EJERCICIOS HARDENING

Prerrequisitos

- Descargar una de las "Debian.iso" de: Drive > Máquinas Virtuales > Blue Team
- Crear la máquina virtual virtual e instalar el sistema operativo Debian elegido en VirtualBox.

Ejercicios - CIS Benchmark

Realiza las siguientes tareas de hardening o bastionado sobre el sistema operativo Debian siguiendo las instrucciones de la guía CIS Benchmark:

- **1.1.2 Configure /tmp**

  Ensure /tmp is a separate partition → en el kernel podemos comprobar que no existe partición alguna debido a que durante la instalación no la hemos creado.

```
root@DEBIAN11:/tmp# findmnt --kernel
TARGET                       SOURCE     FSTYPE   OPTIONS
/                            /dev/sda1  ext4     rw,relatime,errors=remount-ro
├─/sys                       sysfs      sysfs    rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/security     securityfs security rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/cgroup           cgroup2    cgroup2  rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_
│ ├─/sys/fs/pstore           pstore     pstore   rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/bpf              none       bpf      rw,nosuid,nodev,noexec,relatime,mode=700
│ ├─/sys/kernel/tracing      tracefs    tracefs  rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/debug        debugfs    debugfs  rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/config       configfs   configfs rw,nosuid,nodev,noexec,relatime
│ └─/sys/fs/fuse/connections fusectl    fusectl  rw,nosuid,nodev,noexec,relatime
├─/proc                      proc       proc     rw,nosuid,nodev,noexec,relatime
│ └─/proc/sys/fs/binfmt_misc systemd-1  autofs   rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxp
├─/dev                       udev       devtmpfs rw,nosuid,relatime,size=984572k,nr_inodes=246143,m
│ ├─/dev/pts                 devpts     devpts   rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=
│ ├─/dev/shm                 tmpfs      tmpfs    rw,nosuid,nodev
│ ├─/dev/mqueue              mqueue     mqueue   rw,nosuid,nodev,noexec,relatime
│ └─/dev/hugepages           hugetlbfs  hugetlbf rw,relatime,pagesize=2M
└─/run                       tmpfs      tmpfs    rw,nosuid,nodev,noexec,relatime,size=201848k,mode=
  ├─/run/lock                tmpfs      tmpfs    rw,nosuid,nodev,noexec,relatime,size=5120k
  └─/run/user/1000           tmpfs      tmpfs    rw,nosuid,nodev,relatime,size=201844k,nr_inodes=50
    └─/run/user/1000/gvfs    gvfsd-fuse fuse.gvf rw,nosuid,nodev,relatime,user_id=1000,group_id=100
```

  Por tanto /tmp está en la misma partición que el sistema raíz

```
root@DEBIAN11:/tmp# df -h /tmp
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        19G  4.7G   13G  27% /
```

  Ensure nodev option set on /tmp partition→ en caso de haber tenido una partición realizando un nano del archivo fstab modificaríamos una línea similar a esta **/dev/sdXnúmero /tmp ext4 defaults 0 0**

```
  GNU nano 5.4                                 /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).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=4364a055-25f0-4ef0-95ad-d7c1510fea65 /               ext4    errors=remount-ro 0       1
# swap was on /dev/sda5 during installation
UUID=b65fa38d-865f-4b7e-8ca2-865e3ed7d9eb none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

  Ensure noexec option set on /tmp partition → esto guarda relación con el anterior enunciado, tendríamos que modificar

la línea mencionada anteriormente y añadir la opción noexec

```
  GNU nano 5.4                                 /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).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=4364a055-25f0-4ef0-95ad-d7c1510fea65 /               ext4    errors=remount-ro 0       1
# swap was on /dev/sda5 during installation
UUID=b65fa38d-865f-4b7e-8ca2-865e3ed7d9eb none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

