

# Born2beRoot

Miguel Eguzquiza Fernandez



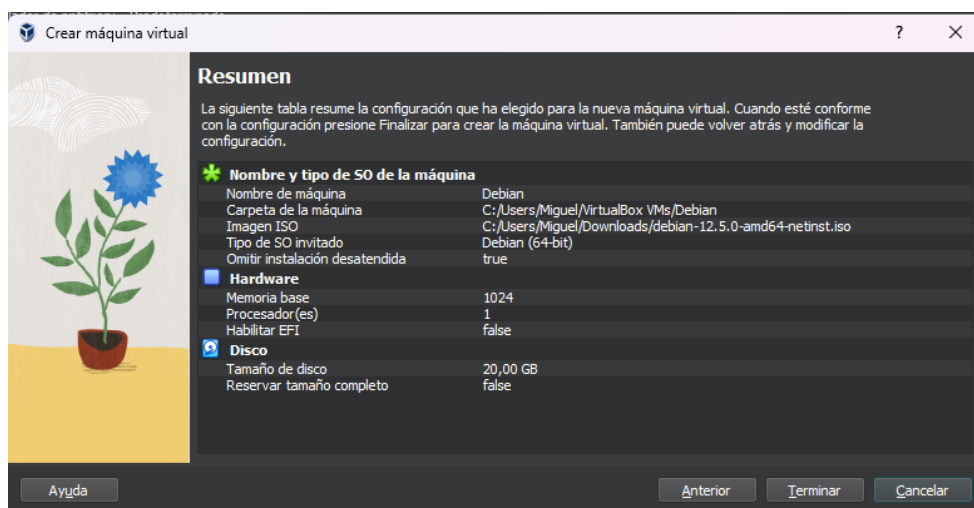
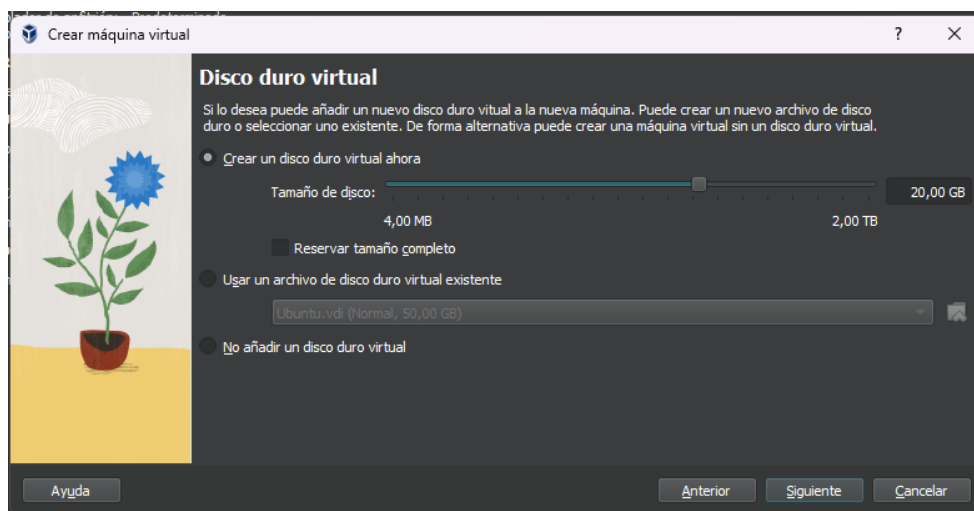
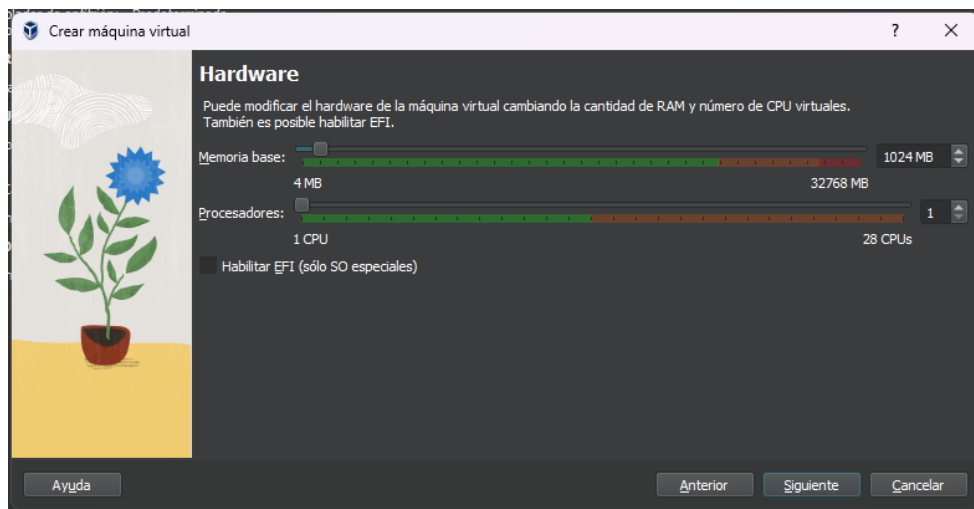
## Pasos a seguir para completar la actividad Born2beRoot.

Estos son los requisitos que pide la actividad:

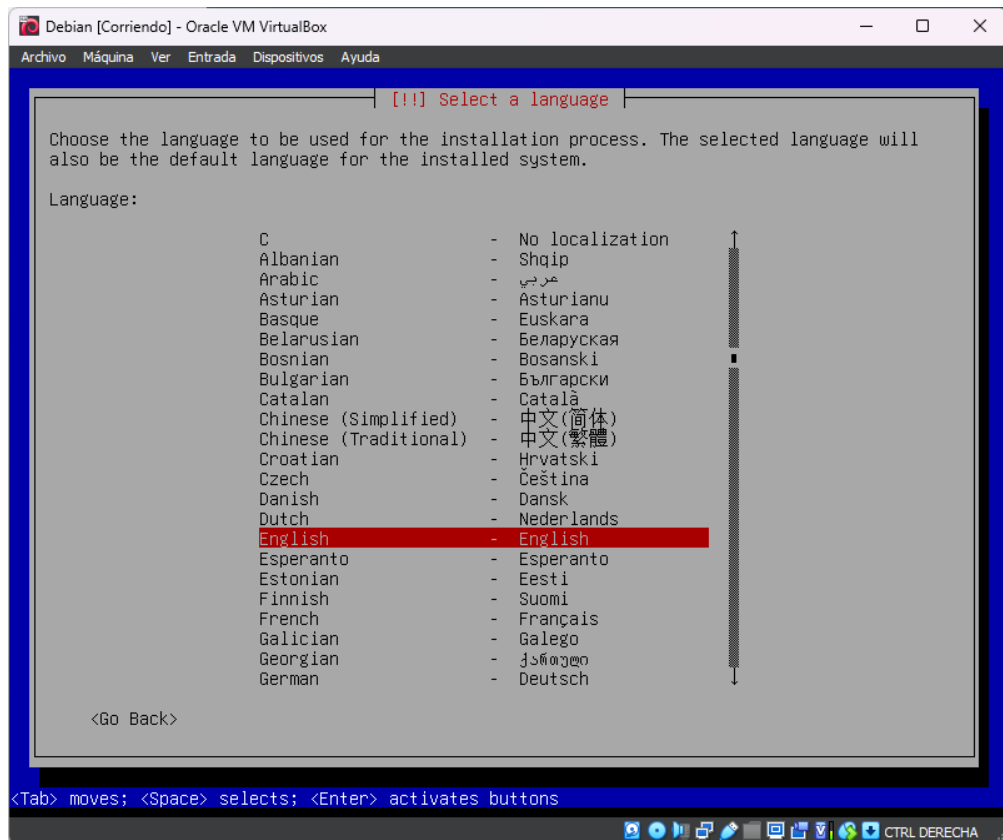
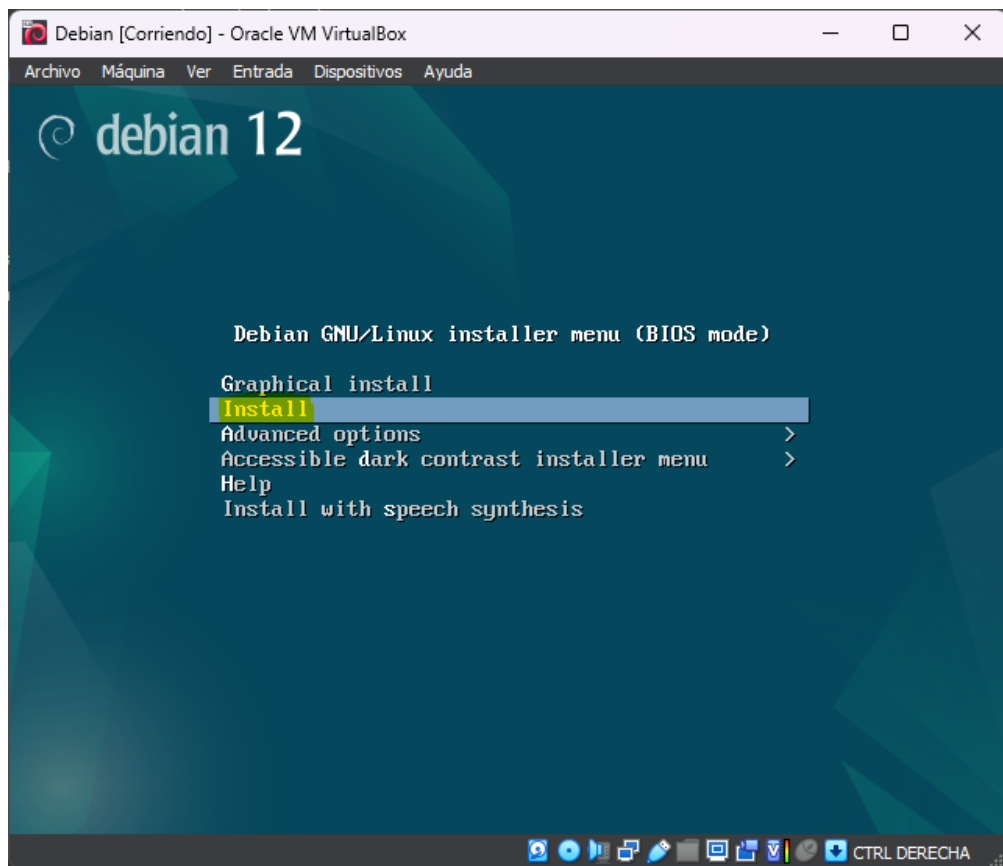
- Deberás elegir como sistema operativo la última versión estable de Debian (no testing/unstable), o la última versión estable de Rocky. Se recomienda encarecidamente.
- Debes crear al menos 2 particiones cifradas usando LVM.
- El servicio SSH se ejecutará en el puerto 4242 solo. Por seguridad, no debe ser posible conectarte a través de SSH como root.
- Debes configurar tu sistema operativo con el firewall UFW, (o firewalld en Rocky) dejando solamente el puerto 4242 abierto.
- El hostname de tu máquina virtual debe ser tu login terminado en 42 (por ejemplo, wil42). Deberás modificar este hostname durante tu evaluación.
- Debes implementar una política de contraseñas fuerte.
- Debes instalar y configurar sudo siguiendo reglas estrictas.
- Además del usuario root, un usuario con tu login como nombre debe existir.
- Este usuario debe pertenecer a los grupos user42 y sudo.
- Para configurar una política de contraseñas fuerte, deberás cumplir los siguientes requisitos:
  - Tu contraseña debe expirar cada 30 días.
  - El número mínimo de días permitido antes de modificar una contraseña deberá ser 2.
  - El usuario debe recibir un mensaje de aviso 7 días antes de que su contraseña expire.
  - Tu contraseña debe tener como mínimo 10 caracteres de longitud. Debe contener una mayúscula y un número. Por cierto, no puede tener más de 3 veces consecutivas el mismo carácter.
  - La contraseña no puede contener el nombre del usuario.
  - La siguiente regla no se aplica a la contraseña para root: La contraseña debe tener al menos 7 caracteres que no sean parte de la antigua contraseña.
  - Evidentemente, tu contraseña para root debe seguir esta política
- Para configurar una contraseña fuerte para tu grupo sudo, debes cumplir con los siguientes requisitos:
  - Autenticarte con sudo debe estar limitado a tres intentos en el caso de introducir una contraseña incorrecta.
  - Un mensaje personalizado de tu elección debe mostrarse en caso de que la contraseña introducida sea incorrecta cuando se utilice sudo.
  - Para cada comando ejecutado con sudo, tanto el input como el output deben quedar archivados en el directorio /var/log/sudo/.
  - El modo TTY debe estar activado por razones de seguridad.
  - Por seguridad, los directorios utilizables por sudo deben estar restringidos. Por ejemplo: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

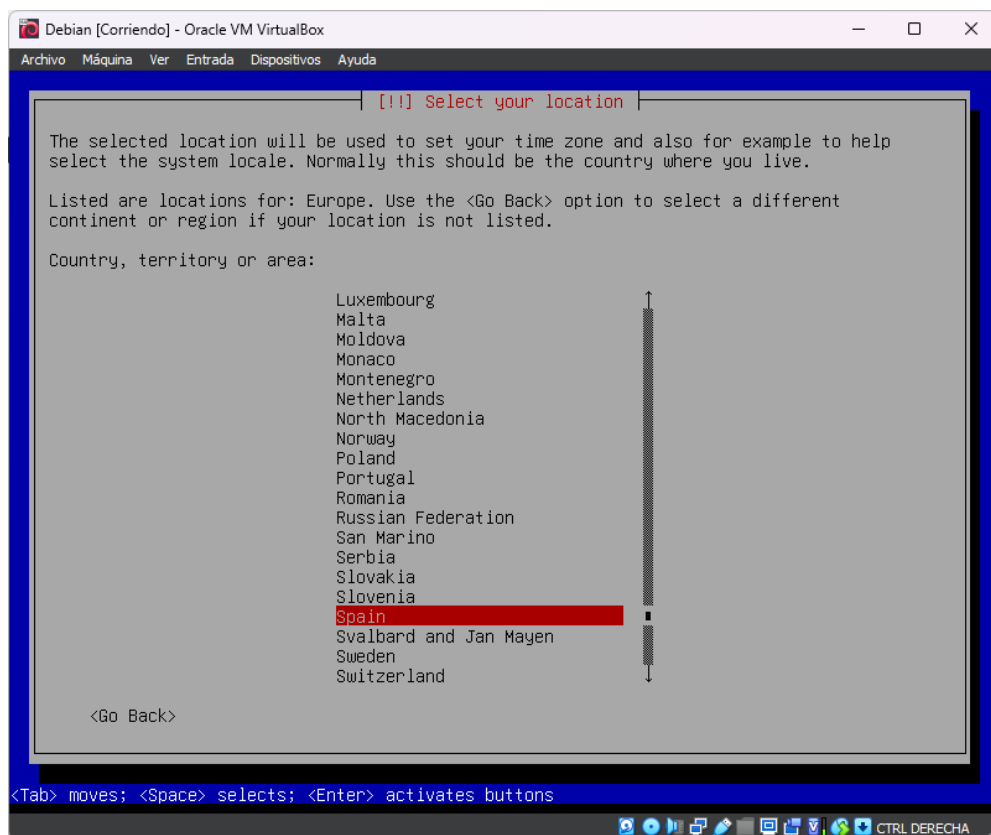
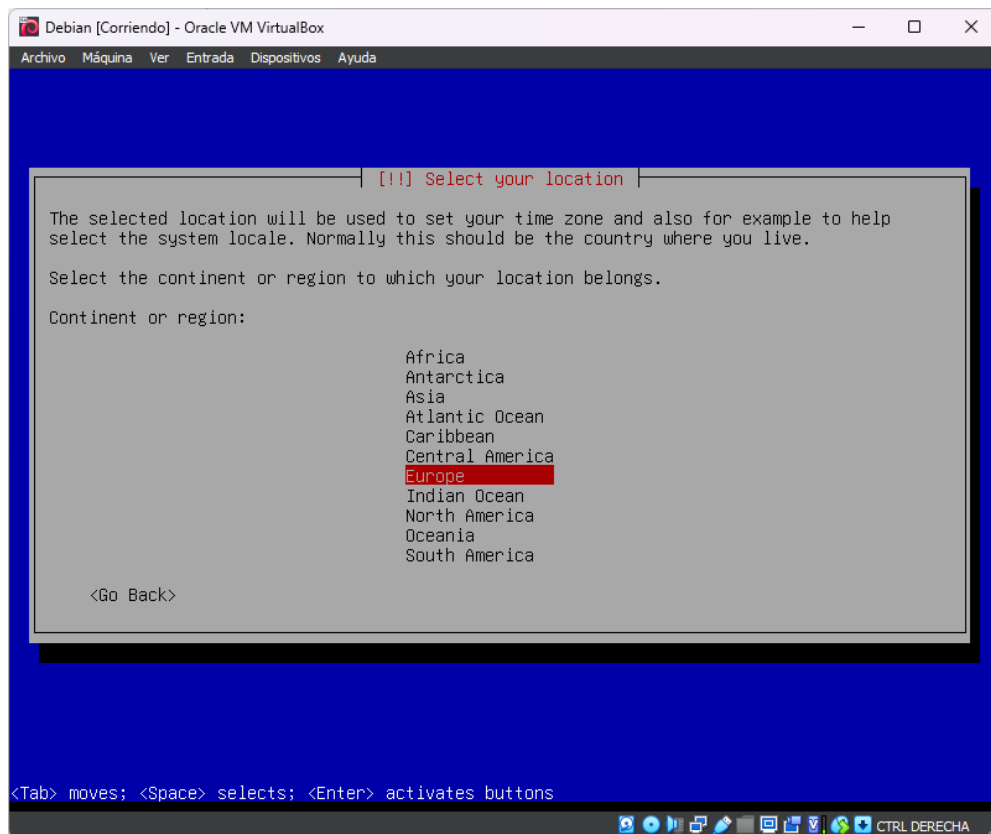
- SCRIPT. Se debe crear un script en bash que cada 10 minutos presente en todos los monitores de los equipos la siguiente información.
  - La arquitectura de tu sistema operativo y su versión de kernel.
  - El número de núcleos físicos.
  - El número de núcleos virtuales.
  - La memoria RAM disponible actualmente en tu servidor y su porcentaje de uso.
  - La memoria disponible actualmente en tu servidor y su utilización como un porcentaje.
  - El porcentaje actual de uso de tus núcleos.
  - La fecha y hora del último reinicio.
  - Si LVM está activo o no.
  - El número de conexiones activas.
  - El número de usuarios del servidor.
  - La dirección IPv4 de tu servidor y su MAC (Media Access Control)
  - El número de comandos ejecutados con sudo.

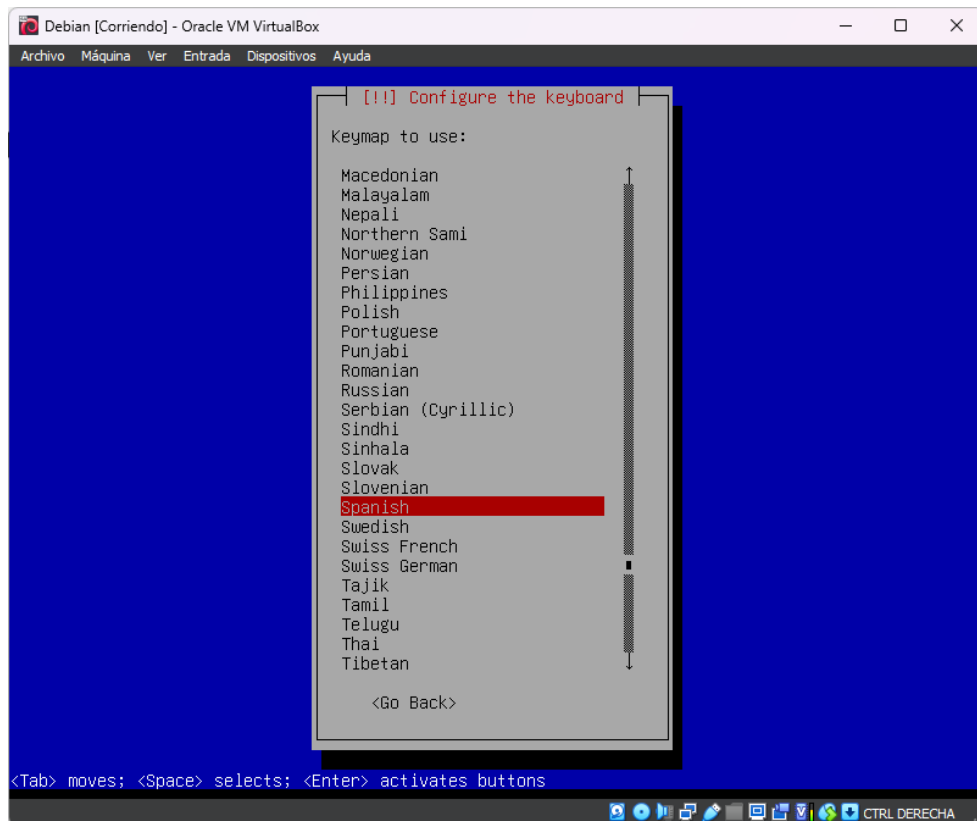
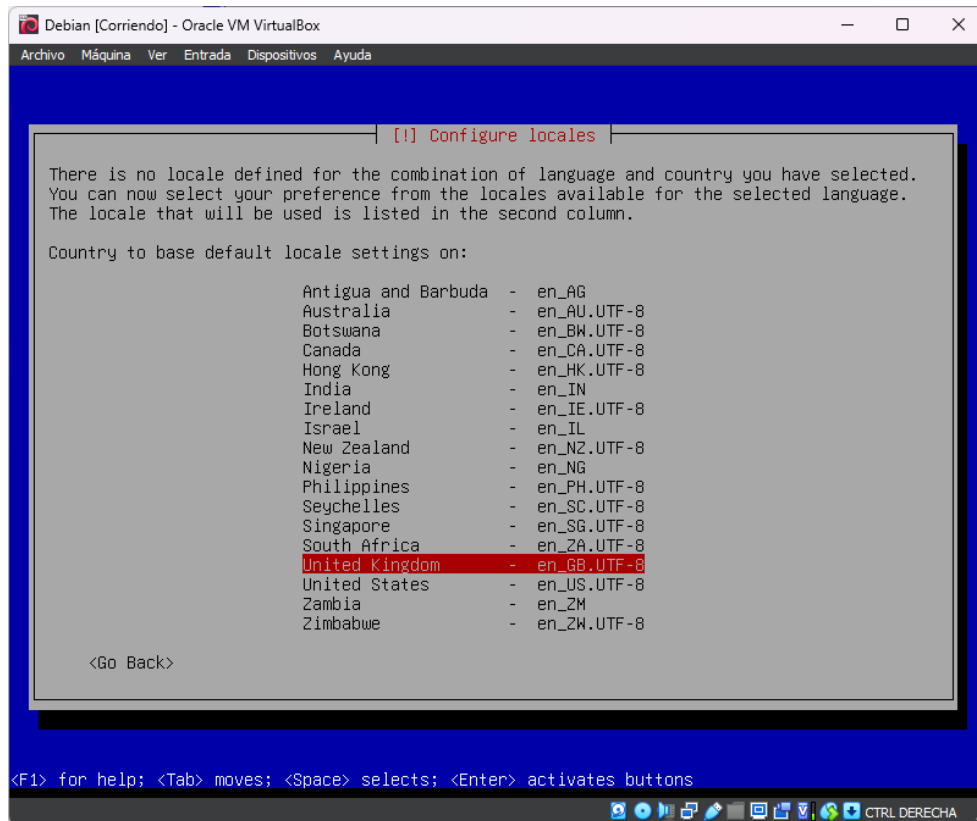
## 1. Creación de la máquina en VirtualBox.



