

Actividad 13. Configuración de seguridad de Linux

- [1. Busca información sobre cómo proteger la seguridad de Linux](#)
- [2. Elabora un resumen sobre las opciones de configuración de Linux](#)
- [3. Revisa y muestra las opciones de seguridad de tu equipo Linux](#)

1. Busca información sobre cómo proteger la seguridad de Linux.
2. Elabora un resumen sobre las opciones de configuración de Linux.
3. Revisa y muestra las opciones de seguridad de tu equipo Linux.

1. Busca información sobre cómo proteger la seguridad de Linux

Proteger la seguridad de tu sistema Linux implica implementar una serie de prácticas y configuraciones para minimizar las vulnerabilidades y proteger los datos.

1. **Mantener el Sistema Actualizado**: Instalar actualizaciones de seguridad y parches regularmente para cerrar cualquier vulnerabilidad conocida.
2. **Configurar un Firewall**: Utilizar herramientas como “*iptables*” o “*firewalld*” para controlar el tráfico entrante y saliente.
3. **Usar Autenticación Fuerte**: Configurar la autenticación de Dos Factores (2FA) usando contraseñas fuertes y seguras, deshabilitando el acceso root directo.
4. **Configurar SELinux o AppArmor**: Utilizar Security-Enhanced Linux (SELinux) o AppArmor para aplicar las políticas de seguridad estrictas.
5. **Configurar el Sistema de Archivos**: Montar las particiones con opciones de seguridad, como “*noexec*”, “*nosuid*”, “*nodev*”.
6. **Auditoría y Monitoreo**: Utilizar herramientas como “*auditd*” y “*logwatch*” para monitorear el sistema y revisar logs regularmente.

7. **Deshabilitar Servicios Innecesarios**: Desactivar los servicios y dominios que no sean necesarios para reducir la superficie de ataques.
8. **Usar Software de Antivirus**: Software como ClamAV puede ayudar a detectar malware y ser más seguro el sistema.
9. **Configurar Permisos y Propietarios de Archivos**: Usar los permisos mínimos necesarios y configurar los propietarios correctamente.
10. **Habilitar CIFS y Configuración de Seguridad**: Utilizar opciones como “/etc/hosts.deny” y “/etc/hosts.allow” para controlar el acceso a los servicios.

2. Elabora un resumen sobre las opciones de configuración de Linux

Las opciones de configuración de Linux son variadas y dependen de la distribución específica, pero algunas áreas comunes son:

1. **Configuración del Sistema y Red**: Establecer interfaces de red, direcciones IP, gateways y servidores DNS.

ARCHIVOS DE CONFIGURACIÓN DE RED:

- **Debian/Ubuntu**: “/etc/network/interfaces”
- **General**: “/etc/hostname”

2. **Gestión de Usuarios y Grupos**: Controlar la creación, gestión y permisos de usuarios y grupos.

ARCHIVOS CLAVE:

- **Lista de usuarios**: “/etc/passwd”
- **General**: “/etc/shadow”
- **Lista de grupos**: “/etc/group”

3. **Configuración del Sistema de Archivos**: Asegurar que los sistemas de archivos se monten correctamente con las opciones adecuadas para mejorar la seguridad.

ARCHIVO PRINCIPAL:

- **Cómo y dónde se van a montar los sistemas de archivos al inicio:** `“/etc/fstab”`

OPCIONES DE MONTAJE:

- `“defaults”`, `“noexec”`, `“nosuid”`, `“nodev”`, `“ro”` (sólo lectura), etc.

4. **Configuración de Inicio y Servicios**: Controlar qué servicios se inician al arrancar y gestionar el estado de los servicios.

HERRAMIENTAS DE GESTIÓN:

- **Systemd**: Archivos de unidad en `“/etc/systemd/system/”` y comandos como `“systemctl”`.
- **SysVinit**: Scripts de inicio en `“/etc/init.d/”` y comandos como `“service”`.

5. **Configuración de Seguridad**: Configurar las políticas de acceso y controlar el tráfico de la red para proteger el sistema.

SSH:

- **Archivos de Configuración:** `“/etc/ssh/sshd_config”`
- **Parámetros Clave:** `“PermitRootLogin”`, `“PasswordAuthentication”`, `“PubkeyAuthentication”`.

SELinux:

- **Archivo de Configuración:** `“/etc/selinux/config”`
- **Comando:** `“sestatus”` para verificar el estado.

AppArmor:

- **Archivos de Configuración:** `“/etc/apparmor.d/”`
- **Comando:** `“sudo aa-status”` para verificar el estado.

Firewall:

- **Herramientas:** `“iptables”`, `“ufw”`, `“firewalld”`
- **Archivos de Configuración:** `“/etc/iptables/rules.v4”` (iptables), reglas definidas en `“/etc/ufw”` (ufw).

6. **Configuración de Paquetes y Repositorios**: Gestionar la instalación, actualización y eliminación de los paquetes de software.

DEBIAN/UBUNTU:

- **Archivo de Repositorios:** `/etc/apt/sources.list`
- **Comando:** `apt-get`, `apt-cache`

RED HAT/CENTOS/FEDORA:

- **Archivos de Configuración:** `/etc/yum.repos.d/`
- **Comando:** `yum`, `dnf`

7. **Configuración de Kernel:** Ajustar las configuraciones de bajo nivel del kernel para optimizar su rendimiento y seguridad.

