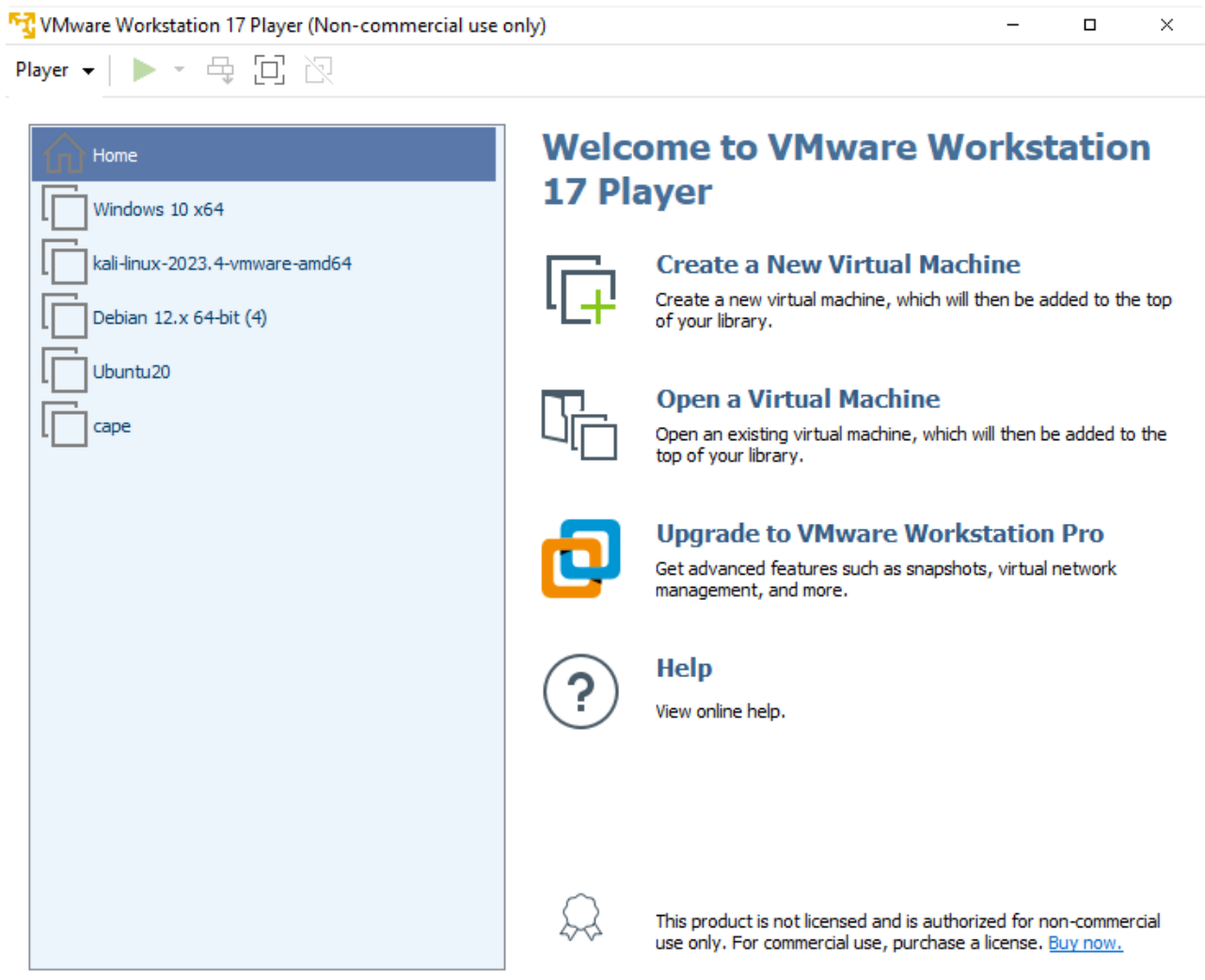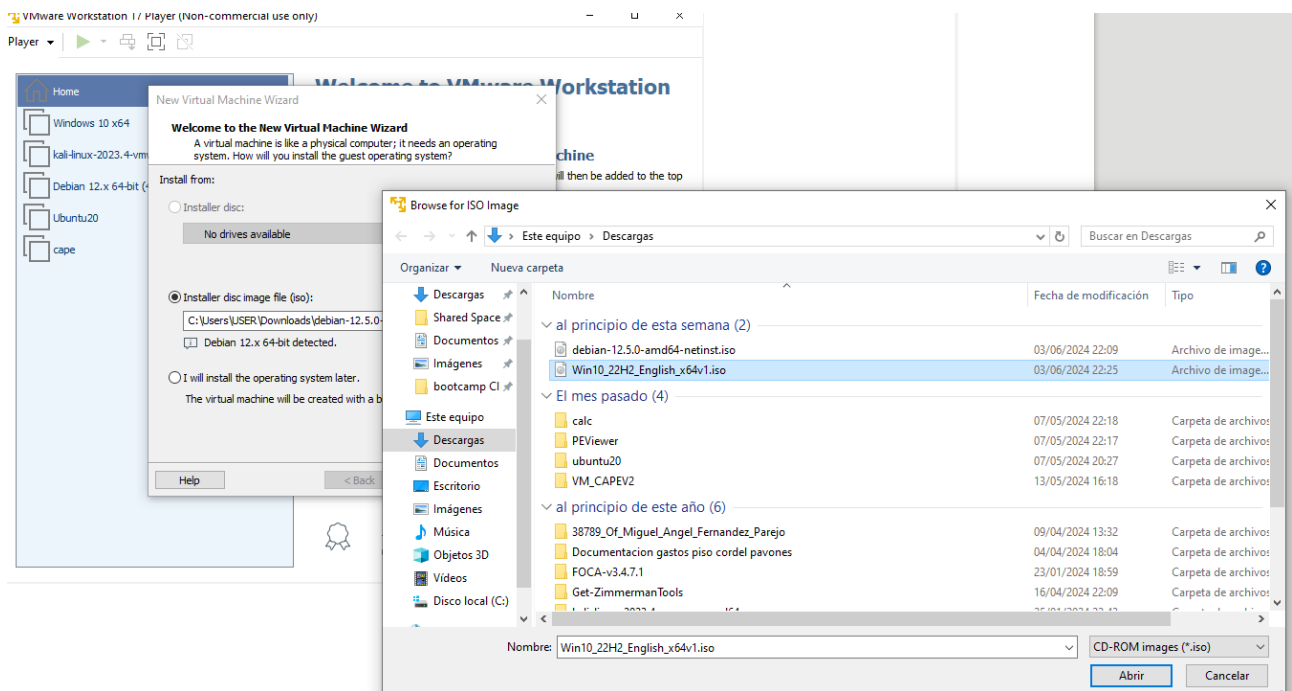Ejercicio 2 Construir un laboratorio:
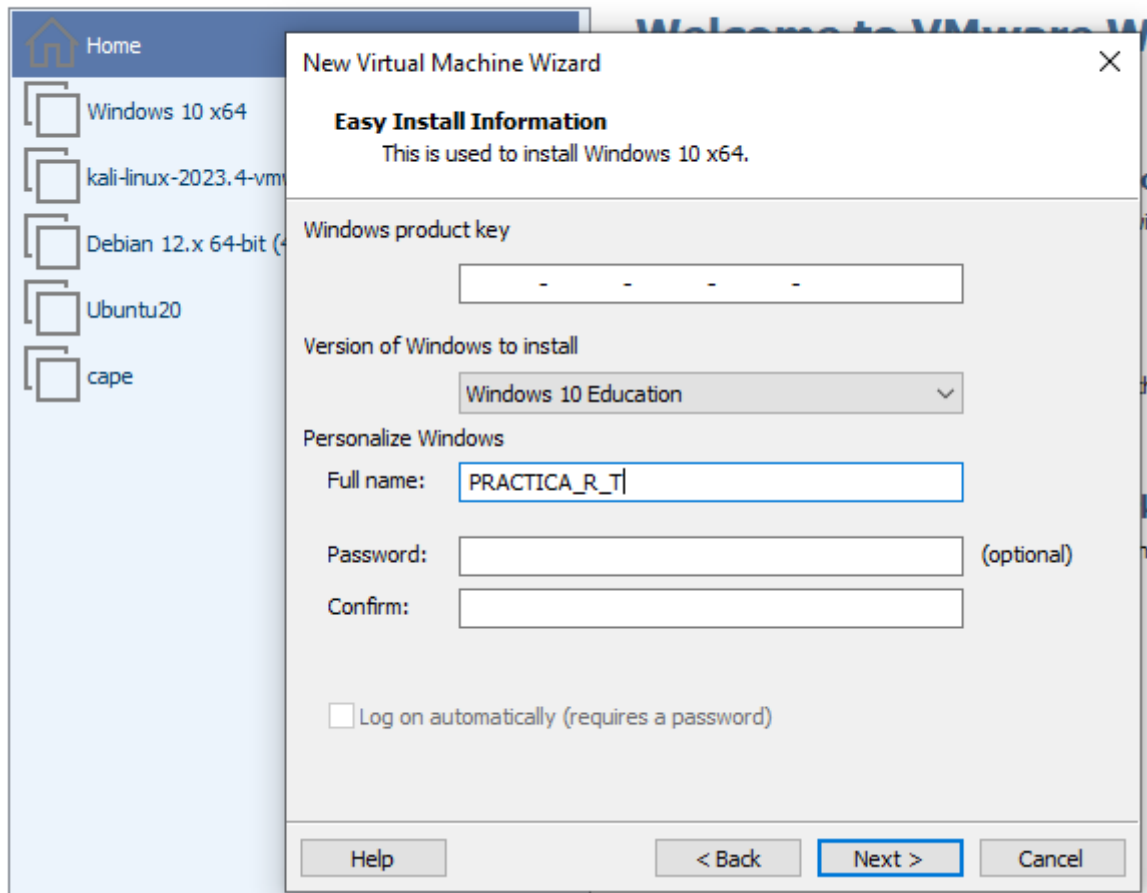
Máquina Windows 10:

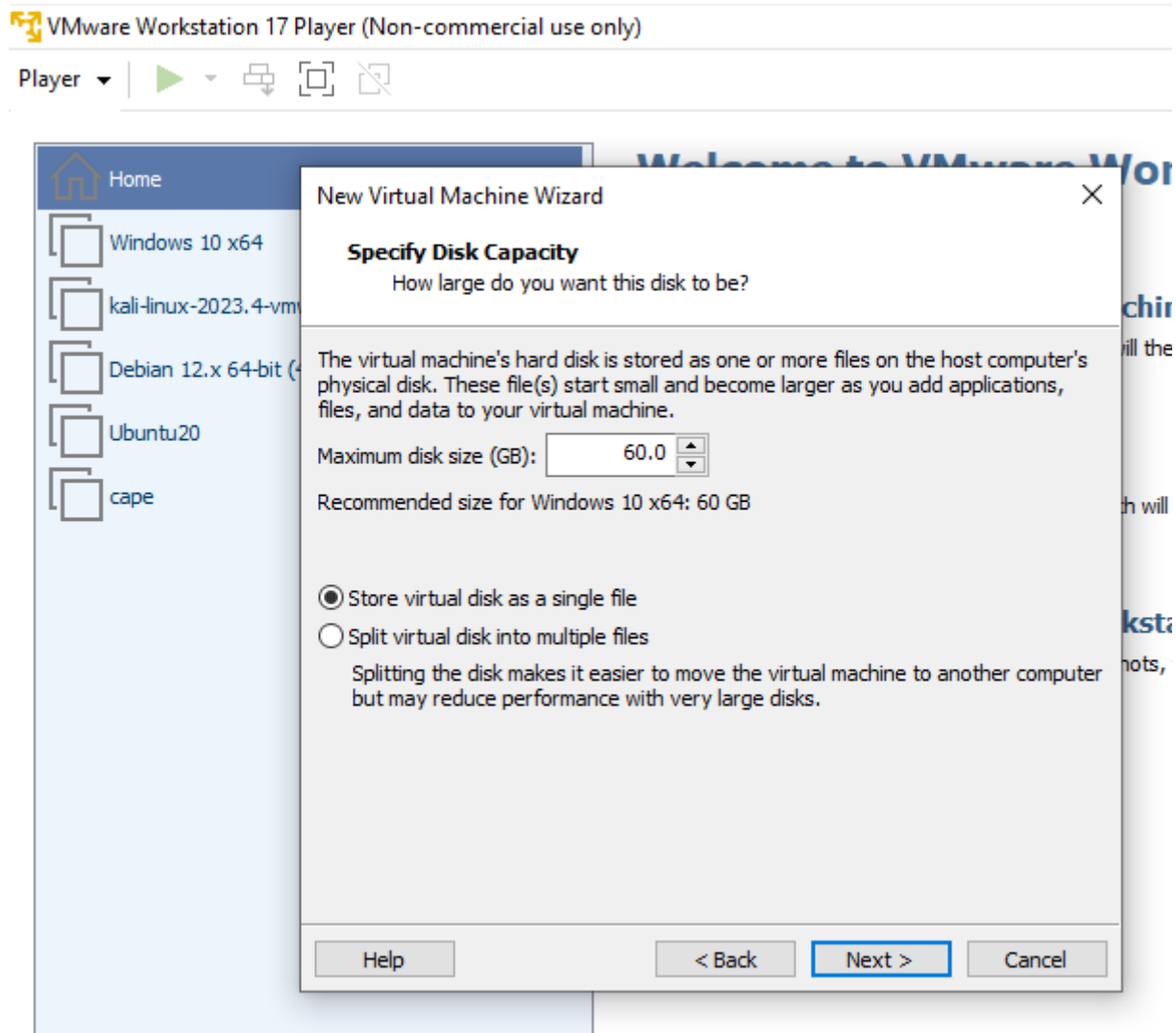Hacer click en Create a New Virtual Machine

Elijo la .iso de window10:

Le doy un nombre:

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

Aumento memoria RAM a 4GB

Hardware ✕

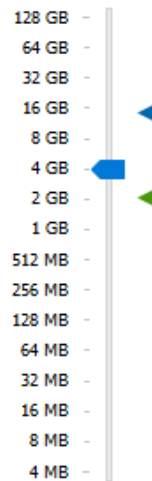| Device	Summary
🖥 Memory	2 GB
⚙ Processors	2
◎ New CD/DVD (SATA)	Using file C:\Users\USER\Do…
🔌 Network Adapter	NAT
🔌 USB Controller	Present
🔊 Sound Card	Auto detect
🖵 Display	Auto detect

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

```
128 GB -
 64 GB -
 32 GB -
 16 GB -   ◄          ■ Maximum recommended memory
  8 GB -               (Memory swapping may
  4 GB - ◀─            occur beyond this size.)
  2 GB -   ◄           13.4 GB
  1 GB -
512 MB -              ■ Recommended memory
256 MB -               2 GB
128 MB -
 64 MB -              ■ Guest OS recommended minimum
 32 MB -               2 GB
 16 MB -
  8 MB -
  4 MB -
```

Add…   Remove

Close   Help

Setup is starting

Player ▾

Windows Setup

Installing Windows

Status

✓ Copying Windows files
Getting files ready for installation (0%)
Installing features
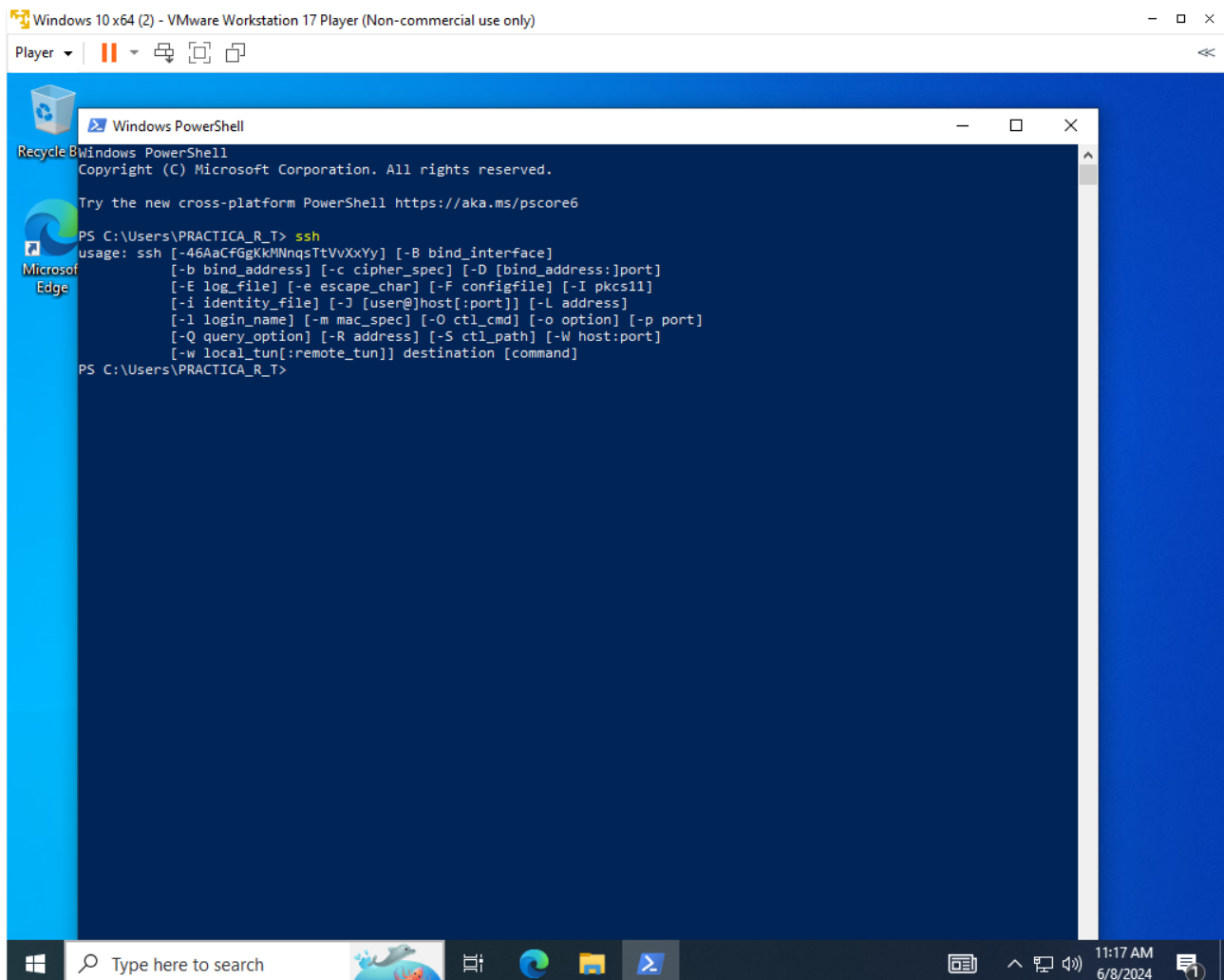Installing updates
Finishing up

