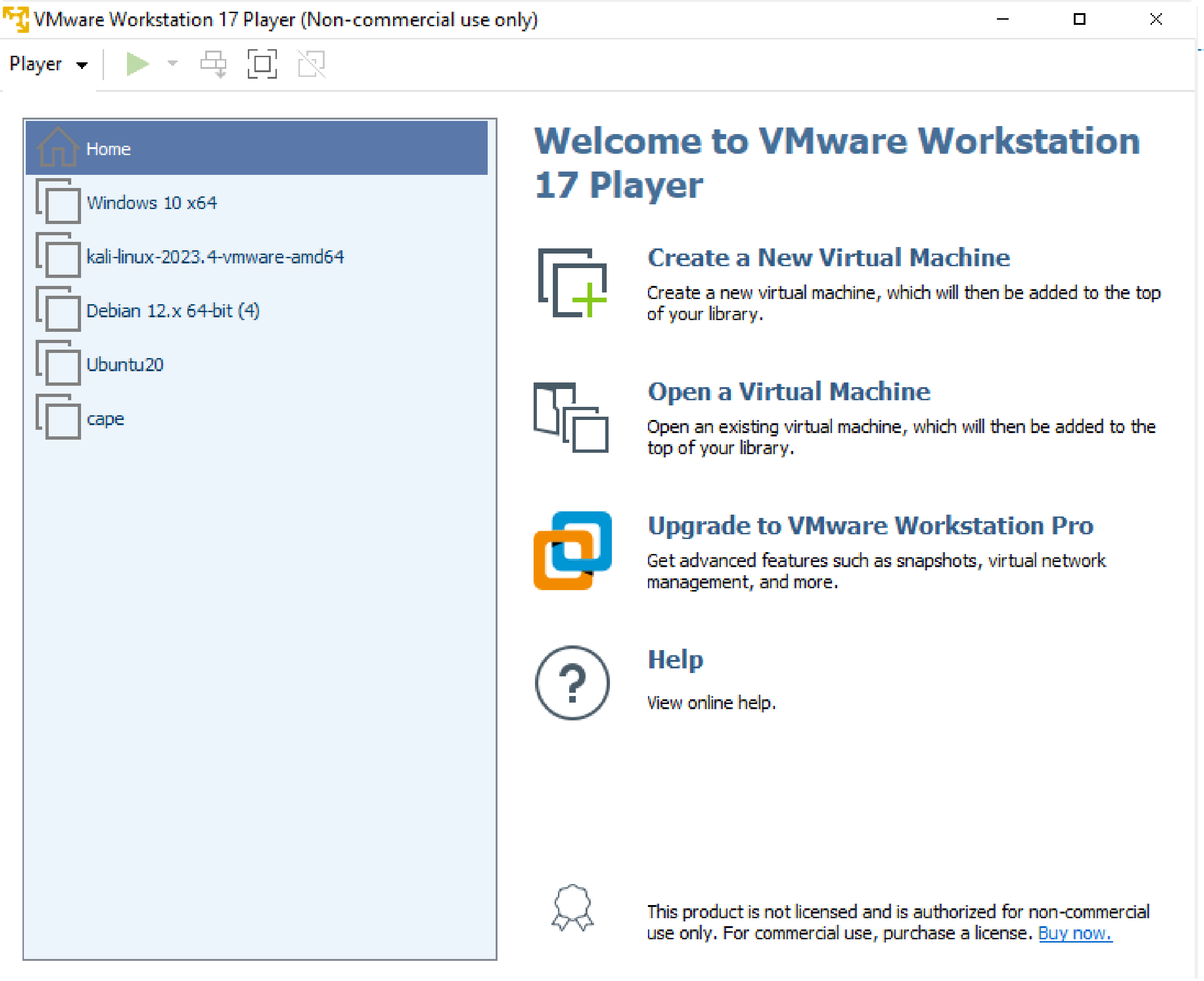
Ejercicio 2 Construir un laboratorio:

Máquina Windows 10:

Hacer click en Create a New Virtual Machine



VMware Workstation 17 Player (Non-commercial use only)

Welcome to VMware Workstation 17 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro

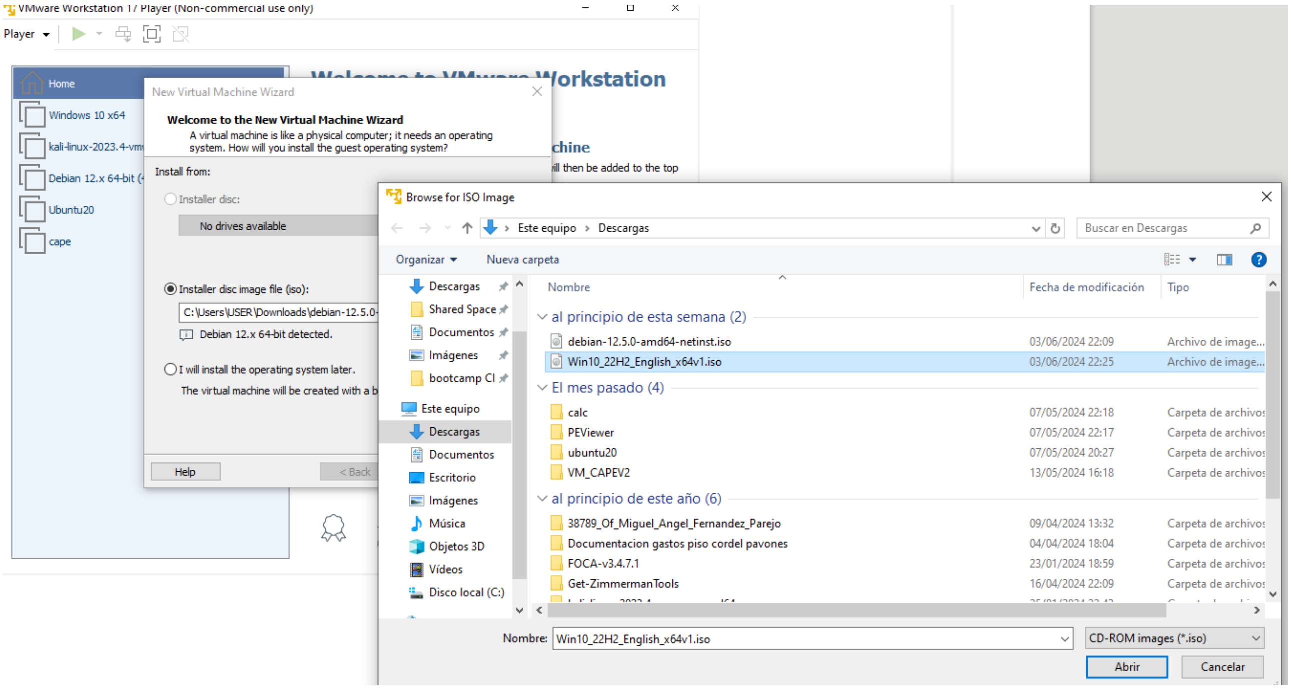
Get advanced features such as snapshots, virtual network management, and more.

Help

View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

Elijo la .iso de window10:



VMware Workstation 17 Player (Non-commercial use only)
Player
Home
Windows 10 x64
kali-linux-2023.4-vm
Debian 12.x 64-bit (
Ubuntu20
cape
Welcome to VMware Workstation
chine
ill then be added to the top

New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

C:\Users\USER\Downloads\debian-12.5.0-

Debian 12.x 64-bit detected.

○ I will install the operating system later.

The virtual machine will be created with a b

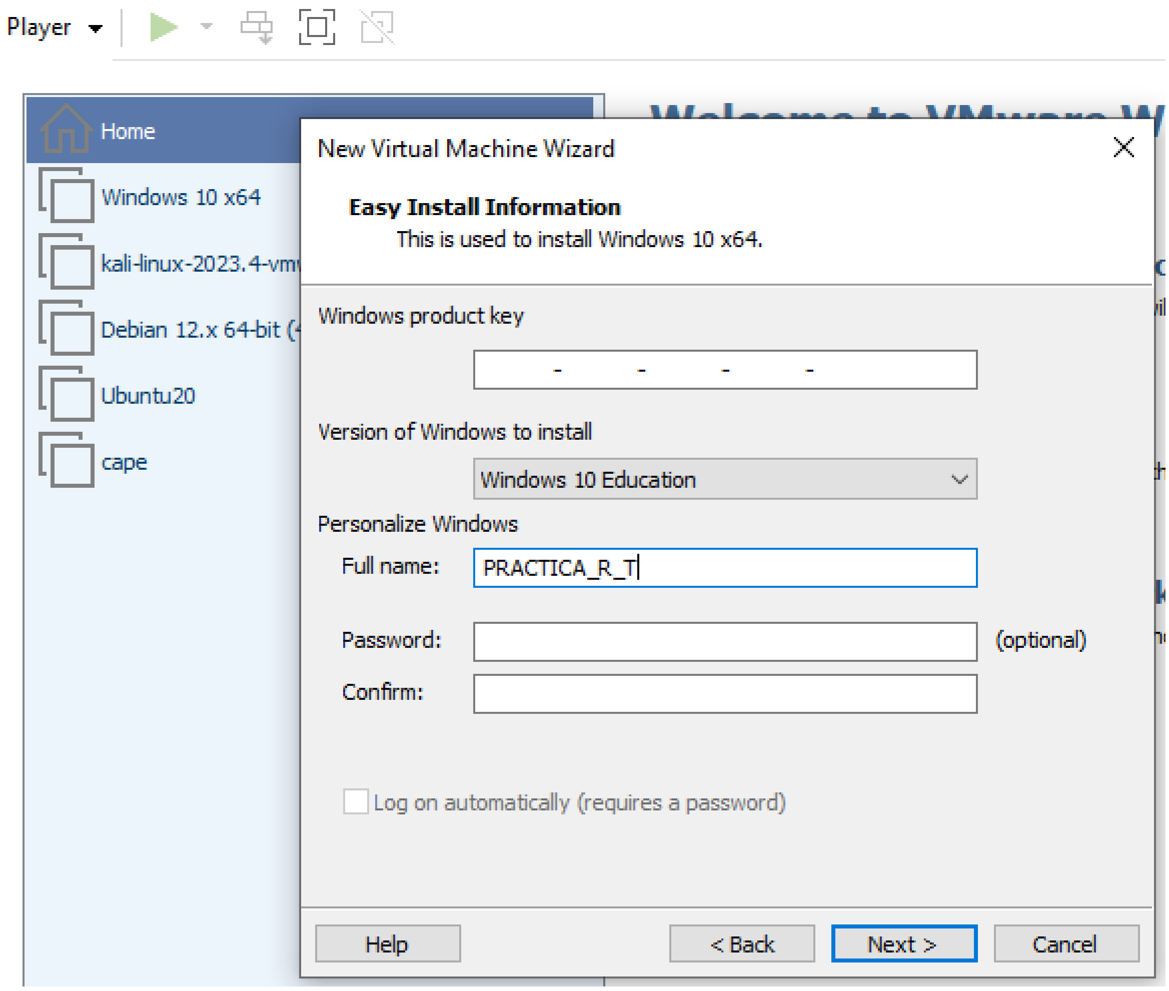
Browse for ISO Image

Nombre	Fecha de modificación	Tipo
al principio de esta semana (2)		
debian-12.5.0-amd64-netinst.iso	03/06/2024 22:09	Archivo de image...
Win10_22H2_English_x64v1.iso	03/06/2024 22:25	Archivo de image...
El mes pasado (4)		
calc	07/05/2024 22:18	Carpeta de archivos
PEViewer	07/05/2024 22:17	Carpeta de archivos
ubuntu20	07/05/2024 20:27	Carpeta de archivos
VM_CAPEV2	13/05/2024 16:18	Carpeta de archivos
al principio de este año (6)		
38789_Of_Miguel_Angel_Fernandez_Parejo	09/04/2024 13:32	Carpeta de archivos
Documentacion gastos piso cordel pavones	04/04/2024 18:04	Carpeta de archivos
FOCA-v3.4.7.1	23/01/2024 18:59	Carpeta de archivos
Get-ZimmermanTools	16/04/2024 22:09	Carpeta de archivos

Nombre: Win10_22H2_English_x64v1.iso

CD-ROM images (*.iso)

Le doy un nombre:



New Virtual Machine Wizard

Easy Install Information

This is used to install Windows 10 x64.

Windows product key

-   -   -   -

Version of Windows to install

Windows 10 Education

Personalize Windows

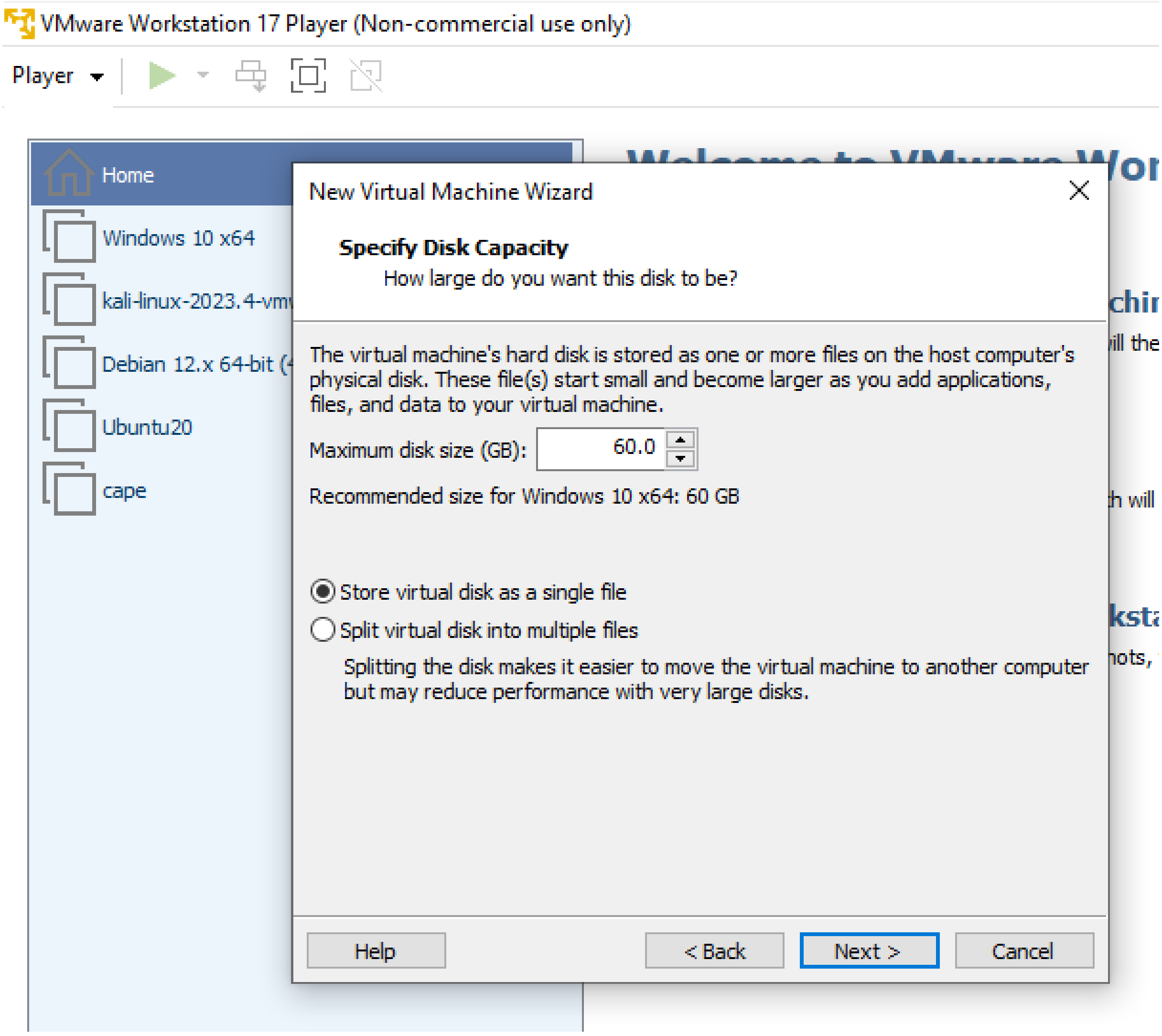
Full name: PRACTICA_R_T

Password: (optional)

Confirm:

□ Log on automatically (requires a password)

Dejo 60 GB de tamaño de disco y selecciono la opción Store virtual disk as single file, (disco virtual como un solo archivo)



New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

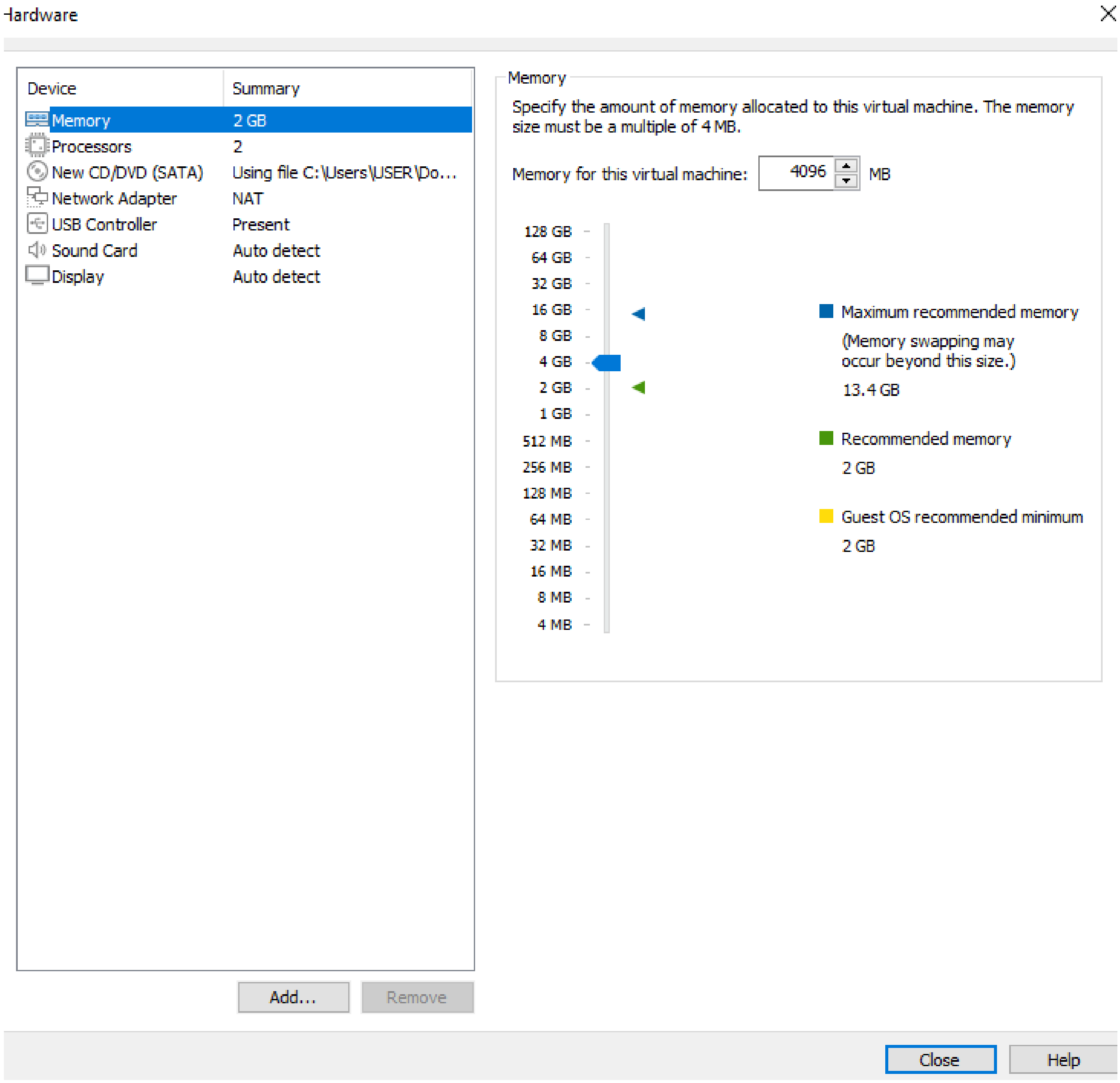
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 60.0

Recommended size for Windows 10 x64: 60 GB

● Store virtual disk as a single file
○ Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Aumento memoria RAM a 4GB



Hardware

Device	Summary
Memory	2 GB
Processors	2
New CD/DVD (SATA)	Using file C:\Users\USER\Do...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

🟦 Maximum recommended memory

(Memory swapping may occur beyond this size.)