ARCHIVOS PRINCIPAL Y COMANDOS:

- **Parámetros del kernel:** `/etc/sysctl.conf`
- **Comando:** `sysctl -a`
- **Aplicar los cambios:** `sysctl -p`

8. **Automatización y Scripts:** Programar tareas que se ejecutan periódicamente pero sin la dependencia estricta de la hora exacta.

CRONTAB:

- **Archivos:** `/etc/crontab`, `crontab -e`
- **Propósito:** Programar tareas automáticas en intervalos regulares.

ANACRON:

- **Archivos:** `/etc/anacrontab`
- **Propósito:** Programar tareas que se ejecutan periódicamente pero sin la dependencia estricta de la hora exacta.

9. **Auditoría y Monitoreo:** Monitorizar y registrar los eventos del sistema para detectar y responder a los incidentes de seguridad.

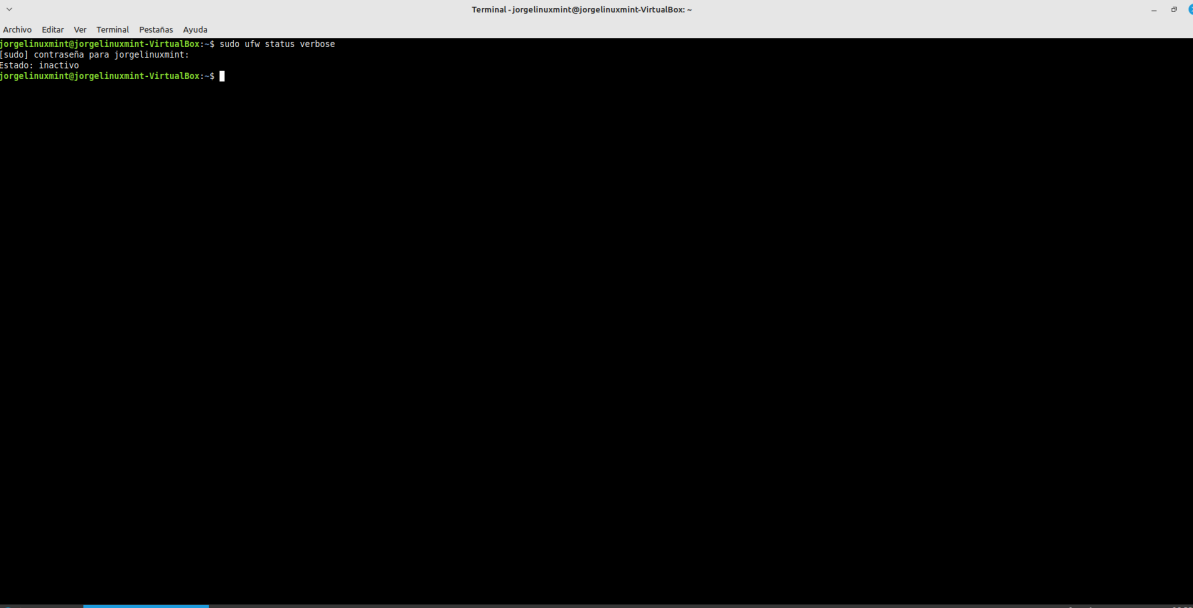
HERRAMIENTAS:

- **Sistema de auditoría del kernel:** `audit`
- **Archivos de configuración:** `/etc/audit/auditd.conf`
- **Comandos:** `auditctl`, `ausearch`, `aureport`

3. Revisa y muestra las opciones de seguridad de tu equipo Linux

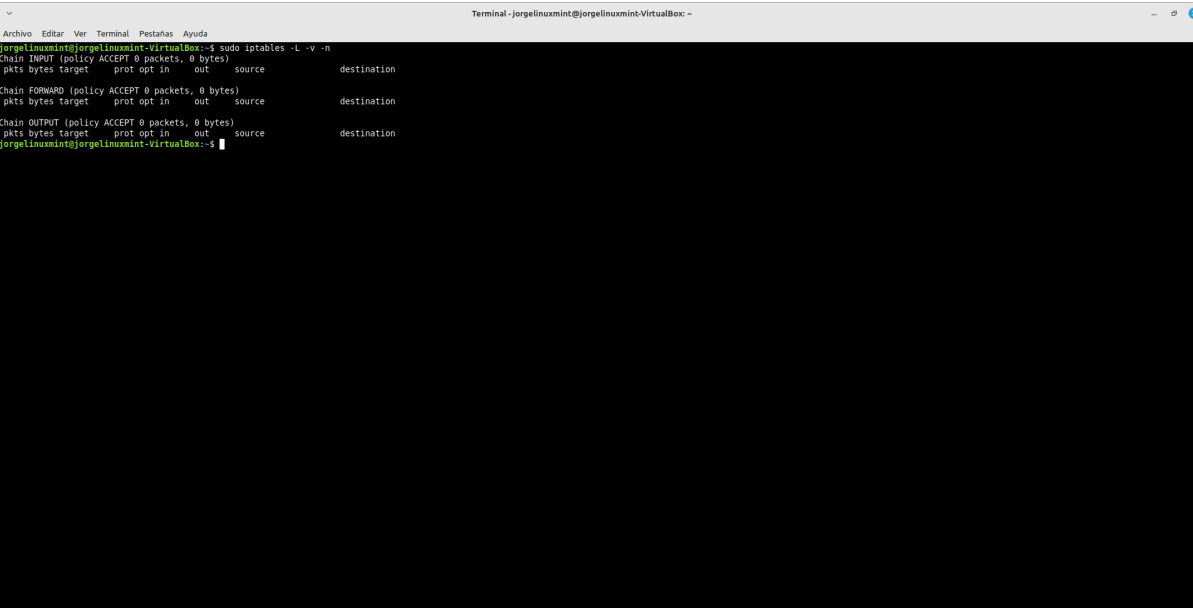
Estado del Firewall:

UFW: “*sudo ufw status verbose*”

A terminal window titled "Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -" showing the command "sudo ufw status verbose" being executed. The output indicates that UFW is inactive and prompts for a password.

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo ufw status verbose
[sudo] contraseña para jorgelinuxmint:
Estado: inactivo
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

IPTables: “*sudo iptables -L -v -n*”

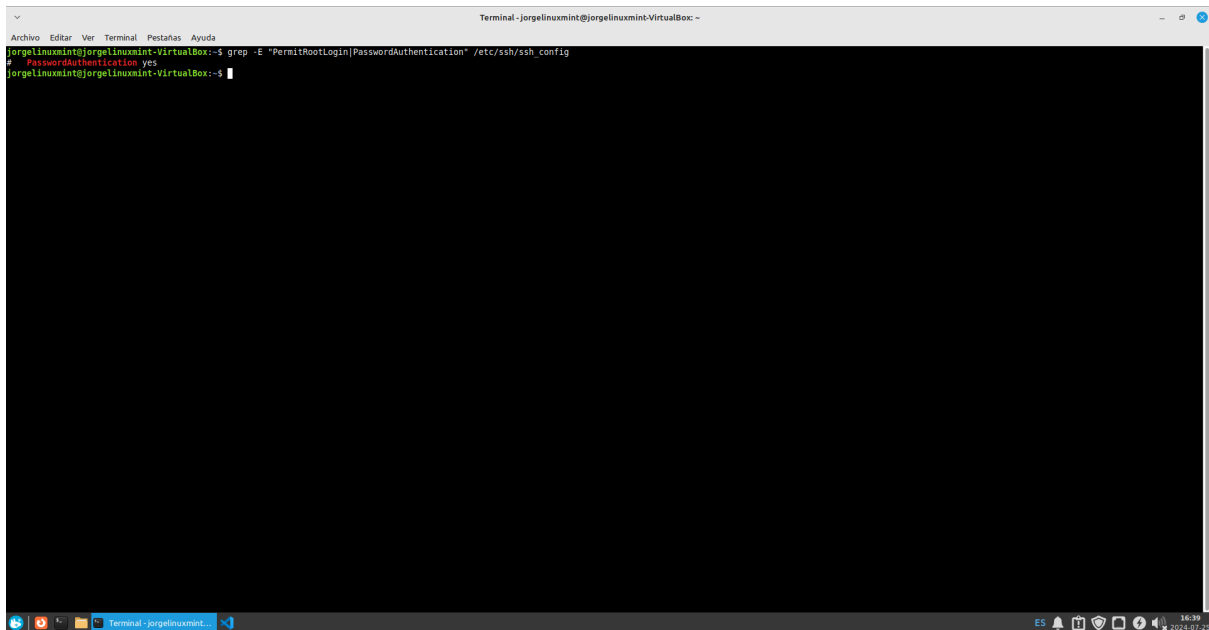
A terminal window titled "Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -" showing the command "sudo iptables -L -v -n" being executed. The output displays the default iptables rules for INPUT, FORWARD, and OUTPUT chains.

