

UNIVERSIDAD CENTRAL DEL ECUADOR



FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

CARRERA DE COMPUTACIÓN

Laboratorio – Configuración entorno Hacking Ético

Mauricio Alejandro López Yépez

Alexis Esteban Troya Bermudez

Ariel Marcelo Elizalde Calderon

2025 – 2026

Visión General

Esta es una práctica de seguridad informática que simula un entorno real de pentesting, donde configurarás una máquina objetivo (host) y utilizarás Kali Linux como máquina atacante para evaluar la seguridad.

Recomendaciones por Fase

Fase 1: Elección e Instalación del Hipervisor

Opciones:

- VirtualBox (gratuito, más fácil para principiantes)
- VMware Workstation Player (gratuito para uso personal, más robusto)
- Hyper-V (si tienes Windows 10/11 Pro, ya integrado)
- WSL2 (solo si necesitas Linux específicamente, menos control de red)

Elección de Hipervisor: VirtualBox para mayor flexibilidad y facilidad de configuración de red.

Fase 2: Instalación del Sistema Operativo Host

Para Windows Server:

- Descarga Windows Server 2019/2022 (versión de evaluación gratuita por 180 días)
- Asigna mínimo 4GB RAM y 40GB de disco
- Habilita Desktop Experience durante la instalación para facilitar la configuración

Para Linux Server:

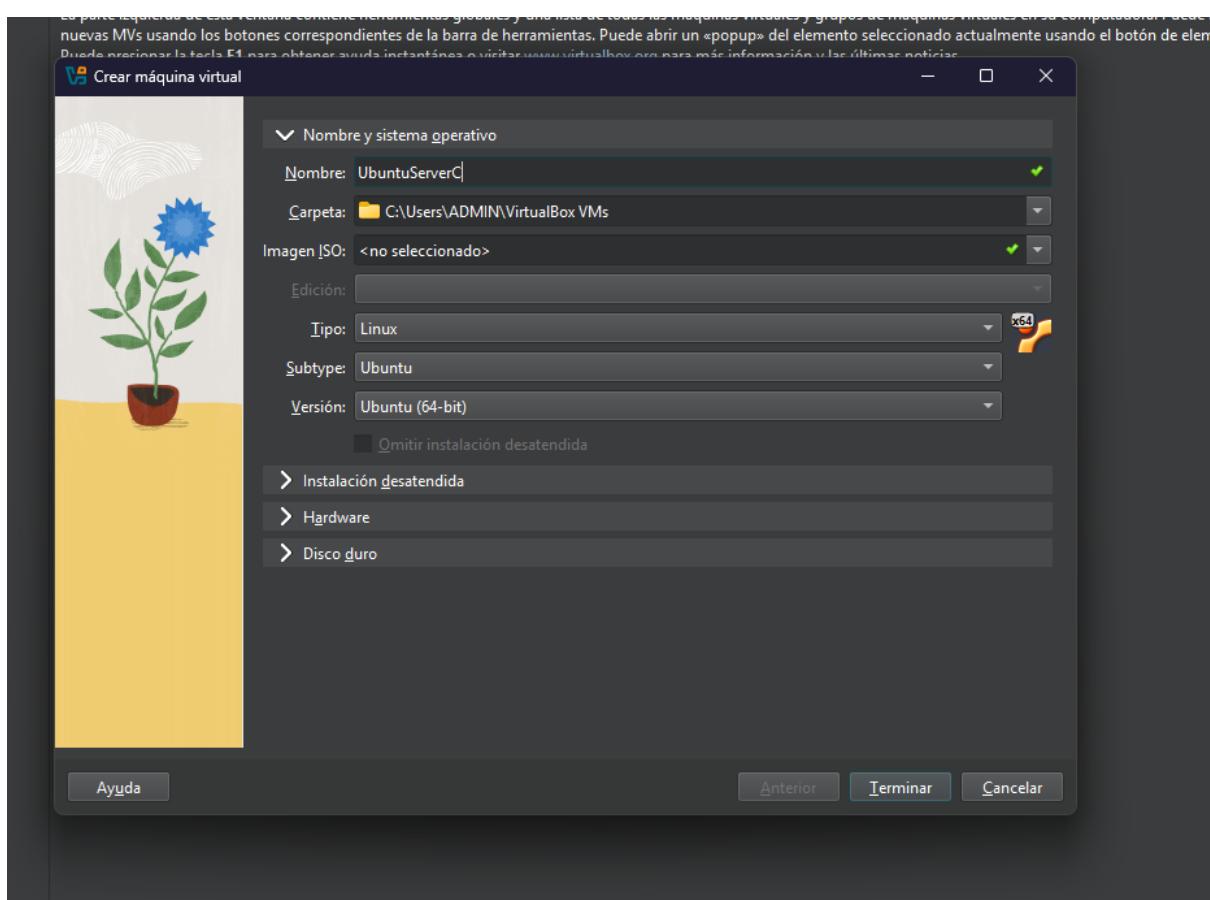
- Ubuntu Server 22.04 LTS o Debian 12 (más estables)
- Asigna mínimo 2GB RAM y 25GB de disco
- Instala con SSH habilitado para gestión remota

Fase 3: Configuración de Seguridad Básica

Creación de la Máquina Virtual en VirtualBox

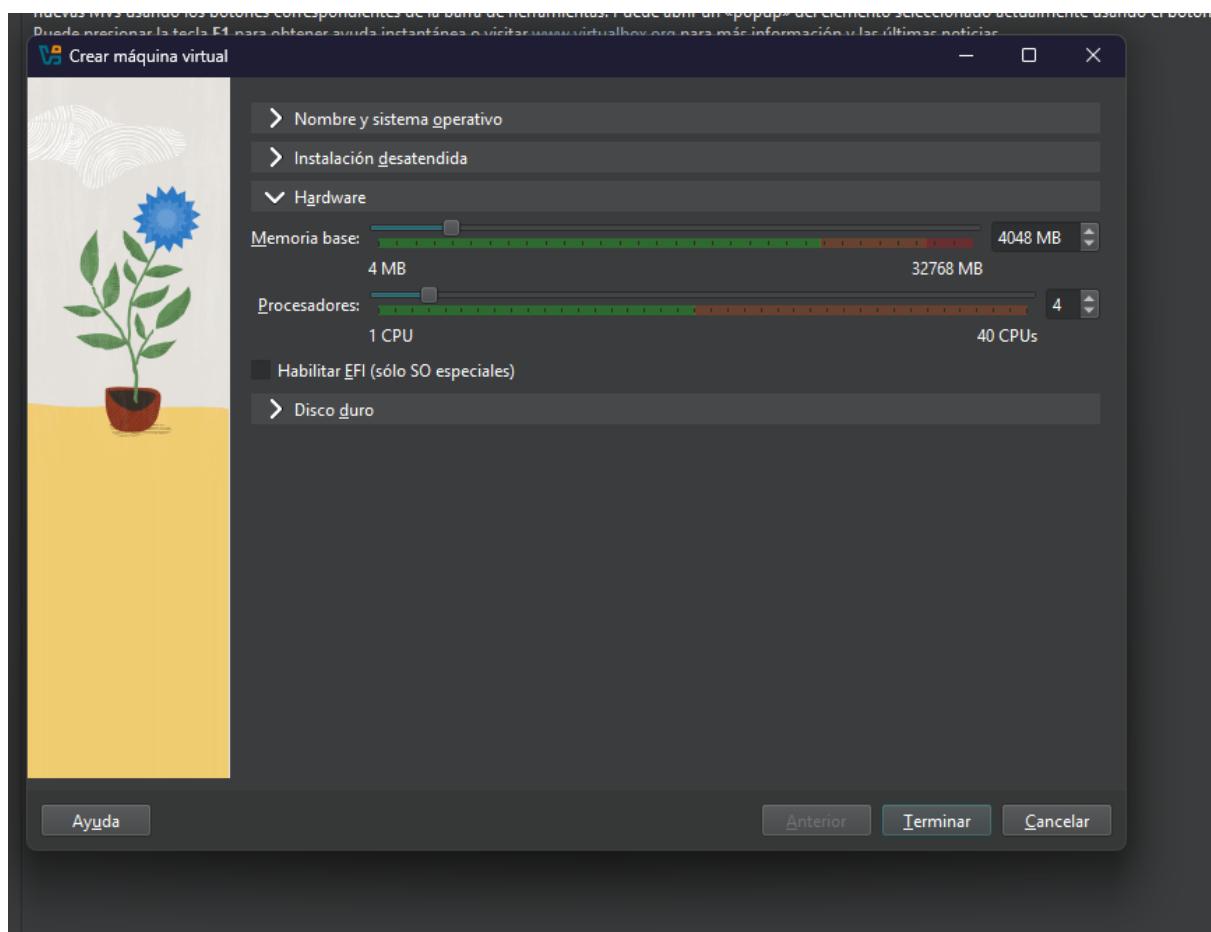
Configuración básica:

- **Nombre:** Ubuntu-ServerC
- **Carpeta:** Dejar la predeterminada o elige una ubicación con suficiente espacio
- **Tipo:** Linux
- **Versión:** Ubuntu (64-bit)



Asignación de Memoria RAM

- **Memoria RAM:** 2048 MB (2 GB) como mínimo
- **Recomendado:** 4096 MB (4 GB) si la PC tiene 16GB o más

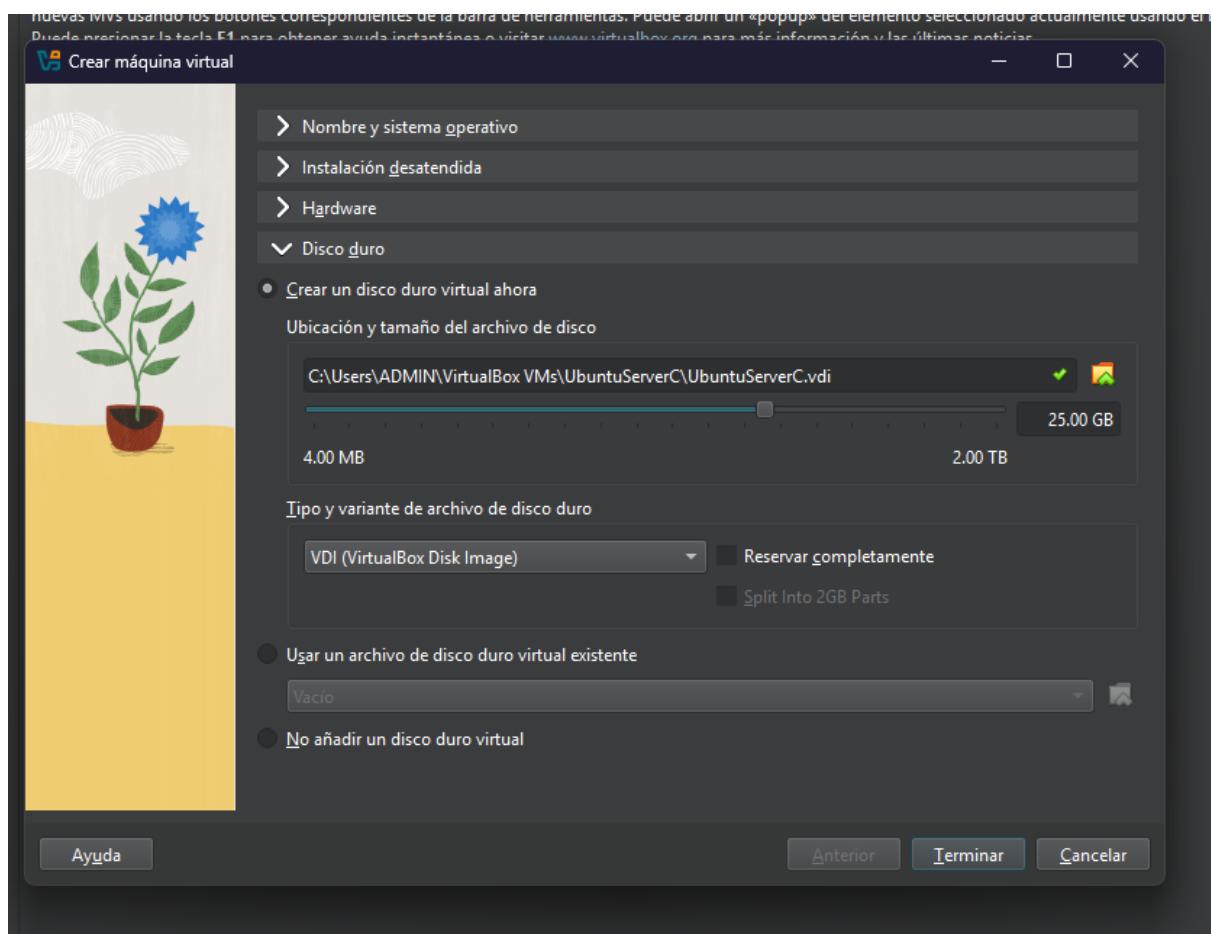


Disco Duro Virtual

1. Seleccionar "Crear un disco duro virtual ahora"

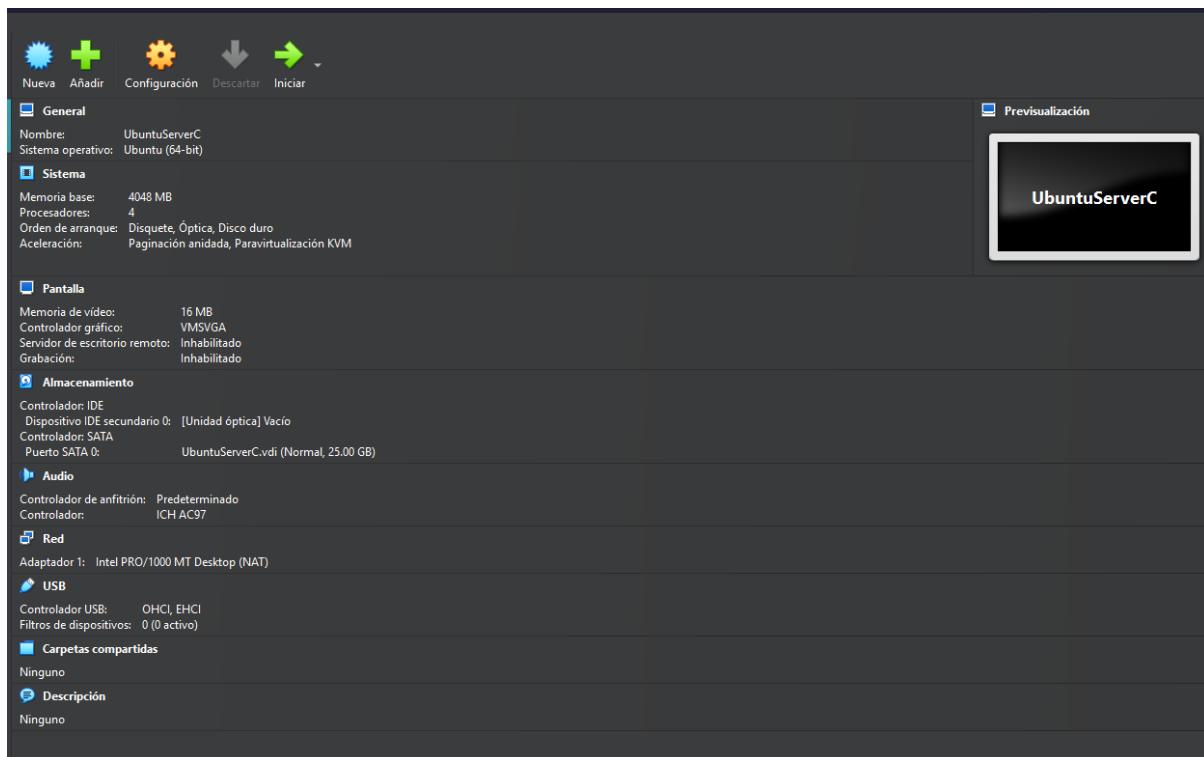
Configuración del disco:

- **Tipo de archivo:** VDI (VirtualBox Disk Image)
- **Almacenamiento:** Reservado dinámicamente
- **Tamaño:** 25 GB (mínimo) o 40 GB (recomendado)