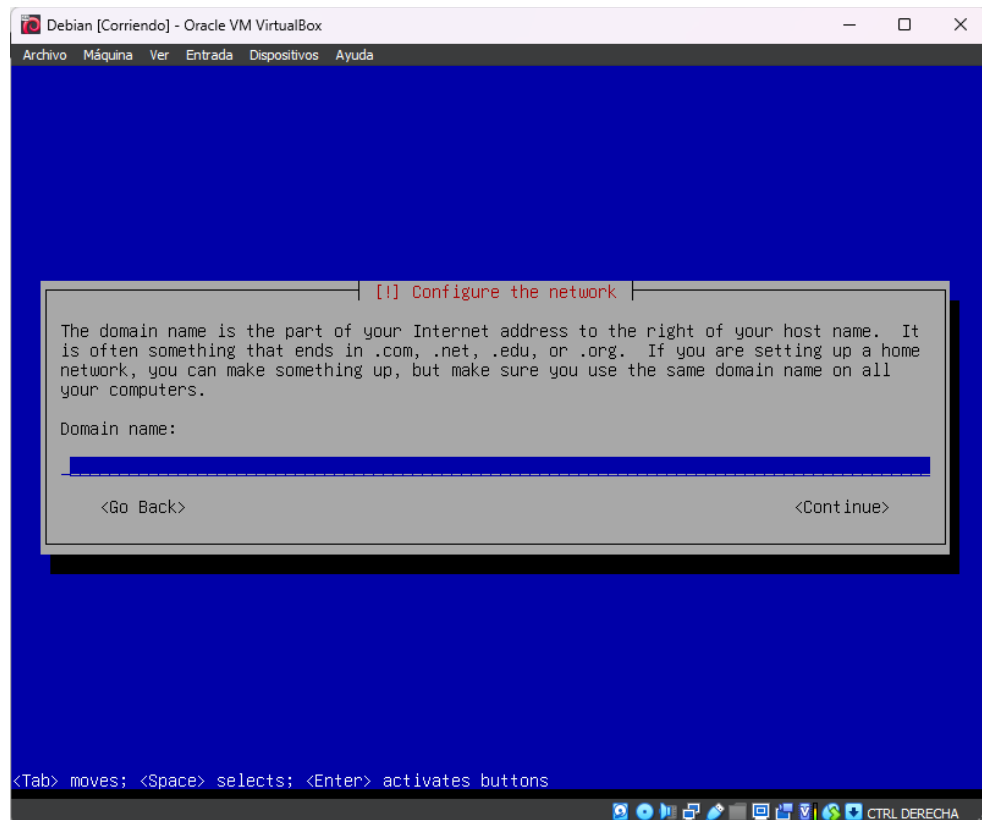
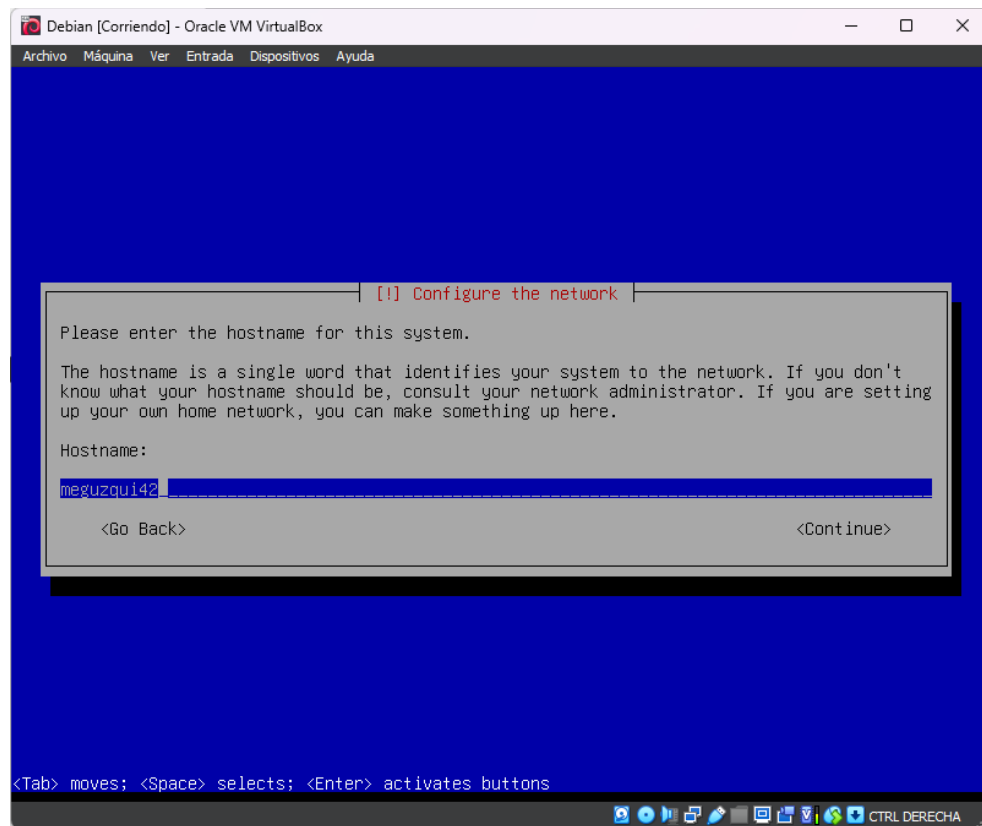
2. La iniciamos y empezamos la configuración de idioma.



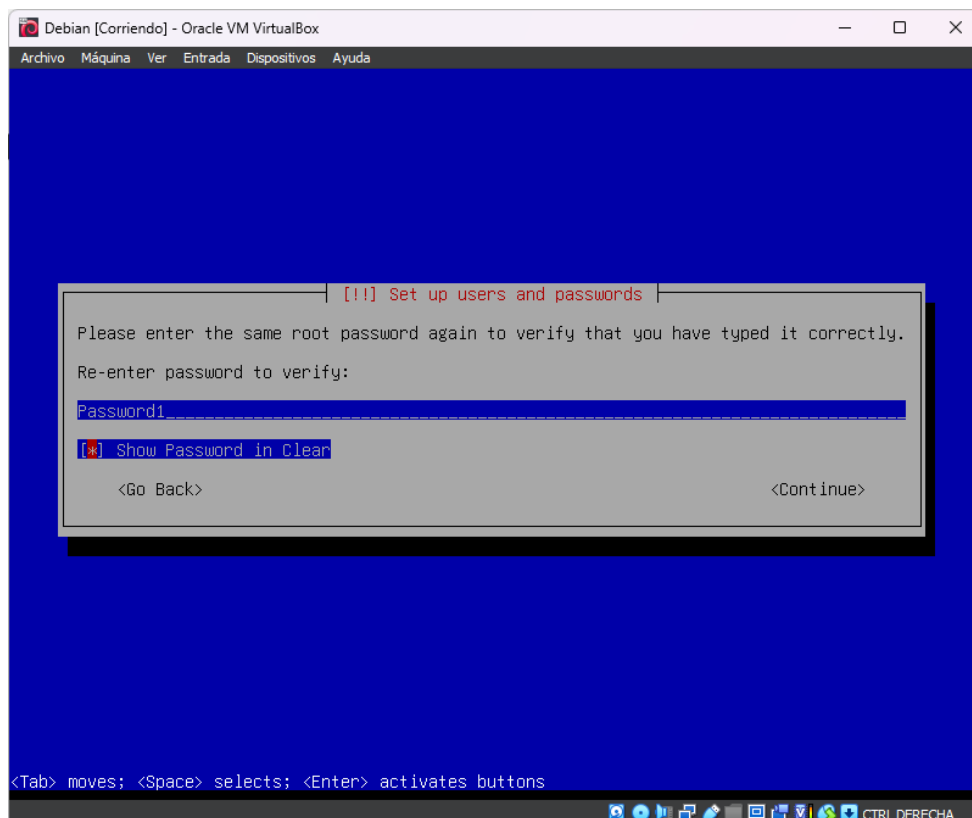
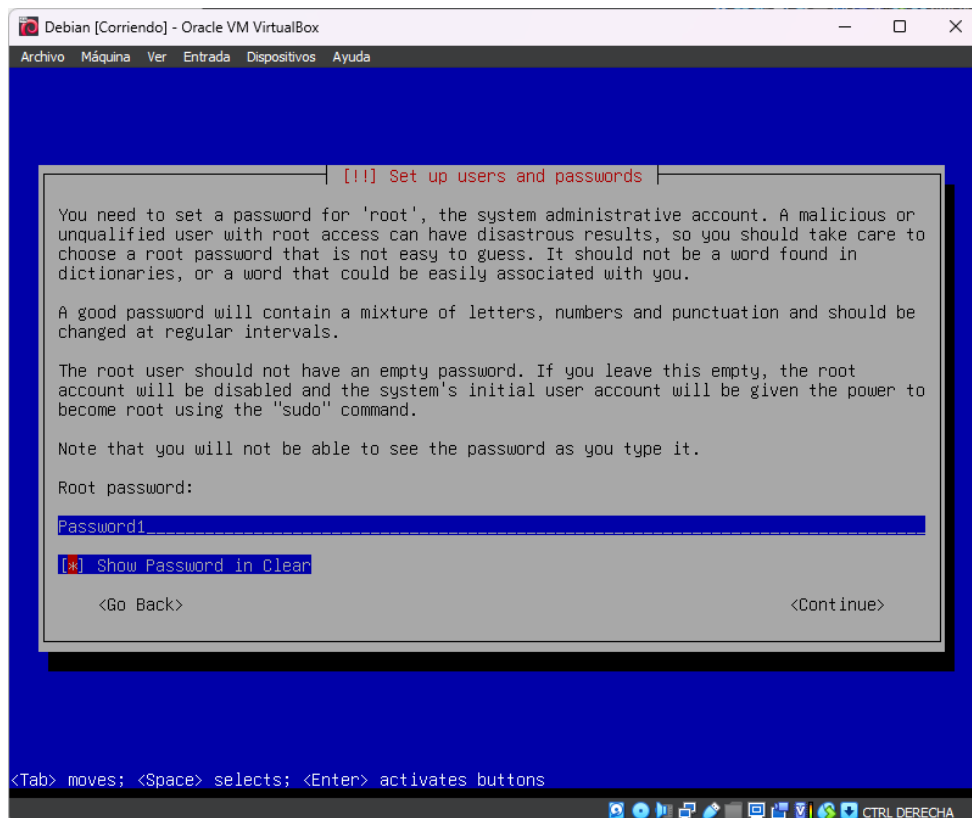




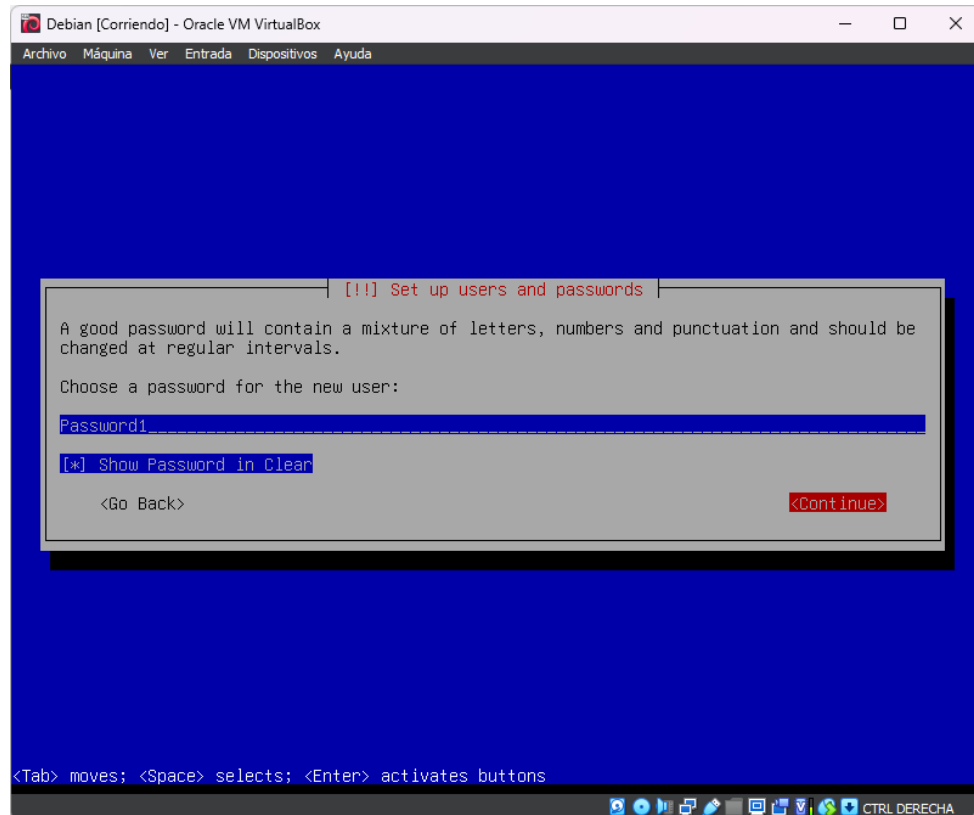
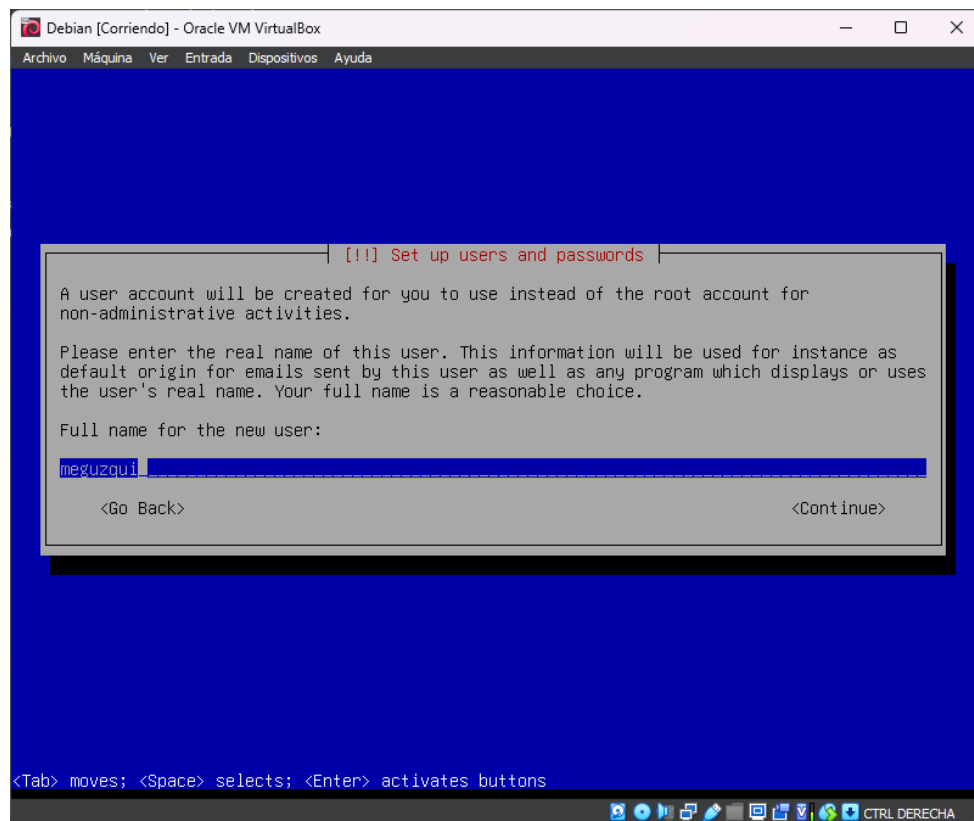
3. Una vez configurado el idioma y distribución de teclado ponemos el hotname como nos pide.

