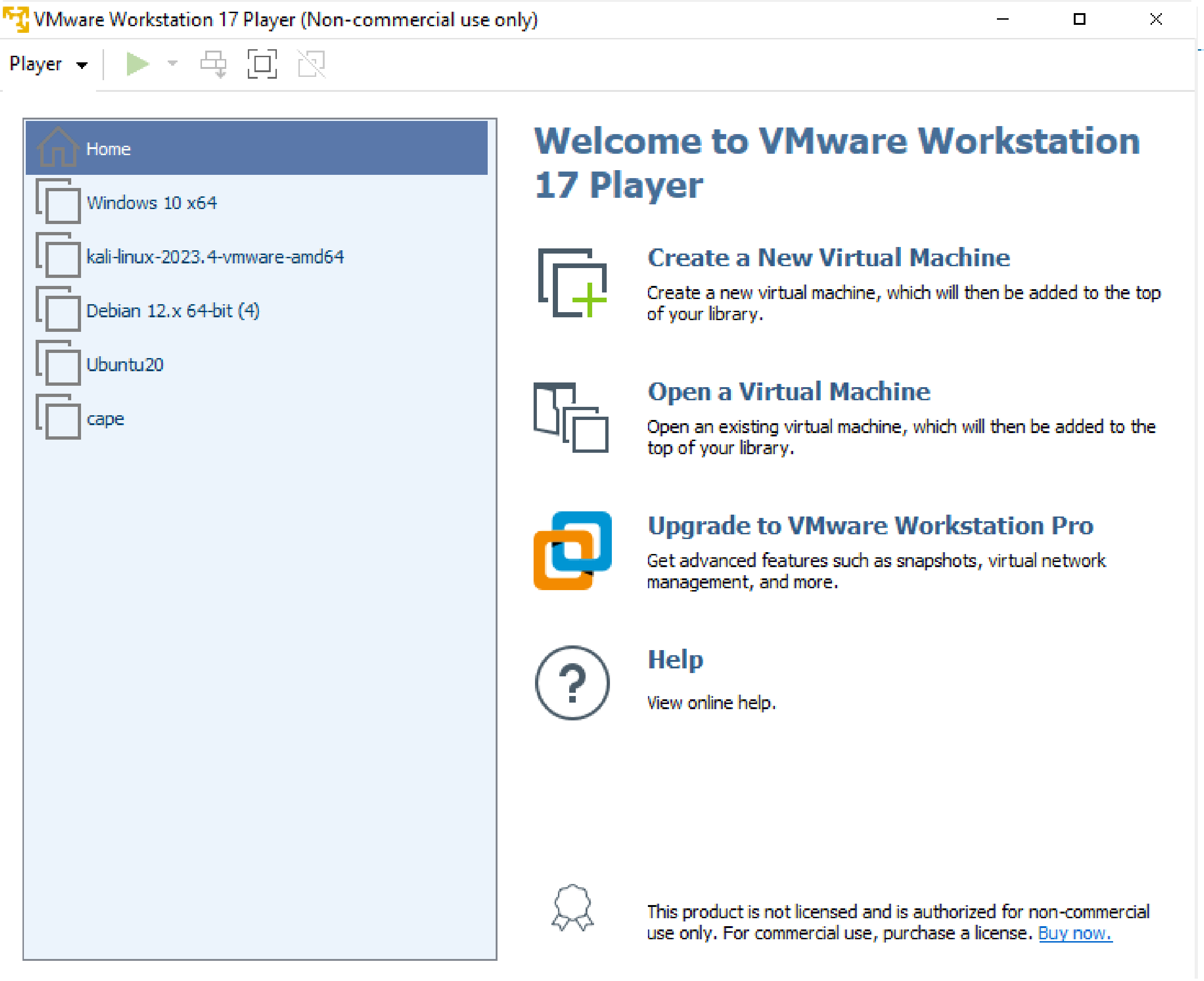
Ejercicio 2 Construir un laboratorio:

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

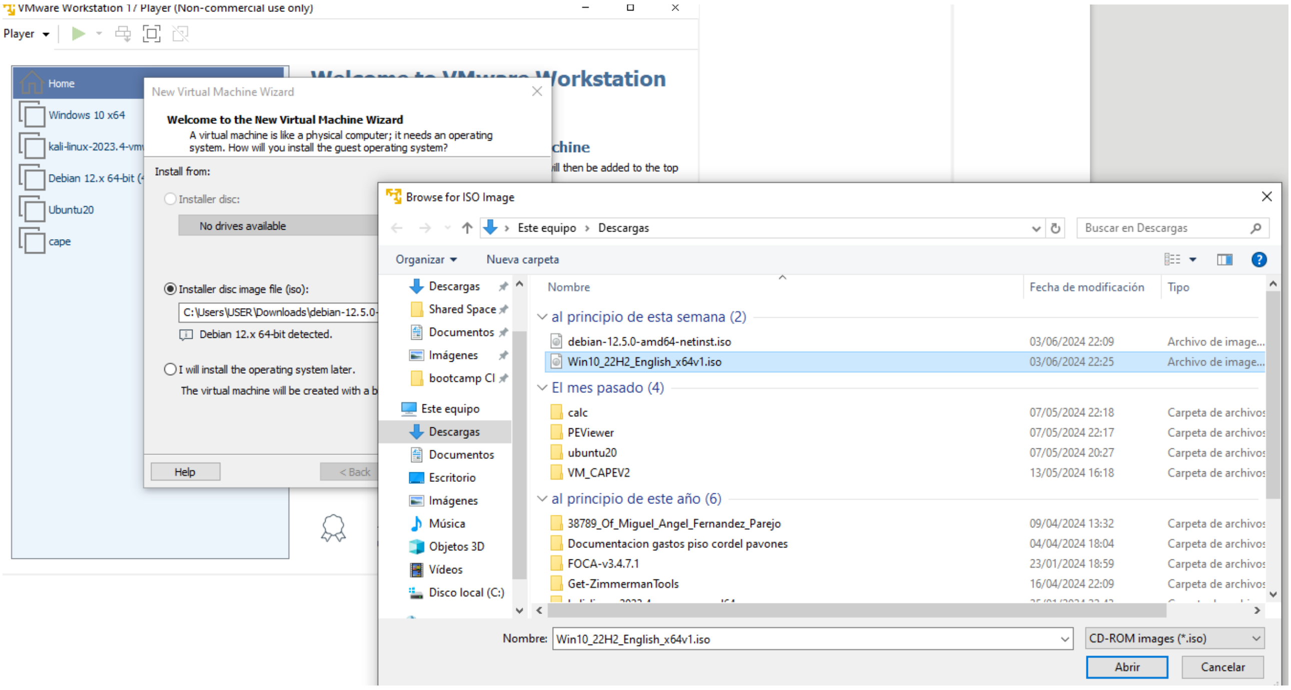
Get advanced features such as snapshots, virtual network management, and more.

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)

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

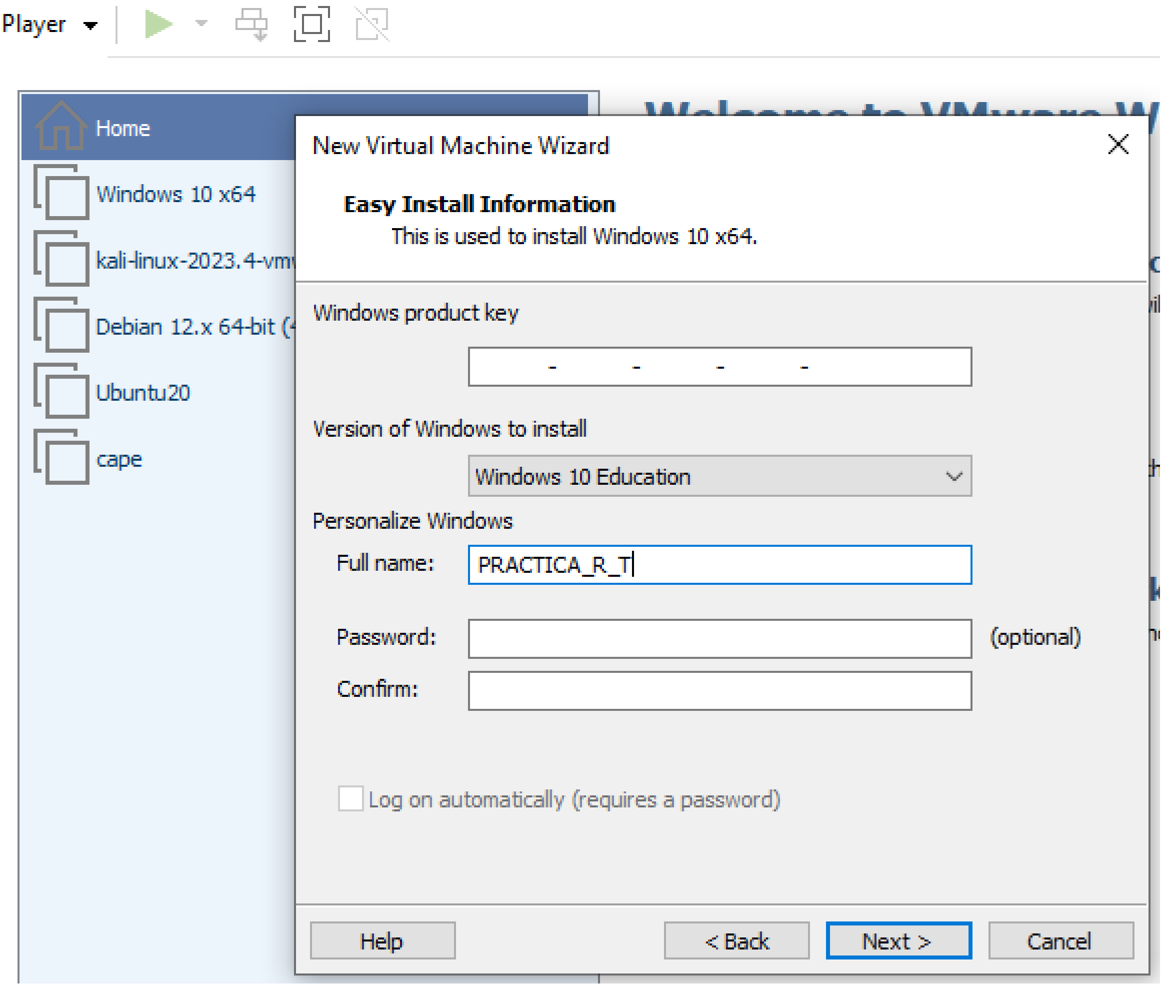
Este equipo › Descargas

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

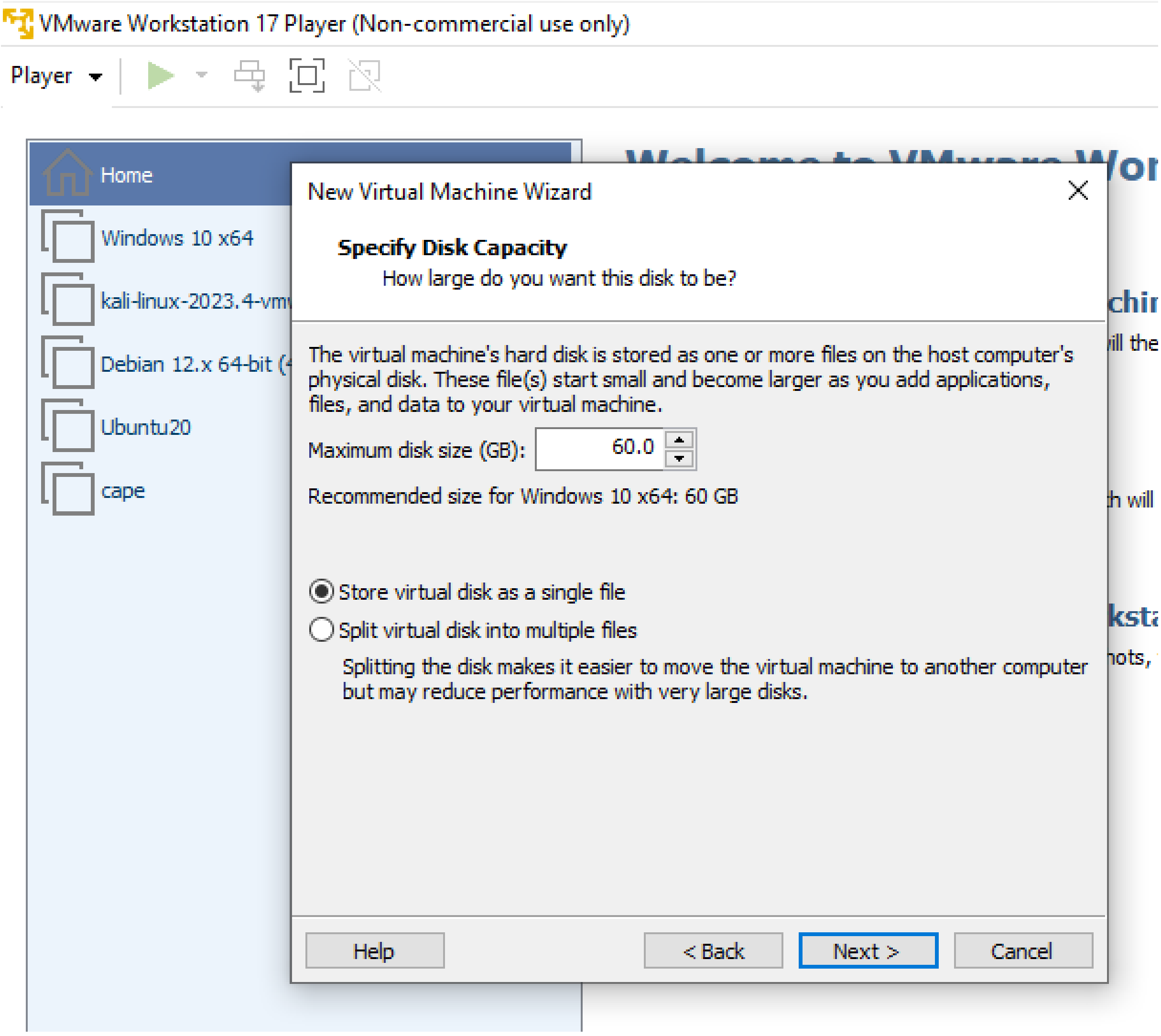
Full name: PRACTICA_R_T

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

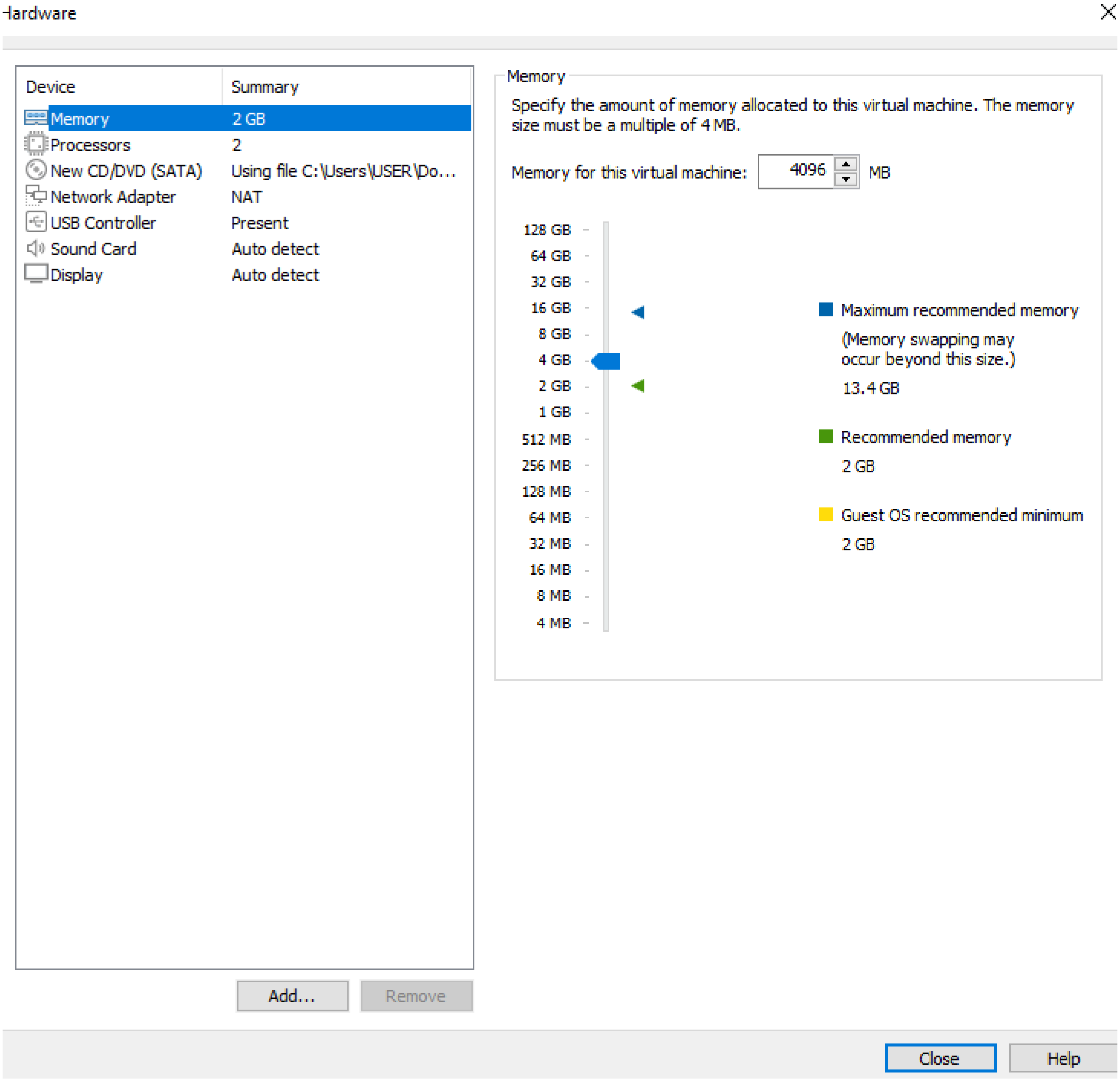
Recommended size for Windows 10 x64: 60 GB

● 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.)

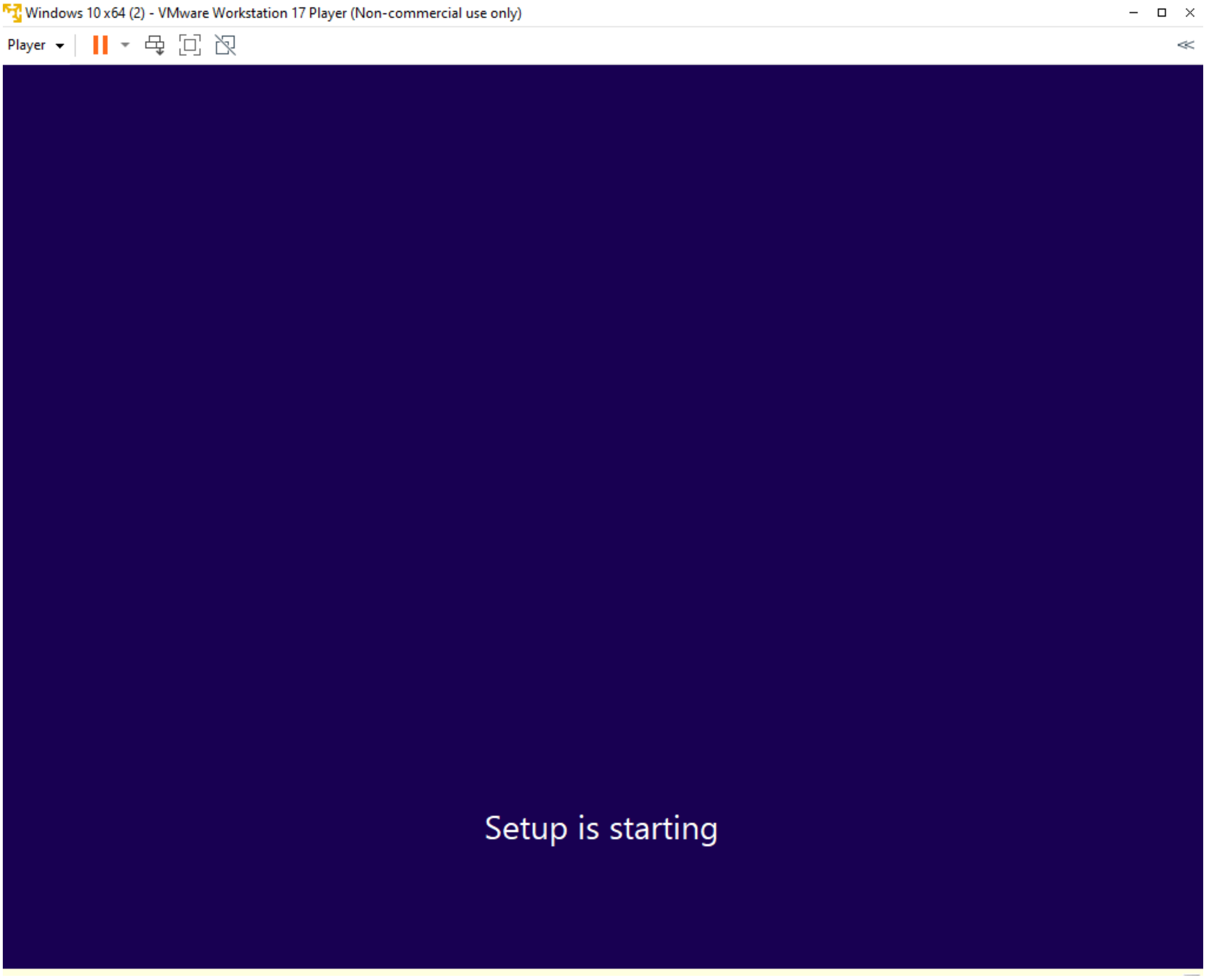
13.4 GB

🟩 Recommended memory

2 GB

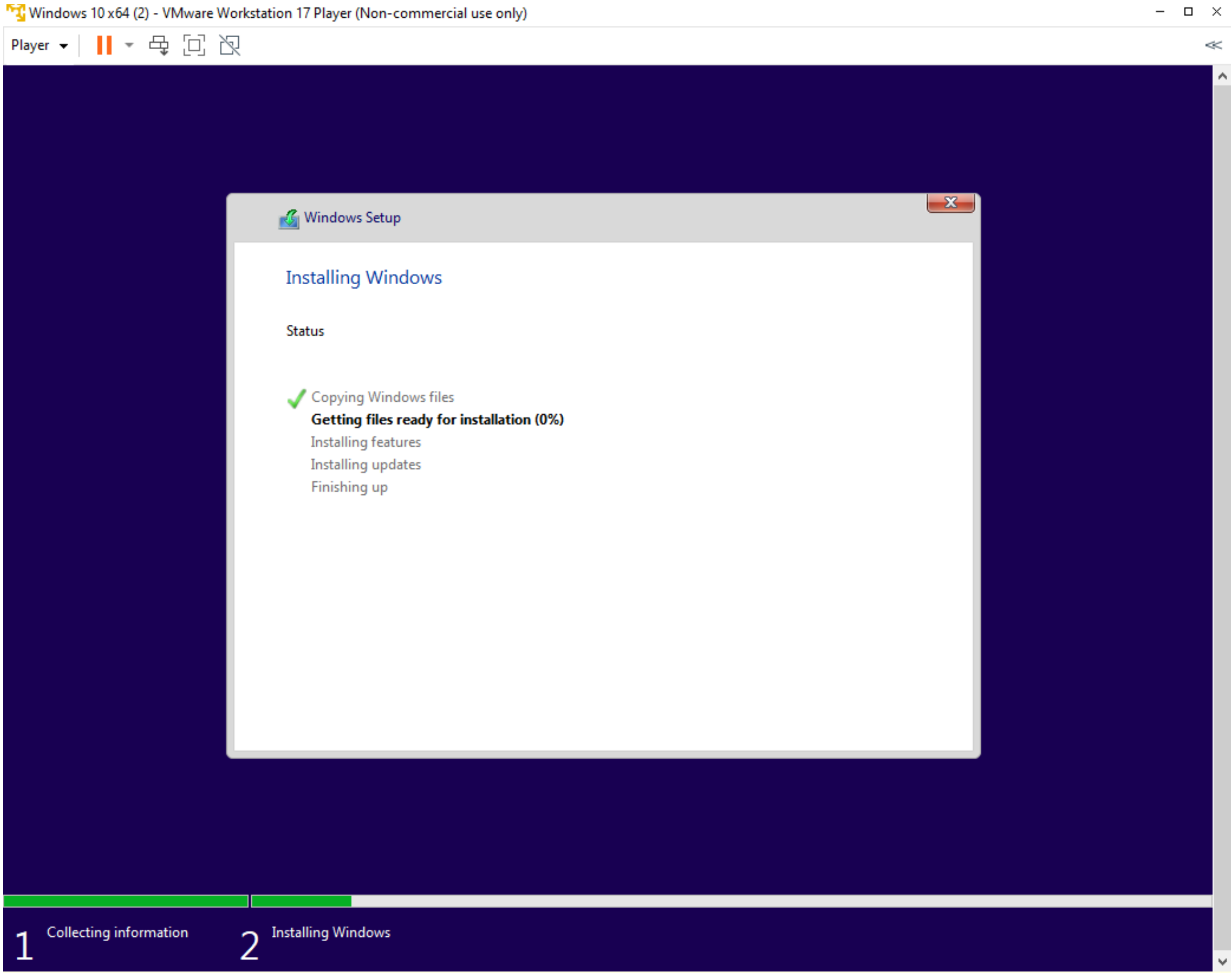
🟨 Guest OS recommended minimum

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)

