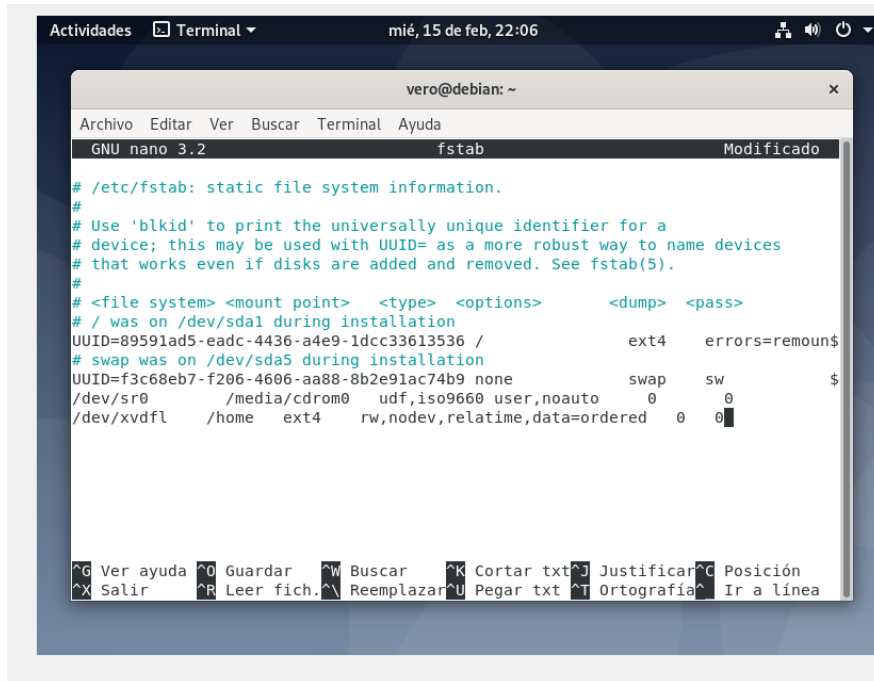
root@debian:/run/systemd/generator#

### 1.1.13 Ensure separate partition exists for /home (Scored)

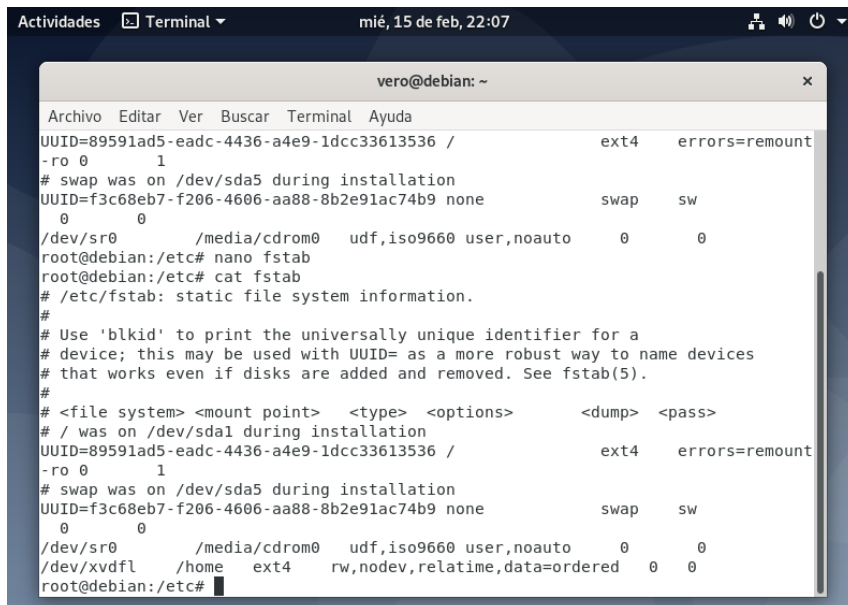
No hay particion para /home

```
vero@debian: ~  
Archivo  Editor  Ver  Buscar  Terminal  Ayuda  
root@debian:/run/systemd/generator# cd ..  
root@debian:/run/systemd# cd ..  
root@debian:/run# cd ..  
root@debian:/# mount | grep /home  
root@debian:/# df -Th  
S.ficheros      Tipo      Tamaño Usados  Disp Uso% Montado en  
udev            devtmpfs  1,5G    0      1,5G  0% /dev  
tmpfs            tmpfs     301M    4,9M   296M  2% /run  
/dev/sda1        ext4      37G     4,2G   31G   13% /  
tmpfs            tmpfs     1,5G    0      1,5G  0% /dev/shm  
tmpfs            tmpfs     5,0M    4,0K   5,0M  1% /run/lock  
tmpfs            tmpfs     1,5G    0      1,5G  0% /sys/fs/cgroup  
tmpfs            tmpfs     1,5G    64K    1,5G  1% /tmp  
tmpfs            tmpfs     301M    4,6M   296M  2% /run/user/1000  
  
root@debian:/# cat /etc/fstab  
# /etc/fstab: static file system information.  
#  
# Use 'blkid' to print the universally unique identifier for a  
# device; this may be used with UUID= as a more robust way to name devices  
# that works even if disks are added and removed. See fstab(5).  
#  
# <file system> <mount point> <type> <options>          <dump> <pass>  
# / was on /dev/sda1 during installation  
UUID=86068048-8fcc-4a12-87da-886301d4eef4 /          ext4      errors=remount  
-ro 0          1  
# swap was on /dev/sda5 during installation  
UUID=a707db5f-9935-4c4a-bdf9-93dbefaacf05 none          swap      sw  
0          0  
/dev/sr0        /media/cdrom0  udf,iso9660 user,noauto    0          0  
tmpfs /tmp      tmpfs          defaults,rw,nosuid,nodev,noexec,relatime 0 0  
root@debian:/#
```

## Creamos una partición y securizamos



```
vero@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
GNU nano 3.2          fstab          Modificado  
  
# /etc/fstab: static file system information.  
#  
# Use 'blkid' to print the universally unique identifier for a  
# device; this may be used with UUID= as a more robust way to name devices  
# that works even if disks are added and removed. See fstab(5).  
#  
# <file system> <mount point> <type> <options>          <dump> <pass>  
# / was on /dev/sda1 during installation  
UUID=89591ad5-eadc-4436-a4e9-1dcc33613536 /          ext4      errors=remoun$  
# swap was on /dev/sda5 during installation  
UUID=f3c68eb7-f206-4606-aa88-8b2e91ac74b9 none          swap      sw          $  
/dev/sr0          /media/cdrom0    udf,iso9660 user,noauto    0          0  
/dev/xvdf1        /home            ext4        rw,nodev,relatime,data=ordered 0          0
```

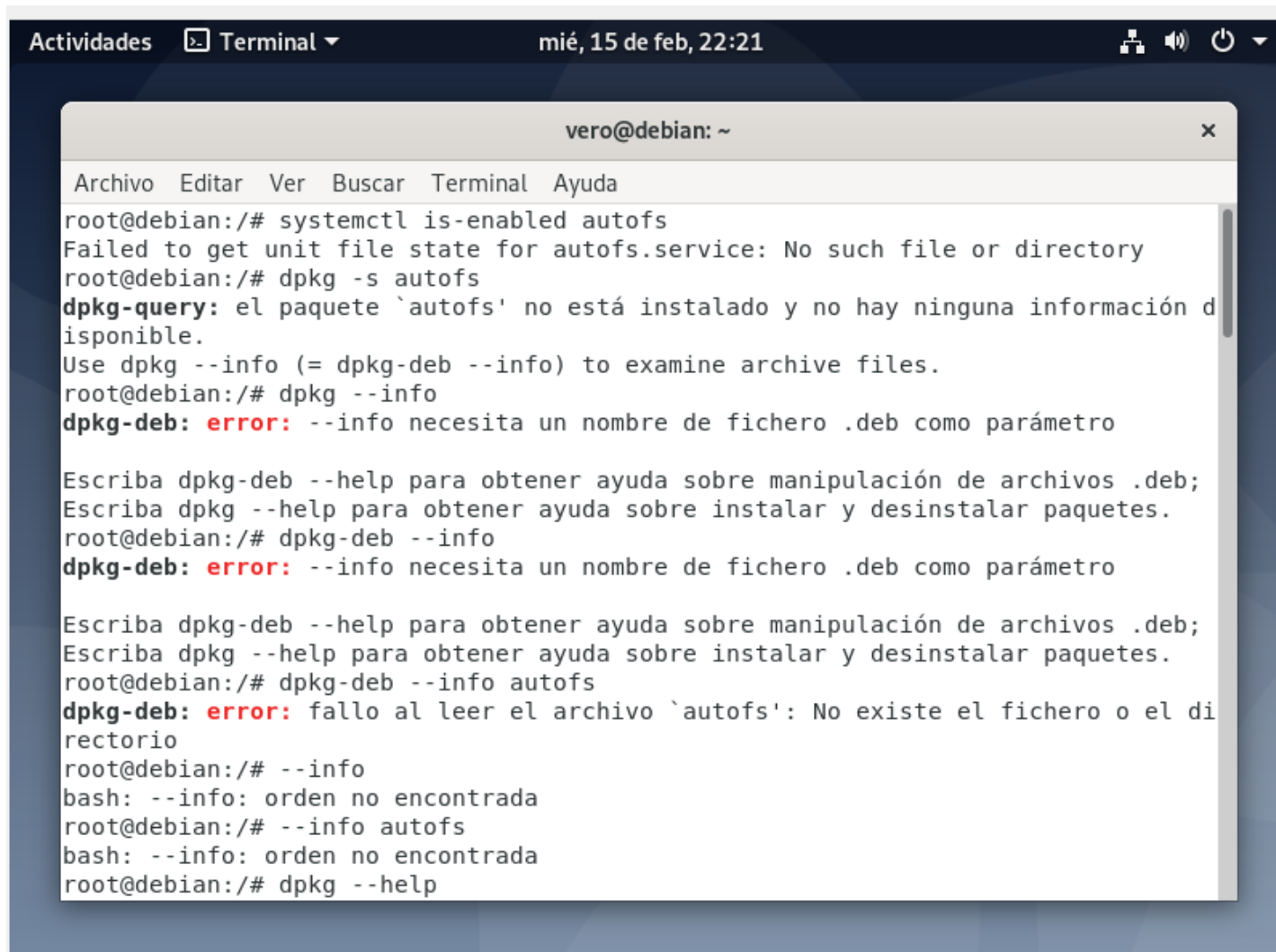


```
vero@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
UUID=89591ad5-eadc-4436-a4e9-1dcc33613536 /          ext4      errors=remount  
-ro 0          1  
# swap was on /dev/sda5 during installation  
UUID=f3c68eb7-f206-4606-aa88-8b2e91ac74b9 none          swap      sw  
0          0  
/dev/sr0          /media/cdrom0    udf,iso9660 user,noauto    0          0  
root@debian:/etc# nano fstab  
root@debian:/etc# cat fstab  
# /etc/fstab: static file system information.  
#  
# Use 'blkid' to print the universally unique identifier for a  
# device; this may be used with UUID= as a more robust way to name devices  
# that works even if disks are added and removed. See fstab(5).  
#  
# <file system> <mount point> <type> <options>          <dump> <pass>  
# / was on /dev/sda1 during installation  
UUID=89591ad5-eadc-4436-a4e9-1dcc33613536 /          ext4      errors=remount  
-ro 0          1  
# swap was on /dev/sda5 during installation  
UUID=f3c68eb7-f206-4606-aa88-8b2e91ac74b9 none          swap      sw  
0          0  
/dev/sr0          /media/cdrom0    udf,iso9660 user,noauto    0          0  
/dev/xvdf1        /home            ext4        rw,nodev,relatime,data=ordered 0          0  
root@debian:/etc#
```

Al reiniciar para que tome la particion me da un error y se cuelga y no puedo volver a abrir la maquina.

### 1.1.22 Disable Automounting (Scored)

El archivo no esta instalado y no se encuentra información del sistema.



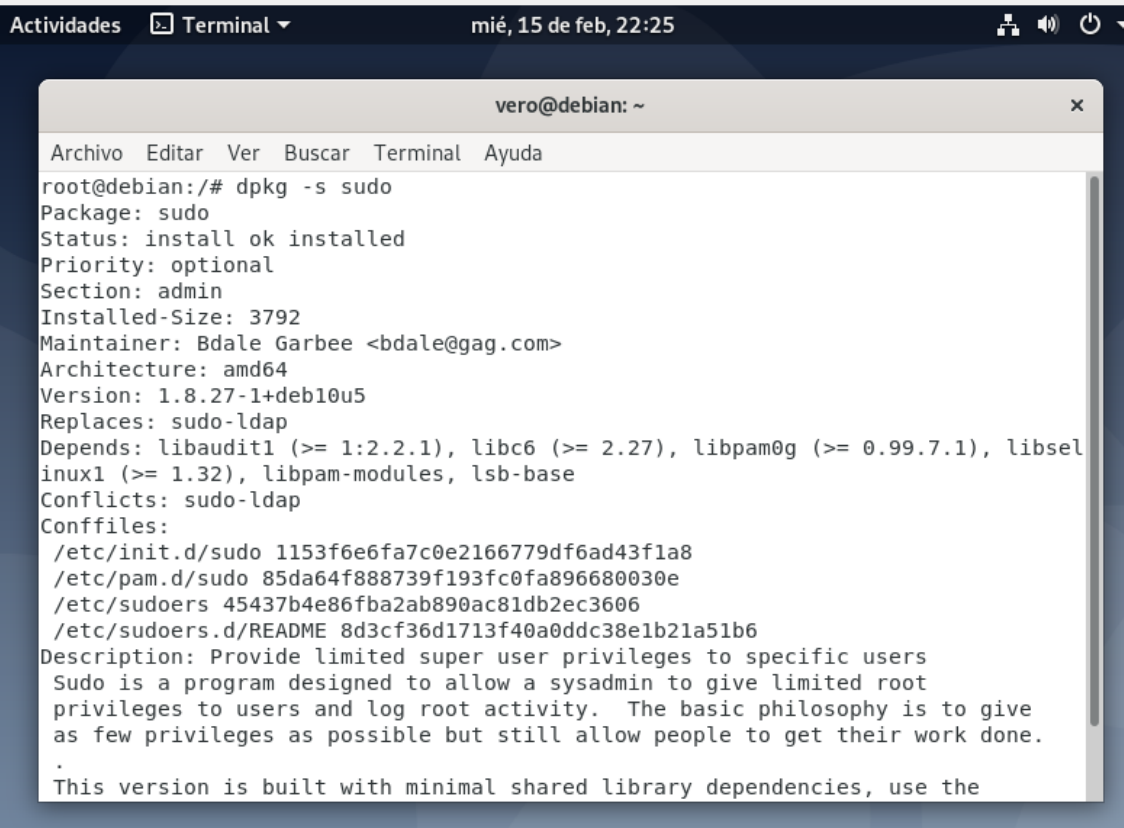
```
Actividades Terminal ▼ mié, 15 de feb, 22:21
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/# systemctl is-enabled autofs
Failed to get unit file state for autofs.service: No such file or directory
root@debian:/# dpkg -s autofs
dpkg-query: el paquete `autofs' no está instalado y no hay ninguna información disponible.
Use dpkg --info (= dpkg-deb --info) to examine archive files.
root@debian:/# dpkg --info
dpkg-deb: error: --info necesita un nombre de fichero .deb como parámetro

Escriba dpkg-deb --help para obtener ayuda sobre manipulación de archivos .deb;
Escriba dpkg --help para obtener ayuda sobre instalar y desinstalar paquetes.
root@debian:/# dpkg-deb --info
dpkg-deb: error: --info necesita un nombre de fichero .deb como parámetro

Escriba dpkg-deb --help para obtener ayuda sobre manipulación de archivos .deb;
Escriba dpkg --help para obtener ayuda sobre instalar y desinstalar paquetes.
root@debian:/# dpkg-deb --info autofs
dpkg-deb: error: fallo al leer el archivo `autofs': No existe el fichero o el directorio
root@debian:/# --info
bash: --info: orden no encontrada
root@debian:/# --info autofs
bash: --info: orden no encontrada
root@debian:/# dpkg --help
```