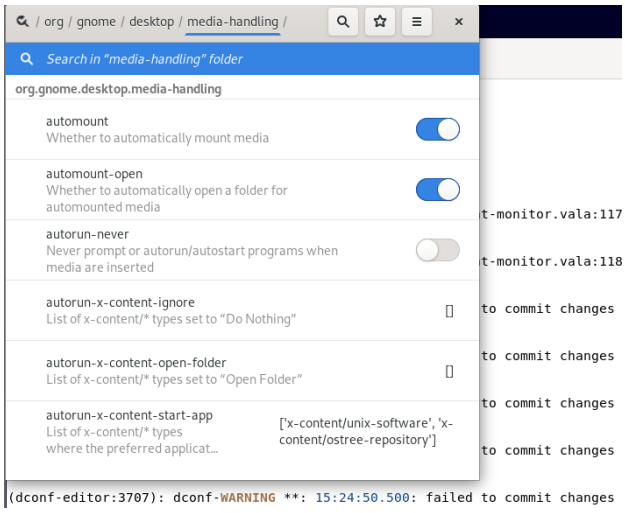
- **1.1.7 Configure /home**

  Ensure separate partition exists for /home→ como en el anterior ejercicio, ocurre que no existe partición del directorio /home y por tanto no podemos visualizarla

```
root@DEBIAN11:/home# findmnt --kernel
TARGET                          SOURCE     FSTYPE   OPTIONS
/                               /dev/sda1  ext4     rw,relatime,errors=remount-ro
├─/sys                          sysfs      sysfs    rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/security        securityfs security rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/cgroup              cgroup2    cgroup2  rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_
│ ├─/sys/fs/pstore              pstore     pstore   rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/bpf                 none       bpf      rw,nosuid,nodev,noexec,relatime,mode=700
│ ├─/sys/kernel/tracing         tracefs    tracefs  rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/debug           debugfs    debugfs  rw,nosuid,nodev,noexec,relatime
│ ├─/sys/kernel/config          configfs   configfs rw,nosuid,nodev,noexec,relatime
│ └─/sys/fs/fuse/connections    fusectl    fusectl  rw,nosuid,nodev,noexec,relatime
├─/proc                         proc       proc     rw,nosuid,nodev,noexec,relatime
│ └─/proc/sys/fs/binfmt_misc    systemd-1  autofs   rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxp
├─/dev                          udev       devtmpfs rw,nosuid,relatime,size=984572k,nr_inodes=246143,m
│ ├─/dev/pts                    devpts     devpts   rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=
│ ├─/dev/shm                    tmpfs      tmpfs    rw,nosuid,nodev
│ ├─/dev/mqueue                 mqueue     mqueue   rw,nosuid,nodev,noexec,relatime
│ └─/dev/hugepages              hugetlbfs  hugetlbf rw,relatime,pagesize=2M
└─/run                          tmpfs      tmpfs    rw,nosuid,nodev,noexec,relatime,size=201848k,mode=
  ├─/run/lock                   tmpfs      tmpfs    rw,nosuid,nodev,noexec,relatime,size=5120k
  └─/run/user/1000              tmpfs      tmpfs    rw,nosuid,nodev,relatime,size=201844k,nr_inodes=50
    └─/run/user/1000/gvfs       gvfsd-fuse fuse.gvf rw,nosuid,nodev,relatime,user_id=1000,group_id=100
```

- **1.1.9 Disable Automounting**

  Para esto instalamos la herramienta dconf-editor



Intentamos deshabilitar automount-open y no nos permite hacerlo debido a que no está habilitado de fábrica el automounting. Podríamos habilitarlo desde la carpeta /etc pero el objetivo de la práctica es deshabilitarlo

- **5.3.1 Ensure sudo is installed**

  Auditamos con el siguiente comando y verificamos que no está instalado

```
>  dpkg-query -W sudo sudo-ldap > /dev/null 2>&1 && dpkg-query -W -
f='${binary:Package}\t${Status}\t${db:Status-Status}\n' sudo sudo-ldap | awk
'($4=="installed" && $NF=="installed") {print "\n""PASS:""\n""Package
""\""$1"\""" is installed""\n"}' || echo -e "\nFAIL:\nneither \"sudo\" or
\"sudo-ldap\" package is installed\n"
bash: awk($4=="installed" && $NF=="installed") {print "\n""PASS:""\n""Package""\""$1"\""" is instal
led""\n"}: command not found

FAIL:
neither "sudo" or
 dpkg-query -W sudo sudo-ldap > /dev/null 2>&1 && dpkg-query -W -
f='
' sudo sudo-ldap | awk
'(==installed && ==installed) {print nPASS:nPackage
```