Windows Setup

Installing Windows

Status

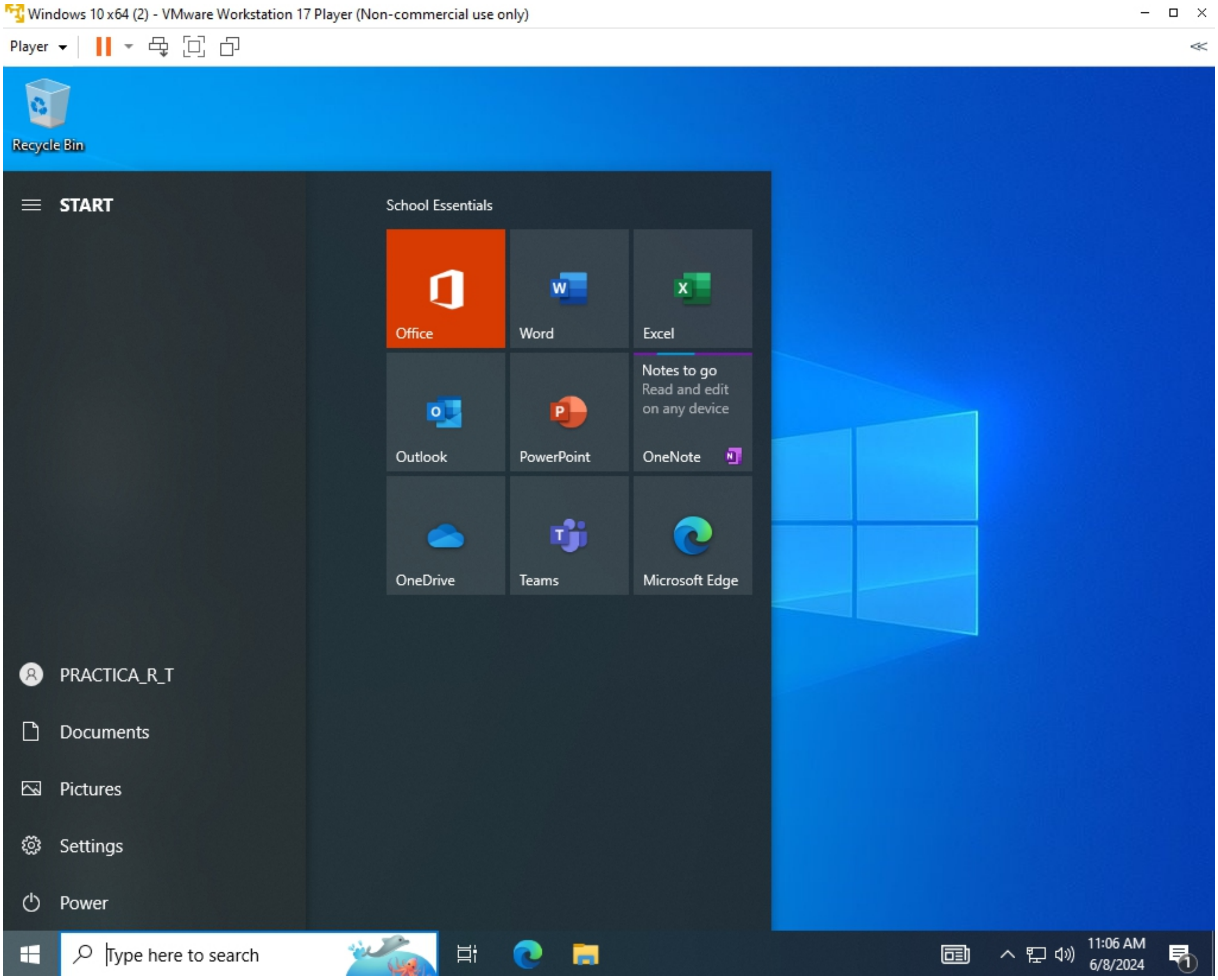
✓ Copying Windows files

Getting files ready for installation (0%)

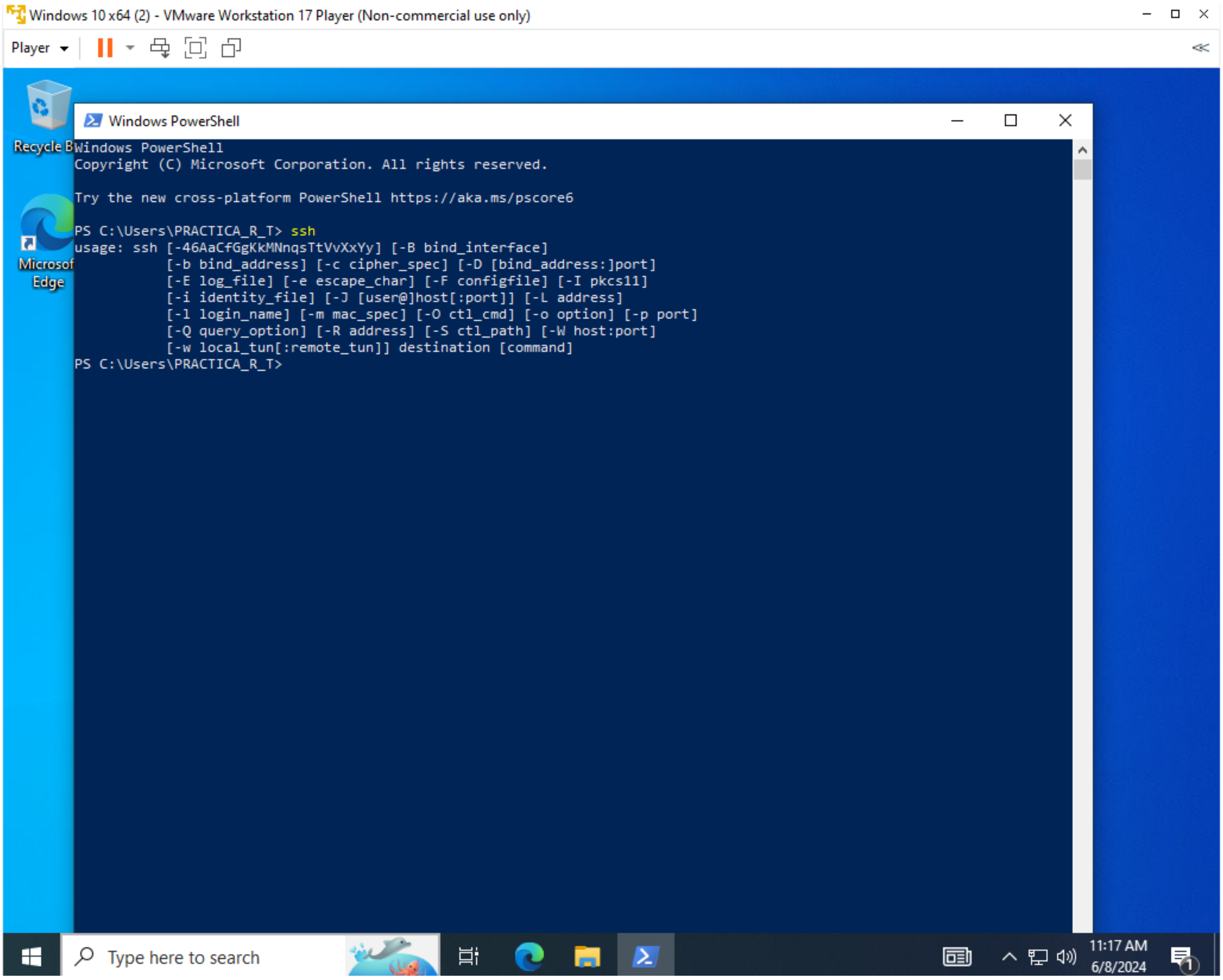
Installing features

Installing updates

Finishing up



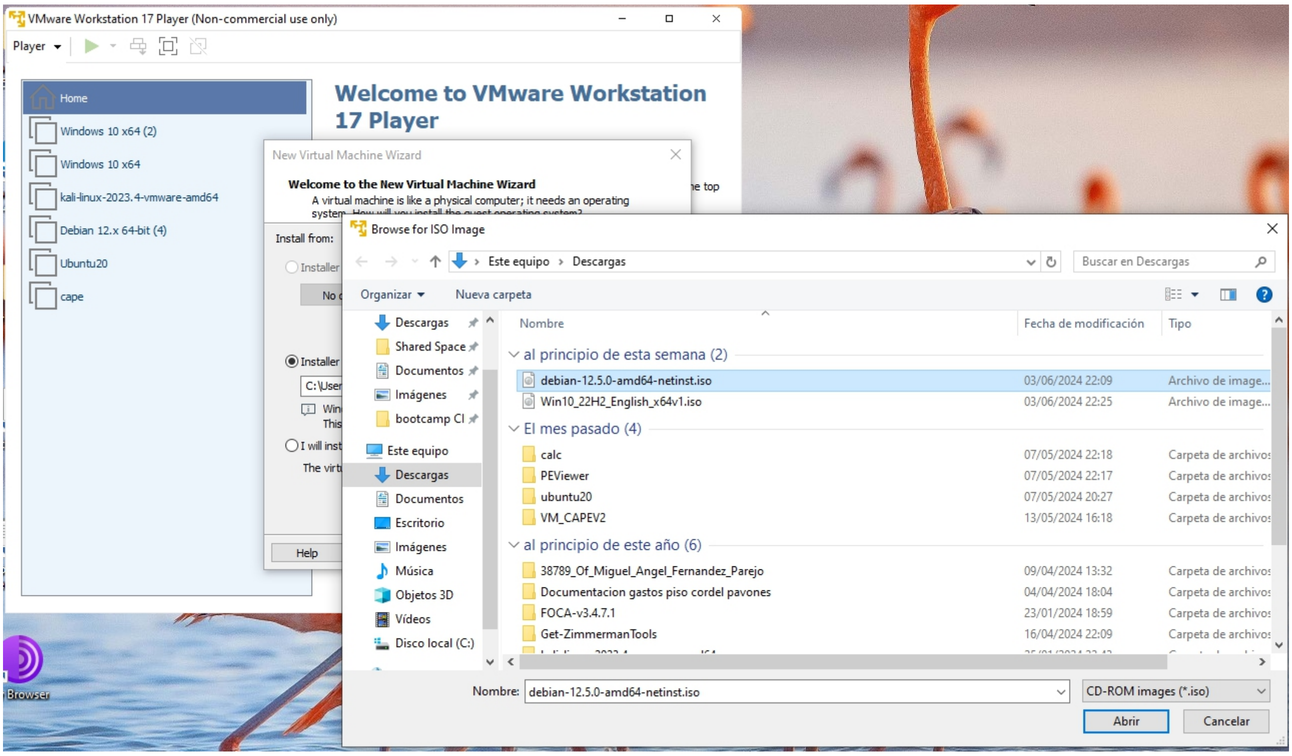
comprobamos el ssh



```
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:

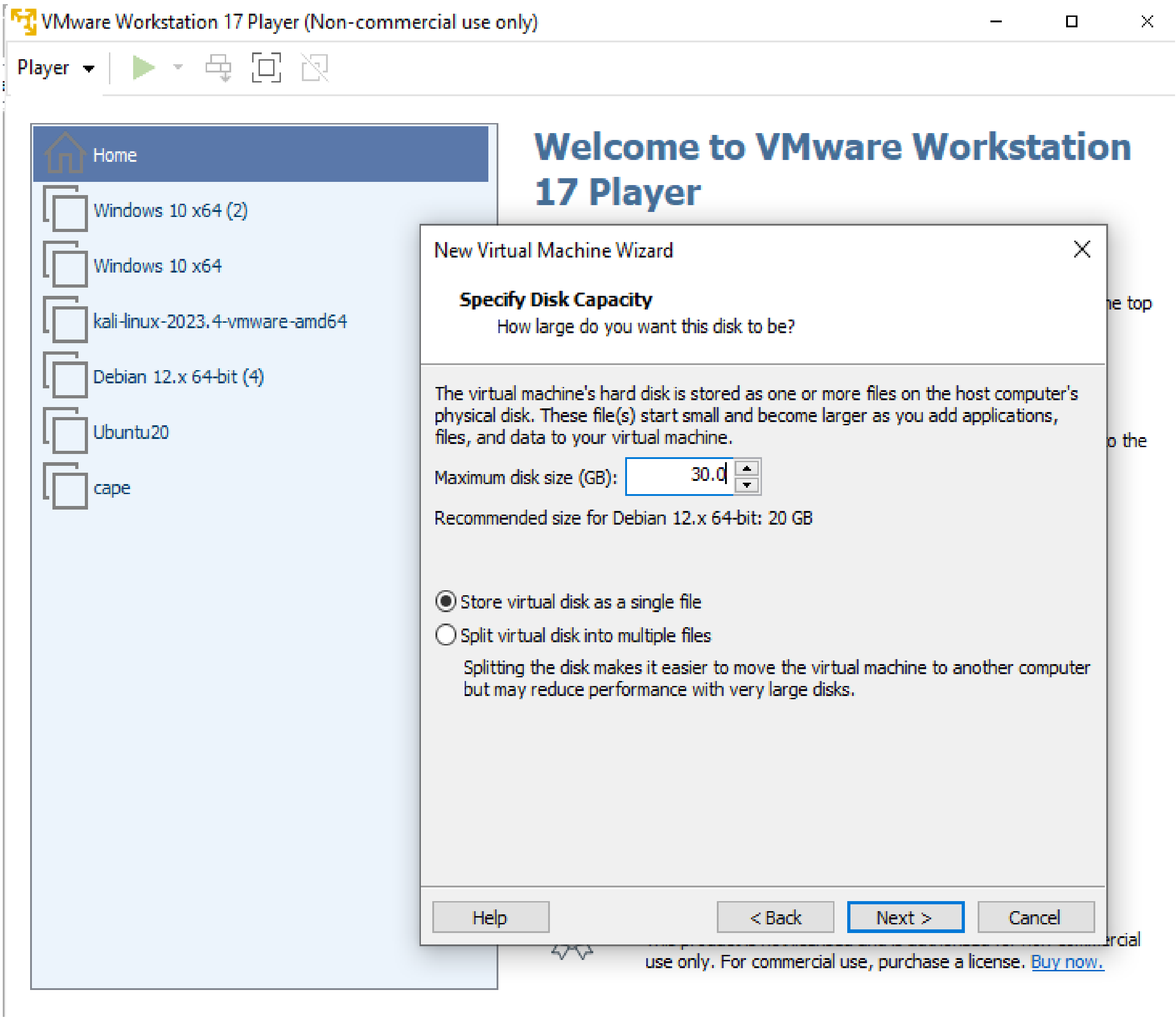


Nombre	Fecha de modificación	Tipo
al principio de esta semana (2)		
debian-12.5.0-amd64-netinst.iso	03/06/2024 22:09	Archivo de image...
Win10_22H2_English_x64v1.iso	03/06/2024 22:25	Archivo de image...
El mes pasado (4)		
calc	07/05/2024 22:18	Carpeta de archivos
PEViewer	07/05/2024 22:17	Carpeta de 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
Help
< Back
Next >
Cancel

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

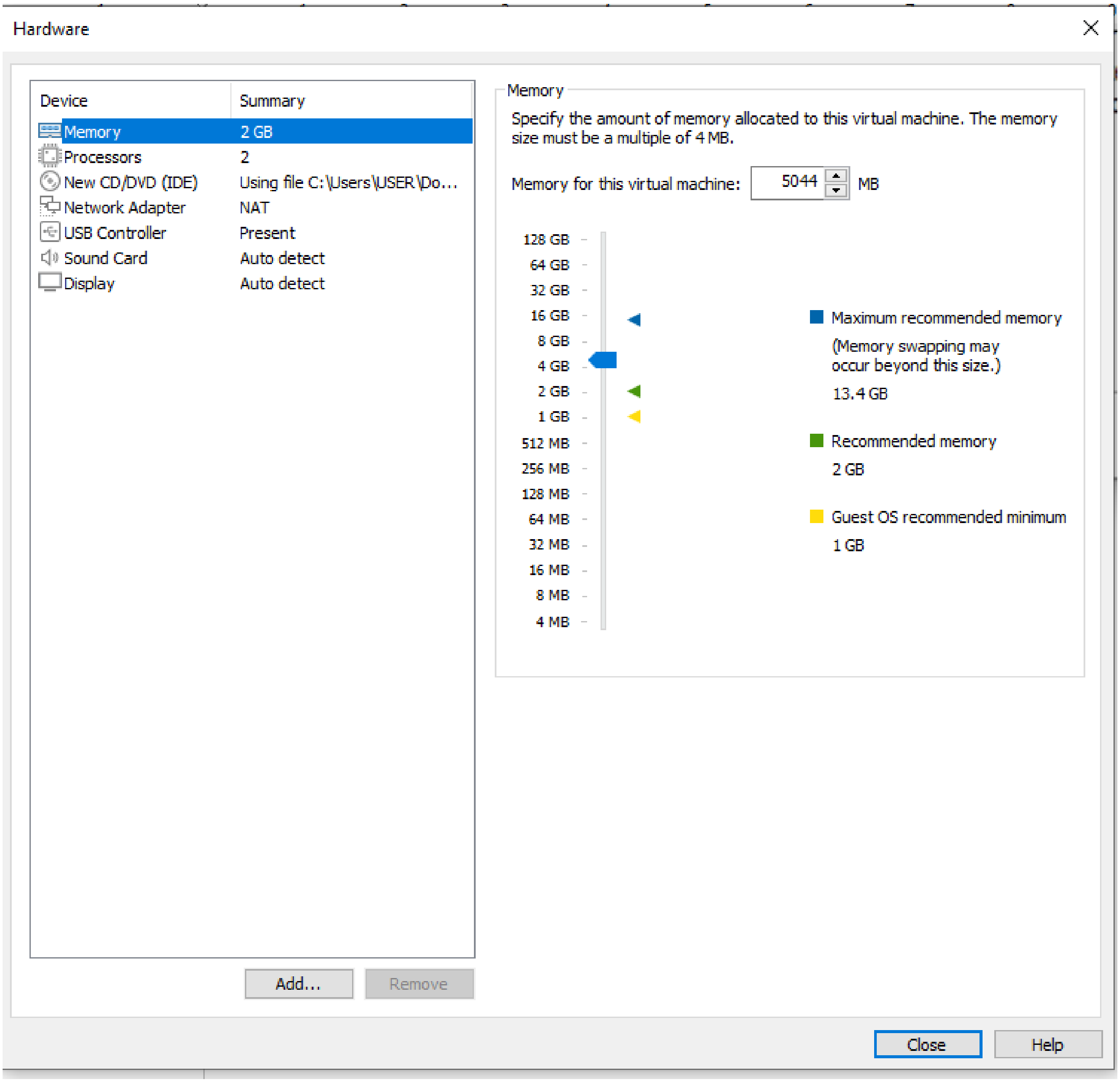
● Store virtual disk as a single file

○ 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.

use only. For commercial use, purchase a license. Buy now.

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

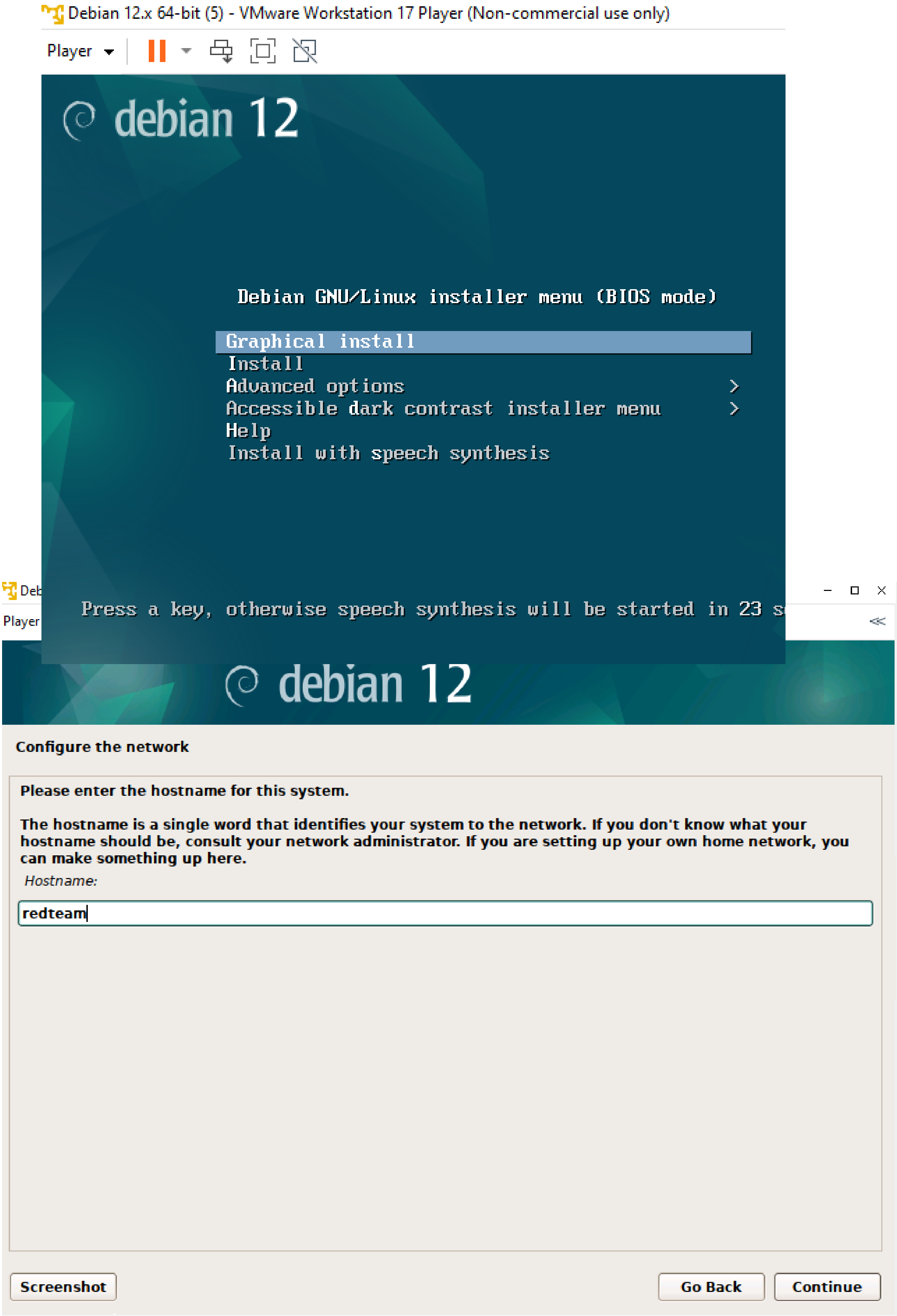
🟩 Recommended memory

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

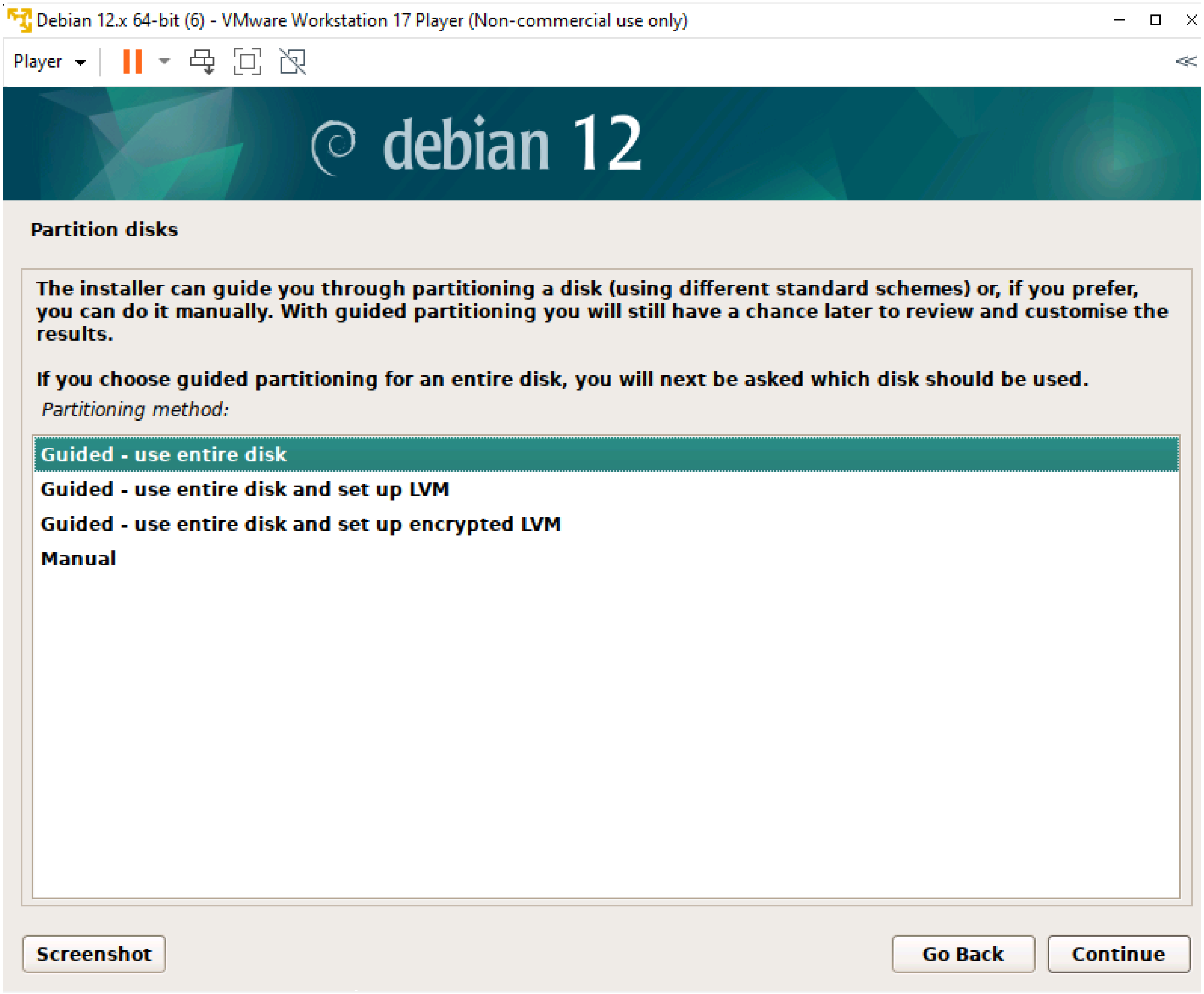
Please enter the hostname for this system.

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

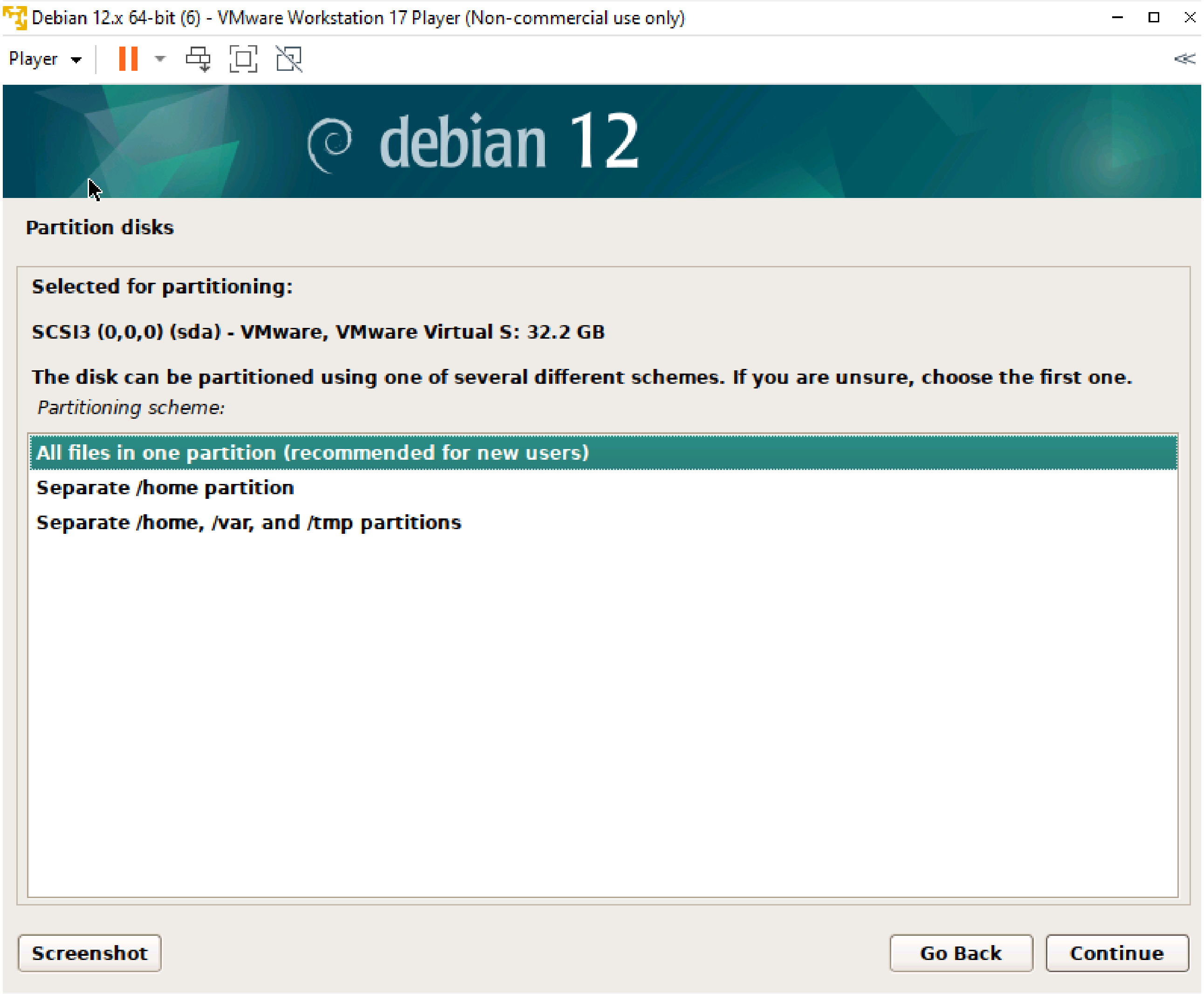
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

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:

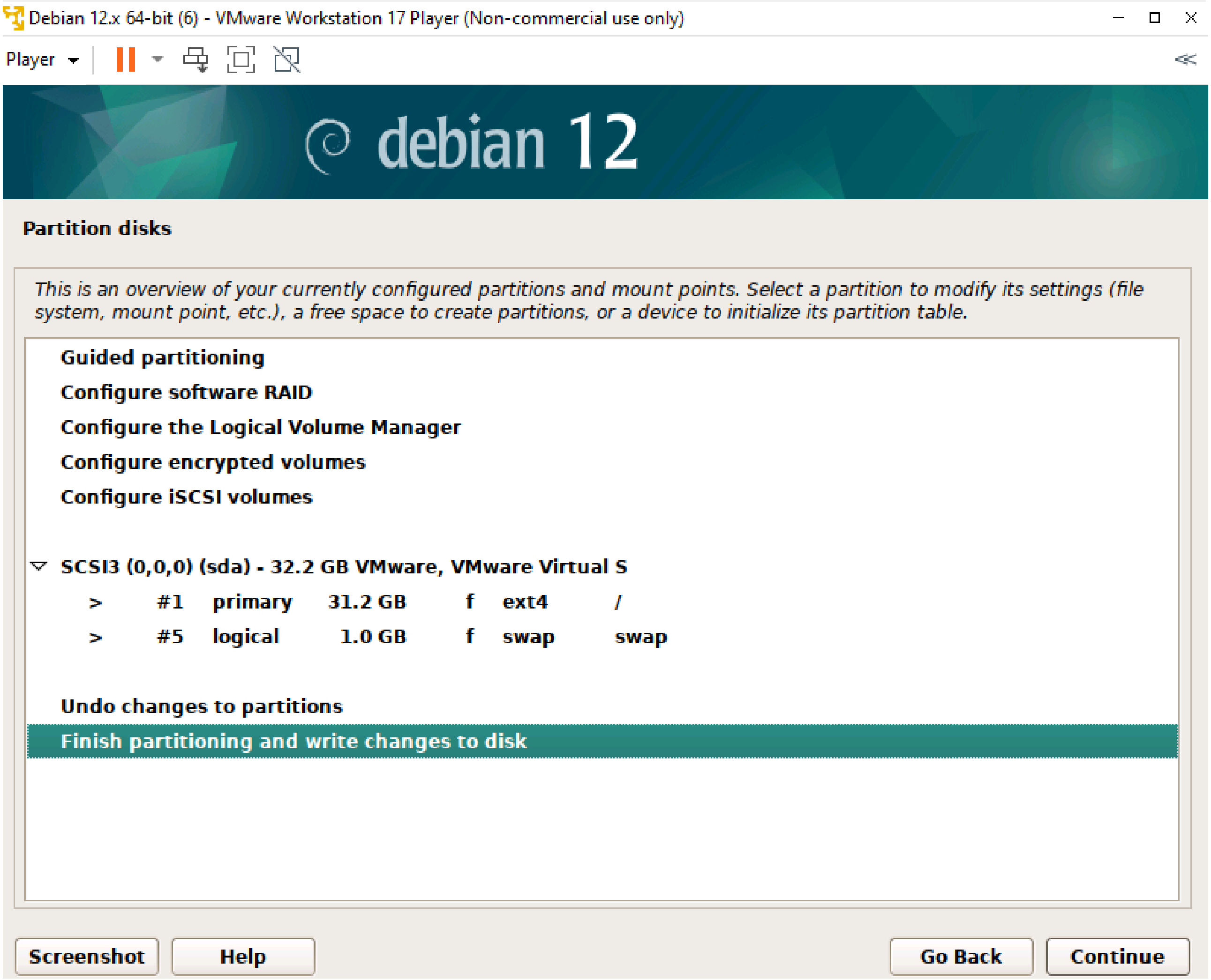
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 32.2 GB

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



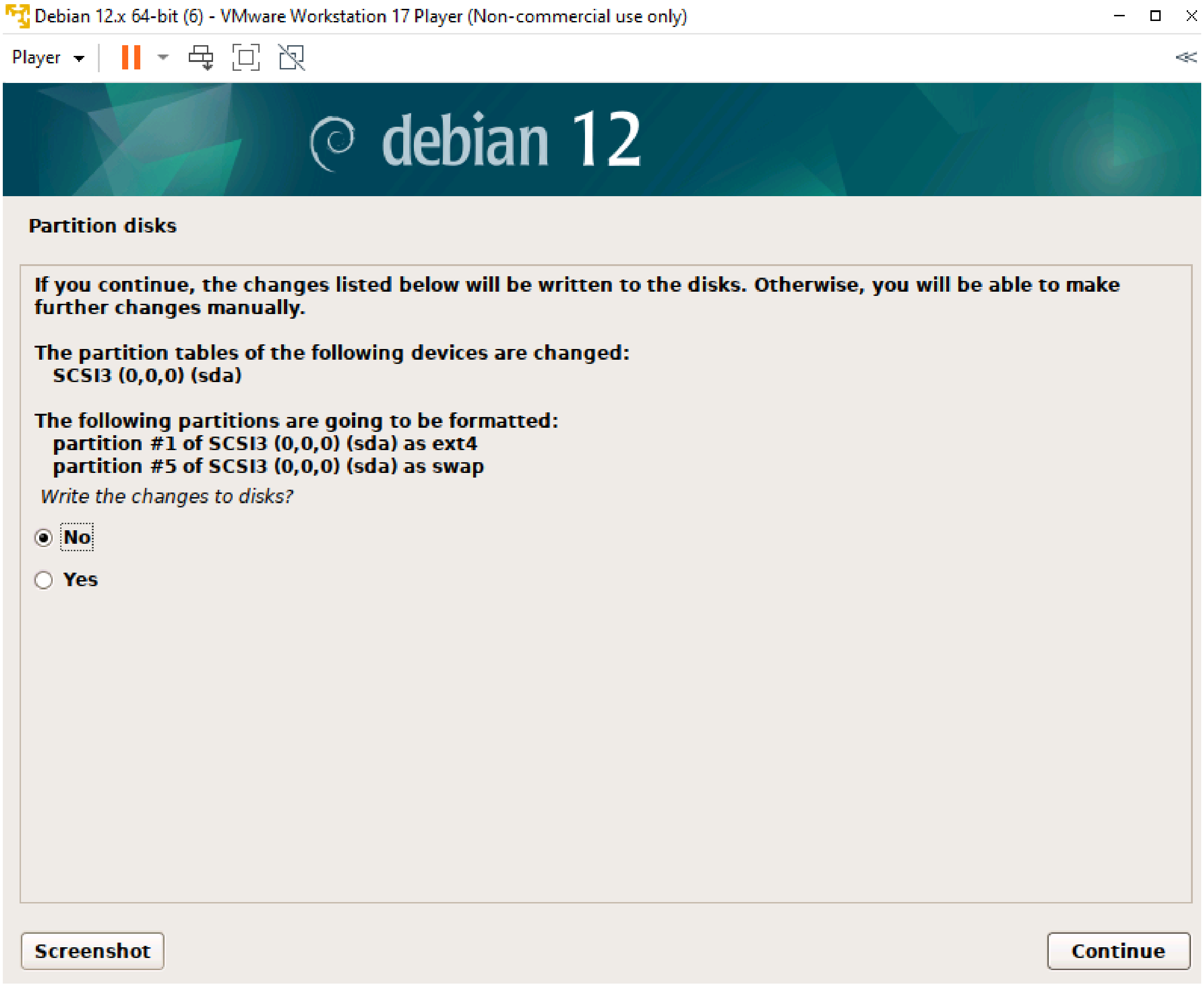
Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

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)

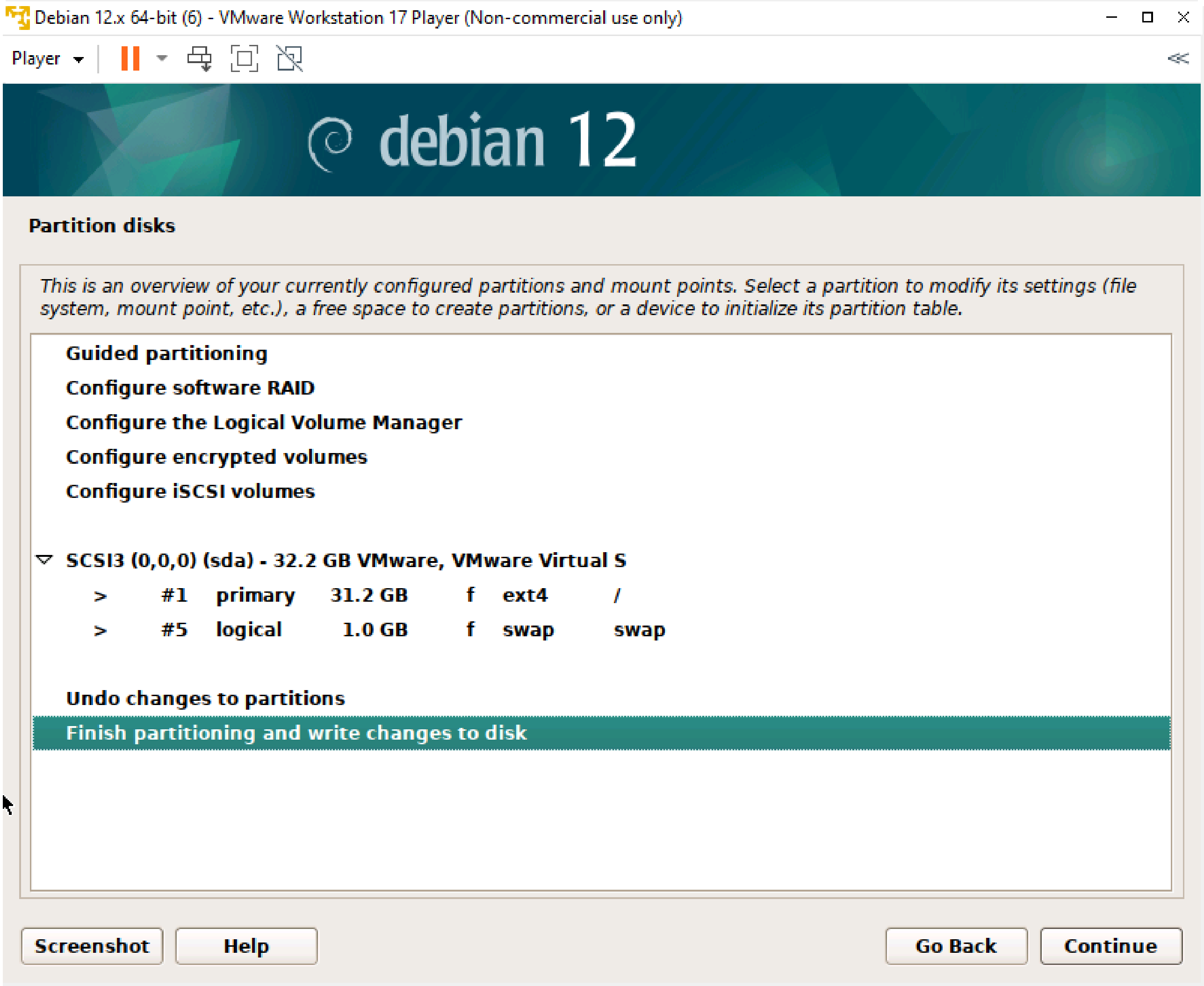
The following partitions are going to be formatted:
  partition #1 of SCSI3 (0,0,0) (sda) as ext4
  partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

● No

○ Yes

Finalizo la partición

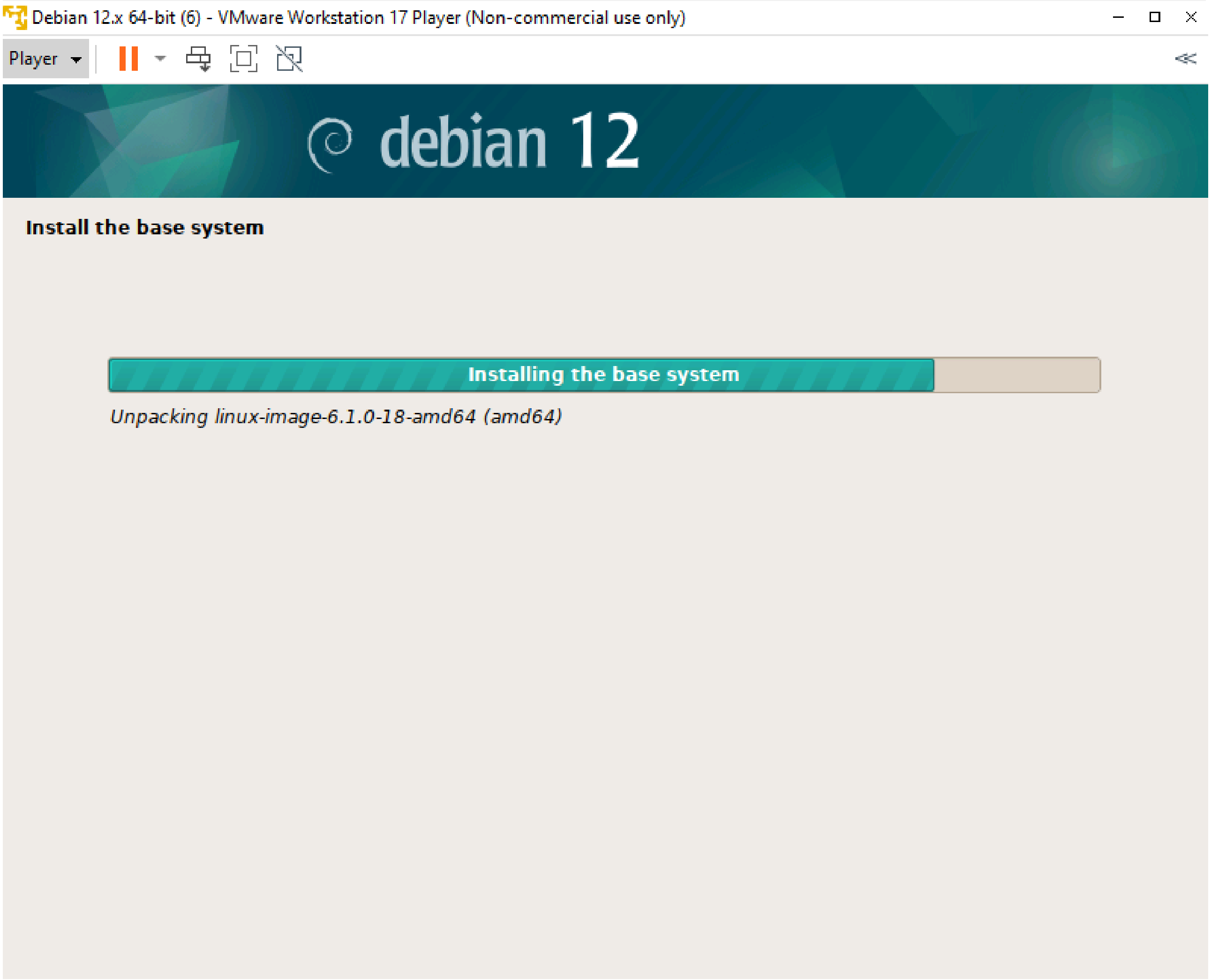


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)

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
```