### 1.3.1 Ensure Sudo is installed (Scored)

Esta instalado

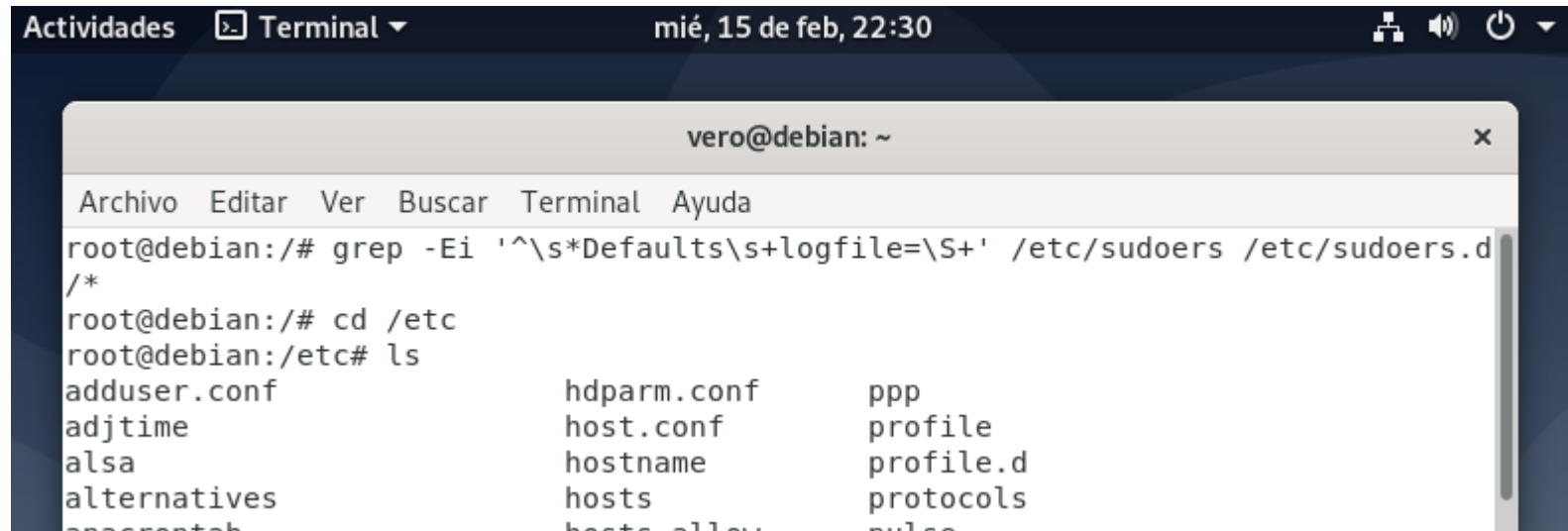


A terminal window titled 'vero@debian: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The window shows the output of the command 'dpkg -s sudo' executed as root. The output displays package details for 'sudo', including its status, priority, section, size, maintainer, architecture, version, dependencies, conflicts, and configuration files. The description states that sudo is designed to allow a sysadmin to give limited root privileges to users and log root activity.

```
root@debian:/# dpkg -s sudo
Package: sudo
Status: install ok installed
Priority: optional
Section: admin
Installed-Size: 3792
Maintainer: Bdale Garbee <bdale@gag.com>
Architecture: amd64
Version: 1.8.27-1+deb10u5
Replaces: sudo-ldap
Depends: libaudit1 (>= 1:2.2.1), libc6 (>= 2.27), libpam0g (>= 0.99.7.1), libselinux1 (>= 1.32), libpam-modules, lsb-base
Conflicts: sudo-ldap
Conffiles:
 /etc/init.d/sudo 1153f6e6fa7c0e2166779df6ad43f1a8
 /etc/pam.d/sudo 85da64f888739f193fc0fa896680030e
 /etc/sudoers 45437b4e86fba2ab890ac81db2ec3606
 /etc/sudoers.d/README 8d3cf36d1713f40a0ddc38e1b21a51b6
Description: Provide limited super user privileges to specific users
 Sudo is a program designed to allow a sysadmin to give limited root
 privileges to users and log root activity. The basic philosophy is to give
 as few privileges as possible but still allow people to get their work done.
.
This version is built with minimal shared library dependencies, use the
```

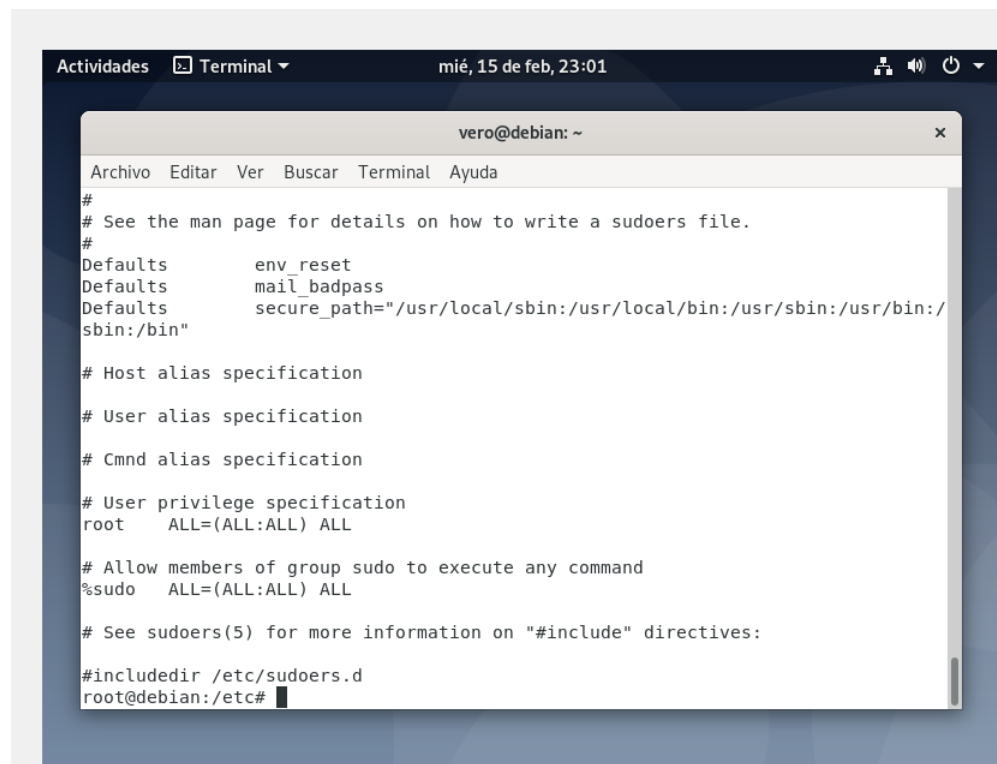


### 1.3.3 Ensure sudo log file exists (Scored)



A terminal window titled 'vero@debian: ~' with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda) and a status bar (mié, 15 de feb, 22:30). The terminal shows the following commands and output:

```
root@debian:/# grep -Ei '^\\s*Defaults\\s+logfile=\\S+' /etc/sudoers /etc/sudoers.d/*
root@debian:/# cd /etc
root@debian:/etc# ls
adduser.conf          hdparm.conf          ppp
adjtime               host.conf            profile
alsa                  hostname             profile.d
alternatives          hosts                protocols
anacrontab            hosts.allow          pulse
```



A terminal window titled 'vero@debian: ~' with a menu bar (Archivo, Editar, Ver, Buscar, Terminal, Ayuda) and a status bar (mié, 15 de feb, 23:01). The terminal shows the contents of the /etc/sudoers file:

```
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin"

# Host alias specification

# User alias specification

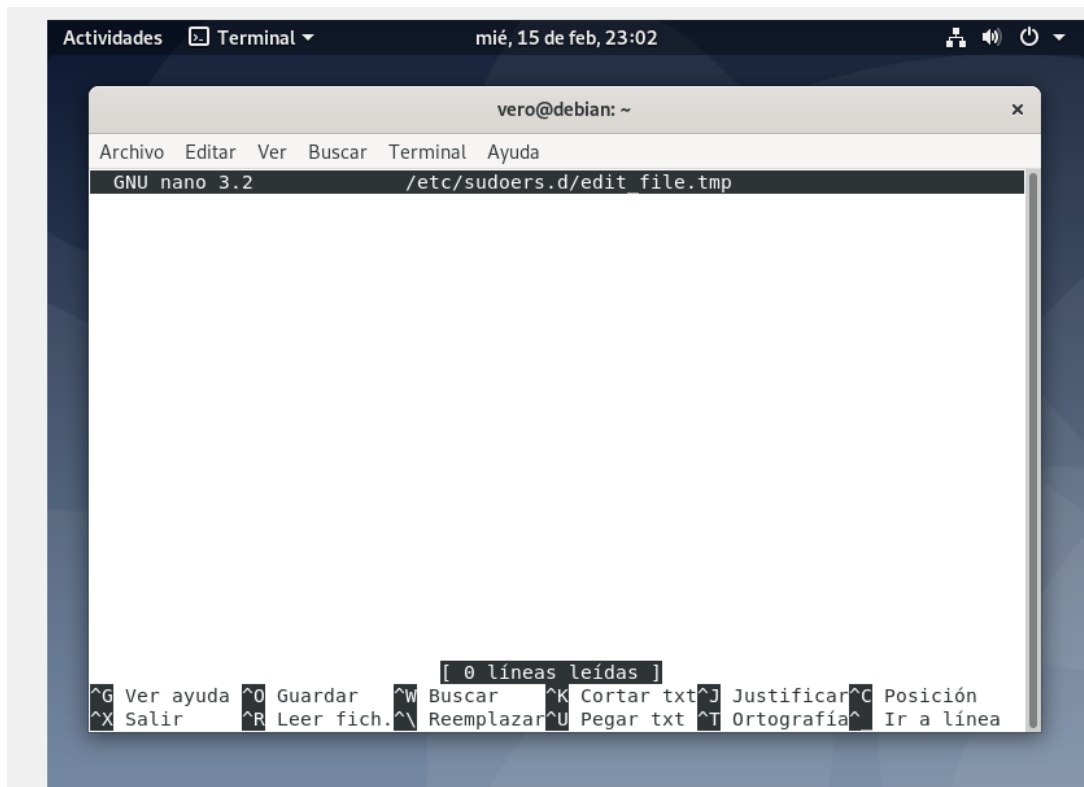
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

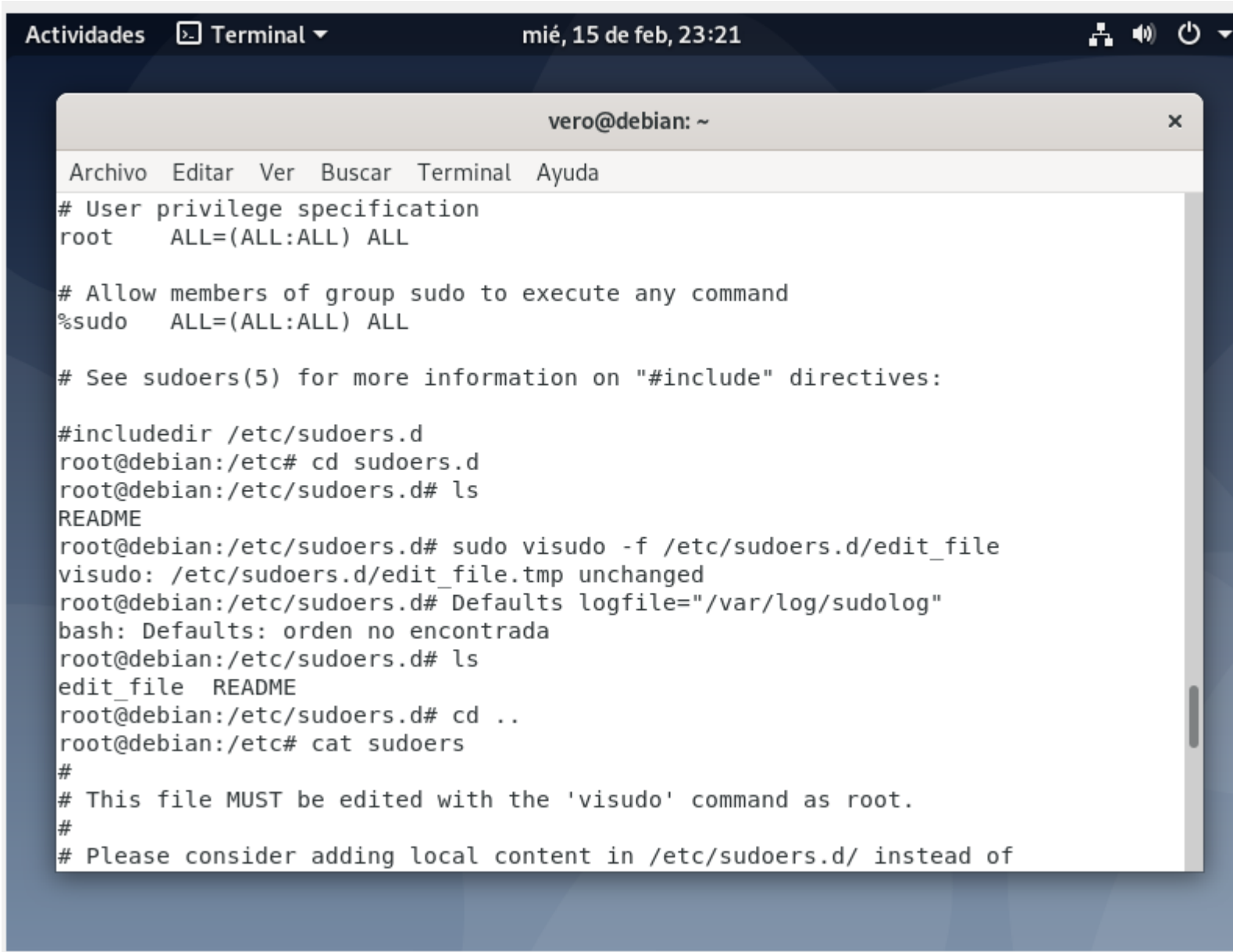
#include_dir /etc/sudoers.d
root@debian:/etc#
```



```
# See sudoers(5) for more information on "#include" directives:

#include_dir /etc/sudoers.d
root@debian:/etc# cd sudoers.d
root@debian:/etc/sudoers.d# ls
README
root@debian:/etc/sudoers.d# sudo visudo -f /etc/sudoers.d/edit_file
visudo: /etc/sudoers.d/edit_file.tmp unchanged
root@debian:/etc/sudoers.d#
```

Intente editar un nuevo file en la carpeta sudoers.d pero no añade el path a sudoers por ende edite directamente el archivo sudoers y me creo el file sudo.log

A terminal window titled 'vero@debian: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows a sequence of commands and their outputs. The user navigates to /etc/sudoers.d, lists files, and uses 'visudo' to edit a file. The output of 'visudo' shows the file was unchanged. The user then checks the 'Defaults' section, which reports 'orden no encontrada'. Finally, the user lists files again, showing 'edit\_file' and 'README', and navigates back to the parent directory. The terminal ends with the contents of the /etc/sudoers file, which includes instructions on how to edit it and where to add local content.