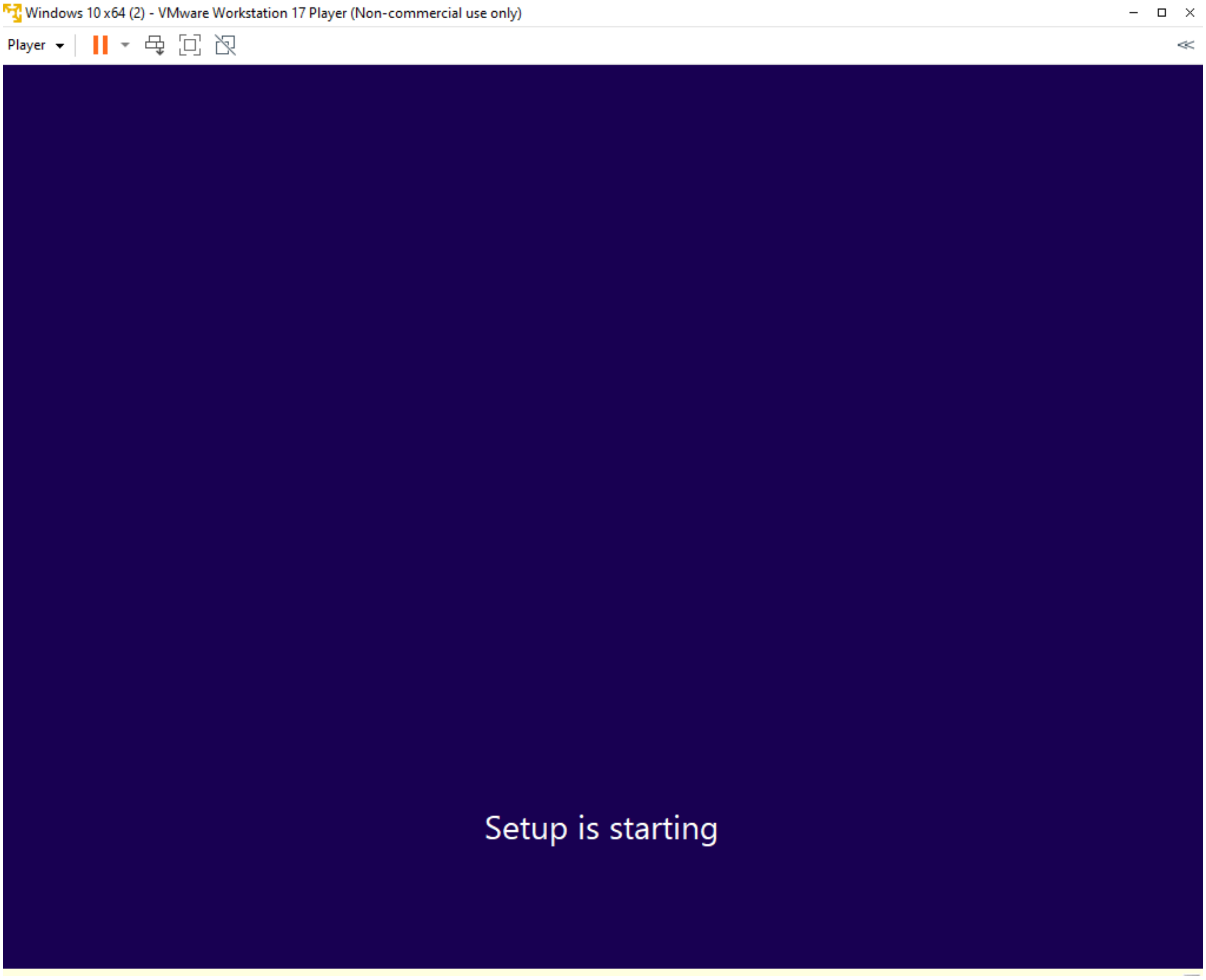
13.4 GB

🟩 Recommended memory

2 GB

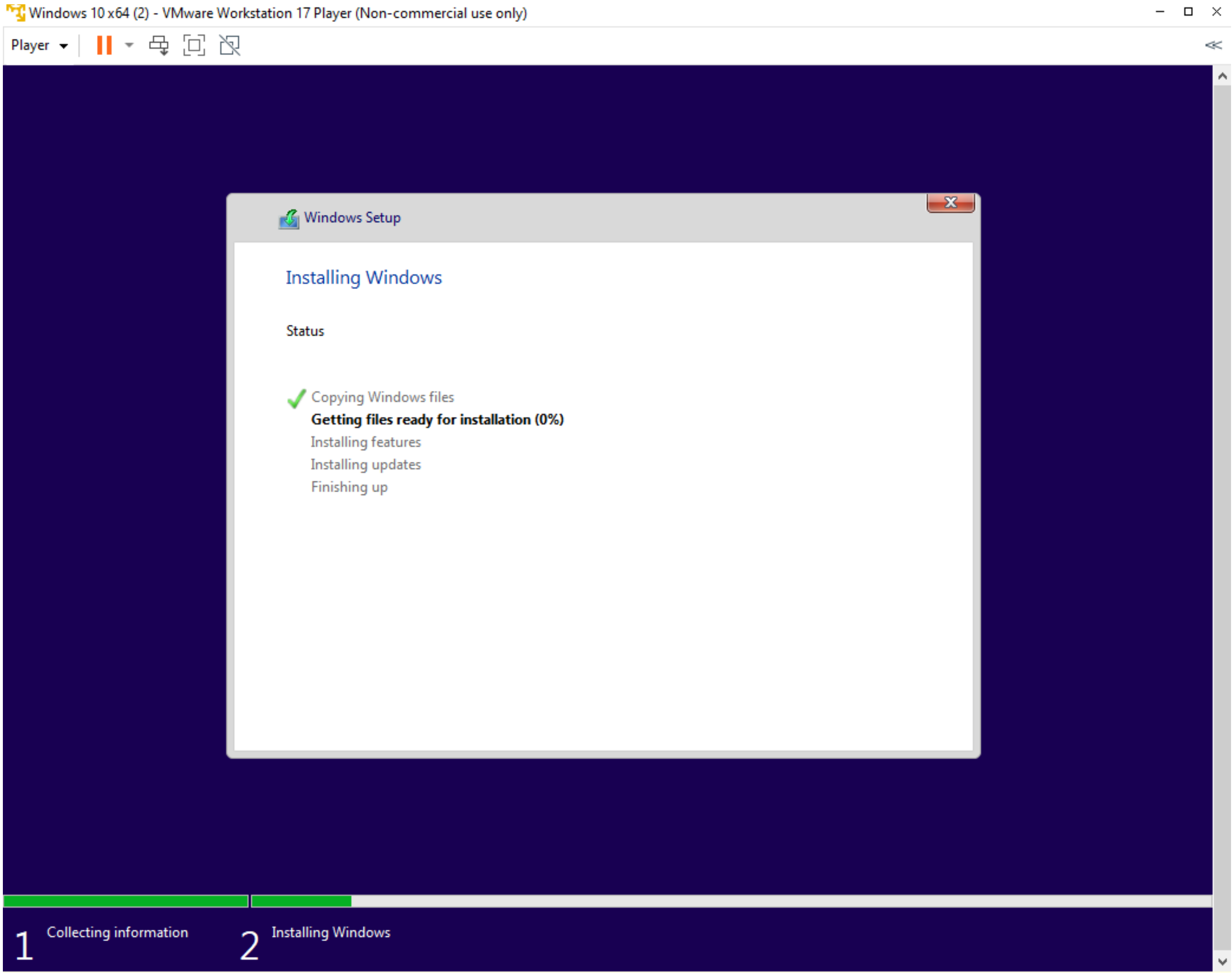
🟨 Guest OS recommended minimum

2 GB



Windows 10 x64 (2) - VMware Workstation 17 Player (Non-commercial use only)
Player

Setup is starting



Windows 10 x64 (2) - VMware Workstation 17 Player (Non-commercial use only)
Player

Installing Windows

Status

✓ Copying Windows files

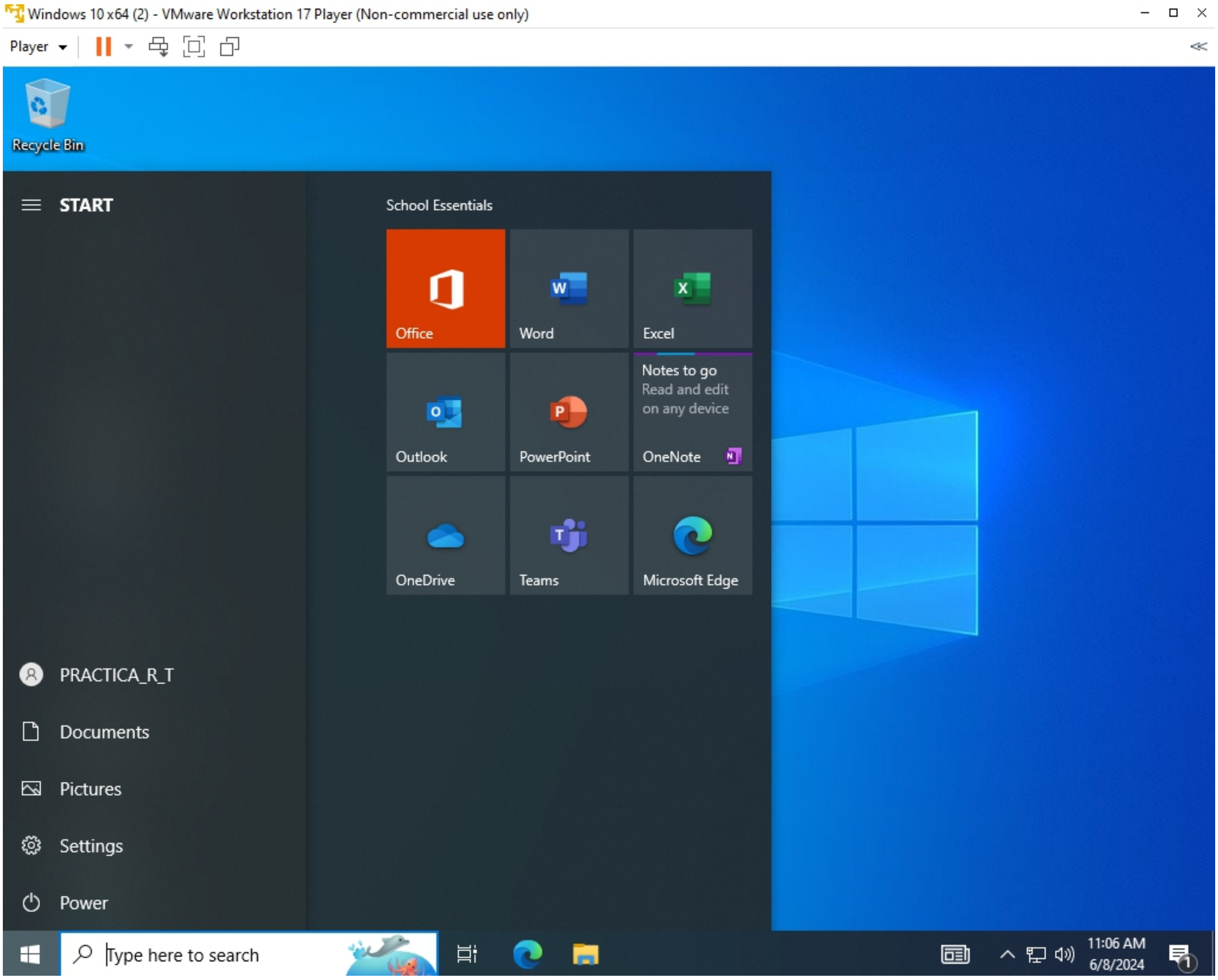
Getting files ready for installation (0%)