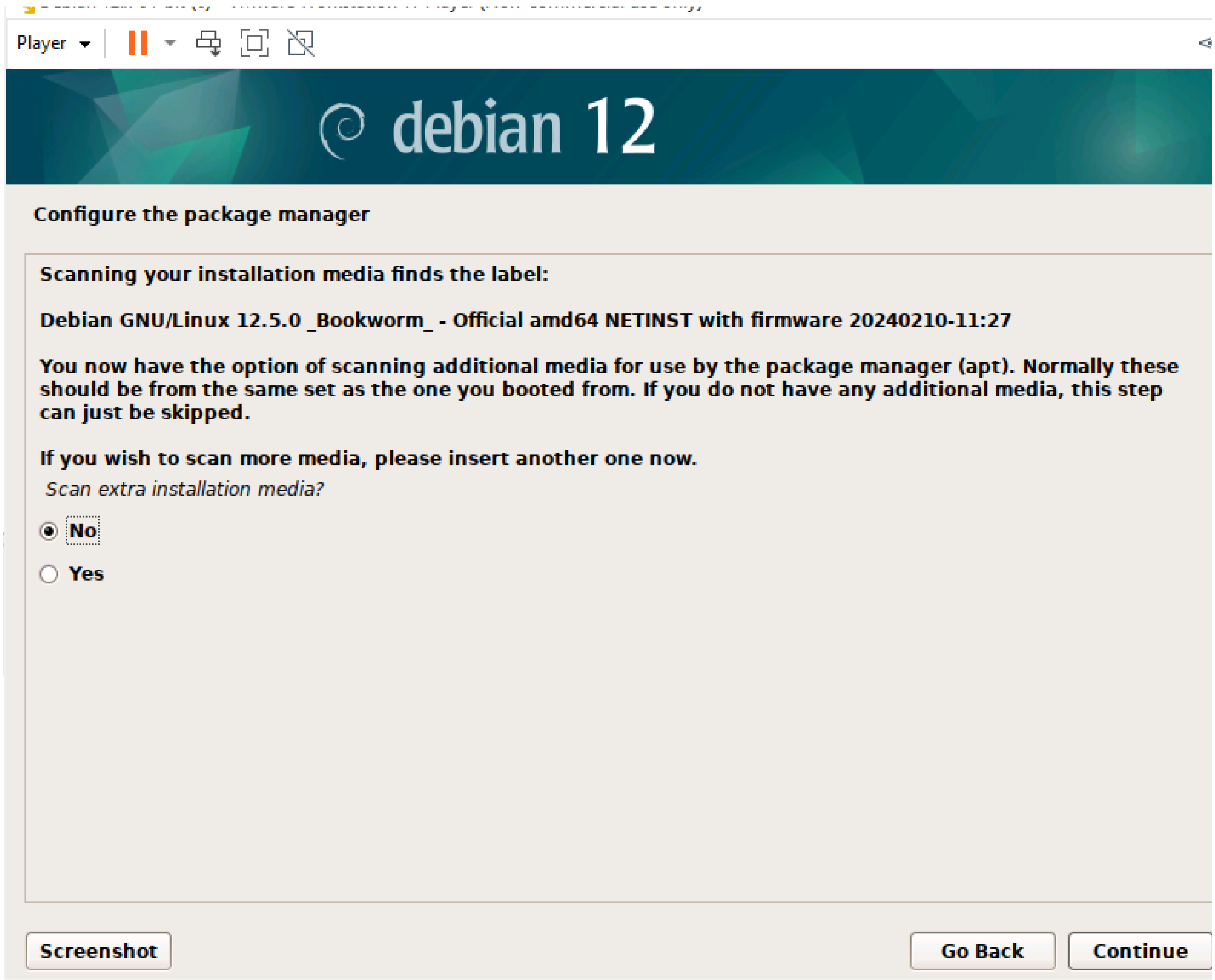
Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)

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

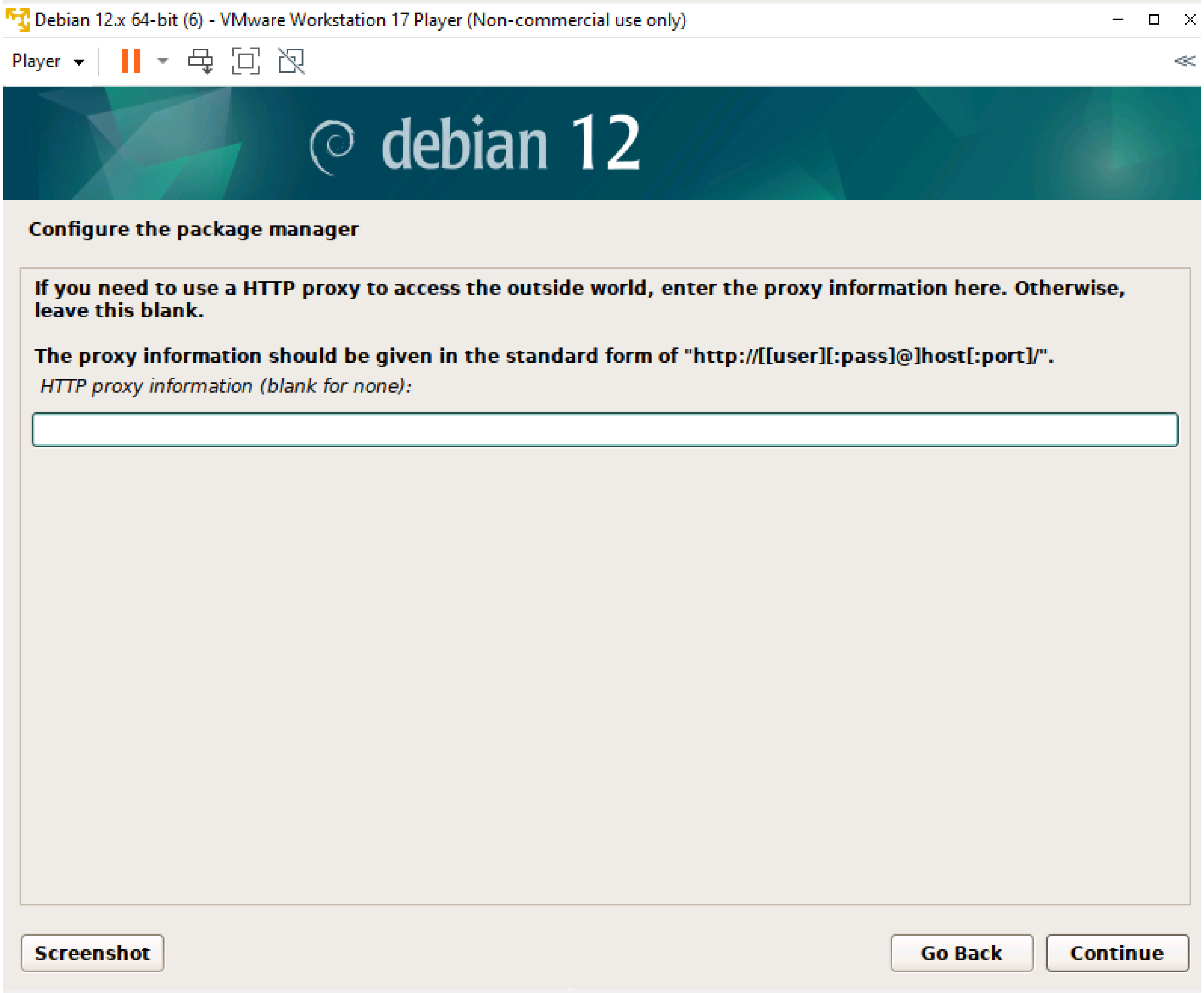
You now have the option of scanning additional media for use by the package manager (apt). Normally these should be from the same set as the one you booted from. If you do not have any additional media, this step can just be skipped.

