Investigue qué es el protocolo SSH y para qué sirve (10 puntos)

El protocolo SSH (Secure Shell) es un método para enviar comandos de manera segura a una computadora a través de una red vulnerable. Este protocolo usa criptografía para autenticar y encriptar conexiones entre dispositivos. También, SSH permite hacer *tunneling*, lo cual es básicamente lograr que paquetes de datos crucen redes que normalmente no podrían atravesar. El protocolo se usa generalmente para controlar servidores de manera remota, administrar infraestructuras y transferir archivos (Cloudflare, s.f.-a).

SSH establece una conexión entre un dispositivo y una máquina que se encuentra lejos, normalmente un servidor, y usa encriptación para mezclar la información que se mueve a través de esa conexión. También, como se mencionó anteriormente, el protocolo permite hacer *tunneling*, específicamente partiendo los datos en pedazos pequeños (paquetes), y envolviéndolos en información adicional, llamada *headers*, para cambiar así su destino (Cloudflare, s.f.-a).

Investigue qué es el protocolo SSL y para qué sirve (10 puntos)

SSL (Secure Sockets Layer) es un protocolo de seguridad de Internet basado en encriptación. Fue desarrollado por Netscape en 1995 con el propósito de garantizar privacidad, autenticación e integridad de datos en comunicaciones a través de Internet. Es el predecesor de TLS (Transport Layer Security), que es la encriptación moderna usada en el presente, ya que SSL no se actualiza desde 1996. Como dato extra, un sitio web que implementa SSL tiene HTTPS en su URL en lugar de HTTP (Cloudflare, s.f.-b).

SSL encripta la data que transmite a través de la red, lo que significa que cualquiera que trate de interceptar esta información únicamente verá una serie de caracteres sin ningún orden en particular, y prácticamente imposibles de desencriptar. También inicia un proceso de autenticación llamado *handshake* entre dos dispositivos que se estén comunicando, esto para asegurarse de que ambos dispositivos verdaderamente son quien dicen ser. Adicionalmente, este protocolo firma digitalmente los datos para proveer integridad, verificando que la información no sea manipulada antes de llegar a su receptor (Cloudflare, s.f.-b).

Investigue cómo funciona el algoritmo RSA y para qué sirve la llave pública y la llave privada en el proceso de cifrado (20 puntos) - Nico

La criptografía RSA, empleada masivamente en Internet, se caracteriza por usar cifrado asimétrico con dos claves complementarias: una pública para cifrado y otra privada para descifrado. La robustez del algoritmo consiste en que ningún algoritmo puede calcular la llave privada partiendo de la llave pública. (Equipo editorial de IONOS, 2022)

El funcionamiento entre las llaves del algoritmo es mediante una llave pública cumple el rol de cifrar la información y una llave privada la cual descifra la misma permitiendo dentro de la red comunicaciones seguras, aunque las mismas sean interceptadas pues solamente se pueden desencriptar el destinatario quien es quien posee la llave privada. (Bhatt, 2024)

Investigue el algoritmo AES y compárelo con RSA (10 puntos)

El estándar de encriptación avanzada implementa un cifrado simétrico por bloques para datos simétrico, utilizando el mismo protocolo de encriptación común de convertir el mensaje original en uno nuevo protegiendo su contenido, pero en este caso utiliza una única llave compartida tanto para encriptar como desencriptar. Sin embargo, agregando dificultad a la encriptación mediante el uso de mezcla, trasposición y sustitución dentro del texto encriptado. (Panda Security, 2023)