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d
root@debian:/etc# cd sudoers.d
root@debian:/etc/sudoers.d# ls
README
root@debian:/etc/sudoers.d# sudo visudo -f /etc/sudoers.d/edit_file
visudo: /etc/sudoers.d/edit_file.tmp unchanged
root@debian:/etc/sudoers.d# Defaults logfile="/var/log/sudolog"
bash: Defaults: orden no encontrada
root@debian:/etc/sudoers.d# ls
edit_file  README
root@debian:/etc/sudoers.d# cd ..
root@debian:/etc# cat sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
```

vero@debian: ~

x

Archivo Editar Ver Buscar Terminal Ayuda

```
#includedir /etc/sudoers.d
root@debian:/etc# sudo visudo -f sudoers
root@debian:/etc# cd /var/log
root@debian:/var/log# ls
alternatives.log  daemon.log      hp              speech-dispatcher
apt               debug           installer      sudo.log
auth.log          dpkg.log        kern.log        syslog
boot.log          faillog         lastlog         unattended-upgrades
btmp              fontconfig.log  messages       user.log
cups              gdm3            private        wtmp
root@debian:/var/log# cat sudoers
cat: sudoers: No existe el fichero o el directorio
root@debian:/var/log# cd /etc
root@debian:/etc# cat sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults          env_reset
```

Archivo Editar Ver Buscar Terminal Ayuda

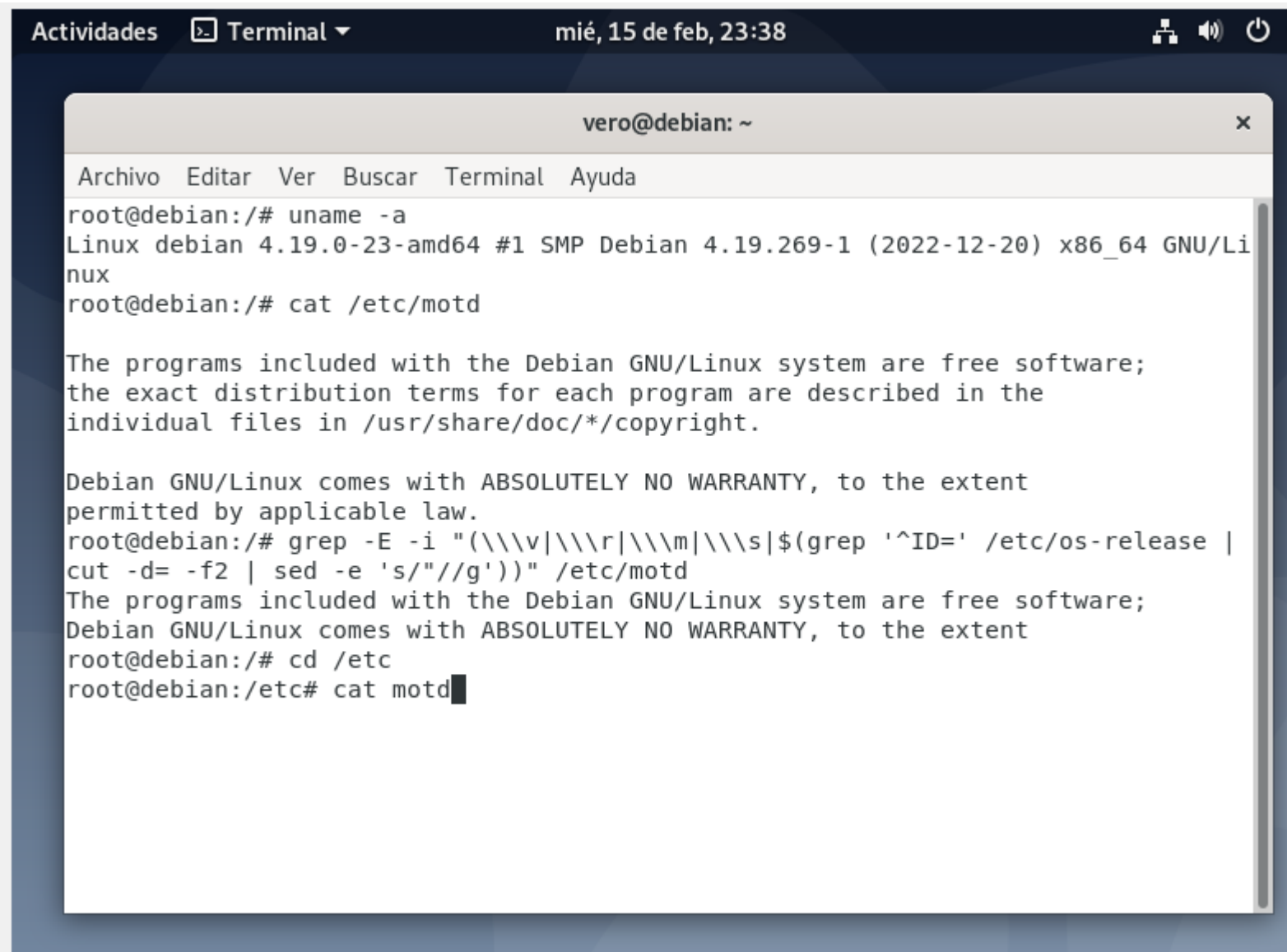
cat: sudoers: No existe el fichero o el directorio

root@debian:/var/log# cd /etc

root@debian:/etc# cat sudoers

```
#  
# This file MUST be edited with the 'visudo' command as root.  
#  
# Please consider adding local content in /etc/sudoers.d/ instead of  
# directly modifying this file.  
#  
# See the man page for details on how to write a sudoers file.  
#  
Defaults      env_reset  
Defaults      mail_badpass  
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"  
Defaults      logfile="/var/log/sudo.log"  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification
```

#### 1.8.1.1 Ensure message of the day is configured properly (Scored)



The screenshot shows a terminal window titled "vero@debian: ~" with a menu bar containing "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The terminal output shows the following commands and their results:

```
root@debian:/# uname -a
Linux debian 4.19.0-23-amd64 #1 SMP Debian 4.19.269-1 (2022-12-20) x86_64 GNU/Linux
root@debian:/# cat /etc/motd

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:/# grep -E -i "(\v|r|m|s|$(grep '^ID=' /etc/os-release |
cut -d= -f2 | sed -e 's//g'))" /etc/motd
The programs included with the Debian GNU/Linux system are free software;
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
root@debian:/# cd /etc
root@debian:/etc# cat motd
```

No trae gran informacion al correr el segundo comando, de cualquier manera verificamos el file.

Actividades Terminal ▼ mié, 15 de feb, 23:42

vero@debian: ~

Archivo Editar Ver Buscar Terminal Ayuda

GNU nano 3.2 motd Modificado

The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/copyright.

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^\_ Ir a línea

Borre las líneas que pueden ser leídas, pero se puede eliminar el archivo por seguridad.

```
Actividades Terminal mié, 15 de feb, 23:44
```

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:/etc# nano motd
Use «fg» para volver a nano.

[1]+  Detenido          nano motd
root@debian:/etc# nano motd
root@debian:/etc# cat motd

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:/etc# nano motd
root@debian:/etc# grep -E -i "(\|v|\|r|\|m|\|s|$(grep '^ID=' /etc/os-release
| cut -d= -f2 | sed -e 's/"/'g'))" /etc/motd
The programs included with the Debian GNU/Linux system are free software;
root@debian:/etc# nano motd
root@debian:/etc# grep -E -i "(\|v|\|r|\|m|\|s|$(grep '^ID=' /etc/os-release
| cut -d= -f2 | sed -e 's/"/'g'))" /etc/motd
root@debian:/etc#
```

```
Actividades Terminal mié, 15 de feb, 23:48
```

```
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

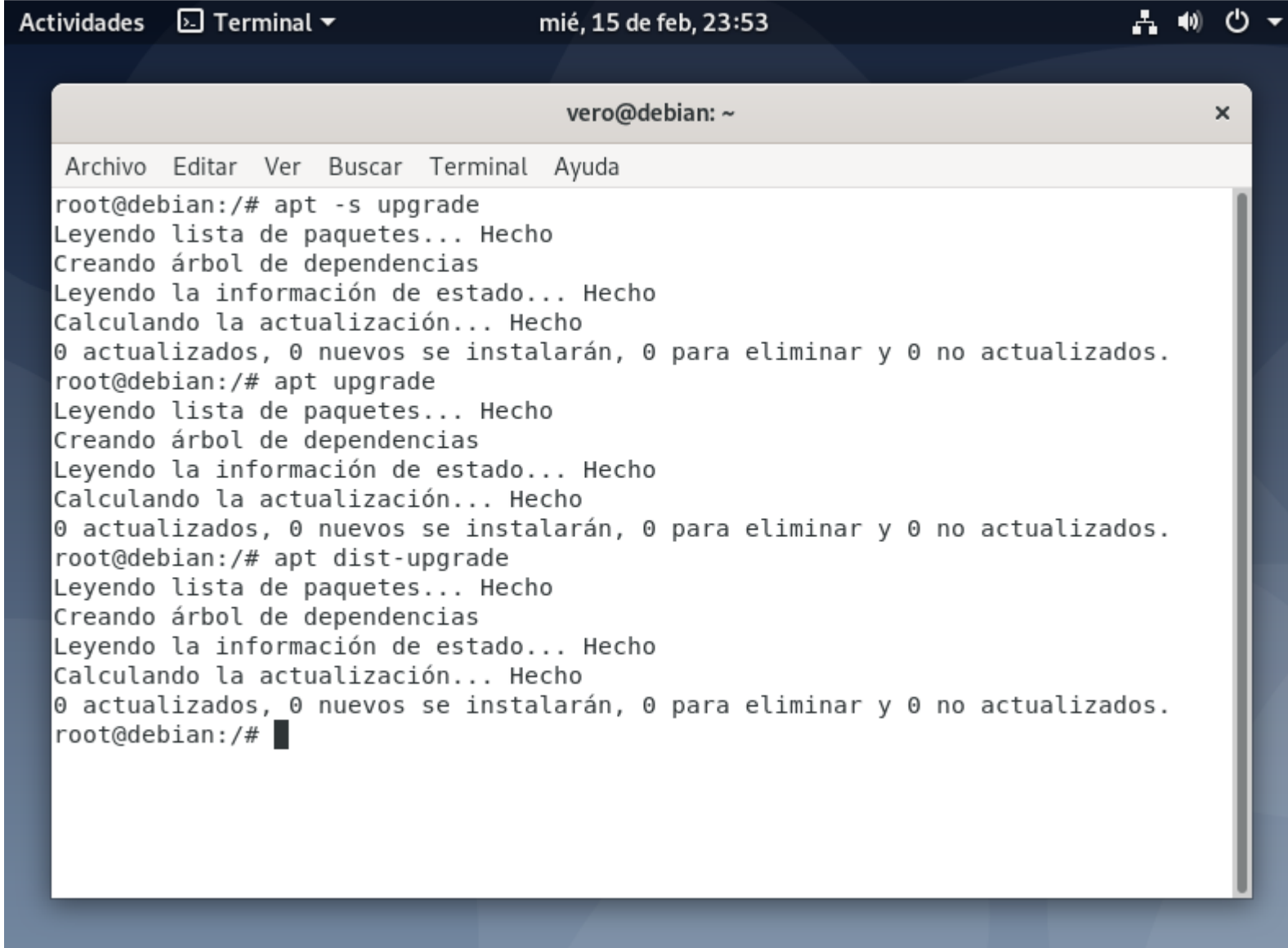
.
1. The origin of this software must not be misrepresented; you must not
   claim that you wrote the original software. If you use this software
   in a product, an acknowledgment in the product documentation would be
   appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
   misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.
.
Jean-loup Gailly          Mark Adler
jloup@zip.org            madler@alumni.caltech.edu
.

If you use the zlib library in a product, we would appreciate *not* receiving
lengthy legal documents to sign. The sources are provided for free but without
warranty of any kind. The library has been entirely written by Jean-loup
Gailly and Mark Adler; it does not include third-party code.
.

If you redistribute modified sources, we would appreciate that you include in
the file ChangeLog history information documenting your changes. Please read
the FAQ for more information on the distribution of modified source versions.
root@debian:/usr/share/doc#
```



# 1.9 Ensure updates, patches, and additional security software are installed (Not Scored)

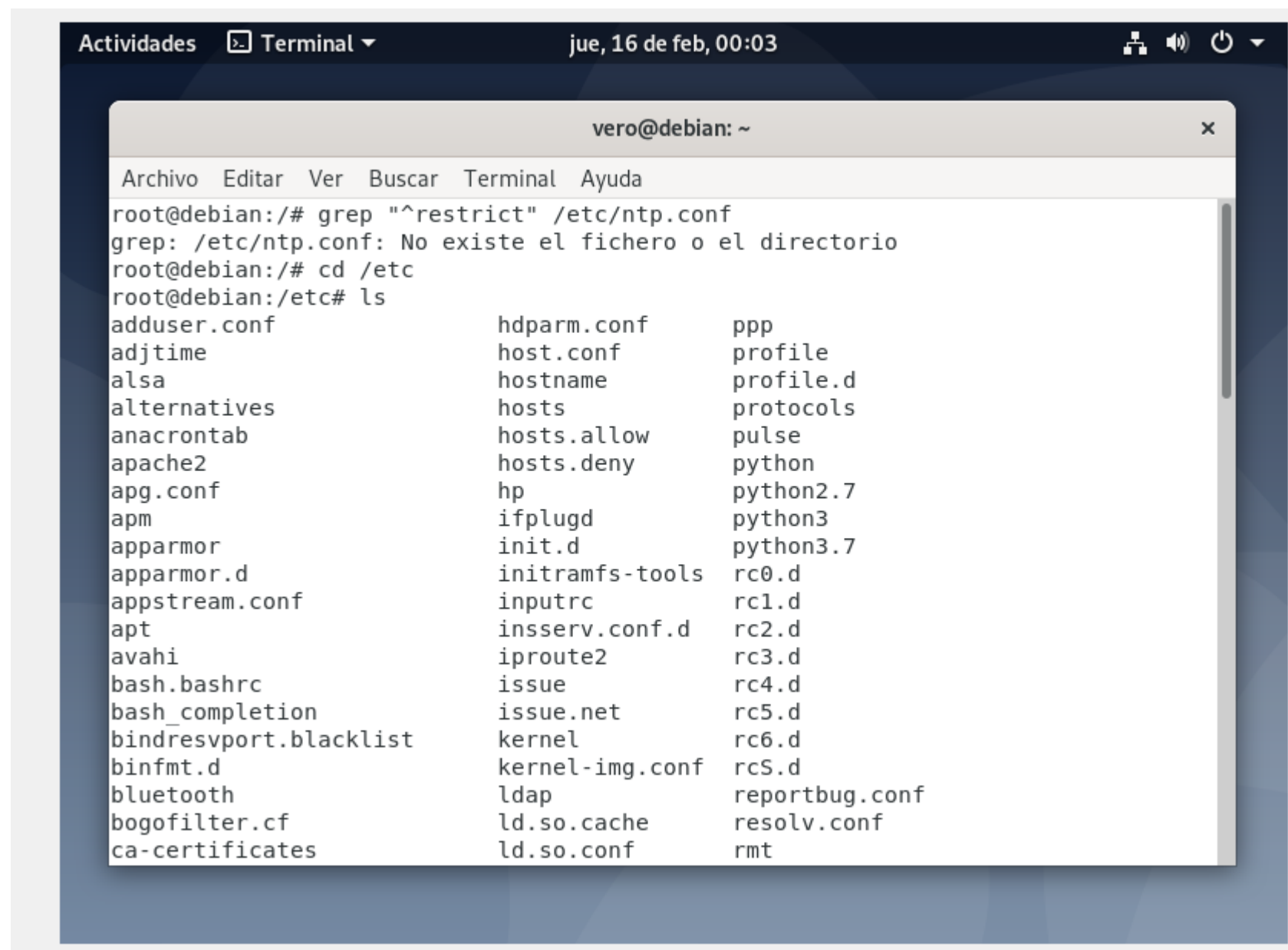


The screenshot shows a terminal window titled 'vero@debian: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal output shows three sequential upgrade commands being executed as root. Each command follows a similar pattern: reading package lists, creating dependency trees, reading state information, calculating updates, and reporting that 0 packages were updated, 0 new ones would be installed, 0 would be removed, and 0 were not updated.

```
root@debian:/# apt -s upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debian:/# apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debian:/# apt dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debian:/#
```

#### 2.2.1.4 Ensure ntp is configured (Scored)

NTP NO ESTA EN USO EN EL SISTEMA



The image shows a terminal window titled 'vero@debian: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal output shows the user running a command to search for 'restrict' in '/etc/ntp.conf', which fails because the file does not exist. Subsequently, the user changes the directory to '/etc' and runs 'ls', displaying a long list of files and directories in three columns.