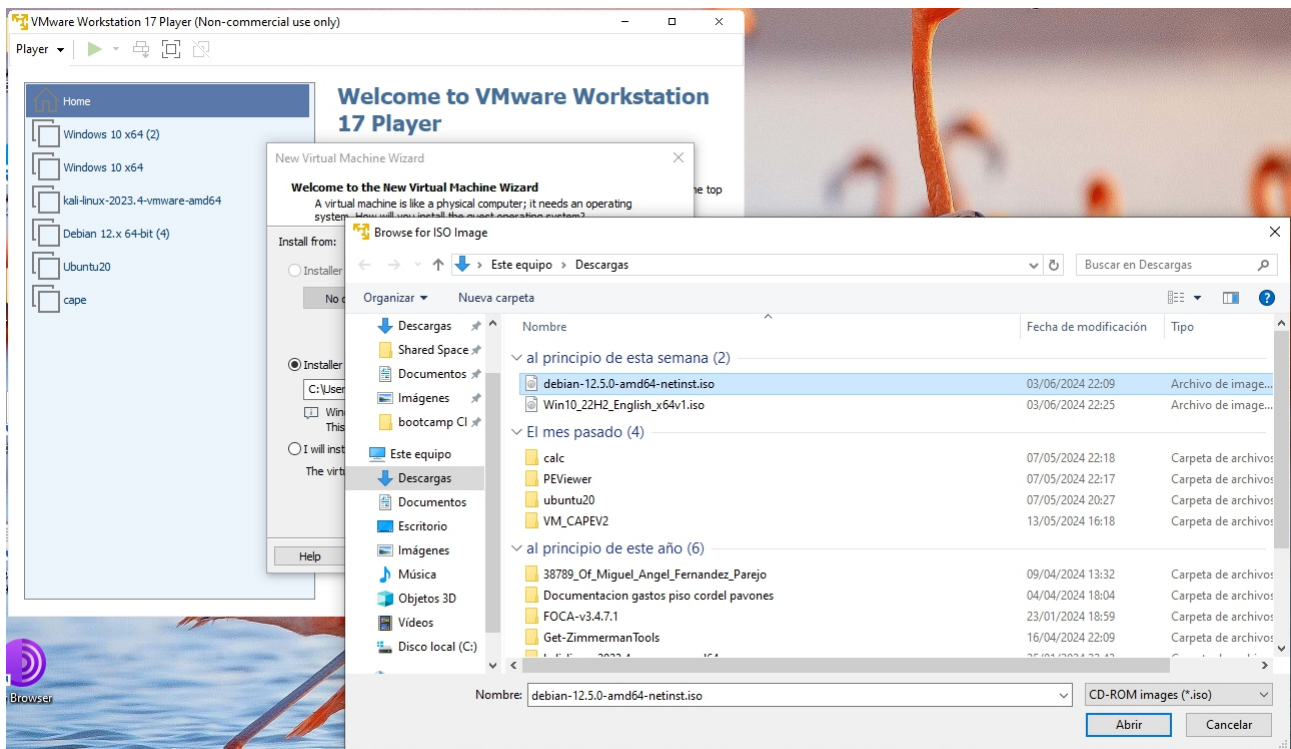1 Collecting information   2 Installing Windows

comprobamos el ssh

Máquina Linux (Debian C&C)

Creo nueva MV eligiendo la .iso Debian:

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

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

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.
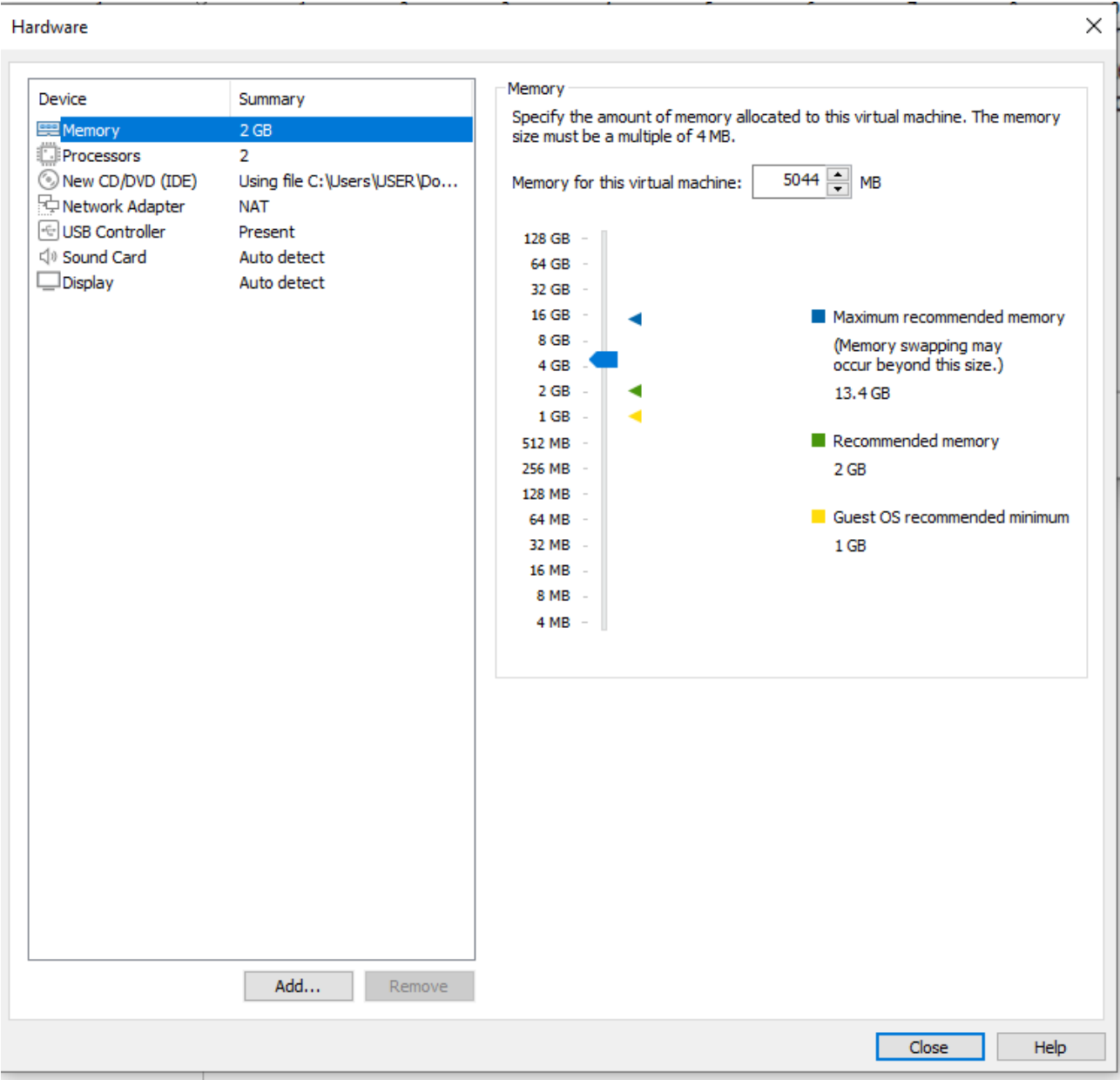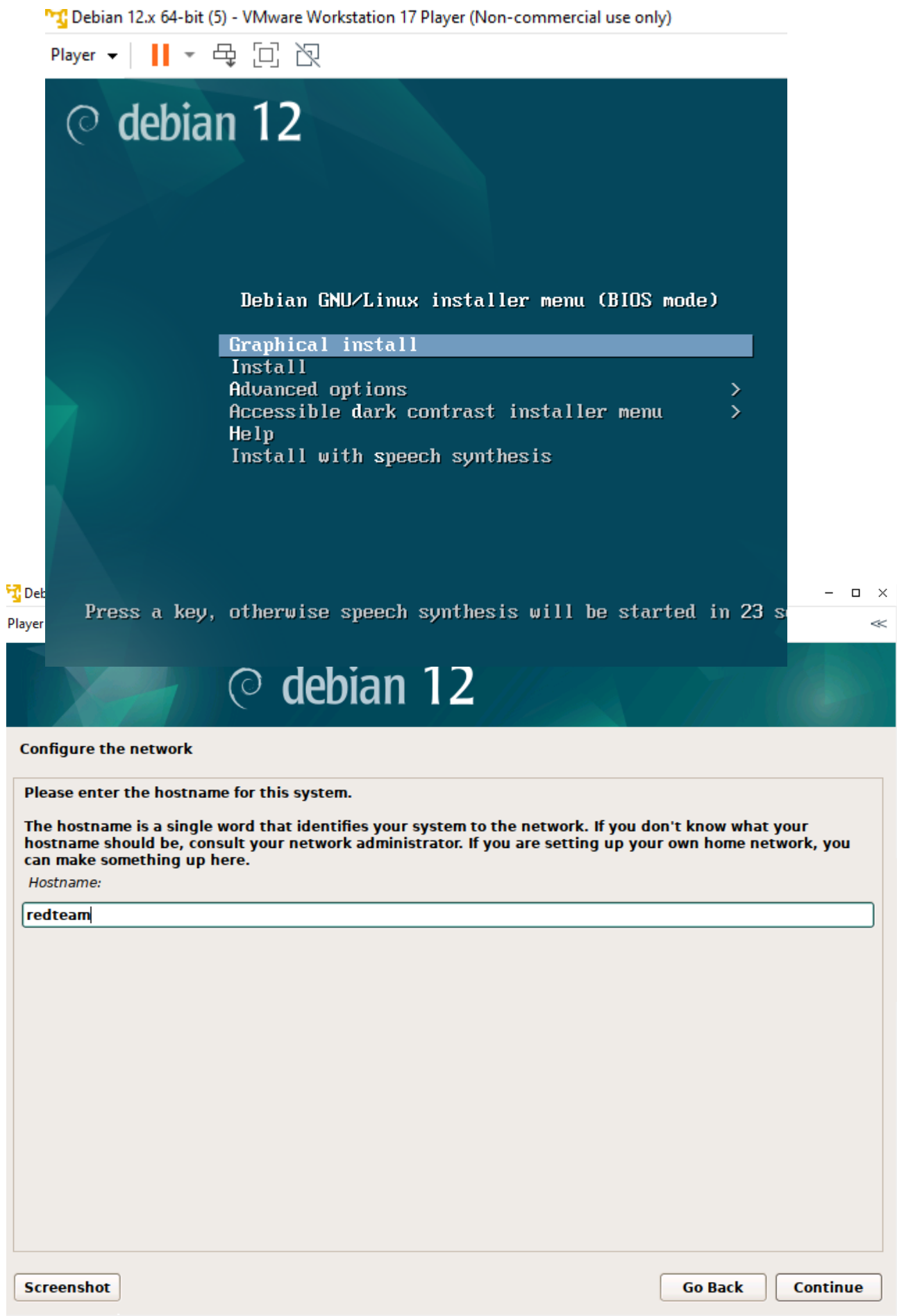
Help   < Back   Next >   Cancel