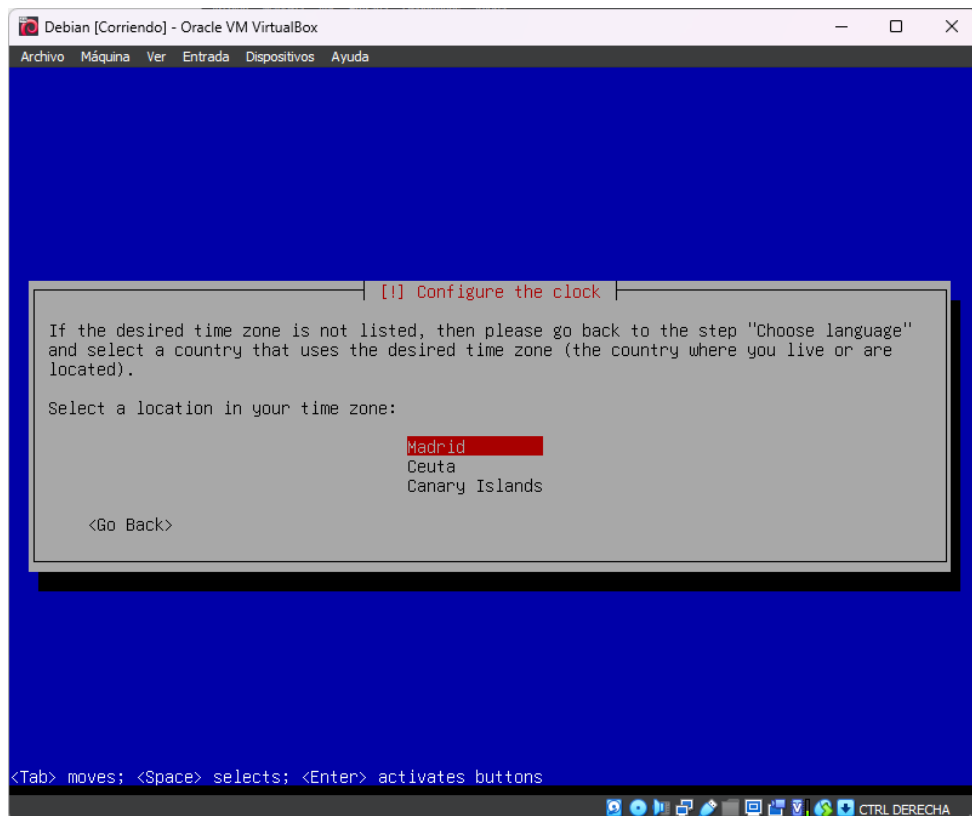




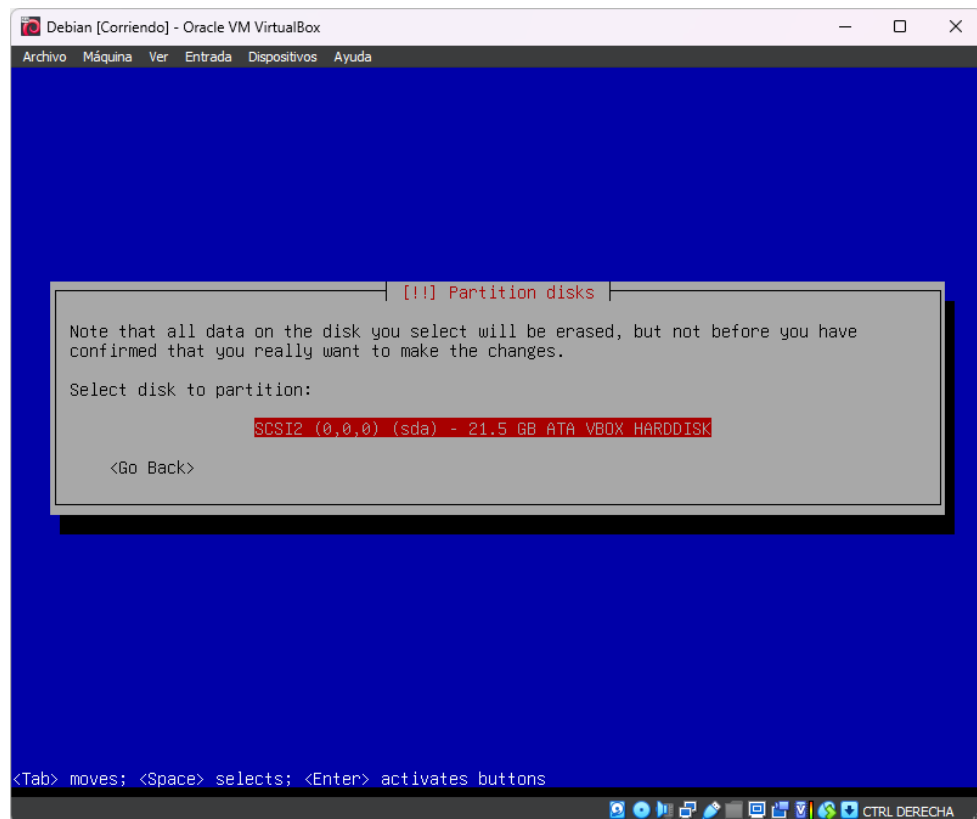
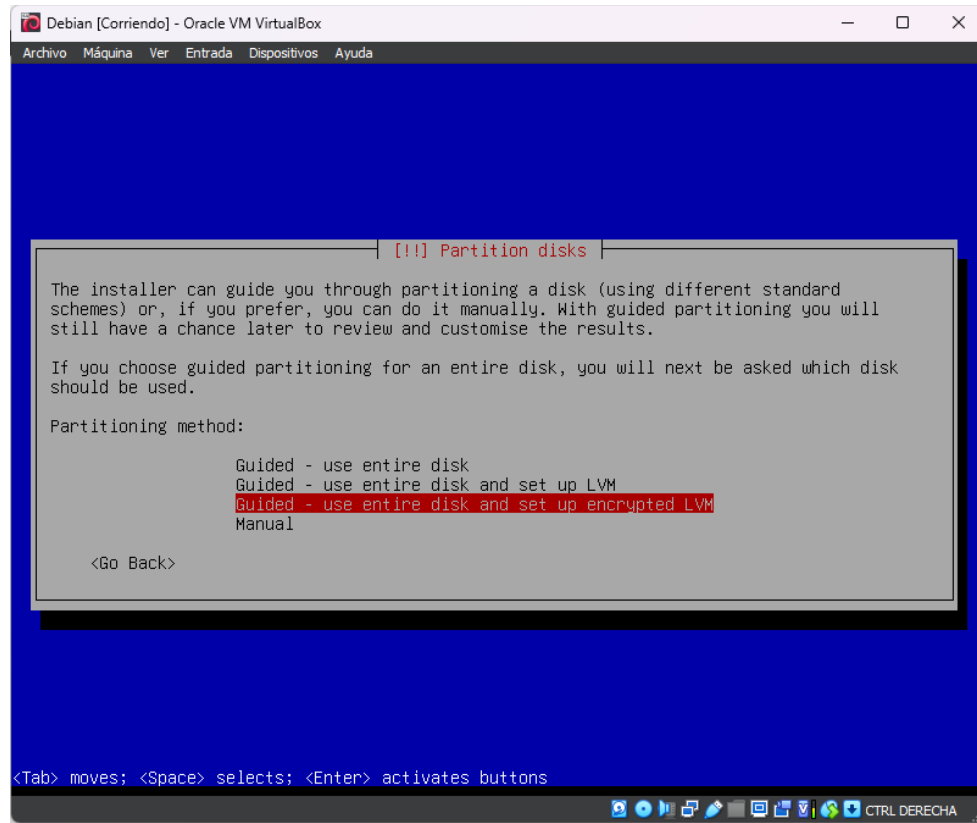


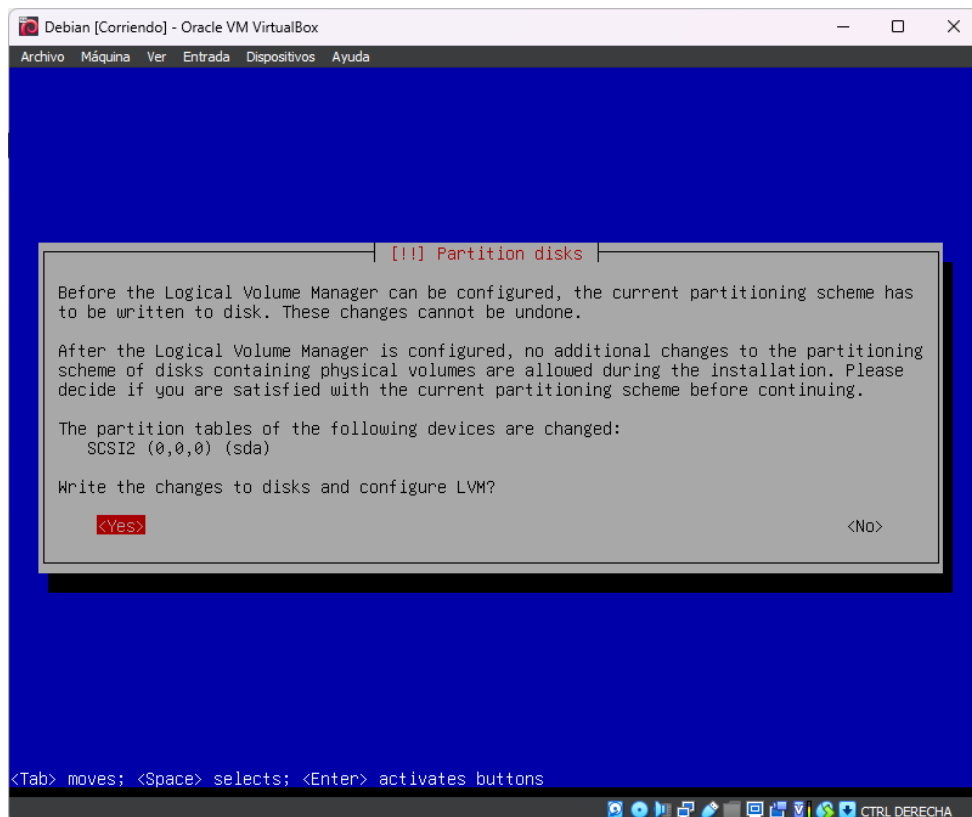
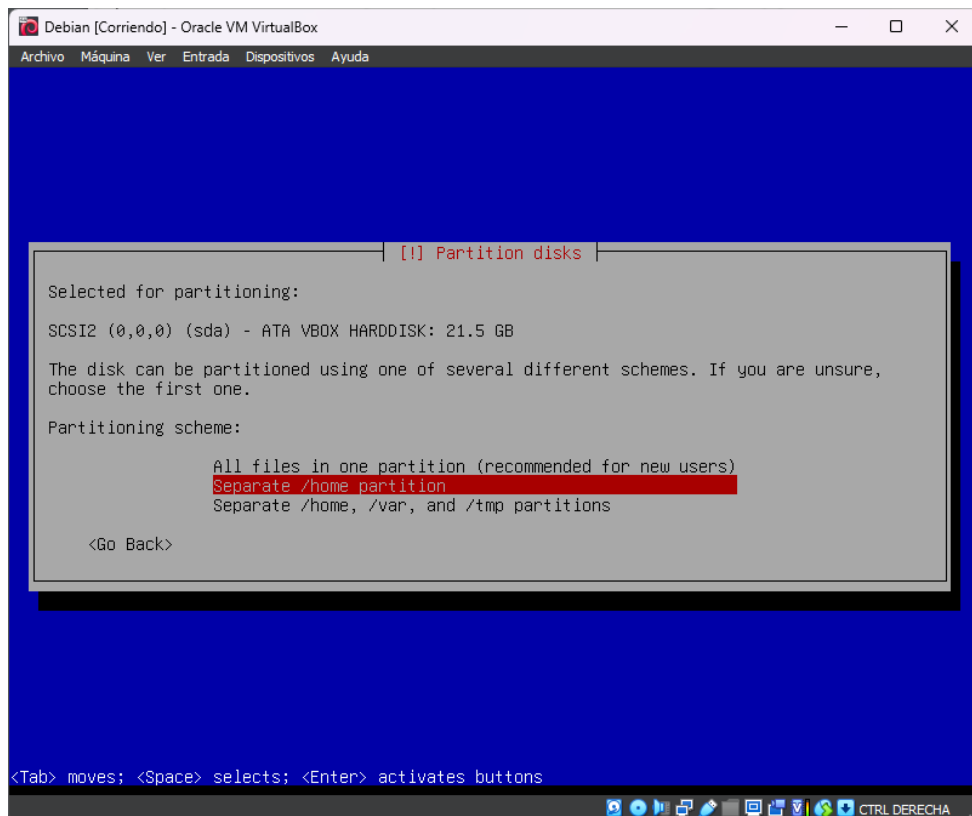
#### 4. Creamos el nuevo usuario con nuestro login.

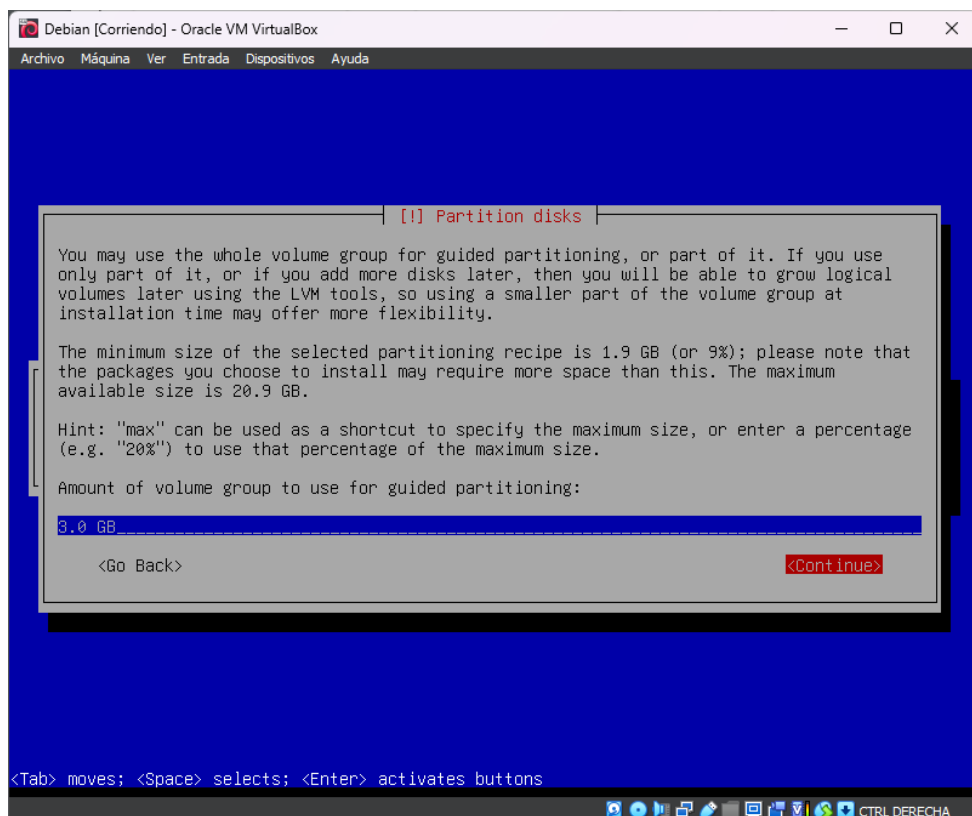
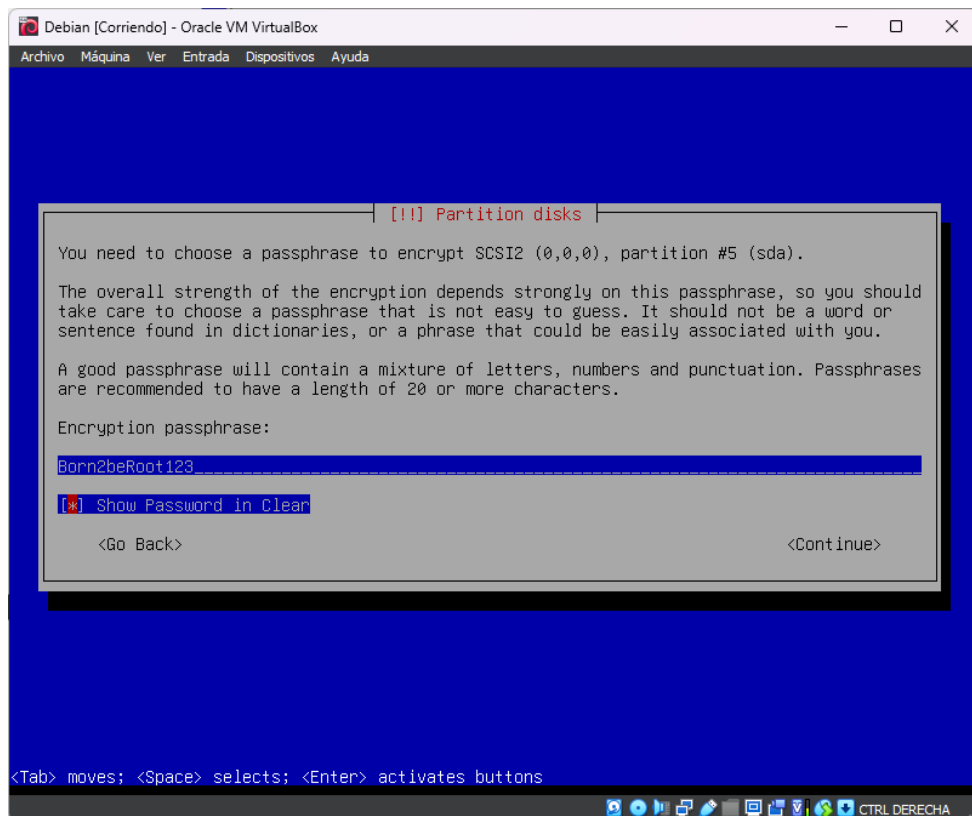


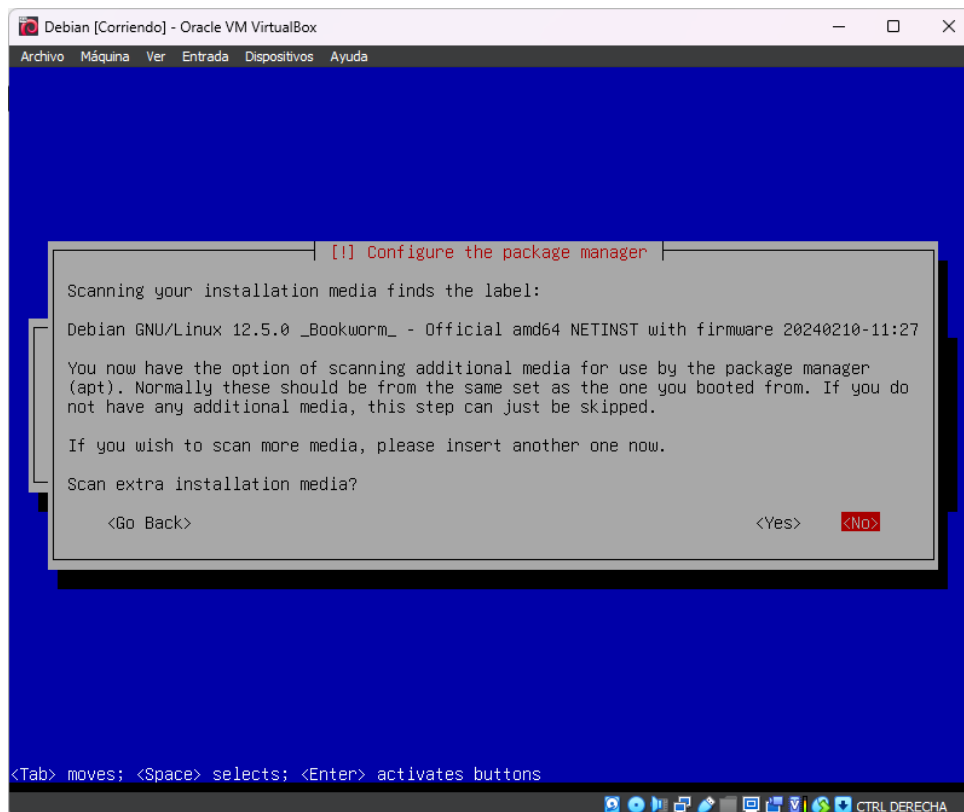
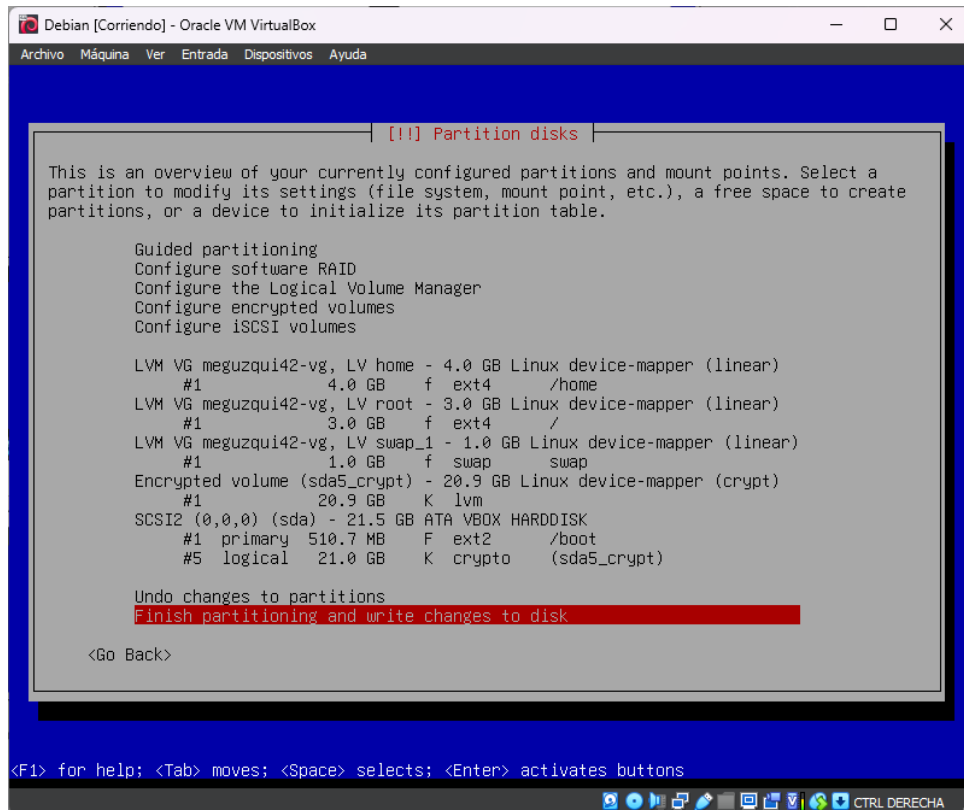