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination

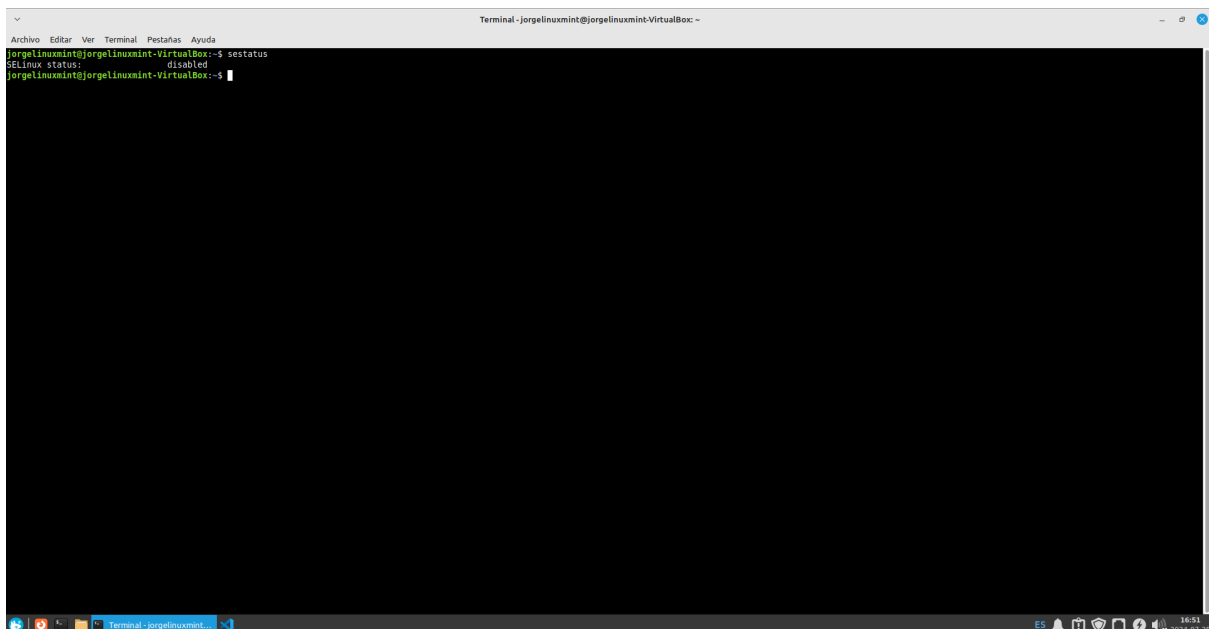
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source    destination
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Configuración de SSH: “`grep -E "PermitRootLogin|PasswordAuthentication" /etc/ssh/sshd_config`”, “`/etc/ssh/sshd_config`”

A terminal window titled 'Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox' showing a command being executed. The command is 'grep -E "PermitRootLogin|PasswordAuthentication" /etc/ssh/sshd_config'. The output shows 'PasswordAuthentication yes'. The terminal has a dark background with a light-colored prompt and output text. The window's title bar and menu bar are visible at the top, and the system tray is at the bottom right.

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ grep -E "PermitRootLogin|PasswordAuthentication" /etc/ssh/sshd_config
# PasswordAuthentication yes
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Políticas de SELinux o AppArmor:
SELinux: “`sestatus`”

A terminal window titled 'Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox' showing a command being executed. The command is 'sestatus'. The output shows 'SELinux status: disabled'. The terminal has a dark background with a light-colored prompt and output text. The window's title bar and menu bar are visible at the top, and the system tray is at the bottom right.

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sestatus
SELinux status: disabled
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

AppArmor: “`sudo aa-status`”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo aa-status
apparmor module is loaded.
29 profiles are loaded.
27 profiles are in enforce mode.
  /usr/bin/evince
  /usr/bin/evince-previewer
  /usr/bin/evince-previewer/sanitized_helper
  /usr/bin/evince-thumbnailer
  /usr/bin/evince/sanitized_helper
  /usr/bin/evince/snap_browsers
  /usr/bin/evince
  /usr/bin/redshift
  /usr/lib/NetworkManager/nm-dhcp-client.action
  /usr/lib/NetworkManager/nm-dhcp-helper
  /usr/lib/connman/scripts/dhclient-script
  /usr/lib/cups/backend/cups-pdf
  /usr/lib/lightdm/lightdm-guest-session
  /usr/lib/lightdm/lightdm-guest-session/chromium
  /usr/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/cupsd/third_party
  /usr/sbin/dhclient
  libreoffice-senddoc
  libreoffice-soffice/ppq
  libreoffice.xpdiffimport
  lib release
  man filter
  man groff
  nvidia_modprobe
  nvidia_modprobe/kmod
  tcpdump
2 profiles are in complain mode.
  libreoffice-oosplash
  libreoffice-soffice
8 profiles are in kill mode.
8 profiles are in unconfined mode.
2 processes have profiles defined.
2 processes are in enforce mode.
  /usr/sbin/cups-browsed (833)
  /usr/sbin/cupsd (788)
8 processes are in complain mode.
8 processes are unconfined but have a profile defined.
8 processes are in mixed mode.
8 processes are in kill mode.
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Usuarios y Grupos:

Listar Usuarios: “cat /etc/passwd”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:100:systemd Network Management,,/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:100:systemd Resolver,,/run/systemd:/usr/sbin/nologin
messagebus:x:102:105:nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,/run/systemd:/usr/sbin/nologin
syslog:x:104:111:/home/syslog:/usr/sbin/nologin
apt:x:105:65534:nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,/var/lib/tpm:/bin/false
rtkit:x:107:113:RealtimeKit,,/proc:/usr/sbin/nologin
systemd-coredump:x:108:114:systemd Core Dumper,,/run/systemd:/usr/sbin/nologin
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,/usr/sbin/nologin
uidm:x:110:115:/run/uidm:/usr/sbin/nologin
cups-pk-helper:x:111:115:user for cups-pk-helper service,,/home/cups-pk-helper:/usr/sbin/nologin
lightdm:x:112:120:Light Display Manager:/var/lib/lightdm:/bin/false
tcpdump:x:113:122:/nonexistent:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,/run/speech-dispatcher:/bin/false
avahi-autoipd:x:115:125:Avahi autoip daemon,,/var/lib/avahi-autoipd:/usr/sbin/nologin
ushm:x:116:46:ushm daemon,,/var/lib/ushm:/usr/sbin/nologin
nm-openvpn:x:117:126:NetworkManager OpenVPN,,/var/lib/openvpn/chroot:/usr/sbin/nologin
geoclue:x:118:127:/var/lib/geoclue:/usr/sbin/nologin
dmesg:x:119:65534:dmesg,,/var/lib/dmcc:/usr/sbin/nologin
pulse:x:120:128:PulseAudio daemon,,/run/pulse:/usr/sbin/nologin
flatpak:x:121:131:Flatpak system-wide installation helper,,/nonexistent:/usr/sbin/nologin
avahi:x:122:132:Avahi mDNS daemon,,/run/avahi-daemon:/usr/sbin/nologin
saned:x:123:133:/var/lib/saned:/usr/sbin/nologin
colord:x:124:134:colord colour management daemon,,/var/lib/colord:/usr/sbin/nologin
fwupd-refresh:x:125:135:fwupd-refresh user,,/run/systemd:/usr/sbin/nologin
hplip:x:126:7:HPLIP system user,,/run/hplip:/bin/false
jorgelinuxmint:x:1000:1000:jorgelinuxmint,,/home/jorgelinuxmint:/bin/bash
sssd:x:127:137:SSSD system user,,/var/lib/sss:/usr/sbin/nologin
vboxadd:x:999:1:/var/run/vboxadd:/bin/false
whoopsie:x:128:138:/nonexistent:/bin/false
gdm:x:129:138:Gnome Display Manager:/var/lib/gdm3:/bin/false
usuario1:x:1001:1001:/home/usuario1:/bin/sh
usuario2:x:1002:1002:/home/usuario2:/bin/sh
```

Listar Grupos: “cat /etc/group”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,jorgelinuxmint
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:jorgelinuxmint
floppy:x:25:
tape:x:26:
audio:x:27:jorgelinuxmint
audio:x:29:pulse
dip:x:30:jorgelinuxmint
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:jorgelinuxmint
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
crontab:x:104:
messagebus:x:105:
systemd-timesync:x:106:
input:x:107:
sgx:x:108:
wmx:x:109:
render:x:110:
syslog:x:111:
ts:x:112:
rtkit:x:113:
```

Configuración de Auditoría: “*sudo cat /etc/audit/auditd.conf*”

```
Terminal - root@jorgelinuxmint-VirtualBox: /etc/audit
root@jorgelinuxmint-VirtualBox:/etc/audit# cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
name_format = NONE
#name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
#etcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
#etcp_client_ports = 1024-65535
tcp_client_max_idle = 0
transport = TCP
krb5_principal = auditd
#krb5_key_file = /etc/audit/audit.key
distribute_network = no
q_depth = 1280
overflow_action = SYSLOG
max_restarts = 10
plugin_dir = /etc/audit/plugins.d
end_of_event_timeout = 2
root@jorgelinuxmint-VirtualBox:/etc/audit#
```