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

- 128 GB
- 64 GB
- 32 GB
- 16 GB
- 8 GB
- 4 GB
- 2 GB
- 1 GB
- 512 MB
- 256 MB
- 128 MB
- 64 MB
- 32 MB
- 16 MB
- 8 MB
- 4 MB

■ Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.4 GB

■ Recommended memory
2 GB

■ Guest OS recommended minimum
1 GB

Add...   Remove

Close   Help
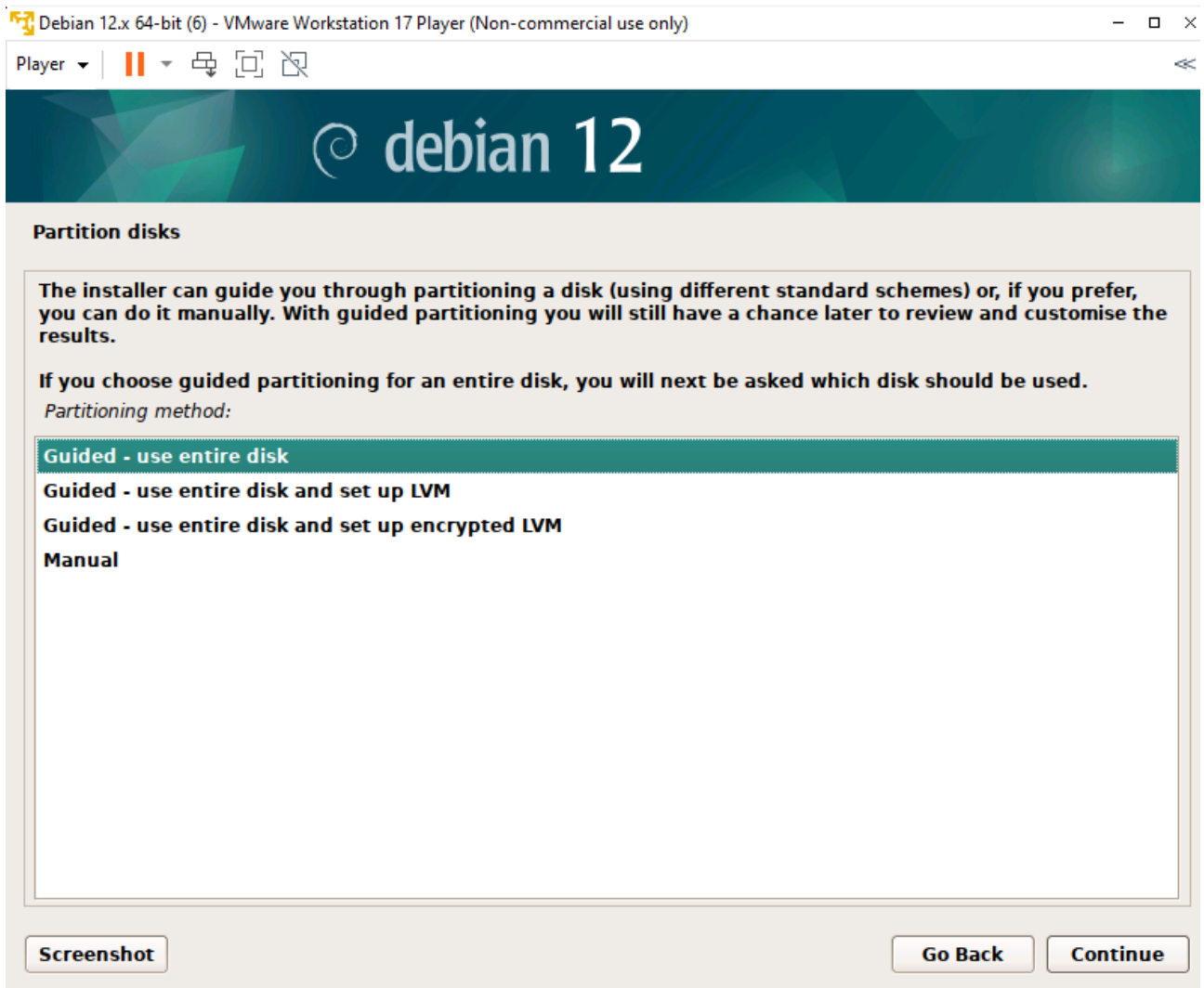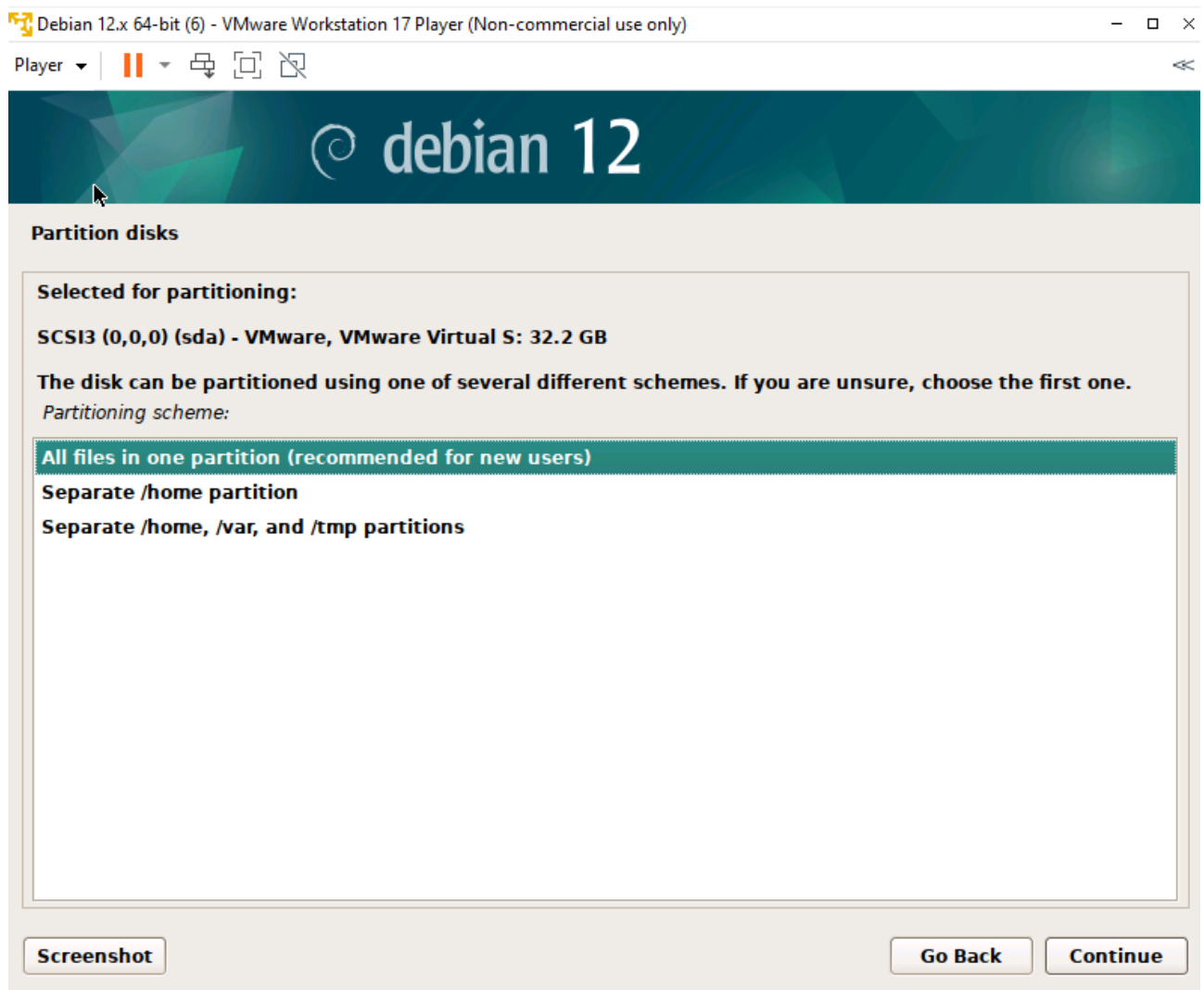
selecciono Graphical install y le pongo nombre de root readteam:

selecciono la primera opción "usar el disco completo"

Selecciono la primera opción. Todos los ficheros en una partición

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

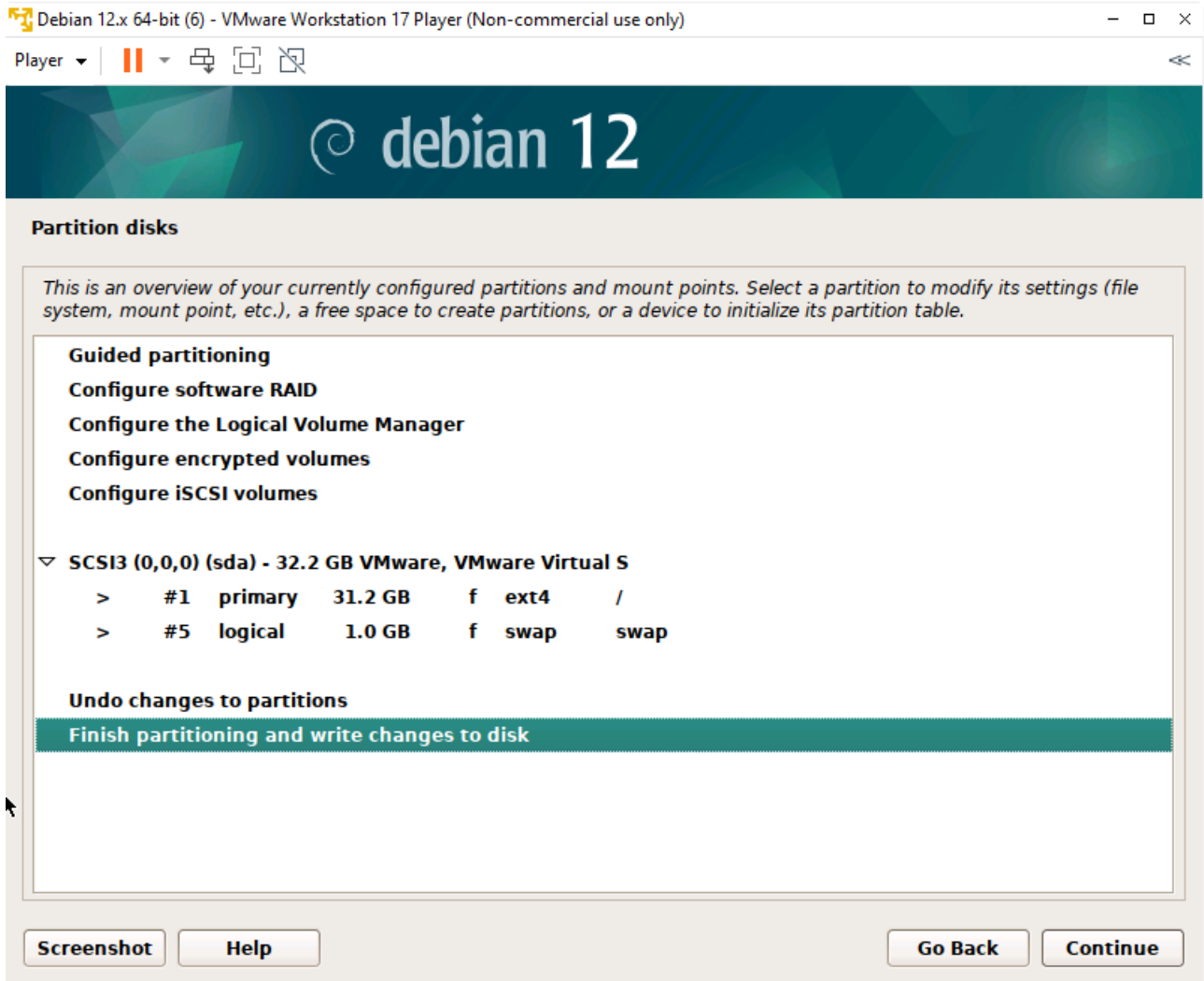**Finish partitioning and write changes to disk**