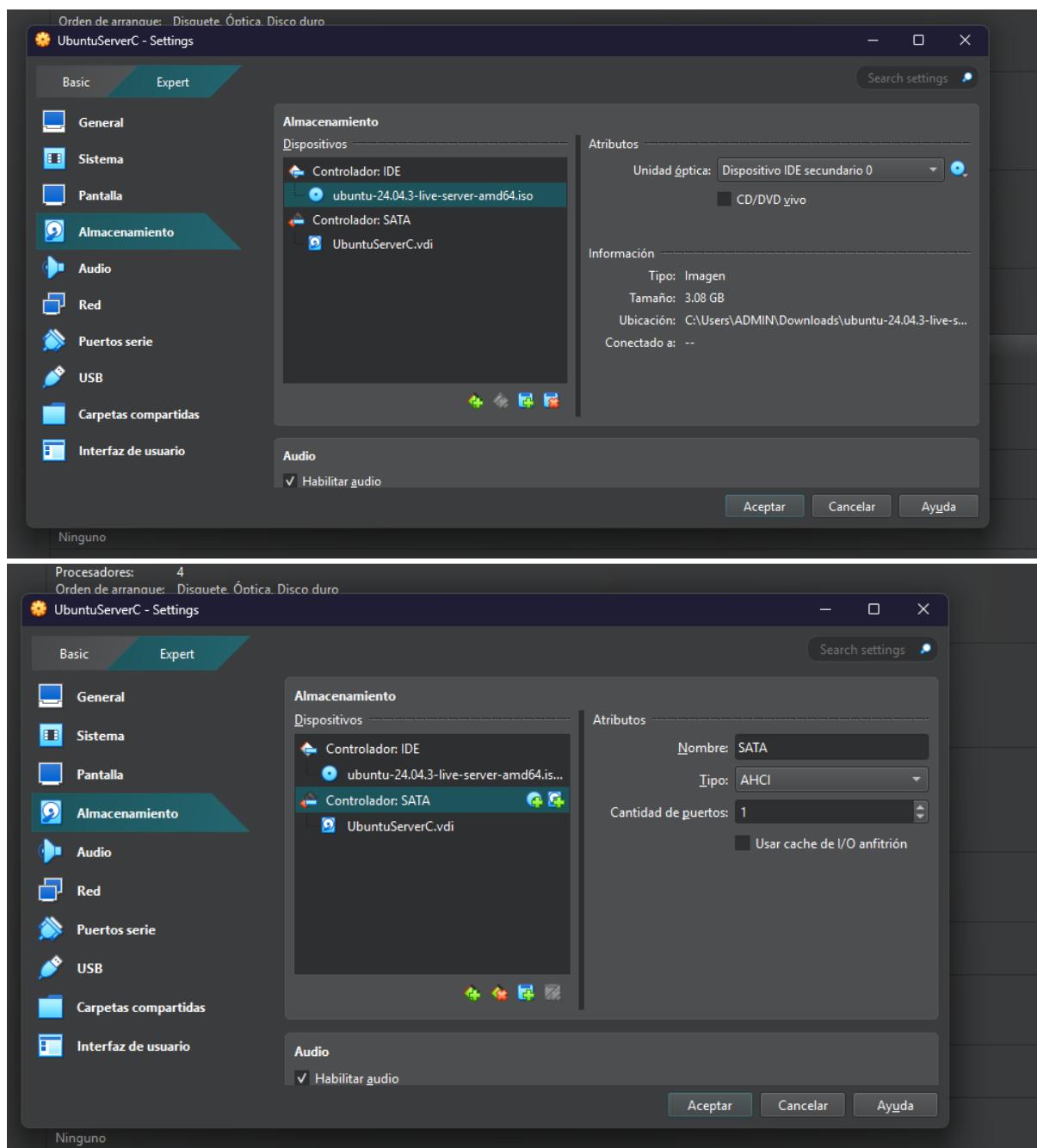
Configuración Adicional de la VM

Seleccionar la VM creada y hacer clic en "Configuración":



Almacenamiento:

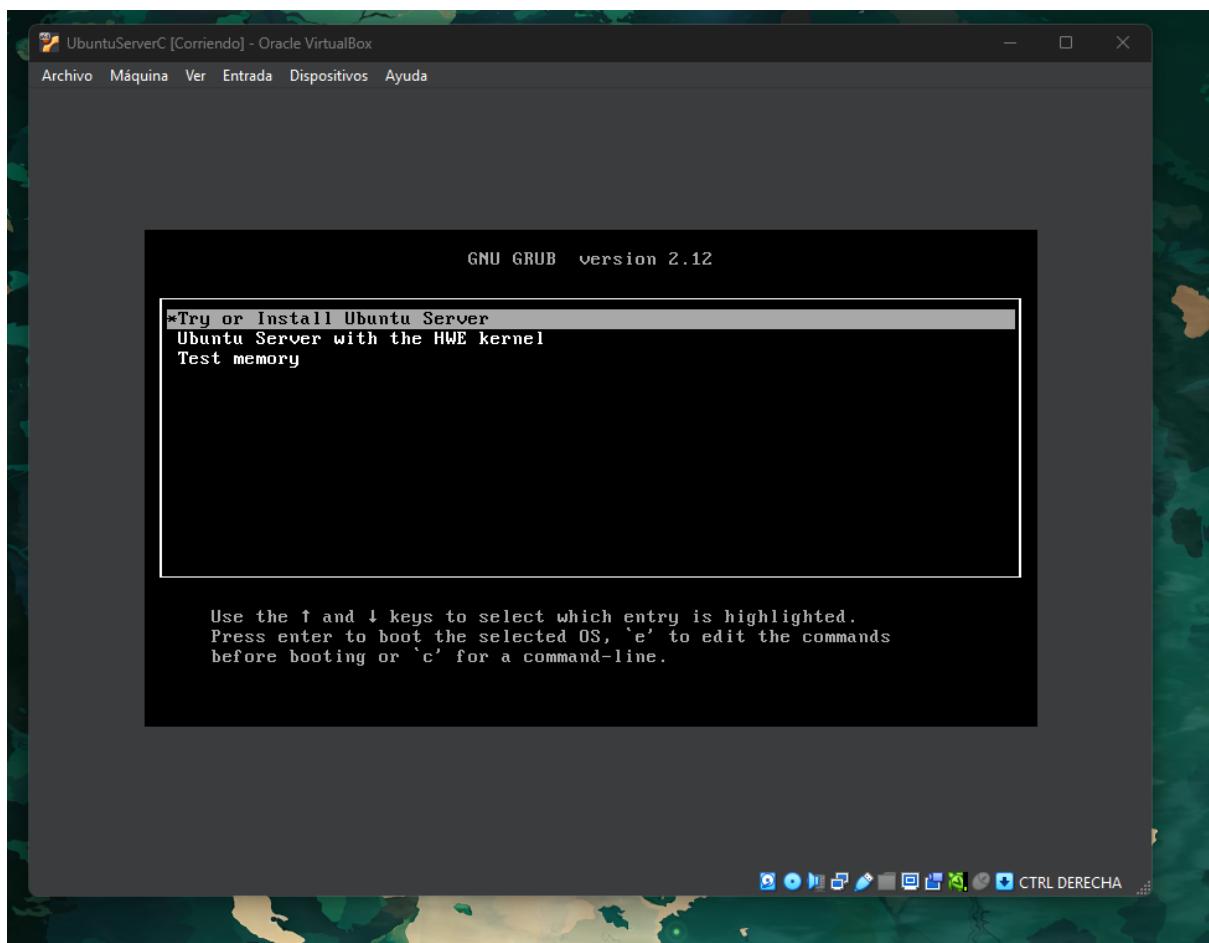
1. En "**Controlador: IDE**", seleccionar el disco vacío (ícono de CD)
2. En "**Atributos**", hacer clic en el ícono de disco junto a "**Unidad óptica:**"
3. Selecciona "**Elegir archivo de disco...**"
4. Busca y selecciona la ISO de Ubuntu Server descargada



Instalación de Ubuntu Server 22.04

Iniciar la Instalación

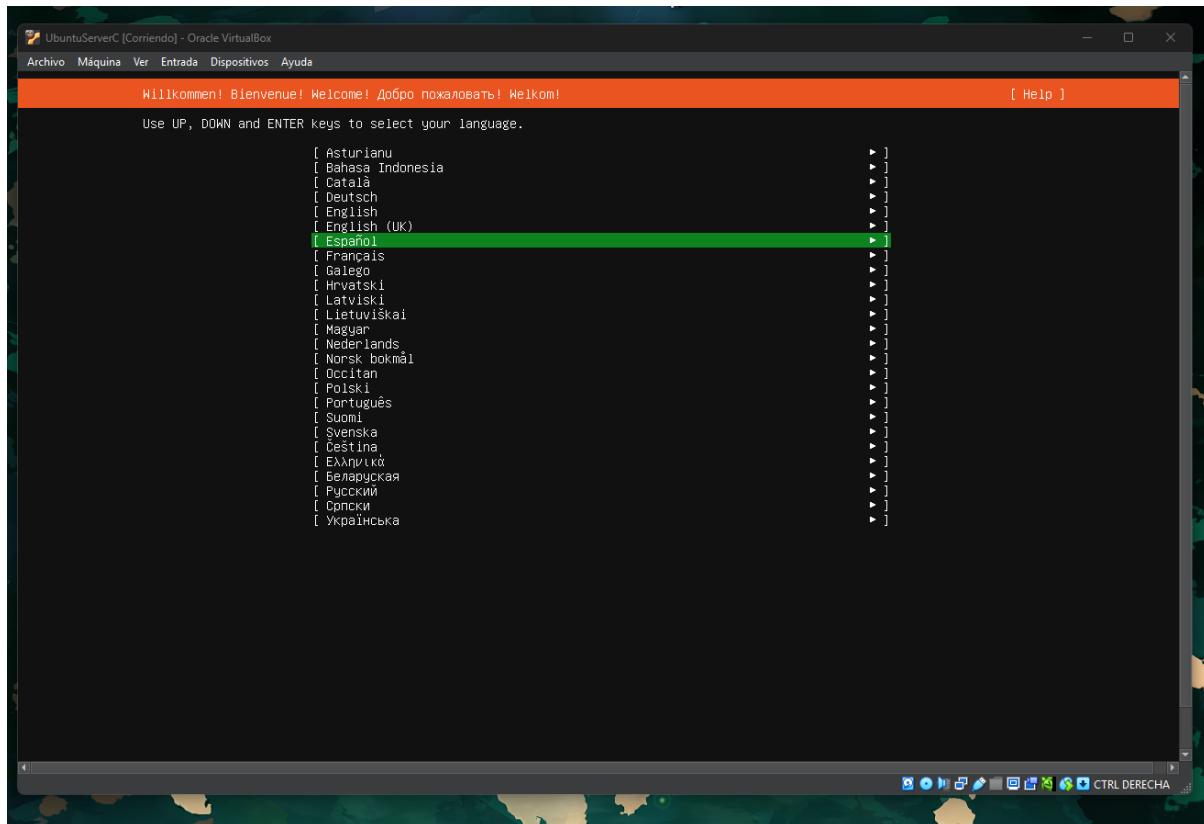
1. Selecciona la VM y haz clic en "Iniciar"
2. La VM arrancará desde la ISO de Ubuntu Server



Proceso de Instalación

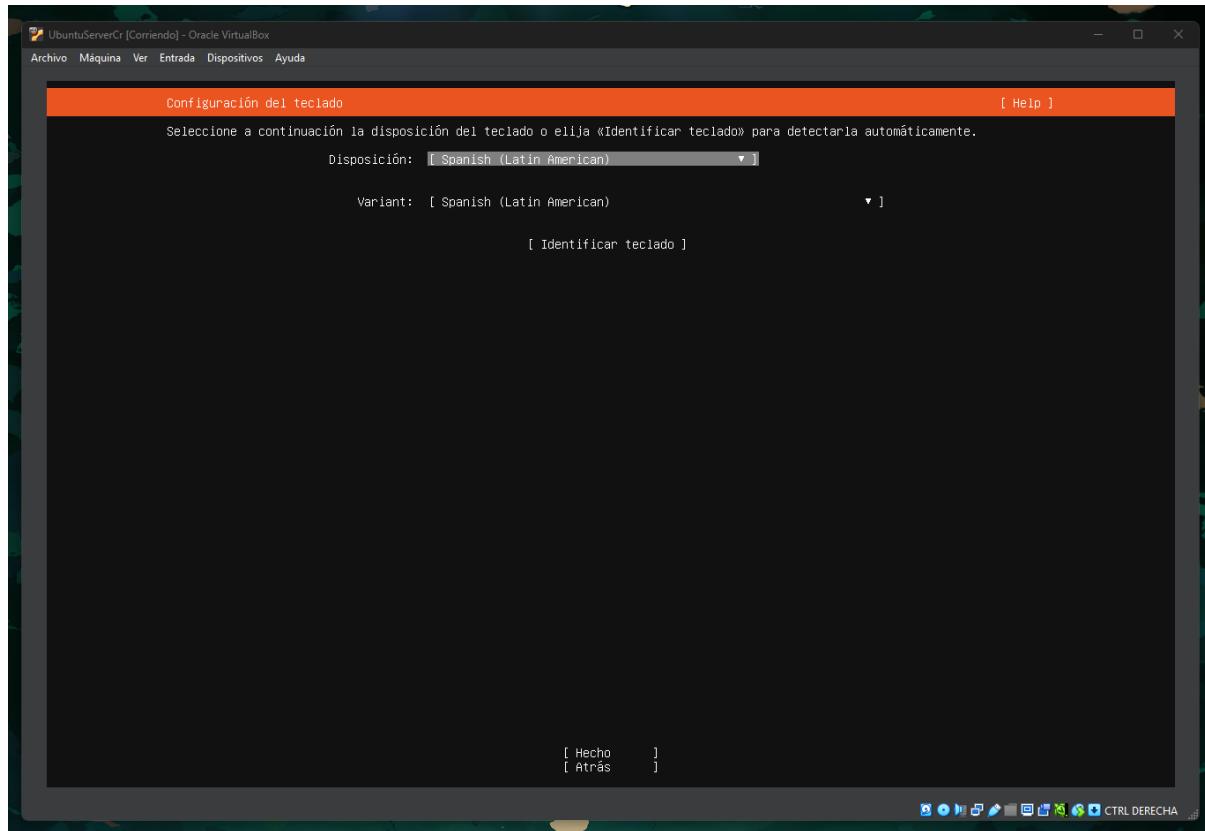
Selección de idioma:

- Seleccionar "Español"



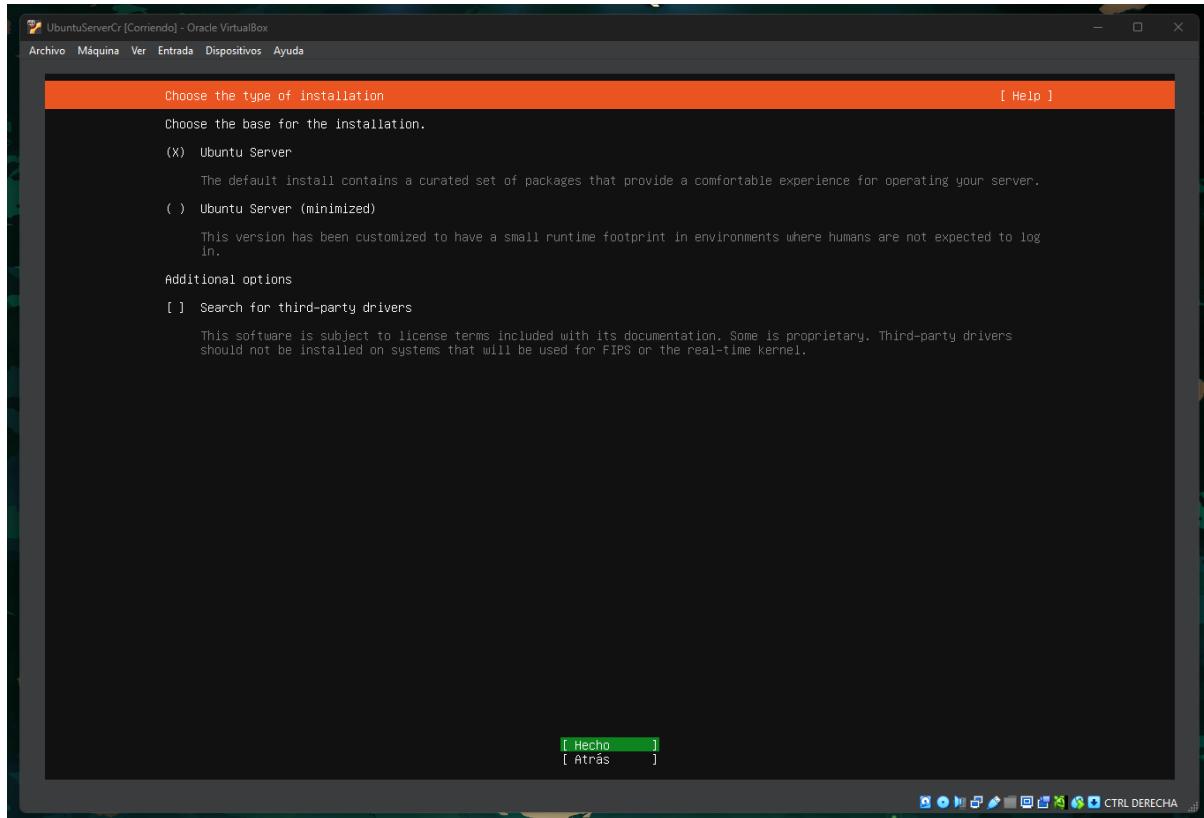
Configuración de teclado:

- Layout: "**Spanish (Latin American)**" o su distribución de teclado
- Puede probarlo escribiendo en el campo de prueba



Tipo de instalación:

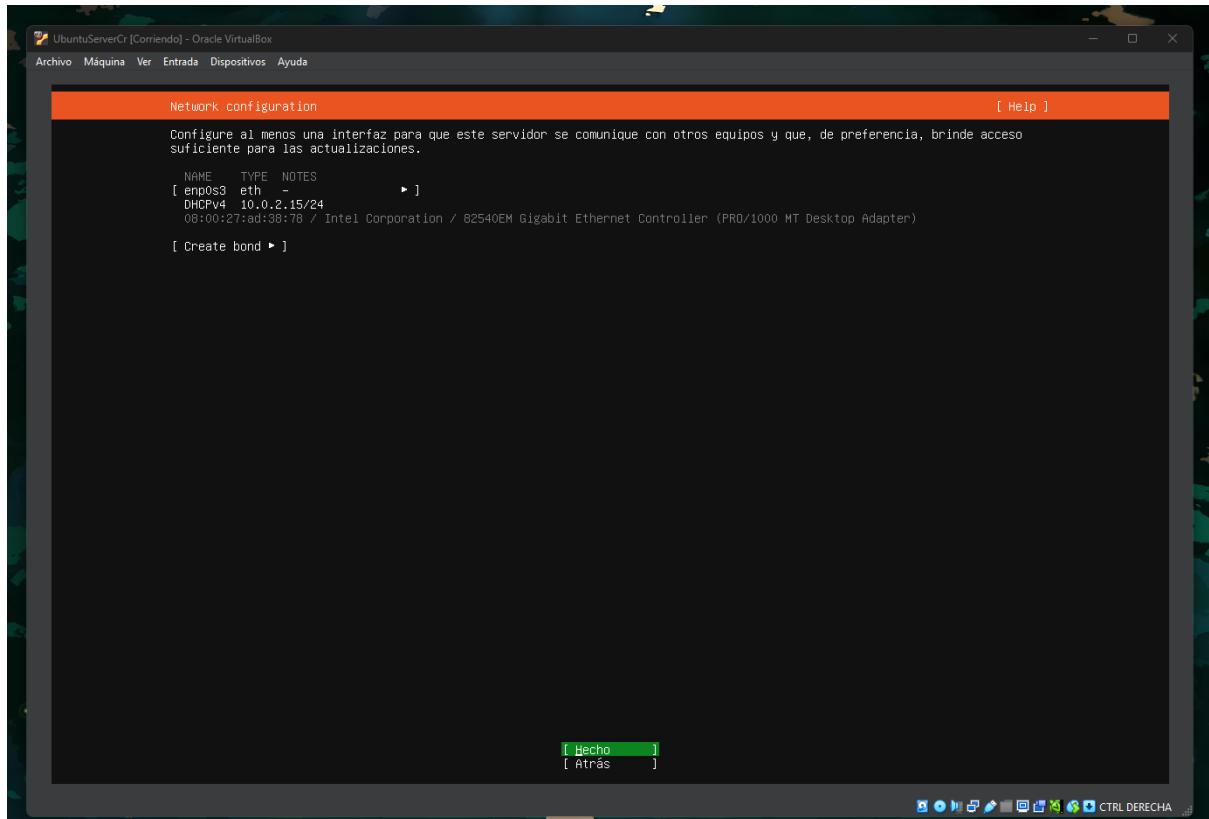
- Seleccionar "**Ubuntu Server**" (opción por defecto)



Configuración de red:

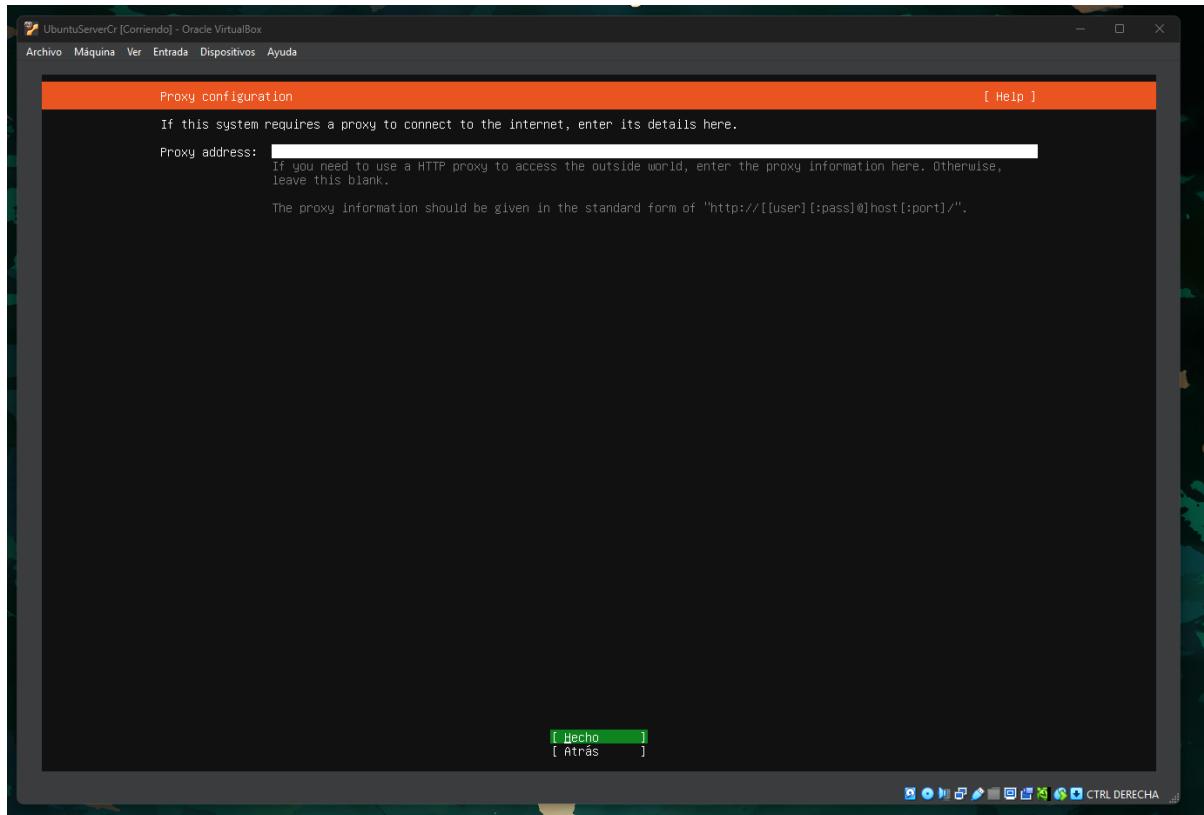
- Debería detectar automáticamente la interfaz de red (enp0s3)
- Mostrará una IP asignada por DHCP (ejemplo: 10.0.2.15)

Anota esta IP (se usa más adelante)



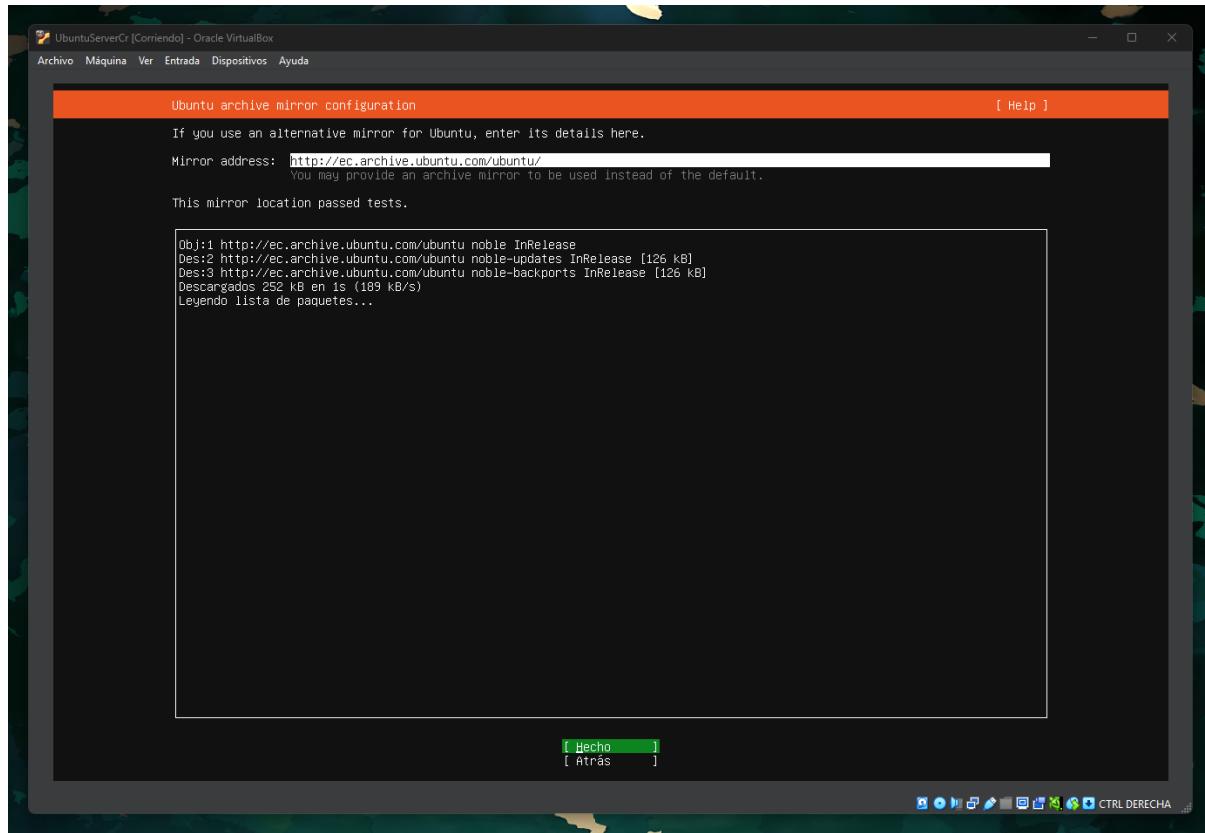
Configuración de proxy:

- Dejar en blanco si no usa proxy



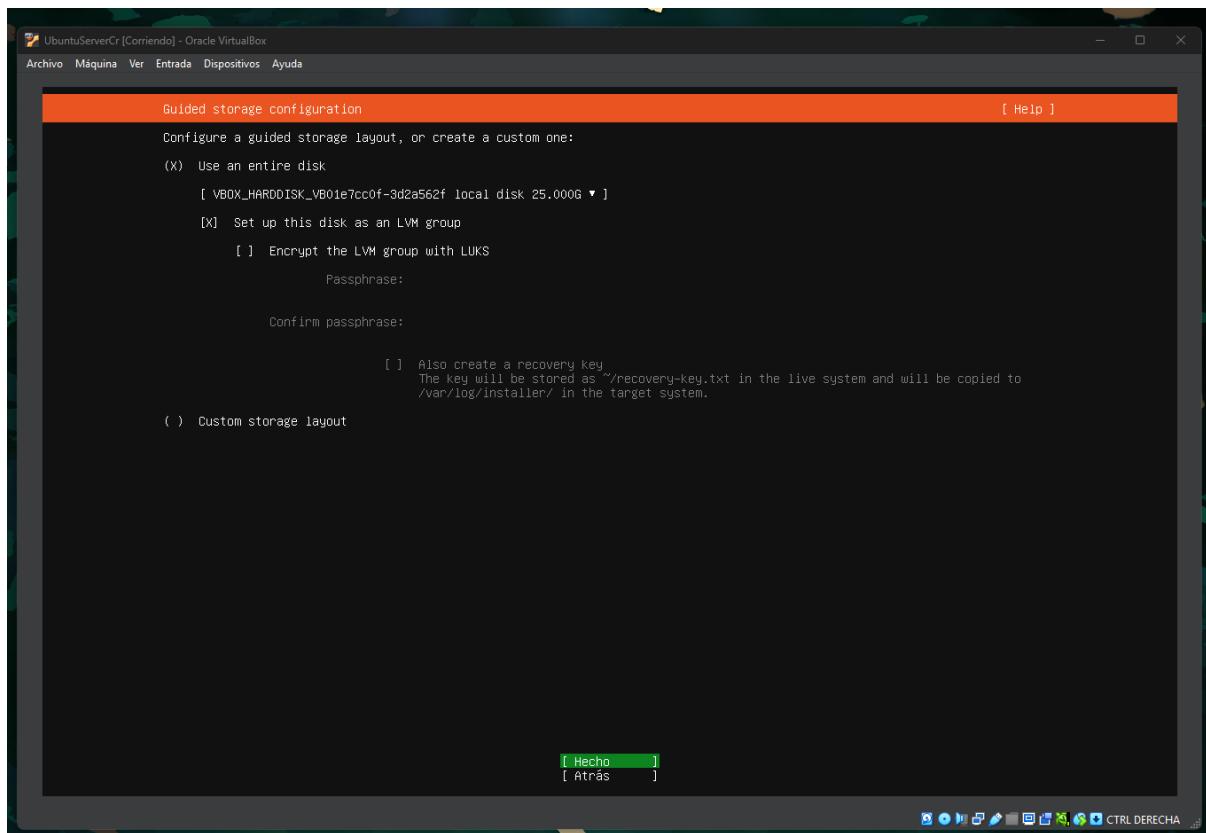
Mirror de Ubuntu:

- Dejar el mirror por defecto

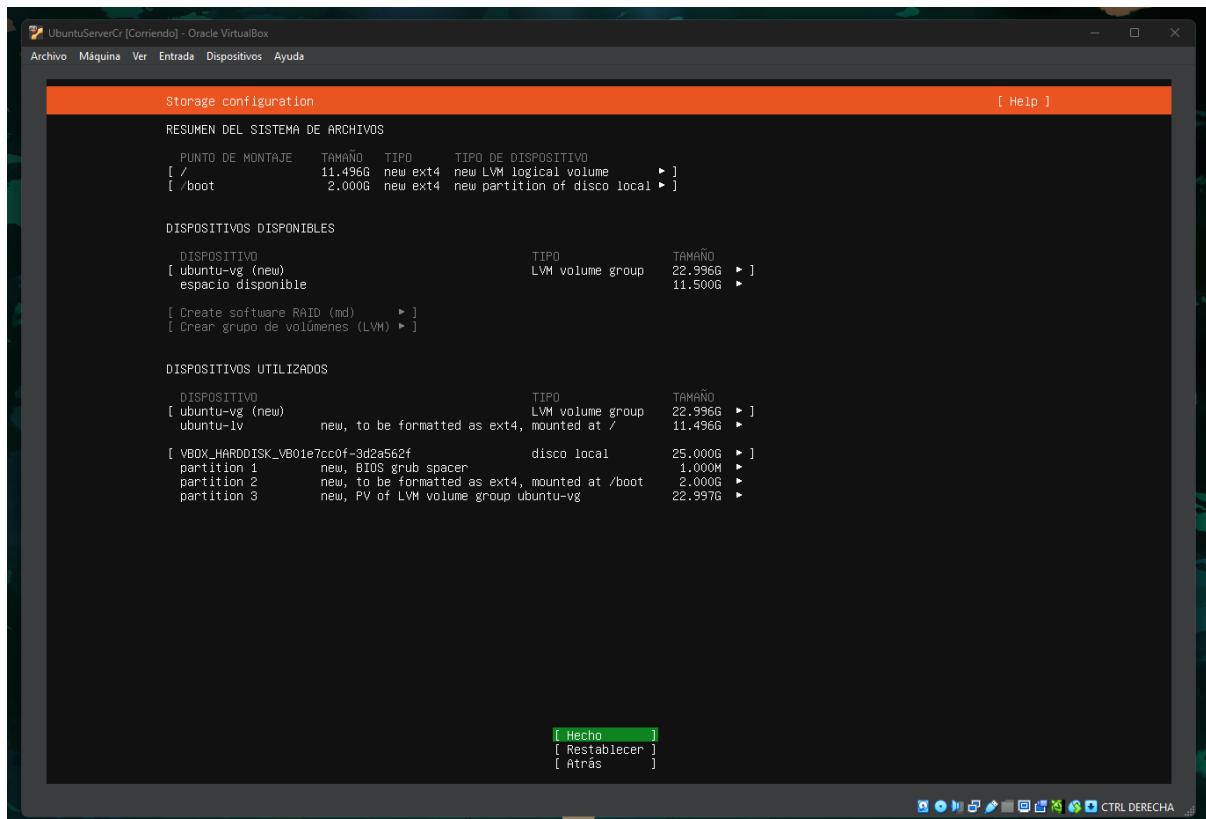


Configuración de almacenamiento:

- Seleccionar "**Use an entire disk**"
- Confirmar el disco virtual creado
- **NO** configure LVM de momento (más simple)



- Confirmar el resumen de particiones

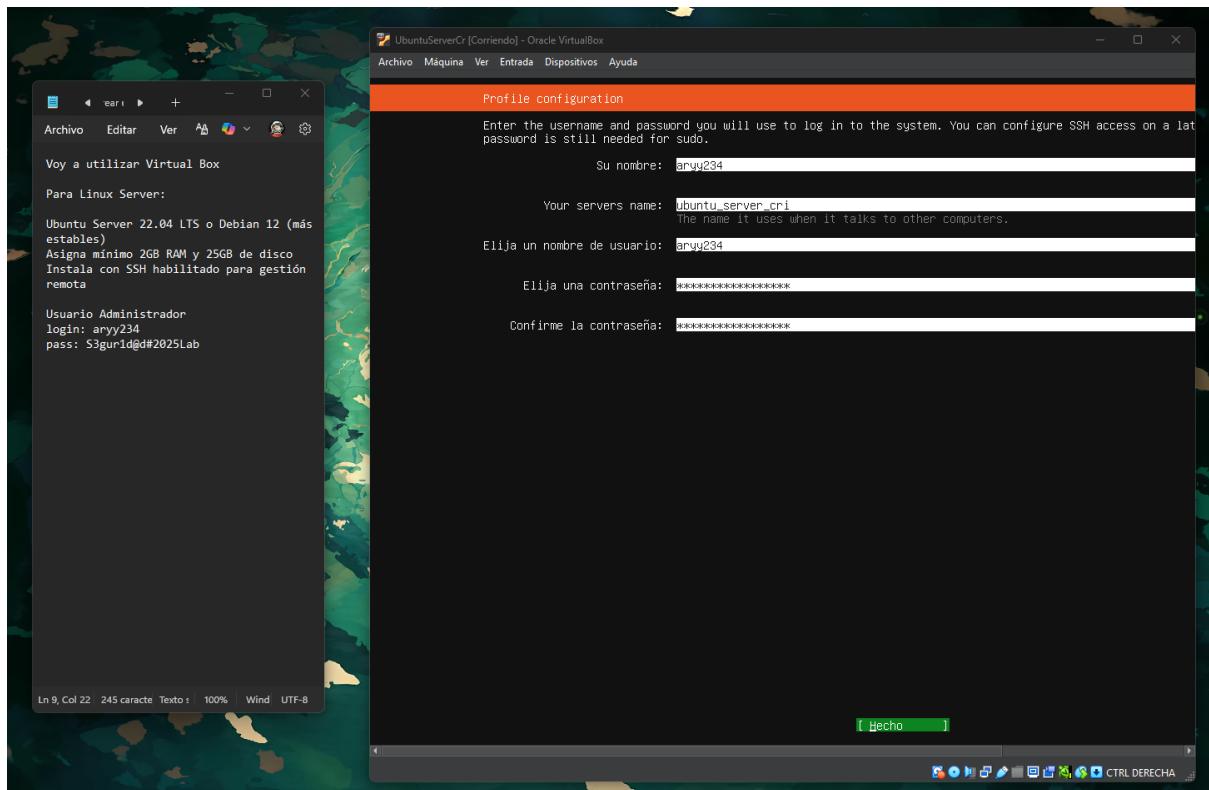


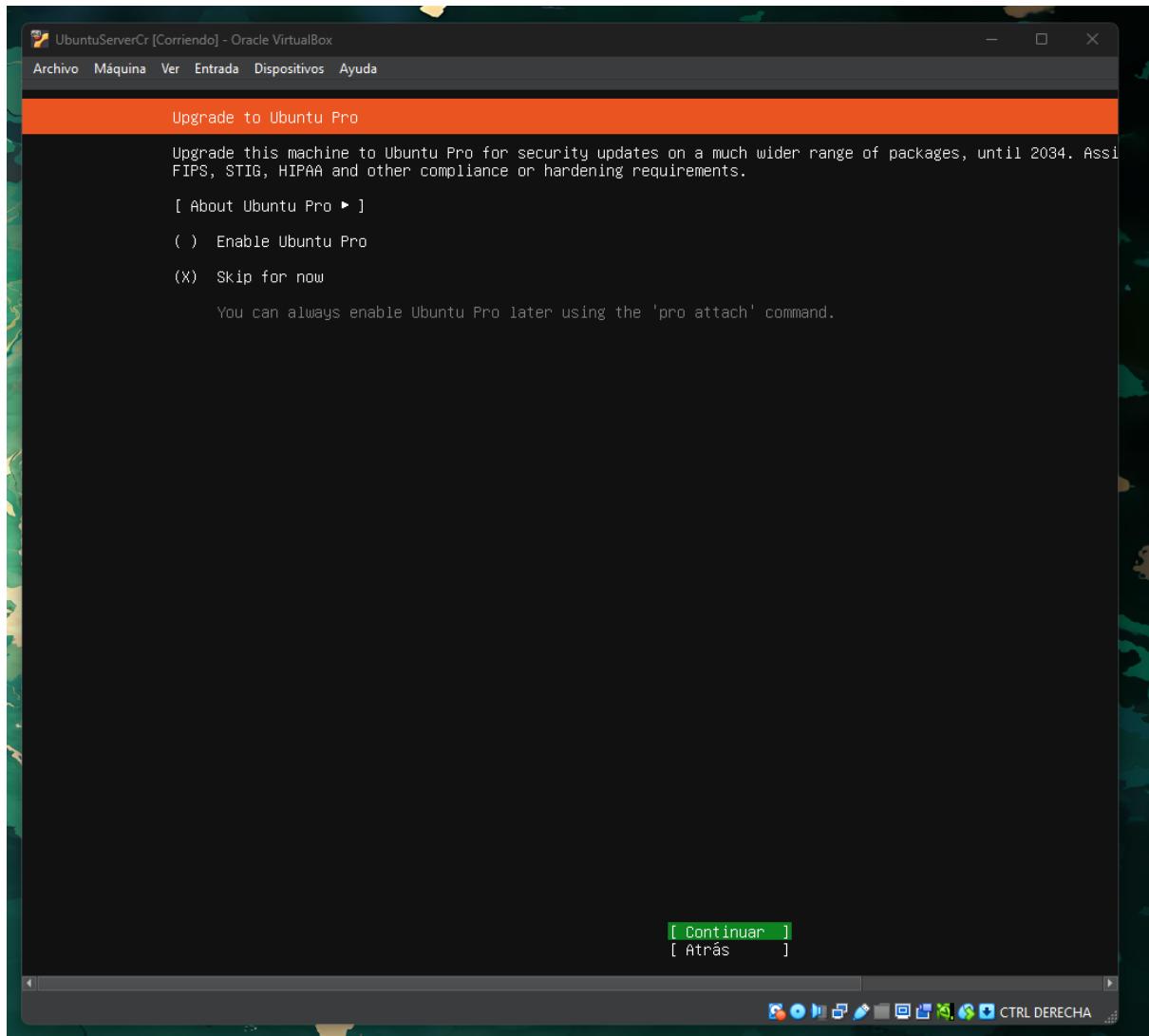
Configuración de perfil:

Datos a configurar:

- **Your name:** aryy234
- **Your server name:** ubuntu-server-cri
- **Username:** aryy234
- **Password:** Contraseña segura (ejemplo: S3gur1d@d#2025Lab)
- **Confirm your password:** Repite la contraseña

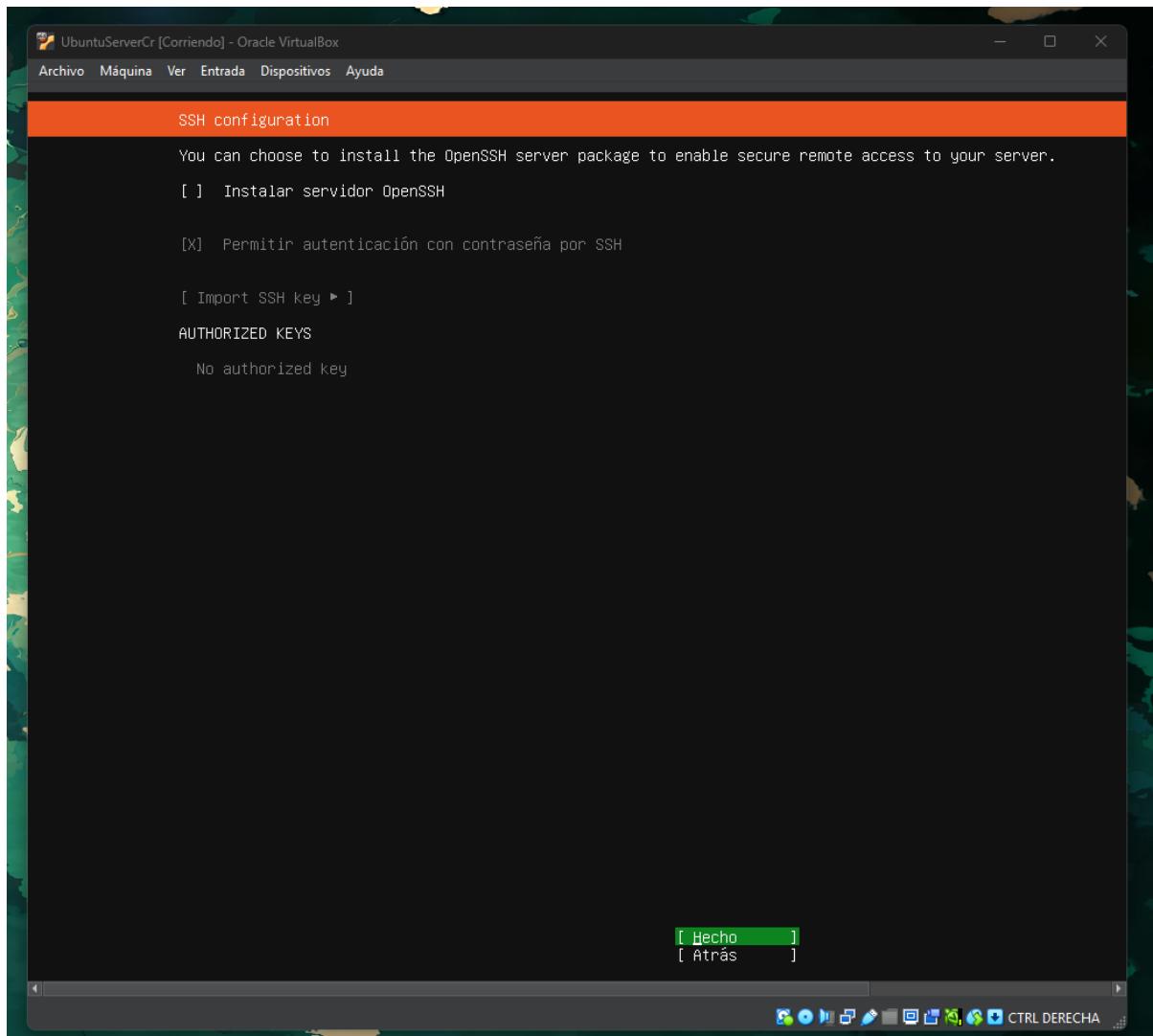
IMPORTANTE: Anotar estos datos, lo necesitará para acceder al servidor.





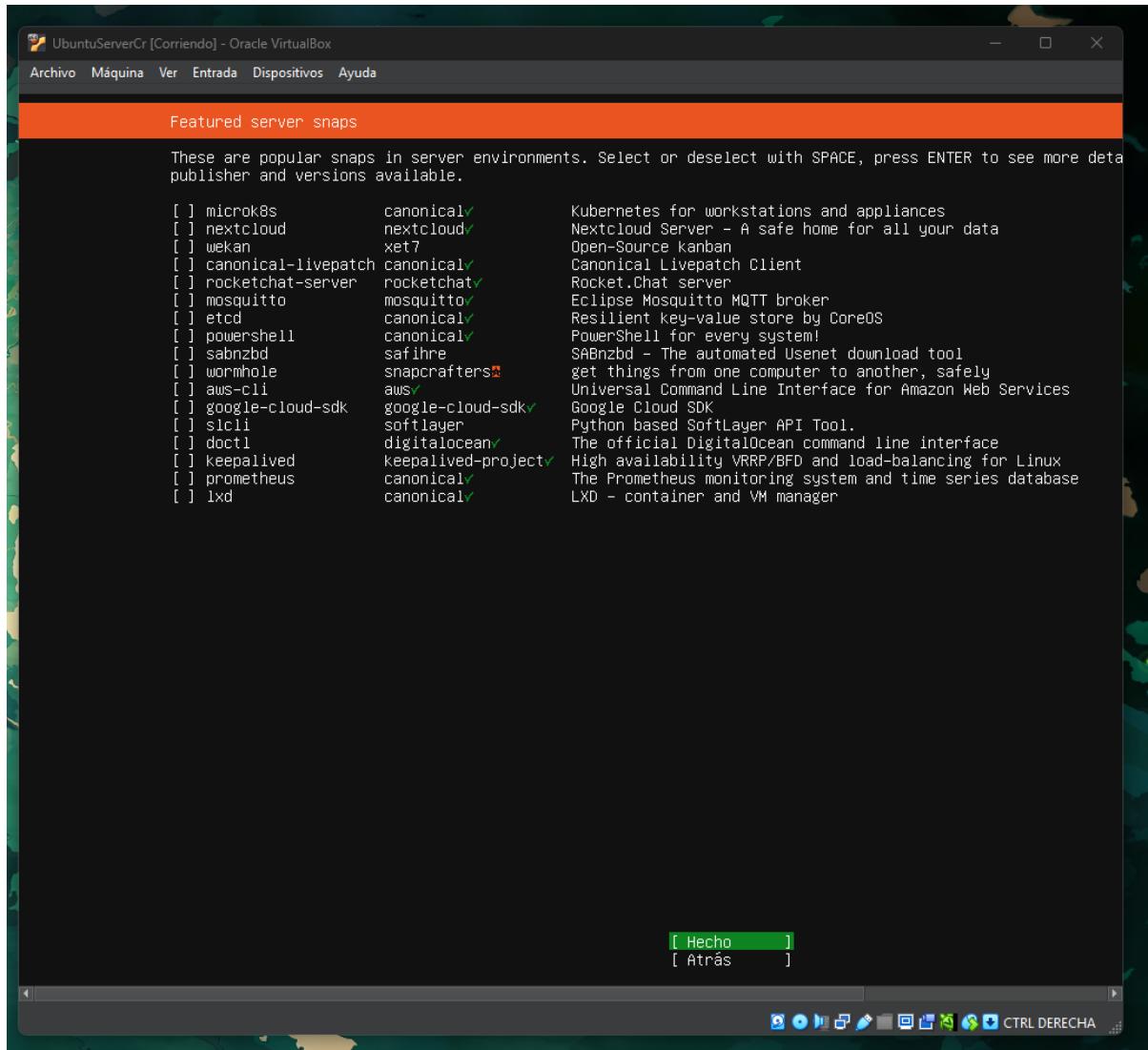
SSH Setup:

- **Marcar la opción:** "Instalar servidor OpenSSH"
- **NO** importe identidad SSH de GitHub/Launchpad



Featured Server Snaps:

- No seleccione ninguno por ahora (puede instalar después)



Esperar la Instalación

- El proceso tardará 5-15 minutos dependiendo del hardware
- Verá el progreso de descarga e instalación de paquetes

The screenshot shows a terminal window titled "UbuntuServerCr [Corriendo] - Oracle VirtualBox". The window has a dark theme with an orange header bar. The title bar includes menu items: Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda. The main area of the terminal displays a log of system commands being executed:

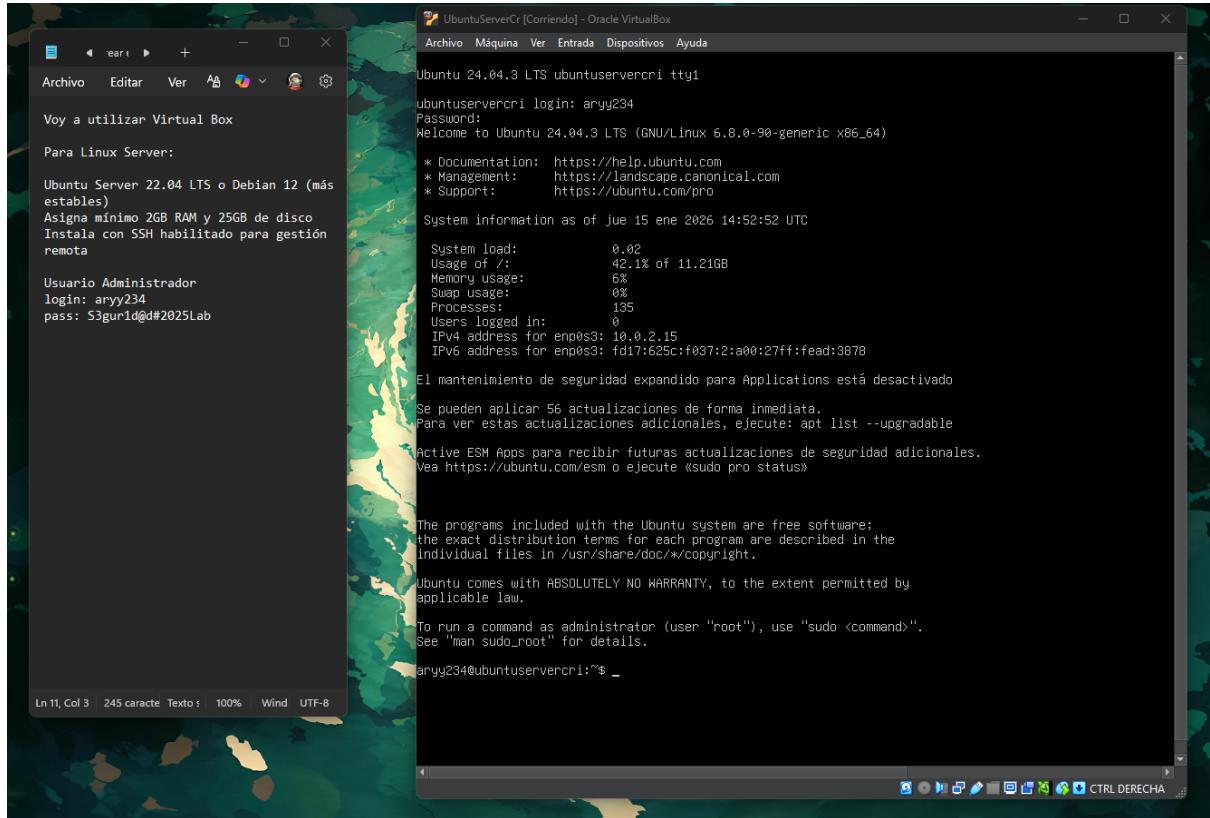
```
configuring format: format-0
configuring partition: partition-2
configuring lvm_vvolgroup: lvm_vvolgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
    acquiring and extracting image from cp:///tmp/tmpdmmmr3g0/mount
configuring keyboard
curtin command in-target
executing curtin install curthooks step
curtin command install
configuring installed system
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['grub-pc']
configuring iscsi service
configuring raid (mdadm) service
configuring NVMe over TCP
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
copying metadata from /cdrom
final system configuration
calculating extra packages to install
configuring cloud-init
downloading and installing security updates
curtin command in-target /
```

At the bottom of the terminal window, there is a link "[View full log]" and a standard Linux desktop toolbar with icons for file operations and system status.

Primer Acceso al Servidor

Iniciar Sesión

1. Esperar a que aparezca la pantalla de login
2. Ingresar **username:** admin
3. Ingresar **password:** (la contraseña que configuró)



Verificar Instalación

```
PS C:\Users\ADMIN> ssh aryy234@192.168.1.39
The authenticity of host '192.168.1.39 (192.168.1.39)' can't be established.
ED25519 key fingerprint is SHA256:U93Nx9IwUri3UK/TdRu38C3Ma2K8VMg3GtoLydclf98.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.39' (ED25519) to the list of known hosts.
arryy234@192.168.1.39's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of jue 15 ene 2026 16:51:58 UTC

System load: 0.0          Processes:           138
Usage of /:   45.0% of 11.21GB  Users logged in:      1
Memory usage: 6%          IPv4 address for enp0s3: 192.168.1.39
Swap usage:   0%

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»
```

arryy234@ubuntuservercri:~\$

Configuración Post-Instalación

Actualizar el Sistema

```
andresosorio@innovasytrusservidor:~$ dpkg -l | grep openssh-server
andresosorio@innovasytrusservidor:~$ sudo apt update
[sudo] password for andresosorio:
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Obj:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:3 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Obj:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Des:5 http://archive.ubuntu.com/ubuntu/noble/main Translation-es [325 kB]
Des:6 http://archive.ubuntu.com/ubuntu/noble/restricted Translation-es [816 B]
Des:7 http://archive.ubuntu.com/ubuntu/noble/universe Translation-es [1.371 kB]
Des:8 http://archive.ubuntu.com/ubuntu/noble/multiverse Translation-es [63,1 kB]
Descargados 1.759 kB en 2s (978 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 26 paquetes. Ejecute «apt list --upgradable» para verlos.
andresosorio@innovasytrusservidor:~$ sudo _
```

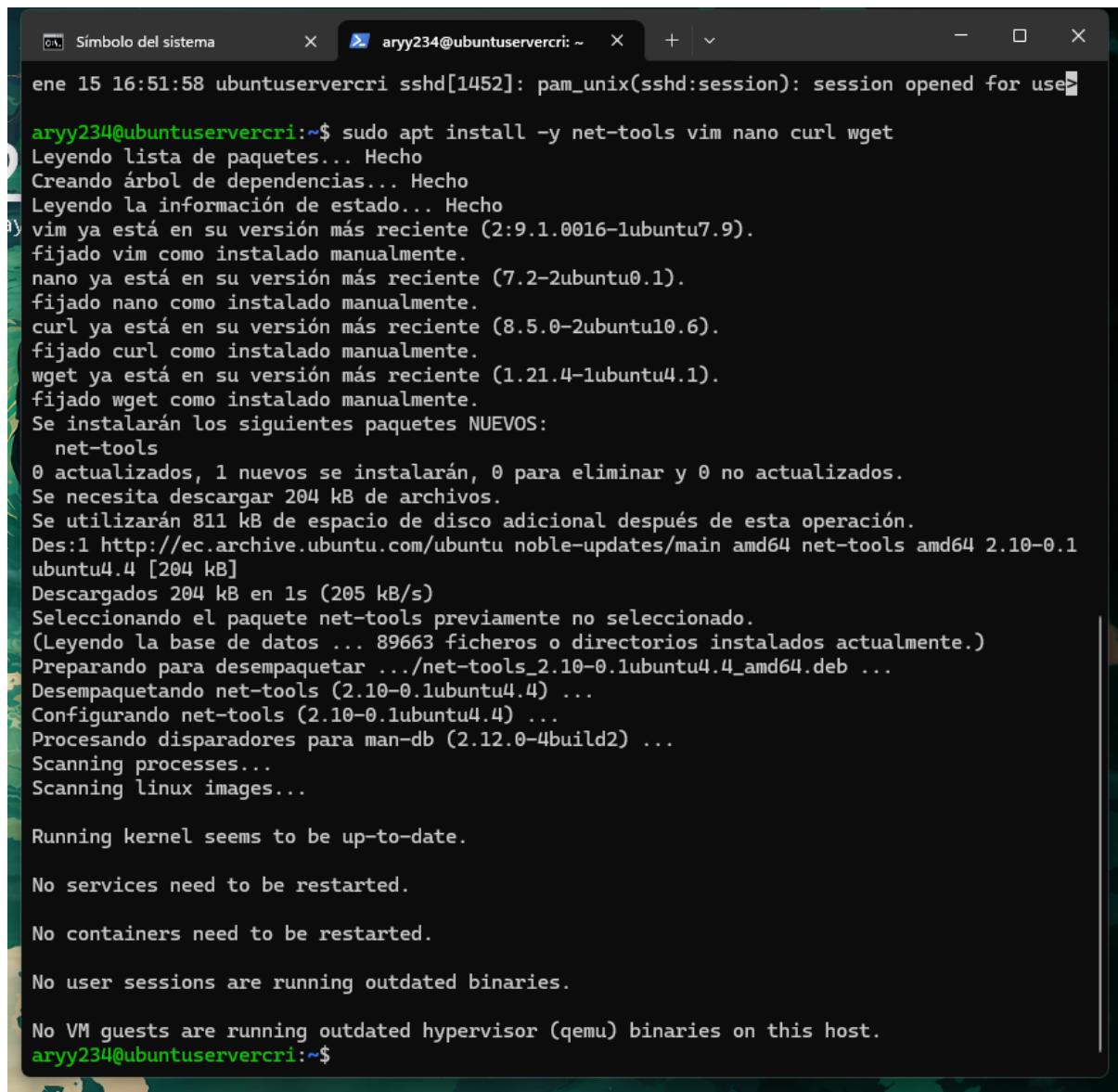
```
Se pueden actualizar 26 paquetes. Ejecute «apt list --upgradable» para verlos.
andresosorio@innovasytrusservidor:~$ sudo apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
```

```
andresosorio@innovasytrusservidor:~$ sudo apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libwrap0 ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass
Se instalarán los siguientes paquetes NUEVOS:
  libwrap0 ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 880 kB de archivos.
```

Instalar Herramientas Básicas

Explicación:

- **net-tools:** Incluye comandos como ifconfig, netstat
- **curl/wget:** Descarga de archivos
- **vim/nano:** Editores de texto



```
Símbolo del sistema aryy234@ubuntuservercri: ~
ene 15 16:51:58 ubuntuservercri sshd[1452]: pam_unix(sshd:session): session opened for user aryy234
aryy234@ubuntuservercri:~$ sudo apt install -y net-tools vim nano curl wget
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
  vim ya está en su versión más reciente (2:9.1.0016-1ubuntu7.9).
  fijado vim como instalado manualmente.
  nano ya está en su versión más reciente (7.2-2ubuntu0.1).
  fijado nano como instalado manualmente.
  curl ya está en su versión más reciente (8.5.0-2ubuntu10.6).
  fijado curl como instalado manualmente.
  wget ya está en su versión más reciente (1.21.4-1ubuntu4.1).
  fijado wget como instalado manualmente.
Se instalarán los siguientes paquetes NUEVOS:
  net-tools
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 204 kB de archivos.
Se utilizarán 811 kB de espacio de disco adicional después de esta operación.
Des:1 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 net-tools amd64 2.10-0.1
ubuntu4.4 [204 kB]
Descargados 204 kB en 1s (205 kB/s)
Seleccionando el paquete net-tools previamente no seleccionado.
(Leyendo la base de datos ... 89663 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../net-tools_2.10-0.1ubuntu4.4_amd64.deb ...
Desempaquetando net-tools (2.10-0.1ubuntu4.4) ...
Configurando net-tools (2.10-0.1ubuntu4.4) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
aryy234@ubuntuservercri:~$
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
arryy234@ubuntuservercri:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
    link/ether 08:00:27:ad:38:78 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.39/24 metric 100 brd 192.168.1.255 scope global dynamic enp0s3
            valid_lft 84436sec preferred_lft 84436sec
        inet6 fe80::a00:27ff:fead:3878/64 scope link
            valid_lft forever preferred_lft forever
arryy234@ubuntuservercri:~$ |
```

Configurar Contraseña de Root

Ingresar una contraseña segura diferente a la del usuario admin.

Ejemplo: R00t#S3cur3Pass2025

```
arryy234@ubuntuservercri:~$ sudo systemctl status ssh
[sudo] password for aryy234:
Sorry, try again.
[sudo] password for aryy234:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Thu 2026-01-15 16:40:49 UTC; 34min ago
  TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 1303 (sshd)
    Tasks: 1 (limit: 4543)
   Memory: 4.0M (peak: 5.2M)
      CPU: 40ms
     CGroup: /system.slice/ssh.service
             └─1303 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

ene 15 16:40:49 ubuntuservercri systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
ene 15 16:40:49 ubuntuservercri sshd[1303]: Server listening on 0.0.0.0 port 22.
ene 15 16:40:49 ubuntuservercri sshd[1303]: Server listening on :: port 22.
ene 15 16:40:49 ubuntuservercri systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
ene 15 16:51:58 ubuntuservercri sshd[1452]: Accepted password for aryy234 from 192.168.1.24 port 55241 ssh2
ene 15 16:51:58 ubuntuservercri sshd[1452]: pam_unix(sshd:session): session opened for user aryy234(uid=1000) by aryy234@ubuntuservercri:~$
```

Crear los Usuarios Requeridos

Usuario con privilegios completos (UserAG03):

```
# Crear usuario  
sudo useradd -m -s /bin/bash UserAG03  
  
# Asignar contraseña  
sudo passwd UserAG03  
  
# Agregar a grupo sudo (privilegios de administrador)  
sudo usermod -aG sudo UserAG03  
  
# Verificar grupos  
groups UserAG03
```

```
aryy234@ubuntuservercri:~$ cls  
Command 'cls' not found, but there are 20 similar ones.  
aryy234@ubuntuservercri:~$ sudo useradd -m -s /bin/bash UserAG03  
[sudo] password for aryy234:  
Sorry, try again.  
[sudo] password for aryy234:  
aryy234@ubuntuservercri:~$ sudo useradd -m -s /bin/bash UserAG03  
useradd: user 'UserAG03' already exists  
aryy234@ubuntuservercri:~$ sudo passwd UserAG03  
New password:  
Retype new password:  
passwd: password updated successfully  
aryy234@ubuntuservercri:~$ sudo usermod -aG sudo UserAG03  
aryy234@ubuntuservercri:~$ groups UserAG03  
UserAG03 : UserAG03 sudo  
aryy234@ubuntuservercri:~$ sudo useradd -m -s /bin/bash UserBG03  
aryy234@ubuntuservercri:~$ sudo passwd UserBG03  
New password:  
Retype new password:  
passwd: password updated successfully  
aryy234@ubuntuservercri:~$ cat /etc/passwd | grep UserG  
aryy234@ubuntuservercri:~$ |
```

Usuario con privilegios mínimos (UserBG03):

Crear usuario

```
sudo useradd -m -s /bin/bash UserBG03
```

Asignar contraseña

```
sudo passwd UserBG03
```

Este usuario NO se agrega al grupo sudo

Verificar usuarios creados:

Ver todos los usuarios

```
cat /etc/passwd | grep UserG
```

Probar cambio de usuario

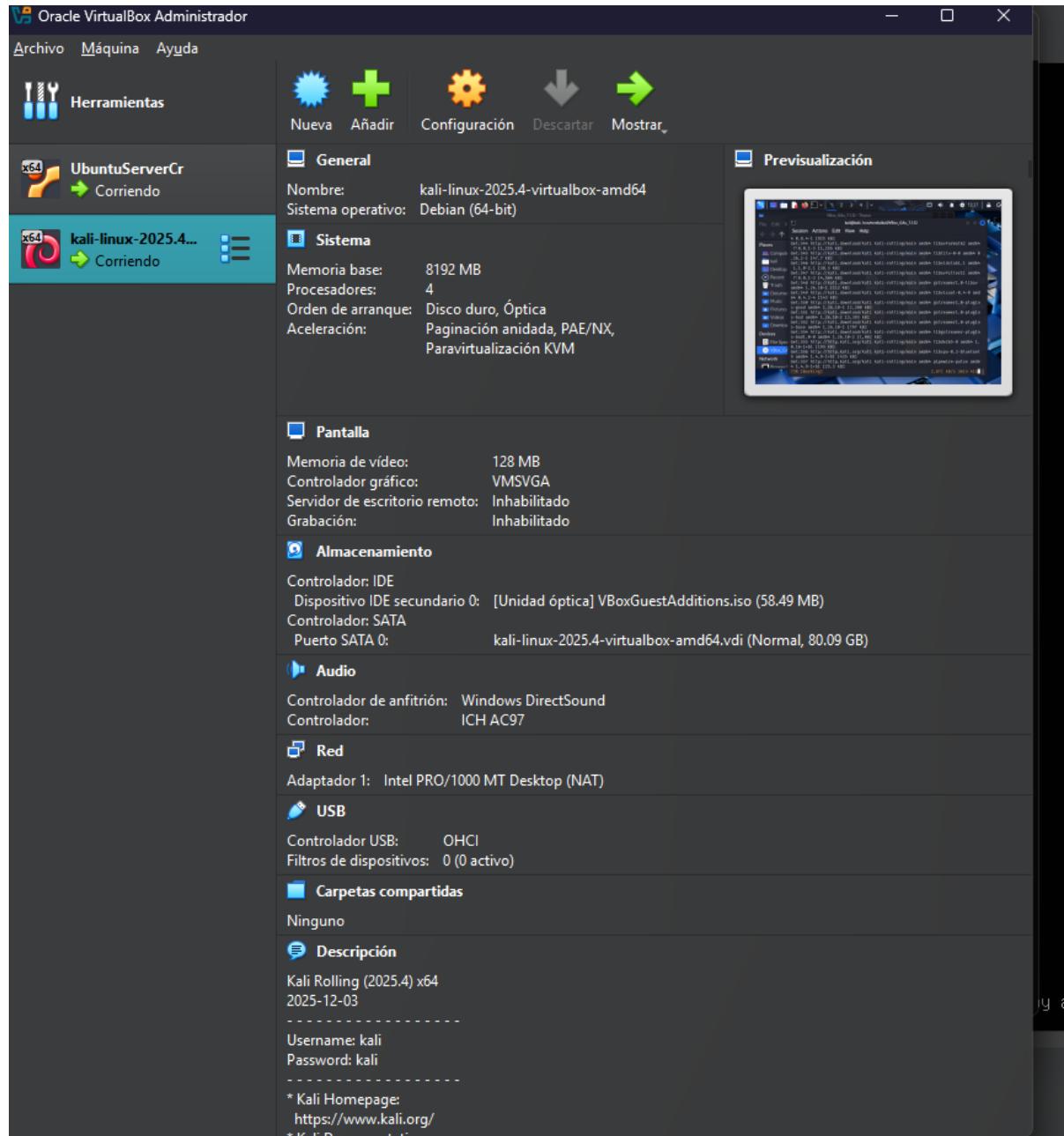
```
su – UserAG03
```

```
aryy234@ubuntuservercri:~$ cls
Command 'cls' not found, but there are 20 similar ones.
aryy234@ubuntuservercri:~$ sudo useradd -m -s /bin/bash UserAG03
[sudo] password for aryy234:
Sorry, try again.
[sudo] password for aryy234:
aryy234@ubuntuservercri:~$ sudo useradd -m -s /bin/bash UserAG03
useradd: user 'UserAG03' already exists
aryy234@ubuntuservercri:~$ sudo passwd UserAG03
New password:
Retype new password:
passwd: password updated successfully
aryy234@ubuntuservercri:~$ sudo usermod -aG sudo UserAG03
aryy234@ubuntuservercri:~$ groups UserAG03
UserAG03 : UserAG03 sudo
aryy234@ubuntuservercri:~$ sudo useradd -m -s /bin/bash UserBG03
aryy234@ubuntuservercri:~$ sudo passwd UserBG03
New password:
Retype new password:
passwd: password updated successfully
aryy234@ubuntuservercri:~$ cat /etc/passwd | grep UserG
aryy234@ubuntuservercri:~$ grep 'User[AB]G03' /etc/passwd
UserAG03:x:1001:1001::/home/UserAG03:/bin/bash
UserBG03:x:1002:1002::/home/UserBG03:/bin/bash
aryy234@ubuntuservercri:~$ su - UserAG03
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

UserAG03@ubuntuservercri:~$ whoami
UserAG03
UserAG03@ubuntuservercri:~$ exit
Logout
aryy234@ubuntuservercri:~$
```

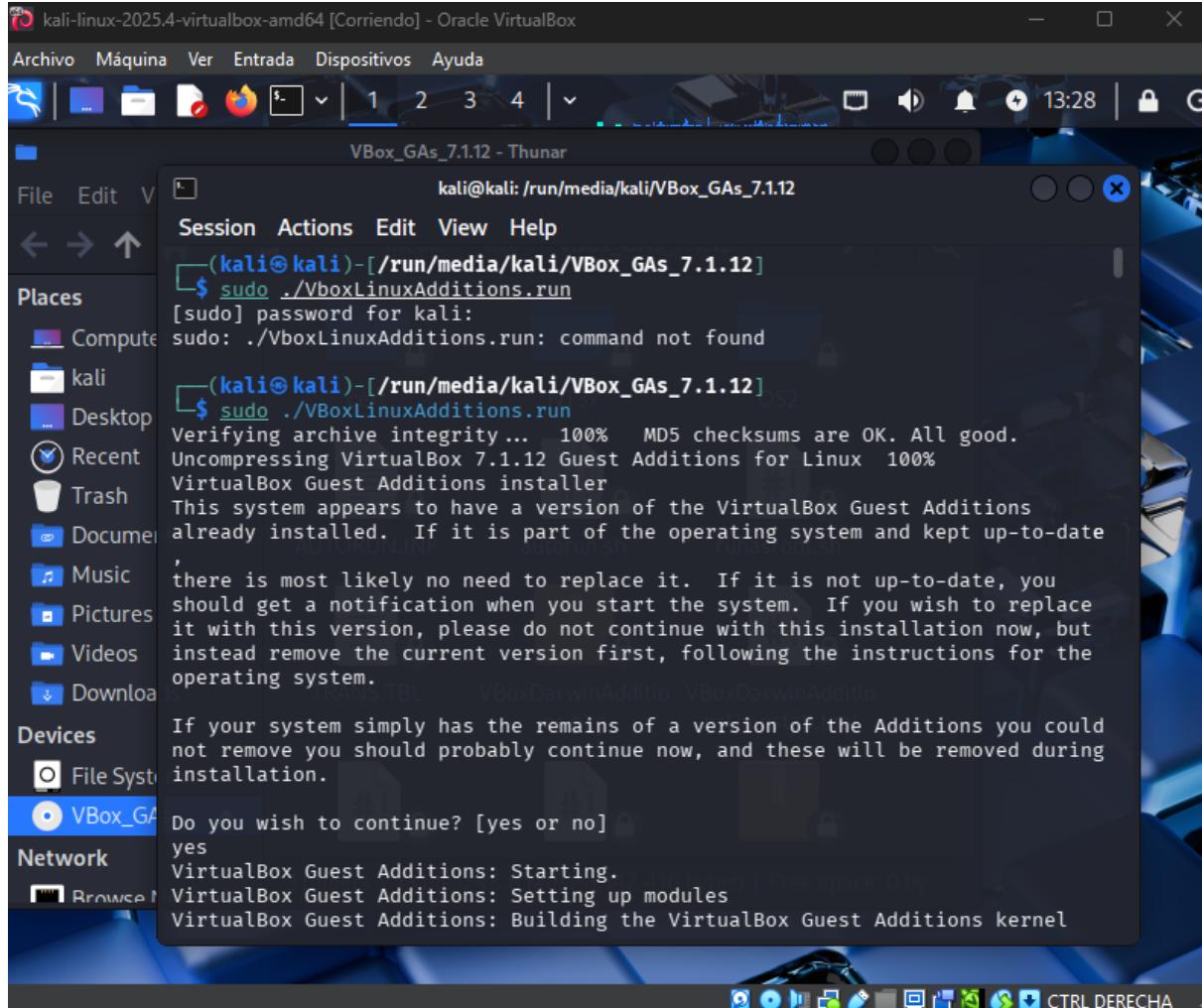
Instalar Kali Linux en otro Hipervisor (otra VM)

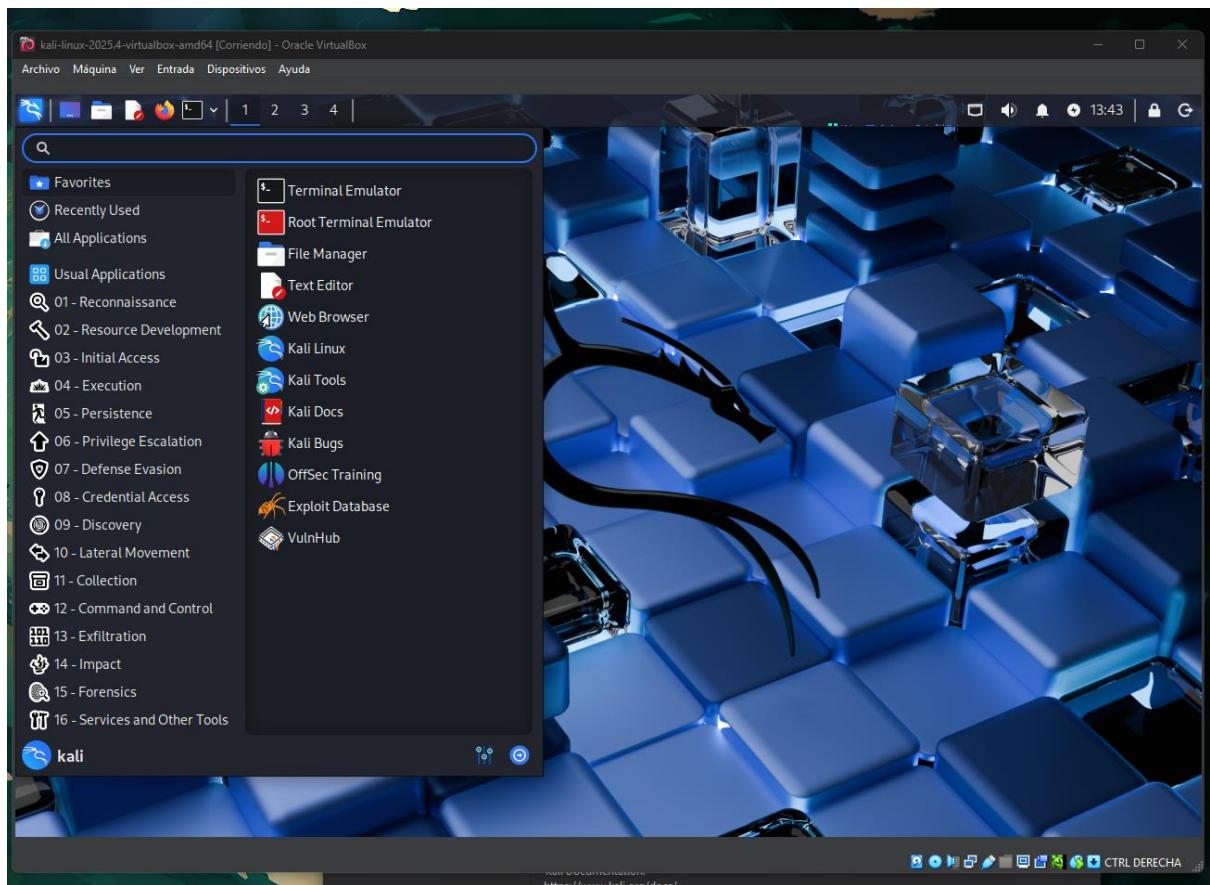
Ahora necesita crear una **segunda máquina virtual** en VirtualBox con Kali Linux.



Configurar la Red

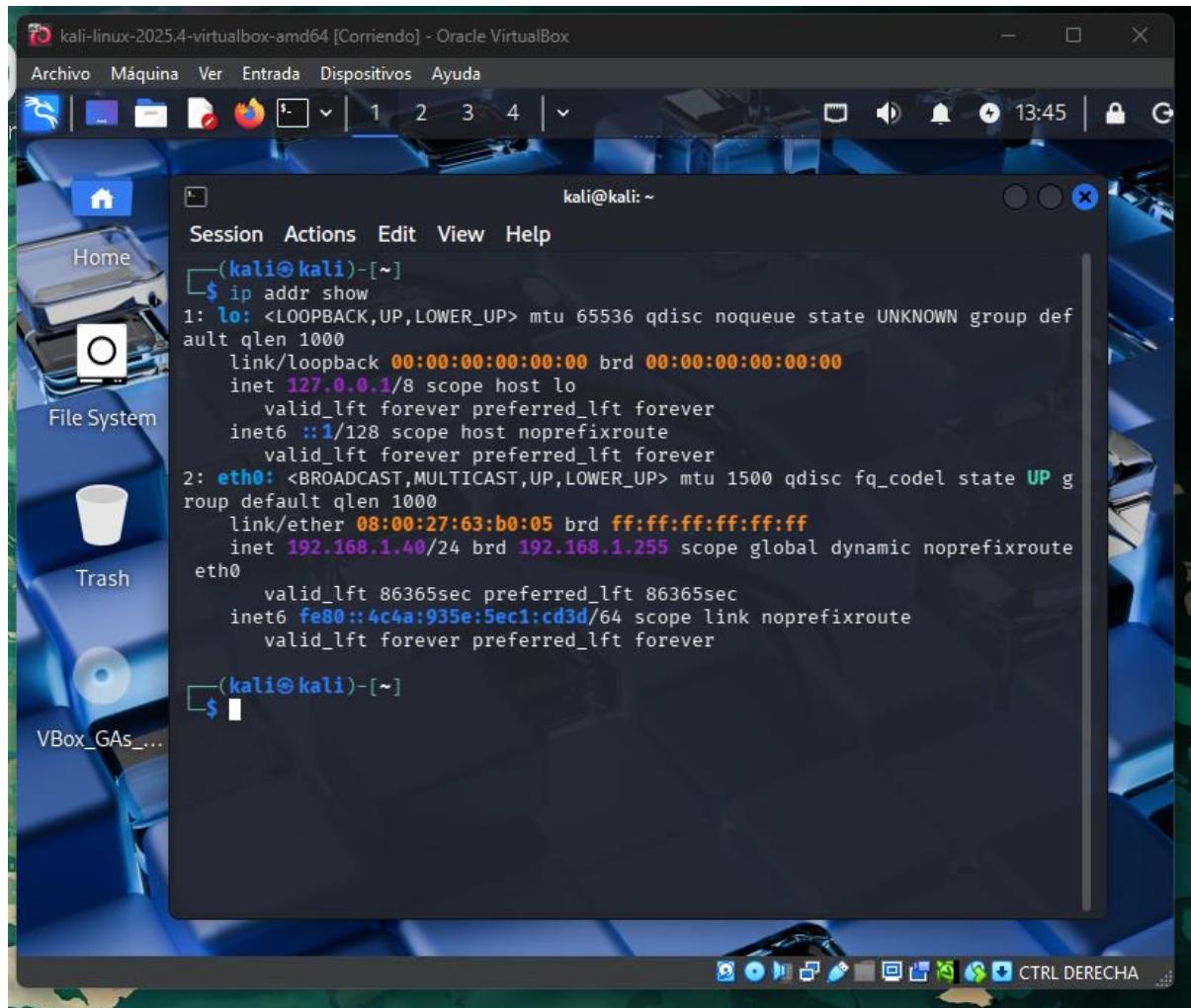
Ambas máquinas deben estar en la **misma red** para comunicarse.





Iniciar Kali y verificar IP:

Debería tener una IP similar: 192.168.1.40 o cercana.