Servicios Activos: “*sudo systemctl list-units --type=service --state=running*”


```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo systemctl list-units --type=service --state=running
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
accounts-daemon.service            loaded active running Accounts Service
acpid.service                      loaded active running ACPI event daemon
auditd.service                     loaded active running Security Auditing Service
avahi-daemon.service               loaded active running Avahi mDNS/DNS-SD Stack
colord.service                     loaded active running Manage, Install and Generate Color Profiles
cron.service                       loaded active running Regular background program processing daemon
cups-browsed.service               loaded active running Make remote CUPS printers available locally
cups.service                       loaded active running CUPS Scheduler
dbus.service                       loaded active running D-Bus System Message Bus
getty@tty1.service                 loaded active running Getty on tty1
irqbalance.service                loaded active running irqbalance daemon
kerneloops.service                loaded active running Tool to automatically collect and submit kernel crash signatures
lightdm.service                    loaded active running Light Display Manager
ModemManager.service              loaded active running Modem Manager
networkd-dispatcher.service         loaded active running Dispatcher daemon for systemd-networkd
NetworkManager.service            loaded active running Network Manager
nmbd.service                       loaded active running Samba SMB Daemon
packagekit.service                loaded active running PackageKit Daemon
polkit.service                     loaded active running Authorization Manager
power-profiles-daemon.service        loaded active running Power Profiles daemon
rsyslog.service                   loaded active running System Logging Service
rtkit-daemon.service               loaded active running RealtimeKit Scheduling Policy Service
smbd.service                       loaded active running Samba SMB Daemon
switcheroo-control.service          loaded active running Switcheroo Control Proxy service
systemd-journald.service            loaded active running Journal Service
systemd-logind.service              loaded active running User Login Management
systemd-resolved.service            loaded active running Network Name Resolution
systemd-udevd.service               loaded active running Rule-based Manager for Device Events and Files
udisks2.service                   loaded active running Disk Manager
upower.service                     loaded active running Daemon for power management
user@1000.service                  loaded active running User Manager for UID 1000
vboxadd-service.service            loaded active running vboxadd-service.service
wpa_supplicant.service             loaded active running WPA supplicant
zfs-zed.service                    loaded active running ZFS Event Daemon (zed)

LOAD = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB = The low-level unit activation state, values depend on unit type.
34 loaded units listed.
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Configuración del Sistema de Archivos: “cat /etc/fstab”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ 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/sda3 during installation
UUID=50d6272e-8692-42c1-bf94-f91b97138029 /
# /boot/efi was on /dev/sda2 during installation
UUID=912E-4027 /boot/efi vfat umask=0077 0 1
#swapfile none none swap sw 0 0
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Parámetros del Kernel: “sudo sysctl -a”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo sysctl -a
abi.vsyscall32 = 1
debug.exception-trace = 1
debug.kprobes-optimization = 1
dev.cdrom.autolose = 1
dev.cdrom.autoject = 0
dev.cdrom.check-media = 0
dev.cdrom.debug = 0
dev.cdrom.info = CD-ROM information, Id: cdrom.c 3.20 2003/12/17
dev.cdrom.info =
dev.cdrom.info = drive name: sr0
dev.cdrom.info = drive speed: 32
dev.cdrom.info = drive # of slots: 1
dev.cdrom.info = Can close tray: 1
dev.cdrom.info = Can open tray: 1
dev.cdrom.info = Can lock tray: 1
dev.cdrom.info = Can change speed: 1
dev.cdrom.info = Can select disk: 0
dev.cdrom.info = Can read multisession: 1
dev.cdrom.info = Can read MCN: 1
dev.cdrom.info = Reports media changed: 1
dev.cdrom.info = Can play audio: 1
dev.cdrom.info = Can write CD-R: 0
dev.cdrom.info = Can write CD-RW: 0
dev.cdrom.info = Can read DVD: 1
dev.cdrom.info = Can write DVD-R: 0
dev.cdrom.info = Can write DVD-RAM: 0
dev.cdrom.info = Can read MMC: 1
dev.cdrom.info = Can write MMC: 1
dev.cdrom.info = Can write RAM: 1
dev.cdrom.info =
dev.cdrom.lock = 0
dev.hpet.max-user-freq = 64
dev.mac_hid.mouse.button2-keycode = 97
dev.mac_hid.mouse.button3-keycode = 100
dev.mac_hid.mouse.button-emulation = 0
dev.parpport.default.spintime = 500
dev.parpport.default.timeslice = 200
dev.raid.speed-limit-max = 200000
dev.raid.speed-limit-min = 10000
dev.scsi.logging-level = 0
dev.tty.ldisc-autoload = 1
fs.aio-max-nr = 65536
fs.aio-nr = 0
fs.binfmt_misc.python3/10 = enabled
fs.binfmt_misc.python3/10 = interpreter /usr/bin/python3.10
fs.binfmt_misc.python3/10 = flags:
fs.binfmt_misc.python3/10 = offset 0
fs.binfmt_misc.python3/10 = magic 0f0d0d0a
fs.binfmt_misc.status = enabled
fs.dentry-state = 54292 24119 45 0 9631 0
fs.dir-notify-enable = 1
```

Tareas Programadas (Cron Jobs):

Tareas del Usuario Actual: “*crontab -l*”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ crontab -l
no crontab for jorgelinuxmint
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Tareas del Sistema: “*sudo cat /etc/crontab*”, “*sudo ls /etc/cron.d/*”, “*sudo ls /etc/cron.daily/*”, “*sudo ls /etc/cron.hourly/*”, “*sudo ls /etc/cron.monthly/*”, “*sudo ls /etc/cron.weekly/*”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo ls /etc/cron.d/
anacron  e2scrub_all  zfsutils-linux
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo ls /etc/cron.daily/
anacron  apt-compat  aptitude  cracklib-runtime  dpkg  logrotate  man-db  plocate  samba
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo ls /etc/cron.hourly/
anacron
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo ls /etc/cron.monthly/
anacron
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo ls /etc/cron.weekly/
anacron  man-db
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Configuración de SSH Detallada: “*sudo cat /etc/ssh/sshd_config*”

```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo cat /etc/ssh/sshd_config
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

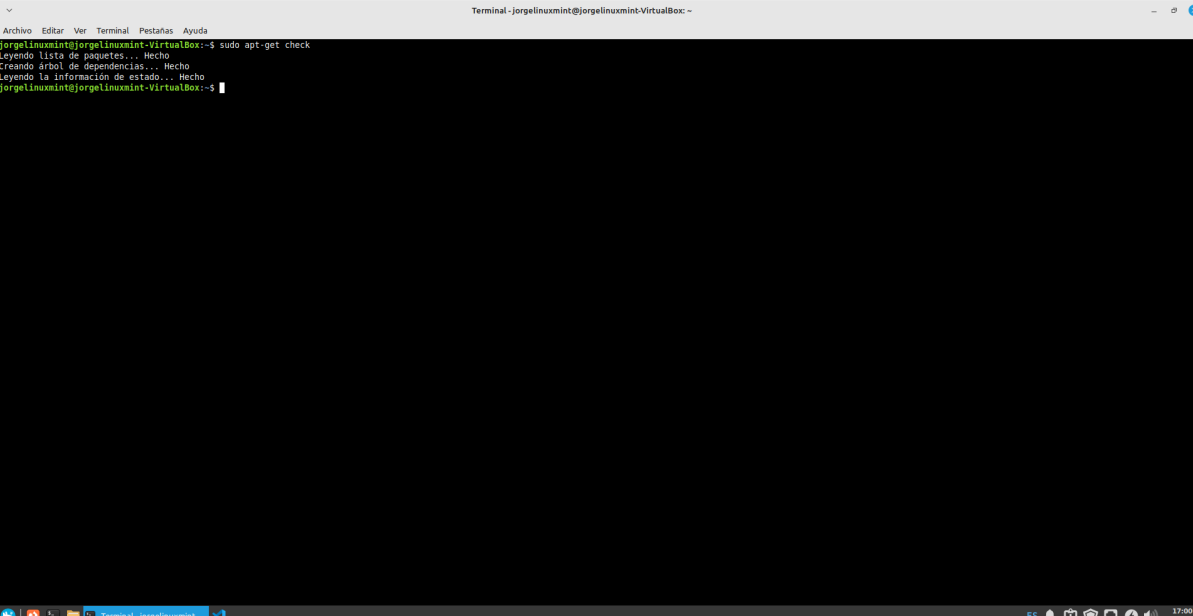
# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Include /etc/ssh/ssh_config.d/*.conf

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/tk
# SendEnv LANG LC *
HashKnownHosts yes
```