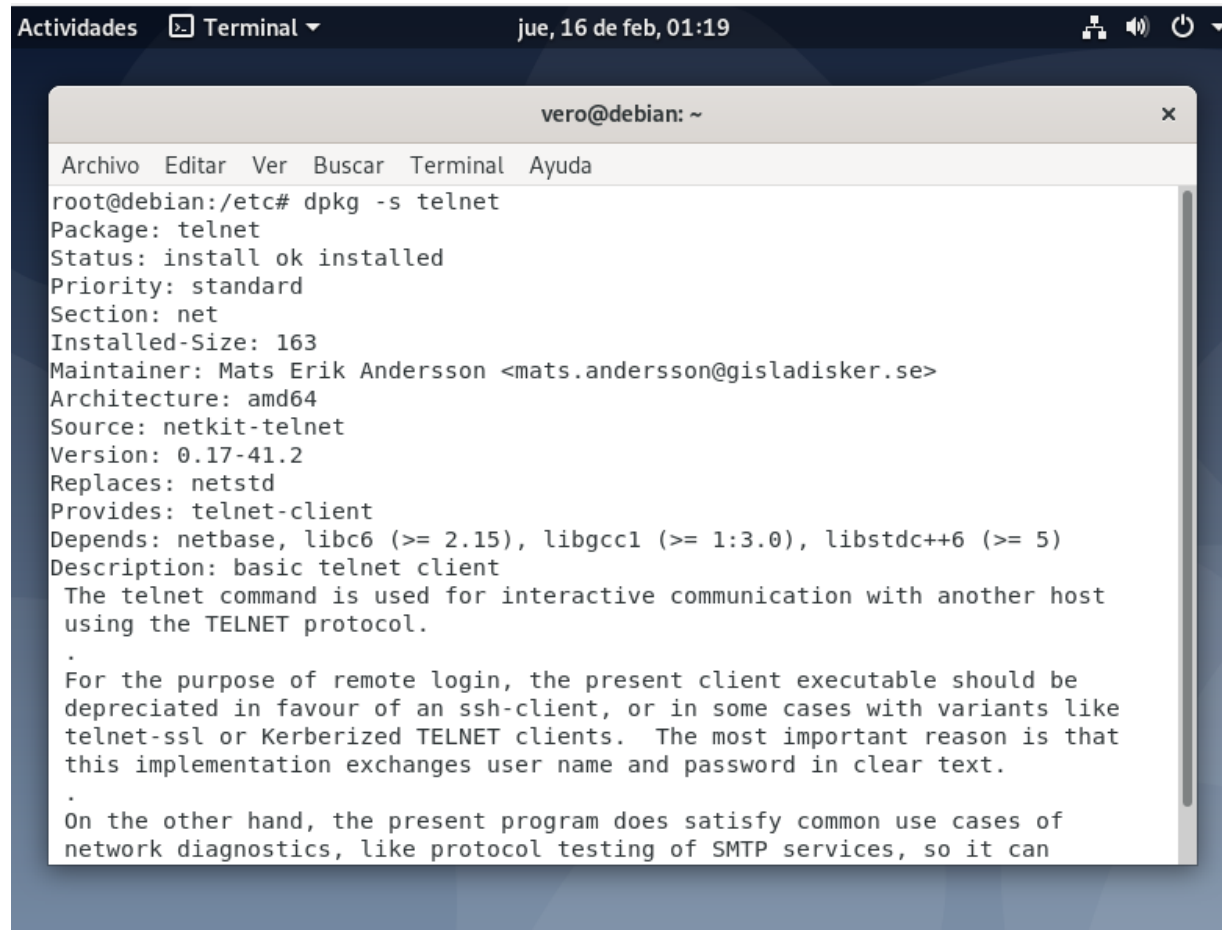
```
root@debian:/# grep "^restrict" /etc/ntp.conf
grep: /etc/ntp.conf: No existe el fichero o el directorio
root@debian:/# cd /etc
root@debian:/etc# ls
adduser.conf          hdparm.conf          ppp
adjtime               host.conf             profile
alsa                  hostname              profile.d
alternatives           hosts                  protocols
anacrontab             hosts.allow            pulse
apache2                hosts.deny             python
apg.conf               hp                     python2.7
apm                    ifplugd                python3
apparmor               init.d                 python3.7
apparmor.d             initramfs-tools        rc0.d
appstream.conf          inputrc                 rc1.d
apt                     insserv.conf.d          rc2.d
avahi                   iproute2                rc3.d
bash.bashrc             issue                   rc4.d
bash_completion         issue.net               rc5.d
bindresvport.blacklist  kernel                 rc6.d
binfmt.d                kernel-img.conf         rcS.d
bluetooth               ldap                    reportbug.conf
bogofilter.cf           ld.so.cache             resolv.conf
ca-certificates         ld.so.conf              rmt
```

## 2.2.10 Ensure HTTP Server is not enabled (Scored)

```
Actividades Terminal jue, 16 de feb, 01:16
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
● connman.service not-found inactive dead connman.service
● console-screen.service not-found inactive dead console-screen.service
console-setup.service loaded active exited Set console font and key
cron.service loaded active running Regular background progr
cups-browsed.service loaded active running Make remote CUPS printer
cups.service loaded active running CUPS Scheduler
dbus.service loaded active running D-Bus System Message Bus
emergency.service loaded inactive dead Emergency Shell
fwupd.service loaded active running Firmware update daemon
gdm.service loaded active running GNOME Display Manager
getty-static.service loaded inactive dead getty on tty2-tty6 if db

root@debian:/etc# systemctl is-enabled apache
Failed to get unit file state for apache.service: No such file or directory
root@debian:/etc# systemctl is-enabled apache2
enabled
root@debian:/etc# systemctl --now disable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apache2
Removed /etc/systemd/system/multi-user.target.wants/apache2.service.
root@debian:/etc# systemctl is-enabled apache2
disabled
root@debian:/etc#
```

### 2.3.4 Ensure telnet client is not installed (Scored)



A terminal window titled "vero@debian: ~" is open. The window has a menu bar with "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The terminal shows the command `root@debian:/etc# dpkg -s telnet` and its output. The output lists package details for telnet, including its status, priority, section, size, maintainer, architecture, source, version, and dependencies. It also includes a description of the telnet command and a note about its deprecation for remote login.

```
root@debian:/etc# dpkg -s telnet
Package: telnet
Status: install ok installed
Priority: standard
Section: net
Installed-Size: 163
Maintainer: Mats Erik Andersson <mats.andersson@gisladisker.se>
Architecture: amd64
Source: netkit-telnet
Version: 0.17-41.2
Replaces: netstd
Provides: telnet-client
Depends: netbase, libc6 (>= 2.15), libgcc1 (>= 1:3.0), libstdc++6 (>= 5)
Description: basic telnet client
 The telnet command is used for interactive communication with another host
 using the TELNET protocol.
.
 For the purpose of remote login, the present client executable should be
 depreciated in favour of an ssh-client, or in some cases with variants like
 telnet-ssl or Kerberized TELNET clients. The most important reason is that
 this implementation exchanges user name and password in clear text.
.
 On the other hand, the present program does satisfy common use cases of
 network diagnostics, like protocol testing of SMTP services, so it can
```

vero@debian: ~

✕

Archivo Editar Ver Buscar Terminal Ayuda

this implementation exchanges user name and password in clear text.

.

On the other hand, the present program does satisfy common use cases of network diagnostics, like protocol testing of SMTP services, so it can become handy enough.

root@debian:/etc# apt purge telnet

Leyendo lista de paquetes... Hecho

Creando árbol de dependencias

Leyendo la información de estado... Hecho

Los siguientes paquetes se ELIMINARÁN:

telnet\*

0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 0 no actualizados.

Se liberarán 167 kB después de esta operación.

¿Desea continuar? [S/n] S

(Leyendo la base de datos ... 144833 ficheros o directorios instalados actualmente.)

Desinstalando telnet (0.17-41.2) ...

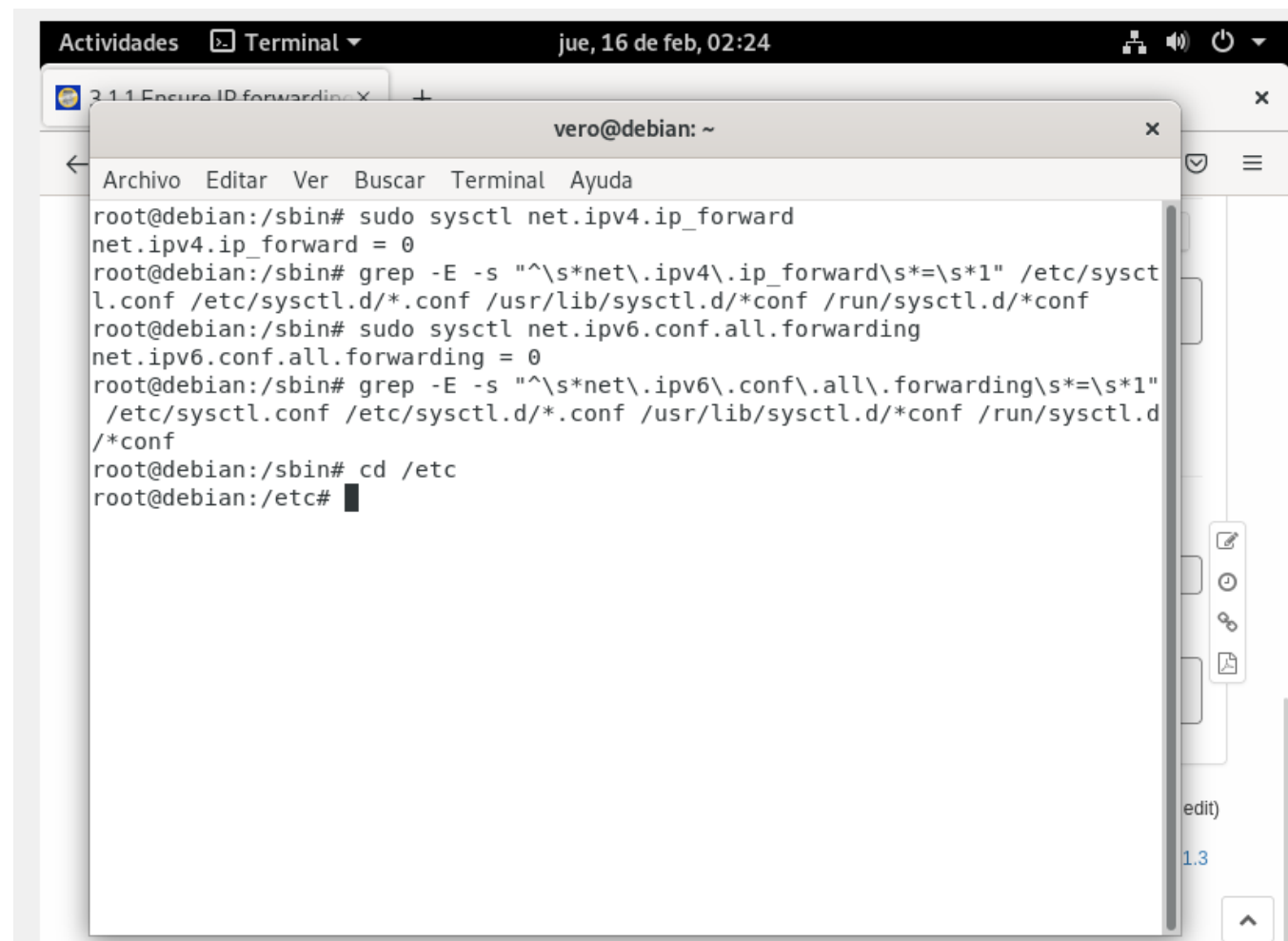
Procesando disparadores para man-db (2.8.5-2) ...

(Leyendo la base de datos ... 144823 ficheros o directorios instalados actualmente.)