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

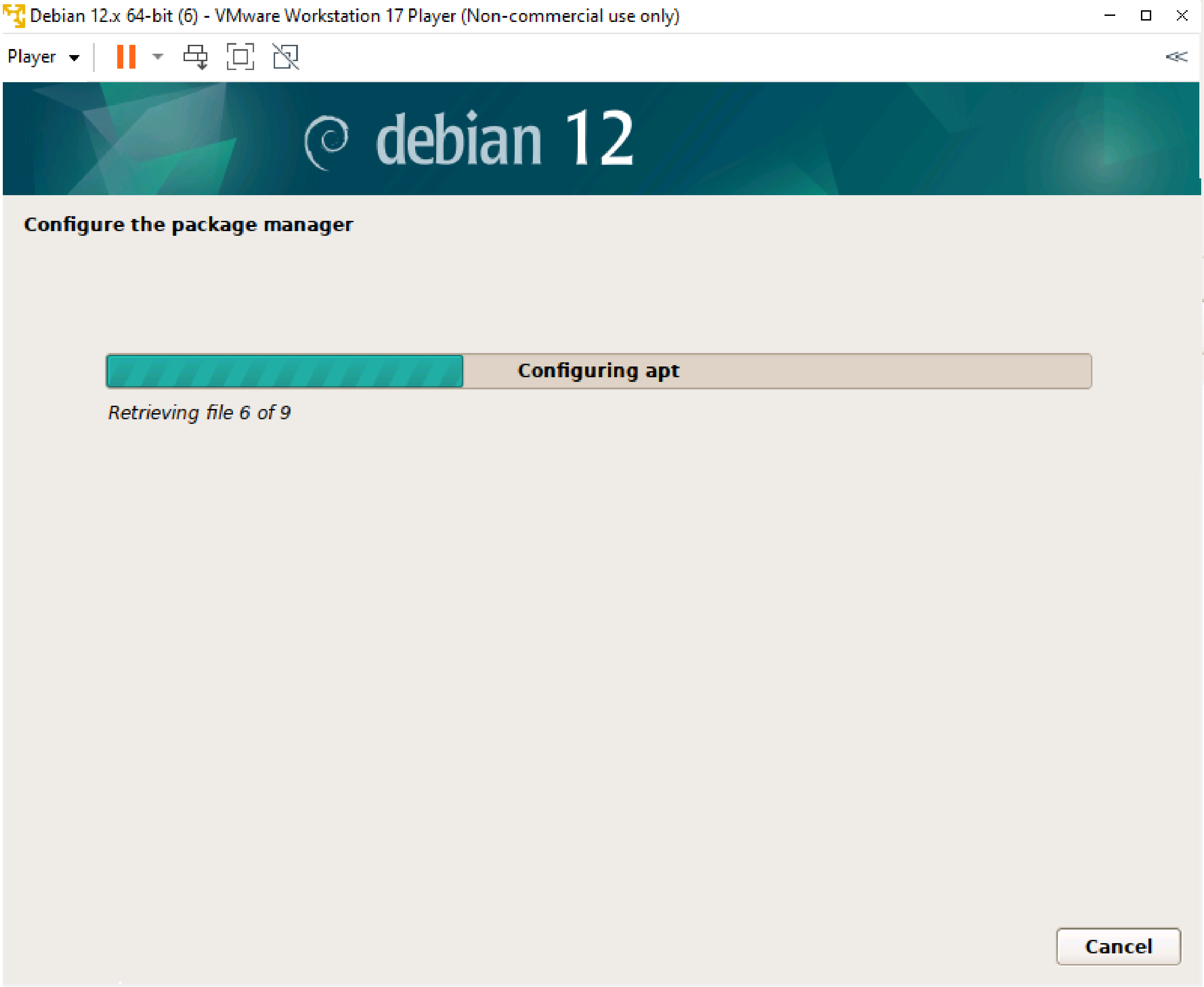
Configure the package manager

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

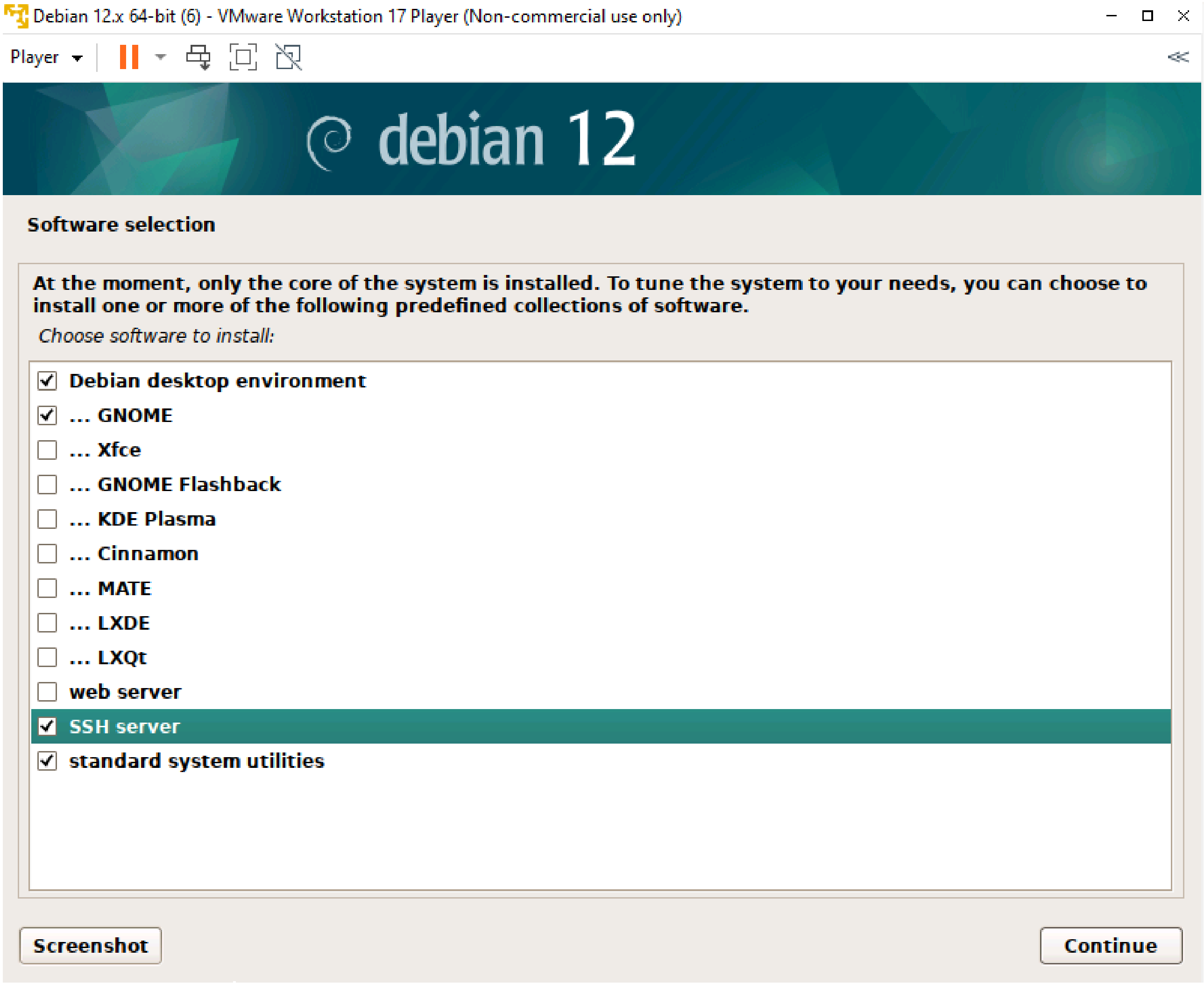

Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

Configure the package manager

Configuring apt

Retrieving file 6 of 9

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



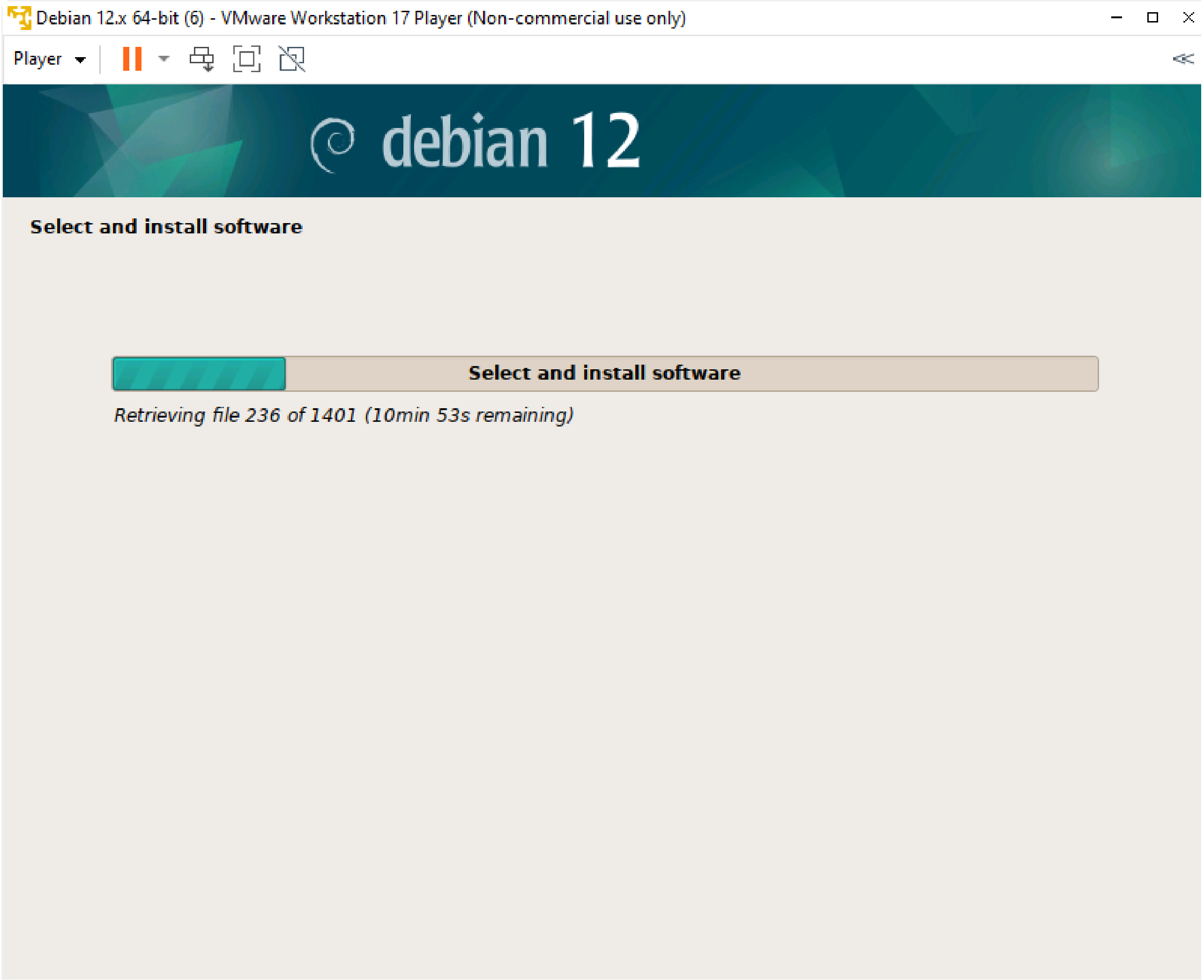
Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

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

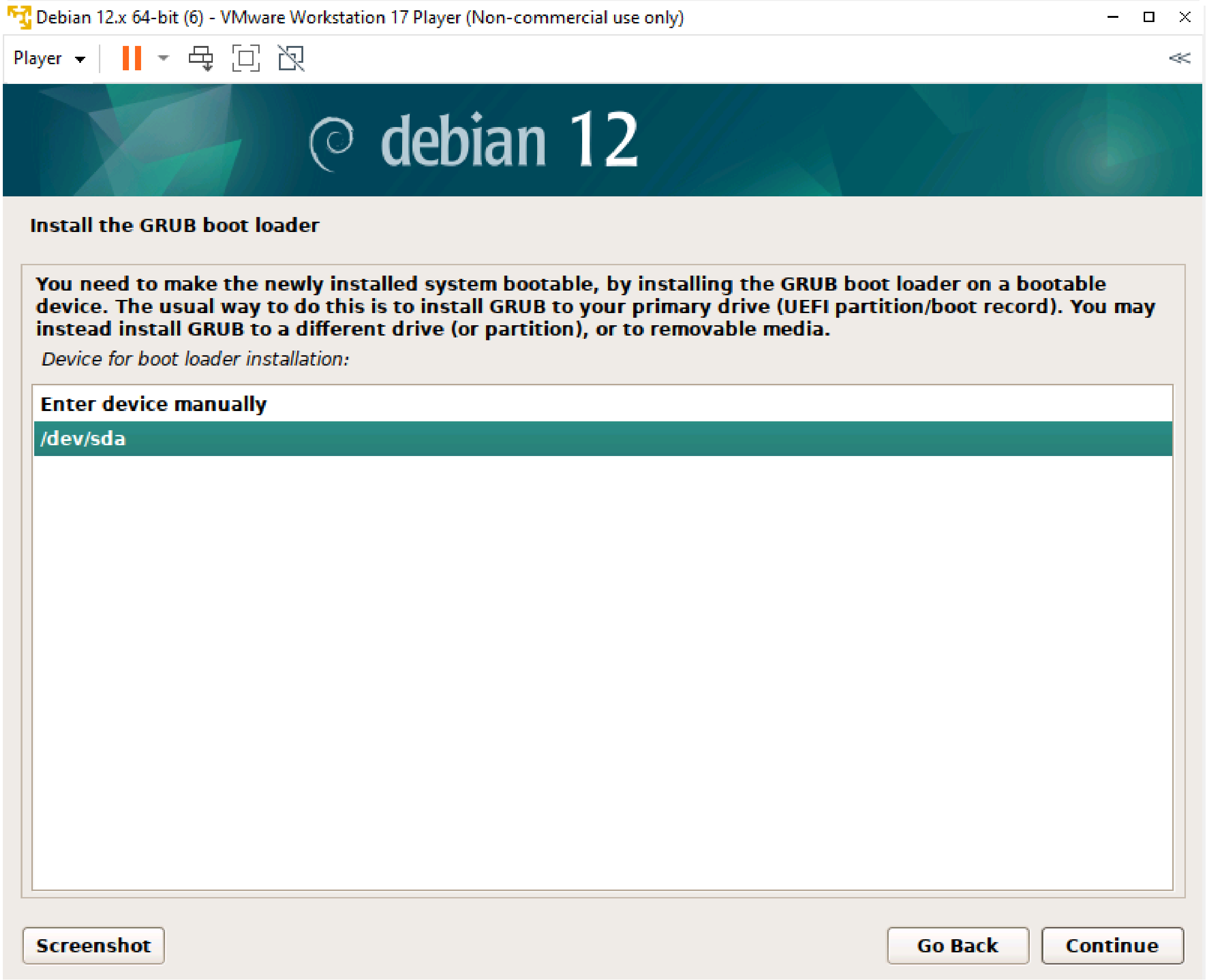


Debian 12.x 64-bit (6) - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12

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

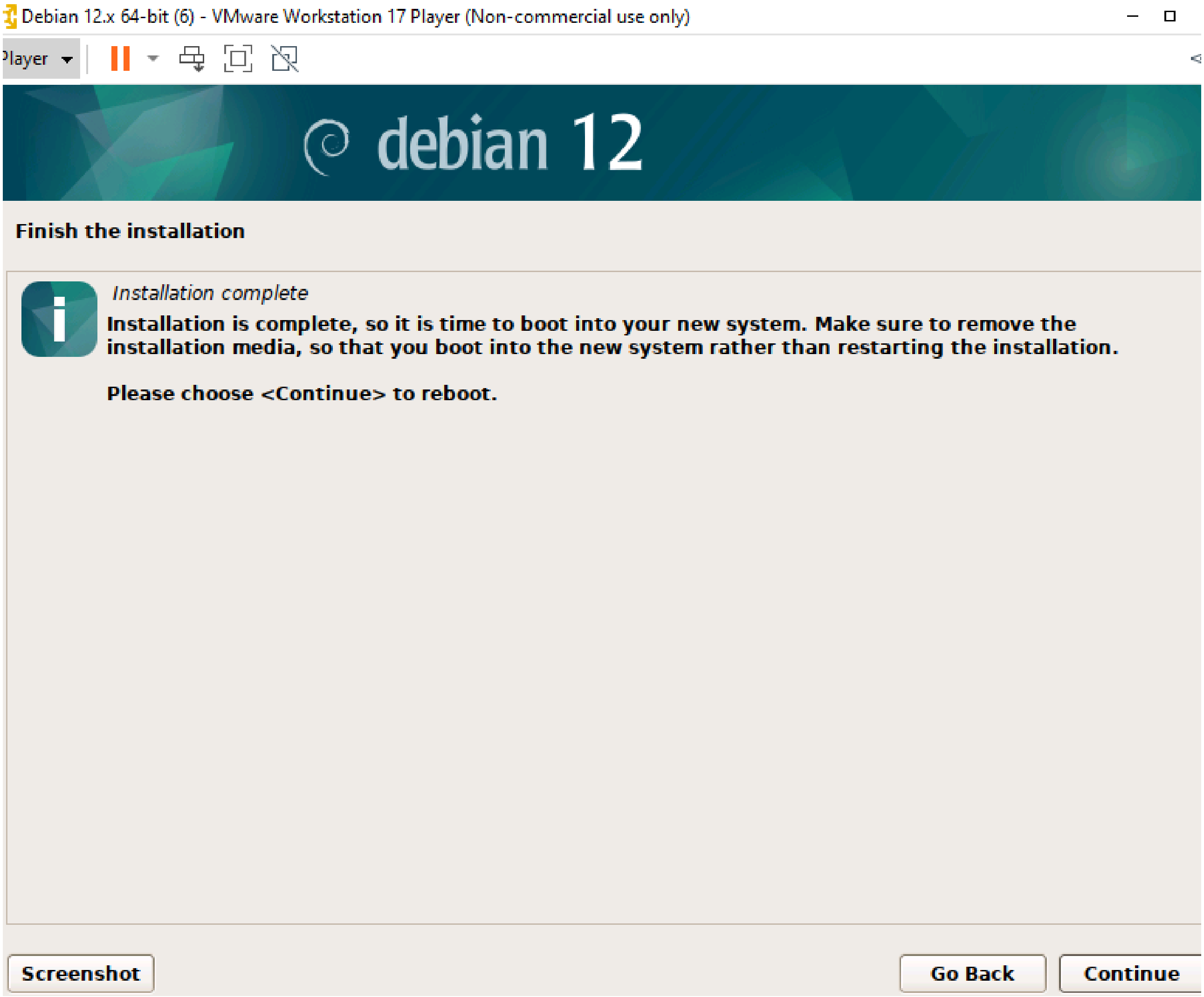
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

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

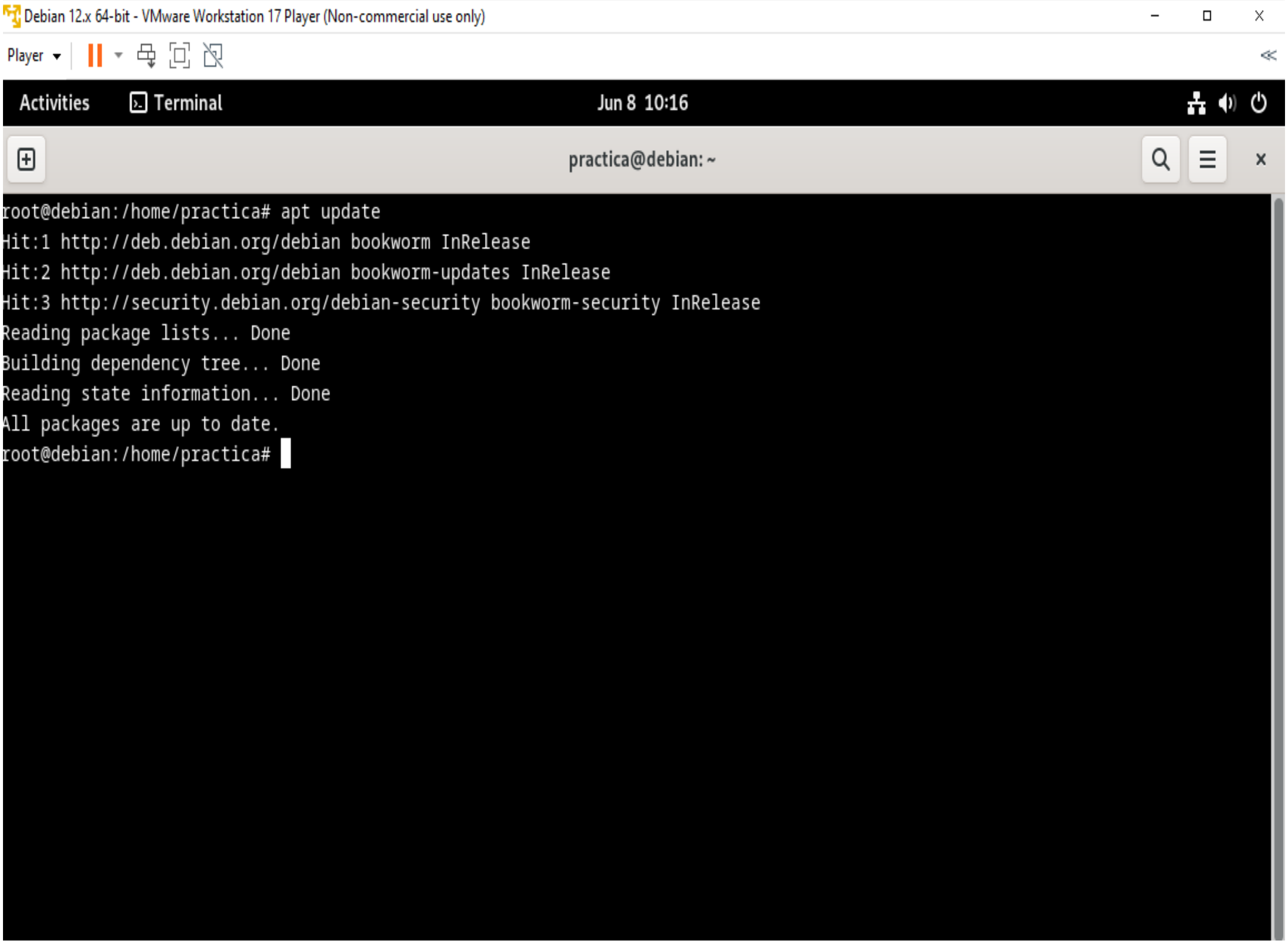
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

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:

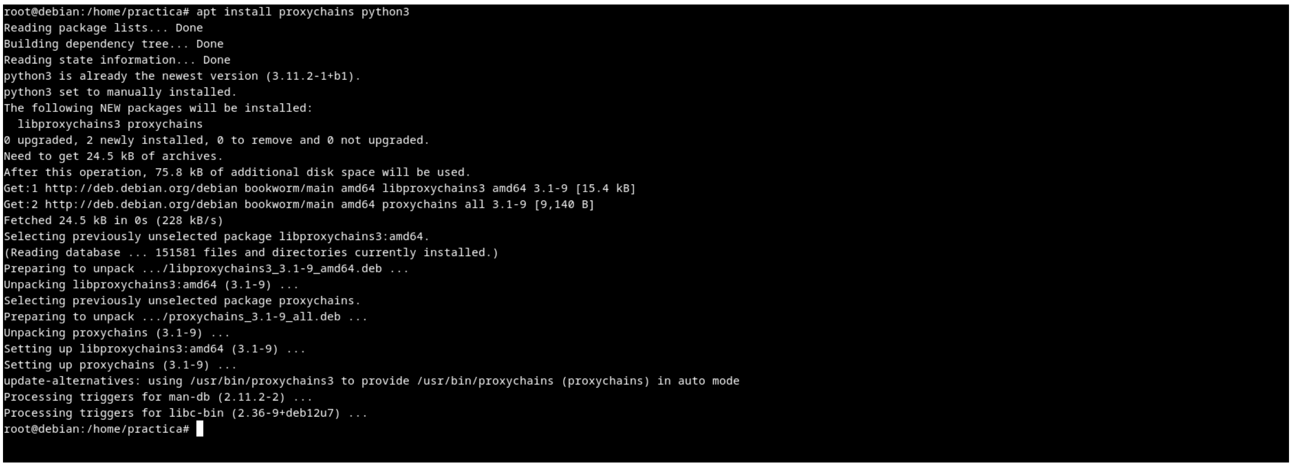
apt update


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#
```

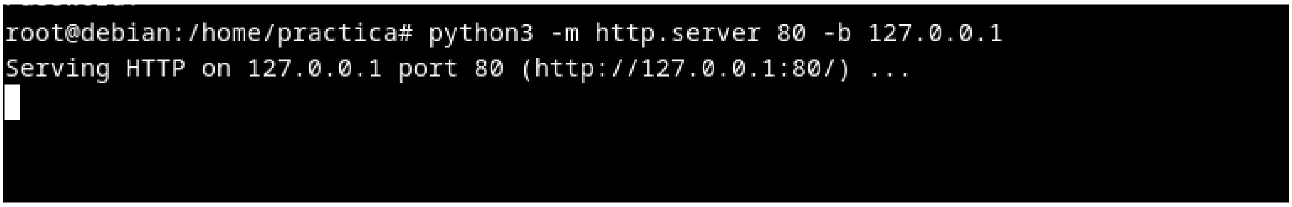
Instalo proxychains y python3

apt proxychains python3



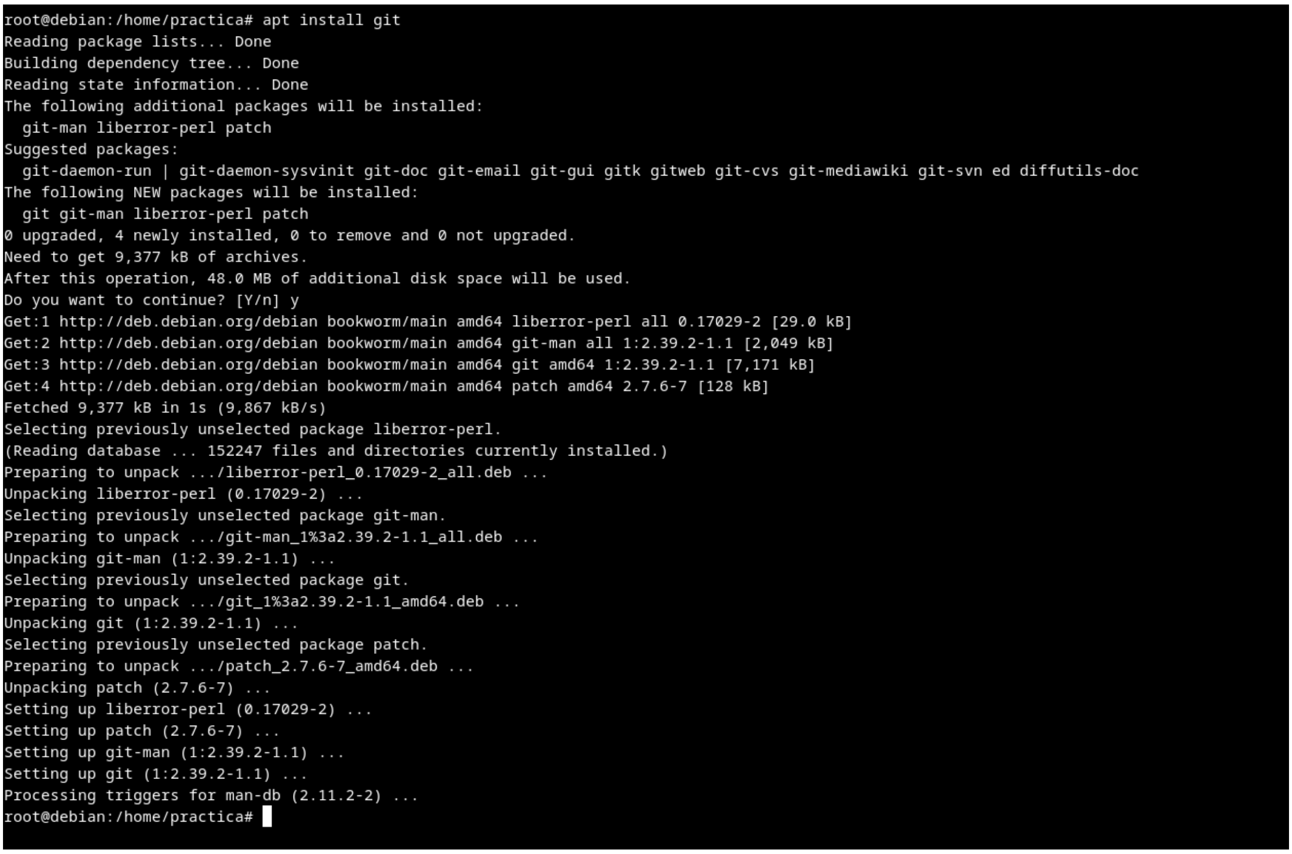
```
root@debian:/home/practica# apt install proxychains python3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.11.2-1+b1).
python3 set to manually installed.
The following NEW packages will be installed:
  libproxychains3 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