Comprobar Integridad de Paquetes:

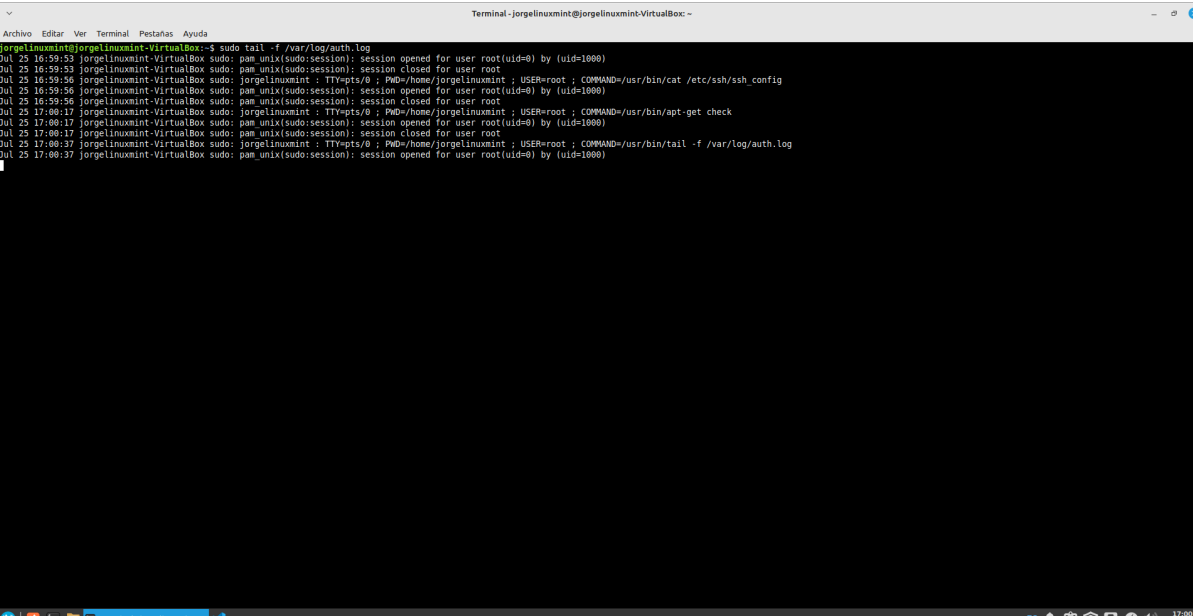
APT: “*sudo apt-get check*”



```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
Archivo Editar Ver Terminal Pestañas Ayuda
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo apt-get check
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$
```

Log de Seguridad y Eventos:

Ver Últimos Logs de Seguridad: *“sudo tail -f /var/log/auth.log”*



```
Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox -
Archivo Editar Ver Terminal Pestañas Ayuda
jorgelinuxmint@jorgelinuxmint-VirtualBox:~$ sudo tail -f /var/log/auth.log
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Jul 25 16:59:56 jorgelinuxmint-VirtualBox sudo: jorgelinuxmint : TTYpts/0 ; PWD=/home/jorgelinuxmint ; USER=root ; COMMAND=/usr/bin/cat /etc/ssh/ssh_config
Jul 25 16:59:56 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 16:59:56 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo: jorgelinuxmint : TTYpts/0 ; PWD=/home/jorgelinuxmint ; USER=root ; COMMAND=/usr/bin/apt-get check
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Jul 25 17:00:37 jorgelinuxmint-VirtualBox sudo: jorgelinuxmint : TTYpts/0 ; PWD=/home/jorgelinuxmint ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Jul 25 17:00:37 jorgelinuxmint-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
```