Purgando ficheros de configuración de telnet (0.17-41.2) ...

root@debian:/etc# █

### 3.2.2 Ensure IP forwarding is disabled (Scored)



The screenshot shows a terminal window titled "Terminal" with a date and time of "jue, 16 de feb, 02:24". The terminal prompt is "vero@debian: ~". The user is running the following commands:

```
root@debian:/sbin# sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
root@debian:/sbin# grep -E -s "^s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl
l.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf
root@debian:/sbin# sudo sysctl net.ipv6.conf.all.forwarding
net.ipv6.conf.all.forwarding = 0
root@debian:/sbin# grep -E -s "^s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1"
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d
/*conf
root@debian:/sbin# cd /etc
root@debian:/etc#
```

The terminal window has a menu bar with "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". On the right side, there is a sidebar with icons for "edit)", "1.3", and an upward arrow.

vero@debian: ~

x

Archivo Editar Ver Buscar Terminal Ayuda

```
root@debian:/etc# grep "^s*linux" /boot/grub/grub.cfg | grep -v "ipv6.disable=l
```

```
"
```

```
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae4e-  
d329df1402b8 ro quiet
```

```
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-48  
8b-ae4e-d329df1402b8 ro quiet
```

```
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-48  
8b-ae4e-d329df1402b8 ro single
```

```
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-48  
8b-ae4e-d329df1402b8 ro quiet
```

```
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-48  
8b-ae4e-d329df1402b8 ro single
```

```
root@debian:/etc# ls
```

adduser.conf	gtk-3.0	polkit-1
adjtime	hdparm.conf	ppp
alsa	host.conf	profile
alternatives	hostname	profile.d
anacrontab	hosts	protocols
analog.cfg	hosts.allow	pulse
apache2	hosts.deny	python
apg.conf	hp	python2.7
apm	ifplugd	python3
apparmor	init.d	python3.7
apparmor.d	initramfs-tools	rc0.d

Run the following command and verify output matches:

```
# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

## Remediation

Set the following parameter in the `/etc/sysctl.conf` file:

```
net.ipv4.ip_forward = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.ip_forward=0
# sysctl -w net.ipv4.route.flush=1
```

centos7/3/1/1.txt Last modified: 2017/05/04 15:19 (external edit)

Except where otherwise noted, content on this wiki is licensed under the following license: [GNU Free Documentation License 1.3](#)



Actividades Terminal jue, 16 de feb, 02:29

3.1.1 Enable IP forwarding X traductor Buscar con Google X

vero@debian: ~

Archivo Editar Ver Buscar Terminal Ayuda

GNU nano 3.2 sysctl.conf Modificado

```
#####3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path fil$
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
# net.ipv4.ip_forward=0

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
```

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía

edit)  
1.3

```

3.1.1 Encure ID forwardin... traductor... Buscar con Google...
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro single
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro single
root@debian:/etc# nano sysctl.conf
root@debian:/etc# sudo sysctl -w net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@debian:/etc# sudo sysctl -w net.ipv4.route.flush=1
net.ipv4.route.flush = 1
root@debian:/etc# grep "^s*linux" /boot/grub/grub.cfg | grep -v "ipv6.disab
le=l"
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae4e-d329
df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro single
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-488b-ae
4e-d329df1402b8 ro single
root@debian:/etc#

```

Actividades 2.2.1 Encure ID forwarding X traductor Buscar con Google +

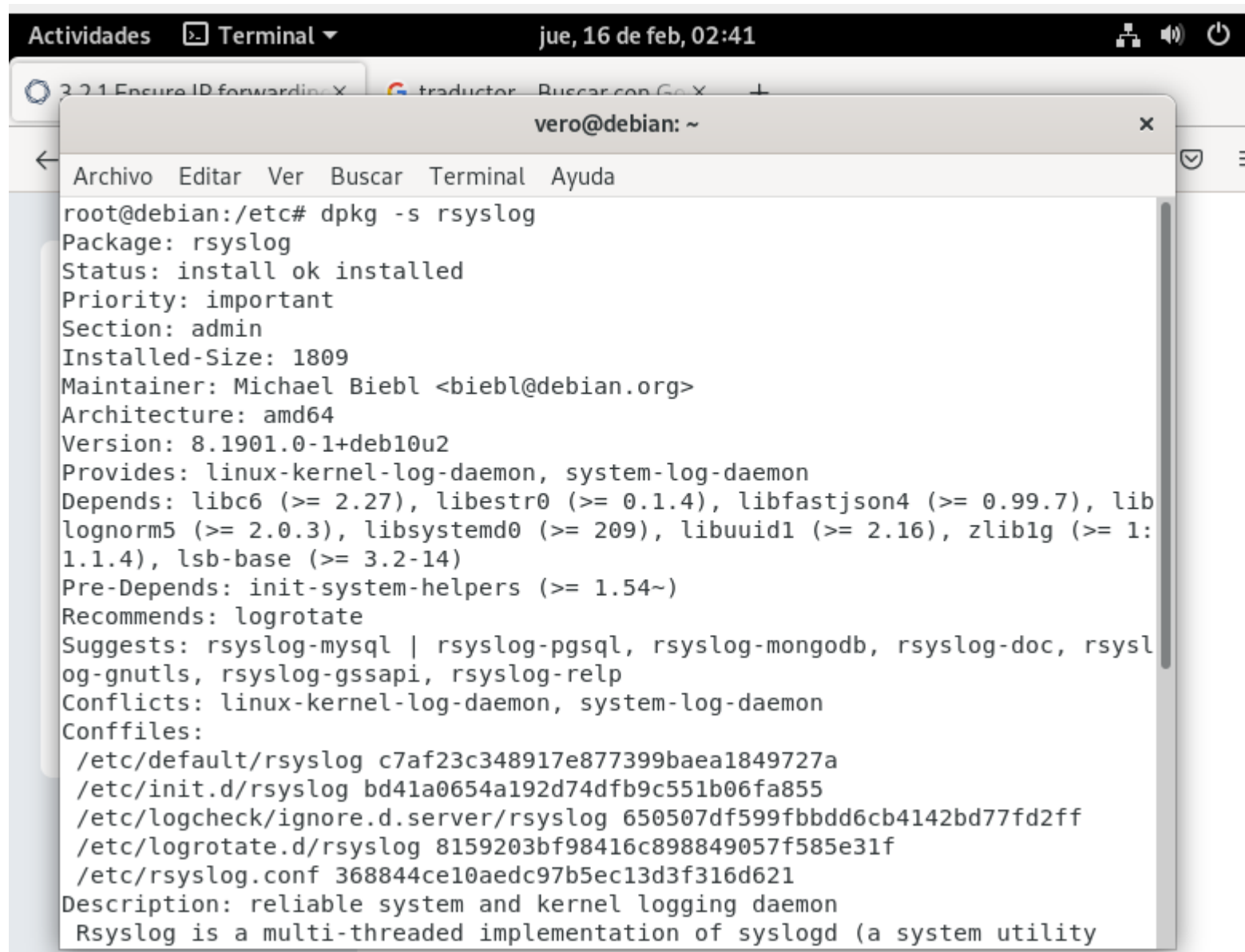
vero@debian: ~

Archivo Editar Ver Buscar Terminal Ayuda

```
le=l"
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-23-amd64 root=UUID=a332b649-b0c1-488b-ae4e-d329df1402b8 ro single
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-488b-ae4e-d329df1402b8 ro quiet
linux /boot/vmlinuz-4.19.0-14-amd64 root=UUID=a332b649-b0c1-488b-ae4e-d329df1402b8 ro single
root@debian:/etc# grep -Els '^s*net.ipv6.conf.all.forwardings*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf
| while read filename; do sed -ri 's/^s*(net.ipv6.conf.all.forwardings*)(=)(s*S+b).*/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1
bash: sysctl: orden no encontrada
bash: sysctl: orden no encontrada
root@debian:/etc# grep -Els '^s*net.ipv6.conf.all.forwardings*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf
| while read filename; do sed -ri 's/^s*(net.ipv6.conf.all.forwardings*)(=)(s*S+b).*/# *REMOVED* 1/' $filename; done; sudo sysctl -w net.ipv6.conf.all.forwarding=0; sudo sysctl -w net.ipv6.route.flush=1
net.ipv6.conf.all.forwarding = 0
net.ipv6.route.flush = 1
root@debian:/etc#
```

## 4.2.1 Configure rsyslog

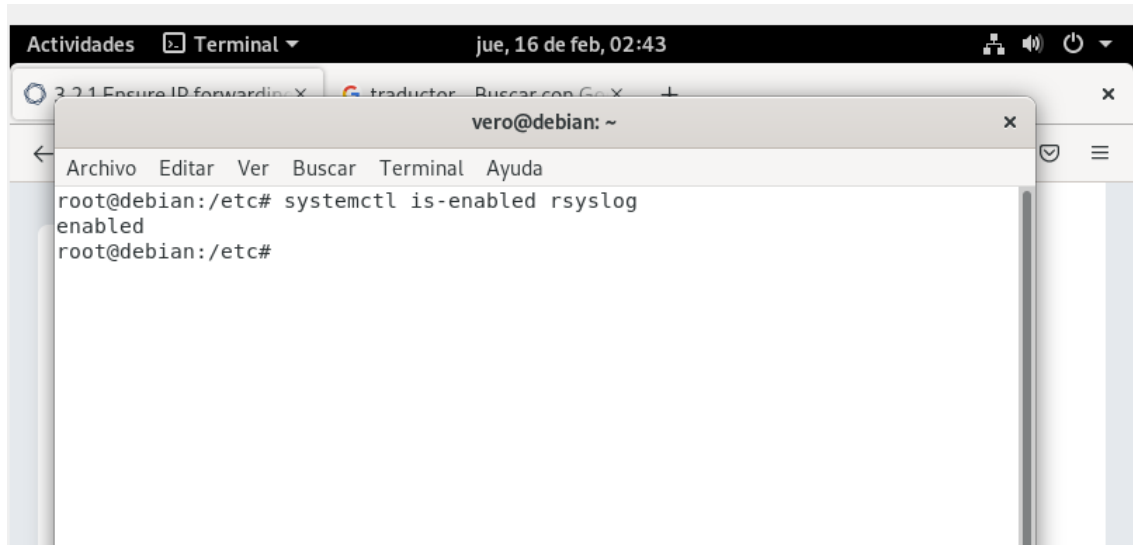
### 4.2.1.1 Ensure rsyslog is installed



The screenshot shows a terminal window titled 'vero@debian: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal displays the command `dpkg -s rsyslog` and its output, which provides detailed information about the installed rsyslog package, including its status, priority, section, size, maintainer, architecture, version, dependencies, and description.

```
root@debian:/etc# dpkg -s rsyslog
Package: rsyslog
Status: install ok installed
Priority: important
Section: admin
Installed-Size: 1809
Maintainer: Michael Biebl <biebl@debian.org>
Architecture: amd64
Version: 8.1901.0-1+deb10u2
Provides: linux-kernel-log-daemon, system-log-daemon
Depends: libc6 (>= 2.27), libestr0 (>= 0.1.4), libfastjson4 (>= 0.99.7), liblognorm5 (>= 2.0.3), libsystemd0 (>= 209), libuuid1 (>= 2.16), zlib1g (>= 1:1.1.4), lsb-base (>= 3.2-14)
Pre-Depends: init-system-helpers (>= 1.54~)
Recommends: logrotate
Suggests: rsyslog-mysql | rsyslog-pgsql, rsyslog-mongodb, rsyslog-doc, rsyslog-gnutls, rsyslog-gssapi, rsyslog-relp
Conflicts: linux-kernel-log-daemon, system-log-daemon
Conffiles:
 /etc/default/rsyslog c7af23c348917e877399baea1849727a
 /etc/init.d/rsyslog bd41a0654a192d74dfb9c551b06fa855
 /etc/logcheck/ignore.d.server/rsyslog 650507df599fbbdd6cb4142bd77fd2ff
 /etc/logrotate.d/rsyslog 8159203bf98416c898849057f585e31f
 /etc/rsyslog.conf 368844ce10aedc97b5ec13d3f316d621
Description: reliable system and kernel logging daemon
 Rsyslog is a multi-threaded implementation of syslogd (a system utility
```

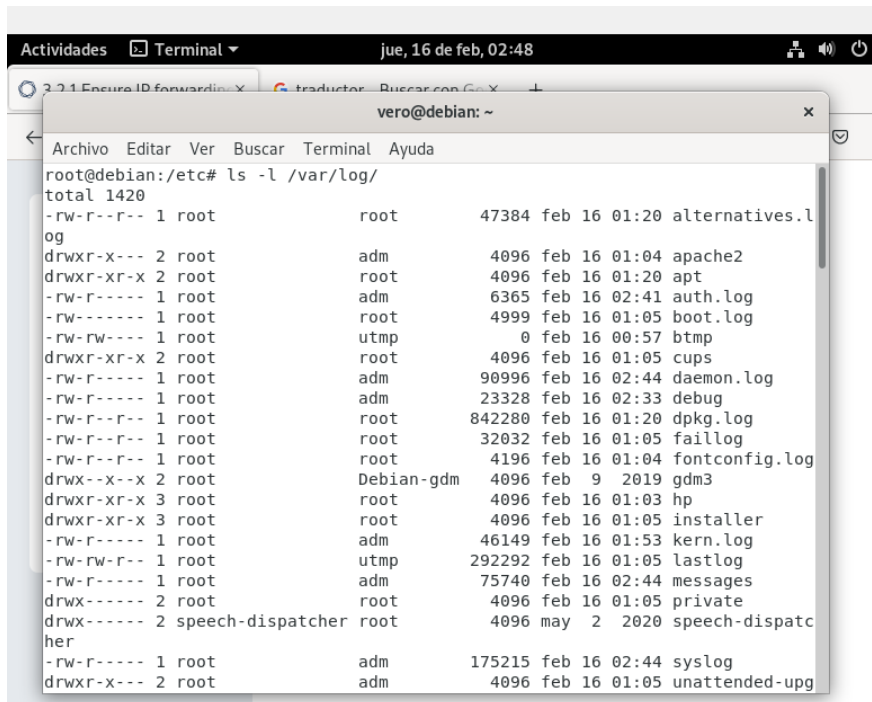
#### 4.2.1.2 Ensure rsyslog service is enable



A terminal window titled 'vero@debian: ~' is open. The command 'systemctl is-enabled rsyslog' has been entered, and the output 'enabled' is displayed. The prompt is now 'root@debian:/etc#'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The system clock at the top right shows 'jue, 16 de feb, 02:43'.

```
root@debian:/etc# systemctl is-enabled rsyslog
enabled
root@debian:/etc#
```

#### 4.2.1.3 Ensure logging is configured



A terminal window titled 'vero@debian: ~' is open. The command 'ls -l /var/log/' has been entered, and the output is a long list of log files with their permissions, sizes, dates, and names. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The system clock at the top right shows 'jue, 16 de feb, 02:48'.