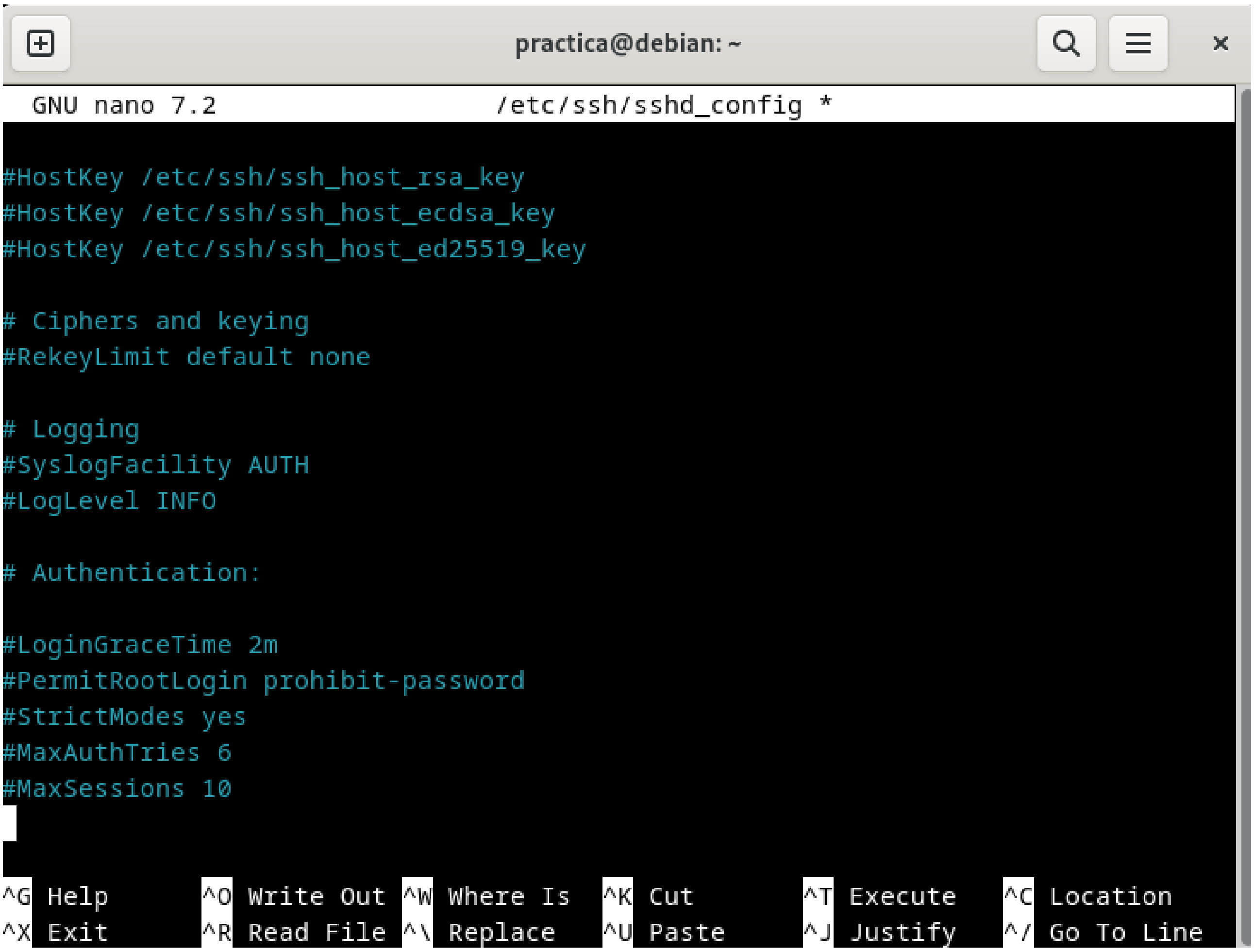
```
root@debian:/home/practica# python3 -m http.server 80 -b 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
```

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

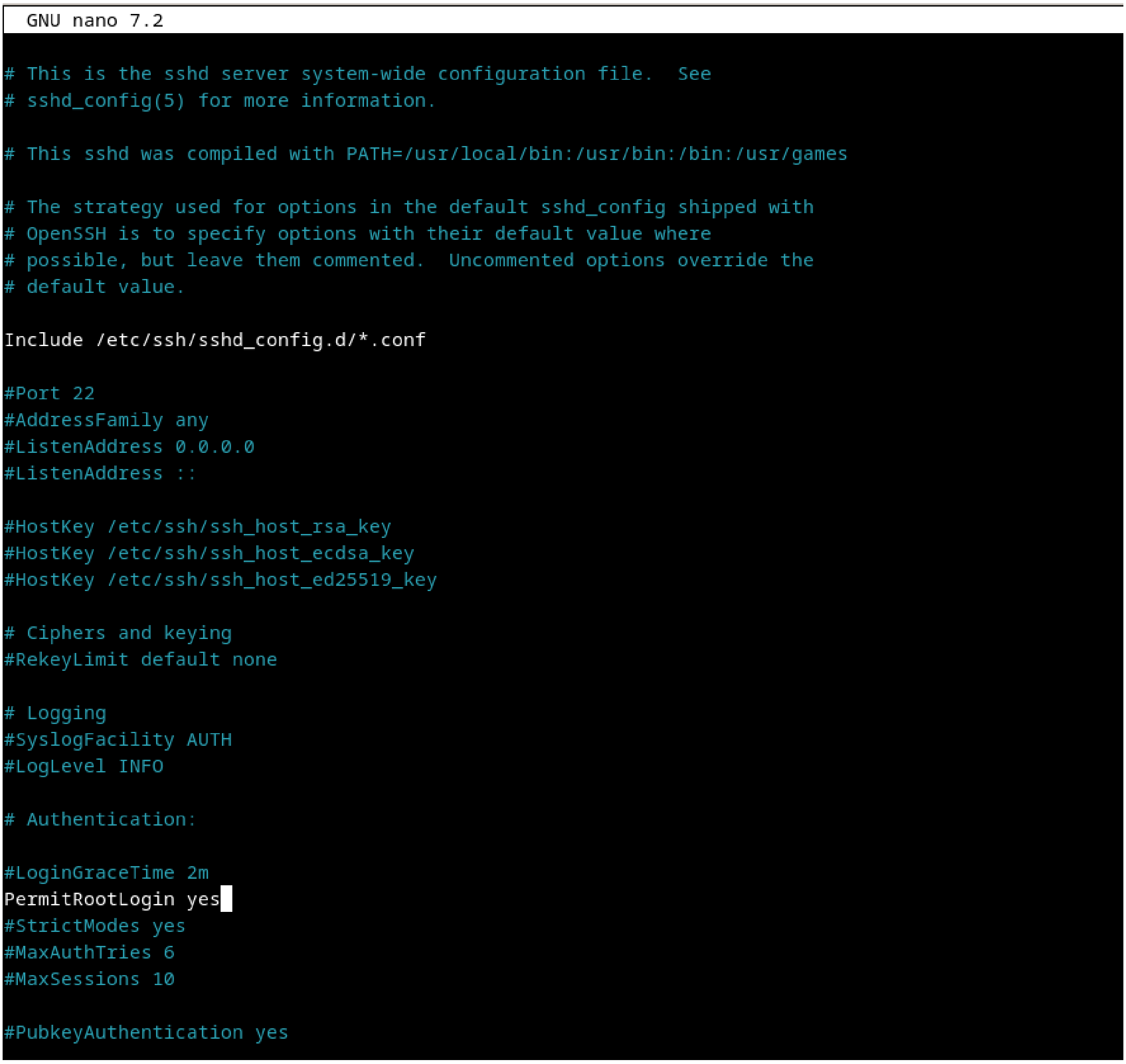


```
  GNU nano 7.2                    /etc/ssh/sshd_config *

#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

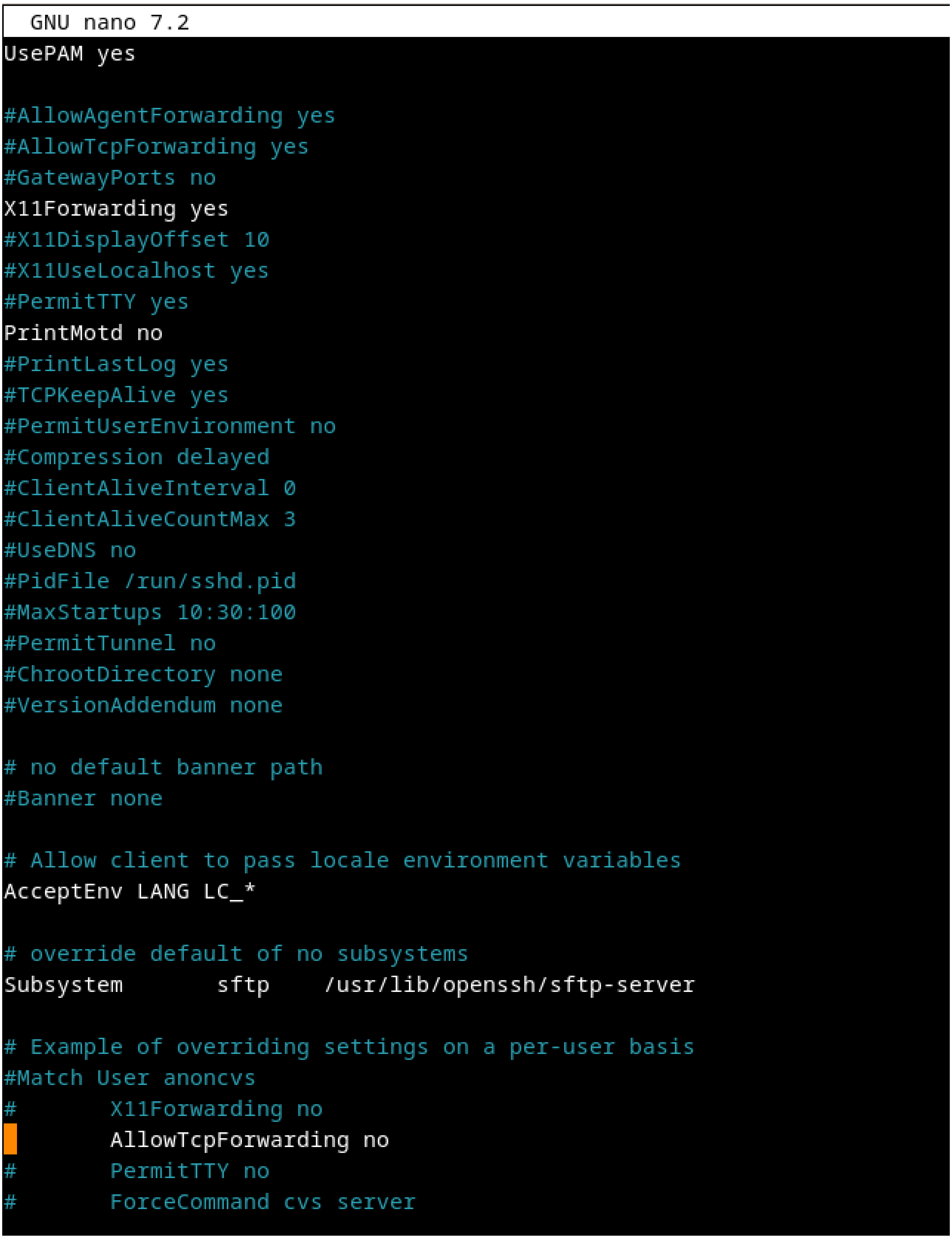
cambiamos la línea #PermitRootLogin prohibit-password por PermitRootLogin yes

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
```

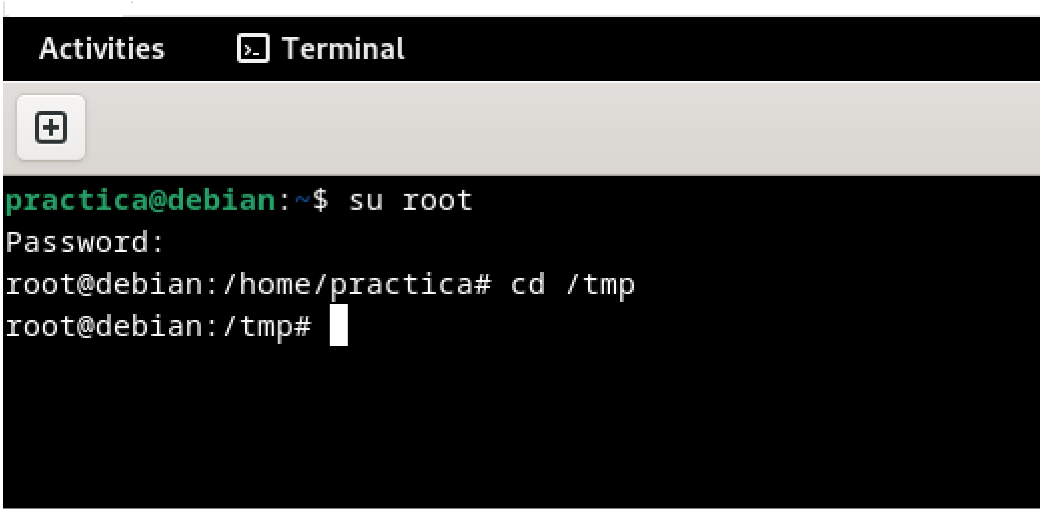
en AllowTcpFowarding no, quito la almohadilla para descomentar



```
  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

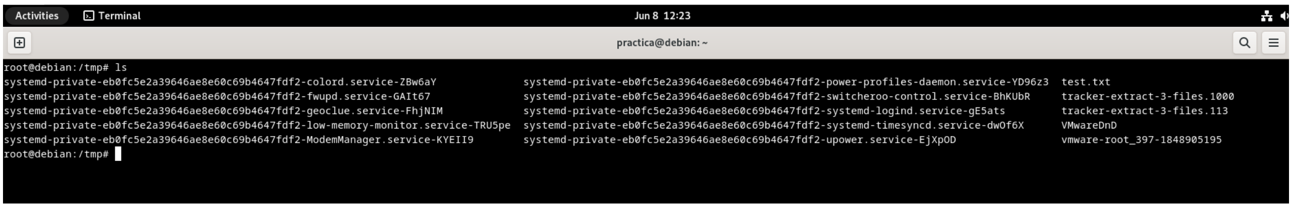


```
practica@debian:~$ su root
Password:
root@debian:/home/practica# cd /tmp
root@debian:/tmp#
```

creo un fichero test

echo “test” > test.txt

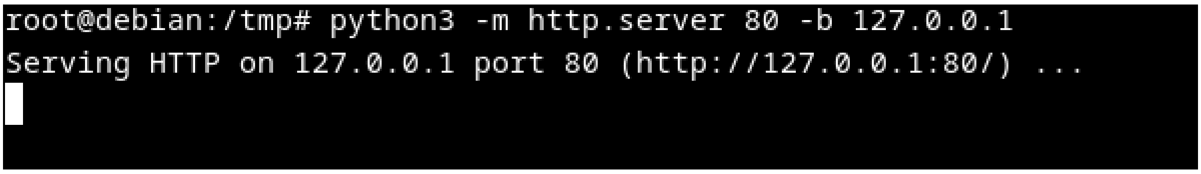
compruebo que se ha creado



```
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#
```

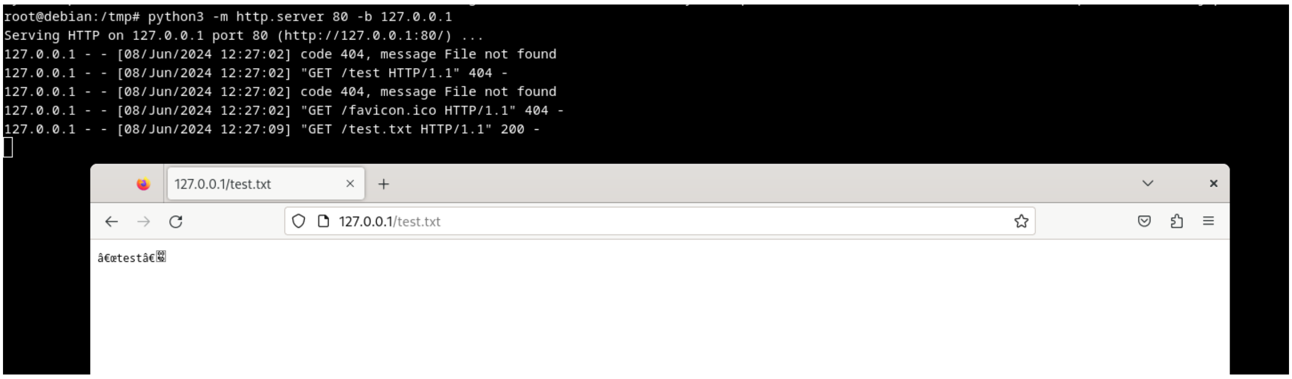
levanto el servidor:

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

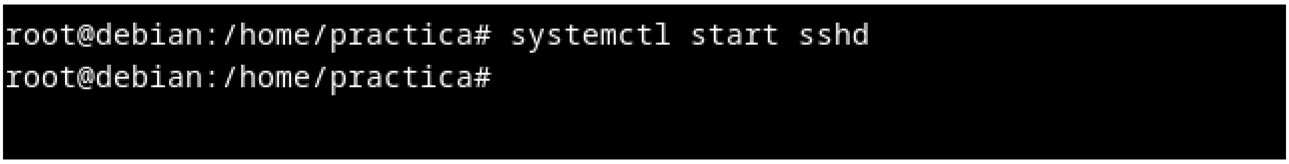


```
root@debian:/tmp# python3 -m http.server 80 -b 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
127.0.0.1 - - [08/Jun/2024 12:27:02] code 404, message File not found
127.0.0.1 - - [08/Jun/2024 12:27:02] "GET /test HTTP/1.1" 404 -
127.0.0.1 - - [08/Jun/2024 12:27:02] code 404,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

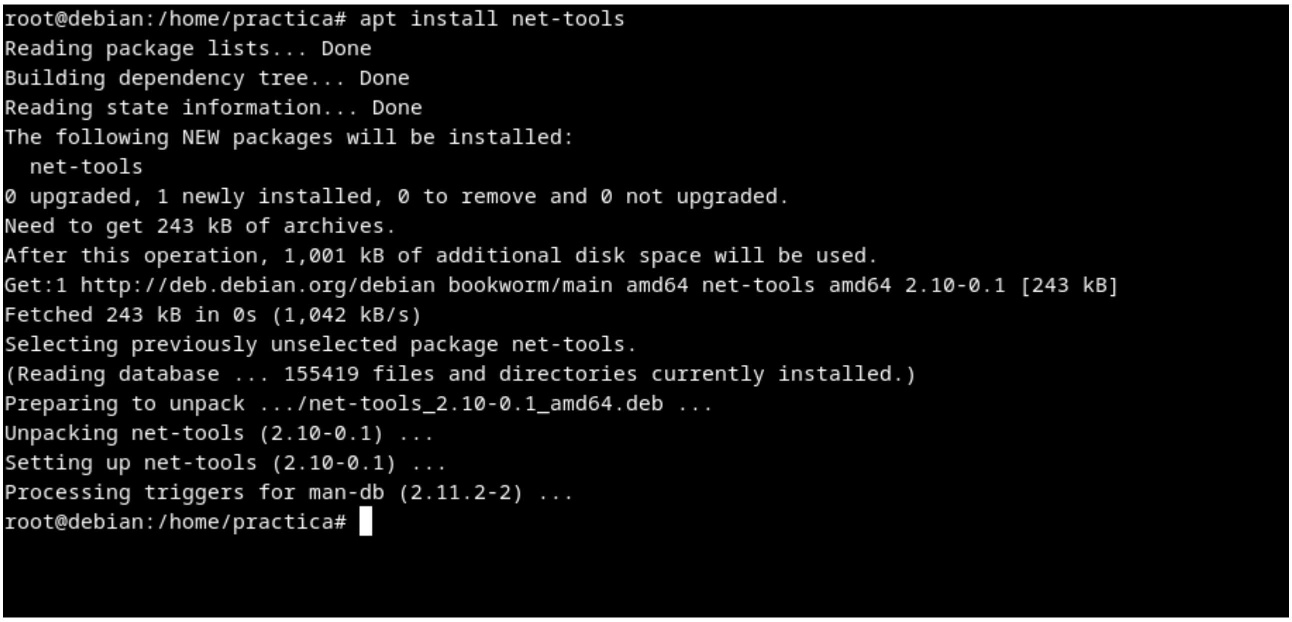
El objetivo es, desde otra máquina, poder leer este fichero test.txt

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



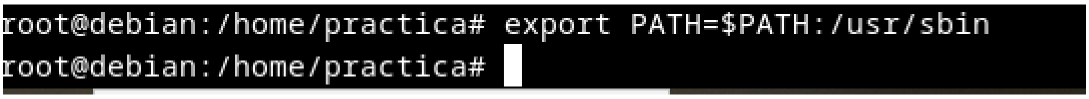
```
root@debian:/home/practica# systemctl start sshd
root@debian:/home/practica#
```

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



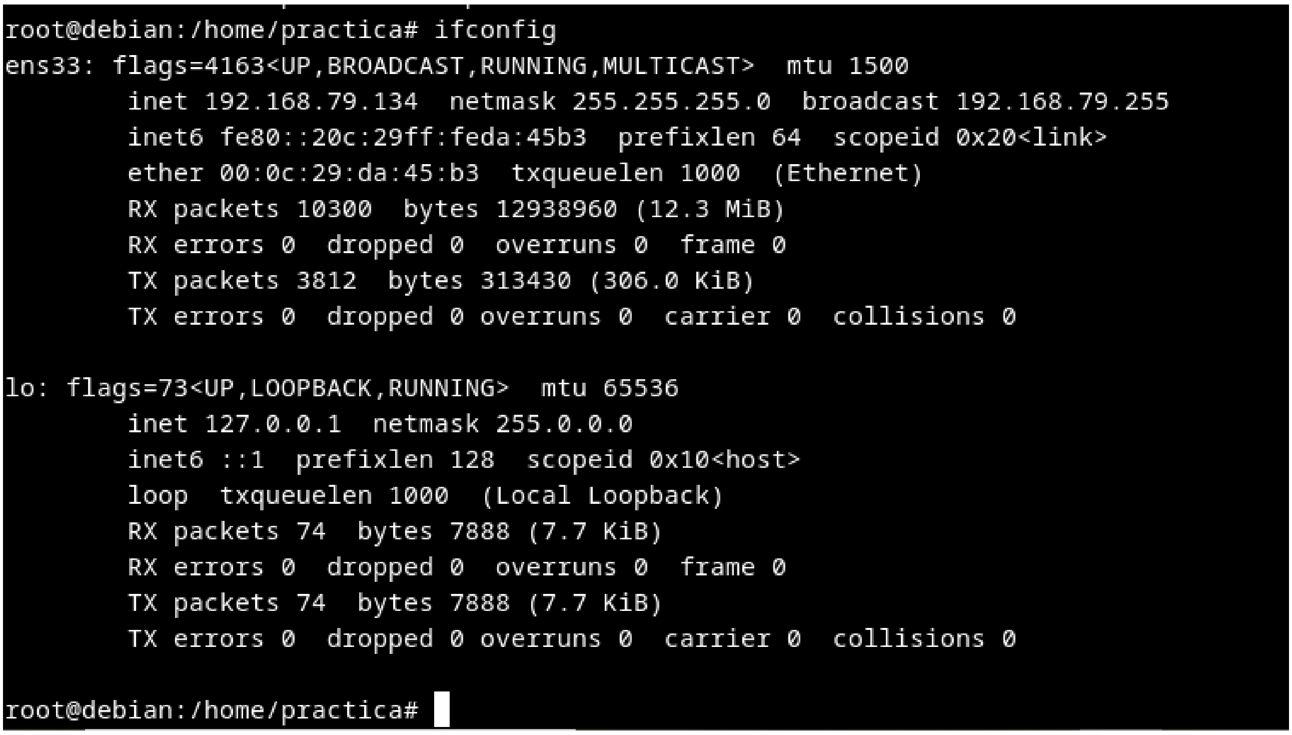
```
root@debian:/home/practica# apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 243 kB of archives.
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



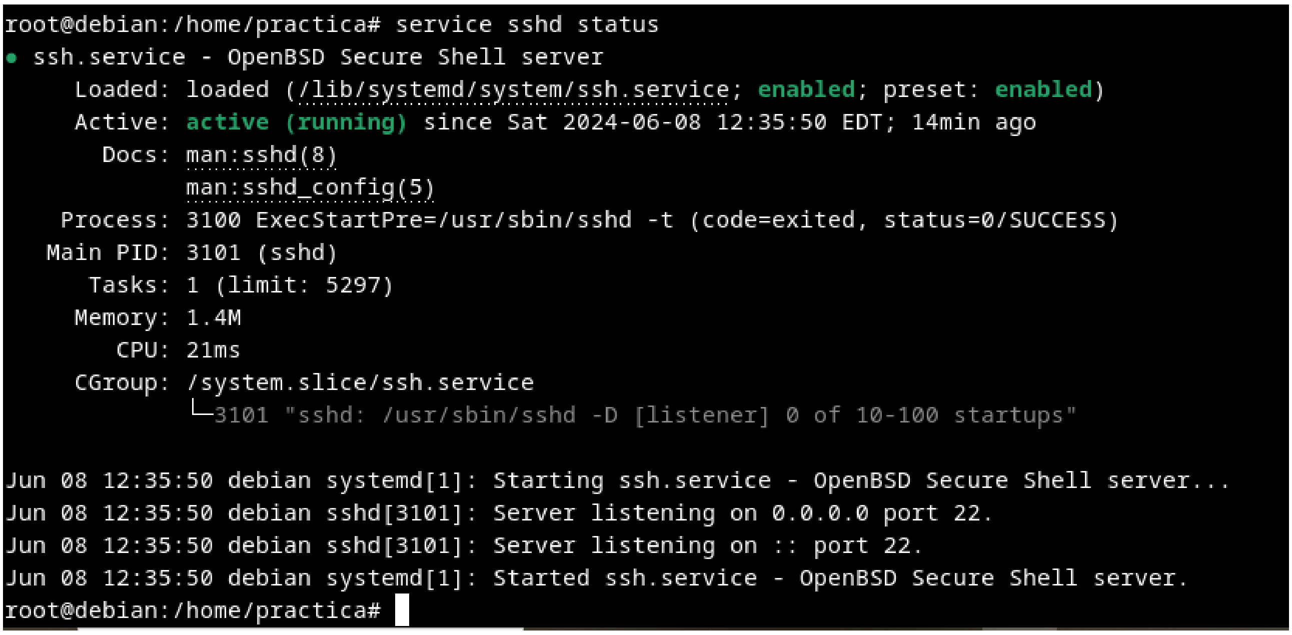
```
root@debian:/home/practica# export PATH=$PATH:/usr/sbin
root@debian:/home/practica# 
```

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#
```