Installing features

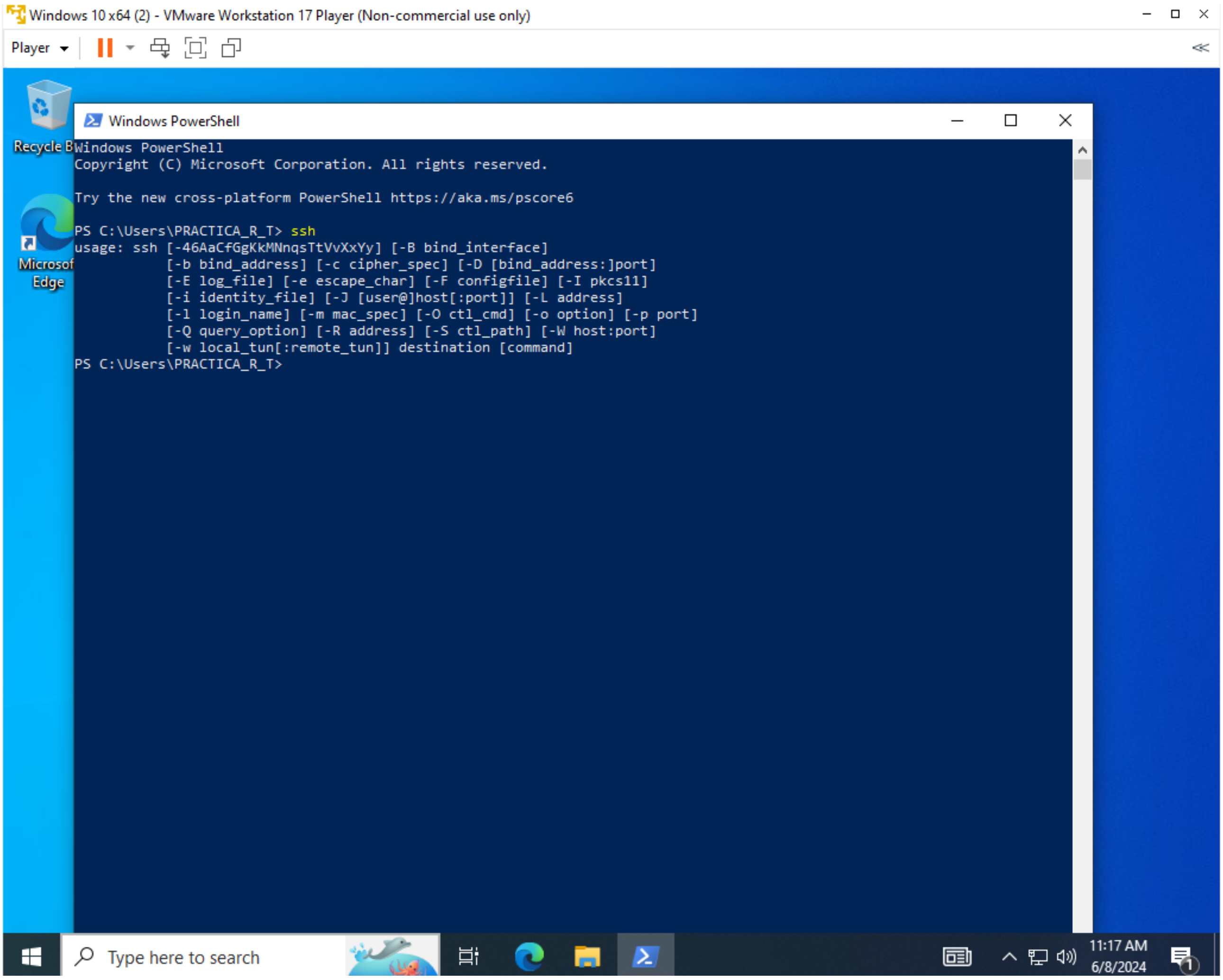
Installing updates

Finishing up

1 Collecting information
2 Installing Windows



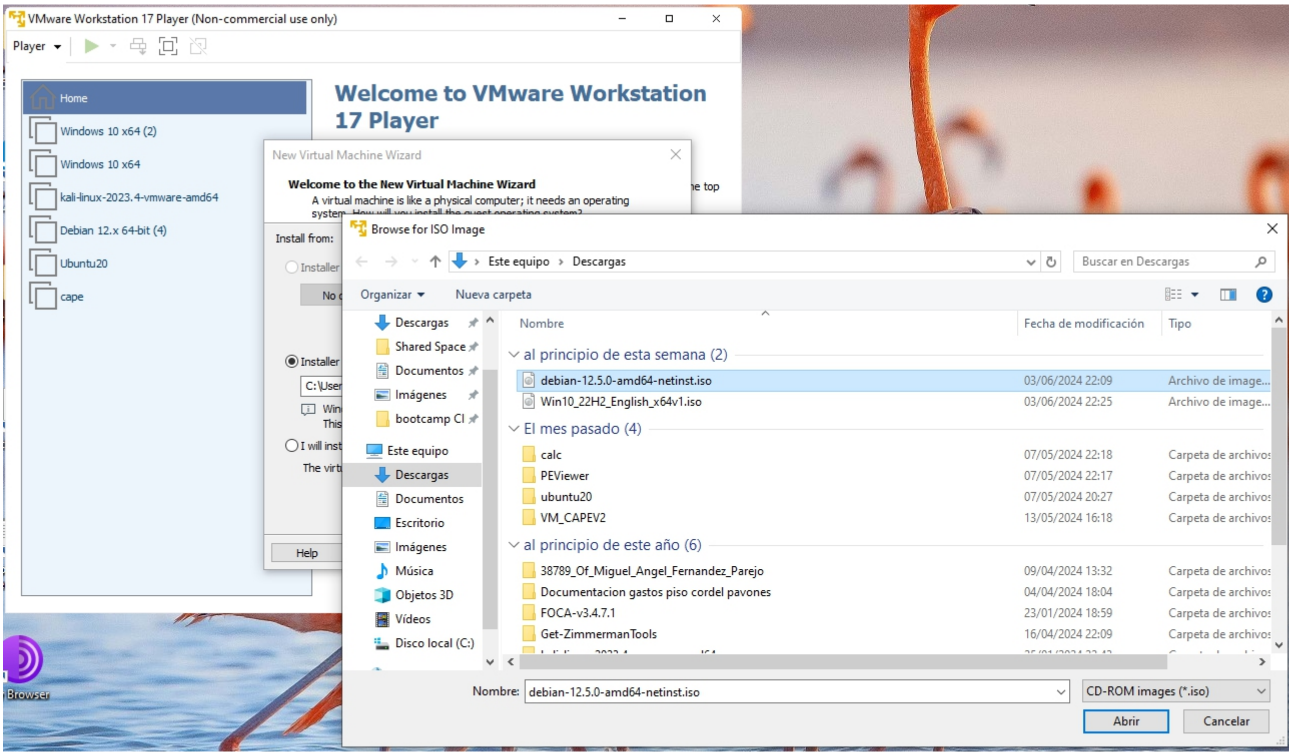
comprobamos el ssh



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\PRACTICA_R_T> ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
PS C:\Users\PRACTICA_R_T>
```

Máquina Linux (Debian C&C)

Creo nueva MV eligiendo la .iso Debian:



Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer

● Installer C:\User

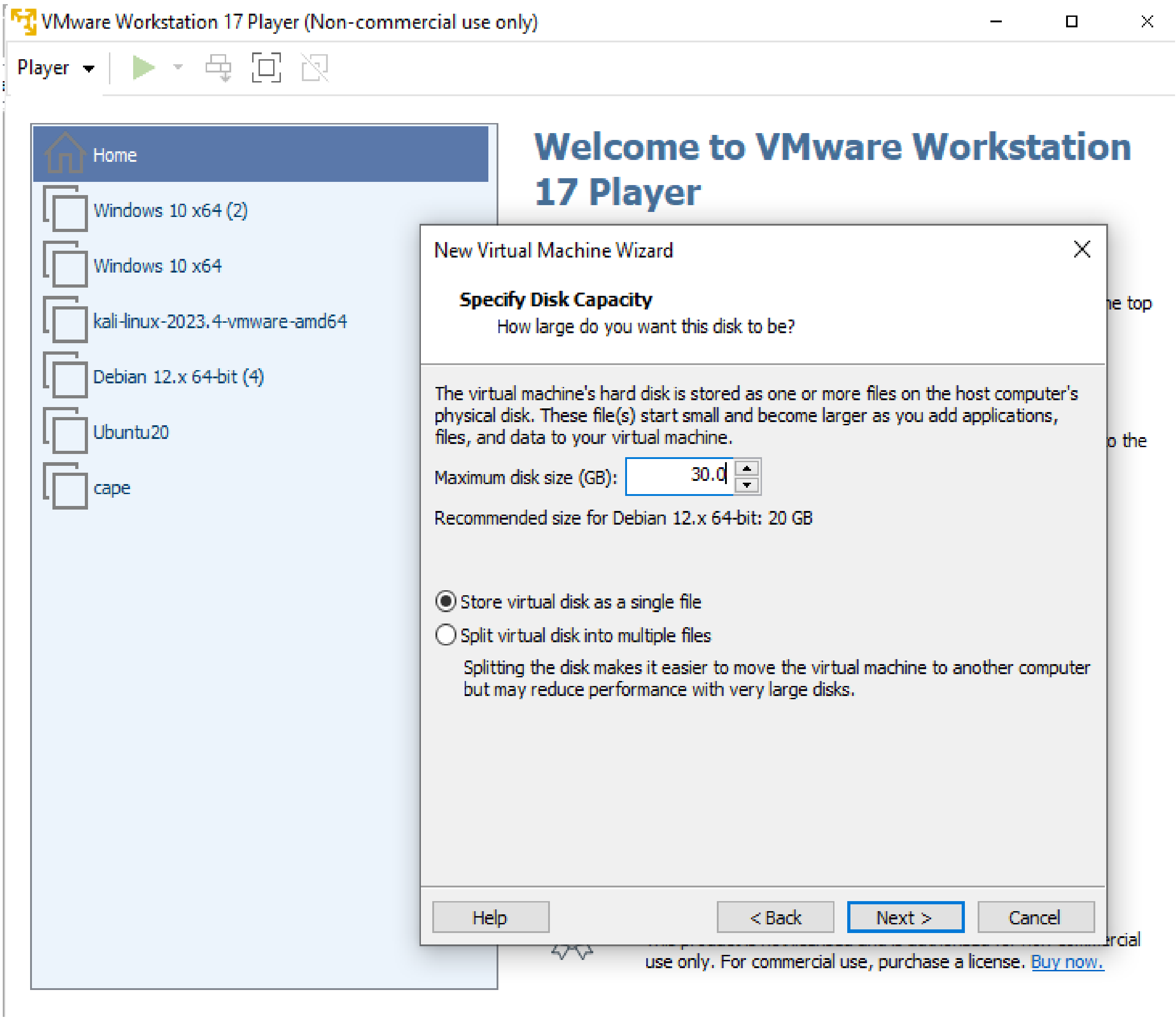
○ I will inst

Nombre	Fecha de modificación	Tipo
al principio de esta semana (2)		
debian-12.5.0-amd64-netinst.iso	03/06/2024 22:09	Archivo de image...
Win10_22H2_English_x64v1.iso	03/06/2024 22:25	Archivo de image...
El mes pasado (4)		
calc	07/05/2024 22:18	Carpeta de archivos
PEViewer	07/05/2024 22:17	Carpeta de archivos
ubuntu20	07/05/2024 20:27	Carpeta de archivos
VM_CAPEV2	13/05/2024 16:18	Carpeta de archivos
al principio de este año (6)		
38789_Of_Miguel_Angel_Fernandez_Parejo	09/04/2024 13:32	Carpeta de archivos
Documentacion gastos piso cordel pavones	04/04/2024 18:04	Carpeta de archivos
FOCA-v3.4.7.1	23/01/2024 18:59	Carpeta de archivos
Get-ZimmermanTools	16/04/2024 22:09	Carpeta de archivos

Nombre: debian-12.5.0-amd64-netinst.iso

CD-ROM images (*.iso)

Dejo 30 GB de tamaño de disco y selecciono la opción Store virtual disk as single file, (disco virtual como un solo archivo)



VMware Workstation 17 Player (Non-commercial use only)
Player
Home
Windows 10 x64 (2)
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Debian 12.x 64-bit (4)
Ubuntu20
cape
Welcome to VMware Workstation 17 Player
ne top
o the
use only. For commercial use, purchase a license. Buy now.

New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 30.0

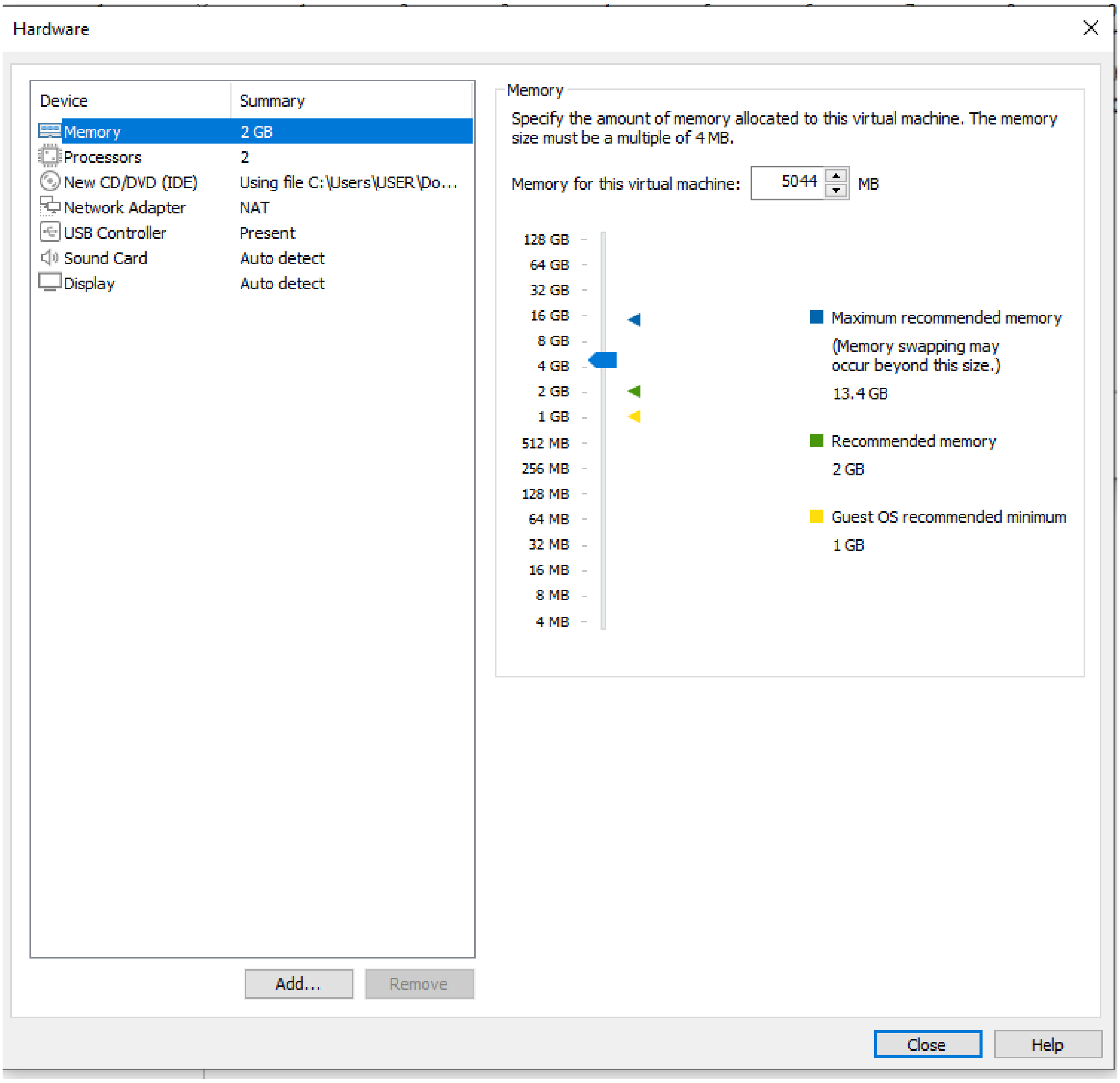
Recommended size for Debian 12.x 64-bit: 20 GB

● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

le pongo 5GB de memoria RAM



Hardware

Device	Summary
Memory	2 GB
Processors	2
New CD/DVD (IDE)	Using file C:\Users\USER\Do...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 5044 MB

🟦 Maximum recommended memory

(Memory swapping may occur beyond this size.)

13.4 GB

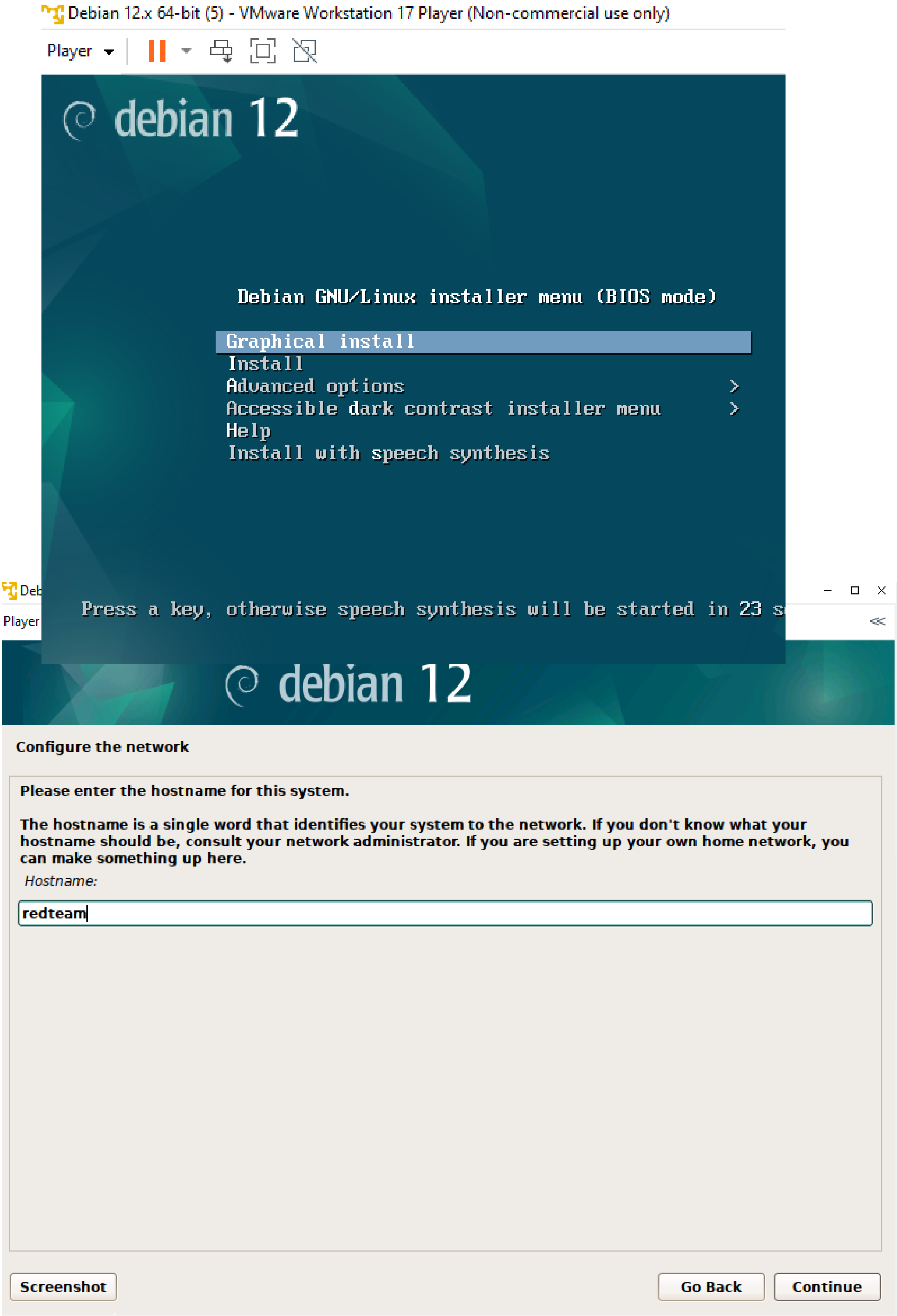
🟩 Recommended memory

2 GB

🟨 Guest OS recommended minimum

1 GB

selecciono Graphical install y le pongo nombre de root readteam:



Debian 12.x 64-bit (5) - VMware Workstation 17 Player (Non-commercial use only)

Debian GNU/Linux installer menu (BIOS mode)

- Graphical install
- Install
- Advanced options >
- Accessible dark contrast installer menu >
- Help
- Install with speech synthesis

Press a key, otherwise speech synthesis will be started in 23 s

Configure the network

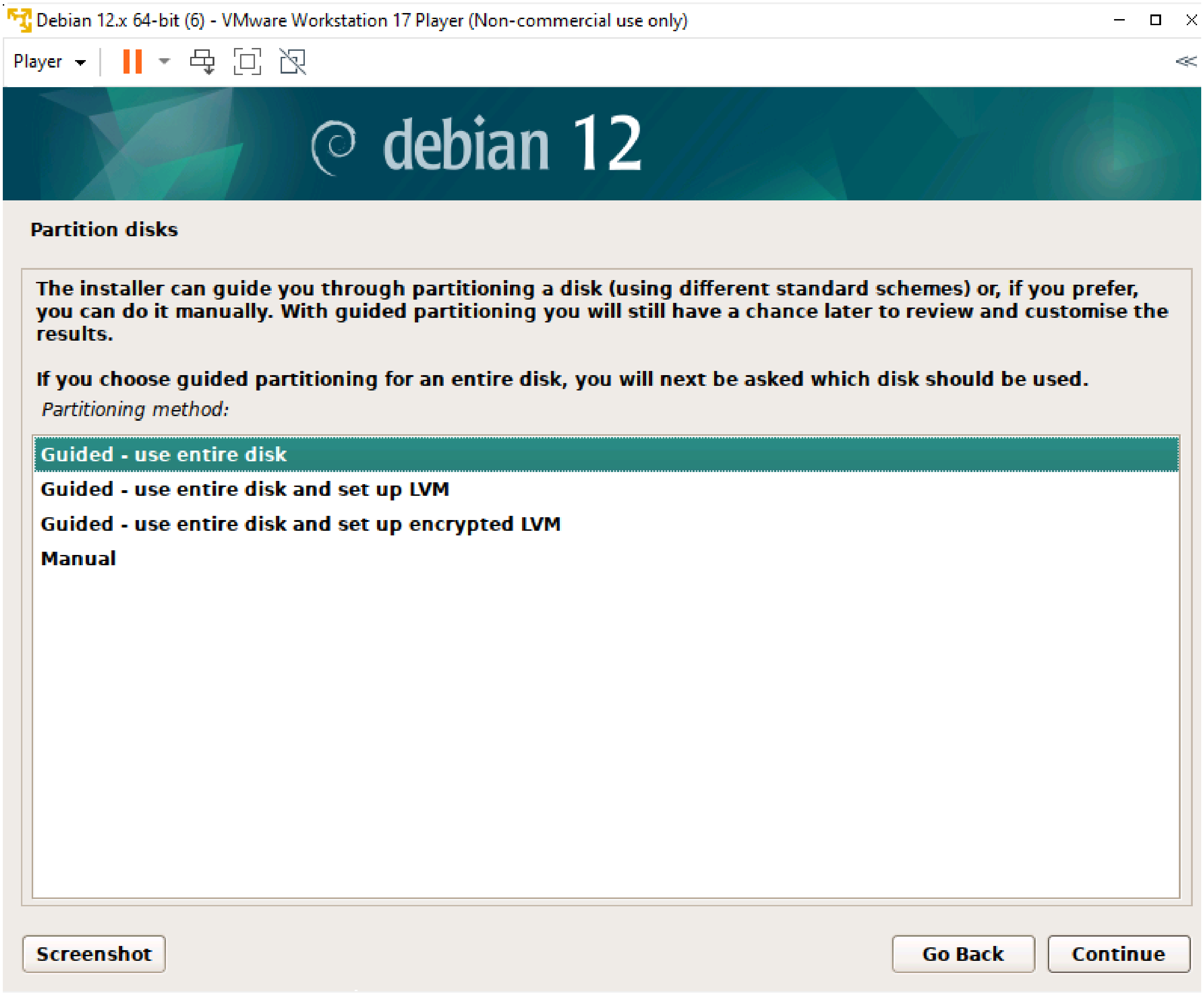
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

redteam

selecciono la primera opción “usar el disco completo”


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Partition disks

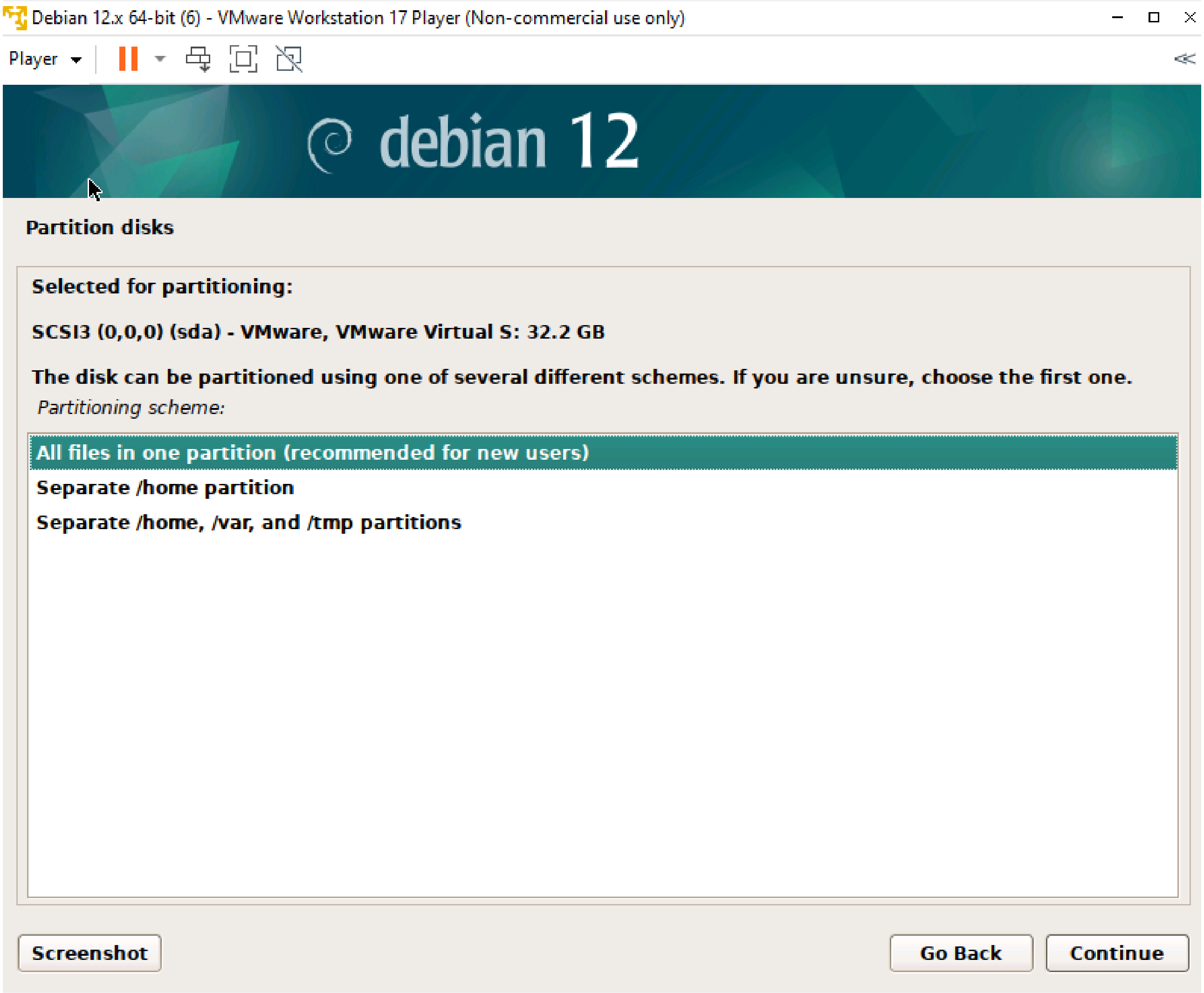
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

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

Selecciono la primera opción. Todos los ficheros en una partición


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Partition disks

Selected for partitioning:

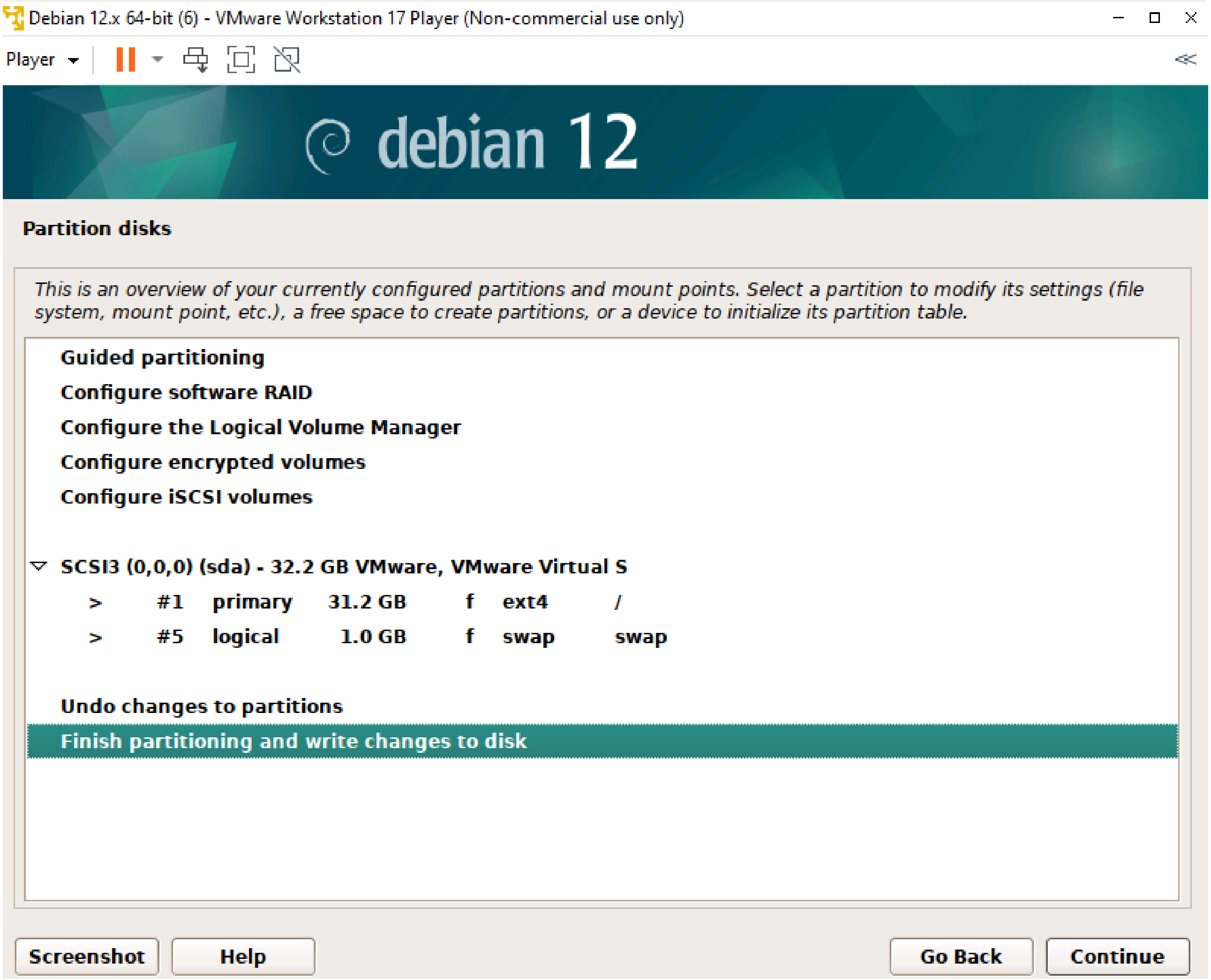
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 32.2 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

- All files in one partition (recommended for new users)
- Separate /home partition
- Separate /home, /var, and /tmp partitions

Screenshot
Go Back
Continue

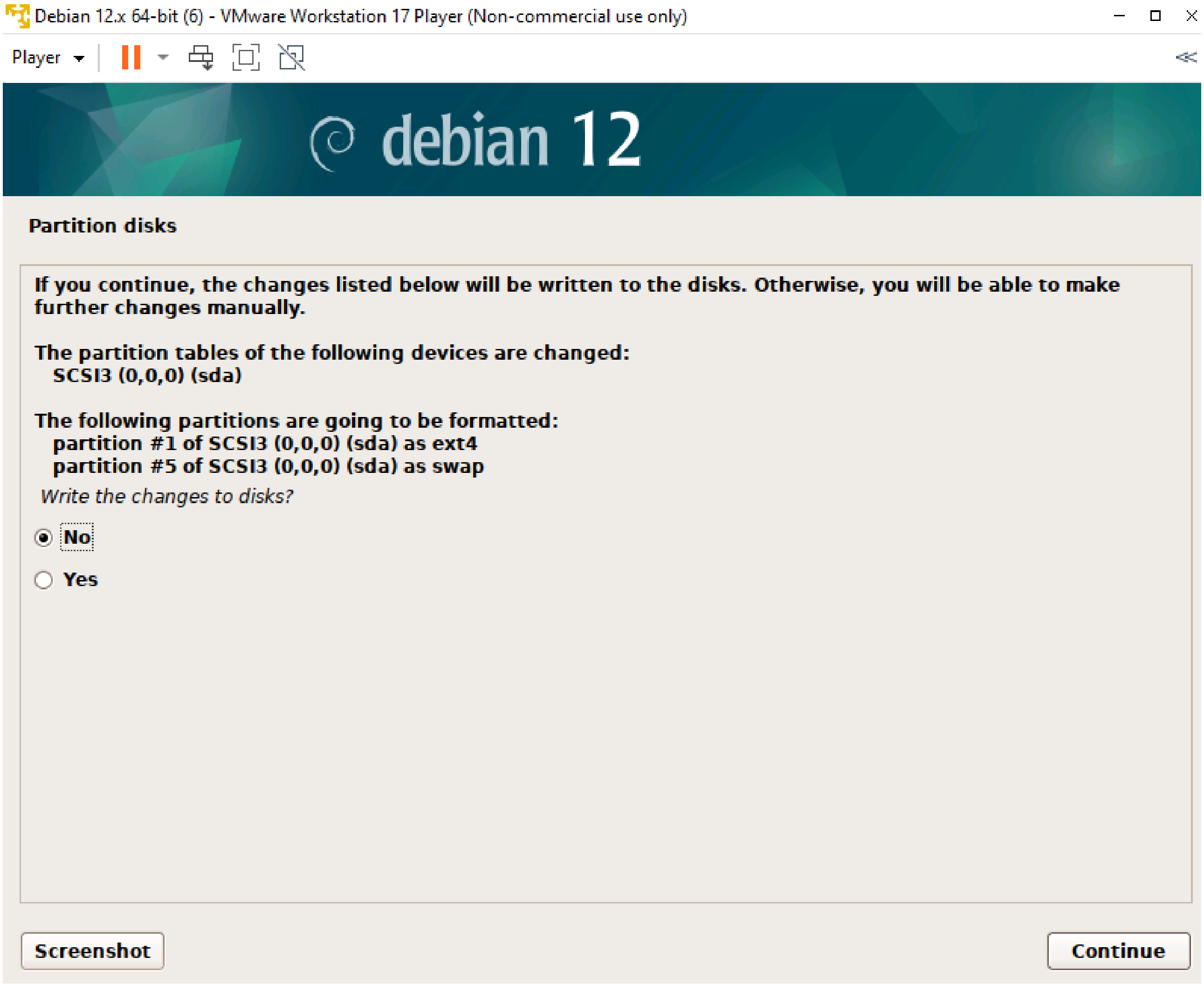

Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