```
root@debian:/etc# ls -l /var/log/
total 1420
-rw-r--r-- 1 root      root      47384 feb 16 01:20 alternatives.log
drwxr-x--- 2 root      adm        4096 feb 16 01:04 apache2
drwxr-xr-x 2 root      root        4096 feb 16 01:20 apt
-rw-r----- 1 root      adm        6365 feb 16 02:41 auth.log
-rw----- 1 root      root        4999 feb 16 01:05 boot.log
-rw-rw---- 1 root      utmp          0 feb 16 00:57 btmp
drwxr-xr-x 2 root      root        4096 feb 16 01:05 cups
-rw-r----- 1 root      adm       90996 feb 16 02:44 daemon.log
-rw-r----- 1 root      adm       23328 feb 16 02:33 debug
-rw-r--r-- 1 root      root     842280 feb 16 01:20 dpkg.log
-rw-r--r-- 1 root      root       32032 feb 16 01:05 faillog
-rw-r--r-- 1 root      root        4196 feb 16 01:04 fontconfig.log
drwx--x--x 2 root      Debian-gdm 4096 feb  9 2019 gdm3
drwxr-xr-x 3 root      root        4096 feb 16 01:03 hp
drwxr-xr-x 3 root      root        4096 feb 16 01:05 installer
-rw-r----- 1 root      adm       46149 feb 16 01:53 kern.log
-rw-rw-r-- 1 root      utmp     292292 feb 16 01:05 lastlog
-rw-r----- 1 root      adm       75740 feb 16 02:44 messages
drwx----- 2 root      root        4096 feb 16 01:05 private
drwx----- 2 speech-dispatcher root      4096 may  2 2020 speech-dispatcher
-rw-r----- 1 root      adm      175215 feb 16 02:44 syslog
drwxr-x--- 2 root      adm        4096 feb 16 01:05 unattended-upg
```

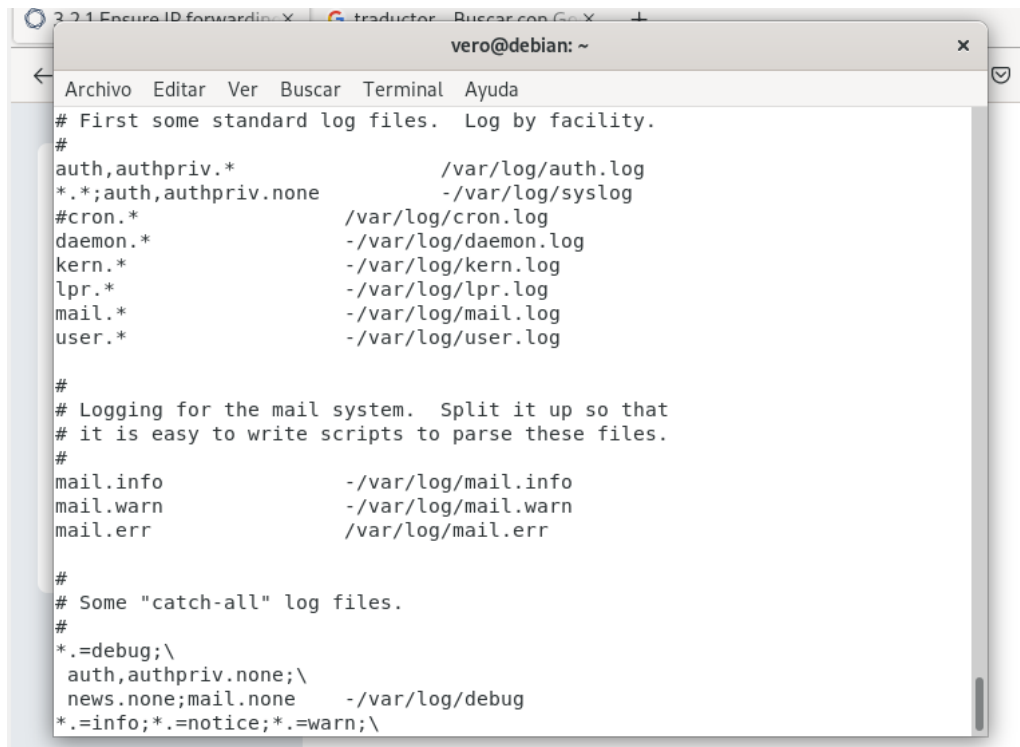
```
Actividades Terminal jue, 16 de feb, 02:51
3.2.1 Encara ID forwardin... traductor...
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
ner
-rw-r----- 1 root adm 177017 feb 16 02:49 syslog
drwxr-x--- 2 root adm 4096 feb 16 01:05 unattended-upg
rades
-rw-r----- 1 root adm 36850 feb 16 02:49 user.log
-rw-rw-r-- 1 root utmp 1152 feb 16 01:05 wtmp
root@debian:/var/log# cat syslog
Feb 16 01:05:30 debian systemd-modules-load[247]: Inserted module 'lp'
Feb 16 01:05:30 debian systemd-modules-load[247]: Inserted module 'ppdev'
Feb 16 01:05:30 debian systemd-modules-load[247]: Inserted module 'parport_p
c'
Feb 16 01:05:30 debian systemd-sysusers[258]: Creating group systemd-coredum
p with gid 999.
Feb 16 01:05:30 debian systemd-sysusers[258]: Creating user systemd-coredum
p (systemd Core Dumper) with uid 999 and gid 999.
Feb 16 01:05:30 debian systemd[1]: Started Create System Users.
Feb 16 01:05:30 debian systemd[1]: Starting Create Static Device Nodes in /d
ev...
Feb 16 01:05:30 debian systemd-tmpfiles[272]: [/usr/lib/tmpfiles.d/speech-di
spatcher.conf:1] Line references path below legacy directory /var/run/, upda
ting /var/run/speech-dispatcher -> /run/speech-dispatcher; please update the
tmpfiles.d/ drop-in file accordingly.
Feb 16 01:05:30 debian systemd-tmpfiles[272]: [/usr/lib/tmpfiles.d/speech-di
spatcher.conf:2] Line references path below legacy directory /var/run/, upda
ting /var/run/speech-dispatcher/.cache -> /run/speech-dispatcher/.cache; plea
se update the tmpfiles.d/ drop-in file accordingly.
```

```
root@debian:/var/log# cat /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html

#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")
```



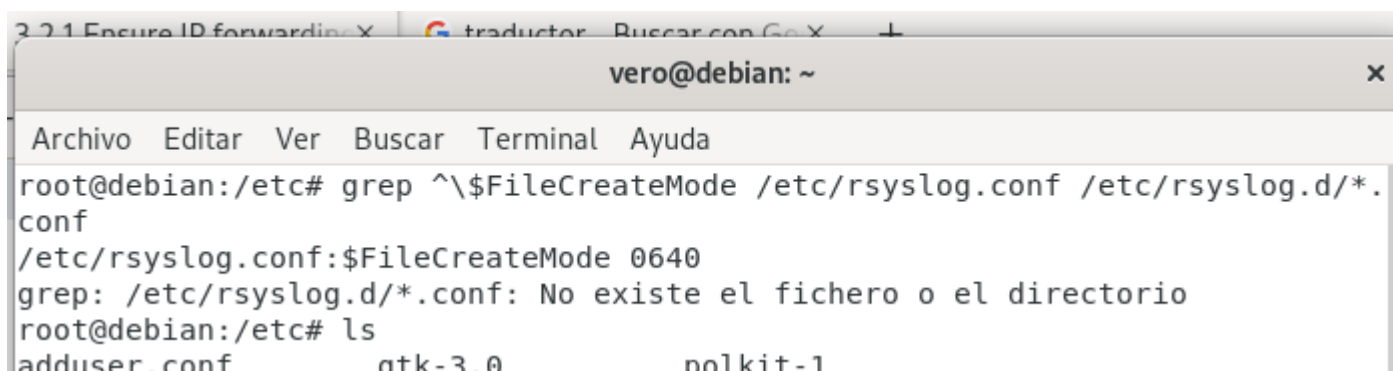
A screenshot of a terminal window titled 'vero@debian: ~'. The window contains a configuration file for rsyslog, showing standard log files and their destinations, as well as logging for the mail system and some 'catch-all' log files.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
# First some standard log files.  Log by facility.
#
auth,authpriv.*          /var/log/auth.log
*.*;auth,authpriv.none   -/var/log/syslog
#cron.*                  /var/log/cron.log
daemon.*                 -/var/log/daemon.log
kern.*                   -/var/log/kern.log
lpr.*                    -/var/log/lpr.log
mail.*                   -/var/log/mail.log
user.*                   -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                -/var/log/mail.info
mail.warn                -/var/log/mail.warn
mail.err                 /var/log/mail.err

#
# Some "catch-all" log files.
#
*.=debug;\
auth,authpriv.none;\
news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warn;
```

#### 4.2.1.4 Ensure rsyslog default file permissions configured

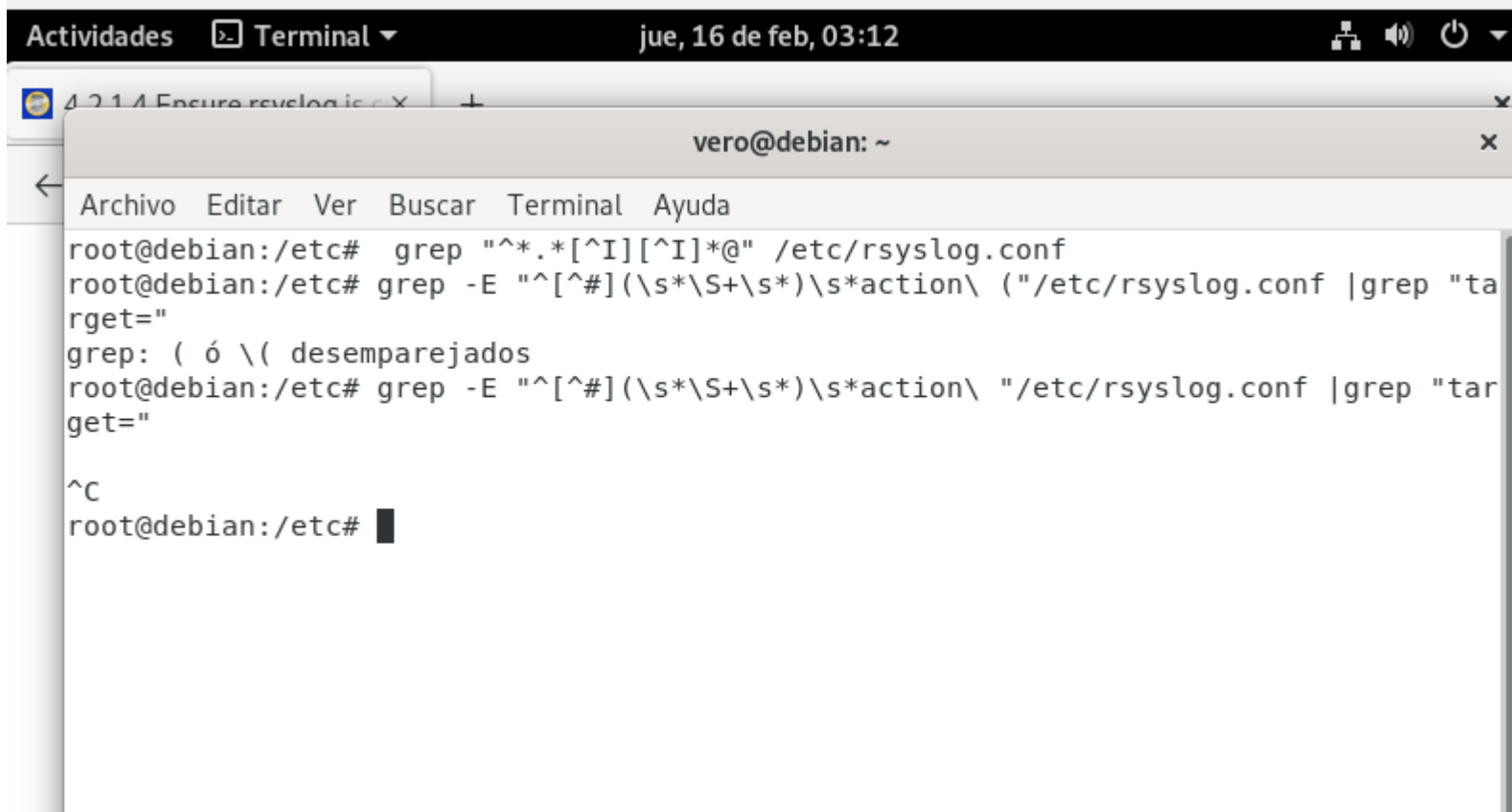


A screenshot of a terminal window titled 'vero@debian: ~'. The window shows the command 'grep ^\\${FileCreateMode} /etc/rsyslog.conf /etc/rsyslog.d/\*.conf' being executed, which returns the file create mode '0640' for /etc/rsyslog.conf. The command 'ls' is also executed, showing the contents of the /etc directory.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian:/etc# grep ^\${FileCreateMode} /etc/rsyslog.conf /etc/rsyslog.d/*.conf
/etc/rsyslog.conf:${FileCreateMode} 0640
grep: /etc/rsyslog.d/*.conf: No existe el fichero o el directorio
root@debian:/etc# ls
adduser.conf      ntk-3.0          ntkit-1
```

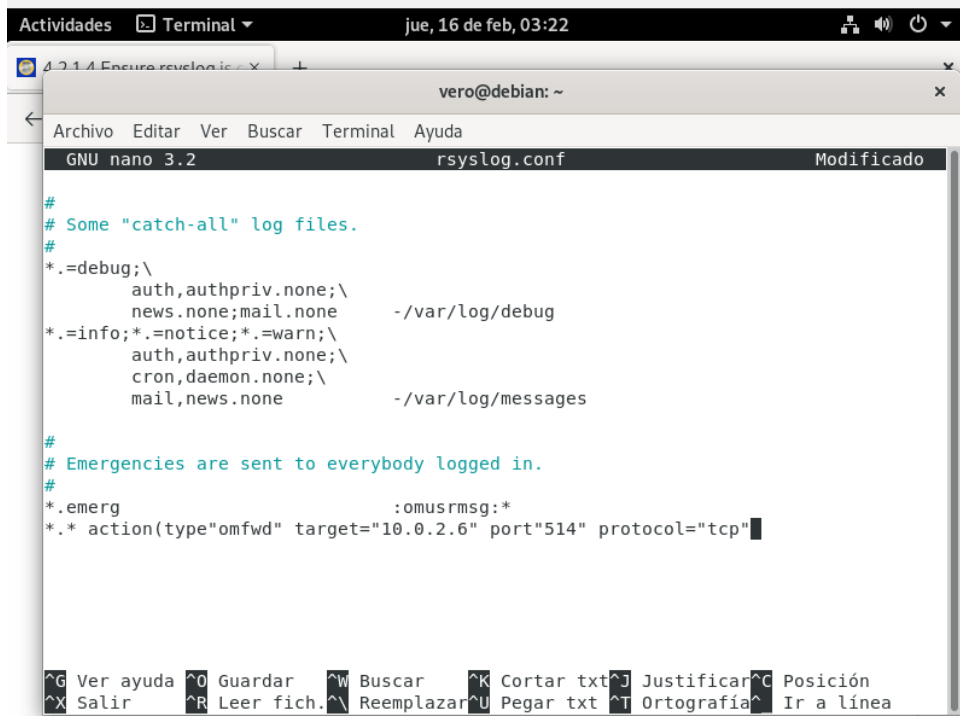
```
root@debian:/etc# cd rsyslog.d
root@debian:/etc/rsyslog.d# ls
root@debian:/etc/rsyslog.d# ls -la
total 8
drwxr-xr-x  2 root root 4096 feb 26  2019 .
drwxr-xr-x 118 root root 4096 feb 16 02:29 ..
root@debian:/etc/rsyslog.d#
```

#### 4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host



```
Actividades Terminal jue, 16 de feb, 03:12
4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc# grep "^*.*[^I][^I]*@" /etc/rsyslog.conf
root@debian:/etc# grep -E "^[^#](\\s*\\S+\\s*)\\s*action\\ ("/etc/rsyslog.conf |grep "ta
rget="
grep: ( ó \\( desemparejados
root@debian:/etc# grep -E "^[^#](\\s*\\S+\\s*)\\s*action\\ "/etc/rsyslog.conf |grep "tar
get="
^C
root@debian:/etc#
```





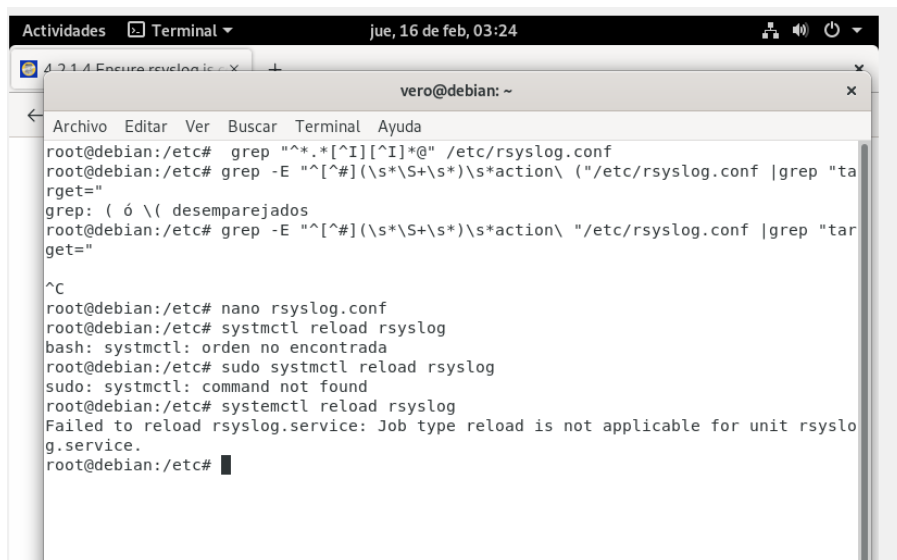
```
GNU nano 3.2 rsyslog.conf