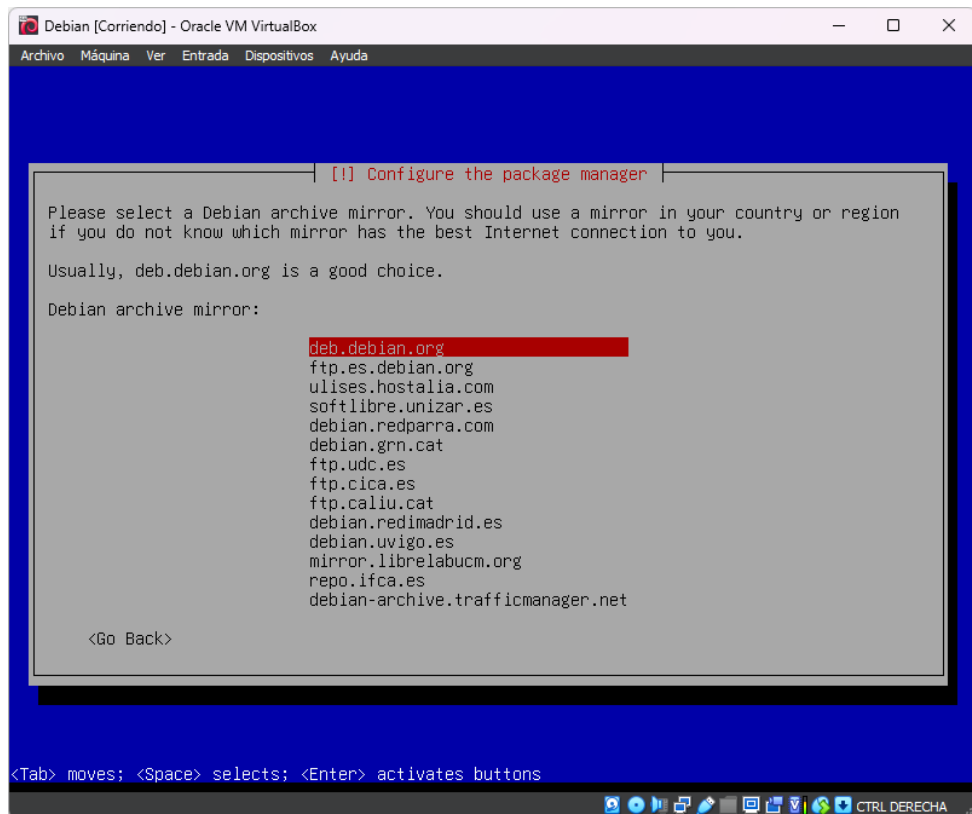
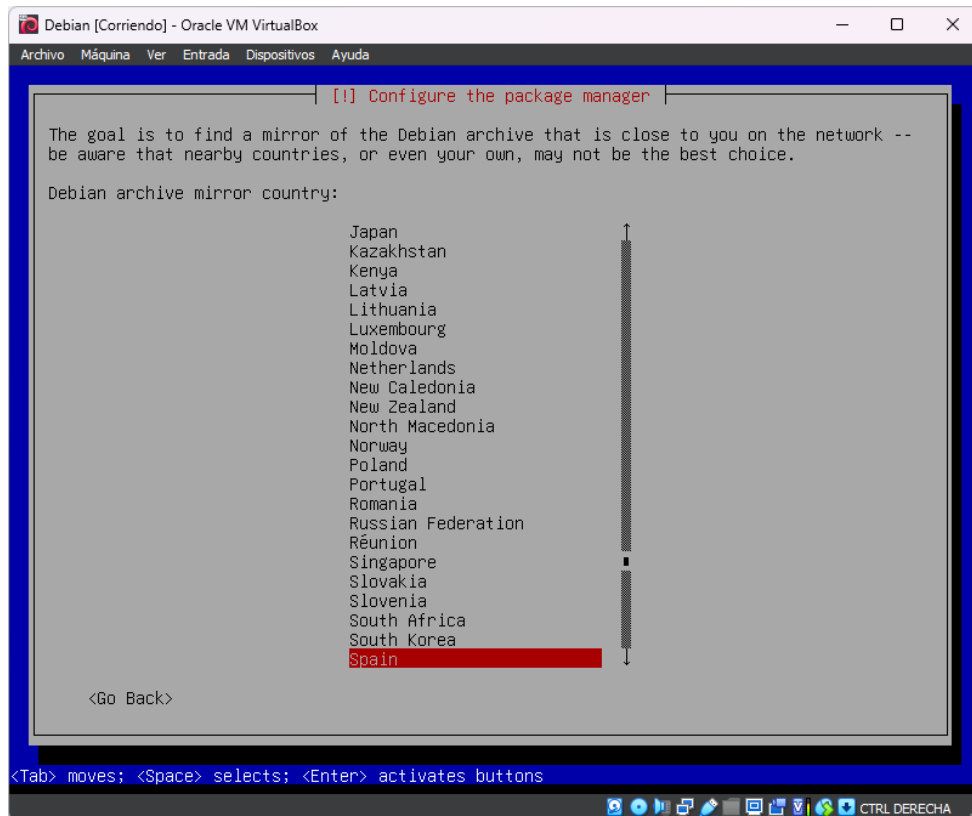
5. Pasamos a crear las dos particiones cifradas LVM, para ello seleccionamos esta opción.



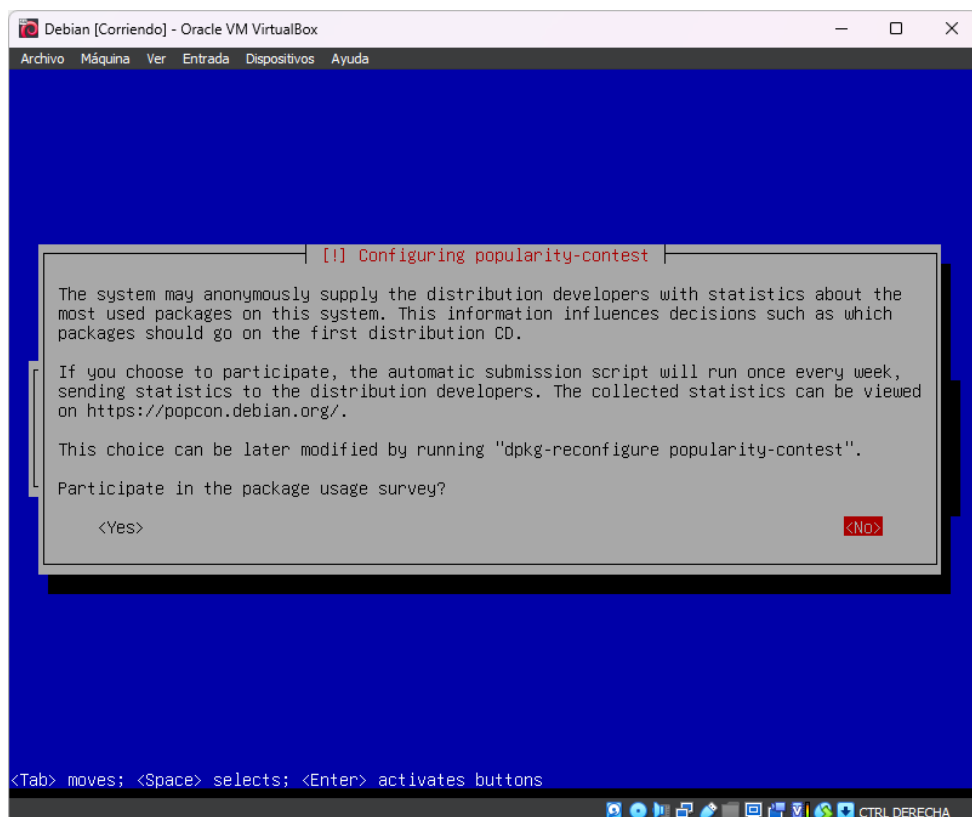
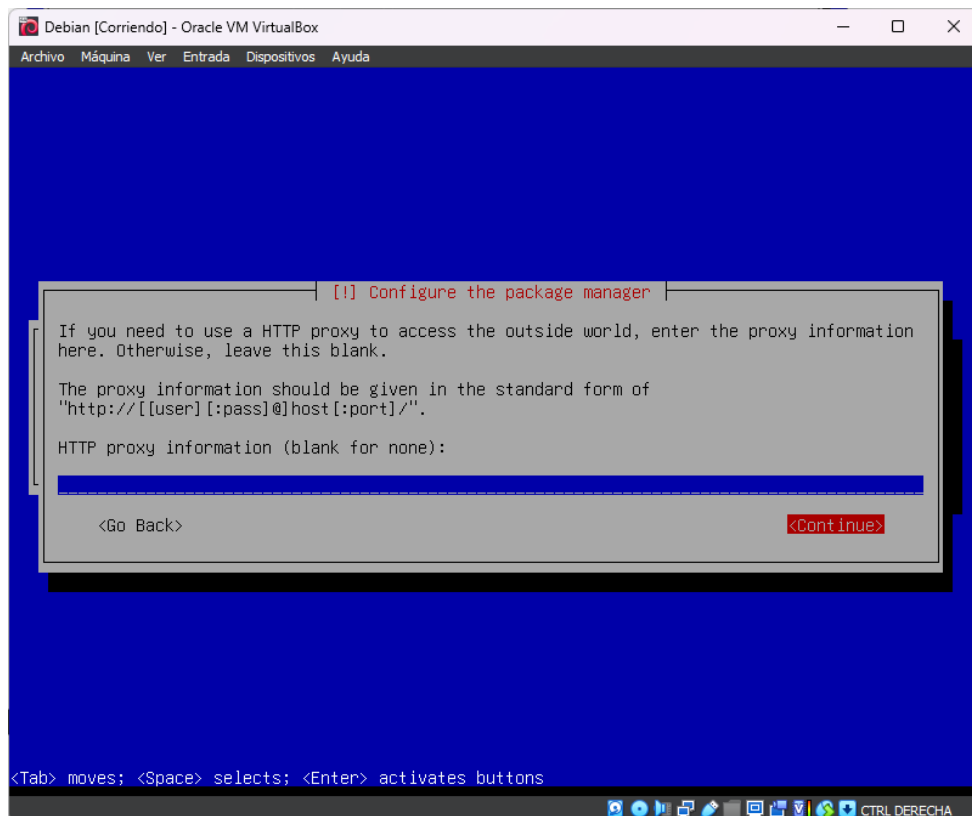


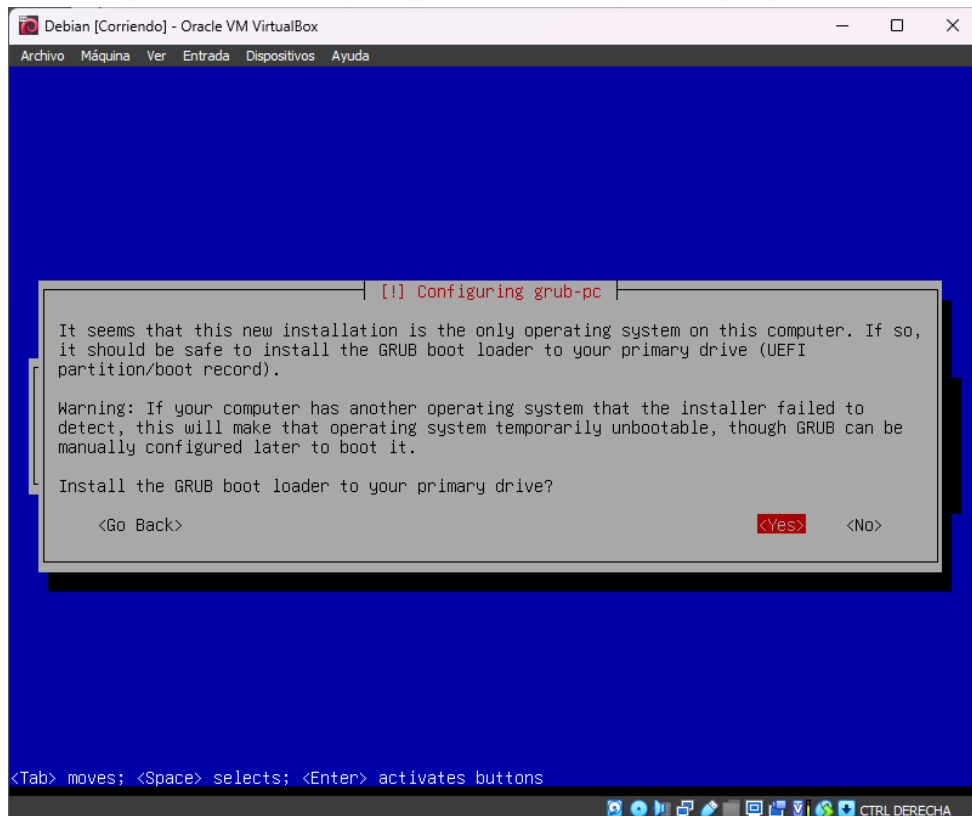
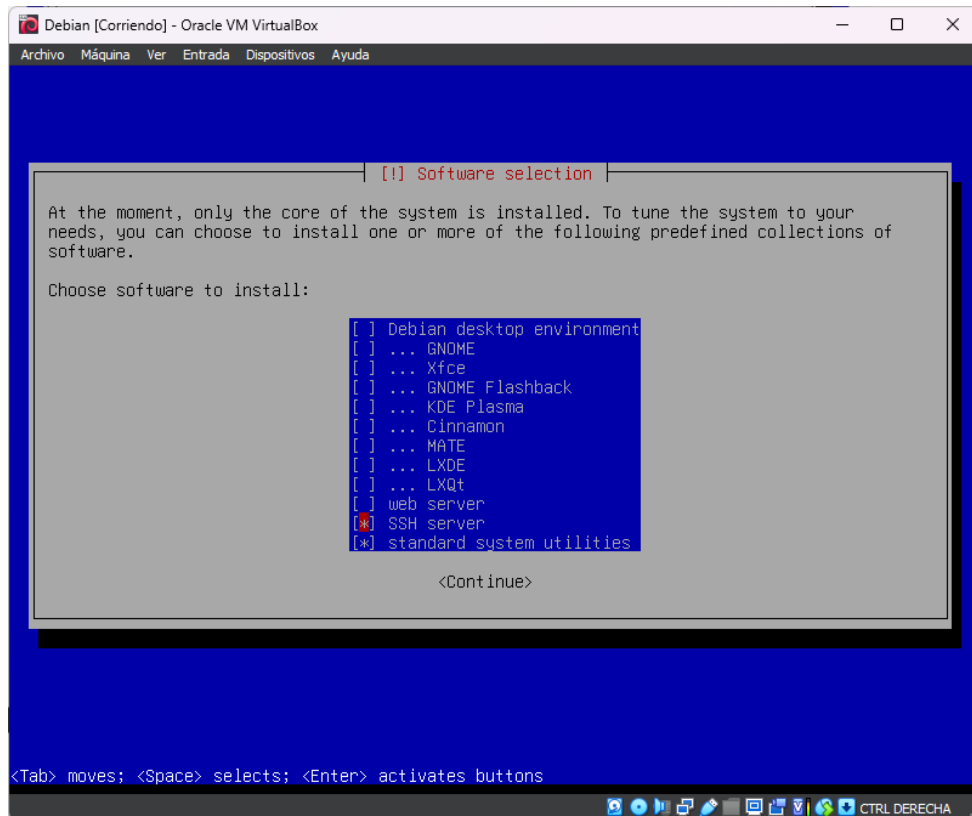


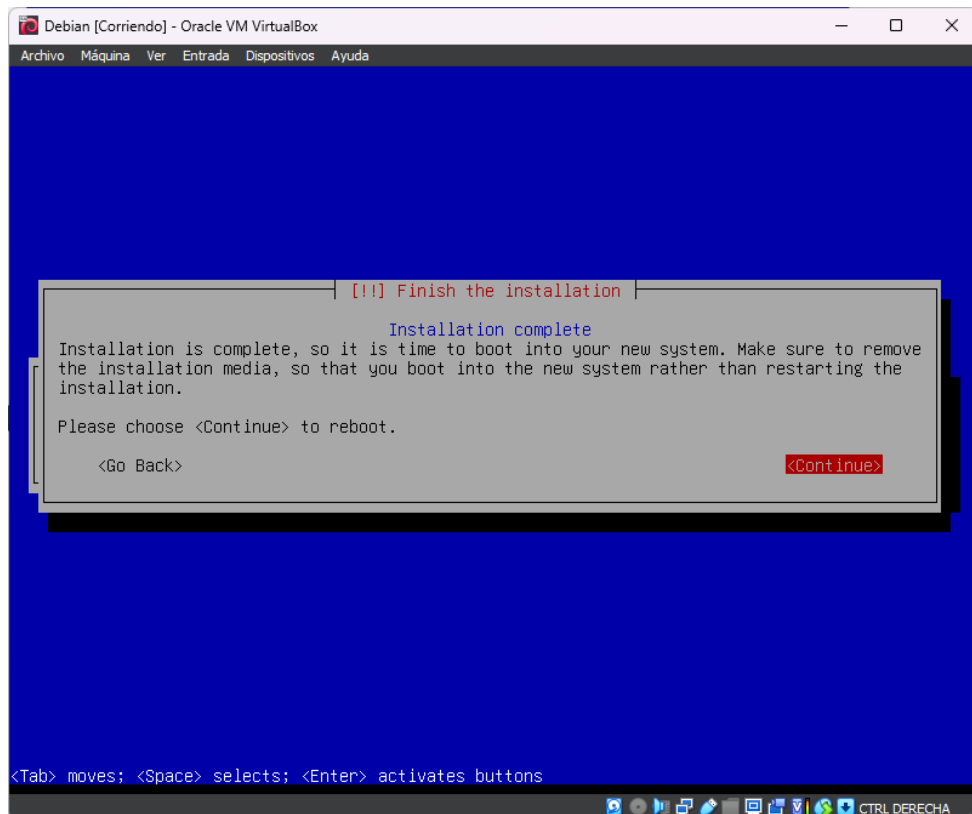
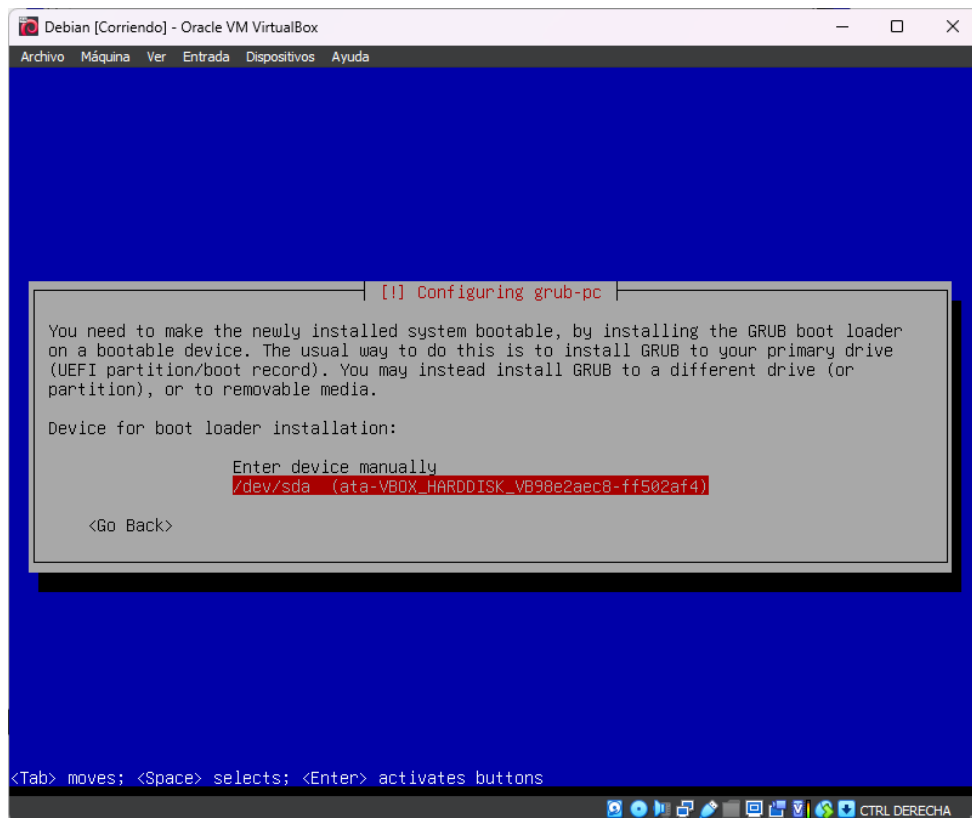