```
    Guided partitioning
    Configure software RAID
    Configure the Logical Volume Manager
    Configure encrypted volumes
    Configure iSCSI volumes

▽  SCSI3 (0,0,0) (sda) - 32.2 GB VMware, VMware Virtual S
        >     #1   primary   31.2 GB     f   ext4      /
        >     #5   logical    1.0 GB     f   swap      swap

    Undo changes to partitions
    Finish partitioning and write changes to disk
```

Selecciono Sí en Escribir los cambios a disco



Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
  SCSI3 (0,0,0) (sda)

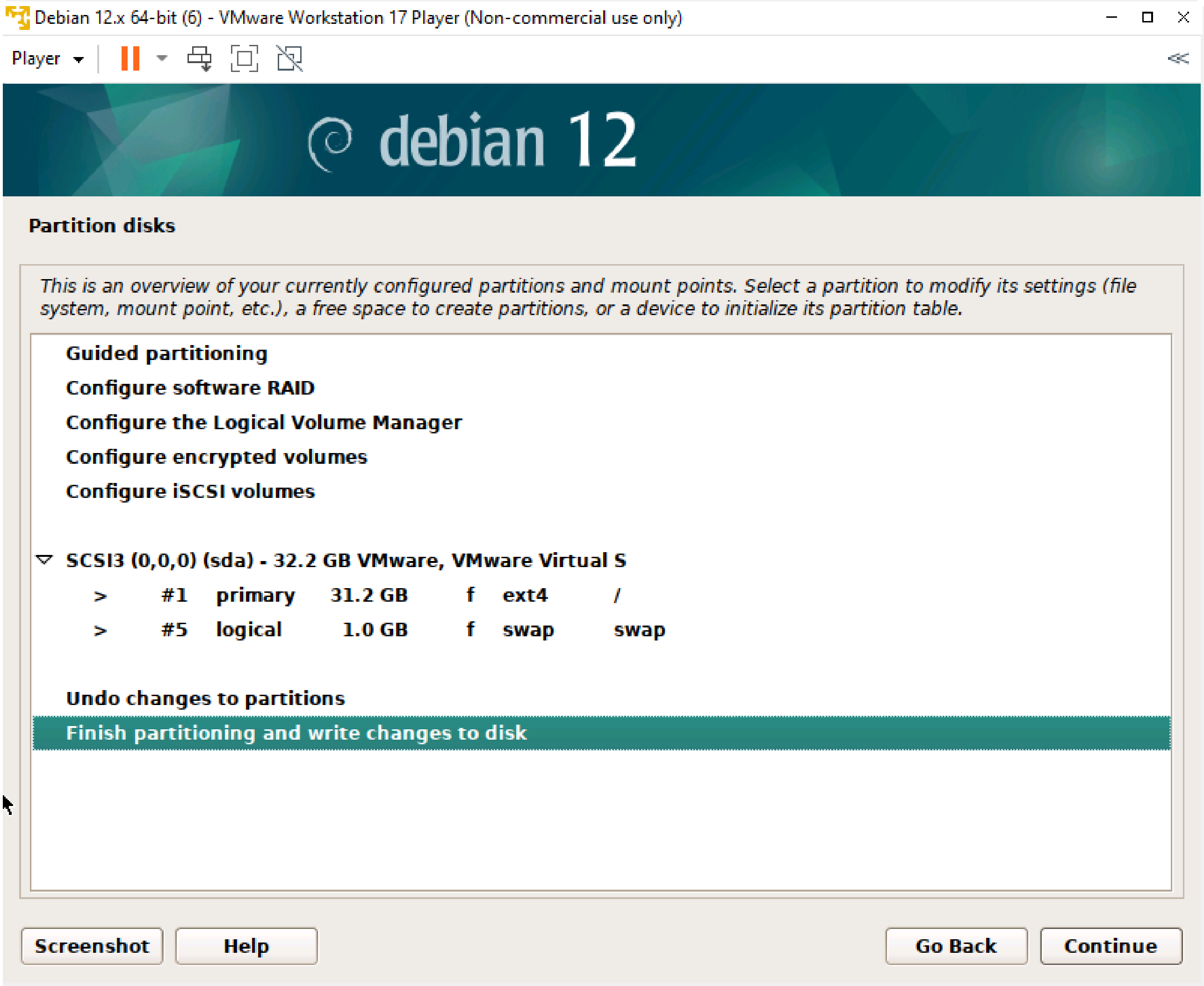
The following partitions are going to be formatted:
  partition #1 of SCSI3 (0,0,0) (sda) as ext4
  partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

● No

○ Yes

Finalizo la partición

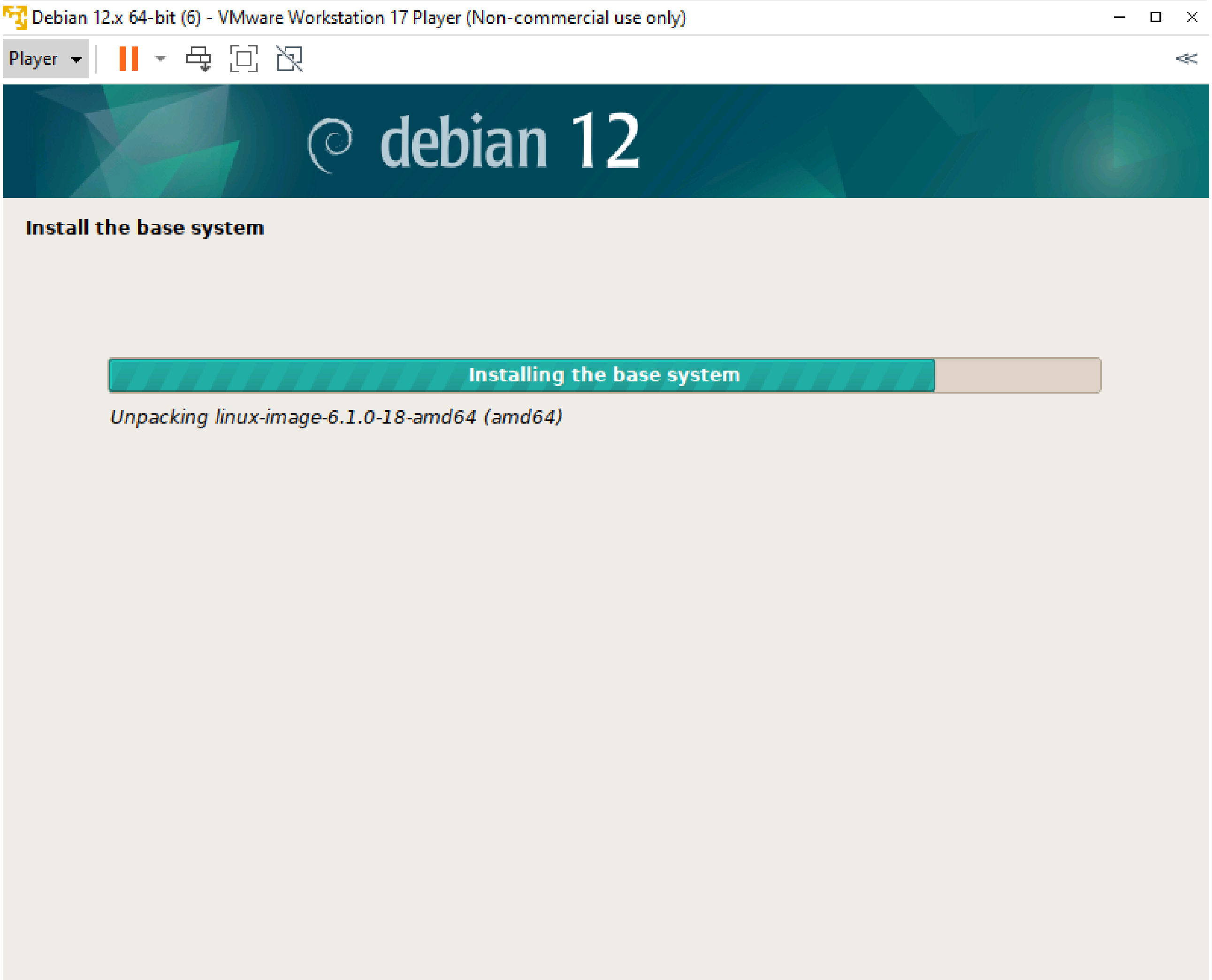


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 32.2 GB VMware, VMware Virtual S
     >     #1   primary    31.2 GB    f   ext4     /
     >     #5   logical     1.0 GB    f   swap     swap

Undo changes to partitions
Finish partitioning and write changes to disk
```