#
# Some "catch-all" log files.
#
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none      -/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none          -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                     :omusrmsg:*
*. * action(type="omfwd" target="10.0.2.6" port="514" protocol="tcp"

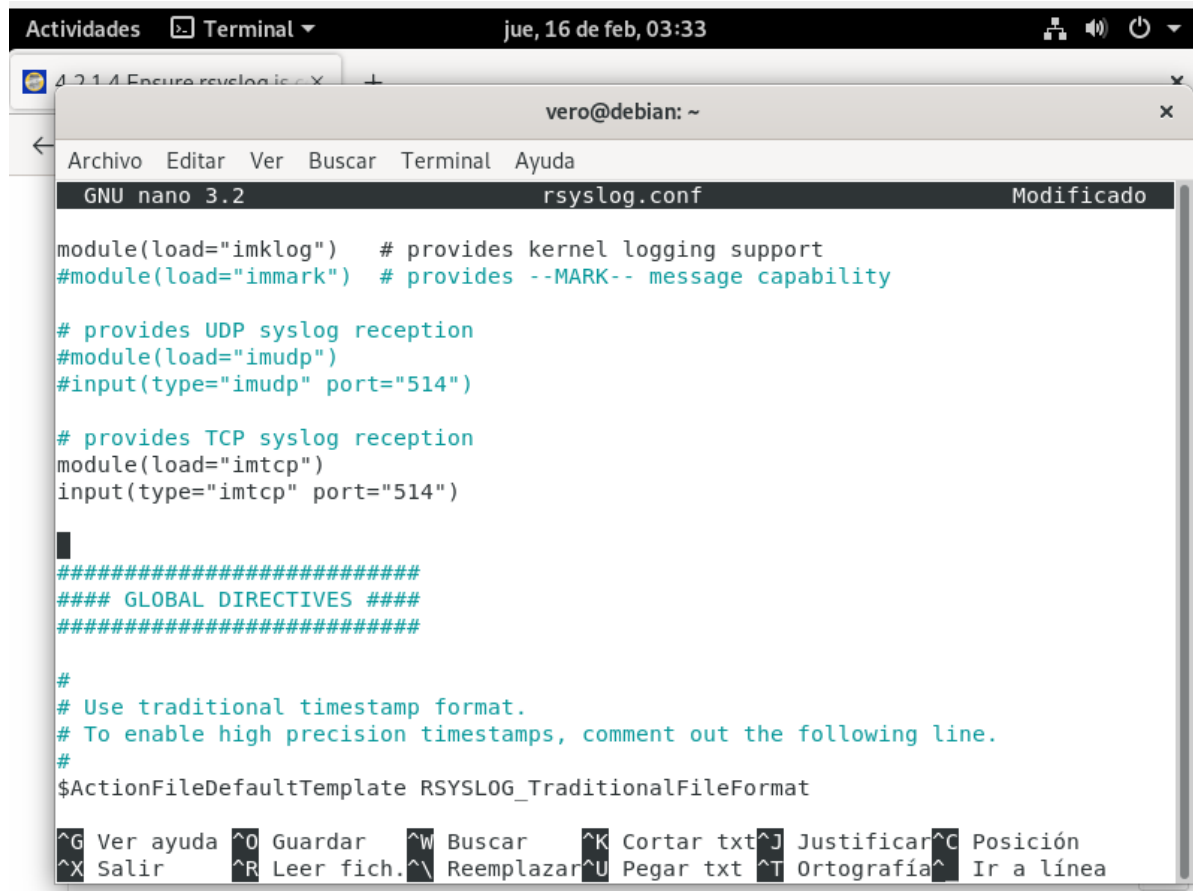
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

NO COMPRENDI BIEN COMO AÑADIR



```
root@debian:/etc# grep "^.*\[[^I]*\]" /etc/rsyslog.conf
root@debian:/etc# grep -E "^[^#](\\s*\\S+\\s*)\\s*action\\ (" /etc/rsyslog.conf |grep "target="
grep: ( ó \\( desemparejados
root@debian:/etc# grep -E "^[^#](\\s*\\S+\\s*)\\s*action\\ " /etc/rsyslog.conf |grep "target="
^C
root@debian:/etc# nano rsyslog.conf
root@debian:/etc# systemctl reload rsyslog
bash: systemctl: orden no encontrada
root@debian:/etc# sudo systemctl reload rsyslog
sudo: systemctl: command not found
root@debian:/etc# systemctl reload rsyslog
Failed to reload rsyslog.service: Job type reload is not applicable for unit rsyslog.service.
root@debian:/etc#
```

#### 4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)



The screenshot shows a terminal window titled 'Terminal' with the date and time 'jue, 16 de feb, 03:33'. The terminal is running the nano text editor, editing the file 'rsyslog.conf'. The file content is as follows:

```
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

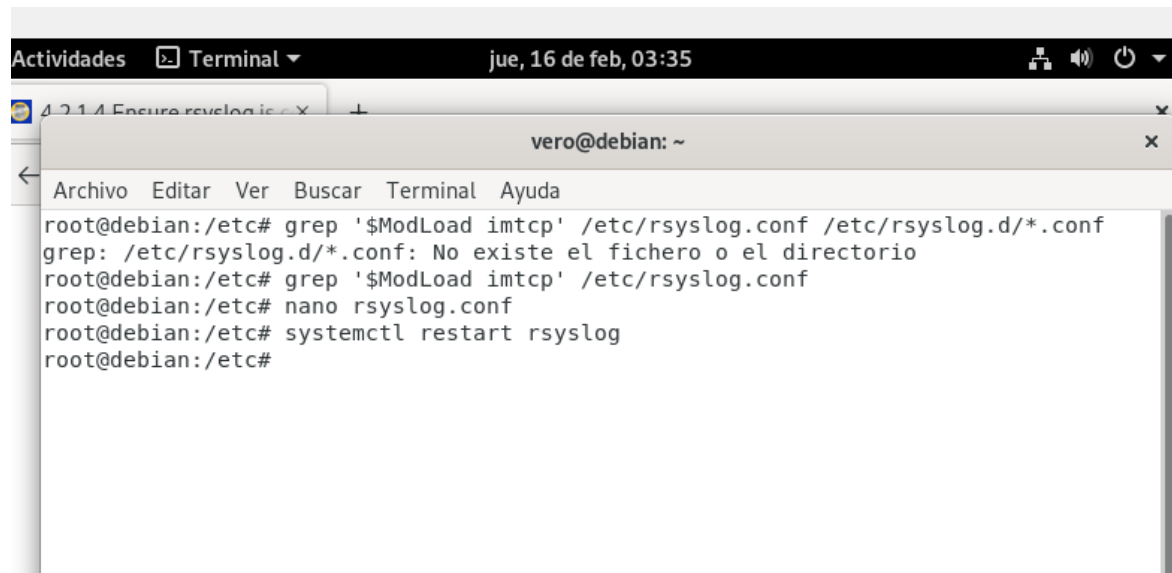
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

#####
#### GLOBAL DIRECTIVES ####
#####

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

At the bottom of the terminal, there is a status bar with various keyboard shortcuts for the nano editor:

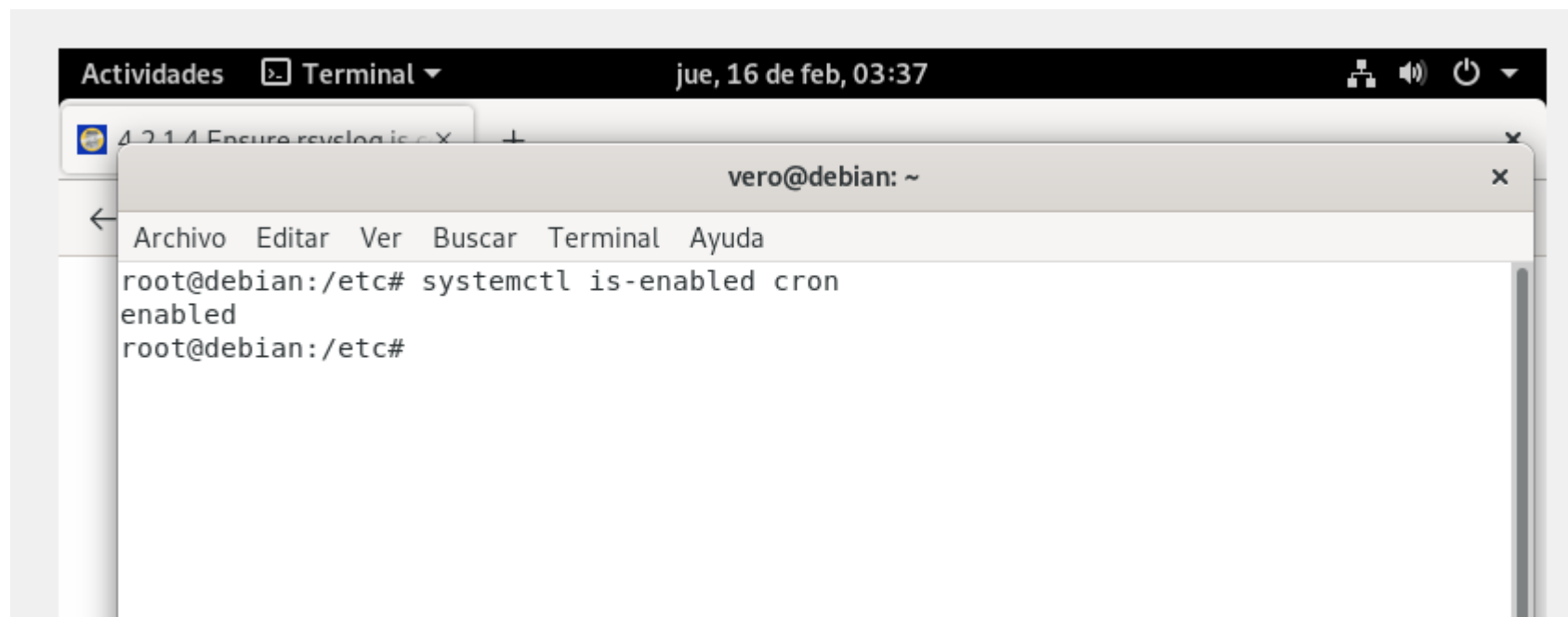
```
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```



A terminal window titled 'Terminal' with a timestamp of 'jue, 16 de feb, 03:35'. The window shows a series of commands and their outputs in a root shell at a Debian machine. The commands are: `grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf`, `grep '$ModLoad imtcp' /etc/rsyslog.conf`, `nano rsyslog.conf`, and `systemctl restart rsyslog`. The output of the first command is an error message: `grep: /etc/rsyslog.d/*.conf: No existe el fichero o el directorio`. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'.

```
root@debian:/etc# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
grep: /etc/rsyslog.d/*.conf: No existe el fichero o el directorio
root@debian:/etc# grep '$ModLoad imtcp' /etc/rsyslog.conf
root@debian:/etc# nano rsyslog.conf
root@debian:/etc# systemctl restart rsyslog
root@debian:/etc#
```

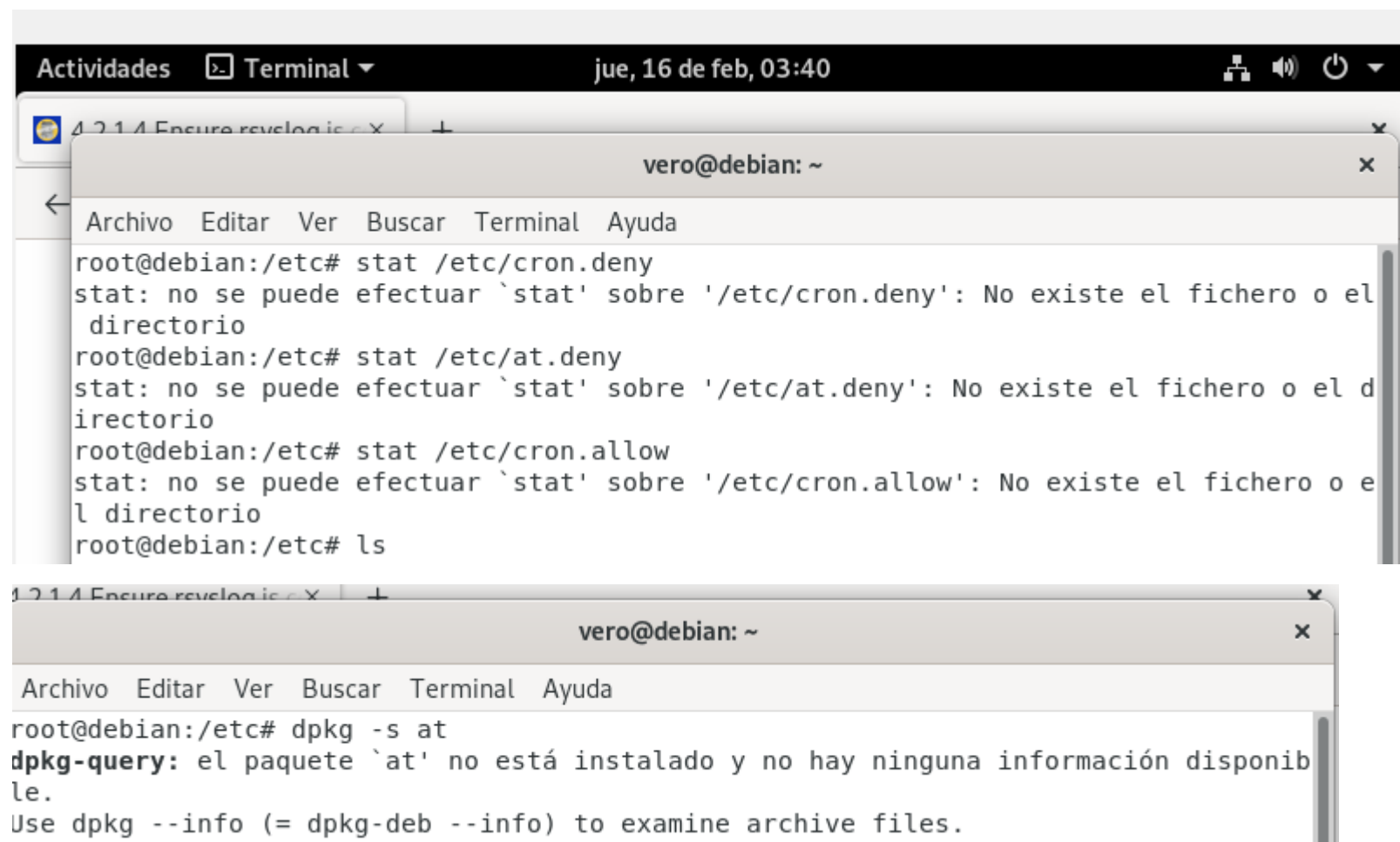
#### 5.1.1 Ensure cron daemon is enabled (Scored)



A terminal window titled 'Terminal' with a timestamp of 'jue, 16 de feb, 03:37'. The window shows a single command and its output in a root shell at a Debian machine: `systemctl is-enabled cron`. The output is `enabled`. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'.

```
root@debian:/etc# systemctl is-enabled cron
enabled
root@debian:/etc#
```

### 5.1.8 Ensure at/cron is restricted to authorized users (Scored)



```
root@debian:/etc# stat /etc/cron.deny
stat: no se puede efectuar `stat' sobre '/etc/cron.deny': No existe el fichero o el directorio
root@debian:/etc# stat /etc/at.deny
stat: no se puede efectuar `stat' sobre '/etc/at.deny': No existe el fichero o el directorio
root@debian:/etc# stat /etc/cron.allow
stat: no se puede efectuar `stat' sobre '/etc/cron.allow': No existe el fichero o el directorio
root@debian:/etc# ls
```

```
root@debian:/etc# dpkg -s at
dpkg-query: el paquete `at' no está instalado y no hay ninguna información disponible.
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

vboxuser@Debian10: ~

File Edit View Search Terminal Help