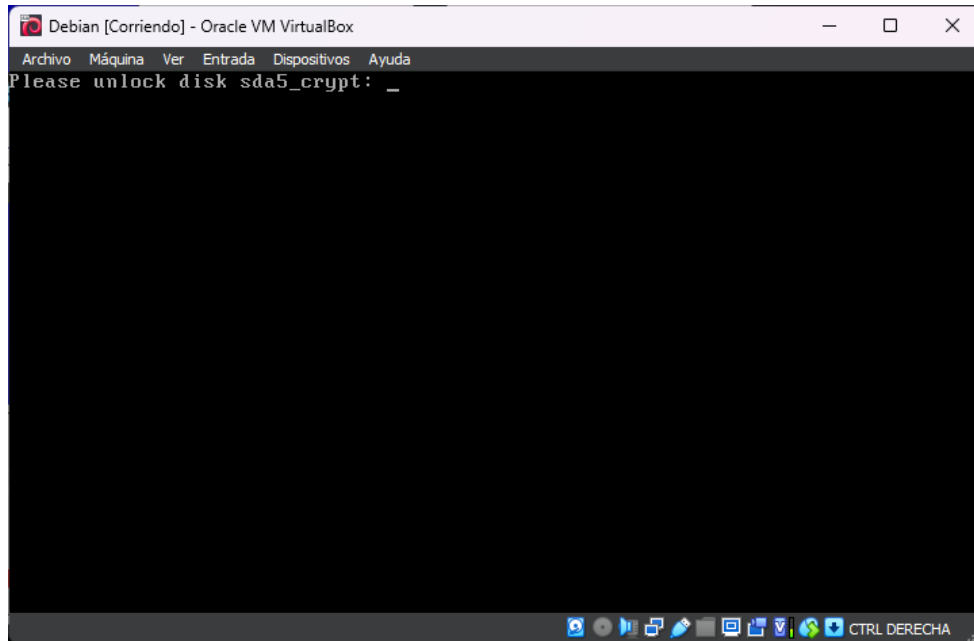




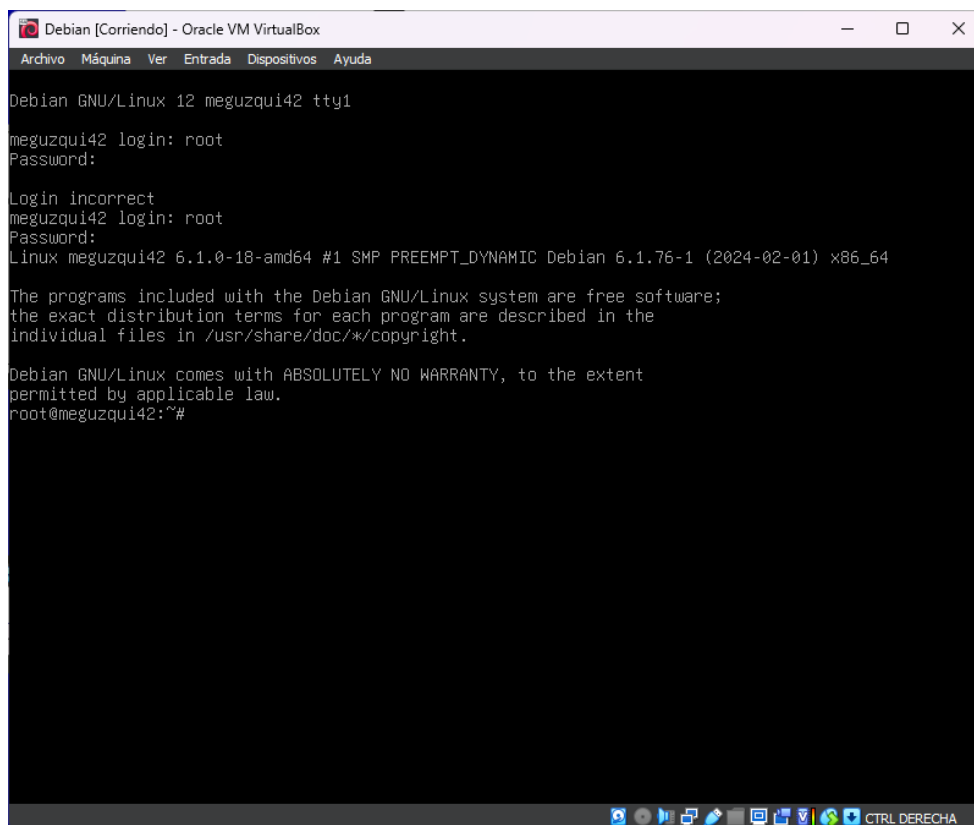




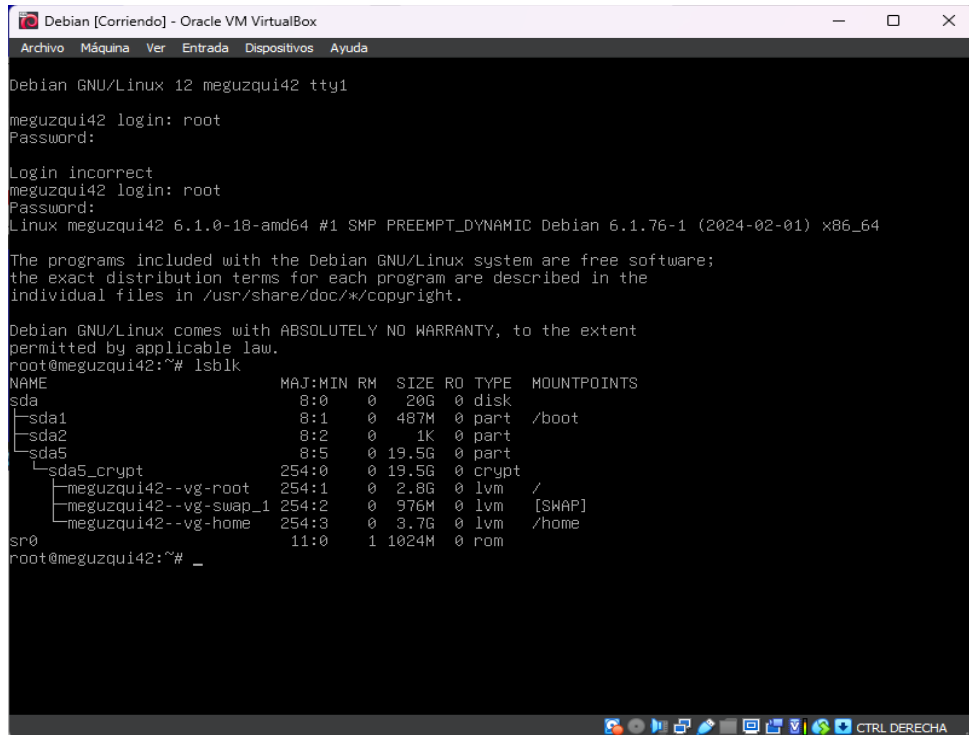
- Una vez terminada la instalación nos aparecerá el Shell negro de nuestro sistema. Nos pedirá la contraseña para desbloquear el disco, pondremos la que usamos para cifrarlo, “Born2beRoot123” en este caso.



- Una vez desbloqueado iniciamos sesión con una cuenta, yo inicio con root pero podemos usar el login creado antes.



- Una vez iniciada sesión vamos a listar las particiones y confirmamos que hay dos LVM al menos creadas.

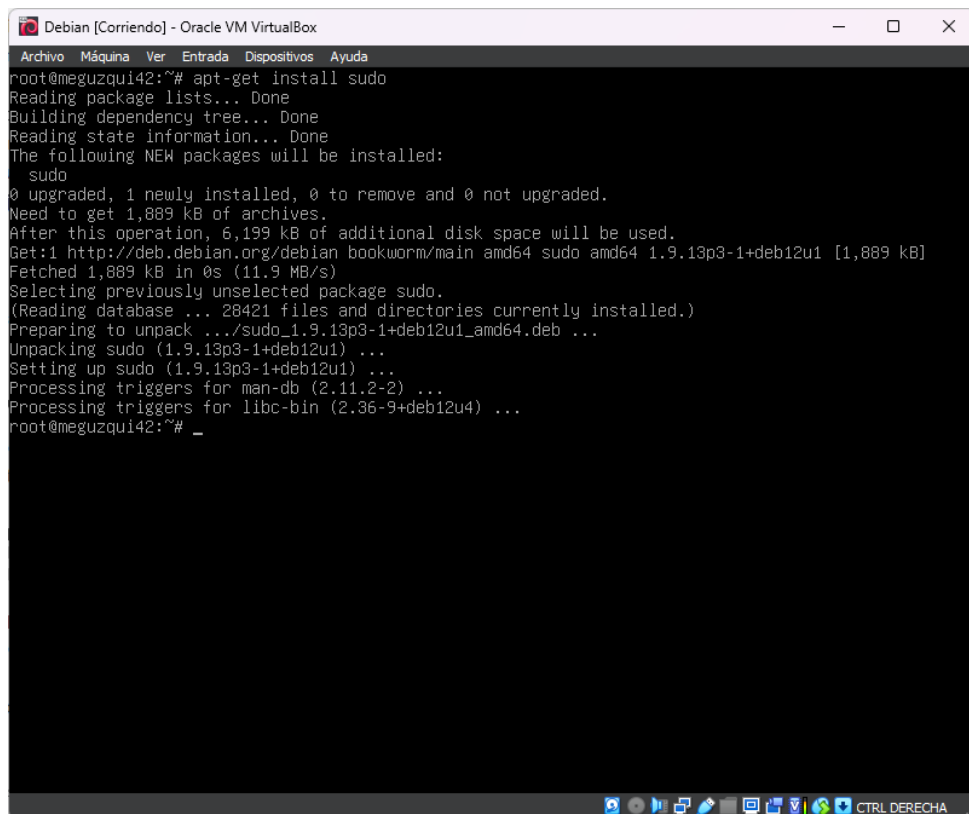


```
Debian GNU/Linux 12 meguzqui42 tty1
meguzqui42 login: root
Password:
Login incorrect
meguzqui42 login: root
Password:
Linux meguzqui42 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

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.

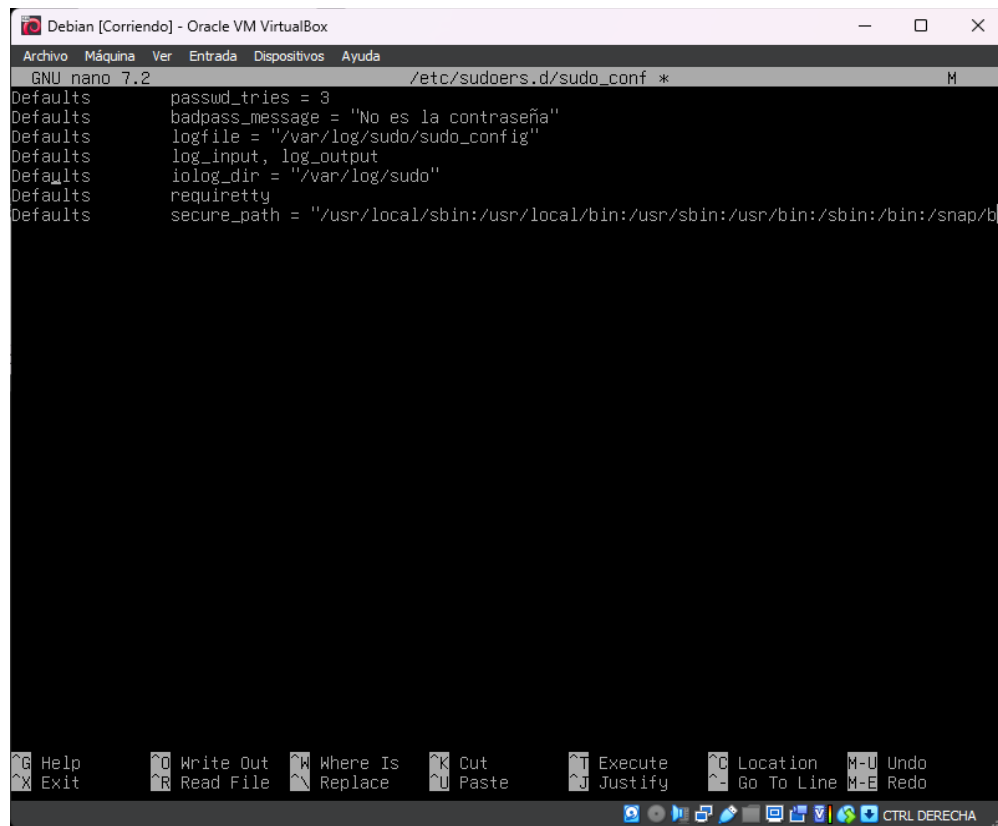
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@meguzqui42:~# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda                                  8:0      0   20G  0 disk
├─sda1                              8:1      0  487M  0 part  /boot
├─sda2                              8:2      0    1K  0 part
└─sda5                              8:5      0  19.5G  0 part
   └─sda5_crypt                    254:0     0  19.5G  0 crypt
      └─meguzqui42--vg-root        254:1     0   2.8G  0 lvm    /
         └─meguzqui42--vg-swap_1  254:2     0   976M  0 lvm    [SWAP]
            └─meguzqui42--vg-home  254:3     0   3.7G  0 lvm    /home
sr0                                  11:0     1  1024M  0 rom
root@meguzqui42:~# _
```

- En primer lugar, con nuestra máquina recién creada vamos a instalar y configurar sudo.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@meguzqui42:~# apt-get install sudo
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sudo
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,889 kB of archives.
After this operation, 6,199 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 sudo amd64 1.9.13p3-1+deb12u1 [1,889 kB]
Fetched 1,889 kB in 0s (11.9 MB/s)
Selecting previously unselected package sudo.
(Reading database ... 28421 files and directories currently installed.)
Preparing to unpack .../sudo_1.9.13p3-1+deb12u1_amd64.deb ...
Unpacking sudo (1.9.13p3-1+deb12u1) ...
Setting up sudo (1.9.13p3-1+deb12u1) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u4) ...
root@meguzqui42:~# _
```

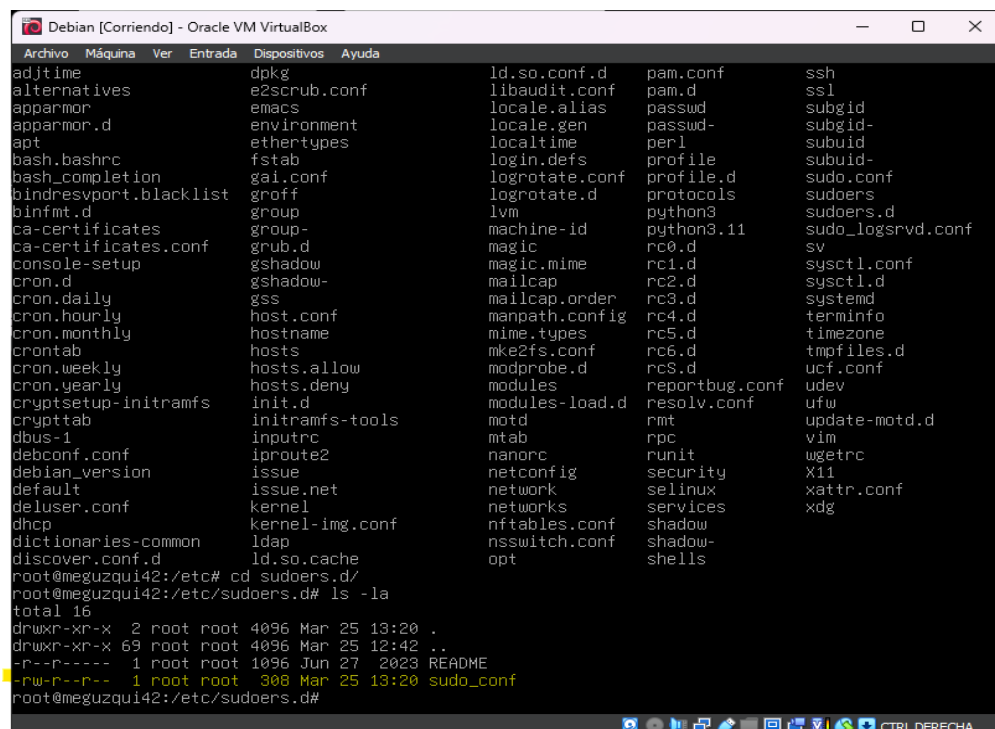
10. Una vez instalado sudo pasamos a configurarlo. Para ello escribimos nano y la ruta del archivo a configurar que estamos creando: nano /etc/sudoers.d/sudo\_conf



```
Debian [Corriendo] - Oracle VM VirtualBox
GNU nano 7.2 /etc/sudoers.d/sudo_conf *
Defaults        passwd_tries = 3
Defaults        badpass_message = "No es la contraseña"
Defaults        logfile = "/var/log/sudo/sudo_config"
Defaults        log_input, log_output
Defaults        iolog_dir = "/var/log/sudo"
Defaults        requiretty
Defaults        secure_path = "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/b
```

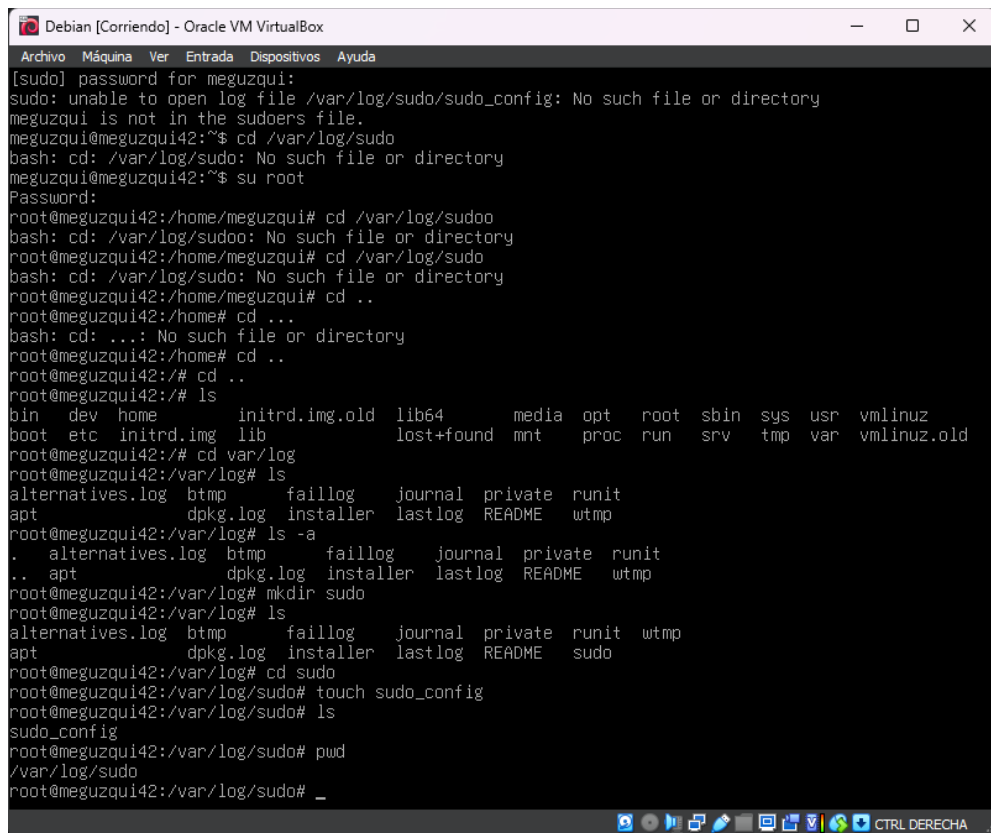
Al terminar de escribir estas líneas guardamos con Control + O y salimos con Control + X.

Como vemos se ha creado el archivo en la ruta /etc/sudoers.d



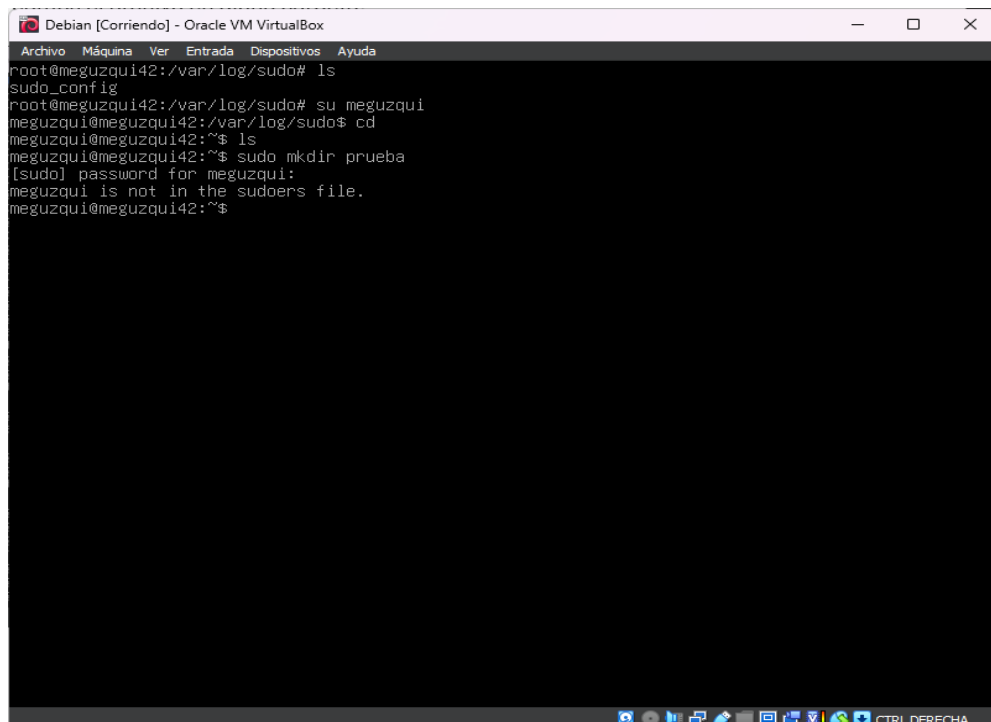
```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
adjtime      dpkg      ld.so.conf.d  pam.conf     ssh
alternatives e2scrub.conf libaudit.conf pam.d         ssl
apparmor     emacs     locale.alias  passwd       subgid
apparmor.d   environment locale.gen     passwd-      subgid-
apt          ethertypes localtime     perl        subuid
bash.bashrc  fstab     login.defs    profile      subuid-
bash_completion gai.conf    logrotate.conf profile.d     sudo.conf
bindresvport.blacklist groff       logrotate.d   protocols    sudoers
binfmt.d     group      lvm           python3       sudoers.d
ca-certificates group-grub.d machine-id     python3.11   sudo_logsrvd.conf
ca-certificates.conf grub.d      magic         rc0.d         sv
console-setup cron.d      gshadow       magic.mime    rc1.d         sysctl.conf
cron.daily   cron.hourly host.conf     mailcap       rc2.d         sysctl.d
cron.monthly cron.monthly hostname     manpath.config rc3.d         systemd
crontab      hosts      mime.types    mke2fs.conf  rc4.d         terminfo
cron.weekly  hosts.allow nftables.conf rc5.d         timezone
cron.yearly  hosts.deny modprobe.d    rc6.d         tmpfiles.d
cryptsetup-initramfs init.d      modules       reportbug.conf ucf.conf
crypttab     initramfs-tools inputrc       modules-load.d resolv.conf   udev
dbus-1       iproute2   mtab          rmt           rfc           ufw
debconf.conf issue       nanorc        rpc           runit         update-motd.d
debconf      debian_version issue.net     security      vim           xdg
deluser.conf kernel      kernel-img.conf ldap          shadow
dhcp         ldap       ld.so.cache   nsswitch.conf shells
dictionaries-common discover.conf.d root@meguzqui42:/etc# cd sudoers.d/
root@meguzqui42:/etc/sudoers.d# ls -la
total 16
drwxr-xr-x  2 root root 4096 Mar 25 13:20 .
drwxr-xr-x 69 root root 4096 Mar 25 12:42 ..
-r--r----- 1 root root 1096 Jun 27  2023 README
-rw-r--r--  1 root root 308 Mar 25 13:20 sudo_conf
root@meguzqui42:/etc/sudoers.d#
```

11. Al no tener el archivo `sudo_config` en la carpeta `/var/log/sudo` nos da un error, para ello creamos el archivo en dicha carpeta.

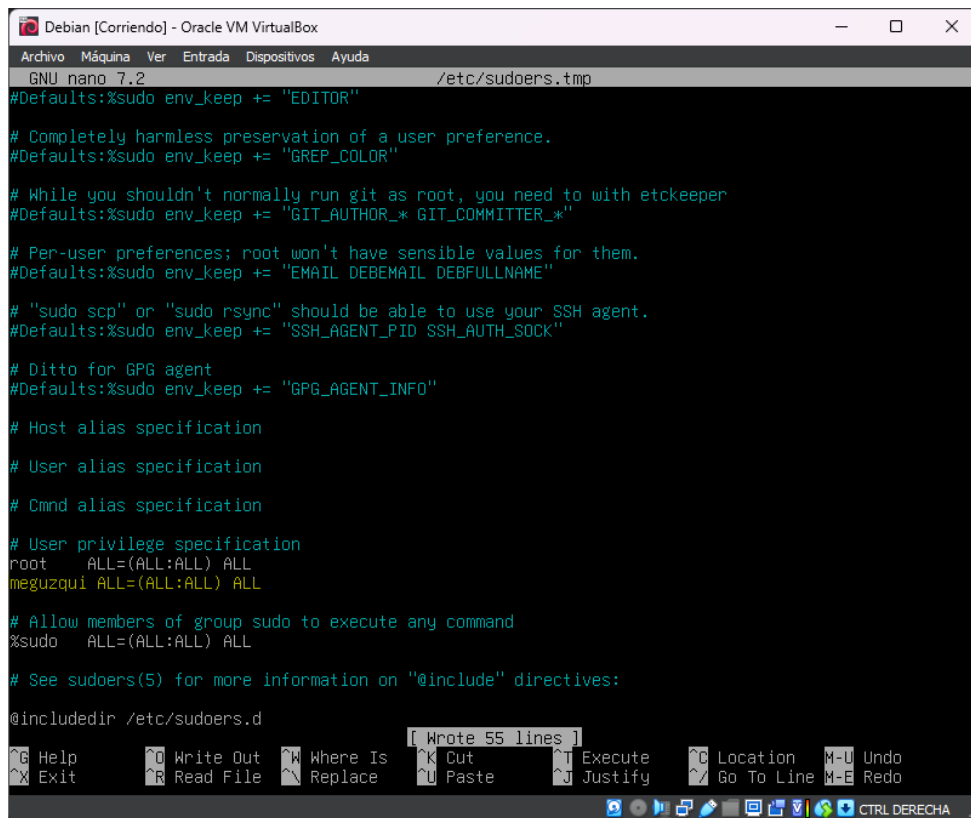