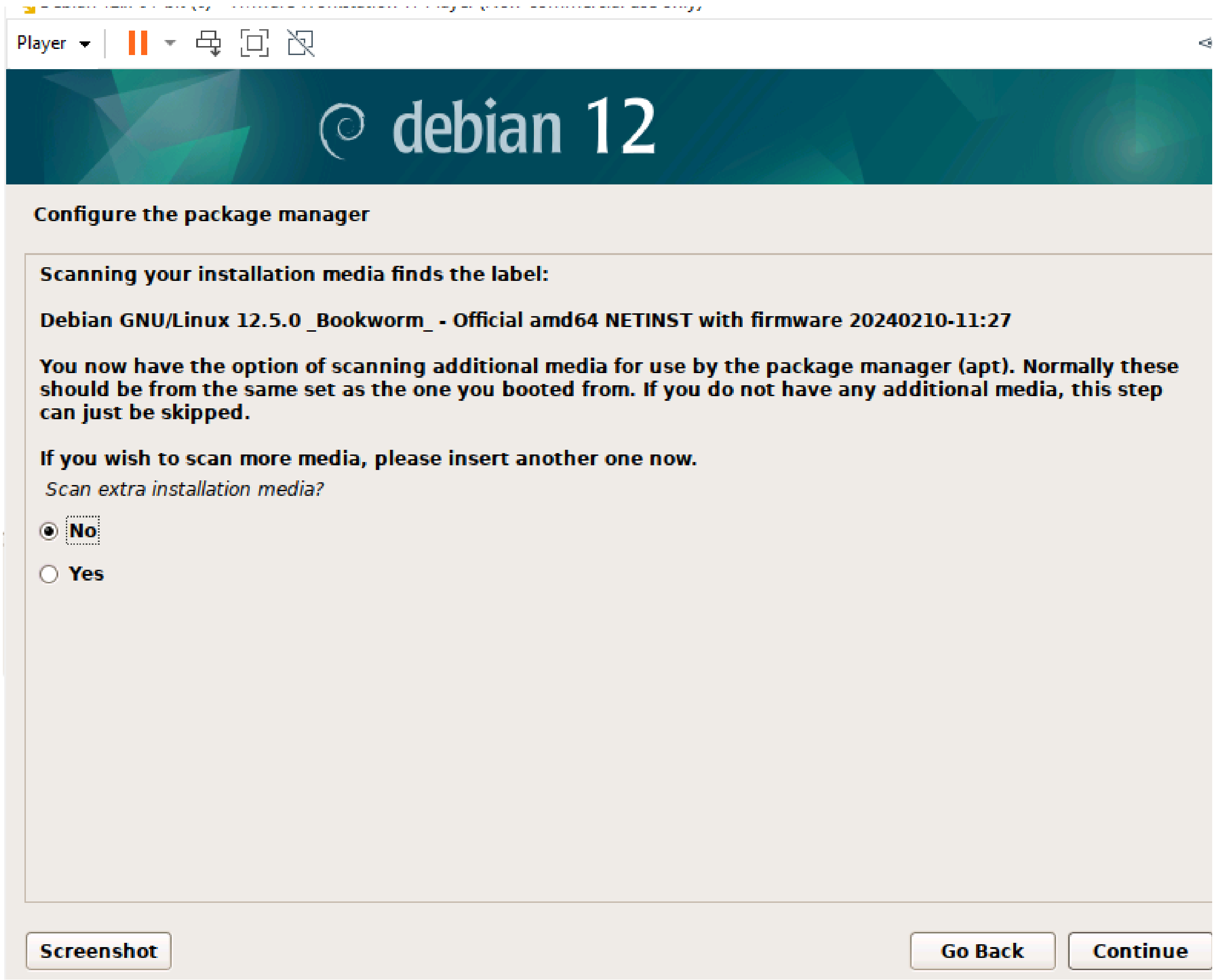
Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Install the base system

Installing the base system

Unpacking linux-image-6.1.0-18-amd64 (amd64)

Selecciono No escaneo medios



Configure the package manager

Scanning your installation media finds the label:

Debian GNU/Linux 12.5.0 _Bookworm_ - Official amd64 NETINST with firmware 20240210-11:27

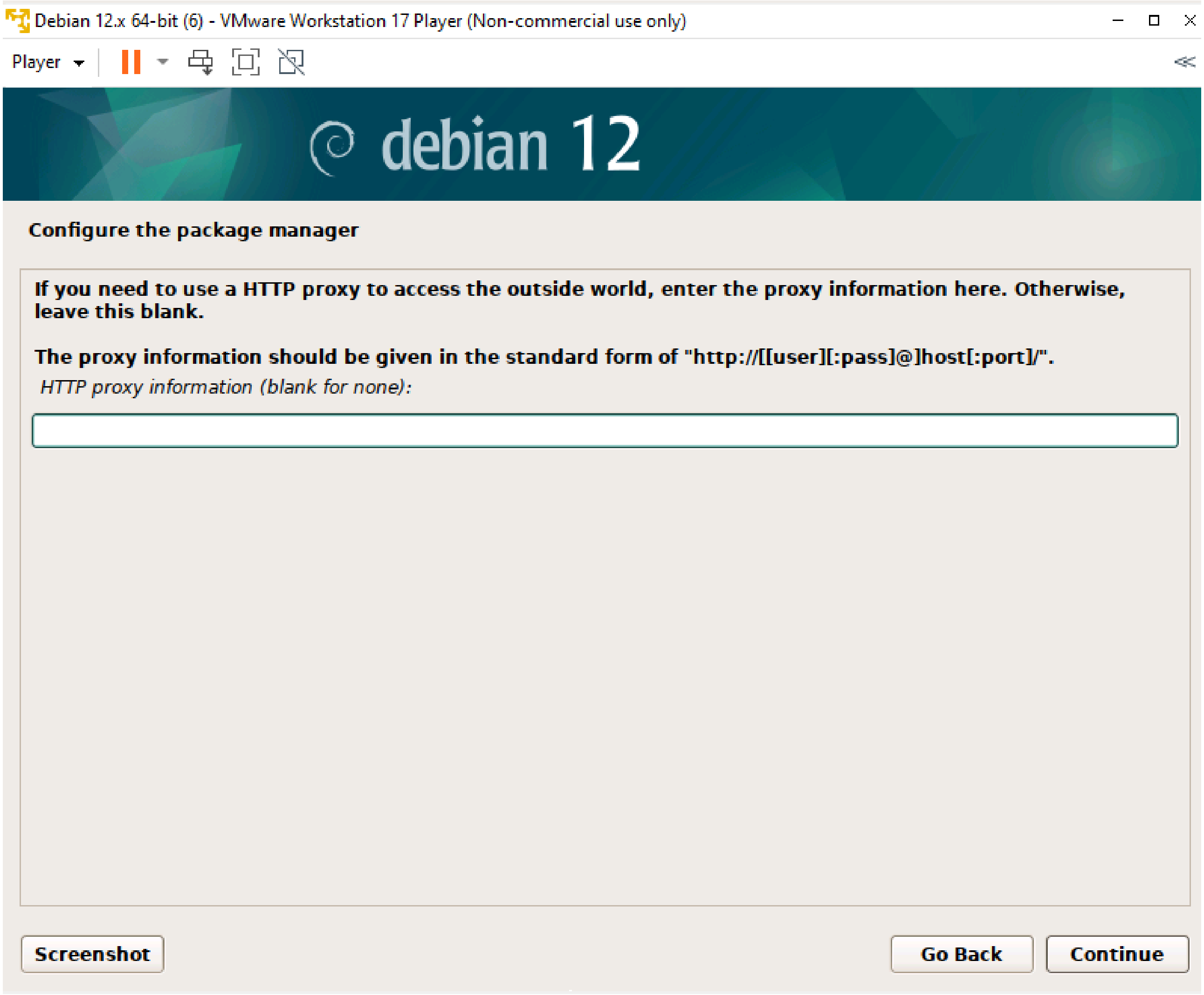
You now have the option of scanning additional media for use by the package manager (apt). Normally these should be from the same set as the one you booted from. If you do not have any additional media, this step can just be skipped.

If you wish to scan more media, please insert another one now.

Scan extra installation media?

● No

○ Yes



Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

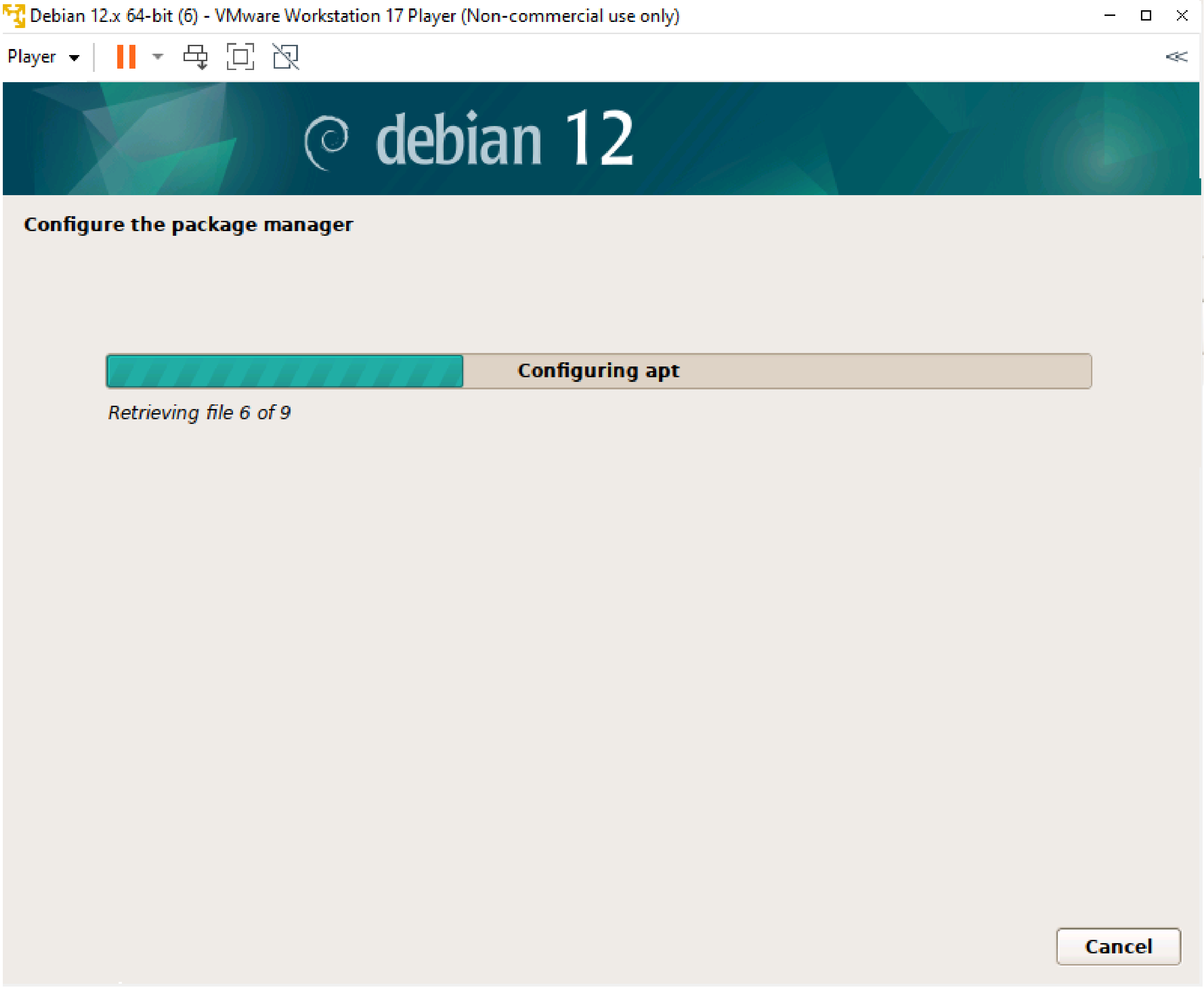
Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

Screenshot
Go Back
Continue

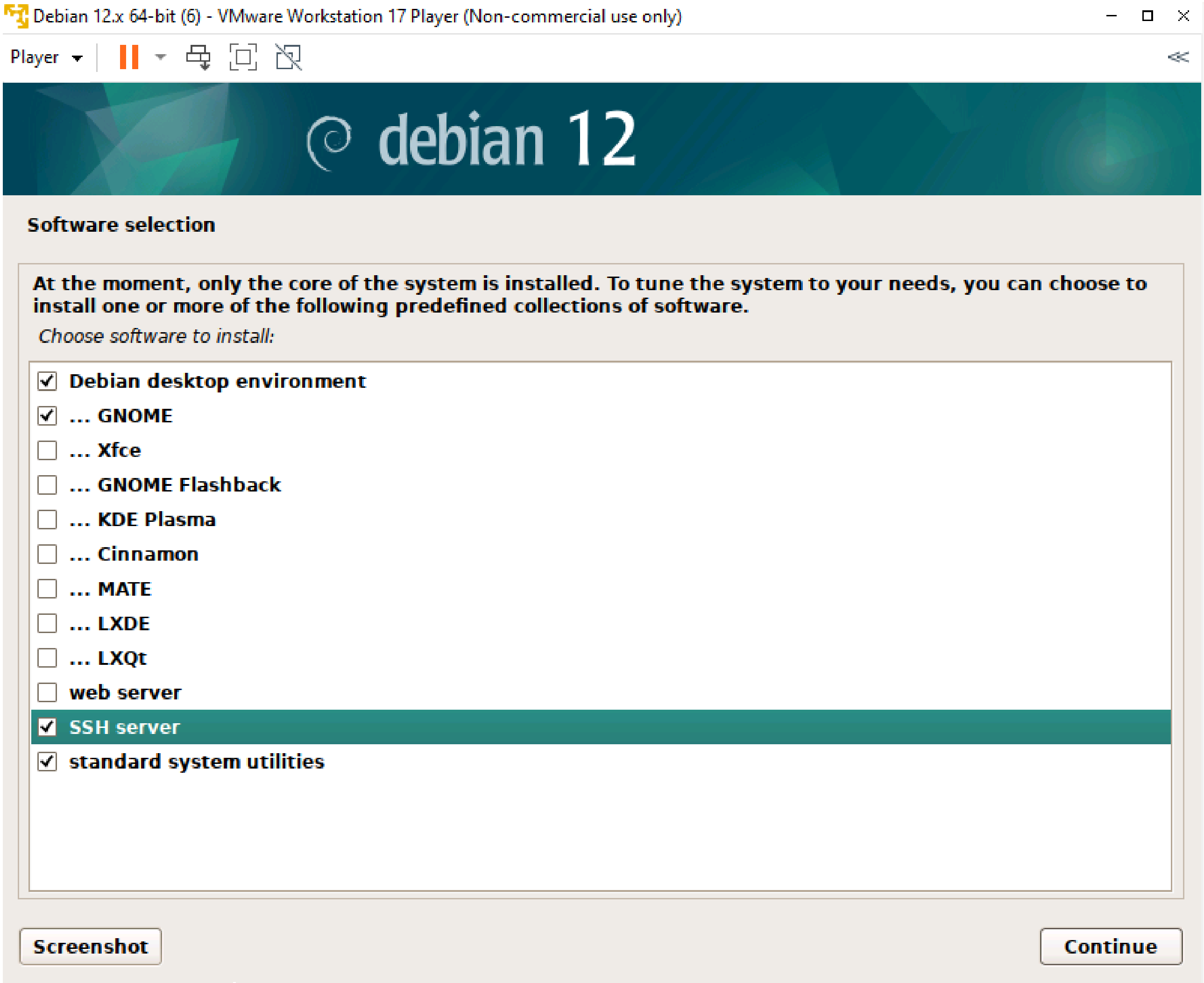

Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Configure the package manager

Configuring apt

Retrieving file 6 of 9

selecciono la opción del ssh server, para instalar el servicio ssh



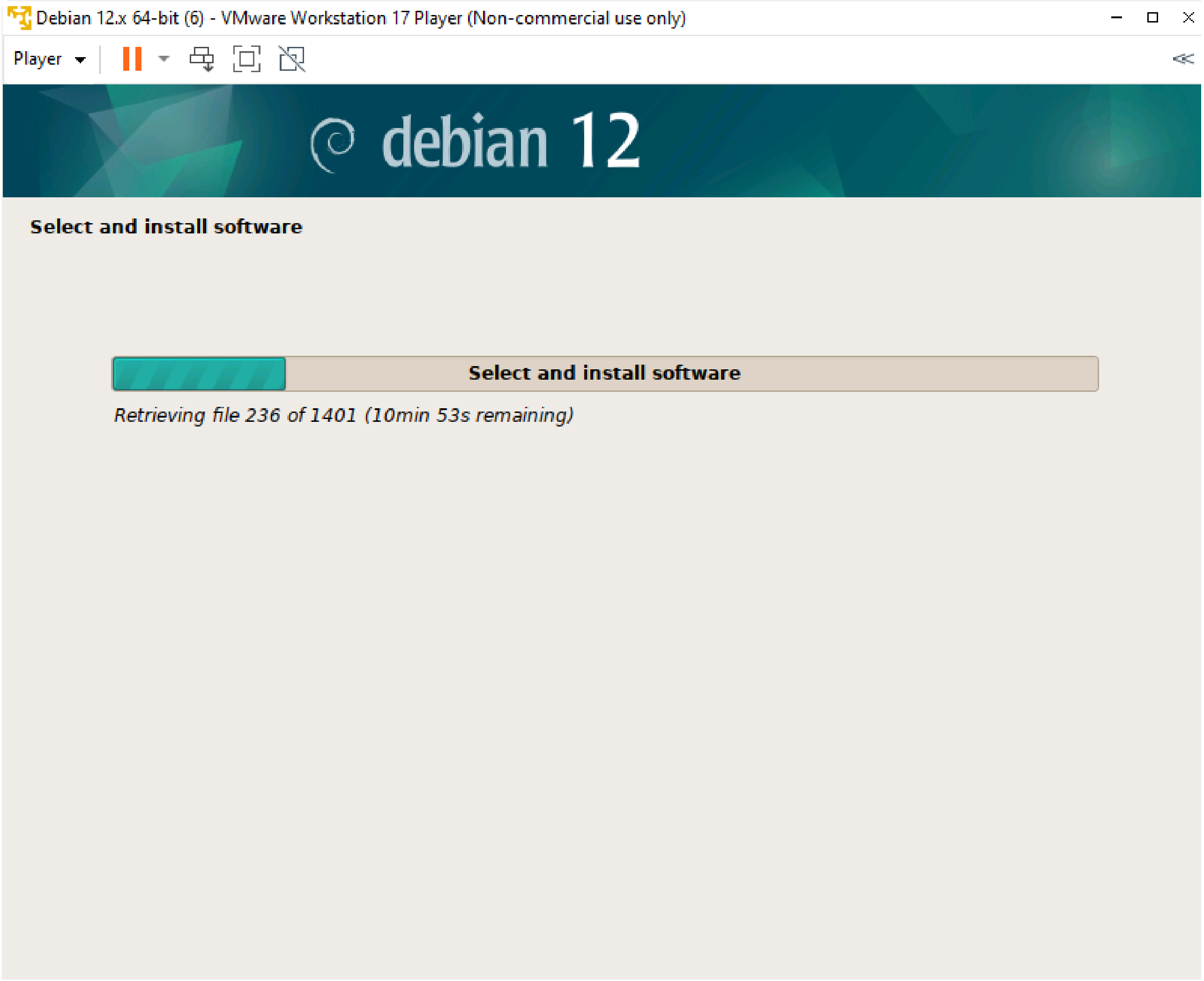
Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Software selection

At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.