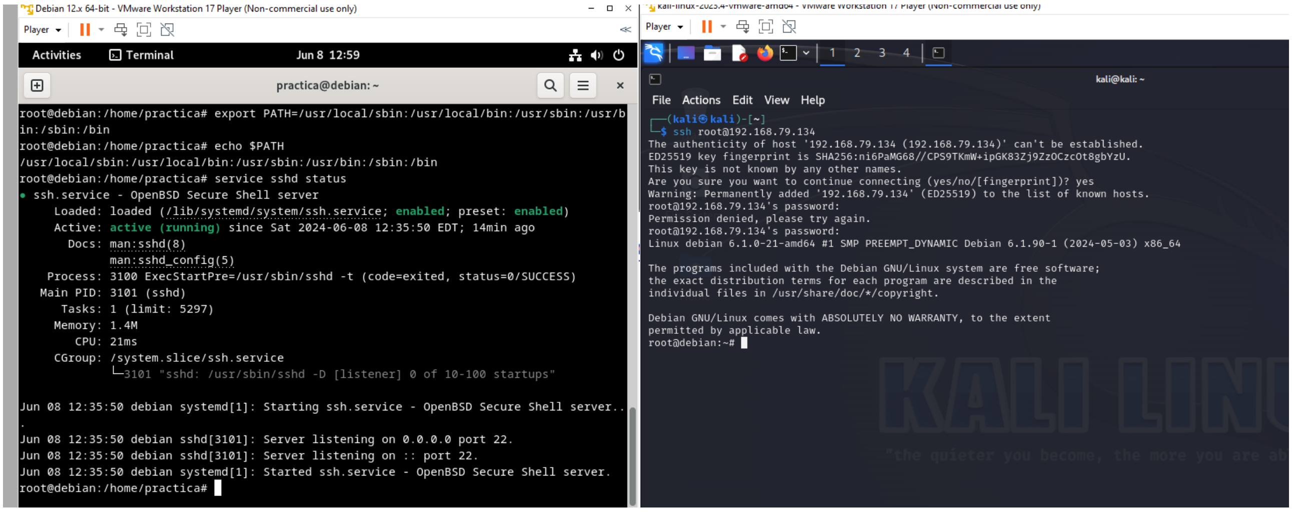
con service sshd status, compruebo que está levantado el servicio ssh, estando el active en verde



```
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

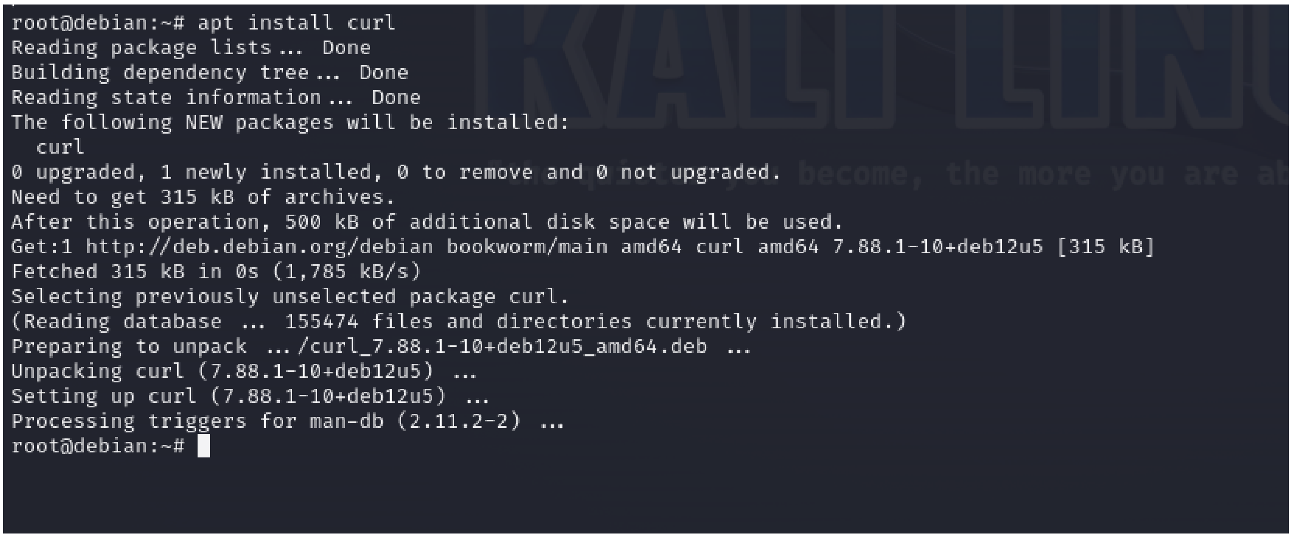
compruebo que la máquina atacante (Debian) se ha metido en la víctima (kali)


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# 
```

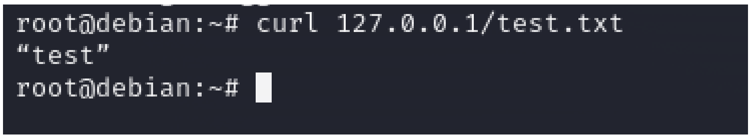
```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.79.134
The authenticity of host '192.168.79.134 (192.168.79.134)' can't be established.
ED25519 key fingerprint is SHA256:ni6PaMG68//CPS9TKmW+ipGK83Zj9ZzOCzcOt8gbYzU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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



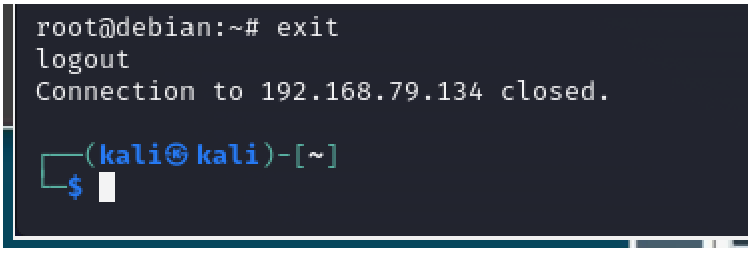
```
root@debian:~# apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 315 kB of archives.
After this operation, 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

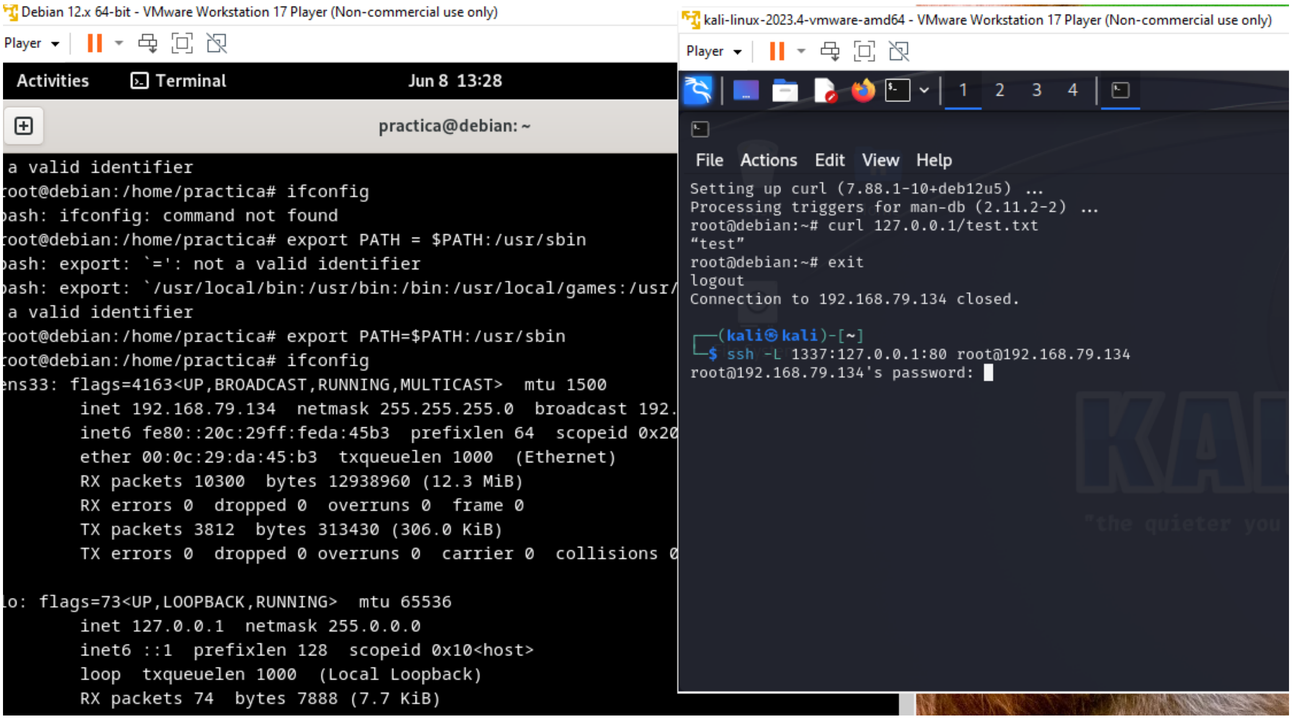


```
root@debian:~# exit
logout
Connection to 192.168.79.134 closed.

┌──(kali㉿kali)-[~]
└─$ 
```

ahora creo el tunel que conecte ambas máquinas, el puerto 1337 es la entrada del mismo. El 127.0.0.1 es la interface donde está el servicio ssh

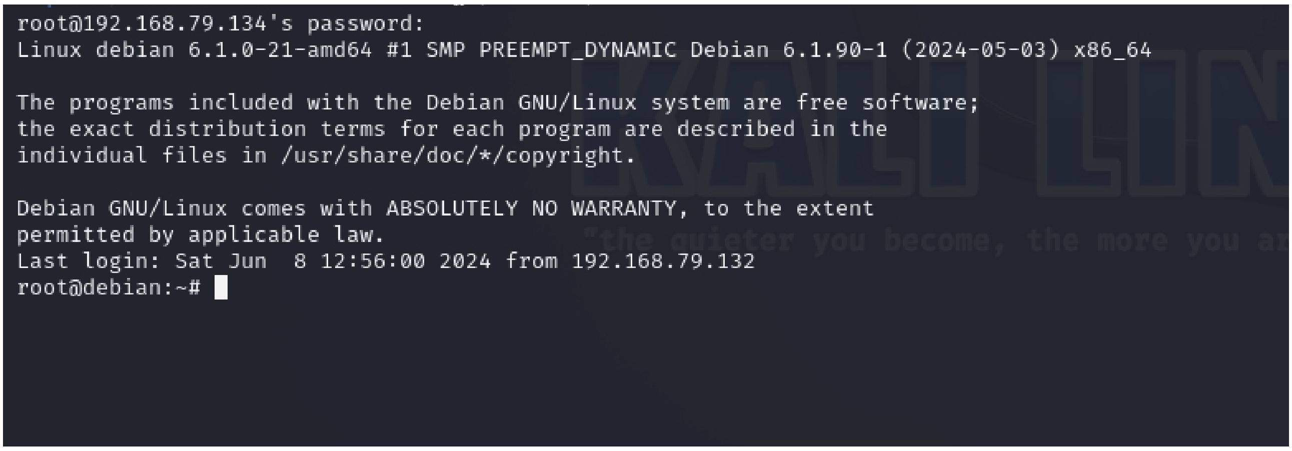
ssh -L 1337:127.0.0.1:80 root@192.168.79.134

el puerto 80 es la salida del túnel,


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Jun 8 13:28
practica@debian: ~
kali-linux-2023.4-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1
2
3
4
File
Actions
Edit
View
Help

```
 a valid identifier
root@debian:/home/practica# ifconfig
bash: ifconfig: command not found
root@debian:/home/practica# export PATH = $PATH:/usr/sbin
bash: export: `=': not a valid identifier
bash: export: `/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/
 a valid identifier
root@debian:/home/practica# export PATH=$PATH:/usr/sbin
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.
        inet6 fe80::20c:29ff:feda:45b3  prefixlen 64  scopeid 0x20
        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)
```

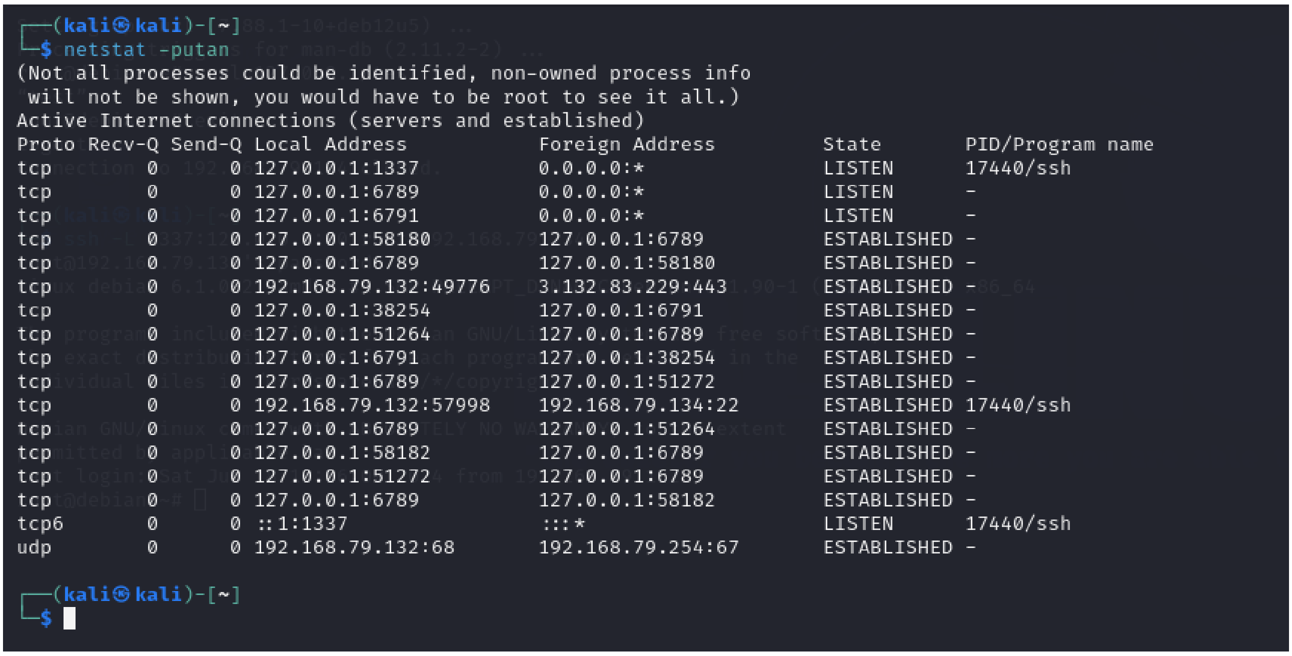
```
Setting up curl (7.88.1-10+deb12u5) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:~# curl 127.0.0.1/test.txt
“test”
root@debian:~# exit
logout
Connection to 192.168.79.134 closed.

┌──(kali㉿kali)-[~]
└─$ ssh -L 1337:127.0.0.1:80 root@192.168.79.134
root@192.168.79.134's password: 
```



```
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.
Last login: Sat Jun  8 12:56:00 2024 from 192.168.79.132
root@debian:~# 
```

en este punto está el túnel hecho.

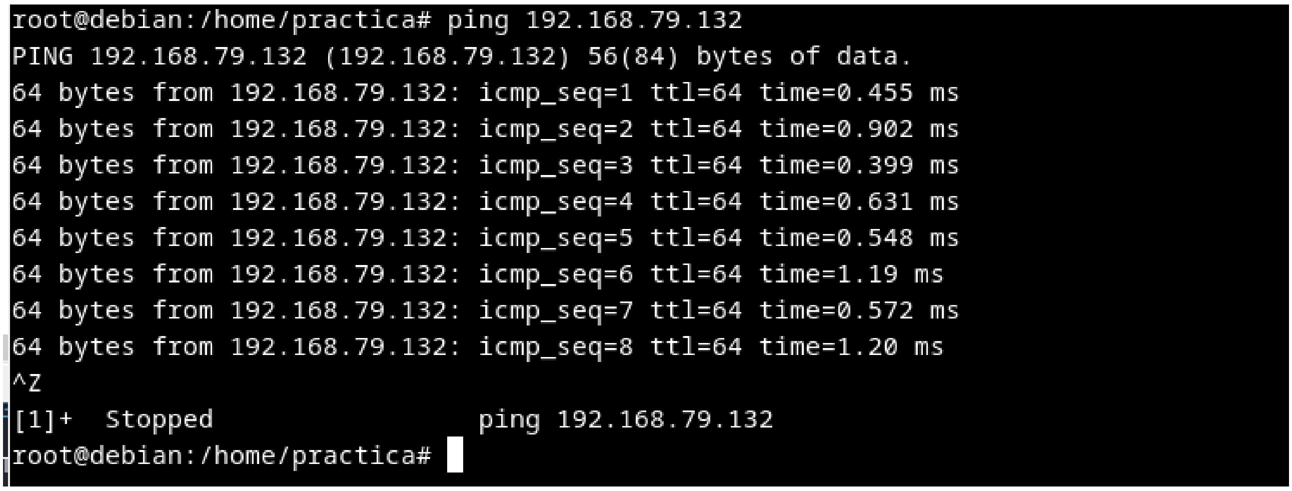
Abro una nueva terminal y ejecuto netstat -putan



```
┌──(kali㉿kali)-[~]
└─$ netstat -putan
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:1337          0.0.0.0:*               LISTEN      17440/ssh
tcp        0      0 127.0.0.1:6789          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6791          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:58180         127.0.0.1:6789          ESTABLISHED -
tcp        0      0 127.0.0.1:6789          127.0.0.1:58180         ESTABLISHED -
tcp        0      0 192.168.79.132:49776    3.132.83.229:443        ESTABLISHED -
tcp        0      0 127.0.0.1:38254         127.0.0.1:6791          ESTABLISHED -
tcp        0      0 127.0.0.1:51264         127.0.0.1:6789          ESTABLISHED -
tcp        0      0 127.0.0.1:6791          127.0.0.1:38254         ESTABLISHED -
tcp        0      0 127.0.0.1:6789          127.0.0.1:51272         ESTABLISHED -
tcp        0      0 192.168.79.132:57998    192.168.79.134:22       ESTABLISHED 17440/ssh
tcp        0      0 127.0.0.1:6789          127.0.0.1:51264         ESTABLISHED -
tcp        0      0 127.0.0.1:58182         127.0.0.1:6789          ESTABLISHED -
tcp        0      0 127.0.0.1:51272         127.0.0.1:6789          ESTABLISHED -
tcp        0      0 127.0.0.1:6789          127.0.0.1:58182         ESTABLISHED -
tcp6       0      0 ::1:1337                :::*                    LISTEN      17440/ssh
udp        0      0 192.168.79.132:68       192.168.79.254:67       ESTABLISHED -

┌──(kali㉿kali)-[~]
└─$ 
```

aquí podemos ver las conexiones, vemos la 127.0.0.1:1337 en modo LISTEN (escucha) el servicio ssh

hago un ping en mi máquina debian para confirmar que tienen visibilidad debian y kali:



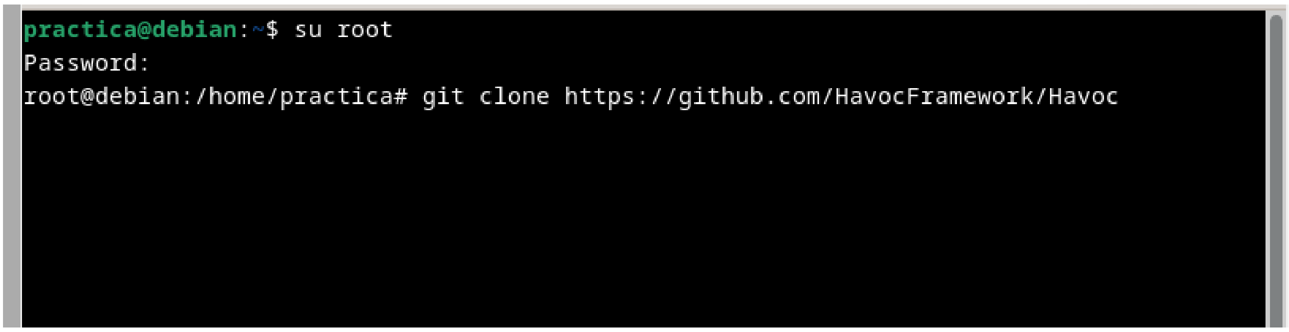
```
root@debian:/home/practica# ping 192.168.79.132
PING 192.168.79.132 (192.168.79.132) 56(84) bytes of data.
64 bytes from 192.168.79.132: icmp_seq=1 ttl=64 time=0.455 ms
64 bytes from 192.168.79.132: icmp_seq=2 ttl=64 time=0.902 ms
64 bytes from 192.168.79.132: icmp_seq=3 ttl=64 time=0.399 ms
64 bytes from 192.168.79.132: icmp_seq=4 ttl=64 time=0.631 ms
64 bytes from 192.168.79.132: icmp_seq=5 ttl=64 time=0.548 ms
64 bytes from 192.168.79.132: icmp_seq=6 ttl=64 time=1.19 ms
64 bytes from 192.168.79.132: icmp_seq=7 ttl=64 time=0.572 ms
64 bytes from 192.168.79.132: icmp_seq=8 ttl=64 time=1.20 ms
^Z
[1]+  Stopped                 ping 192.168.79.132
root@debian:/home/practica# 
```

Command and Control:

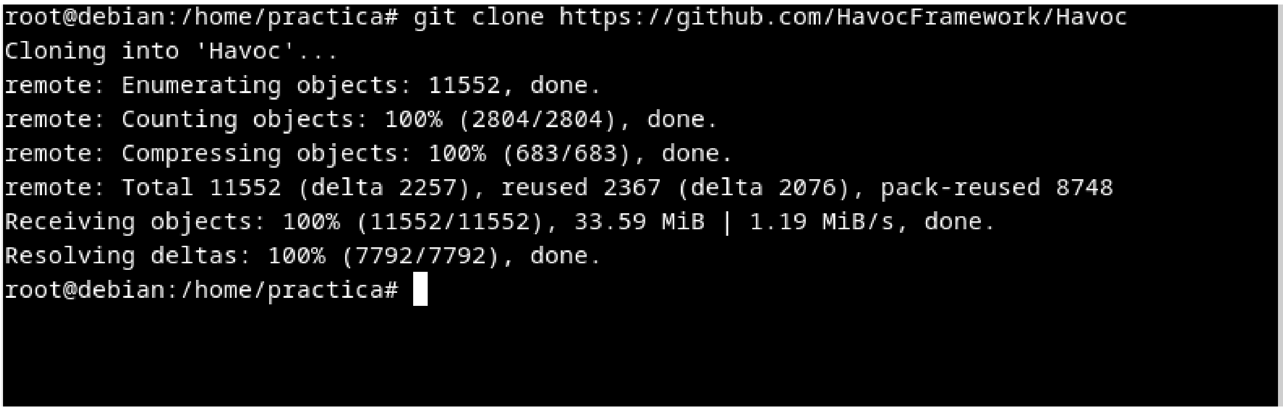
Voy a utilizar, dentro de Windows 10, la carpeta Programdata porque sé con seguridad que va a estar en el sistema, que existe.