```
Debian [Corriendo] - Oracle VM VirtualBox
[sudo] password for meguzqui:
sudo: unable to open log file /var/log/sudo/sudo_config: No such file or directory
meguzqui is not in the sudoers file.
meguzqui@meguzqui42:~$ cd /var/log/sudo
bash: cd: /var/log/sudo: No such file or directory
meguzqui@meguzqui42:~$ su root
Password:
root@meguzqui42:/home/meguzqui# cd /var/log/sudo
bash: cd: /var/log/sudo: No such file or directory
root@meguzqui42:/home/meguzqui# cd /var/log/sudo
bash: cd: /var/log/sudo: No such file or directory
root@meguzqui42:/home/meguzqui# cd ..
root@meguzqui42:/home# cd ...
bash: cd: ...: No such file or directory
root@meguzqui42:/home# cd ..
root@meguzqui42:/# cd ..
root@meguzqui42:/# ls
bin  dev  home  initrd.img.old  lib64  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
root@meguzqui42:/# cd /var/log
root@meguzqui42:/var/log# ls
alternatives.log  btmp  faillog  journal  private  runit
apt  dpkg.log  installer  lastlog  README  wtmp
root@meguzqui42:/var/log# ls -a
.  alternatives.log  btmp  faillog  journal  private  runit
.. apt  dpkg.log  installer  lastlog  README  wtmp
root@meguzqui42:/var/log# mkdir sudo
root@meguzqui42:/var/log# ls
alternatives.log  btmp  faillog  journal  private  runit  wtmp
apt  dpkg.log  installer  lastlog  README  sudo
root@meguzqui42:/var/log# cd sudo
root@meguzqui42:/var/log/sudo# touch sudo_config
root@meguzqui42:/var/log/sudo# ls
sudo_config
root@meguzqui42:/var/log/sudo# pwd
/var/log/sudo
root@meguzqui42:/var/log/sudo# _
```

12. Como nuestro usuario “meguzqui” no está registrado para usar sudo, nos da este error. Lo solucionamos dándolo de alta. Para ello escribimos “sudo visudo” y nos abrirá el archivo `sudoers` en el que añadiremos esta línea.



```
Debian [Corriendo] - Oracle VM VirtualBox
root@meguzqui42:/var/log/sudo# ls
sudo_config
root@meguzqui42:/var/log/sudo# su meguzqui
meguzqui@meguzqui42:/var/log/sudo$ cd
meguzqui@meguzqui42:~$ ls
meguzqui@meguzqui42:~$ sudo mkdir prueba
[sudo] password for meguzqui:
meguzqui is not in the sudoers file.
meguzqui@meguzqui42:~$
```



```
Debian [Corriendo] - Oracle VM VirtualBox
GNU nano 7.2 /etc/sudoers.tmp
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

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

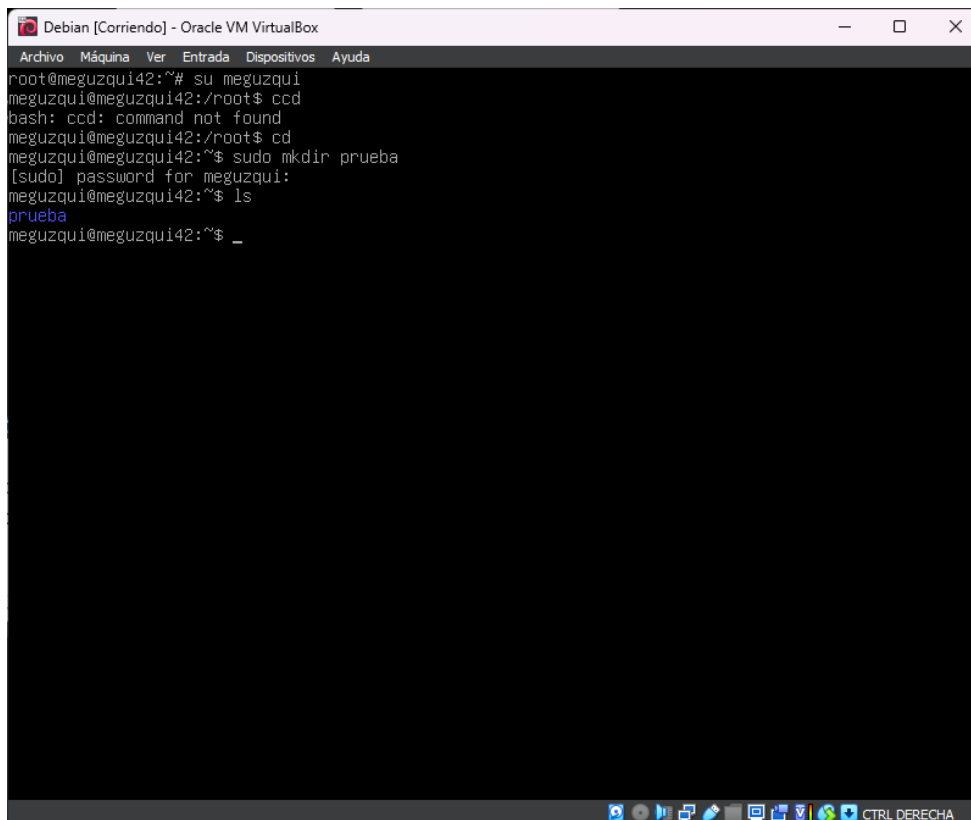
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

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

@include /etc/sudoers.d

Wrote 55 lines
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^V Paste      ^J Justify    ^_ Go To Line   M-E Redo
CTRL DERECHA
```

13. Una vez resueltos estos errores, vamos a probar a realizar un comando con sudo y ver si guarda su salida y entrada en el archivo /var/log/sudo.



```
Debian [Corriendo] - Oracle VM VirtualBox
root@meguzqui42:~# su meguzqui
meguzqui@meguzqui42:/root$ ccd
bash: ccd: command not found
meguzqui@meguzqui42:/root$ cd
meguzqui@meguzqui42:~$ sudo mkdir prueba
[sudo] password for meguzqui:
meguzqui@meguzqui42:~$ ls
prueba
meguzqui@meguzqui42:~$ _
```

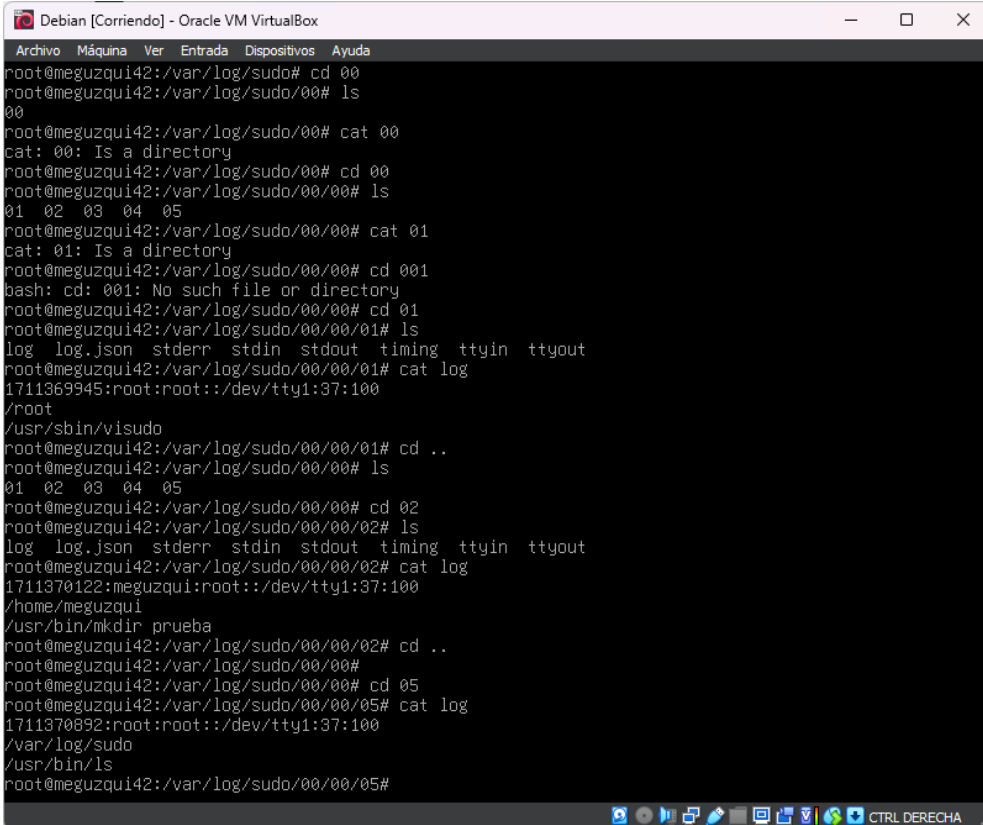


```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
meguzqui@meguzqui42:~$ su root
Password:
root@meguzqui42:/home/meguzqui# cd
root@meguzqui42:~# cd /var/log
root@meguzqui42:/var/log# ls
alternatives.log  btmp      faillog    journal    private    runit      wtmp
apt               dpkg.log  installer  lastlog    README     sudo
root@meguzqui42:/var/log# cd sudo
root@meguzqui42:/var/log/sudo# ls
00  seq  sudo_config
root@meguzqui42:/var/log/sudo# cat sudo_config
Mar 25 13:28:27 : meguzqui : user NOT in sudoers ; TTY=tty1 ; PWD=/home/meguzqui
; USER=root ; COMMAND=/usr/bin/mkdir prueba
Mar 25 13:31:35 : meguzqui : user NOT in sudoers ; TTY=tty1 ; PWD=/home/meguzqui
; USER=root ; COMMAND=/usr/bin/nano
Mar 25 13:32:25 : root : TTY=tty1 ; PWD=/root ; USER=root ; TSID=01 ;
COMMAND=/usr/sbin/visudo
Mar 25 13:35:19 : meguzqui : TTY=tty1 ; PWD=/home/meguzqui ; USER=root ; TSID=02
; COMMAND=/usr/bin/mkdir prueba
root@meguzqui42:/var/log/sudo# _
```

Como podemos observar el archivo “seq” muestra el número de ordenes que se han ejecutado con sudo.

```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:~# cd /var/log/sudo
root@meguzqui42:/var/log/sudo# ls
00  seq  sudo_config
root@meguzqui42:/var/log/sudo# cat seq
000004
root@meguzqui42:/var/log/sudo# cat sudo_config
Mar 25 13:28:27 : meguzqui : user NOT in sudoers ; TTY=tty1 ; PWD=/home/meguzqui
; USER=root ; COMMAND=/usr/bin/mkdir prueba
Mar 25 13:31:35 : meguzqui : user NOT in sudoers ; TTY=tty1 ; PWD=/home/meguzqui
; USER=root ; COMMAND=/usr/bin/nano
Mar 25 13:32:25 : root : TTY=tty1 ; PWD=/root ; USER=root ; TSID=01 ;
COMMAND=/usr/sbin/visudo
Mar 25 13:35:19 : meguzqui : TTY=tty1 ; PWD=/home/meguzqui ; USER=root ; TSID=02
; COMMAND=/usr/bin/mkdir prueba
Mar 25 13:40:36 : root : TTY=tty1 ; PWD=/root ; USER=root ; TSID=03 ;
COMMAND=/usr/bin/ssh server status
Mar 25 13:41:23 : root : TTY=tty1 ; PWD=/root ; USER=root ; TSID=04 ;
COMMAND=/usr/bin/systemctl ssh restart
root@meguzqui42:/var/log/sudo# _
```

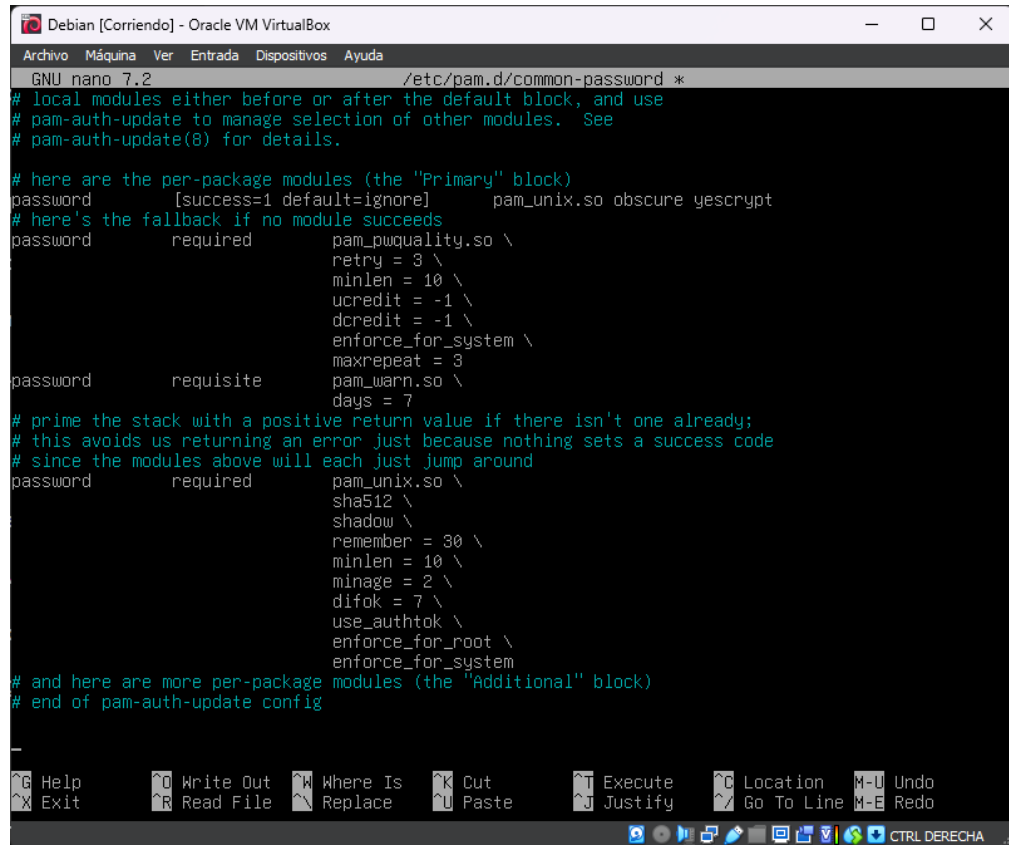
Además de guardarse en el archivo sudo\_conf se guarda en los directorios 00 dentro de var/log/sudo. Cada número de carpeta representa una llamada de sudo.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:/var/log/sudo# cd 00
root@meguzqui42:/var/log/sudo/00# ls
00
root@meguzqui42:/var/log/sudo/00# cat 00
cat: 00: Is a directory
root@meguzqui42:/var/log/sudo/00# cd 00
root@meguzqui42:/var/log/sudo/00/00# ls
01 02 03 04 05
root@meguzqui42:/var/log/sudo/00/00# cat 01
cat: 01: Is a directory
root@meguzqui42:/var/log/sudo/00/00# cd 001
bash: cd: 001: No such file or directory
root@meguzqui42:/var/log/sudo/00/00# cd 01
root@meguzqui42:/var/log/sudo/00/00/01# ls
log log.json stderr stdin stdout timing ttyin ttyout
root@meguzqui42:/var/log/sudo/00/00/01# cat log
1711369945:root:root::/dev/tty1:37:100
/root
/usr/sbin/visudo
root@meguzqui42:/var/log/sudo/00/00/01# cd ..
root@meguzqui42:/var/log/sudo/00/00# ls
01 02 03 04 05
root@meguzqui42:/var/log/sudo/00/00# cd 02
root@meguzqui42:/var/log/sudo/00/00/02# ls
log log.json stderr stdin stdout timing ttyin ttyout
root@meguzqui42:/var/log/sudo/00/00/02# cat log
1711370122:meguzqui:root::/dev/tty1:37:100
/home/meguzqui
/usr/bin/mkdir prueba
root@meguzqui42:/var/log/sudo/00/00/02# cd ..
root@meguzqui42:/var/log/sudo/00/00# 
root@meguzqui42:/var/log/sudo/00/00# cd 05
root@meguzqui42:/var/log/sudo/00/00/05# cat log
1711370892:root:root::/dev/tty1:37:100
/var/log/sudo
/usr/bin/ls
root@meguzqui42:/var/log/sudo/00/00/05#
```

Con todo esto la política de reglas estrictas de sudo está terminada.

14. Política de contraseñas fuerte. Para ello vamos a modificar el archivo de configuración de PAM que se encuentra en `/etc/pam.d/common-password`, añadimos las siguientes líneas que cumplen con los requisitos de seguridad de las contraseñas que nos pedían. Añadimos las líneas de `pam_pwquality.so`, `pam_warn.so` y `pam_unix.so`.