Choose software to install:

☑ Debian desktop environment
☑ ... GNOME
☐ ... Xfce
☐ ... GNOME Flashback
☐ ... KDE Plasma
☐ ... Cinnamon
☐ ... MATE
☐ ... LXDE
☐ ... LXQt
☐ web server
☑ SSH server
☑ standard system utilities

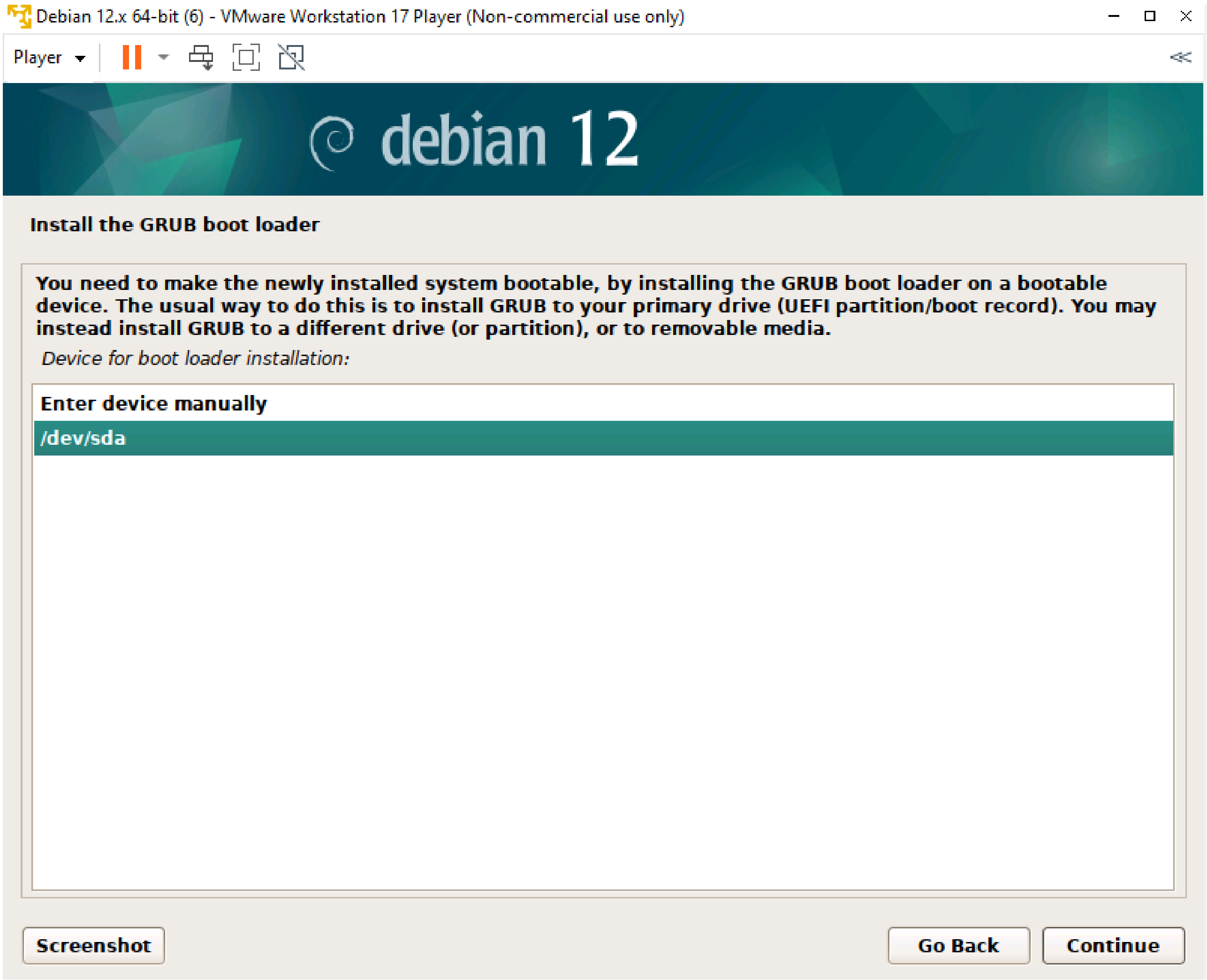


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Select and install software

Select and install software

Retrieving file 236 of 1401 (10min 53s remaining) selecciono el dispositivo de arranque /dev/sda



Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Install the GRUB boot loader

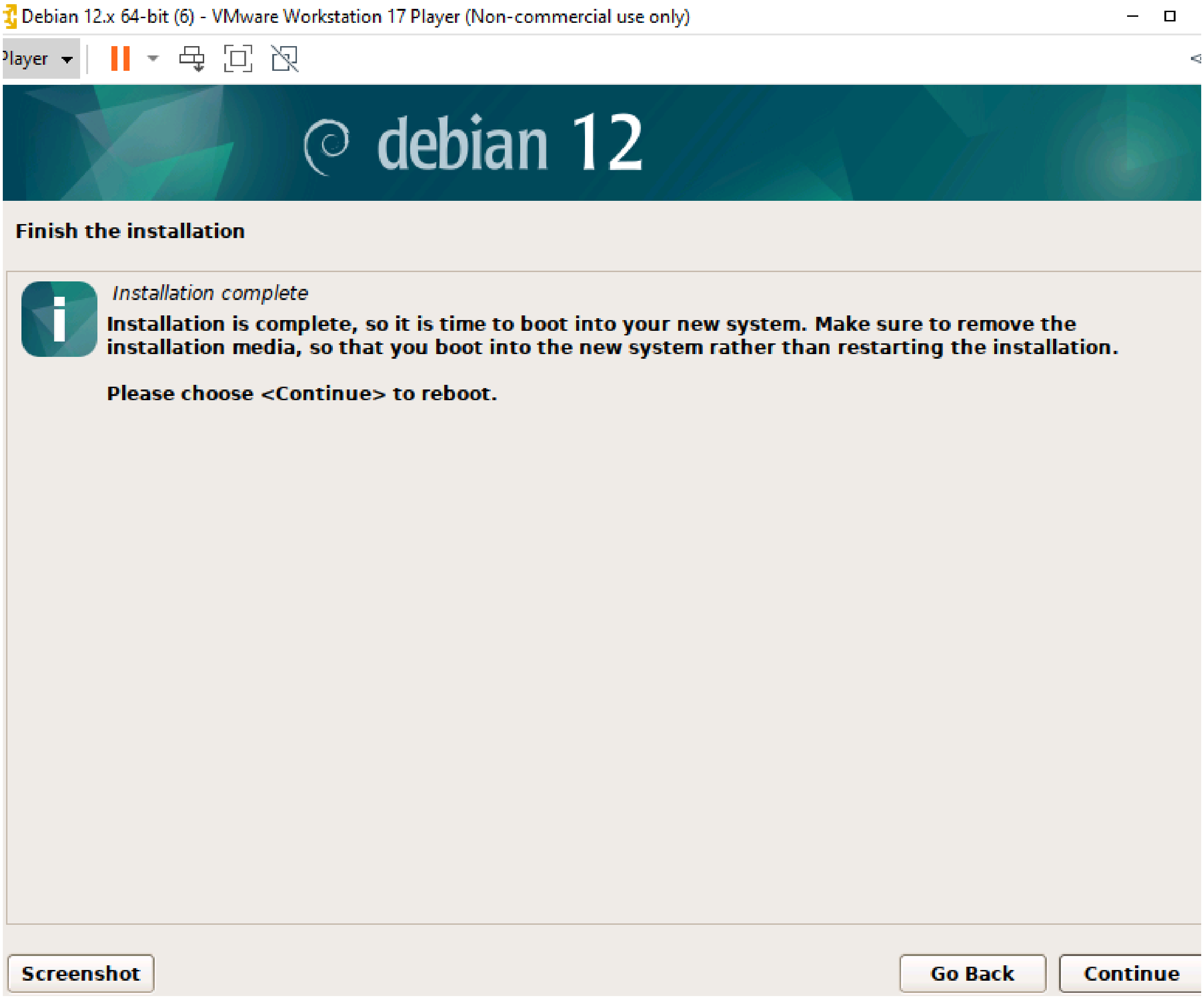
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

Device for boot loader installation:

Enter device manually

/dev/sda

Hago click en continue para reiniciar el debian


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12
Screenshot
Go Back
Continue

Finish the installation

Installation complete

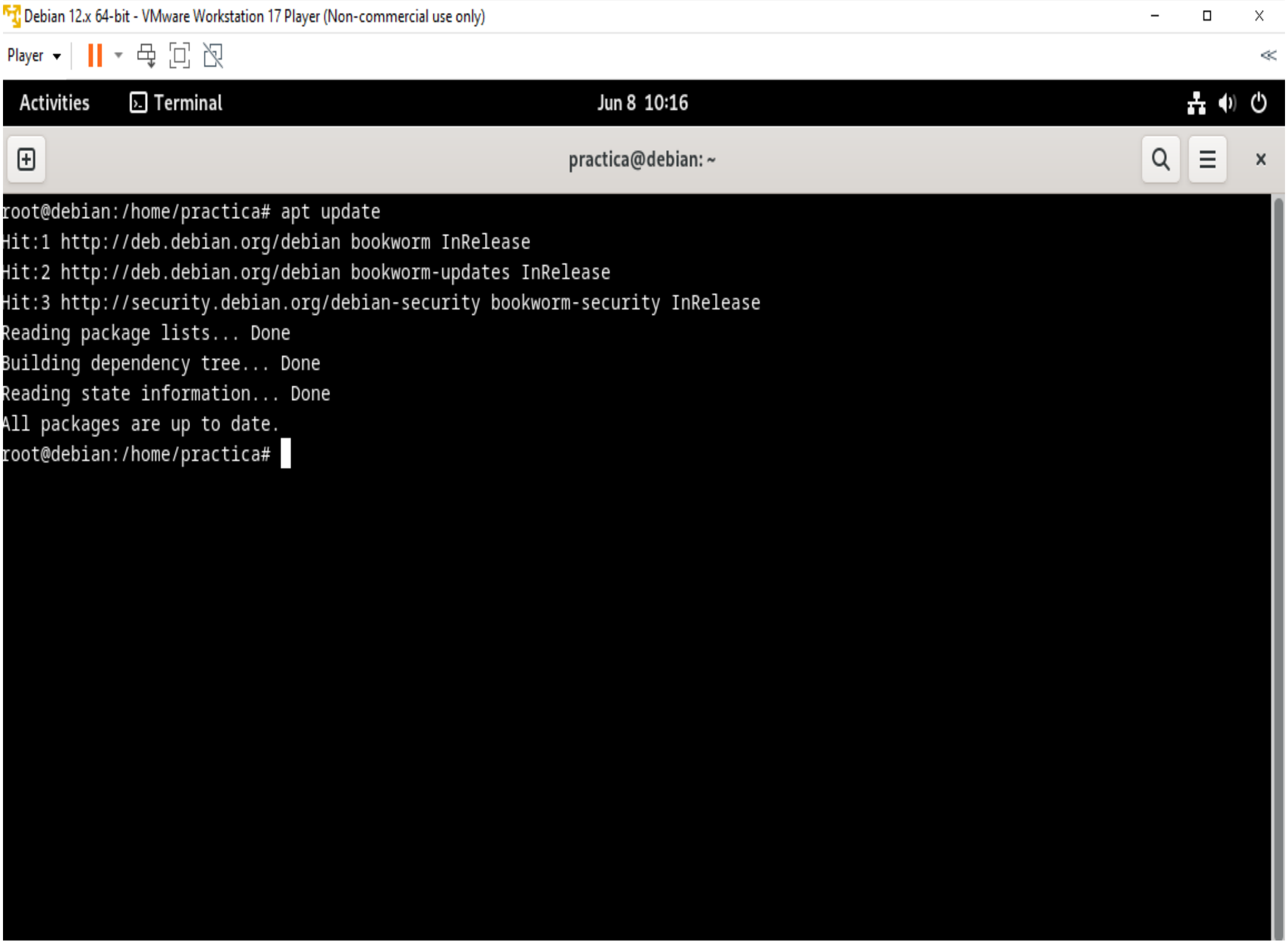
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

Please choose <Continue> to reboot.

Instalación y configuración de herramientas, para la comunicación entre las dos máquinas, Debian y Windows:

Escribo en la línea de comandos de Debian, para actualizarlo:

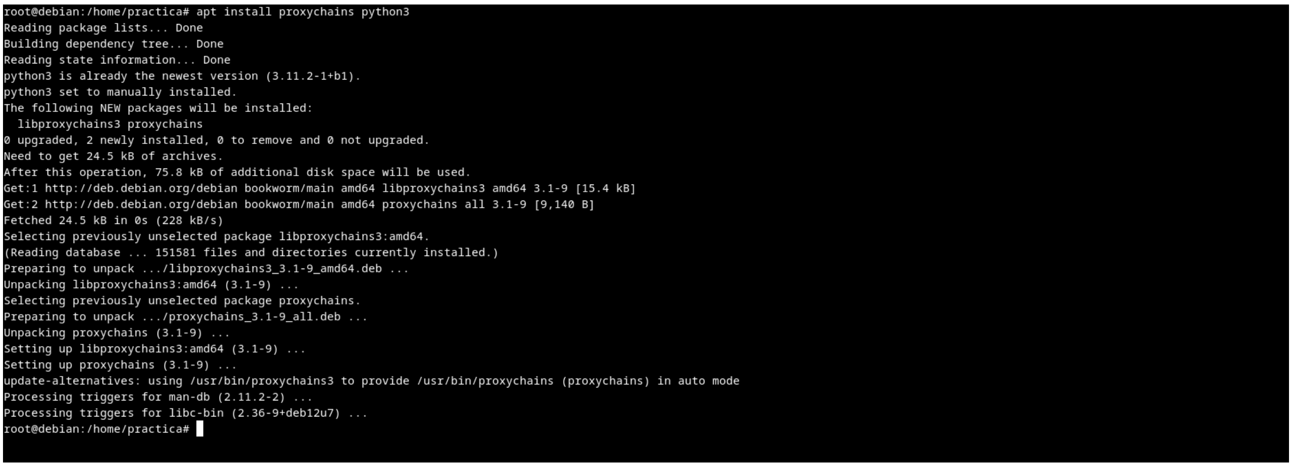
apt update


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Jun 8 10:16
practica@debian: ~

```
root@debian:/home/practica# apt update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian bookworm-updates InRelease
Hit:3 http://security.debian.org/debian-security bookworm-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
root@debian:/home/practica#
```

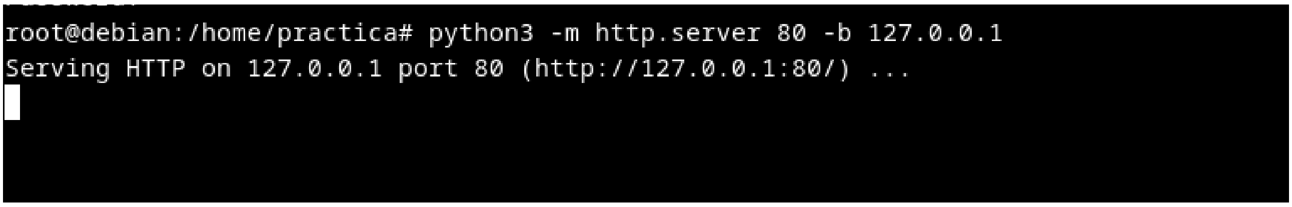
Instalo proxychains y python3

apt proxychains python3



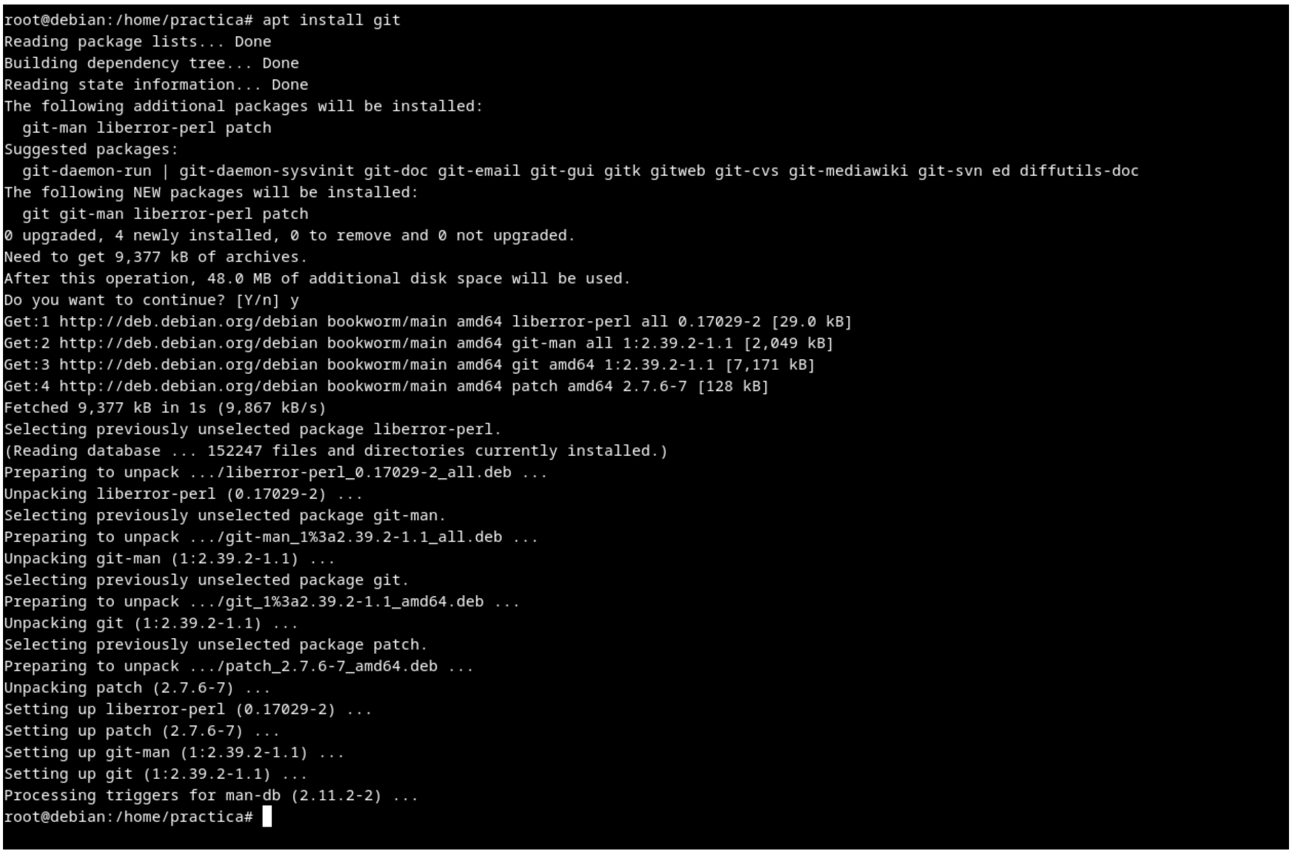
```
root@debian:/home/practica# apt install proxychains python3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.11.2-1+b1).
python3 set to manually installed.
The following NEW packages will be installed:
  libproxychains3 proxychains
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 24.5 kB of archives.
After this operation, 75.8 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 libproxychains3 amd64 3.1-9 [15.4 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 proxychains all 3.1-9 [9,140 B]
Fetched 24.5 kB in 0s (228 kB/s)
Selecting previously unselected package libproxychains3:amd64.
(Reading database ... 151581 files and directories currently installed.)
Preparing to unpack .../libproxychains3_3.1-9_amd64.deb ...
Unpacking libproxychains3:amd64 (3.1-9) ...
Selecting previously unselected package proxychains.
Preparing to unpack .../proxychains_3.1-9_all.deb ...
Unpacking proxychains (3.1-9) ...
Setting up libproxychains3:amd64 (3.1-9) ...
Setting up proxychains (3.1-9) ...
update-alternatives: using /usr/bin/proxychains3 to provide /usr/bin/proxychains (proxychains) in auto mode
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u7) ...
root@debian:/home/practica#
```

ejecuto el comando python3 -m http.server 80 -b 127.0.0.1 para levantar el servidor en localhost