```
root@Debian10:~# stat /etc/at.deny
stat: cannot stat '/etc/at.deny': No such file or directory
root@Debian10:~# stat /etc/cron.allow
stat: cannot stat '/etc/cron.allow': No such file or directory
root@Debian10:~# rm /etc/cron.deny
rm: cannot remove '/etc/cron.deny': No such file or directory
root@Debian10:~# touch /etc/cron.allow
```

vboxuser@Debian10: ~

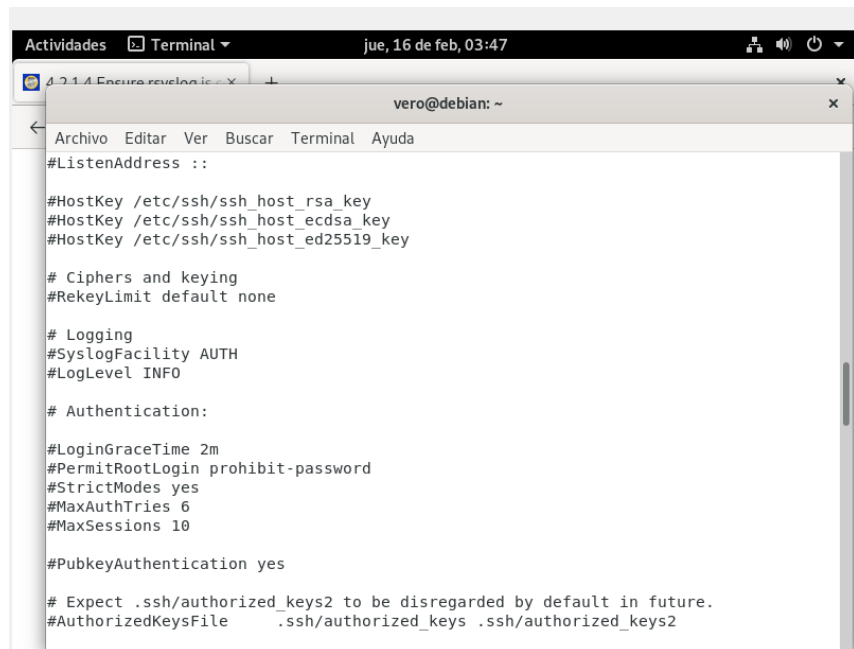
File Edit View Search Terminal Help

```
drwxr-xr-x  2 root root  4096 Feb 17 05:52 sysctl.d
drwxr-xr-x  5 root root  4096 Feb 17 05:52 systemd
drwxr-xr-x  2 root root  4096 Feb 17 05:52 terminfo
-rw-r--r--  1 root root    17 Feb 17 05:52 timezone
drwxr-xr-x  2 root root  4096 Jan 29  2021 tmpfiles.d
-rw-r--r--  1 root root 1260 Dec 14  2018 ucf.conf
drwxr-xr-x  4 root root  4096 Feb 17 05:52 udev
drwxr-xr-x  2 root root  4096 Feb 17 05:55 udisks2
drwxr-xr-x  3 root root  4096 Feb 17 05:54 ufw
drwxr-xr-x  2 root root  4096 Feb 17 05:51 update-motd.d
drwxr-xr-x  2 root root  4096 Feb 17 05:55 UPower
-rw-r--r--  1 root root 1523 Feb 23  2018 usb_modeswitch.conf
drwxr-xr-x  2 root root  4096 Feb 23  2018 usb_modeswitch.d
-rw-r--r--  1 root root   51 Jan 20  2019 vdpau_wrapper.cfg
drwxr-xr-x  2 root root  4096 Feb 17 05:52 vim
drwxr-xr-x  5 root root  4096 Feb 17 05:54 vulkan
-rw-r--r--  1 root root  4942 Apr  5  2019 wgetrc
drwxr-xr-x  2 root root  4096 Feb 17 05:56 wpa_supplicant
drwxr-xr-x 10 root root  4096 Feb 17 05:56 X11
-rw-r--r--  1 root root   642 Mar  1  2019 xattr.conf
drwxr-xr-x  5 root root  4096 Feb 17 05:55 xdg
root@Debian10:/etc# chown root:root /etc/cron.allow
root@Debian10:/etc# chmod g-wx,o-rwx /etc/cron.allow
root@Debian10:/etc#
```

```
vboxuser@Debian10: ~
File Edit View Search Terminal Help
root@Debian10:/etc# rm /etc/at.deny
rm: cannot remove '/etc/at.deny': No such file or directory
root@Debian10:/etc# touch /etc/at.allow
root@Debian10:/etc# chown root:root /etc/at.allow
root@Debian10:/etc# chmod g-wx,o-rwx /etc/at.allow
root@Debian10:/etc#
```

```
vboxuser@Debian10: ~
File Edit View Search Terminal Help
root@Debian10:/etc# rm /etc/at.deny
rm: cannot remove '/etc/at.deny': No such file or directory
root@Debian10:/etc# touch /etc/at.allow
root@Debian10:/etc# chown root:root /etc/at.allow
root@Debian10:/etc# chmod g-wx,o-rwx /etc/at.allow
root@Debian10:/etc# ls -la
total 1036
drwxr-xr-x 122 root root 4096 Feb 20 23:42 .
drwxr-xr-x 19 root root 4096 Feb 17 05:57 ..
-rw-r--r-- 1 root root 2981 Feb 17 05:50 adduser.conf
drwxr-xr-x 3 root root 4096 Feb 17 05:55 alsa
drwxr-xr-x 2 root root 4096 Feb 17 08:03 alternatives
-rw-r--r-- 1 root root 401 May 19 2019 anacrontab
drwxr-xr-x 8 root root 4096 Feb 17 07:24 apache2
-rw-r--r-- 1 root root 433 Oct 1 2017 apg.conf
drwxr-xr-x 3 root root 4096 Feb 17 05:54 apm
drwxr-xr-x 2 root root 4096 Feb 17 05:51 apparmor
drwxr-xr-x 7 root root 4096 Feb 17 08:03 apparmor.d
-rw-r--r-- 1 root root 769 Jan 26 2019 appstream.conf
drwxr-xr-x 7 root root 4096 Feb 17 05:57 apt
-rw-r----- 1 root root 0 Feb 20 23:42 at.allow
-rw-r----- 1 root root 0 Feb 20 23:36 at.allow
drwxr-xr-x 2 root root 4096 Feb 17 07:59 cron.d
drwxr-xr-x 2 root root 4096 Feb 17 07:24 cron.daily
drwxr-xr-x 2 root root 4096 Feb 17 05:50 cron.hourly
drwxr-xr-x 2 root root 4096 Feb 17 05:55 cron.monthly
-rw-r--r-- 1 root root 1042 Oct 11 2019 crontab
drwxr-xr-x 2 root root 4096 Feb 17 05:55 cron.weekly
drwxr-xr-x 5 root lp 4096 Feb 20 23:09 cups
drwxr-xr-x 2 root root 4096 Feb 17 05:56 cupshelpers
drwxr-xr-x 4 root root 4096 Feb 17 05:54 dbus-1
-rw-r--r-- 1 root root 2969 Feb 26 2019 debconf.conf
-rw-r--r-- 1 root root 6 Sep 3 08:00 debian_version
drwxr-xr-x 3 root root 4096 Feb 17 08:03 default
```

## 5.2.10 Ensure SSH root login is disabled (Scored)



A terminal window titled "Terminal" with a subtitle "jue, 16 de feb, 03:47". The window shows the contents of the /etc/ssh/sshd\_config file. The file is a configuration file for the SSH daemon, with various settings for listening address, host keys, ciphers, logging, and authentication. The current setting for PermitRootLogin is "prohibit-password".

```
Archivo Editar Ver Buscar Terminal Ayuda
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

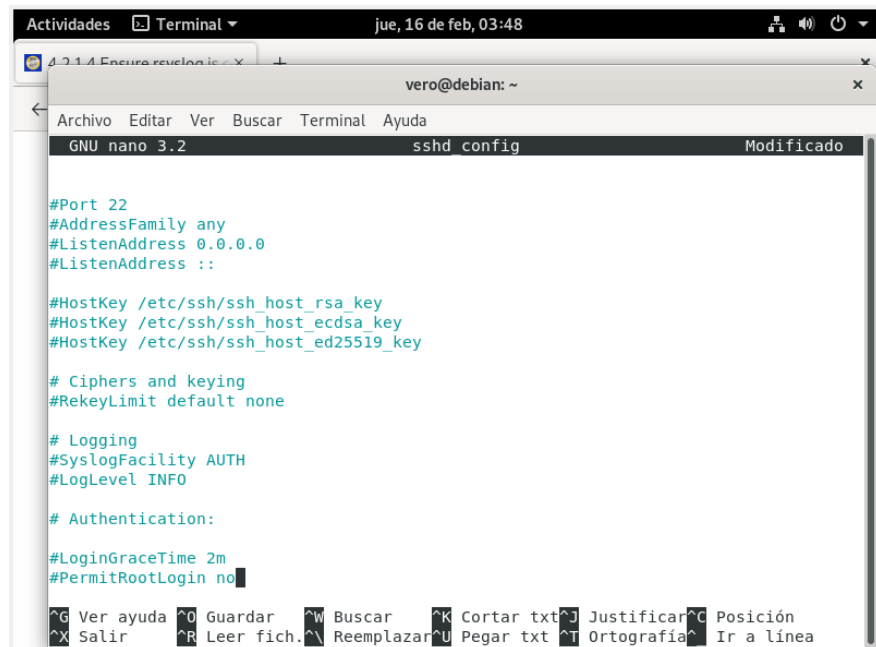
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```



A terminal window titled "Terminal" with a subtitle "jue, 16 de feb, 03:48". The window shows the nano editor editing the /etc/ssh/sshd\_config file. The file is a configuration file for the SSH daemon, with various settings for listening address, host keys, ciphers, logging, and authentication. The current setting for PermitRootLogin is "no".

```
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 3.2 sshd config Modificado

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

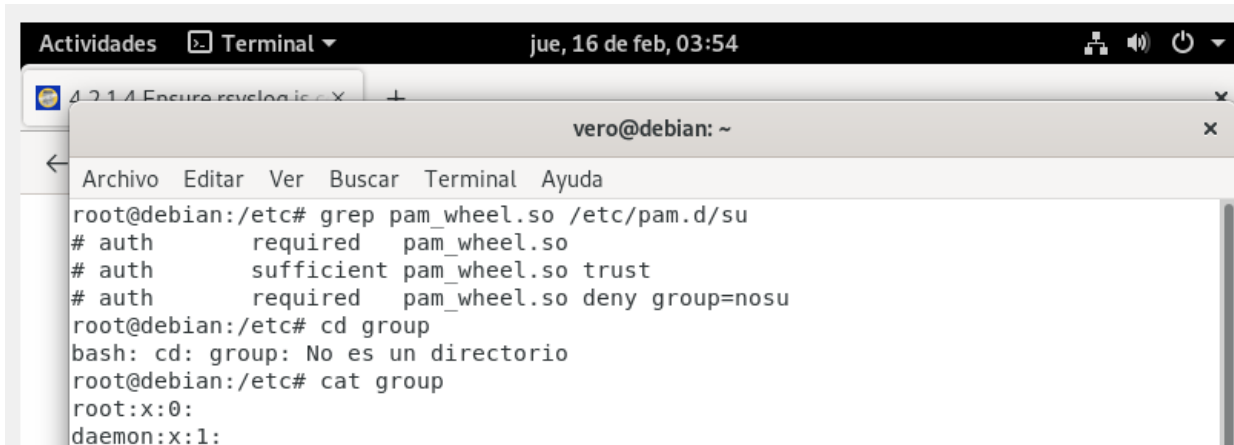
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
```

## 5.6 Ensure access to the su command is restricted (Scored)

A terminal window titled 'Terminal' with a date and time of 'jue, 16 de feb, 03:54'. The window shows a user 'vero@debian' at the root prompt. The user runs 'grep pam\_wheel.so /etc/pam.d/su', which returns three lines of configuration. Then, the user runs 'cd group', which returns an error. Finally, the user runs 'cat group', which returns the contents of the group file.

```
root@debian:/etc# grep pam_wheel.so /etc/pam.d/su
# auth      required    pam_wheel.so
# auth      sufficient  pam_wheel.so trust
# auth      required    pam_wheel.so deny group=nosu
root@debian:/etc# cd group
bash: cd: group: No es un directorio
root@debian:/etc# cat group
root:x:0:
daemon:x:1:
```

```
# Uncomment this to force users to be a member of group root
# before they can use `su'. You can also add "group=foo"
# to the end of this line if you want to use a group other
# than the default "root" (but this may have side effect of
# denying "root" user, unless she's a member of "foo" or explicitly
# permitted earlier by e.g. "sufficient pam_rootok.so").
# (Replaces the `SU_WHEEL_ONLY' option from login.defs)
# auth      required    pam_wheel.so

# Uncomment this if you want wheel members to be able to
# su without a password.
# auth      sufficient  pam_wheel.so trust

# Uncomment this if you want members of a specific group to not
# be allowed to use su at all.
# auth      required    pam_wheel.so deny group=nosu

# Uncomment and edit /etc/security/time.conf if you need to set
# time restraint on su usage.
# (Replaces the `PORTTIME_CHECKS_ENAB' option from login.defs
# as well as /etc/porttime)
# account   requisite   pam_time.so

# This module parses environment configuration file(s)
# and also allows you to use an extended config
```



vero@debian: ~

x

Archivo Editar Ver Buscar Terminal Ayuda

GNU nano 3.2

su

Modificado

```
#  
# The PAM configuration file for the Shadow `su' service  
#  
# This allows root to su without passwords (normal operation)  
auth        sufficient pam_rootok.so  
  
# Uncomment this to force users to be a member of group root  
# before they can use `su'. You can also add "group=foo"  
# to the end of this line if you want to use a group other  
# than the default "root" (but this may have side effect of  
# denying "root" user, unless she's a member of "foo" or explicitly  
# permitted earlier by e.g. "sufficient pam_rootok.so").  
# (Replaces the `SU_WHEEL_ONLY' option from login.defs)  
# auth        required    pam_wheel.so  
auth        required    pam_wheel.so use_uid group=sugroup  
  
# Uncomment this if you want wheel members to be able to  
# su without a password.
```

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición  
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^\_ Ir a línea

```
Actividades Terminal ▼ jue, 16 de feb, 04:18
vero@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
ssh:x:115:
lpadmin:x:116:vero
scanner:x:117:saned,vero
pulse:x:118:
pulse-access:x:119:
avahi:x:120:
saned:x:121:
colord:x:122:
geoclue:x:123:
Debian-gdm:x:124:
vero:x:1000:
systemd-coredump:x:999:
sugroup:x:1001:
root@debian:/etc# cd pam.d
root@debian:/etc/pam.d# ls
chfn          common-session-noninteractive  login      runuser-l
chpasswd      cron                          newusers  sshd
chsh          cups                          other      su
common-account gdm-autologin                passwd    sudo
common-auth   gdm-fingerprint              polkit-1  su-l
common-password gdm-launch-environment      ppp       systemd-user
common-session gdm-password                 runuser
root@debian:/etc/pam.d# nano su
root@debian:/etc/pam.d#
```