  Debido a esto instalamos sudo con apt install sudo

```
root@DEBIAN115:/# apt install sudo
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sudo is already the newest version (1.9.5p2-3+deb11u1).
sudo set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

  Y además lo upgradeamos

```
root@DEBIAN115:/# apt upgrade sudo
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
sudo is already the newest version (1.9.5p2-3+deb11u1).
Calculating upgrade... Done
The following packages will be upgraded:
  libnghttp2-14
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/77.2 kB of archives.
After this operation, 4,096 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Reading changelogs... Done
(Reading database ... 165536 files and directories currently installed.)
Preparing to unpack .../libnghttp2-14_1.43.0-1+deb11u1_amd64.deb ...
Unpacking libnghttp2-14:amd64 (1.43.0-1+deb11u1) over (1.43.0-1) ...
Setting up libnghttp2-14:amd64 (1.43.0-1+deb11u1) ...
Processing triggers for libc-bin (2.31-13+deb11u7) ...
root@DEBIAN115:/#
```

- **5.3.3 Ensure sudo log file exists**

  Primero lo instalamos

```
root@DEBIAN11:/etc/sudoers.d# dpkg-query -W sudo sudo-ldap > /dev/null 2>&1 && dpkg-query -W -
f='${binary:Package}\t${Status}\t${db:Status-Status}\n' sudo sudo-ldap | awk
'($4=="installed" && $NF=="installed") {print "\n""PASS:""\n""Package
""\""$1"\"" is installed""\n"}' || echo -e "\nFAIL:\nneither \"sudo\" or
\"sudo-ldap\" package is installed\n"
dpkg-query: no packages found matching -
Usage: mawk [Options] [Program] [file ...]

Program:
    The -f option value is the name of a file containing program text.
    If no -f option is given, a "--" ends option processing; the following
    parameters are the program text.
```

```
bash: $'($4=="installed" && $NF=="installed") {print "\\n""PASS:""\\n""Package\n""\\""$1"\\""" is i
nstalled""\\n"}': command not found

FAIL:
neither "sudo" or
"sudo-ldap" package is installed
```

Además, editamos el archivo de configuración de sudo

```
  GNU nano 5.4                          /etc/sudoers.tmp
#
# 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
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:

@includedir /etc/sudoers.d
```

Con este comando comprobamos si el archivo de registro de sudo existe en esta ubicación

```
root@DEBIAN11:/etc/sudoers.d# ls /var/log/sudo.log /var/log/auth.log
/var/log/auth.log  /var/log/sudo.log
```

- **1.7.1 Ensure message of the day is configured properly**

  Típicamente el mensaje del día se encuentra en la carpeta /etc/motd

```
root@DEBIAN11:/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.
```

Lanzamos el comando para auditar

```
root@DEBIAN11:/etc/update-motd.d#  grep -Eis "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release |
cut -d= -f2 | sed -e 's/"//g'))" /etc/motd
root@DEBIAN11:/etc/update-motd.d#
```

Al no obtener resultados se extrae que está configurado de manera correcta

- **1.9 Ensure updates, patches, and additional security software are installed**

  Para esto verificamos que se puede upgradear

```
root@DEBIAN11:/etc/update-motd.d# apt -s upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- **2.1.4.1 Ensure ntp access control is configured**

  Para comprobar esto realizamos el siguiente comando

```
root@DEBIAN11:/etc/update-motd.d# grep -P -- '^\h*restrict\h+((-4\h+)?|-
6\h+)default\h+(?:[^#\n\r]+\h+)*(?!(?:\2|\3|\4|\5))(\h*\bkod\b\h*|\h*\bnomodi
fy\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(?:[^#\n\r]+\h
+)*(?!(?:\1|\3|\4|\5))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\
bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(?:[^#\n\r]+\h+)*(?!(?:\1|\2|\4|\5))(\h*\bk
od\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h
*)\h+(?:[^#\n\r]+\h+)*(?!(?:\1|\2|\3|\5))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h
*\bnotrap\b\h*|\h*\bnopeer\b\h*|\h*\bnoquery\b\h*)\h+(?:[^#\n\r]+\h+)*(?!(?:\
1|\2|\3|\4))(\h*\bkod\b\h*|\h*\bnomodify\b\h*|\h*\bnotrap\b\h*|\h*\bnopeer\b\
h*|\h*\bnoquery\b\h*)\h*(?:\h+\H+\h*)*(?:\h+#.*)?$' /etc/ntp.conf
grep: the -P option only supports a single pattern
```