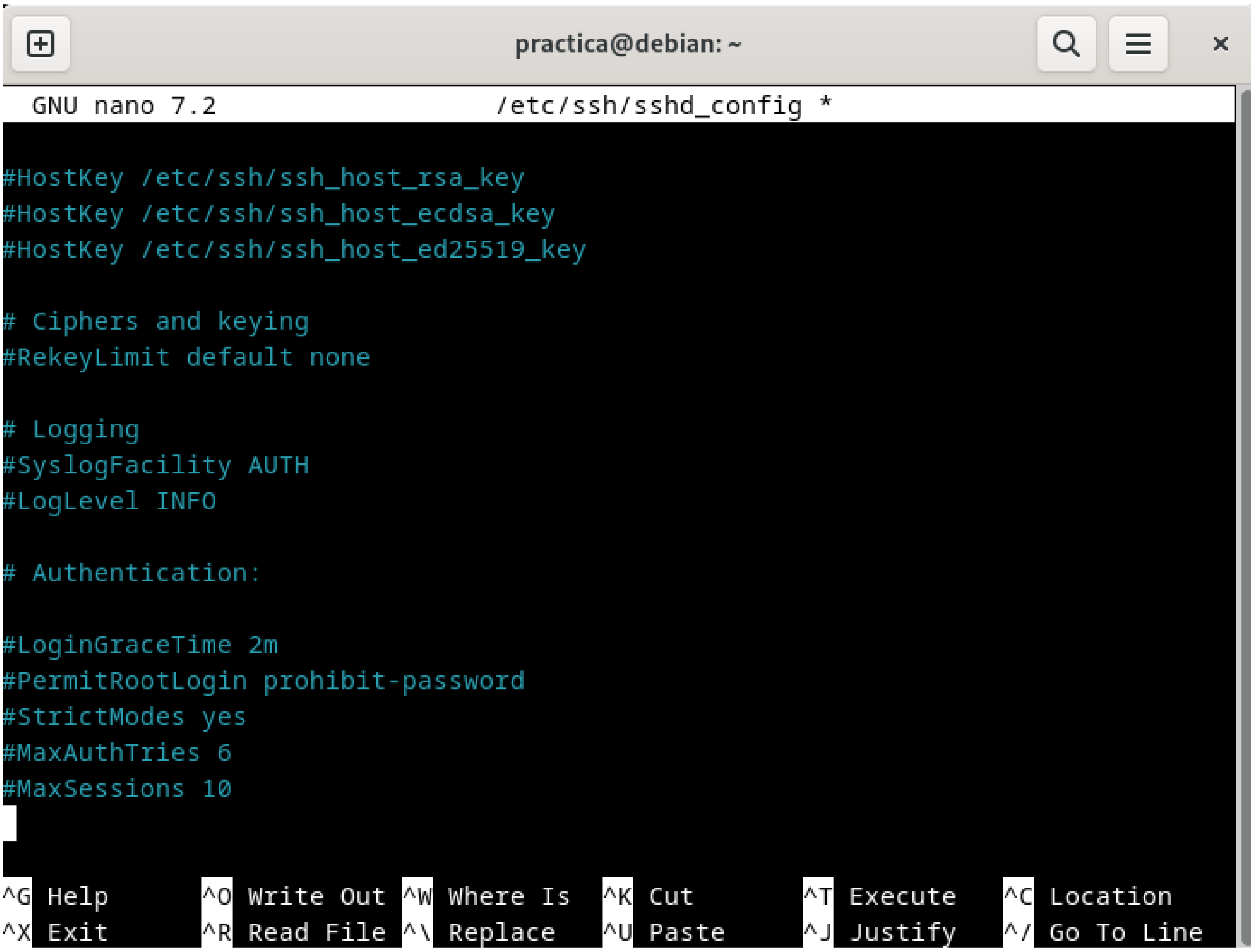
```
root@debian:/home/practica# python3 -m http.server 80 -b 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
```

instalo el git con apt install git



```
root@debian:/home/practica# apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl patch
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn ed diffutils-doc
The following NEW packages will be installed:
  git git-man liberror-perl patch
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 9,377 kB of archives.
After this operation, 48.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bookworm/main amd64 liberror-perl all 0.17029-2 [29.0 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 git-man all 1:2.39.2-1.1 [2,049 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 git amd64 1:2.39.2-1.1 [7,171 kB]
Get:4 http://deb.debian.org/debian bookworm/main amd64 patch amd64 2.7.6-7 [128 kB]
Fetched 9,377 kB in 1s (9,867 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 152247 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-2_all.deb ...
Unpacking liberror-perl (0.17029-2) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.39.2-1.1_all.deb ...
Unpacking git-man (1:2.39.2-1.1) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.39.2-1.1_amd64.deb ...
Unpacking git (1:2.39.2-1.1) ...
Selecting previously unselected package patch.
Preparing to unpack .../patch_2.7.6-7_amd64.deb ...
Unpacking patch (2.7.6-7) ...
Setting up liberror-perl (0.17029-2) ...
Setting up patch (2.7.6-7) ...
Setting up git-man (1:2.39.2-1.1) ...
Setting up git (1:2.39.2-1.1) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:/home/practica# 
```

en la máquina víctima configuro un archivo de ssh

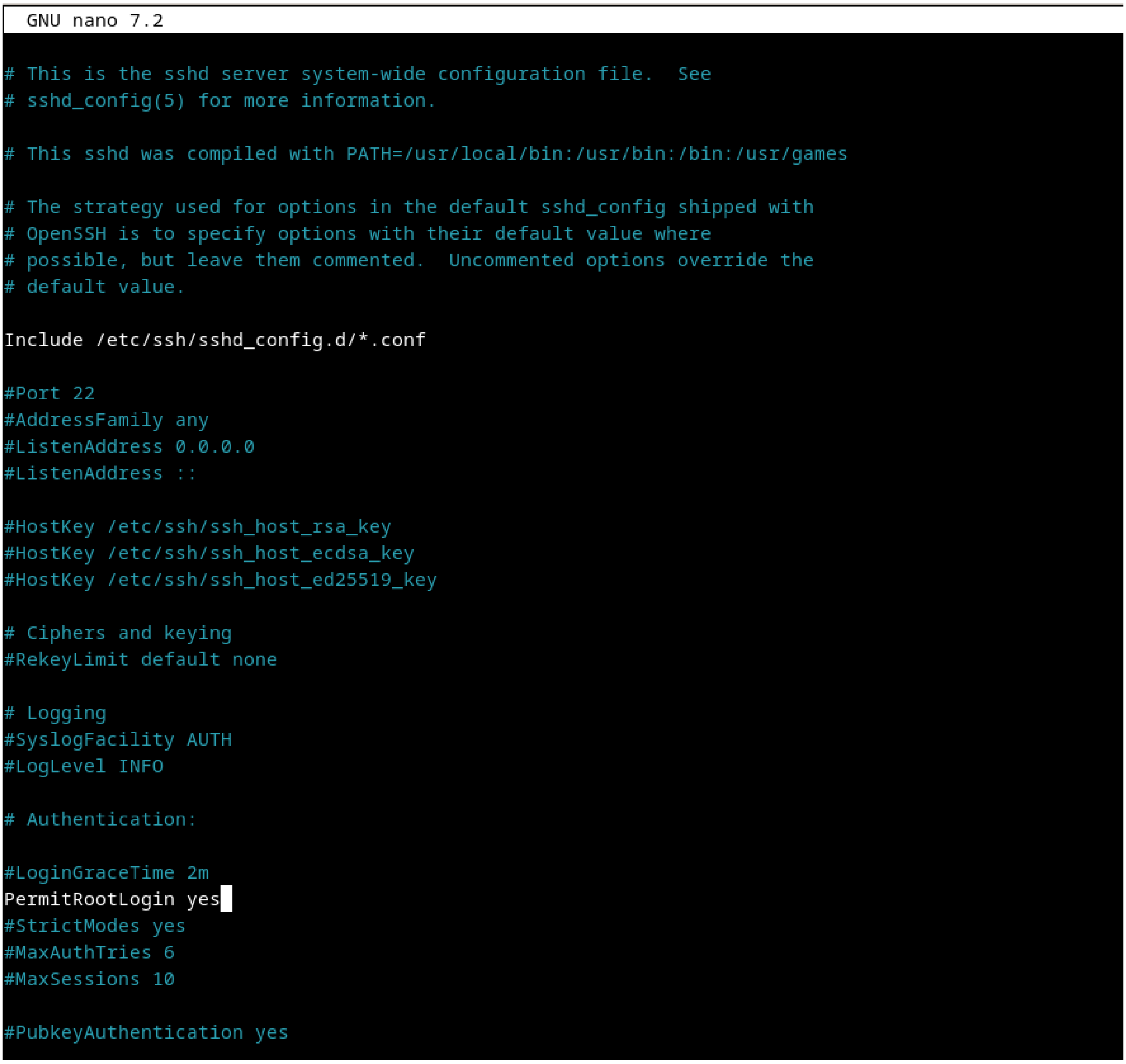


```
  GNU nano 7.2                    /etc/ssh/sshd_config *

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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

```

nano /etc/ssh/sshd_config

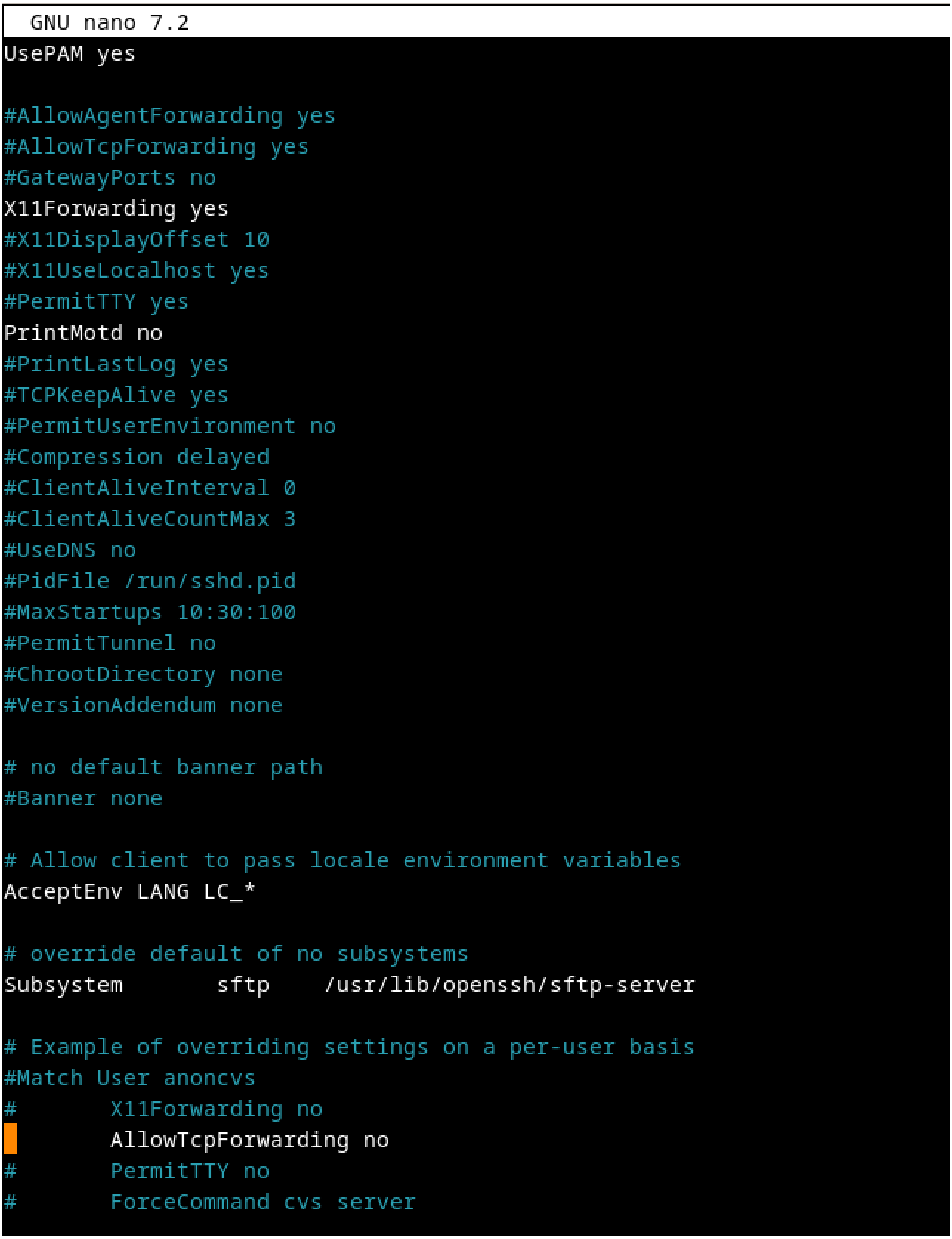
cambiamos la línea #PermitRootLogin prohibit-password por PermitRootLogin yes

permitimos que el root se pueda logear



```
  GNU nano 7.2

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

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

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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

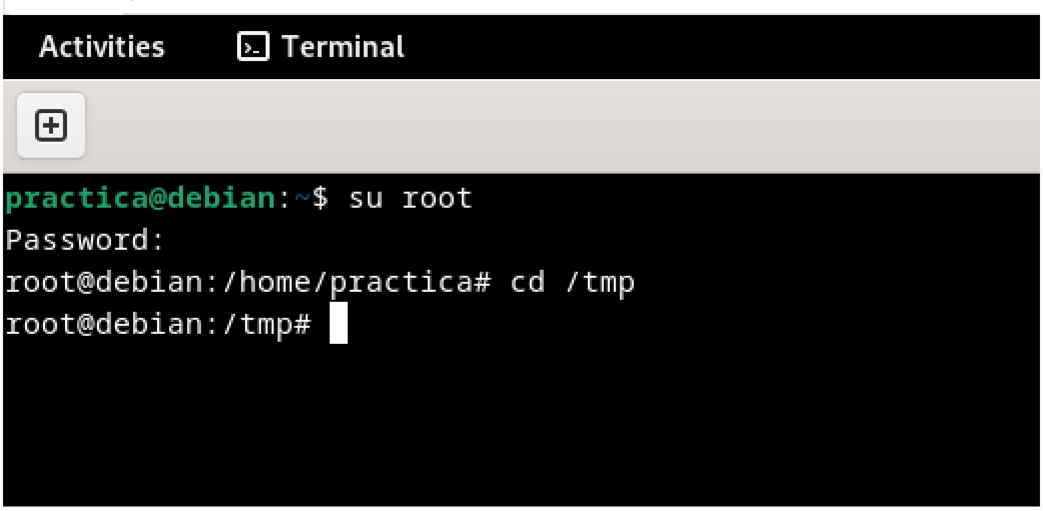
en AllowTcpFowarding no, quito la almohadilla para descomentar



```
  GNU nano 7.2
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
        AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
```

cambiamos a la carpeta /tmp

cd /tmp

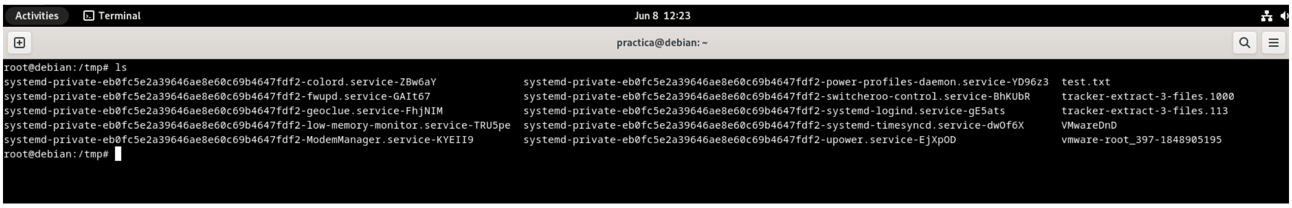


```
practica@debian:~$ su root
Password:
root@debian:/home/practica# cd /tmp
root@debian:/tmp#
```

creo un fichero test

echo “test” > test.txt

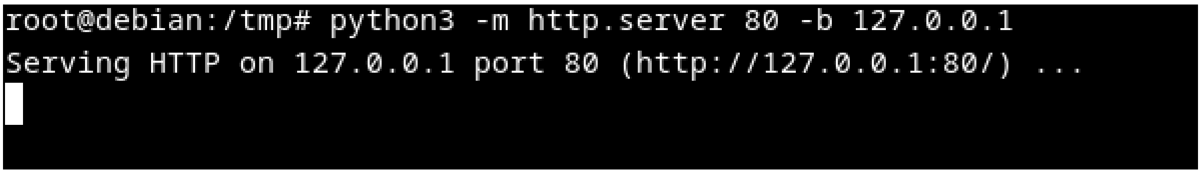
compruebo que se ha creado



```
root@debian:/tmp# ls
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-colord.service-ZBw6aY            systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-power-profiles-daemon.service-YD96z3  test.txt
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-fwupd.service-GAIt67             systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-switcheroo-control.service-BhKUbR     tracker-extract-3-files.1000
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-geoclue.service-FhjNIM           systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-systemd-logind.service-gE5ats         tracker-extract-3-files.113
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-low-memory-monitor.service-TRU5pe  systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-systemd-timesyncd.service-dwOf6X      VMwareDnD
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-ModemManager.service-KYEII9      systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-upower.service-EjXpOD                 vmware-root_397-1848905195
root@debian:/tmp#
```

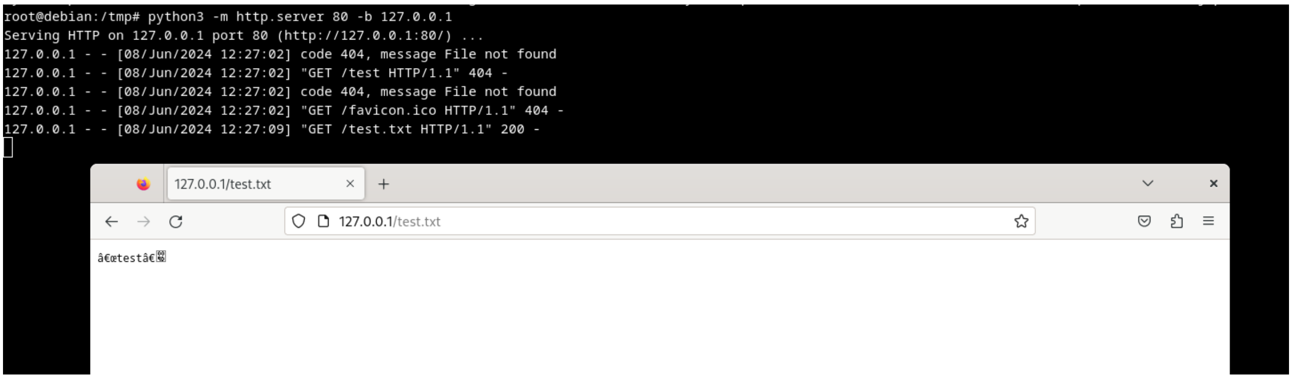
levanto el servidor:

python3 -m http.server 80 -b 127.0.0.1