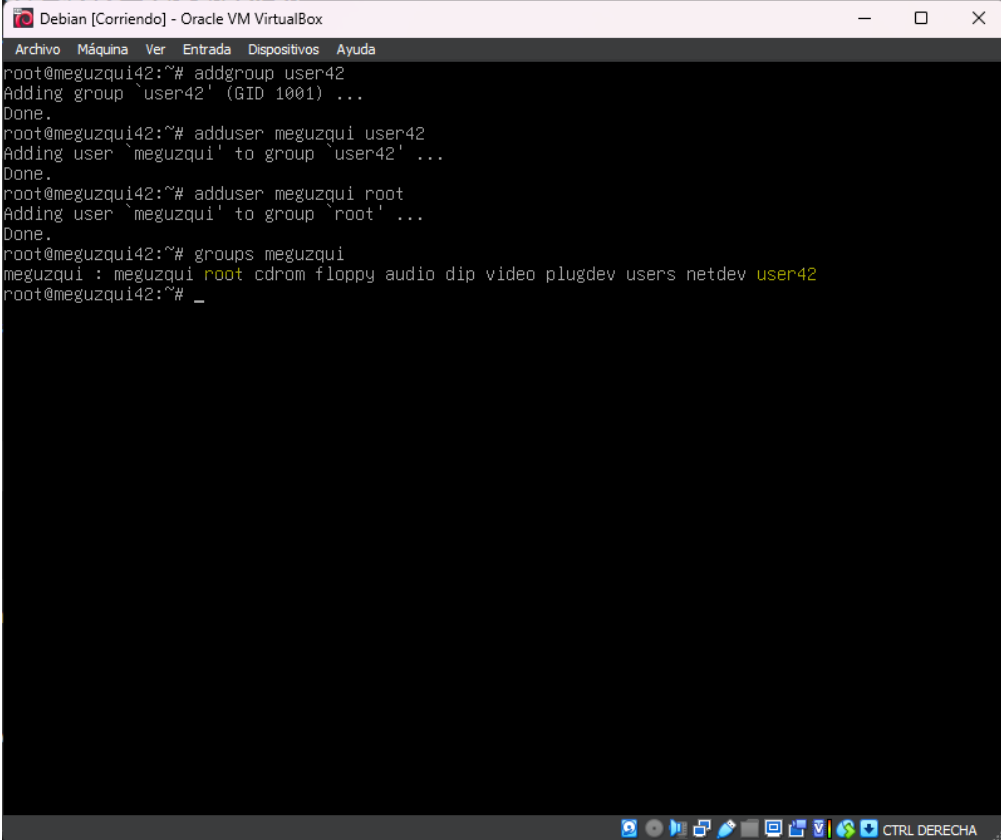


```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 7.2 /etc/pam.d/common-password *
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure yescrypt
# here's the fallback if no module succeeds
password required pam_pwquality.so \
    retry = 3 \
    minlen = 10 \
    ucredit = -1 \
    dcredit = -1 \
    enforce_for_system \
    maxrepeat = 3
password requisite pam_warn.so \
    days = 7
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_unix.so \
    sha512 \
    shadow \
    remember = 30 \
    minlen = 10 \
    minage = 2 \
    difok = 7 \
    use_authok \
    enforce_for_root \
    enforce_for_system
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

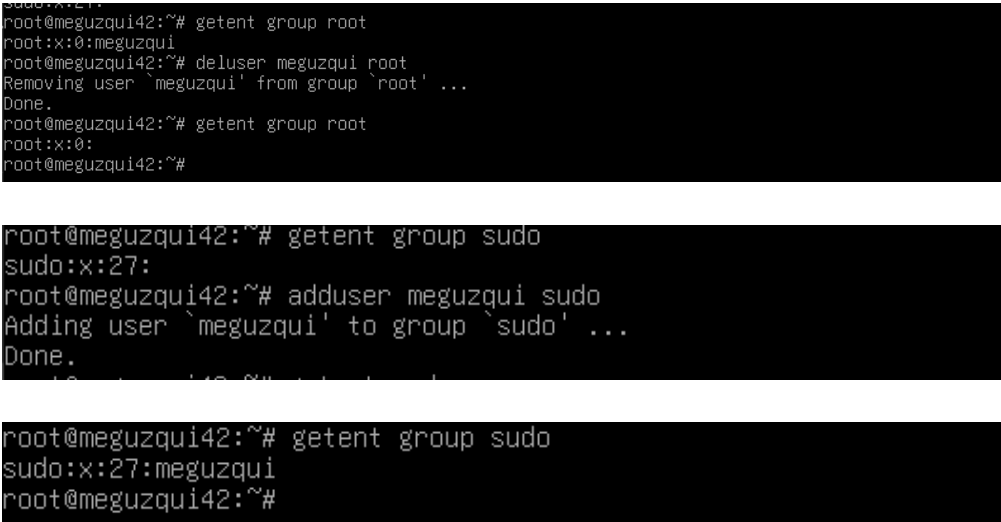
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify  ^_ Go To Line M-E Redo
CTRL DERECHA
```

15. Vamos a añadir a nuestro usuario meguzqui a los grupos user42 y root. Para ello primero creamos el nuevo grupo “user42” y después añadimos el usuario a ambos y verificamos que este añadido.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:~# addgroup user42
Adding group 'user42' (GID 1001) ...
Done.
root@meguzqui42:~# adduser meguzqui user42
Adding user 'meguzqui' to group 'user42' ...
Done.
root@meguzqui42:~# adduser meguzqui root
Adding user 'meguzqui' to group 'root' ...
Done.
root@meguzqui42:~# groups meguzqui
meguzqui : meguzqui root cdrom floppy audio dip video plugdev users netdev user42
root@meguzqui42:~# _
```

16. Hemos añadido meguzqui a root en vez de a sudo que es lo que nos pedía, entonces vamos a eliminarlo de root y añadirlo correctamente a sudo..

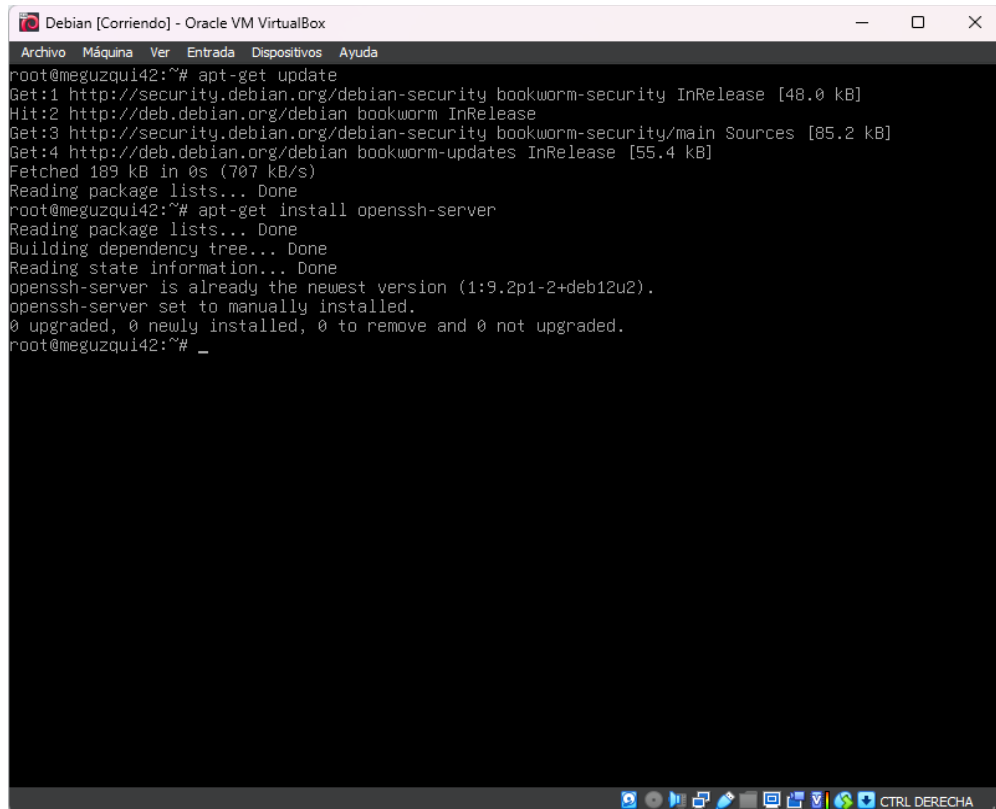


```
root@meguzqui42:~# getent group root
root:x:0:meguzqui
root@meguzqui42:~# deluser meguzqui root
Removing user 'meguzqui' from group 'root' ...
Done.
root@meguzqui42:~# getent group root
root:x:0:
root@meguzqui42:~#

root@meguzqui42:~# getent group sudo
sudo:x:27:
root@meguzqui42:~# adduser meguzqui sudo
Adding user 'meguzqui' to group 'sudo' ...
Done.

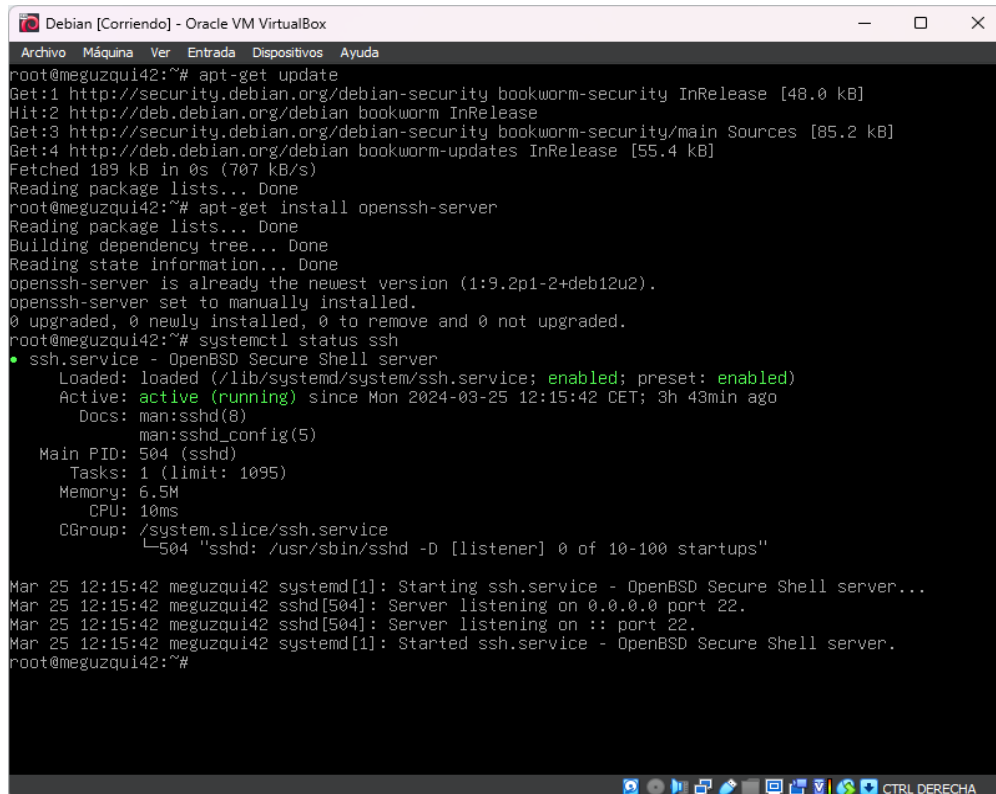
root@meguzqui42:~# getent group sudo
sudo:x:27:meguzqui
root@meguzqui42:~#
```

17. Instalamos y configuramos el servicio SSH. Como ya venía instalado no requiere ninguna modificación.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:~# apt-get update
Get:1 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:2 http://deb.debian.org/debian bookworm InRelease
Get:3 http://security.debian.org/debian-security bookworm-security/main Sources [85.2 kB]
Get:4 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Fetched 189 kB in 0s (707 kB/s)
Reading package lists... Done
root@meguzqui42:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:9.2p1-2+deb12u2).
openssh-server set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@meguzqui42:~# _
```

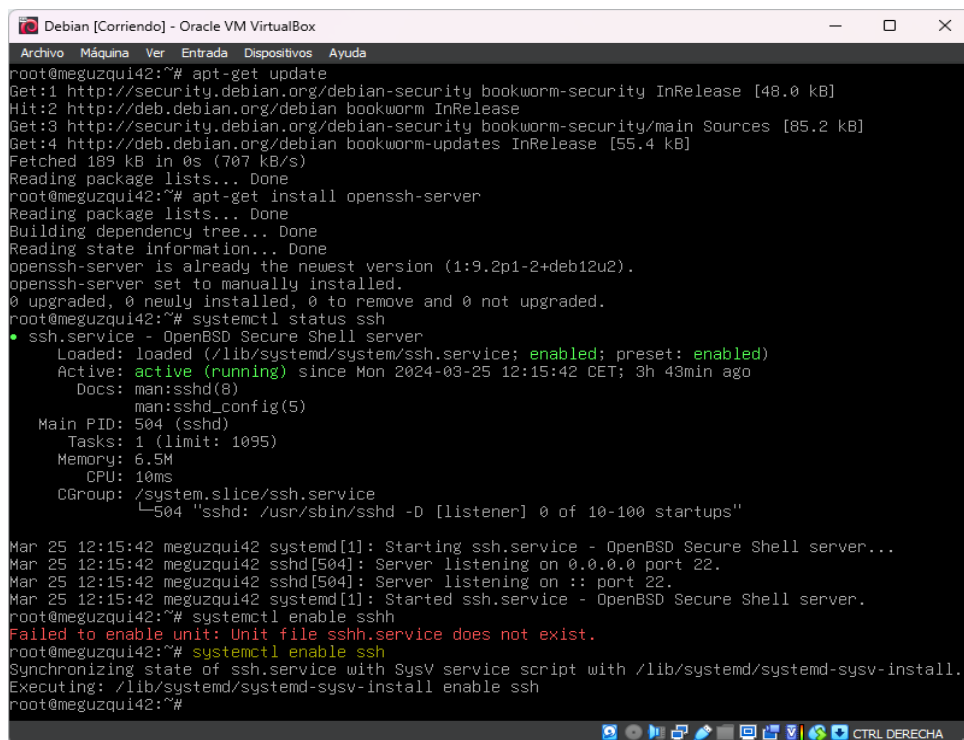
18. Vemos que se encuentra en funcionamiento con este comando.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:~# apt-get update
Get:1 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:2 http://deb.debian.org/debian bookworm InRelease
Get:3 http://security.debian.org/debian-security bookworm-security/main Sources [85.2 kB]
Get:4 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Fetched 189 kB in 0s (707 kB/s)
Reading package lists... Done
root@meguzqui42:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:9.2p1-2+deb12u2).
openssh-server set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@meguzqui42:~# systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-03-25 12:15:42 CET; 3h 43min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 504 (sshd)
     Tasks: 1 (limit: 1095)
    Memory: 6.5M
       CPU: 10ms
   CGroup: /system.slice/ssh.service
           └─504 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 25 12:15:42 meguzqui42 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 25 12:15:42 meguzqui42 sshd[504]: Server listening on 0.0.0.0 port 22.
Mar 25 12:15:42 meguzqui42 sshd[504]: Server listening on :: port 22.
Mar 25 12:15:42 meguzqui42 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@meguzqui42:~#
```

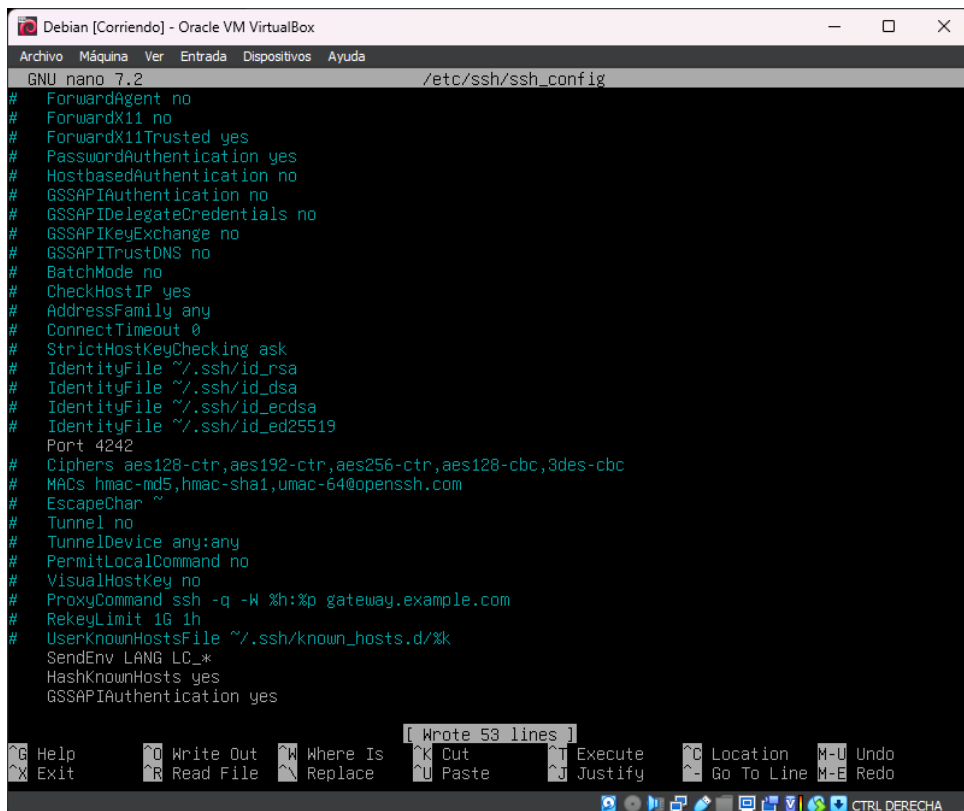
19. Configuramos su inicio al arranque con este otro comando.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:~# apt-get update
Get:1 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:2 http://deb.debian.org/debian bookworm InRelease
Get:3 http://security.debian.org/debian-security bookworm-security/main Sources [85.2 kB]
Get:4 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Fetched 189 kB in 0s (707 kB/s)
Reading package lists... Done
root@meguzqui42:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:9.2p1-2+deb12u2).
openssh-server set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@meguzqui42:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-03-25 12:15:42 CET; 3h 43min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 504 (sshd)
     Tasks: 1 (limit: 1095)
    Memory: 6.5M
       CPU: 10ms
    CGroup: /system.slice/ssh.service
            └─504 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 25 12:15:42 meguzqui42 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 25 12:15:42 meguzqui42 sshd[504]: Server listening on 0.0.0.0 port 22.
Mar 25 12:15:42 meguzqui42 sshd[504]: Server listening on :: port 22.
Mar 25 12:15:42 meguzqui42 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@meguzqui42:~# systemctl enable sshh
Failed to enable unit: Unit file sshh.service does not exist.
root@meguzqui42:~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@meguzqui42:~#
```

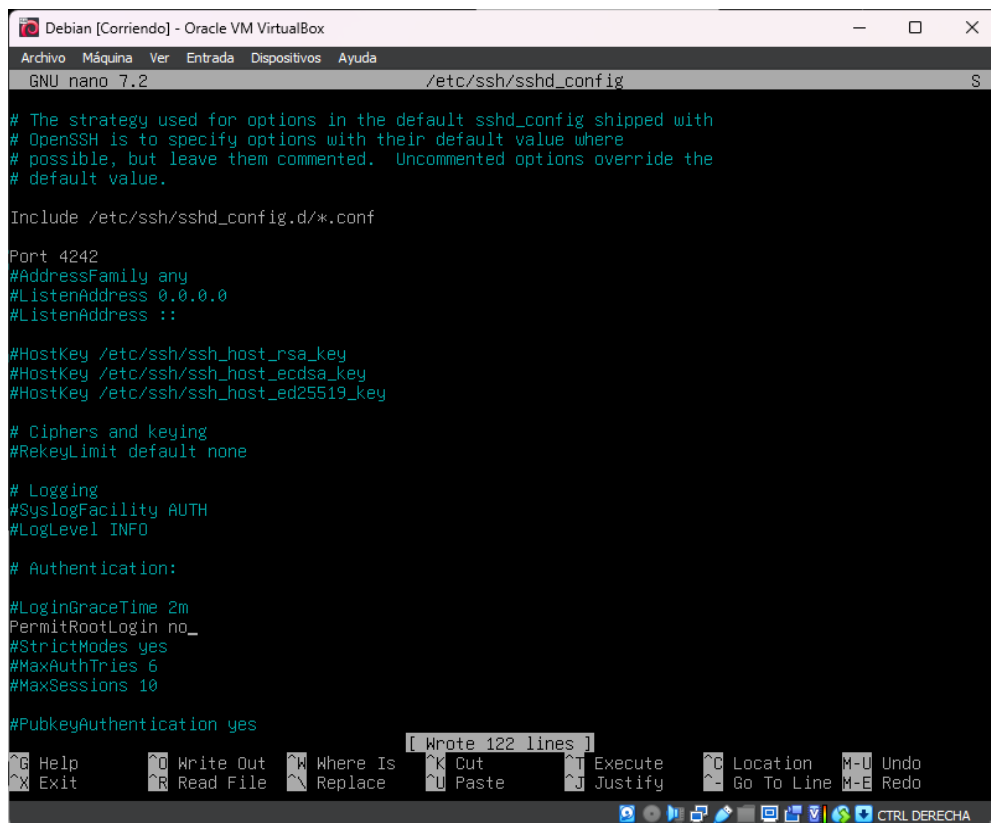
20. Pasamos a la configuración de SSH para que funcione solo en el puerto 4242 en el fichero ssh\_config.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 7.2 /etc/ssh/ssh_config
# 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 4242
# 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