Como resultado obtenemos lo siguiente así que nos dirigimos a la carpeta /etc/ntp.conf.

```
root@DEBIAN11:/etc# ls
adduser.conf                fuse.conf        machine-id      rmt
alsa                        fwupd            magic           rpc
alternatives                gai.conf         magic.mime      rsyslog.conf
anacrontab                  gdm3             mailcap         rsyslog.d
apache2                     geoclue          mailcap.order   rygel.conf
apg.conf                    ghostscript      manpath.config  sane.d
apparmor                    glvnd            mime.types      security
apparmor.d                  gnome            mke2fs.conf     selinux
appstream.conf              gnome-chess      modprobe.d      sensors3.conf
apt                         groff            modules         sensors.d
avahi                       group            modules-load.d  services
bash.bashrc                 group-           mtab            sgml
bash_completion             grub.d           nanorc          shadow
bindresvport.blacklist      gshadow          netconfig       shadow-
binfmt.d                    gshadow-         network         shells
bluetooth                   gss              NetworkManager  skel
bogofilter.cf               gtk-2.0          networks        snmp
ca-certificates             gtk-3.0          nftables.conf   speech-dispatcher
ca-certificates.conf        host.conf        nsswitch.conf   ssh
chatscripts                 hostname         openal          ssl
```

Verificamos que no existe ningún archivo .conf de ntp

- **2.2.9 Ensure HTTP Server is not installed**

  Realizamos el siguiente comando y comprobamos que sí está instalado

```
root@DEBIAN11:/etc# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'
apache2
accountsservice install ok installed    installed
```

  Así que realizamos lo siguiente, lo eliminamos y lo volvemos a comprobar

```
root@DEBIAN11:/etc# apt purge apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'apache2' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@DEBIAN11:/etc#  dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'
accountsservice install ok installed    installed
acl     install ok installed    installed
adduser install ok installed    installed
adwaita-icon-theme      install ok installed    installed
aisleriot       install ok installed    installed
alsa-topology-conf      install ok installed    installed
```

- **2.3.4 Ensure telnet client is not installed**

  Aplicamos el anterior comando y confirmamos que está instalado

```
root@DEBIAN11:/etc# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'
tasksel-data    install ok installed    installed
telnet  install ok installed    installed
timgm6mb-soundfont      install ok installed    installed
totem   install ok installed    installed
```

  Los desinstalamos

```
root@DEBIAN11:/etc#  apt purge telnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  telnet*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 167 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 165623 files and directories currently installed.)
Removing telnet (0.17-42) ...
Processing triggers for man-db (2.9.4-2) ...
(Reading database ... 165613 files and directories currently installed.)
Purging configuration files for telnet (0.17-42) ...
```

- **3.2.2 Ensure IP forwarding is disabled**

  Para asegurarnos de esto tenemos que crear un script, nos dirigimos a /root

```
root@DEBIAN11:/etc# cd /root
root@DEBIAN11:~# nano script.sh
```

  Pegamos el script

```
  GNU nano 5.4                                  script.sh *
#!/usr/bin/env bash
{
        l_output="" l_output2=""
        l_parlist="net.ipv4.ip_forward=0 net.ipv6.conf.all.forwarding=0"
        l_searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf $([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/
{print $2}' /etc/default/ufw)"
        KPC()
        {
                l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)"
                l_pafile="$(grep -Psl -- "^\h*$l_kpname\h*=\h*$l_kpvalue\b\h*(#.*)?$"
$l_searchloc)"
                l_fafile="$(grep -s -- "^\s*$l_kpname" $l_searchloc | grep -Pv --
"\h*=\h*$l_kpvalue\b\h*" | awk -F: '{print $1}')"
                if [ "$l_krp" = "$l_kpvalue" ]; then
                l_output="$l_output\n - \"$l_kpname\" is set to \"$l_kpvalue\" in
the running configuration"
                else
                l_output2="$l_output2\n - \"$l_kpname\" is set to \"$l_krp\" in the
running configuration"
                fi
                if [ -n "$l_pafile" ]; then
                l_output="$l_output\n - \"$l_kpname\" is set to \"$l_kpvalue\" in
```