```
root@debian:/tmp# python3 -m http.server 80 -b 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
```

me voy al navegador a la dirección 127.0.0.1/test.txt

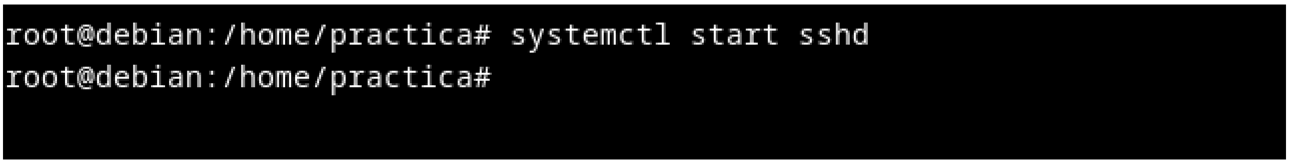


```
root@debian:/tmp# python3 -m http.server 80 -b 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
127.0.0.1 - - [08/Jun/2024 12:27:02] code 404, message File not found
127.0.0.1 - - [08/Jun/2024 12:27:02] "GET /test HTTP/1.1" 404 -
127.0.0.1 - - [08/Jun/2024 12:27:02] code 404, message File not found
127.0.0.1 - - [08/Jun/2024 12:27:02] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [08/Jun/2024 12:27:09] "GET /test.txt HTTP/1.1" 200 -
```

```
â€œtestâ€
```

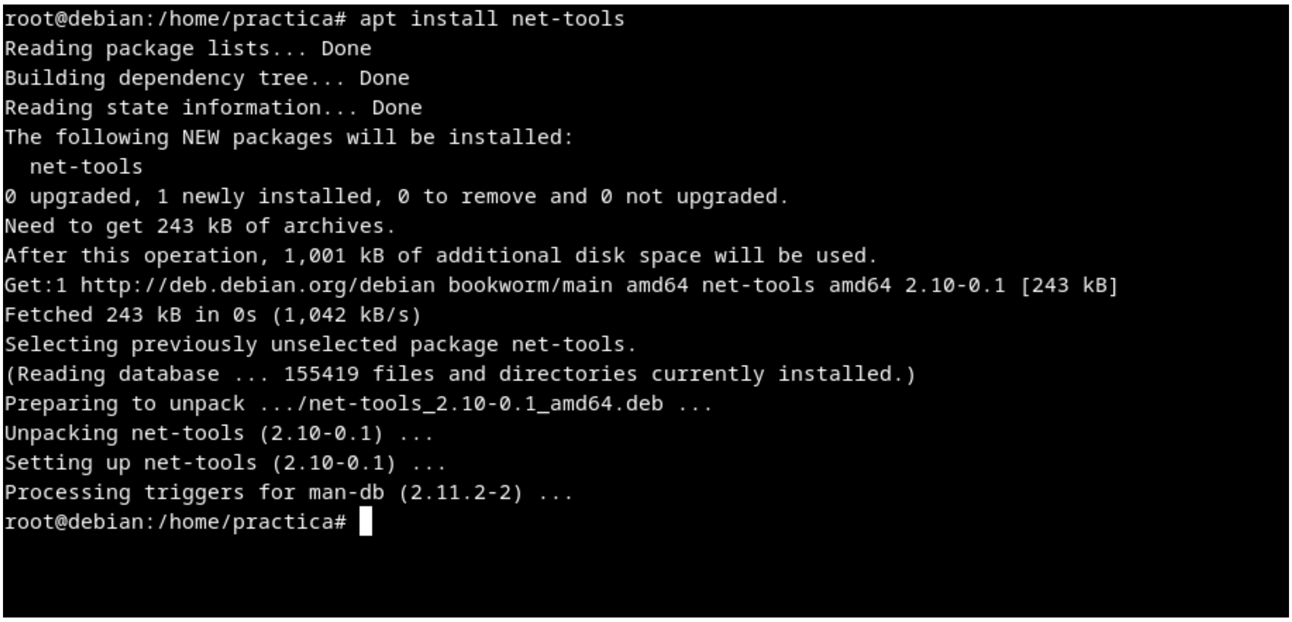
El objetivo es, desde otra máquina, poder leer este fichero test.txt

en otra terminal, reinicio el servicio ssh, porque he modificado la configuración hago un systemctl stop sshd y un systemctl start sshd



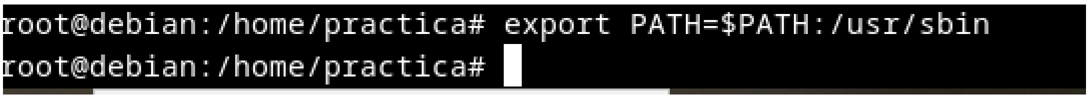
```
root@debian:/home/practica# systemctl start sshd
root@debian:/home/practica#
```

hago un apt install net-tools para instalación herramientas de internet y poder coger la ip



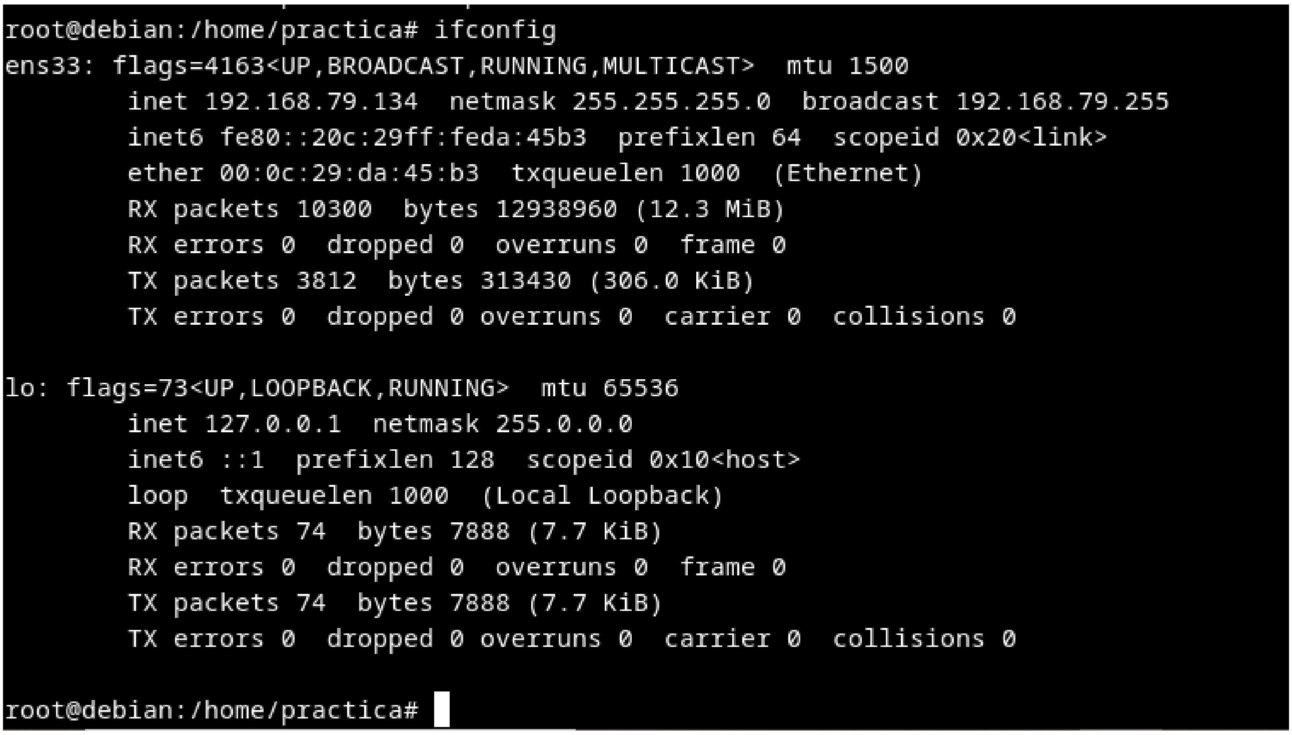
```
root@debian:/home/practica# apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 243 kB of archives.
After this operation, 1,001 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 net-tools amd64 2.10-0.1 [243 kB]
Fetched 243 kB in 0s (1,042 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 155419 files and directories currently installed.)
Preparing to unpack .../net-tools_2.10-0.1_amd64.deb ...
Unpacking net-tools (2.10-0.1) ...
Setting up net-tools (2.10-0.1) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:/home/practica#
```

hago un export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin



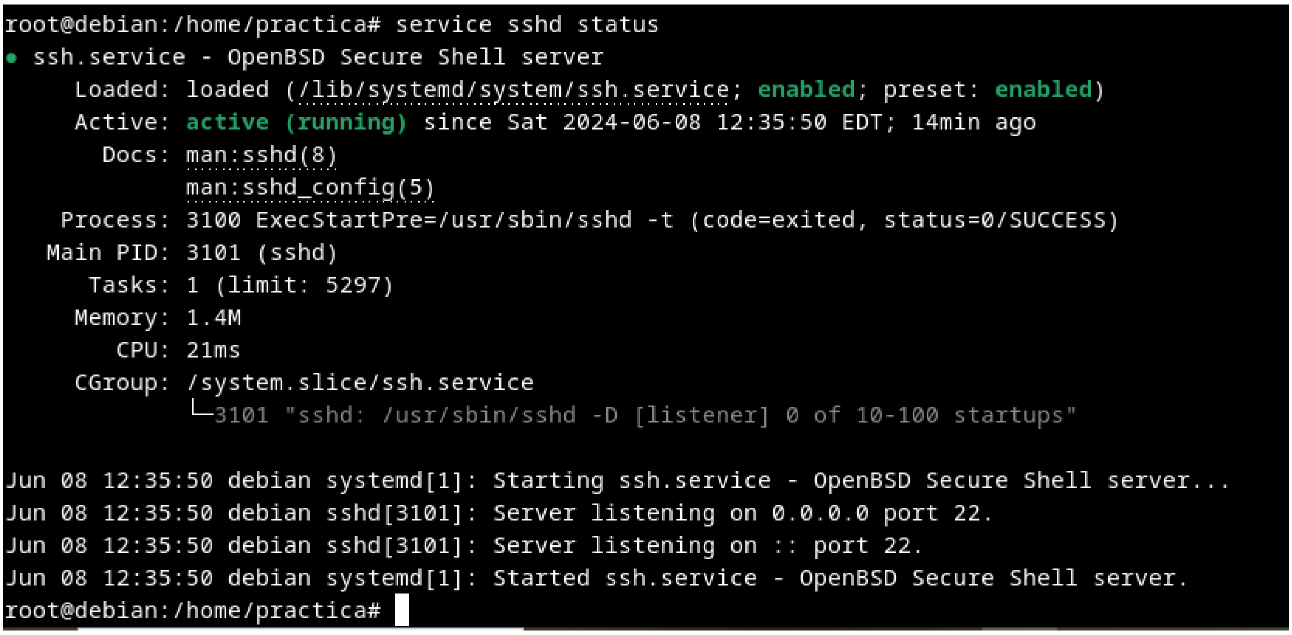
```
root@debian:/home/practica# export PATH=$PATH:/usr/sbin
root@debian:/home/practica#
```

ahora sí puedo copiar la ip: ifconfig



```
root@debian:/home/practica# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.79.134  netmask 255.255.255.0  broadcast 192.168.79.255
        inet6 fe80::20c:29ff:feda:45b3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:da:45:b3  txqueuelen 1000  (Ethernet)
        RX packets 10300  bytes 12938960 (12.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3812  bytes 313430 (306.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 74  bytes 7888 (7.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 7888 (7.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@debian:/home/practica# 
```

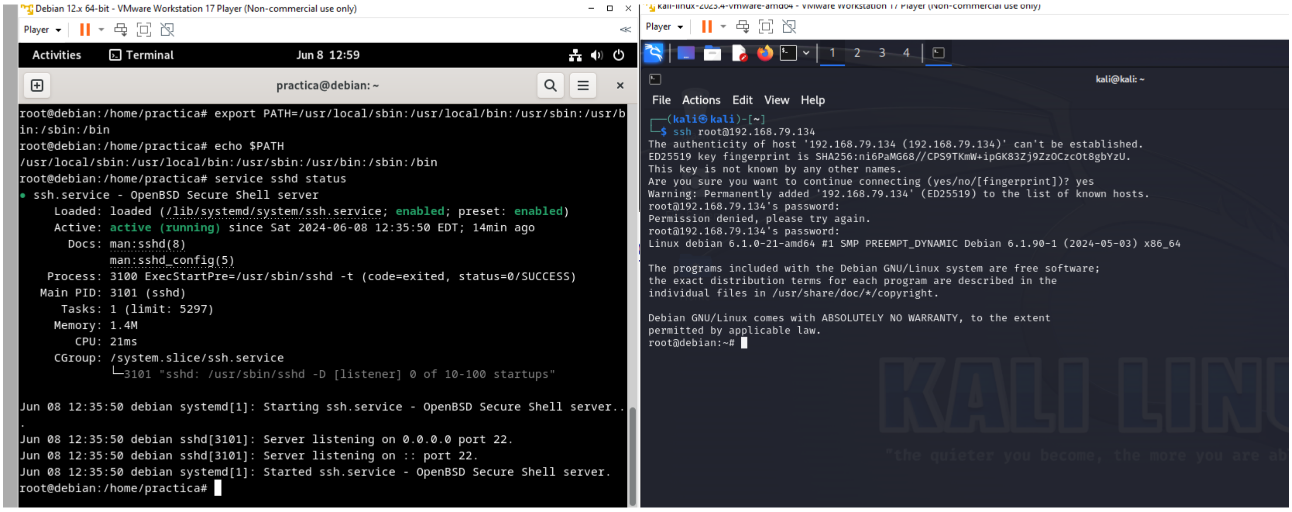
con service sshd status, compruebo que está levantado el servicio ssh, estando el active en verde



```
root@debian:/home/practica# service sshd status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-06-08 12:35:50 EDT; 14min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3100 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3101 (sshd)
      Tasks: 1 (limit: 5297)
     Memory: 1.4M
        CPU: 21ms
     CGroup: /system.slice/ssh.service
             └─3101 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 08 12:35:50 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 08 12:35:50 debian sshd[3101]: Server listening on 0.0.0.0 port 22.
Jun 08 12:35:50 debian sshd[3101]: Server listening on :: port 22.
Jun 08 12:35:50 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@debian:/home/practica# 
```

desde otra máquina pongo ssh root@192.168.79.134

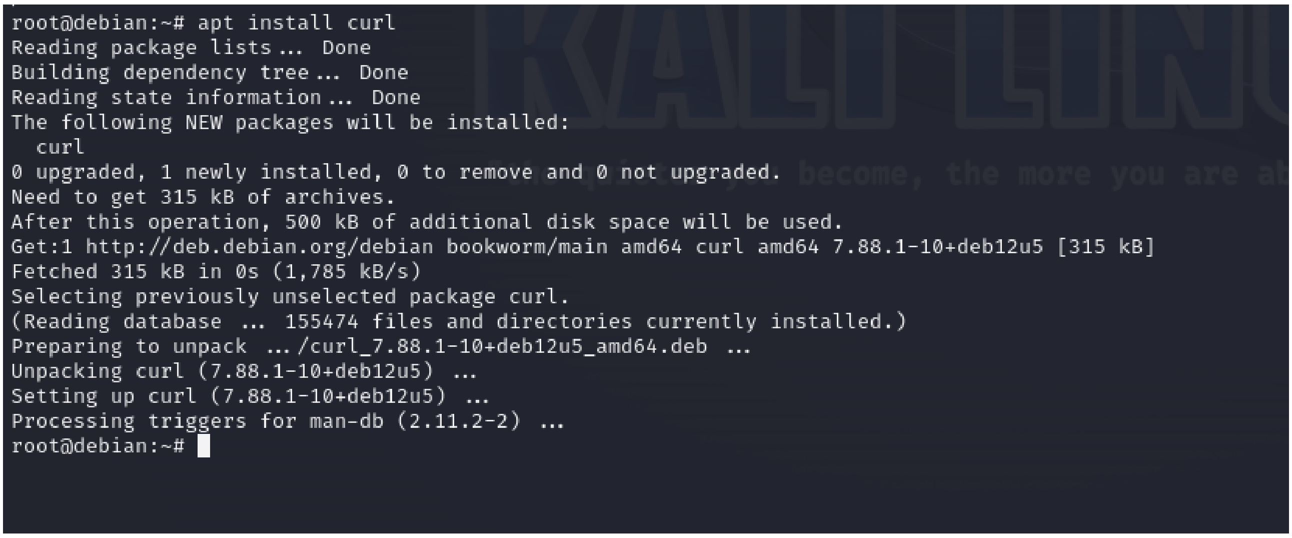
compruebo que la máquina atacante (Debian) se ha metido en la víctima (kali)


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Jun 8 12:59
practica@debian: ~
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
kali@kali: ~
File
Actions
Edit
View
Help
KALI LINU
"the quieter you become, the more you are ab

```
root@debian:/home/practica# export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/b
in:/sbin:/bin
root@debian:/home/practica# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
root@debian:/home/practica# service sshd status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-06-08 12:35:50 EDT; 14min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3100 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3101 (sshd)
      Tasks: 1 (limit: 5297)
     Memory: 1.4M
        CPU: 21ms
     CGroup: /system.slice/ssh.service
             └─3101 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 08 12:35:50 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server..
.
Jun 08 12:35:50 debian sshd[3101]: Server listening on 0.0.0.0 port 22.
Jun 08 12:35:50 debian sshd[3101]: Server listening on :: port 22.
Jun 08 12:35:50 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@debian:/home/practica# 
```

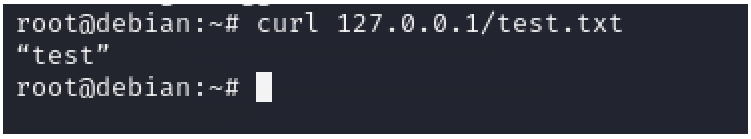
```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.79.134
The authenticity of host '192.168.79.134 (192.168.79.134)' can't be established.
ED25519 key fingerprint is SHA256:ni6PaMG68//CPS9TKmW+ipGK83Zj9ZzOCzcOt8gbYzU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.79.134' (ED25519) to the list of known hosts.
root@192.168.79.134's password:
Permission denied, please try again.
root@192.168.79.134's password:
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) 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@debian:~# 
```

hago un apt install curl



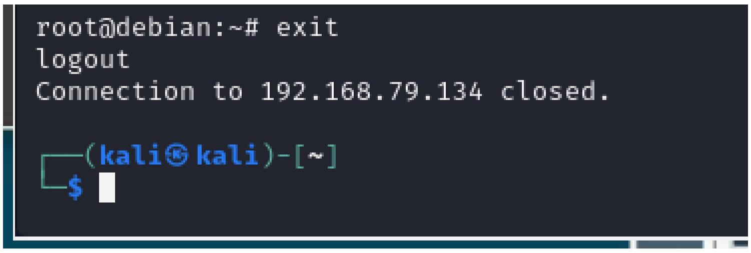
```
root@debian:~# apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 315 kB of archives.
After this operation, 500 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 curl amd64 7.88.1-10+deb12u5 [315 kB]
Fetched 315 kB in 0s (1,785 kB/s)
Selecting previously unselected package curl.
(Reading database ... 155474 files and directories currently installed.)
Preparing to unpack .../curl_7.88.1-10+deb12u5_amd64.deb ...
Unpacking curl (7.88.1-10+deb12u5) ...
Setting up curl (7.88.1-10+deb12u5) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:~# 
```

hago un curl 127.0.0.1/test.txt



```
root@debian:~# curl 127.0.0.1/test.txt
“test”
root@debian:~# 
```

escribo exit para cerrar la conexión



```
root@debian:~# exit
logout
Connection to 192.168.79.134 closed.

┌──(kali㉿kali)-[~]
└─$ 
```