| Screenshot | Help | | Go Back | Continue |

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

Screenshot   Continue

Finalizo la partición

Player ▾

debian 12

Install the base system

Installing the base system

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

Selecciono No escaneo medios

Player ▾

debian 12
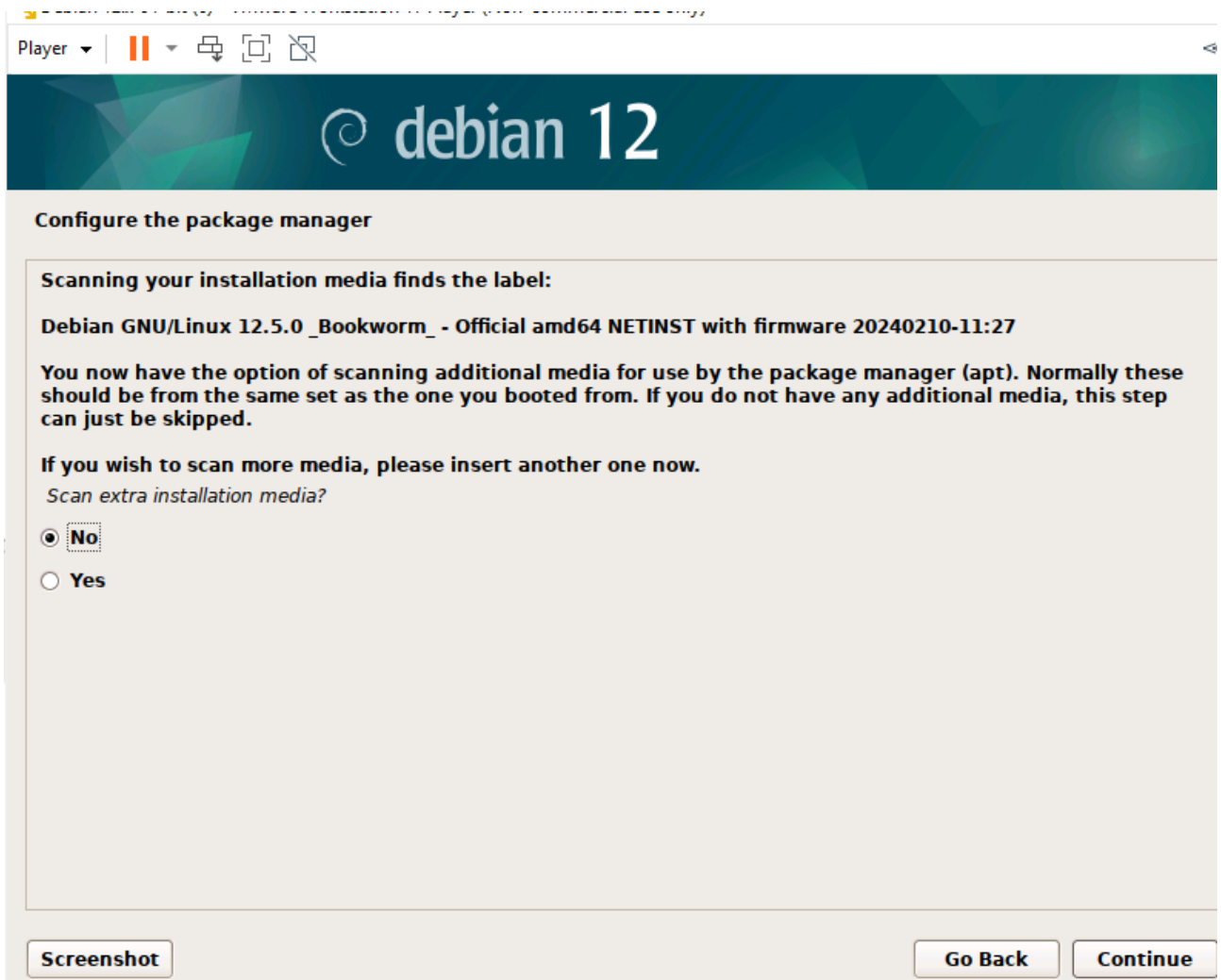
Configure the package manager

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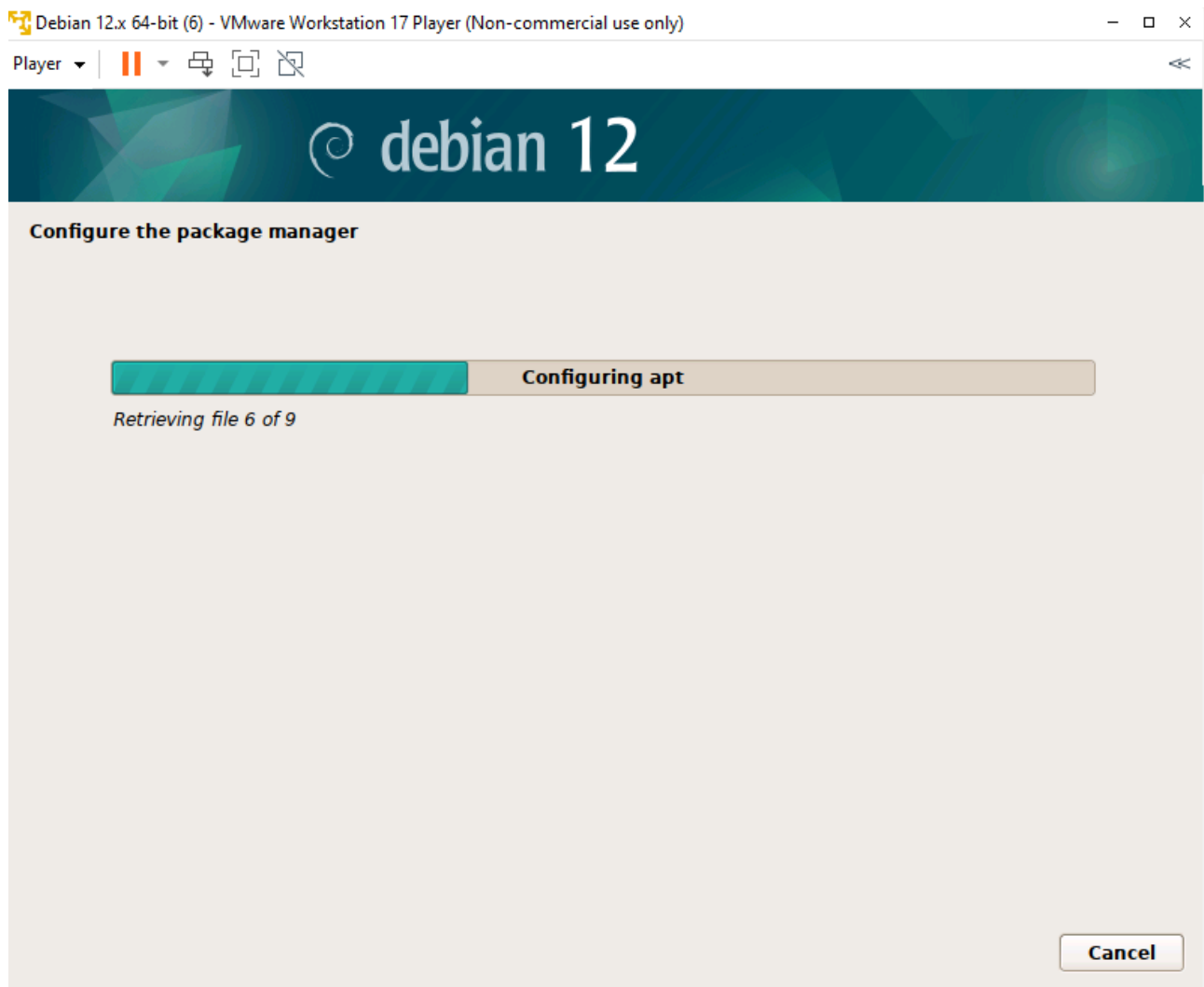
selecciono la opción del ssh server, para installar el servicio ssh