  Le damos permiso al archivo

```
root@DEBIAN11:~# chmod 744 script.sh
```

  Ejecutamos el comando

```
root@DEBIAN11:~# ./script.sh
root@DEBIAN115:~# ./script.sh
./script.sh: line 49: syntax error near unexpected token `&&'
./script.sh: line 49: `&& \'
```

Probamos con otro comando y damos el valor 0 para desahbilitarlo

```
root@DEBIAN115:~# "sysctl net.ipv6.conf.all.forwarding" (`ipv6') "sysctl net.ipv
4.ip_forward" (ipv4)
> 0
```

- **4.2.2 Configure rsyslog**

Ensure rsyslog is installed→ aplicamos el siguiente comando y confirmamos que está instalado

```
root@DEBIAN11:/etc# dpkg-query -W -f='${binary:Package}\t${Status}\t${db:Status-Status}\n'
rhythmbox-plugins       install ok installed    installed
rsyslog install ok installed    installed
rtkit   install ok installed    installed
rygel   install ok installed    installed
```

Ensure rsyslog service is enabled → verificamos de que esté habilitado de la siguiente manera

```
root@DEBIAN11:~# systemctl is-enabled rsyslog
enabled
root@DEBIAN11:~#
```

Ensure journald is configured to send logs to Rsyslog→ para esto nos dirigimos a la siguiente carpeta y modificamos el siguiente archivo

```
root@DEBIAN11:/etc/systemd# ls
journald.conf  network        pstore.conf    sleep.conf  system.conf     user
logind.conf    networkd.conf  resolved.conf  system      timesyncd.conf  user.conf
```

Añadimos la siguiente línea

```
  GNU nano 5.4                                journald.conf *
# See journald.conf(5) for details.

[Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
#SyncIntervalSec=5m
#RateLimitIntervalSec=30s
#RateLimitBurst=10000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#ForwardToSyslog=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
```

A continuación, guardamos el documento y reiniciamos el sistema

```
root@DEBIAN11:/etc/systemd# systemctl restart rsyslog
```

Ensure rsyslog default file permissions are configured → para esto nos dirigimos a la siguiente carpeta

```
root@DEBIAN11:/etc# nano rsyslog.conf
root@DEBIAN11:/etc#
```

En este archivo comprobamos que esté en 0640 o en un modo más restrictivo, en nuestro caso nos sirve con este modo.

```
  GNU nano 5.4                                    rsyslog.conf
#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

#
# Set the default permissions for all log files.
#
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
```

Ensure logging is configured (Manual)→ Dentro del mismo archivo .conf anterior modificamos una línea

```
 GNU nano 5.4                          rsyslog.conf *
#
$IncludeConfig /etc/rsyslog.d/*.conf


###############
#### RULES ####
###############

#
# 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

#
```