[ Wrote 53 lines ]
^G Help  ^O Write Out  ^W Where Is  ^K Cut        ^T Execute    ^C Location  M-U Undo
^X Exit  ^R Read File  ^M Replace   ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
CTRL DERECHA
```

21. Impedimos el acceso de SSH como root en el fichero sshd\_config.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 7.2 /etc/ssh/sshd_config S

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

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

Port 4242
#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

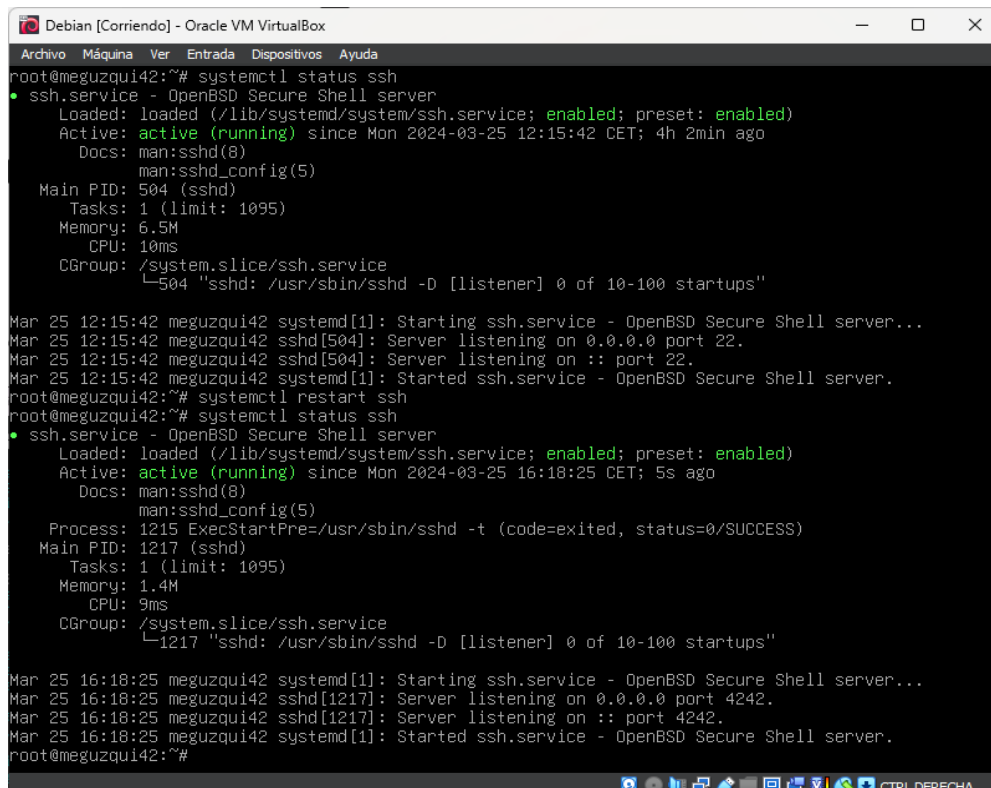
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

22. Debemos reiniciar el servicio para que se aplique la configuración correctamente y al hacer status vemos que ya funciona en el puerto 4242.

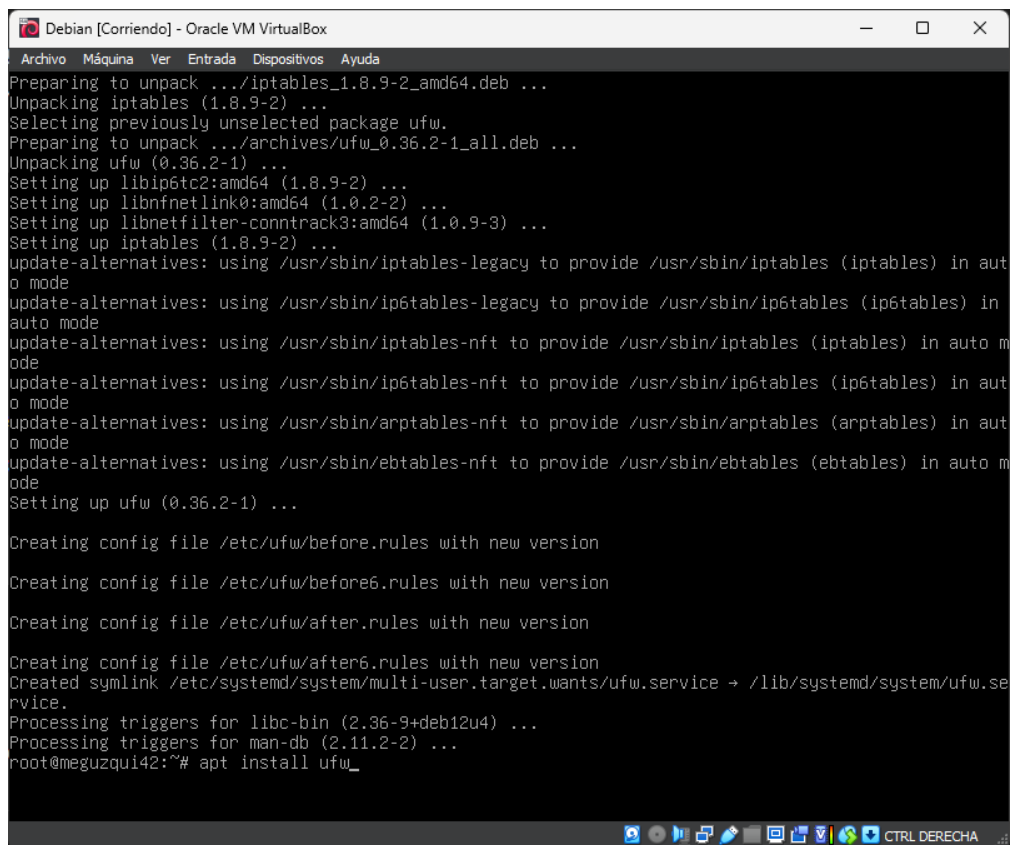


```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@meguzqui42:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-03-25 12:15:42 CET; 4h 2min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 504 (sshd)
     Tasks: 1 (limit: 1095)
    Memory: 6.5M
       CPU: 10ms
   CGroup: /system.slice/ssh.service
           └─504 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 25 12:15:42 meguzqui42 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 25 12:15:42 meguzqui42 sshd[504]: Server listening on 0.0.0.0 port 22.
Mar 25 12:15:42 meguzqui42 sshd[504]: Server listening on :: port 22.
Mar 25 12:15:42 meguzqui42 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@meguzqui42:~# systemctl restart ssh
root@meguzqui42:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-03-25 16:18:25 CET; 5s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1215 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1217 (sshd)
     Tasks: 1 (limit: 1095)
    Memory: 1.4M
       CPU: 9ms
   CGroup: /system.slice/ssh.service
           └─1217 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 25 16:18:25 meguzqui42 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 25 16:18:25 meguzqui42 sshd[1217]: Server listening on 0.0.0.0 port 4242.
Mar 25 16:18:25 meguzqui42 sshd[1217]: Server listening on :: port 4242.
Mar 25 16:18:25 meguzqui42 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@meguzqui42:~#
```

23. Instalamos el firewall UFW. Usamos apt install ufw.



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Preparing to unpack .../iptables_1.8.9-2_amd64.deb ...
Unpacking iptables (1.8.9-2) ...
Selecting previously unselected package ufw.
Preparing to unpack .../archives/ufw_0.36.2-1_all.deb ...
Unpacking ufw (0.36.2-1) ...
Setting up libip6tc2:amd64 (1.8.9-2) ...
Setting up libnfnetlink0:amd64 (1.0.2-2) ...
Setting up libnetfilter-conntrack3:amd64 (1.0.9-3) ...
Setting up iptables (1.8.9-2) ...
update-alternatives: using /usr/sbin/iptables-legacy to provide /usr/sbin/iptables (iptables) in auto mode
update-alternatives: using /usr/sbin/ip6tables-legacy to provide /usr/sbin/ip6tables (ip6tables) in auto mode
update-alternatives: using /usr/sbin/iptables-nft to provide /usr/sbin/iptables (iptables) in auto mode
update-alternatives: using /usr/sbin/ip6tables-nft to provide /usr/sbin/ip6tables (ip6tables) in auto mode
update-alternatives: using /usr/sbin/arptables-nft to provide /usr/sbin/arptables (arptables) in auto mode
update-alternatives: using /usr/sbin/ebtables-nft to provide /usr/sbin/ebtables (ebtables) in auto mode
Setting up ufw (0.36.2-1) ...

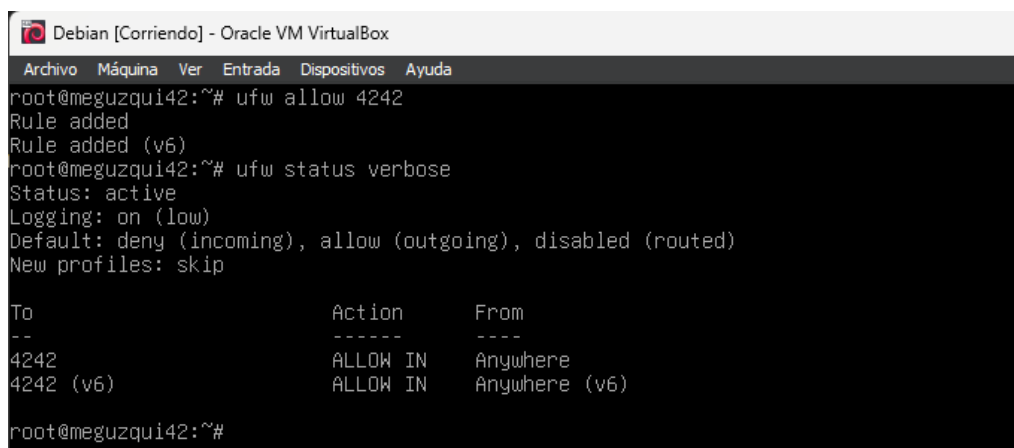
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.service.
Processing triggers for libc-bin (2.36-9+deb12u4) ...
Processing triggers for man-db (2.11.2-2) ...
root@meguzqui42:~# apt install ufw_
```

24. Comprobamos su estado y lo activamos si esta apagado.



```
root@meguzqui42:~# ufw status
Status: inactive
root@meguzqui42:~# ufw enable
Firewall is active and enabled on system startup
root@meguzqui42:~#
```

25. Permitimos la entrada al puerto 4242 que es el que estamos usando en nuestro ssh.



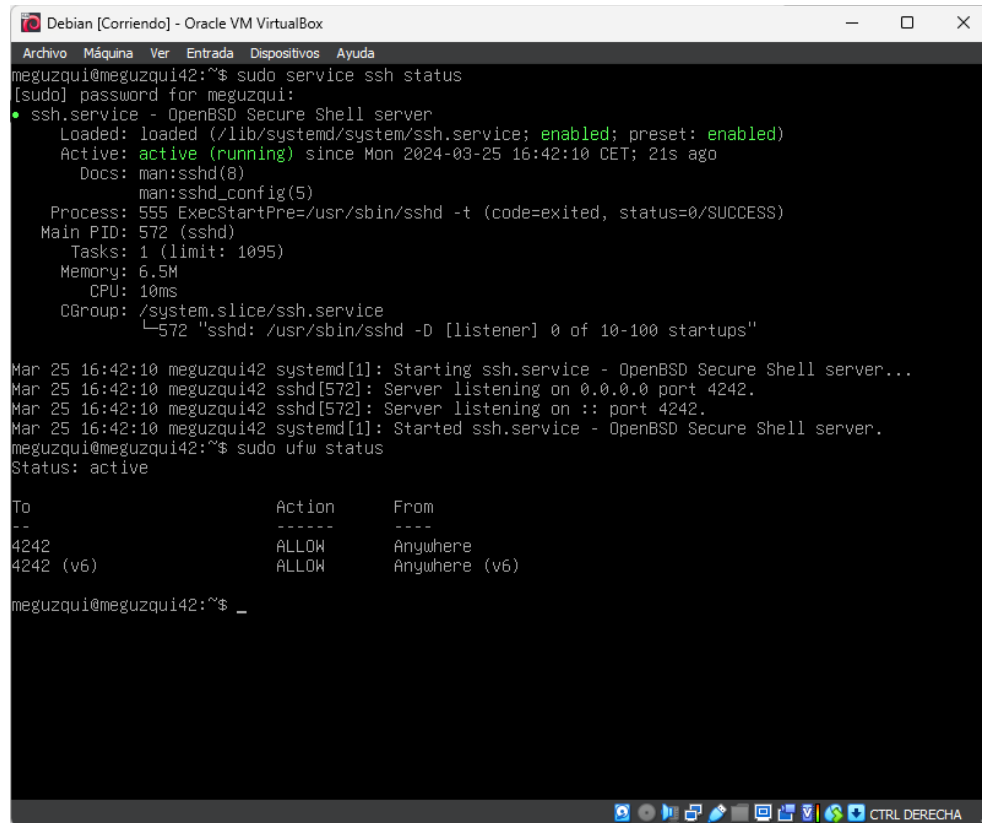
```
root@meguzqui42:~# ufw allow 4242
Rule added
Rule added (v6)
root@meguzqui42:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
4242 ALLOW IN Anywhere
4242 (v6) ALLOW IN Anywhere (v6)

root@meguzqui42:~#
```



26. Reiniciamos la máquina para corroborar que los servicios hasta ahora están bien instalados y configurados.



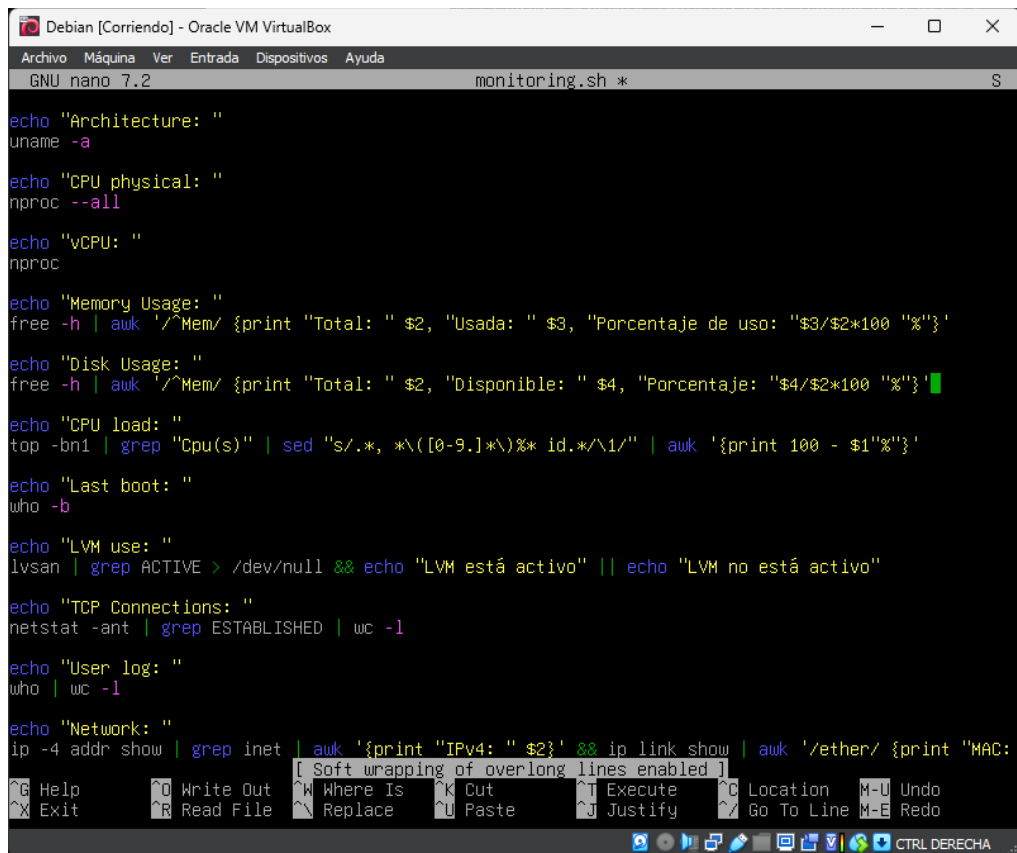
```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
meguzqui@meguzqui42:~$ sudo service ssh status
[sudo] password for meguzqui:
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-03-25 16:42:10 CET; 21s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 555 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 572 (sshd)
    Tasks: 1 (limit: 1095)
   Memory: 6.5M
      CPU: 10ms
   CGroup: /system.slice/ssh.service
           └─572 'sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 25 16:42:10 meguzqui42 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Mar 25 16:42:10 meguzqui42 sshd[572]: Server listening on 0.0.0.0 port 4242.
Mar 25 16:42:10 meguzqui42 sshd[572]: Server listening on :: port 4242.
Mar 25 16:42:10 meguzqui42 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
meguzqui@meguzqui42:~$ sudo ufw status
Status: active

To
--
4242
4242 (v6)
Action
-----
ALLOW
ALLOW
From
----
Anywhere
Anywhere (v6)

meguzqui@meguzqui42:~$ _
```

27. Vamos a hacer el bash que muestre la información en pantalla del sistema. Empezando por “#!/bin/bash”.



```
Debian [Corriendo] - Oracle VM VirtualBox
GNU nano 7.2 monitoring.sh *

echo "Architecture: "
uname -a

echo "CPU physical: "
nproc --all

echo "vCPU: "
nproc

echo "Memory Usage: "
free -h | awk '/Mem/ {print "Total: " $2, "Usada: " $3, "Porcentaje de uso: "$3/$2*100 "%"}'

echo "Disk Usage: "
free -h | awk '/Mem/ {print "Total: " $2, "Disponible: " $4, "Porcentaje: "$4/$2*100 "%"}'

echo "CPU load: "
top -bn1 | grep "Cpu(s)" | sed "s/.*, *\([0-9.]*\)%* id.*\/1/" | awk '{print 100 - $1"%"}'

echo "Last boot: "
who -b

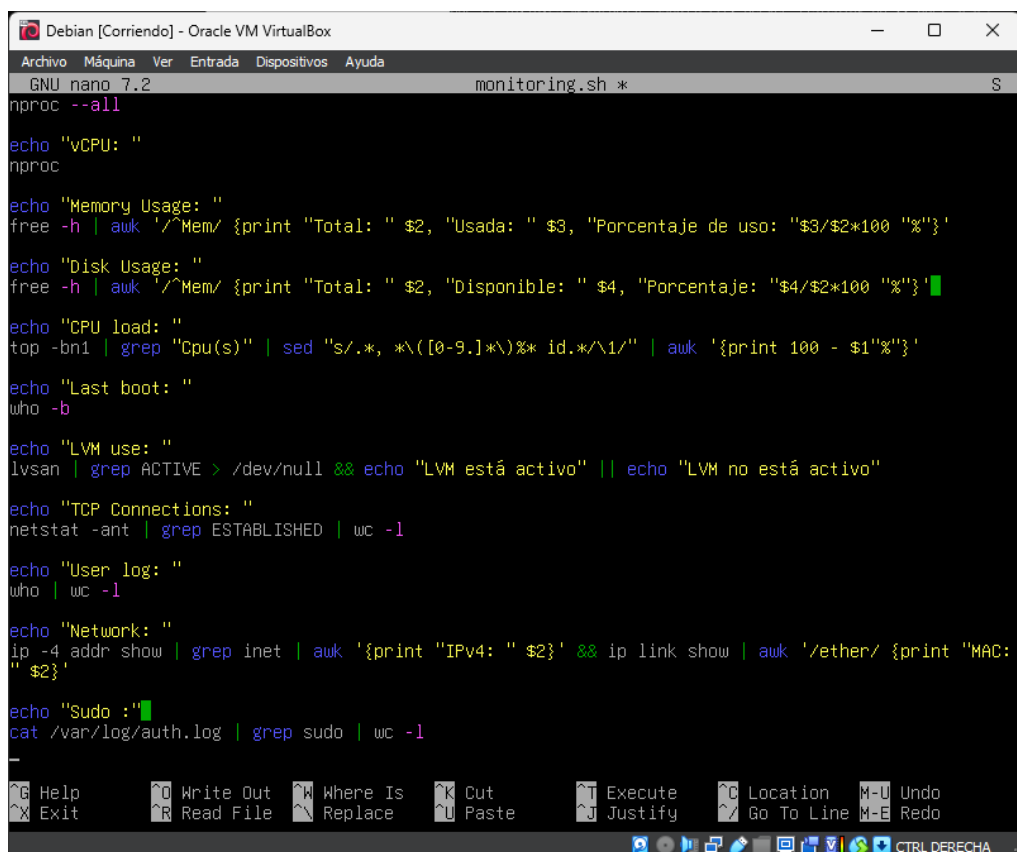
echo "LVM use: "
lvsan | grep ACTIVE > /dev/null && echo "LVM está activo" || echo "LVM no está activo"

echo "TCP Connections: "
netstat -ant | grep ESTABLISHED | wc -l

echo "User log: "
who | wc -l

echo "Network: "
ip -4 addr show | grep inet | awk '{print "IPv4: " $2}' && ip link show | awk '/ether/ {print "MAC: " $2}'

[ Soft wrapping of overlong lines enabled ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo
CTRL DERECHA
```



```
Debian [Corriendo] - Oracle VM VirtualBox
GNU nano 7.2 monitoring.sh *

nproc --all

echo "vCPU: "
nproc

echo "Memory Usage: "
free -h | awk '/Mem/ {print "Total: " $2, "Usada: " $3, "Porcentaje de uso: "$3/$2*100 "%"}'

echo "Disk Usage: "
free -h | awk '/Mem/ {print "Total: " $2, "Disponible: " $4, "Porcentaje: "$4/$2*100 "%"}'

echo "CPU load: "
top -bn1 | grep "Cpu(s)" | sed "s/.*, *\([0-9.]*\)%* id.*\/1/" | awk '{print 100 - $1"%"}'

echo "Last boot: "
who -b

echo "LVM use: "
lvsan | grep ACTIVE > /dev/null && echo "LVM está activo" || echo "LVM no está activo"

echo "TCP Connections: "
netstat -ant | grep ESTABLISHED | wc -l

echo "User log: "
who | wc -l

echo "Network: "
ip -4 addr show | grep inet | awk '{print "IPv4: " $2}' && ip link show | awk '/ether/ {print "MAC: " $2}'

echo "Sudo : "
cat /var/log/auth.log | grep sudo | wc -l

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo
CTRL DERECHA
```