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**

Screenshot　　　　　　　　　　　　　　　　　　　　　　**Continue**

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
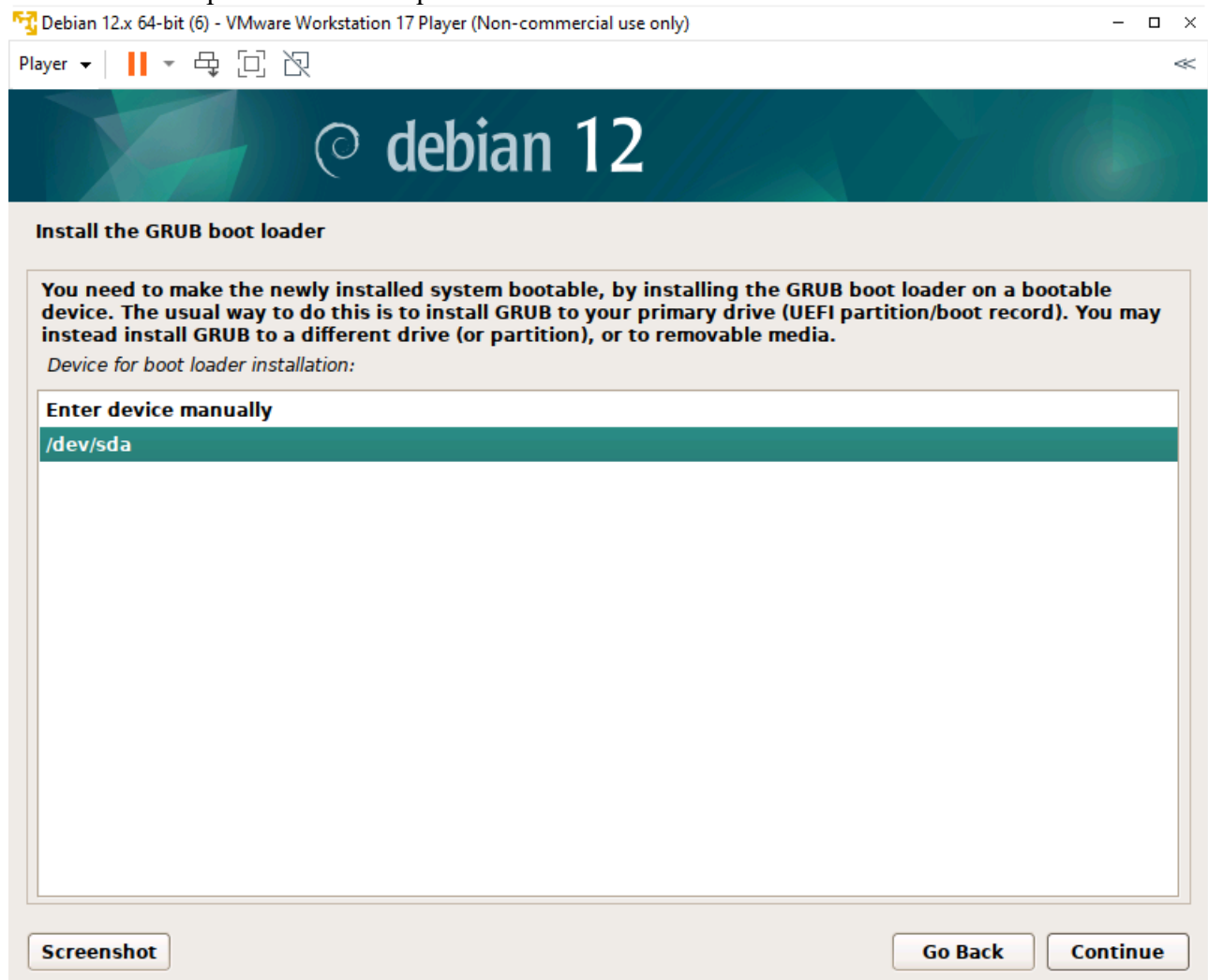
Hago click en continue para reiniciar el debian
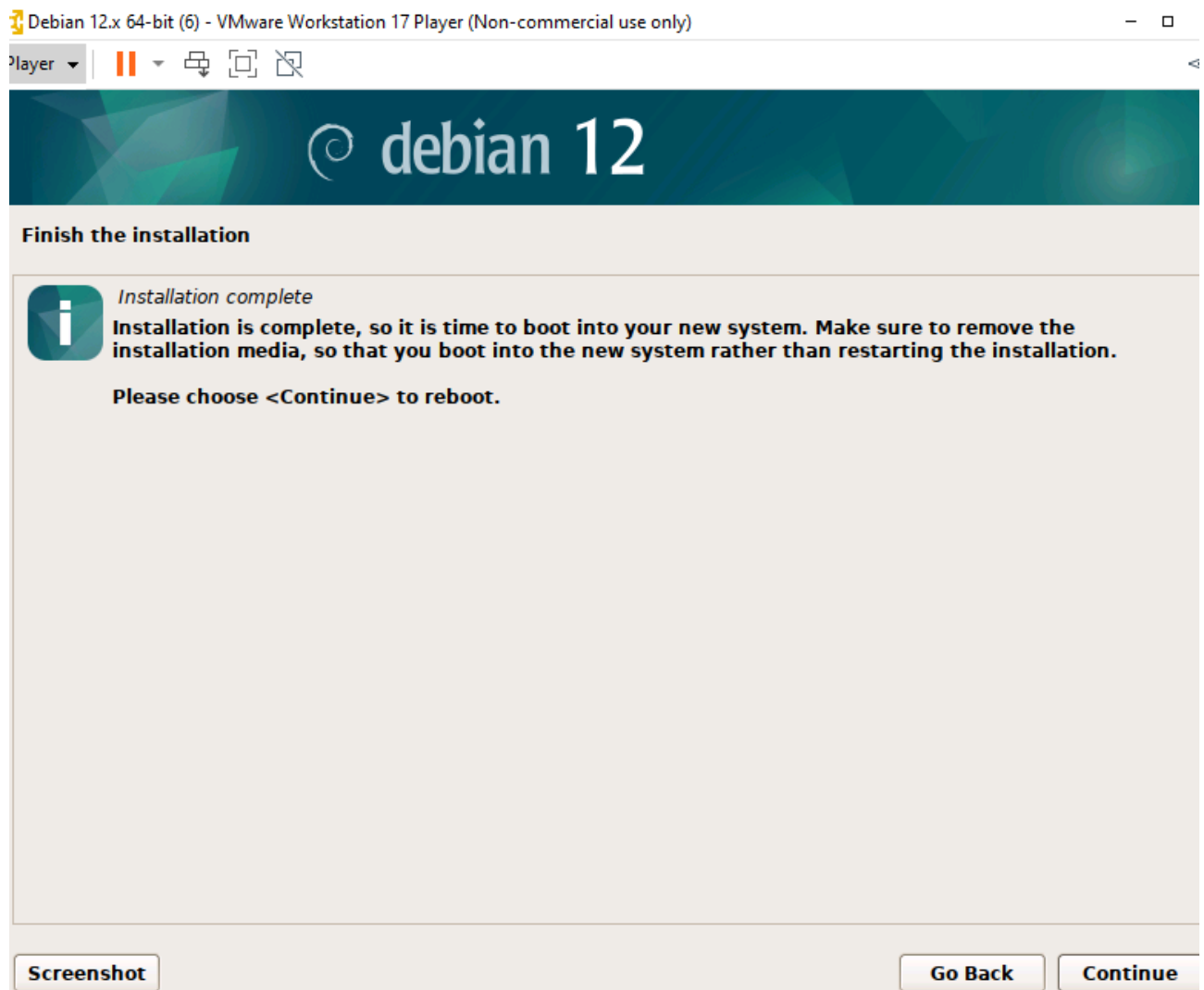
Instalación y configuración de herramientas, para la comunicación entre las dos máquinas, Debian y Windows:

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

apt update

Instalo proxychains y python3

apt proxychains python3

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

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


```
practica@debian: ~

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

^G Help      ^O Write Out  ^W Where Is   ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste    ^J Justify   ^/ Go To Line
```

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

creo un fichero test

echo "test" > test.txt
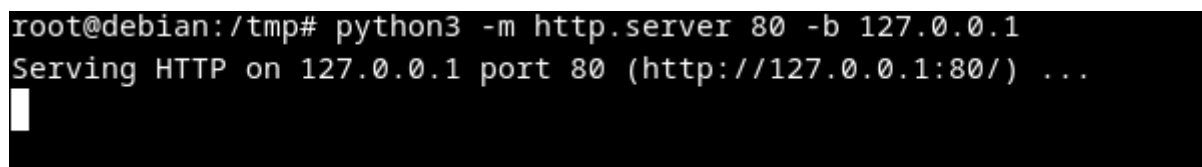
compruebo que se ha creado

levanto el servidor:

python3 -m http.server 80 -b 127.0.0.1

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

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#
```
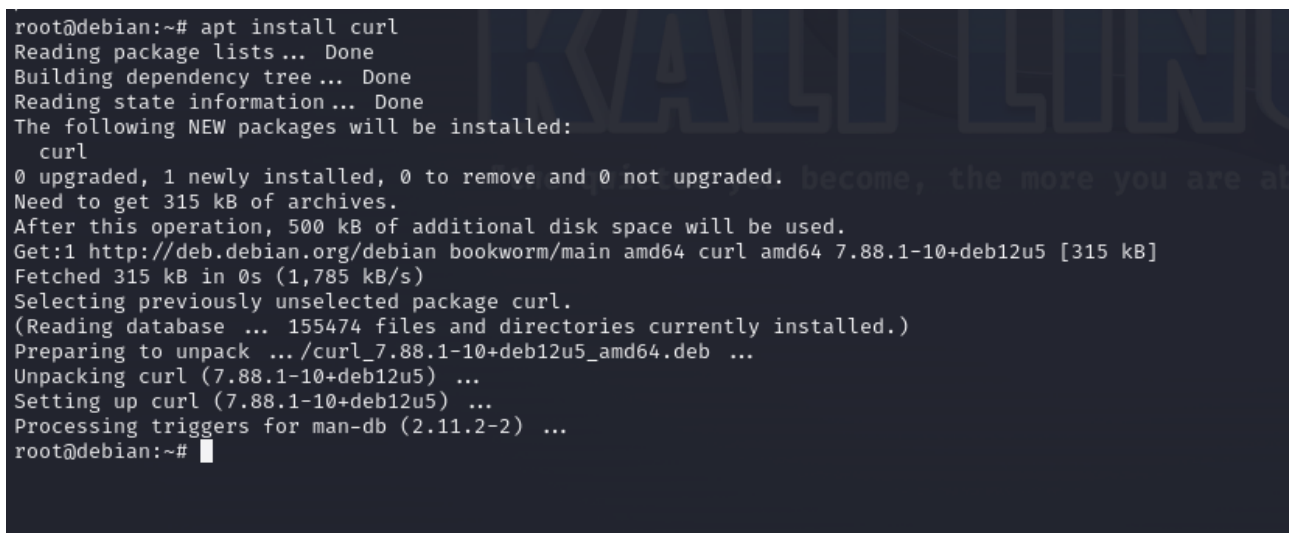
desde otra máquina pongo ssh root@192.168.79.134
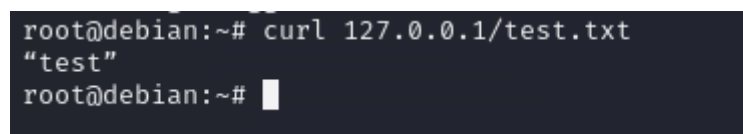
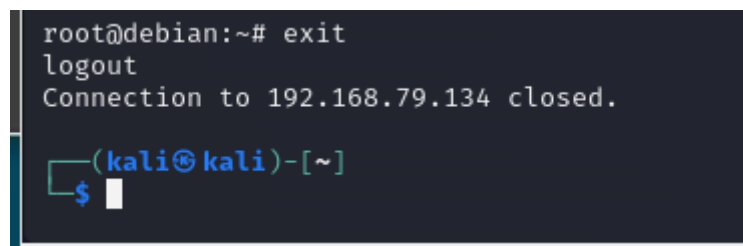compruebo que la máquina atacante (Debian) se ha metido en la víctima (kali)
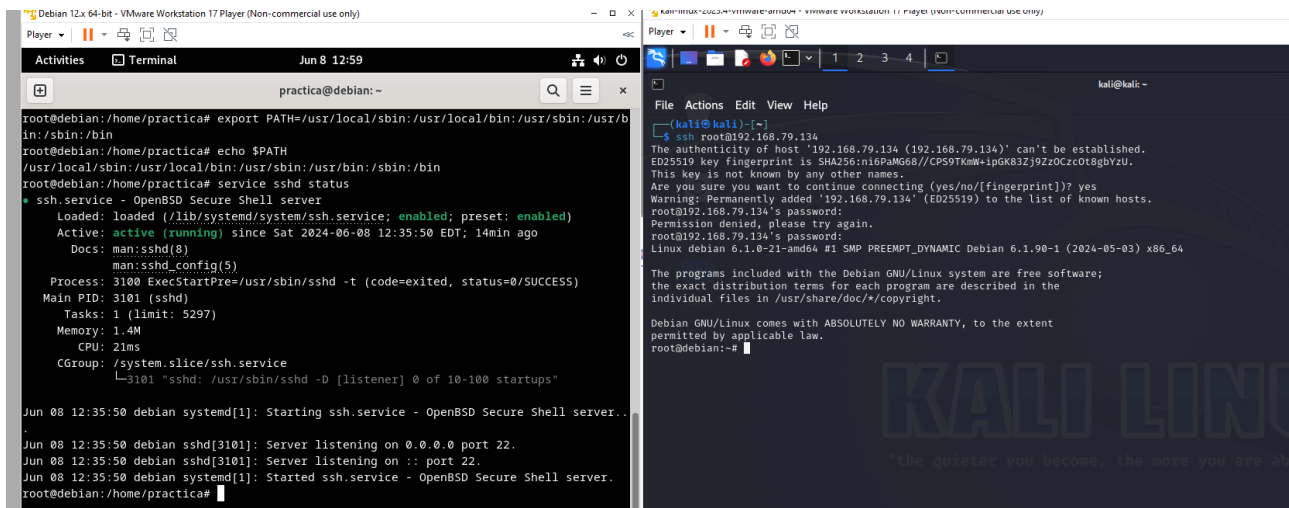
hago un apt install curl
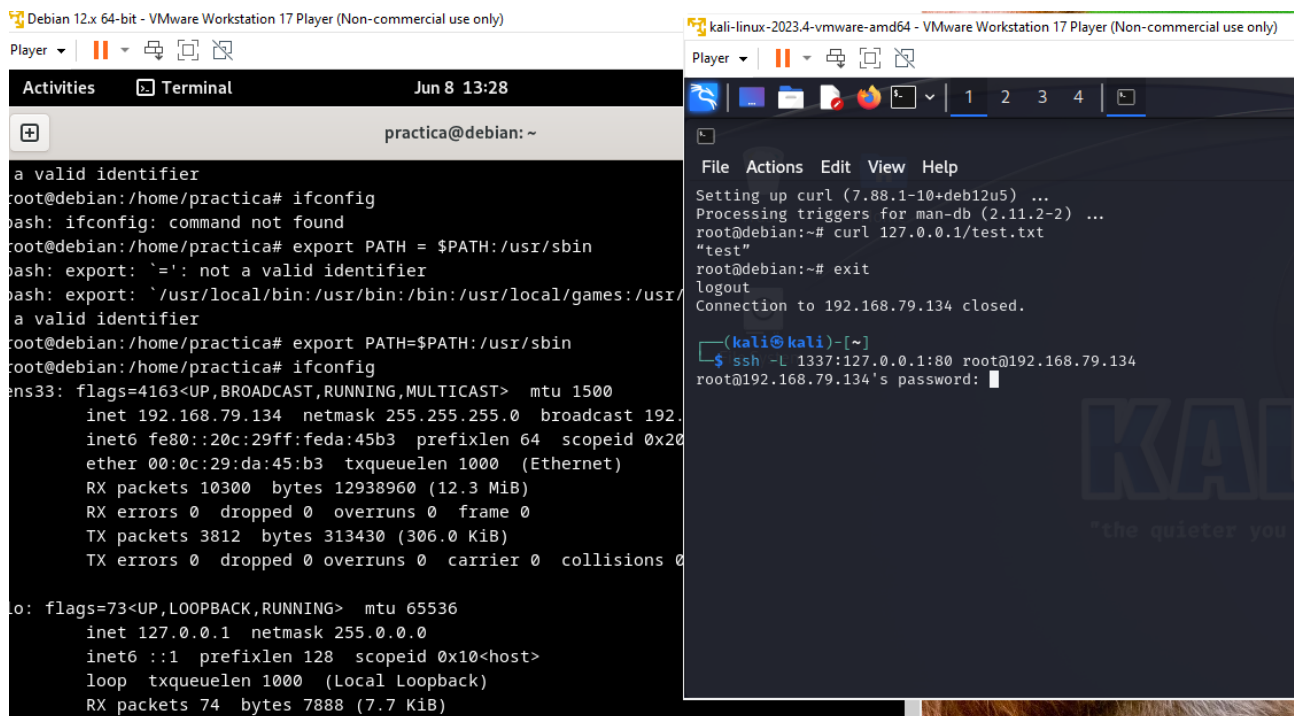

hago un curl 127.0.0.1/test.txt

escribo exit para cerrar la conexión

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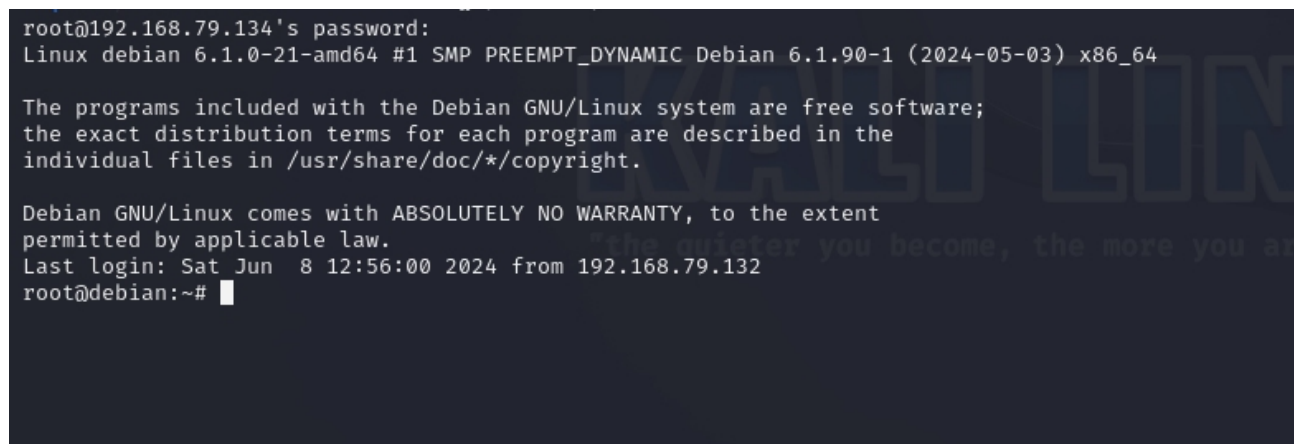El 127.0.0.1 es la interface donde está el servicio ssh

ssh -L 1337:127.0.0.1:80 root@192.168.79.134

el puerto 80 es la salida del túnel,

en este punto está el túnel hecho.

Abro una nueva terminal y ejecuto netstat -putan

```
┌──(kali㊀kali)-[~]
└─$ 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 -

┌──(kali㊀kali)-[~]
└─$ ▮
```

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