Ver Últimos Logs del Sistema: *“sudo journalctl -xe”*

```

Terminal - jorgelinuxmint@jorgelinuxmint-VirtualBox ~
Archivo Editar Ver Terminal Pestanas Ayuda

jorgelinuxmint-VirtualBox:~$ sudo journalctl -xe
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: USER ACCT pid=3207 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:accounting grantors=pan permit acct=jorgelinuxmint* exe=/usr/bin/sudo hostname=? addr=? term
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: USER CHO pid=3207 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=cmd=/home/jorgelinuxmint/ cnd=636174202f6574633277373682f737368645f636f66666967 exe=/usr/bin/sudo/ ter
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: jorgelinuxmint : TTYpts/0 : PwD=/home/jorgelinuxmint : USER=root : COMMAND=/usr/bin/cat /etc/ssh/sshd_config
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: CHO REFR pid=3207 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: USER START pid=3207 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session open grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 16:59:40 jorgelinuxmint-VirtualBox sudo[3207]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 16:59:40 jorgelinuxmint-VirtualBox sudo[3207]: pam_unix(sudo:session): session closed for user root
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: USER END pid=3207 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session close grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 16:59:40 jorgelinuxmint-VirtualBox audit[3207]: CHO DIS9 pid=3207 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3210]: USER ACCT pid=3210 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:accounting grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3210]: USER CHO pid=3210 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=cmd=/home/jorgelinuxmint/ cnd=636174202f6574633277373682f737368645f636f66666967 exe=/usr/bin/sudo/ term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo[3210]: jorgelinuxmint : TTYpts/0 : PwD=/home/jorgelinuxmint : USER=root : COMMAND=/usr/bin/cat /etc/ssh/sshd_config
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3210]: CHO REFR pid=3210 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo[3210]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3210]: USER START pid=3210 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session open grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo[3210]: pam_unix(sudo:session): session closed for user root
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3210]: USER END pid=3210 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session close grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3210]: CHO DIS9 pid=3210 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3214]: USER ACCT pid=3214 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:accounting grantors=pan permit acct=jorgelinuxmint* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3214]: USER CHO pid=3214 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=cmd=/home/jorgelinuxmint/ cnd=636174202f6574633277373682f737368645f636f66666967 exe=/usr/bin/sudo/ term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo[3214]: jorgelinuxmint : TTYpts/0 : PwD=/home/jorgelinuxmint : USER=root : COMMAND=/usr/bin/cat /etc/ssh/sshd_config
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3214]: CHO REFR pid=3214 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo[3214]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3214]: USER START pid=3214 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session open grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 16:59:53 jorgelinuxmint-VirtualBox sudo[3214]: pam_unix(sudo:session): session closed for user root
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3214]: USER END pid=3214 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session close grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 16:59:53 jorgelinuxmint-VirtualBox audit[3214]: CHO DIS9 pid=3214 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3218]: USER ACCT pid=3218 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:accounting grantors=pan permit acct=jorgelinuxmint* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3218]: USER CHO pid=3218 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=cmd=/home/jorgelinuxmint/ cnd=6107420676574206368656308 exe=/usr/bin/sudo/ terminal=pts/0 ressource=
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3218]: jorgelinuxmint : TTYpts/0 : PwD=/home/jorgelinuxmint : USER=root : COMMAND=/usr/bin/apt-get check
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3218]: CHO REFR pid=3218 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3218]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3218]: USER START pid=3218 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session open grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3218]: pam_unix(sudo:session): session closed for user root
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3218]: USER END pid=3218 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session close grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3224]: USER ACCT pid=3224 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:accounting grantors=pan permit acct=jorgelinuxmint* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3224]: USER CHO pid=3224 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=cmd=/home/jorgelinuxmint/ cnd=74667572665163746628207865 exe=/usr/bin/sudo/ terminal=pts/0 ressource=
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3224]: jorgelinuxmint : TTYpts/0 : PwD=/home/jorgelinuxmint : USER=root : COMMAND=/usr/bin/journalctl -xe
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3224]: CHO REFR pid=3224 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3224]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3224]: USER START pid=3224 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session open grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3224]: pam_unix(sudo:session): session closed for user root
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3228]: USER ACCT pid=3228 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:accounting grantors=pan permit acct=jorgelinuxmint* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3228]: USER CHO pid=3228 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=cmd=/home/jorgelinuxmint/ cnd=6667572665163746628207865 exe=/usr/bin/sudo/ terminal=pts/0 ressource=
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3228]: jorgelinuxmint : TTYpts/0 : PwD=/home/jorgelinuxmint : USER=root : COMMAND=/usr/bin/journalctl -xe
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3228]: CHO REFR pid=3228 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:setcred grantors=pan permit,pan ecryptfs,pan cap acct=root* exe=/usr/bin/sudo/ hostname=? addr=? term
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3228]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Jul 25 17:00:17 jorgelinuxmint-VirtualBox audit[3228]: USER START pid=3228 uid=1000 auid=4294967295 ses=4294967295 subj=unconfined msg=op-PAM:session open grantors=pan_limits,pan_env,pan_env,pan_permit,pan_umask,pan_unix,pan_ecryptfs ac
Jul 25 17:00:17 jorgelinuxmint-VirtualBox sudo[3228]: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Lines 3144-3194/3194 [END]

```