Hago un git clone de Havoc en debian:

git clone HavocFramework/Havoc: The Havoc Framework. (github.com)



```
practica@debian:~$ su root
Password:
root@debian:/home/practica# git clone https://github.com/HavocFramework/Havoc
```

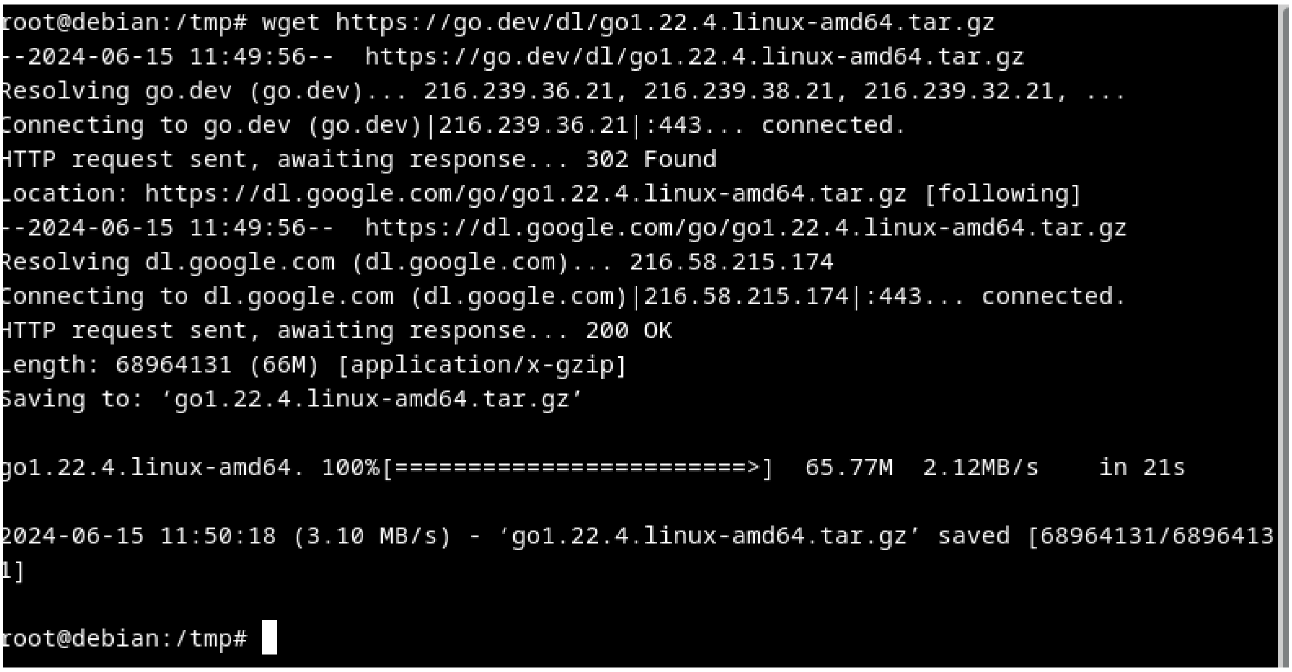


```
root@debian:/home/practica# git clone https://github.com/HavocFramework/Havoc
Cloning into 'Havoc'...
remote: Enumerating objects: 11552, done.
remote: Counting objects: 100% (2804/2804), done.
remote: Compressing objects: 100% (683/683), done.
remote: Total 11552 (delta 2257), reused 2367 (delta 2076), pack-reused 8748
Receiving objects: 100% (11552/11552), 33.59 MiB | 1.19 MiB/s, done.
Resolving deltas: 100% (7792/7792), done.
root@debian:/home/practica# 
```

voy a /tmp

lanzo este comando:

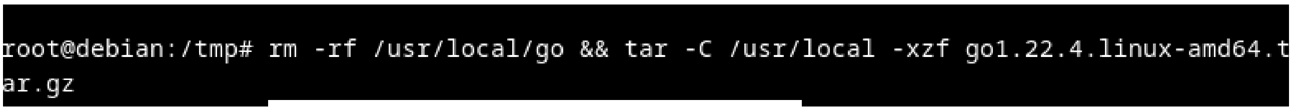
wget https://go.dev/dl/go1.22.4.linux-amd64.tar.gz



```
root@debian:/tmp# wget https://go.dev/dl/go1.22.4.linux-amd64.tar.gz
--2024-06-15 11:49:56--  https://go.dev/dl/go1.22.4.linux-amd64.tar.gz
Resolving go.dev (go.dev)... 216.239.36.21, 216.239.38.21, 216.239.32.21, ...
Connecting to go.dev (go.dev)|216.239.36.21|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://dl.google.com/go/go1.22.4.linux-amd64.tar.gz [following]
--2024-06-15 11:49:56--  https://dl.google.com/go/go1.22.4.linux-amd64.tar.gz
Resolving dl.google.com (dl.google.com)... 216.58.215.174
Connecting to dl.google.com (dl.google.com)|216.58.215.174|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68964131 (66M) [application/x-gzip]
Saving to: ‘go1.22.4.linux-amd64.tar.gz’

go1.22.4.linux-amd64. 100%[=======================>]  65.77M  2.12MB/s    in 21s

2024-06-15 11:50:18 (3.10 MB/s) - ‘go1.22.4.linux-amd64.tar.gz’ saved [68964131/6896413
1]

root@debian:/tmp# 
```

lanzo este:

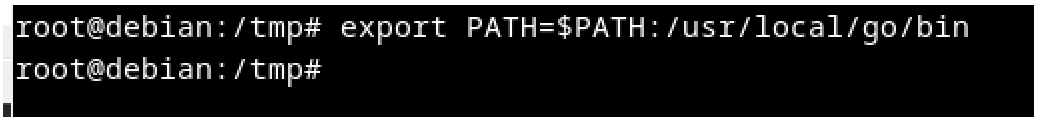
rm -rf /usr/local/go && tar -C /usr/local -xzf go1.22.4.linux-amd64.tar.gz



```
root@debian:/tmp# rm -rf /usr/local/go && tar -C /usr/local -xzf go1.22.4.linux-amd64.t
ar.gz
```

luego lanzo este:

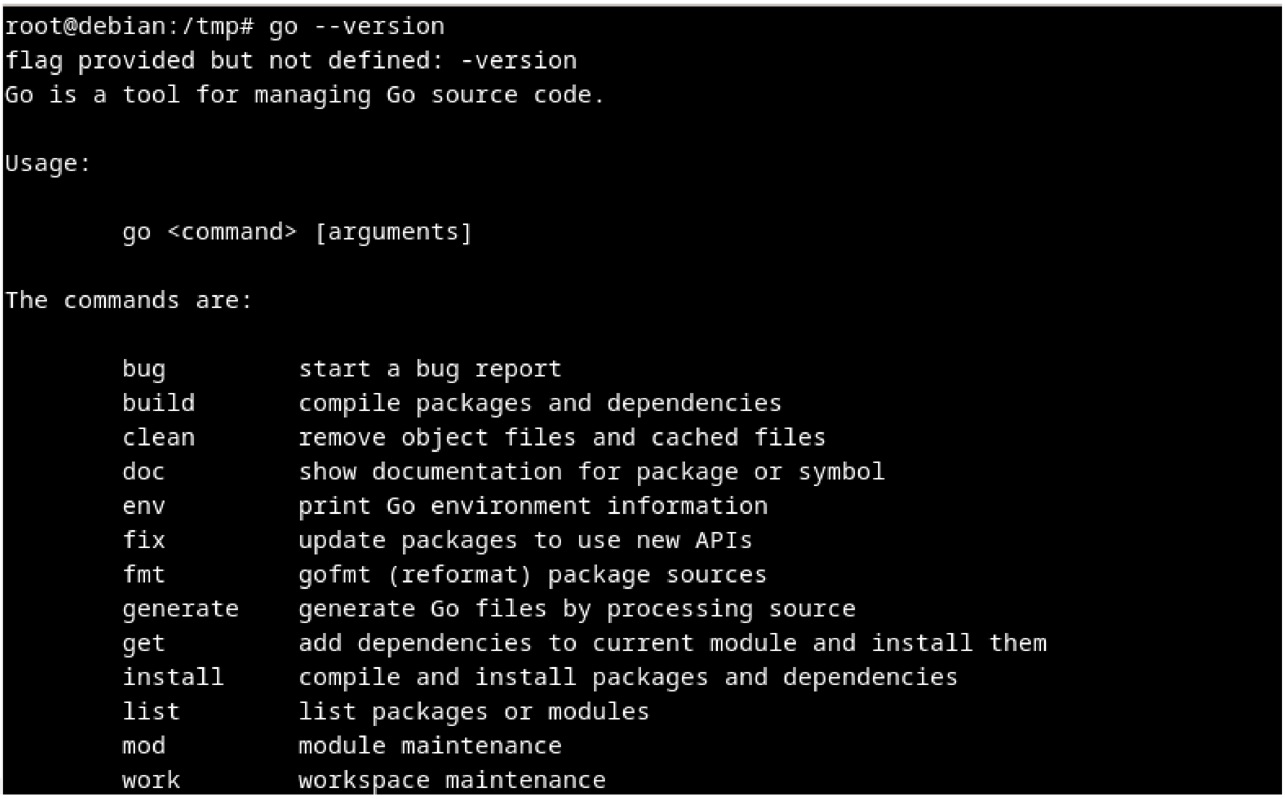
export PATH=$PATH:/usr/local/go/bin



```
root@debian:/tmp# export PATH=$PATH:/usr/local/go/bin
root@debian:/tmp#
```

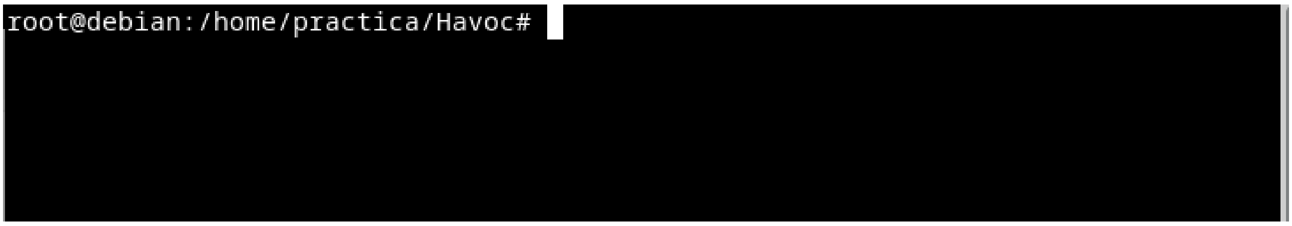
a continuación lanzo:

go --version



```
root@debian:/tmp# go --version
flag provided but not defined: -version
Go is a tool for managing Go source code.

Usage:

        go <command> [arguments]

The commands are:

        bug         start a bug report
        build       compile packages and dependencies
        clean       remove object files and cached files
        doc         show documentation for package or symbol
        env         print Go environment information
        fix         update packages to use new APIs
        fmt         gofmt (reformat) package sources
        generate    generate Go files by processing source
        get         add dependencies to current module and install them
        install     compile and install packages and dependencies
        list        list packages or modules
        mod         module maintenance
        work        workspace maintenance
```

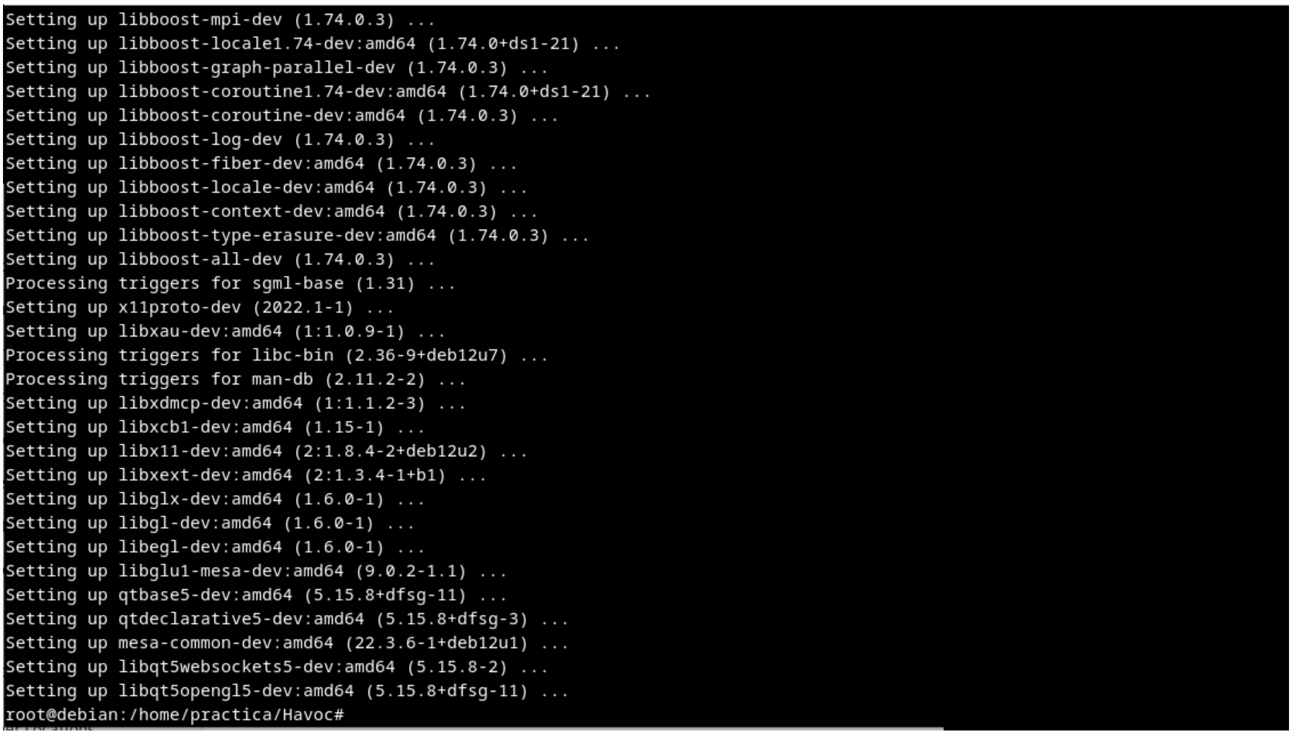
me muevo a la carpeta Havoc:



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

luego lanzo este comando:

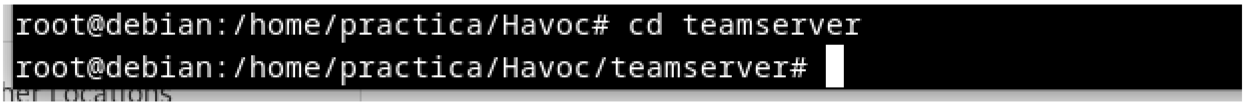
apt install -y git build-essential apt-utils cmake libfontconfig1 libglu1-mesa-dev libgtest-dev libspdlog-dev libboost-all-dev libncurses5-dev libgdbm-dev libssl-dev libreadline-dev libffi-dev libsqlite3-dev libbz2-dev mesa-common-dev qtbase5-dev qtchooser qt5-qmake qtbase5-dev-tools libqt5websockets5 libqt5websockets5-dev qtdeclarative5-dev golang-go qtbase5-dev libqt5websockets5-dev python3-dev libboost-all-dev mingw-w64 nasm



```
Setting up libboost-mpi-dev (1.74.0.3) ...
Setting up libboost-locale1.74-dev:amd64 (1.74.0+ds1-21) ...
Setting up libboost-graph-parallel-dev (1.74.0.3) ...
Setting up libboost-coroutine1.74-dev:amd64 (1.74.0+ds1-21) ...
Setting up libboost-coroutine-dev:amd64 (1.74.0.3) ...
Setting up libboost-log-dev (1.74.0.3) ...
Setting up libboost-fiber-dev:amd64 (1.74.0.3) ...
Setting up libboost-locale-dev:amd64 (1.74.0.3) ...
Setting up libboost-context-dev:amd64 (1.74.0.3) ...
Setting up libboost-type-erasure-dev:amd64 (1.74.0.3) ...
Setting up libboost-all-dev (1.74.0.3) ...
Processing triggers for sgml-base (1.31) ...
Setting up x11proto-dev (2022.1-1) ...
Setting up libxau-dev:amd64 (1:1.0.9-1) ...
Processing triggers for libc-bin (2.36-9+deb12u7) ...
Processing triggers for man-db (2.11.2-2) ...
Setting up libxdmcp-dev:amd64 (1:1.1.2-3) ...
Setting up libxcb1-dev:amd64 (1.15-1) ...
Setting up libx11-dev:amd64 (2:1.8.4-2+deb12u2) ...
Setting up libxext-dev:amd64 (2:1.3.4-1+b1) ...
Setting up libglx-dev:amd64 (1.6.0-1) ...
Setting up libgl-dev:amd64 (1.6.0-1) ...
Setting up libegl-dev:amd64 (1.6.0-1) ...
Setting up libglu1-mesa-dev:amd64 (9.0.2-1.1) ...
Setting up qtbase5-dev:amd64 (5.15.8+dfsg-11) ...
Setting up qtdeclarative5-dev:amd64 (5.15.8+dfsg-3) ...
Setting up mesa-common-dev:amd64 (22.3.6-1+deb12u1) ...
Setting up libqt5websockets5-dev:amd64 (5.15.8-2) ...
Setting up libqt5opengl5-dev:amd64 (5.15.8+dfsg-11) ...
root@debian:/home/practica/Havoc#
```

luego cambio a teamserver

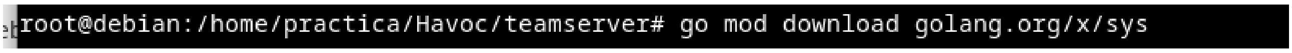
cd teamserver



```
root@debian:/home/practica/Havoc# cd teamserver
root@debian:/home/practica/Havoc/teamserver#
```

lanzo este comando:

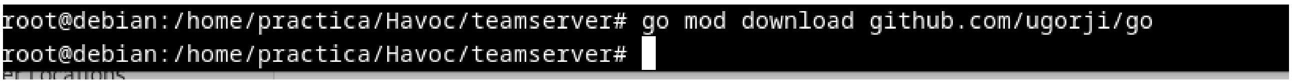
go mod download golang.org/x/sys



```
root@debian:/home/practica/Havoc/teamserver# go mod download golang.org/x/sys
```

y luego:

go mod download github.com/ugorji/go

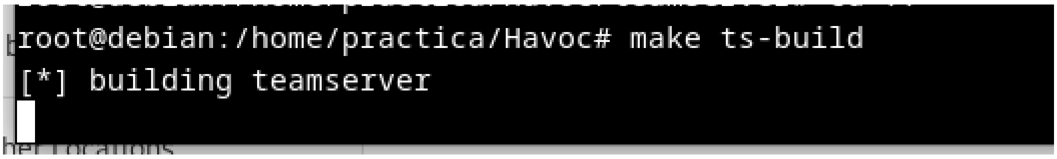


```
root@debian:/home/practica/Havoc/teamserver# go mod download github.com/ugorji/go
root@debian:/home/practica/Havoc/teamserver#
```

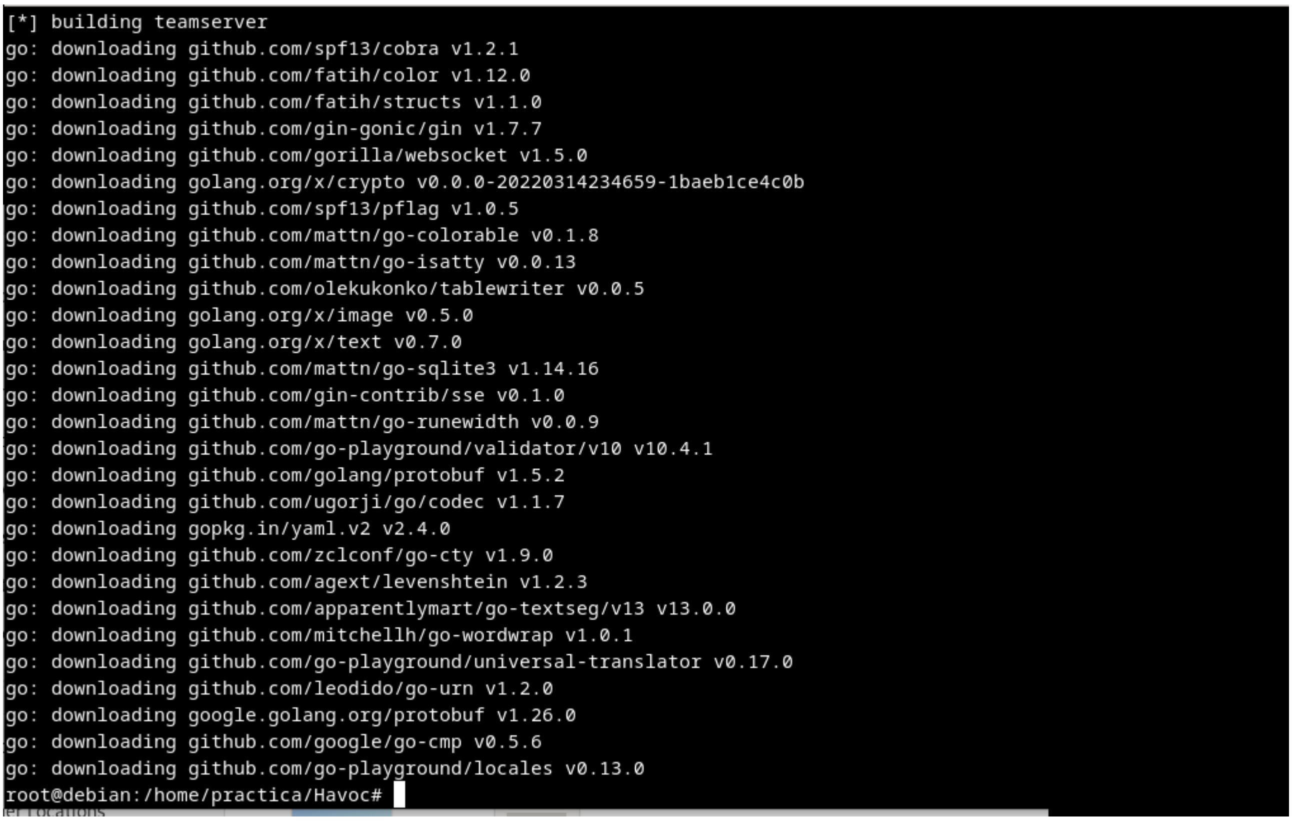
cd ..

make ts-build

aquí está compilando teamserver

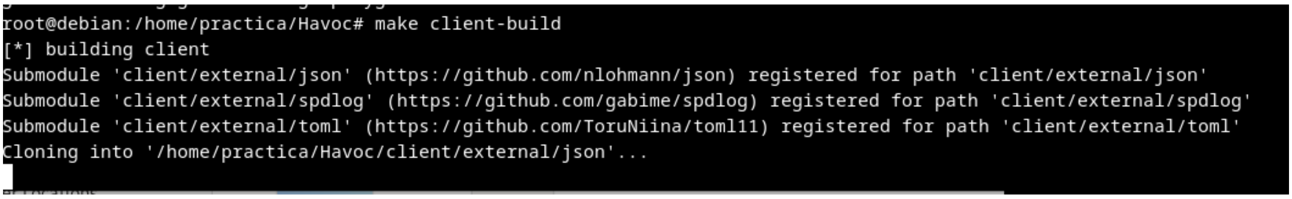


```
root@debian:/home/practica/Havoc# make ts-build
[*] building teamserver
```

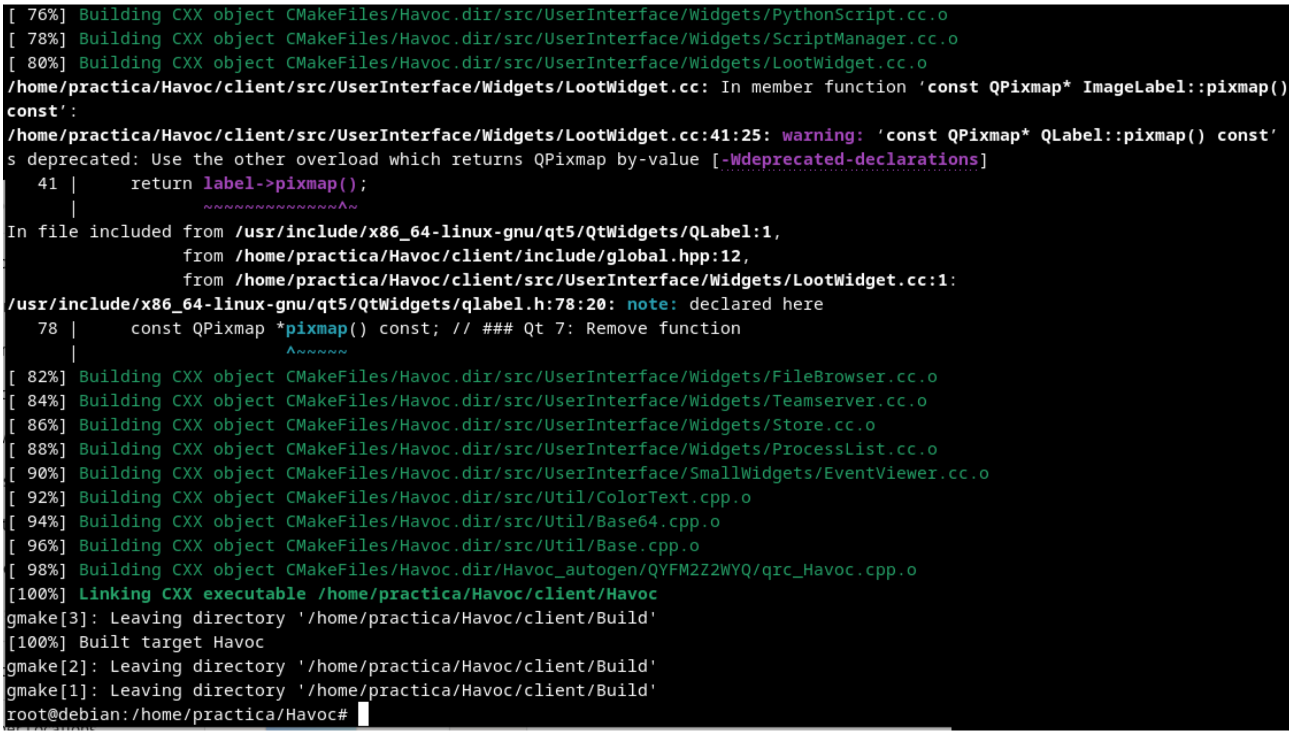


```
[*] building teamserver
go: downloading github.com/spf13/cobra v1.2.1
go: downloading github.com/fatih/color v1.12.0
go: downloading github.com/fatih/structs v1.1.0
go: downloading github.com/gin-gonic/gin v1.7.7
go: downloading github.com/gorilla/websocket v1.5.0
go: downloading golang.org/x/crypto v0.0.0-20220314234659-1baeb1ce4c0b
go: downloading github.com/spf13/pflag v1.0.5
go: downloading github.com/mattn/go-colorable v0.1.8
go: downloading github.com/mattn/go-isatty v0.0.13
go: downloading github.com/olekukonko/tablewriter v0.0.5
go: downloading golang.org/x/image v0.5.0
go: downloading golang.org/x/text v0.7.0
go: downloading github.com/mattn/go-sqlite3 v1.14.16
go: downloading github.com/gin-contrib/sse v0.1.0
go: downloading github.com/mattn/go-runewidth v0.0.9
go: downloading github.com/go-playground/validator/v10 v10.4.1
go: downloading github.com/golang/protobuf v1.5.2
go: downloading github.com/ugorji/go/codec v1.1.7
go: downloading gopkg.in/yaml.v2 v2.4.0
go: downloading github.com/zclconf/go-cty v1.9.0
go: downloading github.com/agext/levenshtein v1.2.3
go: downloading github.com/apparentlymart/go-textseg/v13 v13.0.0
go: downloading github.com/mitchellh/go-wordwrap v1.0.1
go: downloading github.com/go-playground/universal-translator v0.17.0
go: downloading github.com/leodido/go-urn v1.2.0
go: downloading google.golang.org/protobuf v1.26.0
go: downloading github.com/google/go-cmp v0.5.6
go: downloading github.com/go-playground/locales v0.13.0
root@debian:/home/practica/Havoc#
```

make client-build



```
root@debian:/home/practica/Havoc# make client-build
[*] building client
Submodule 'client/external/json' (https://github.com/nlohmann/json) registered for path 'client/external/json'
Submodule 'client/external/spdlog' (https://github.com/gabime/spdlog) registered for path 'client/external/spdlog'
Submodule 'client/external/toml' (https://github.com/ToruNiina/toml11) registered for path 'client/external/toml'
Cloning into '/home/practica/Havoc/client/external/json'...
```