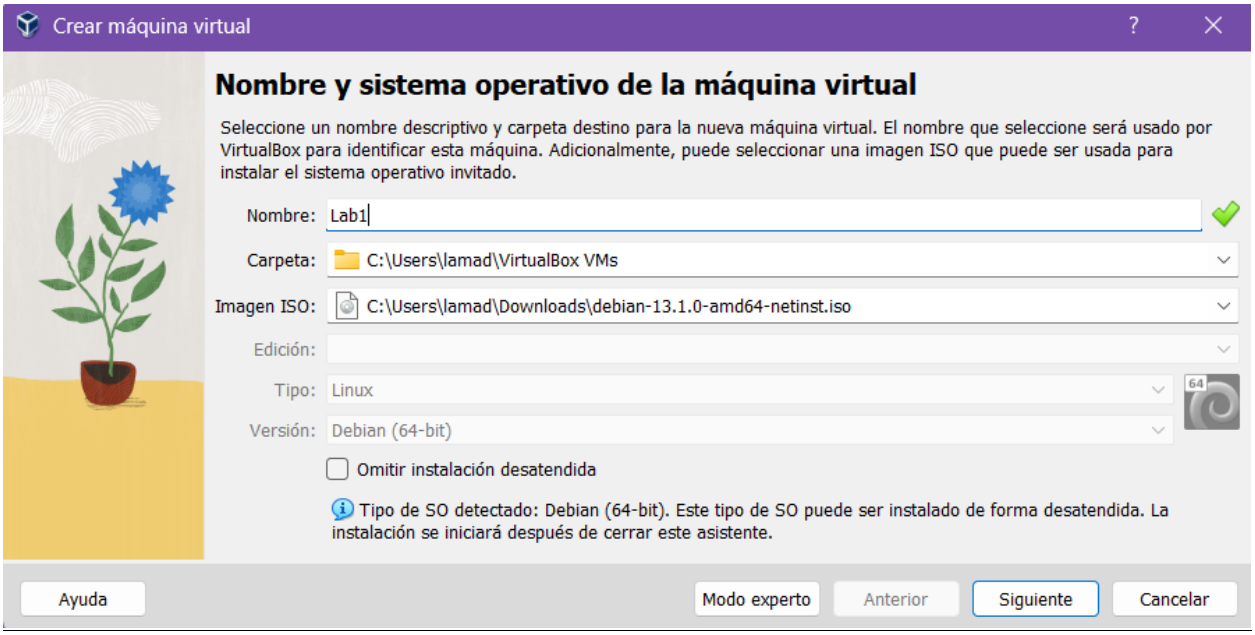
Los algoritmos RSA y AES contienen diferencias significativas donde RSA es asimétrico por lo que utiliza dos llaves para el proceso de encriptación y desencriptación mientras que AES es simétrico utilizado solamente una llave para ambos procesos permitiendo que este sea más rápido para gestionar. (Gitlan, 2025)

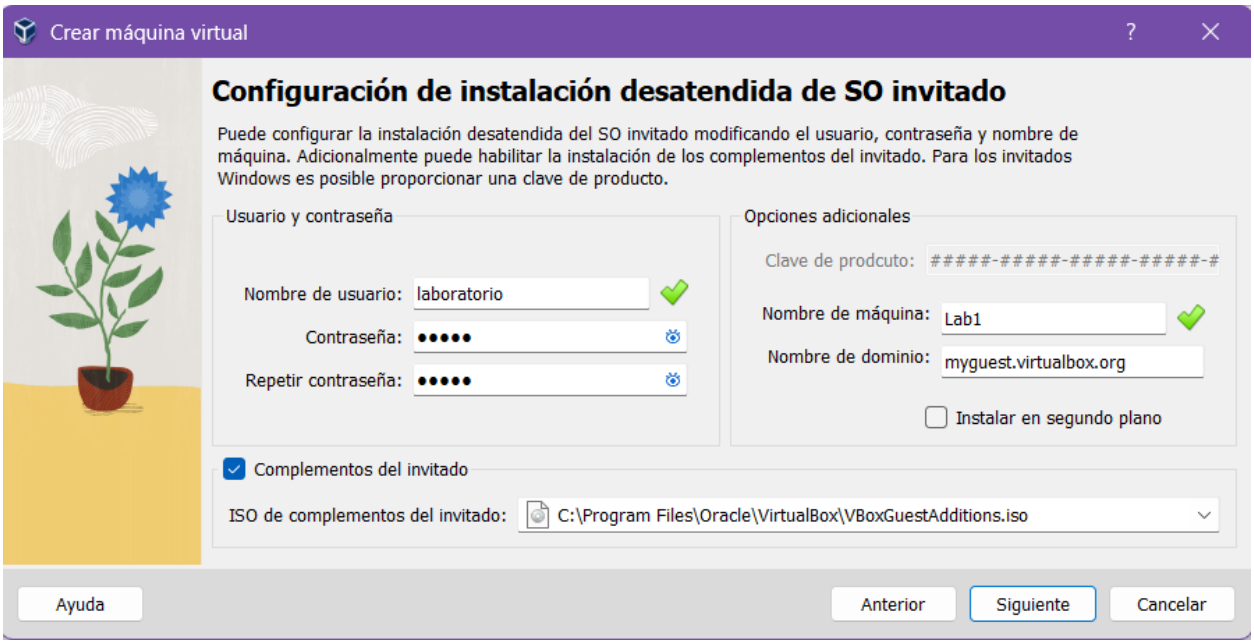
Entre las principales características de ambos algoritmos son sus usos puesto que en el RSA es más lento, es usado cifrados de correos electrónicos, firmas digitales y protocolo SSL, el AES es más eficaz, utilizado para grandes cantidades de datos, implementándose en trasmisión de datos, VPN y seguridad inalámbrica. (Gitlan, 2025)