Comprobar Conectividad entre Máquinas

Desde Ubuntu Server (192.168.1.40):

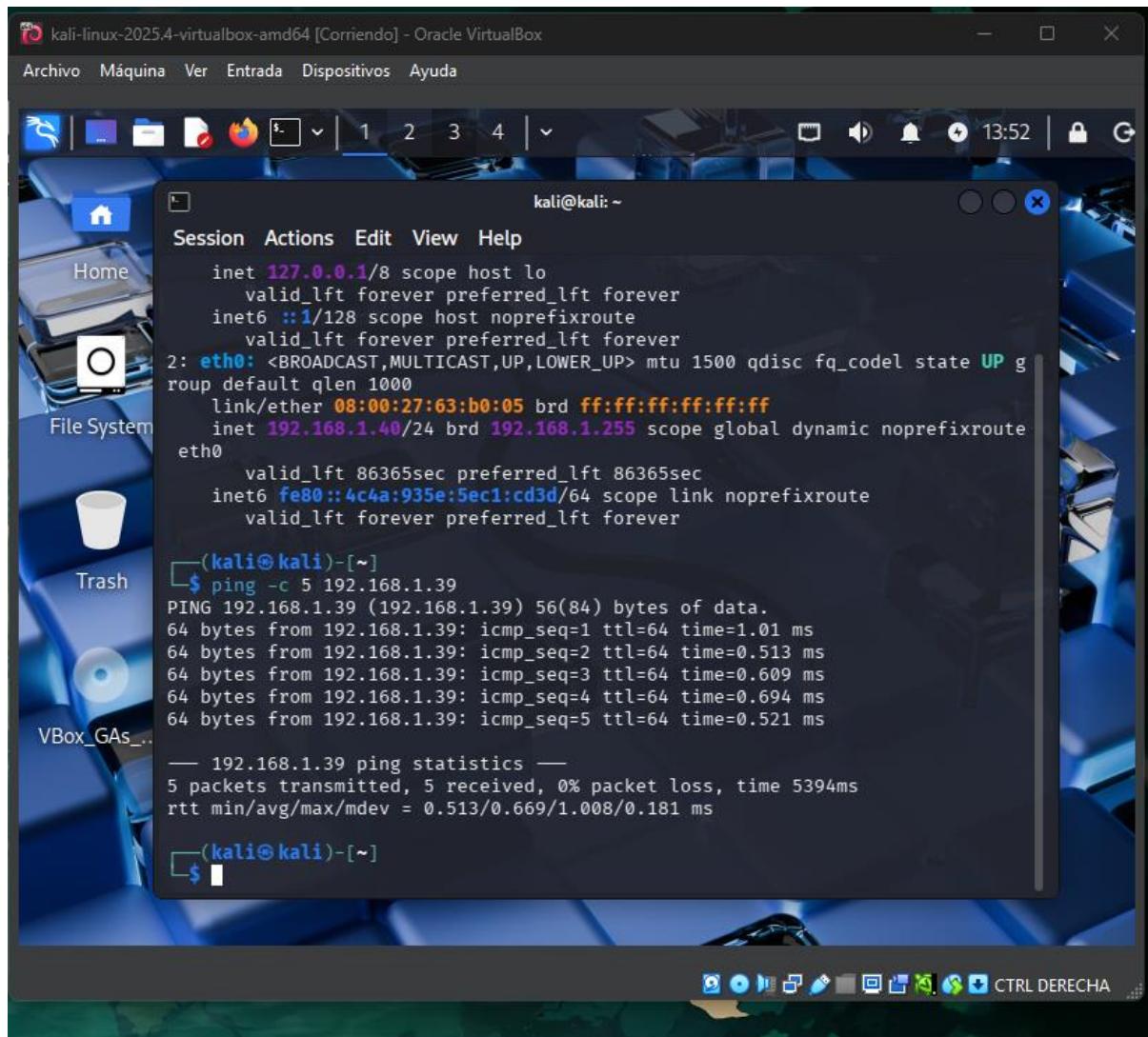
```
aryy234@ubuntuservercri:~$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=3.16 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.594 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.565 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.571 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.622 ms
64 bytes from 192.168.1.40: icmp_seq=7 ttl=64 time=0.588 ms
64 bytes from 192.168.1.40: icmp_seq=8 ttl=64 time=0.473 ms
64 bytes from 192.168.1.40: icmp_seq=9 ttl=64 time=39.1 ms
64 bytes from 192.168.1.40: icmp_seq=10 ttl=64 time=0.613 ms
64 bytes from 192.168.1.40: icmp_seq=11 ttl=64 time=0.662 ms
64 bytes from 192.168.1.40: icmp_seq=12 ttl=64 time=0.551 ms
64 bytes from 192.168.1.40: icmp_seq=13 ttl=64 time=0.602 ms
64 bytes from 192.168.1.40: icmp_seq=14 ttl=64 time=0.793 ms
64 bytes from 192.168.1.40: icmp_seq=15 ttl=64 time=0.724 ms
64 bytes from 192.168.1.40: icmp_seq=16 ttl=64 time=0.682 ms
64 bytes from 192.168.1.40: icmp_seq=17 ttl=64 time=0.665 ms
64 bytes from 192.168.1.40: icmp_seq=18 ttl=64 time=0.606 ms
64 bytes from 192.168.1.40: icmp_seq=19 ttl=64 time=0.856 ms
64 bytes from 192.168.1.40: icmp_seq=20 ttl=64 time=0.455 ms
64 bytes from 192.168.1.40: icmp_seq=21 ttl=64 time=0.640 ms
64 bytes from 192.168.1.40: icmp_seq=22 ttl=64 time=0.524 ms
64 bytes from 192.168.1.40: icmp_seq=23 ttl=64 time=0.982 ms
64 bytes from 192.168.1.40: icmp_seq=24 ttl=64 time=0.616 ms
64 bytes from 192.168.1.40: icmp_seq=25 ttl=64 time=0.525 ms
64 bytes from 192.168.1.40: icmp_seq=26 ttl=64 time=0.618 ms
64 bytes from 192.168.1.40: icmp_seq=27 ttl=64 time=0.595 ms
64 bytes from 192.168.1.40: icmp_seq=28 ttl=64 time=0.777 ms
64 bytes from 192.168.1.40: icmp_seq=29 ttl=64 time=0.516 ms
64 bytes from 192.168.1.40: icmp_seq=30 ttl=64 time=0.733 ms
64 bytes from 192.168.1.40: icmp_seq=31 ttl=64 time=0.562 ms
64 bytes from 192.168.1.40: icmp_seq=32 ttl=64 time=0.576 ms
64 bytes from 192.168.1.40: icmp_seq=33 ttl=64 time=0.570 ms
64 bytes from 192.168.1.40: icmp_seq=34 ttl=64 time=0.614 ms
64 bytes from 192.168.1.40: icmp_seq=35 ttl=64 time=0.508 ms
```

```
Símbolo del sistema      x  ary234@ubuntuservercri: ~  +  v
64 bytes from 192.168.1.40: icmp_seq=138 ttl=64 time=0.623 ms
64 bytes from 192.168.1.40: icmp_seq=139 ttl=64 time=0.520 ms
64 bytes from 192.168.1.40: icmp_seq=140 ttl=64 time=0.540 ms
64 bytes from 192.168.1.40: icmp_seq=141 ttl=64 time=0.586 ms
64 bytes from 192.168.1.40: icmp_seq=142 ttl=64 time=0.478 ms
64 bytes from 192.168.1.40: icmp_seq=143 ttl=64 time=31.0 ms
64 bytes from 192.168.1.40: icmp_seq=144 ttl=64 time=0.563 ms
64 bytes from 192.168.1.40: icmp_seq=145 ttl=64 time=0.592 ms
64 bytes from 192.168.1.40: icmp_seq=146 ttl=64 time=0.543 ms
64 bytes from 192.168.1.40: icmp_seq=147 ttl=64 time=0.596 ms
64 bytes from 192.168.1.40: icmp_seq=148 ttl=64 time=0.469 ms
64 bytes from 192.168.1.40: icmp_seq=149 ttl=64 time=0.658 ms
64 bytes from 192.168.1.40: icmp_seq=150 ttl=64 time=0.726 ms
64 bytes from 192.168.1.40: icmp_seq=151 ttl=64 time=0.620 ms
64 bytes from 192.168.1.40: icmp_seq=152 ttl=64 time=0.859 ms
64 bytes from 192.168.1.40: icmp_seq=153 ttl=64 time=0.582 ms
64 bytes from 192.168.1.40: icmp_seq=154 ttl=64 time=0.491 ms
64 bytes from 192.168.1.40: icmp_seq=155 ttl=64 time=0.525 ms
64 bytes from 192.168.1.40: icmp_seq=156 ttl=64 time=0.674 ms
64 bytes from 192.168.1.40: icmp_seq=157 ttl=64 time=0.568 ms
64 bytes from 192.168.1.40: icmp_seq=158 ttl=64 time=1.13 ms
64 bytes from 192.168.1.40: icmp_seq=159 ttl=64 time=0.644 ms
64 bytes from 192.168.1.40: icmp_seq=160 ttl=64 time=0.588 ms
64 bytes from 192.168.1.40: icmp_seq=161 ttl=64 time=0.847 ms
64 bytes from 192.168.1.40: icmp_seq=162 ttl=64 time=0.567 ms
64 bytes from 192.168.1.40: icmp_seq=163 ttl=64 time=0.571 ms
64 bytes from 192.168.1.40: icmp_seq=164 ttl=64 time=0.824 ms
64 bytes from 192.168.1.40: icmp_seq=165 ttl=64 time=0.879 ms
64 bytes from 192.168.1.40: icmp_seq=166 ttl=64 time=0.730 ms
64 bytes from 192.168.1.40: icmp_seq=167 ttl=64 time=0.560 ms
64 bytes from 192.168.1.40: icmp_seq=168 ttl=64 time=0.681 ms
64 bytes from 192.168.1.40: icmp_seq=169 ttl=64 time=0.650 ms
64 bytes from 192.168.1.40: icmp_seq=170 ttl=64 time=0.742 ms
64 bytes from 192.168.1.40: icmp_seq=171 ttl=64 time=0.703 ms
64 bytes from 192.168.1.40: icmp_seq=172 ttl=64 time=0.717 ms
^C
--- 192.168.1.40 ping statistics ---
172 packets transmitted, 172 received, 0% packet loss, time 174950ms
rtt min/avg/max/mdev = 0.345/1.316/39.075/4.392 ms
```

Desde Kali Linux:

```
# Hacer ping a Ubuntu
```

```
ping 192.168.1.39
```



```
# Escanear puertos de Ubuntu
```

```
nmap 192.168.1.39
```

The screenshot shows a terminal window titled "kali@kali: ~" running on a Kali Linux desktop environment. The terminal displays the following command-line session:

```
(kali㉿kali)-[~]
$ ping -c 5 192.168.1.39
PING 192.168.1.39 (192.168.1.39) 56(84) bytes of data.
64 bytes from 192.168.1.39: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 192.168.1.39: icmp_seq=2 ttl=64 time=0.513 ms
64 bytes from 192.168.1.39: icmp_seq=3 ttl=64 time=0.609 ms
64 bytes from 192.168.1.39: icmp_seq=4 ttl=64 time=0.694 ms
64 bytes from 192.168.1.39: icmp_seq=5 ttl=64 time=0.521 ms

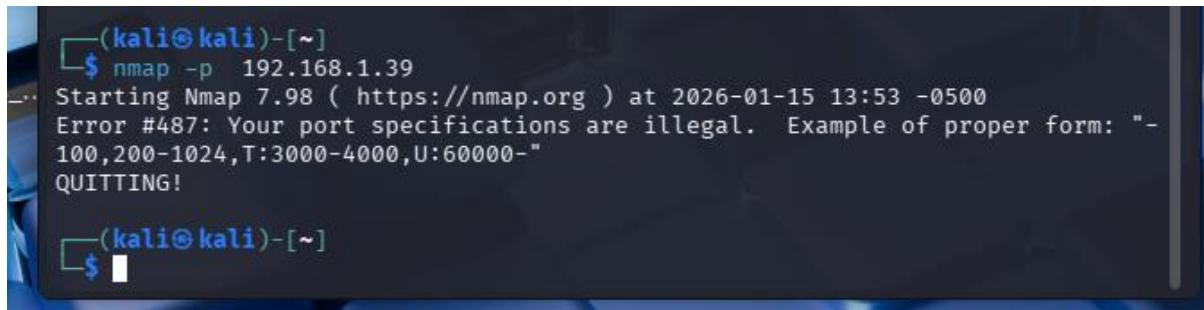
--- 192.168.1.39 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 5394ms
rtt min/avg/max/mdev = 0.513/0.669/1.008/0.181 ms

(kali㉿kali)-[~]
$ nmap 192.168.1.39
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-15 13:52 -0500
Nmap scan report for 192.168.1.39
Host is up (0.00068s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:AD:38:78 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.20 seconds
```

```
# Ver si SSH está abierto
```

```
nmap -p 192.168.1.39
```

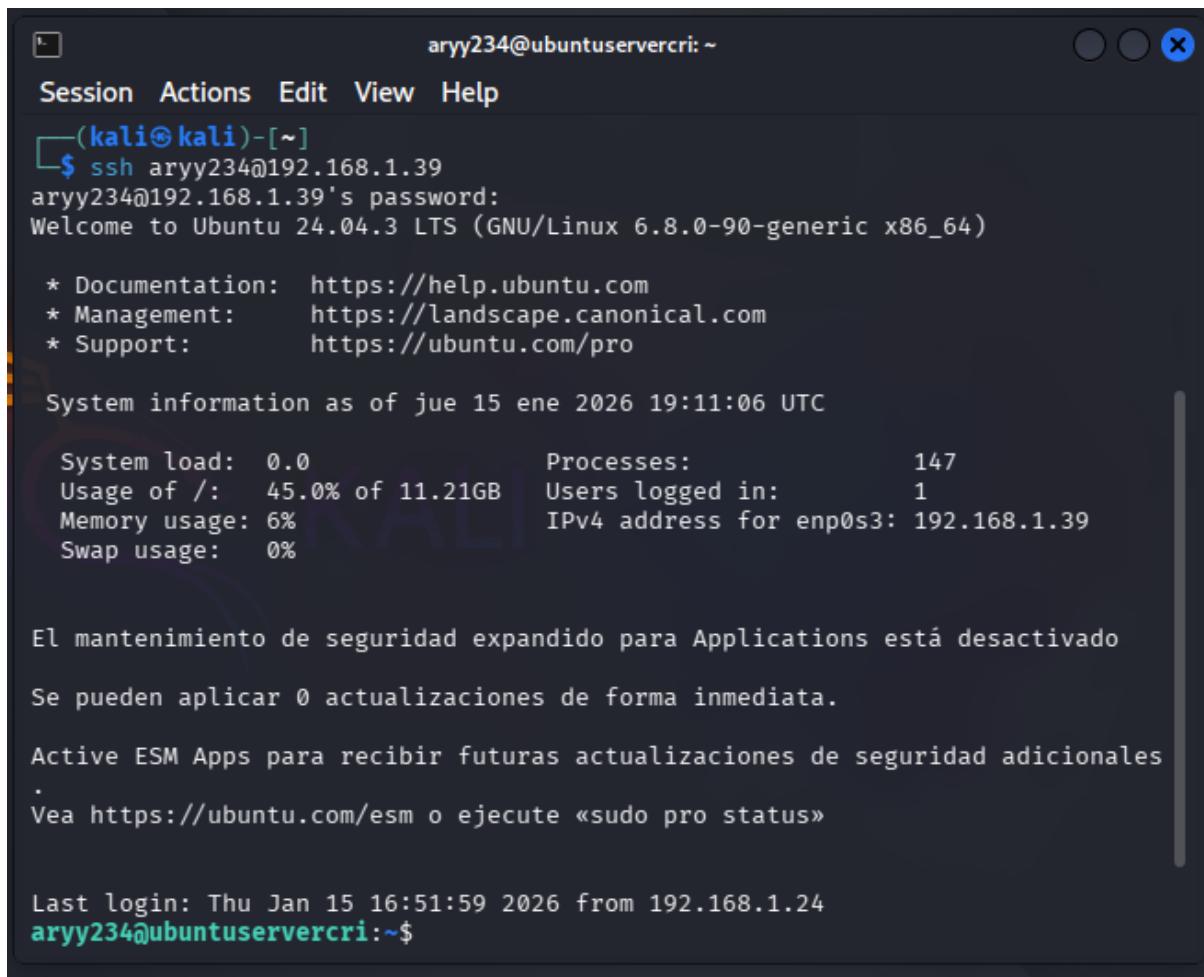


```
(kali㉿kali)-[~]
$ nmap -p 192.168.1.39
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-15 13:53 -0500
Error #487: Your port specifications are illegal. Example of proper form: "-100,2000-1024,T:3000-4000,U:60000-"
QUITTING!
```

Probar conexión SSH desde Kali a Ubuntu:

Conectar con tu usuario administrador

```
ssh aryy234@192.168.1.39
```



```
aryy234@ubuntuservercri: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ssh aryy234@192.168.1.39
aryy234@192.168.1.39's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of jue 15 ene 2026 19:11:06 UTC

System load:  0.0          Processes:           147
Usage of /:   45.0% of 11.21GB  Users logged in:      1
Memory usage: 6%
Swap usage:   0%
IPv4 address for enp0s3: 192.168.1.39

El mantenimiento de seguridad expandido para Applications está desactivado

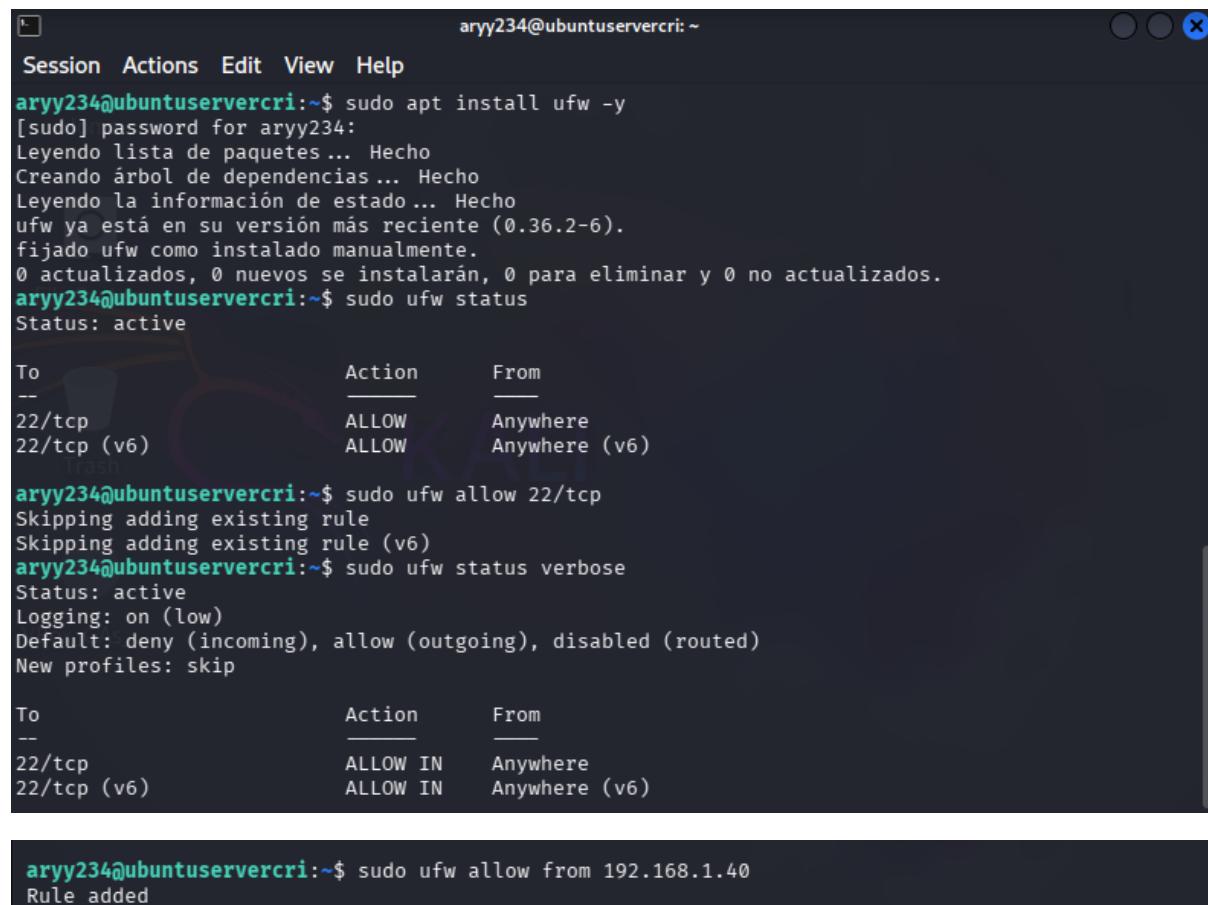
Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales
.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Last login: Thu Jan 15 16:51:59 2026 from 192.168.1.24
aryy234@ubuntuservercri:~$
```

1. Firewall (UFW)

```
# Instalar y configurar UFW  
sudo apt install ufw -y  
  
# Ver estado  
sudo ufw status  
  
# Permitir SSH (IMPORTANTE antes de habilitar)  
sudo ufw allow 22/tcp  
  
# Habilitar firewall  
sudo ufw enable  
  
# Ver reglas  
sudo ufw status verbose  
  
# Permitir conexiones desde Kali (opcional)  
sudo ufw allow from 192.168.1.40
```



The screenshot shows a terminal window with the following session:

```
aryy234@ubuntuservercri:~$ sudo apt install ufw -y  
[sudo] password for aryy234:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
ufw ya está en su versión más reciente (0.36.2-6).  
fijado ufw como instalado manualmente.  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
aryy234@ubuntuservercri:~$ sudo ufw status  
Status: active  
  
To                         Action      From  
--                         --         --  
22/tcp                      ALLOW      Anywhere  
22/tcp (v6)                  ALLOW      Anywhere (v6)  
  
aryy234@ubuntuservercri:~$ sudo ufw allow 22/tcp  
Skipping adding existing rule  
Skipping adding existing rule (v6)  
aryy234@ubuntuservercri:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To                         Action      From  
--                         --         --  
22/tcp                      ALLOW IN    Anywhere  
22/tcp (v6)                  ALLOW IN    Anywhere (v6)  
  
aryy234@ubuntuservercri:~$ sudo ufw allow from 192.168.1.40  
Rule added
```

IPS - Sistema de Prevención de Intrusiones (Snort)

Instalar Snort

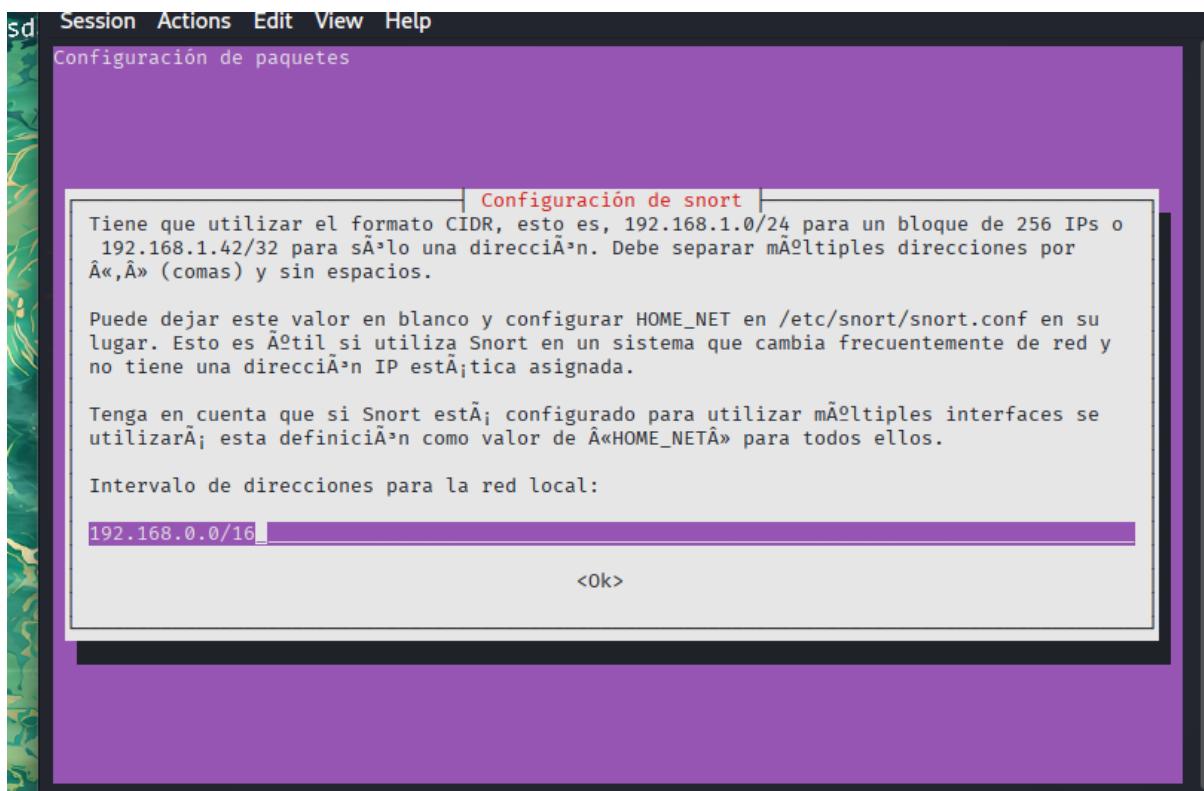
```
sudo apt install snort -y
```

```
Last login: Thu Jan 15 19:26:11 2026 from 192.168.1.40
aryy234@ubuntuservercri:~$ sudo apt install snort -y
[sudo] password for aryy234:
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
 libauthen-sasl-perl libclone-perl libdaq2t64 libdata-dump-perl libdumbnet1
 libencode-locale-perl libfile-listing-perl libfont-afm-perl libhtml-form-perl
 libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl
 libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
 libhttp-negotiate-perl libio-html-perl libio-socket-ssl-perl libluajit-5.1-2
 libluajit-5.1-common liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-perl
 libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl libnetfilter-queue1 libpcre3
 libtimedate-perl libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl oinkmaster
 perl-openssl-defaults snort-common snort-common-libraries snort-rules-default
Paquetes sugeridos:
 libdigest-hmac-perl libgssapi-perl libio-compress-brotli-perl libcrypt-ssleay-perl
 libsub-name-perl libbusiness-isbn-perl libregexp-ipv6-perl libauthen-ntlm-perl debhelper
 snort-doc
Se instalarán los siguientes paquetes NUEVOS:
 libauthen-sasl-perl libclone-perl libdaq2t64 libdata-dump-perl libdumbnet1
 libencode-locale-perl libfile-listing-perl libfont-afm-perl libhtml-form-perl
 libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl
 libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
```

Durante instalación te preguntaran:

- Interfaz de red: enp0s3

- Rango de red: 192.168.1.0/24



Verificar instalación

snort --version

Ver configuración

sudo nano /etc/snort/snort.conf

```
aryy234@ubuntuservercri:~$ snort --version
              -=> Snort! <=-
              Version 2.9.20 GRE (Build 82)
              By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
              Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
              Copyright (C) 1998-2013 Sourcefire, Inc., et al.
              Using libpcap version 1.10.4 (with TPACKET_V3)
              Using PCRE version: 8.39 2016-06-14
              Using ZLIB version: 1.3
aryy234@ubuntuservercri:~$ sudo nano /etc/snort/snort.conf
```

```
kali-linux-2025.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
 1 2 3 4 | v
ary234@ubuntuservercri: ~
Session Actions Edit View Help
Configurando snort (2.9.20-0+deb11u1ubuntu1) ...
Snort configuration: interface default not set, using 'enp0s3'
Configurando libhttp-cookies-perl (6.11-1) ...
Configurando libhtml-tree-perl (5.07-3) ...
Configurando libhtml-format-perl (2.16-2) ...
Configurando libnet-smtp-ssl-perl (1.04-2) ...
Configurando libmailtools-perl (2.21-2) ...
Configurando libhttp-daemon-perl (6.16-1) ...
Configurando libwww-perl (6.76-1) ...
Configurando oinkmaster (2.0-4.2) ...
Configurando liblwp-protocol-https-perl (6.13-1) ...
Procesando disparadores para libc-bin (2.39-0ubuntu8.6) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
Scanning processes ...
Scanning linux images ...
Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

```
ary234@ubuntuservercri: ~
Session Actions Edit View Help
GNU nano 7.2 /etc/snort/snort.conf
#####
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
# http://www.snort.org Snort Website
# http://vrt-blog.snort.org/ Sourcefire VRT Blog
#
# Mailing list Contact: snort-users@lists.snort.org
# False Positive reports: fp@sourcefire.com
# Snort bugs: bugs@snort.org
#
# Compatible with Snort Versions:
# VERSIONS : 2.9.20
#
# Snort build options:
# OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprof>
#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
[ Read 756 lines ]
^G Help      ^O Write Out   ^W Where Is    ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File   ^V Replace     ^U Paste      ^J Justify    ^/ Go To Line
CTRL DERECHA
```

Antivirus (ClamAV)

```
aryy234@ubuntuservercri:~$ sudo apt install clamav clamav-daemon -y
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
  clamav-base clamav-freshclam clamdscan libclamav12
Paquetes sugeridos:
  libclamunrar clamav-doc daemon libclamunrar11
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav12
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 6.886 kB de archivos.
Se utilizarán 32,4 MB de espacio de disco adicional después de esta operación.
Des:1 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-base all 1.4.3+dfsg-0
ubuntu0.24.04.1 [102 kB]
Des:2 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 libclamav12 amd64 1.4.3+dfsg-0
ubuntu0.24.04.1 [3.598 kB]
Des:3 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-freshclam amd64 1.4.3
+dfsg-0ubuntu0.24.04.1 [99,1 kB]
Des:4 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-daemon amd64 1.4.3+df
sg-0ubuntu0.24.04.1 [216 kB]
Des:5 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav amd64 1.4.3+dfsg-0ubu
ntu0.24.04.1 [2.819 kB]
Des:6 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamdscan amd64 1.4.3+dfsg-0
ubuntu0.24.04.1 [51,7 kB]
Descargados 6.886 kB en 3s (2.684 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete clamav-base previamente no seleccionado.
```

Actualizar definiciones de virus

```
sudo systemctl stop clamav-freshclam
```

```
sudo freshclam
```

```
aryy234@ubuntuservercri:~$ sudo systemctl stop clamav-freshclam
aryy234@ubuntuservercri:~$ sudo freshclam
ClamAV update process started at Thu Jan 15 19:39:30 2026
Thu Jan 15 19:39:30 2026 -> daily.cvd database is up-to-date (version: 27881, sigs: 354802, f-l
evel: 90, builder: svc.clamav-publisher)
Thu Jan 15 19:39:30 2026 -> main.cvd database is up-to-date (version: 63, sigs: 3287027, f-leve
l: 90, builder: tomjudge)
Thu Jan 15 19:39:30 2026 -> bytecode.cvd database is up-to-date (version: 339, sigs: 80, f-leve
l: 90, builder: nrandolp)
aryy234@ubuntuservercri:~$
```

```
# Escanear un directorio
```

```
clamscan -r /home
```

```
l: 90, builder: nrandolph
aryy234@ubuntuservercri:~$ clamscan -r /home
Loading:    7s, ETA:   0s [=====]      3.63M/3.63M sigs
Compiling:  2s, ETA:   0s [=====]      41/41 tasks

/home/UserAG03: Can't open directory.
/home/aryy234/.cache/motd.legal-displayed: Empty file
/home/aryy234/.bash_logout: OK
/home/aryy234/.ssh/authorized_keys: Empty file
/home/aryy234/.bash_history: OK
/home/aryy234/.sudo_as_admin_successful: Empty file
/home/aryy234/.profile: OK
/home/aryy234/.bashrc: OK
/home/UserBG03: Can't open directory.

----- SCAN SUMMARY -----
Known viruses: 3627218
Engine version: 1.4.3
Scanned directories: 4
Scanned files: 4
Infected files: 0
Total errors: 2
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 9.245 sec (0 m 9 s)
Start Date: 2026:01:15 19:39:59
End Date: 2026:01:15 19:40:08
aryy234@ubuntuservercri:~$ █
```

```
# Ver estado
```

```
sudo systemctl status clamav-daemon
```

```
aryy234@ubuntuservercri:~$ sudo systemctl status clamav-daemon
● clamav-daemon.service - Clam AntiVirus userspace daemon
  Loaded: loaded (/usr/lib/systemd/system/clamav-daemon.service; enabled; preset: enabled)
  Drop-In: /etc/systemd/system/clamav-daemon.service.d
            └─extend.conf
    Active: inactive (dead)
  TriggeredBy: o clamav-daemon.socket
    Condition: start condition unmet at Thu 2026-01-15 19:38:08 UTC; 2min 38s ago
                └─ ConditionPathExistsGlob=/var/lib/clamav/daily.{c[v]l}d,inc was not met
    Docs: man:clamd(8)
          man:clamd.conf(5)
          https://docs.clamav.net/
[...]
ene 15 19:38:08 ubuntuservercri systemd[1]: clamav-daemon.service - Clam AntiVirus userspace d█
lines 1-13/13 (END)
```