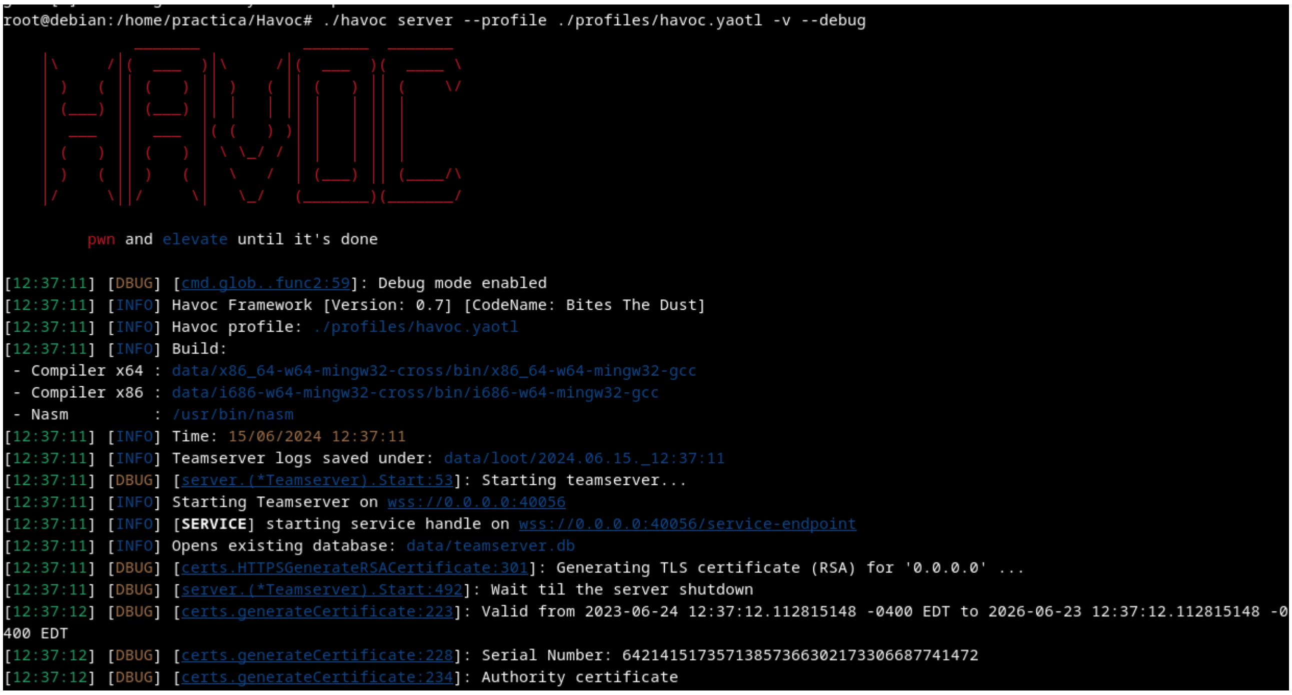


```
[ 76%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/PythonScript.cc.o
[ 78%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/ScriptManager.cc.o
[ 80%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/LootWidget.cc.o
/home/practica/Havoc/client/src/UserInterface/Widgets/LootWidget.cc: In member function ‘const QPixmap* ImageLabel::pixmap()
const’:
/home/practica/Havoc/client/src/UserInterface/Widgets/LootWidget.cc:41:25: warning: ‘const QPixmap* QLabel::pixmap() const’
s deprecated: Use the other overload which returns QPixmap by-value [-Wdeprecated-declarations]
   41 |     return label->pixmap();
      |            ~~~~~~~~~~~~~^~
In file included from /usr/include/x86_64-linux-gnu/qt5/QtWidgets/QLabel:1,
                 from /home/practica/Havoc/client/include/global.hpp:12,
                 from /home/practica/Havoc/client/src/UserInterface/Widgets/LootWidget.cc:1:
/usr/include/x86_64-linux-gnu/qt5/QtWidgets/qlabel.h:78:20: note: declared here
   78 |     const QPixmap *pixmap() const; // ### Qt 7: Remove function
      |                    ^~~~~~
[ 82%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/FileBrowser.cc.o
[ 84%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/Teamserver.cc.o
[ 86%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/Store.cc.o
[ 88%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/Widgets/ProcessList.cc.o
[ 90%] Building CXX object CMakeFiles/Havoc.dir/src/UserInterface/SmallWidgets/EventViewer.cc.o
[ 92%] Building CXX object CMakeFiles/Havoc.dir/src/Util/ColorText.cpp.o
[ 94%] Building CXX object CMakeFiles/Havoc.dir/src/Util/Base64.cpp.o
[ 96%] Building CXX object CMakeFiles/Havoc.dir/src/Util/Base.cpp.o
[ 98%] Building CXX object CMakeFiles/Havoc.dir/Havoc_autogen/QYFM2Z2WYQ/qrc_Havoc.cpp.o
[100%] Linking CXX executable /home/practica/Havoc/client/Havoc
gmake[3]: Leaving directory '/home/practica/Havoc/client/Build'
[100%] Built target Havoc
gmake[2]: Leaving directory '/home/practica/Havoc/client/Build'
gmake[1]: Leaving directory '/home/practica/Havoc/client/Build'
root@debian:/home/practica/Havoc#
```

con este último comando se daría por concluida la instalación del Havoc, que es el Command & Control.

Abro dos terminales en el debian

./havoc server --profile ./profiles/havoc.yaotl -v --debug



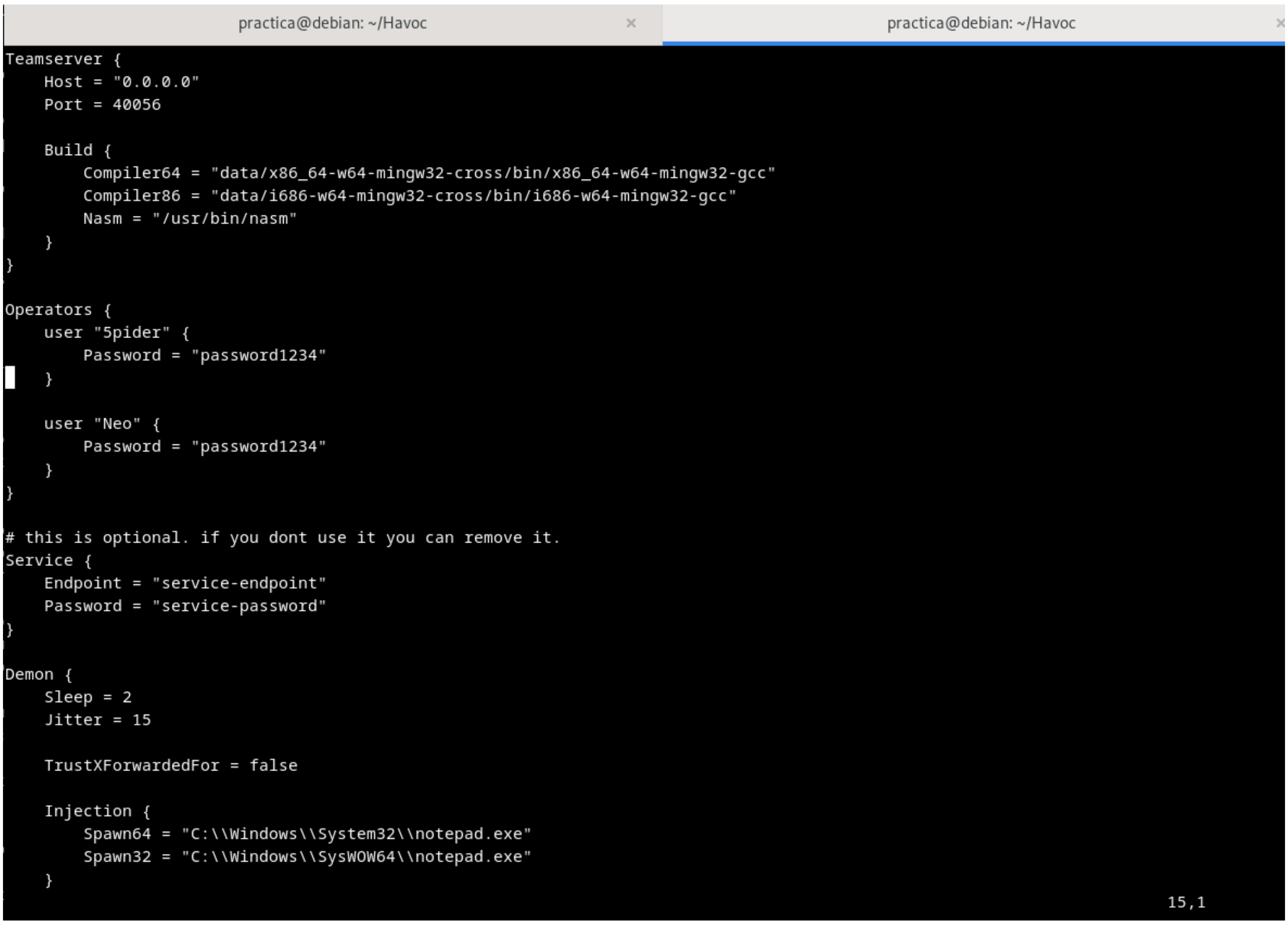
```
root@debian:/home/practica/Havoc# ./havoc server --profile ./profiles/havoc.yaotl -v --debug

              _______           _______  _______
    |\     /|(  ___  )|\     /|(  ___  )(  ____ \
    | )   ( || (   ) || )   ( || (   ) || (    \/
    | (___) || (___) || |   | || |   | || |
    |  ___  ||  ___  |( (   ) )| |   | || |
    | (   ) || (   ) | \ \_/ / | |   | || |
    | )   ( || )   ( |  \   /  | (___) || (____/\
    |/     \||/     \|   \_/   (_______)(_______/

         pwn and elevate until it's done

[12:37:11] [DBUG] [cmd.glob..func2:59]: Debug mode enabled
[12:37:11] [INFO] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[12:37:11] [INFO] Havoc profile: ./profiles/havoc.yaotl
[12:37:11] [INFO] Build:
 - Compiler x64 : data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-gcc
 - Compiler x86 : data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc
 - Nasm         : /usr/bin/nasm
[12:37:11] [INFO] Time: 15/06/2024 12:37:11
[12:37:11] [INFO] Teamserver logs saved under: data/loot/2024.06.15._12:37:11
[12:37:11] [DBUG] [server.(*Teamserver).Start:53]: Starting teamserver...
[12:37:11] [INFO] Starting Teamserver on wss://0.0.0.0:40056
[12:37:11] [INFO] [SERVICE] starting service handle on wss://0.0.0.0:40056/service-endpoint
[12:37:11] [INFO] Opens existing database: data/teamserver.db
[12:37:11] [DBUG] [certs.HTTPSGenerateRSACertificate:301]: Generating TLS certificate (RSA) for '0.0.0.0' ...
[12:37:11] [DBUG] [server.(*Teamserver).Start:492]: Wait til the server shutdown
[12:37:12] [DBUG] [certs.generateCertificate:223]: Valid from 2023-06-24 12:37:12.112815148 -0400 EDT to 2026-06-23 12:37:12.112815148 -0
400 EDT
[12:37:12] [DBUG] [certs.generateCertificate:228]: Serial Number: 64214151735713857366302173306687741472
[12:37:12] [DBUG] [certs.generateCertificate:234]: Authority certificate
```

./havoc client

edito el fichero havoc.yaotl

vim profiles/havoc.yaotl

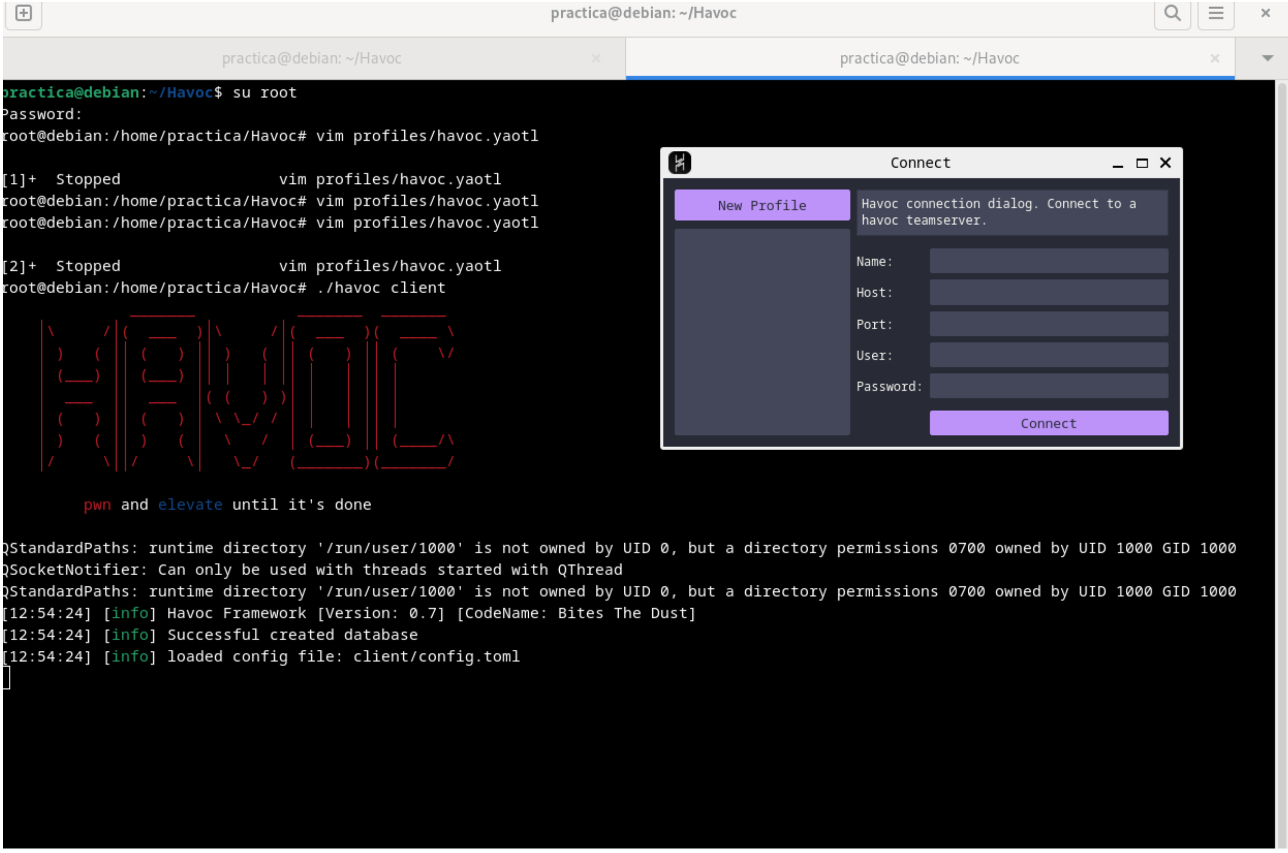
este es el fichero de configuración de Havoc. Aquí podemos añadir usuarios, podemos configurar el tráfico, crear una estructura de tráfico de red. Podemos replicar tráfico de red.



```
Teamserver {
    Host = "0.0.0.0"
    Port = 40056

    Build {
        Compiler64 = "data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-gcc"
        Compiler86 = "data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc"
        Nasm = "/usr/bin/nasm"
    }
}

Operators {
    user "5pider" {
        Password = "password1234"
    }

    user "Neo" {
        Password = "password1234"
    }
}

# this is optional. if you dont use it you can remove it.
Service {
    Endpoint = "service-endpoint"
    Password = "service-password"
}

Demon {
    Sleep = 2
    Jitter = 15

    TrustXForwardedFor = false

    Injection {
        Spawn64 = "C:\\Windows\\System32\\notepad.exe"
        Spawn32 = "C:\\Windows\\SysWOW64\\notepad.exe"
    }
                                                                    15,1
```

Ejecuto el siguiente comando en la carpeta Havoc

./havoc client

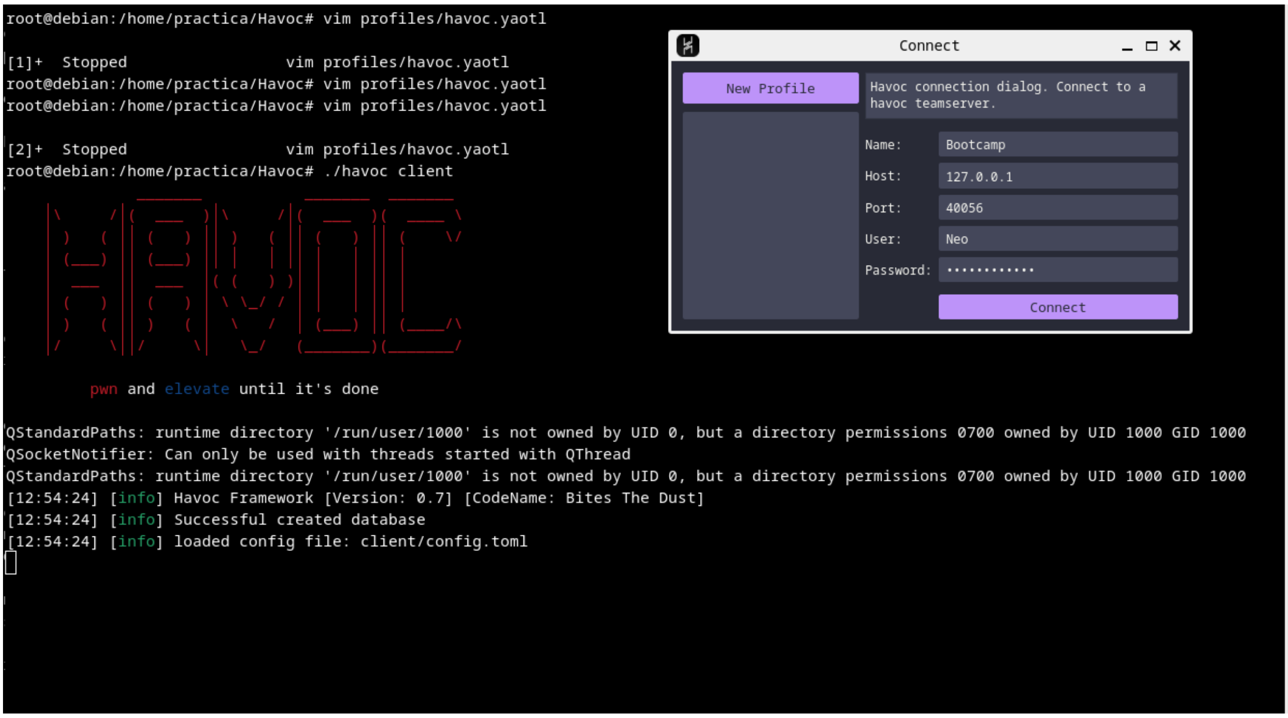


```
practica@debian:~/Havoc$ su root
Password:
root@debian:/home/practica/Havoc# vim profiles/havoc.yaotl

[1]+  Stopped                 vim profiles/havoc.yaotl
root@debian:/home/practica/Havoc# vim profiles/havoc.yaotl
root@debian:/home/practica/Havoc# vim profiles/havoc.yaotl

[2]+  Stopped                 vim profiles/havoc.yaotl
root@debian:/home/practica/Havoc# ./havoc client
              _______           _______  _______
    |\     /|(  ___  )|\     /|(  ___  )(  ____ \
    | )   ( || (   ) || )   ( || (   ) || (    \/
    | (___) || (___) || |   | || |   | || |
    |  ___  ||  ___  |( (   ) )| |   | || |
    | (   ) || (   ) | \ \_/ / | |   | || |
    | )   ( || )   ( |  \   /  | (___) || (____/\
    |/     \||/     \|   \_/   (_______)(_______/

         pwn and elevate until it's done

QStandardPaths: runtime directory '/run/user/1000' is not owned by UID 0, but a directory permissions 0700 owned by UID 1000 GID 1000
QSocketNotifier: Can only be used with threads started with QThread
QStandardPaths: runtime directory '/run/user/1000' is not owned by UID 0, but a directory permissions 0700 owned by UID 1000 GID 1000
[12:54:24] [info] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[12:54:24] [info] Successful created database
[12:54:24] [info] loaded config file: client/config.toml
```

Havoc connection dialog. Connect to a havoc teamserver.

Name:
Host:
Port:
User:
Password:

introducimos los siguientes datos en la cajas de texto:

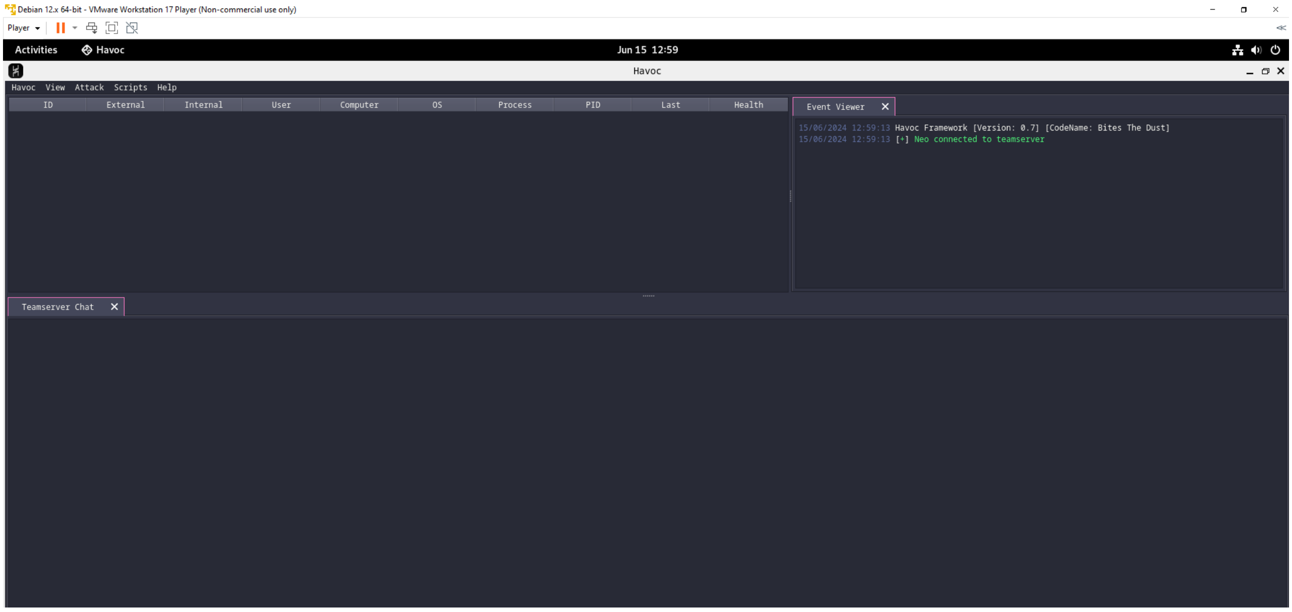


```
root@debian:/home/practica/Havoc# vim profiles/havoc.yaotl

[1]+  Stopped                 vim profiles/havoc.yaotl
root@debian:/home/practica/Havoc# vim profiles/havoc.yaotl
root@debian:/home/practica/Havoc# vim profiles/havoc.yaotl

[2]+  Stopped                 vim profiles/havoc.yaotl
root@debian:/home/practica/Havoc# ./havoc client
              _______           _______  _______
    |\     /|(  ___  )|\     /|(  ___  )(  ____ \
    | )   ( || (   ) || )   ( || (   ) || (    \/
    | (___) || (___) || |   | || |   | || |
    |  ___  ||  ___  |( (   ) )| |   | || |
    | (   ) || (   ) | \ \_/ / | |   | || |
    | )   ( || )   ( |  \   /  | (___) || (____/\
    |/     \||/     \|   \_/   (_______)(_______/

         pwn and elevate until it's done

QStandardPaths: runtime directory '/run/user/1000' is not owned by UID 0, but a directory permissions 0700 owned by UID 1000 GID 1000
QSocketNotifier: Can only be used with threads started with QThread
QStandardPaths: runtime directory '/run/user/1000' is not owned by UID 0, but a directory permissions 0700 owned by UID 1000 GID 1000
[12:54:24] [info] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[12:54:24] [info] Successful created database
[12:54:24] [info] loaded config file: client/config.toml
```

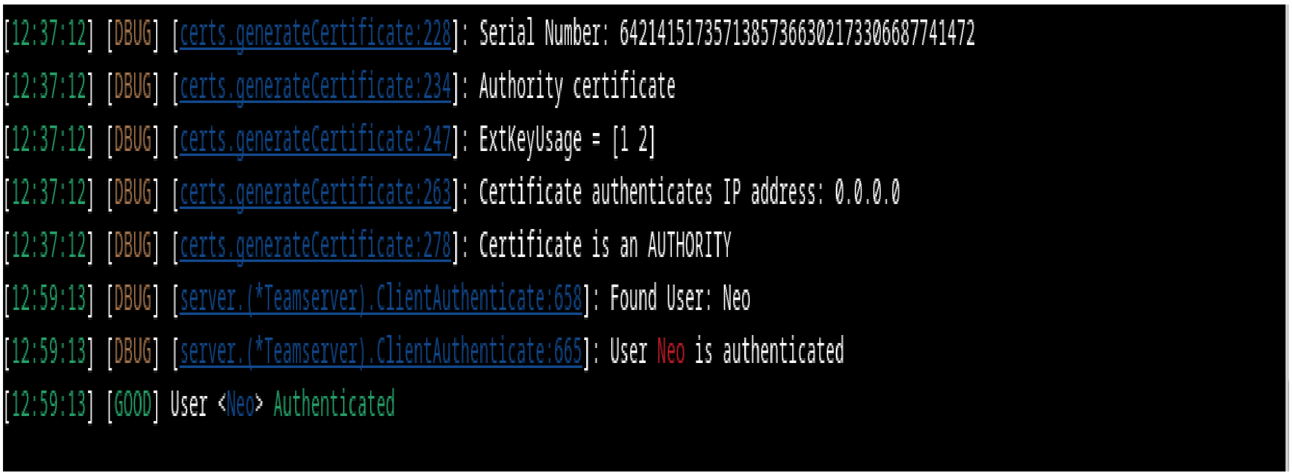
Havoc connection dialog. Connect to a havoc teamserver.

Name: Bootcamp
Host: 127.0.0.1
Port: 40056
User: Neo
Password: ••••••••••••

el puerto se puede cambiar, el usuario/password es el que viene en el fichero de configuración havoc.yaotl, es decir Neo/password1234. Le doy a Connect y me salen estas pantallas:


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Havoc
Jun 15 12:59
Havoc
Havoc View Attack Scripts Help
ID External Internal User Computer OS Process PID Last Health
Event Viewer
Teamserver Chat

```
15/06/2024 12:59:13 Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
15/06/2024 12:59:13 [+] Neo connected to teamserver
```



```
[12:37:12] [DBUG] [certs.generateCertificate:228]: Serial Number: 64214151735713857366302173306687741472
[12:37:12] [DBUG] [certs.generateCertificate:234]: Authority certificate
[12:37:12] [DBUG] [certs.generateCertificate:247]: ExtKeyUsage = [1 2]
[12:37:12] [DBUG] [certs.generateCertificate:263]: Certificate authenticates IP address: 0.0.0.0
[12:37:12] [DBUG] [certs.generateCertificate:278]: Certificate is an AUTHORITY
[12:59:13] [DBUG] [server.(*Teamserver).ClientAuthenticate:658]: Found User: Neo
[12:59:13] [DBUG] [server.(*Teamserver).ClientAuthenticate:665]: User Neo is authenticated
[12:59:13] [GOOD] User <Neo> Authenticated
```