Tras esto verificamos que todo este correcto listando

```
root@DEBIAN11:/etc# ls -l /var/log/
total 1812
-rw-r--r--  1 root              root             46414 Nov 28 17:13 alternatives.log
drwxr-xr-x  2 root              root              4096 Nov 28 17:13 apt
-rw-r-----  1 root              adm               9544 Nov 28 17:49 auth.log
-rw-------  1 root              root              5869 Nov 28 13:48 boot.log
-rw-rw----  1 root              utmp                 0 Nov 28 13:27 btmp
drwxr-xr-x  2 root              root              4096 Nov 28 13:48 cups
-rw-r-----  1 root              adm              96773 Nov 28 17:58 daemon.log
-rw-r-----  1 root              adm               8254 Nov 28 17:58 debug
-rw-r--r--  1 root              root            831727 Nov 28 17:13 dpkg.log
-rw-r--r--  1 root              root             32032 Nov 28 13:46 faillog
-rw-r--r--  1 root              root              4475 Nov 28 13:44 fontconfig.log
drwx--x--x  2 root              Debian-gdm        4096 Nov 28 13:48 gdm3
drwxr-xr-x  3 root              root              4096 Nov 28 13:47 installer
drwxr-sr-x+ 3 root              systemd-journal   4096 Nov 28 13:47 journal
-rw-r-----  1 root              adm             168029 Nov 28 17:28 kern.log
-rw-rw-r--  1 root              utmp            292292 Nov 28 13:46 lastlog
-rw-r-----  1 root              adm             199693 Nov 28 17:53 messages
drwx------  2 root              root              4096 Nov 28 13:47 private
drwx------  2 speech-dispatcher root              4096 Nov 30  2022 speech-dispatcher
-rw-------  1 root              root               199 Nov 28 16:11 sudo.log
-rw-r-----  1 root              adm             304343 Nov 28 17:58 syslog
drwxr-x---  2 root              adm               4096 Nov 28 13:48 unattended-upgrades
-rw-r-----  1 root              adm              36420 Nov 28 17:40 user.log
-rw-------  1 root              root               939 Nov 28 13:46 vboxadd-install.log
-rw-r--r--  1 root              root                46 Nov 28 13:48 vboxadd-setup.log
-rw-r--r--  1 root              root               202 Nov 28 13:46 vboxadd-setup.log.1
-rw-r--r--  1 root              root             20757 Nov 28 13:46 vboxpostinstall.log
-rw-rw-r--  1 root              utmp              1152 Nov 28 13:56 wtmp
root@DEBIAN11:/etc#
```

Ensure rsyslog is configured to send logs to a remote log host → Volvemos a modificar el documento rsyslog.conf concretamente las siguientes líneas

```
  GNU nano 5.4                                  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")
```

Después de esto reiniciamos el servicio

```
root@DEBIAN115:/etc# systemctl restart rsyslog
root@DEBIAN115:/etc#
```

- **5.1.1 Ensure cron daemon is enabled and running**

  Para esto aplicamos el siguiente comando verificando que el Daemon esté habilitado

```
root@DEBIAN11:/etc# systemctl is-enabled cron
enabled
```

  Y corriendo

```
root@DEBIAN11:/etc# systemctl status cron | grep 'Active: active (running)'
     Active: active (running) since Tue 2023-11-28 13:48:12 CET; 4h 17min ago
root@DEBIAN11:/etc#
```

- **5.1.8 Ensure cron is restricted to authorized users**

  Para realizar lo siguiente directamente remediamos el problema y volvimos a preguntar y obtuvimos lo buscado

```
root@DEBIAN11:/etc#  rm /etc/cron.deny
rm: cannot remove '/etc/cron.deny': No such file or directory
root@DEBIAN11:/etc# touch /etc/cron.allow
root@DEBIAN11:/etc# chmod g-wx,o-rwx /etc/cron.allow
root@DEBIAN11:/etc# chown root:root /etc/cron.allow
root@DEBIAN11:/etc# stat /etc/cron.deny
stat: cannot statx '/etc/cron.deny': No such file or directory
```

  Después de esto comprobamos el archivo /cron.allow

```
root@DEBIAN11:/etc#  stat /etc/cron.allow
  File: /etc/cron.allow
  Size: 0               Blocks: 0          IO Block: 4096   regular empty file
Device: 801h/2049d      Inode: 783517      Links: 1
Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2023-11-28 18:06:58.031540130 +0100
Modify: 2023-11-28 18:06:58.031540130 +0100
Change: 2023-11-28 18:07:25.115060535 +0100
 Birth: 2023-11-28 18:06:58.031540130 +0100
```

- **5.2.7 Ensure SSH root login is disabled**

  Para solucionar esto, nos dirigimos a la siguiente carpeta

```
root@DEBIAN11:/etc# cd ssh
root@DEBIAN11:/etc/ssh# nano ssh_config
```

  Una vez dentro modificamos el archivo

```
 GNU nano 5.4                                ssh_config *
Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
    PermitRootLogin no
```

- **5.3.7 Ensure access to the su command is restricted**

  Modificamos el archivo su de la carpeta /pam.d/

```
root@DEBIAN11:/etc/pam.d# nano su
```

```
 GNU nano 5.4                                        su *
#
# 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 wheel
# 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 "wheel" (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 restrainst on su usage.
```