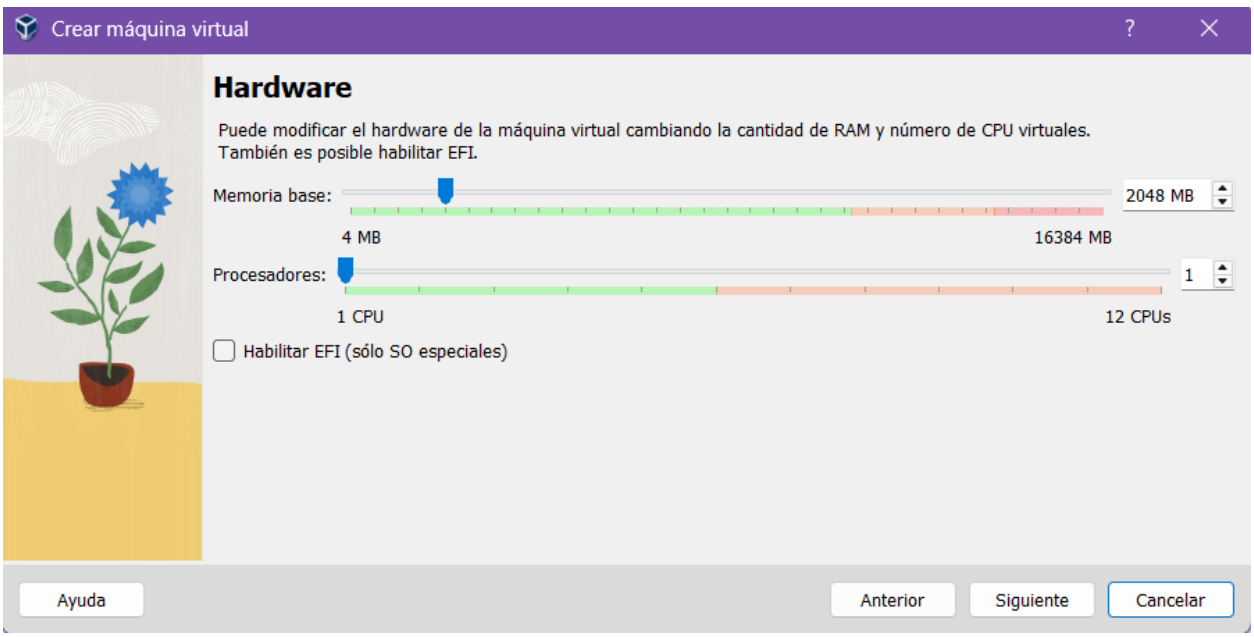
Parte 2. Práctica

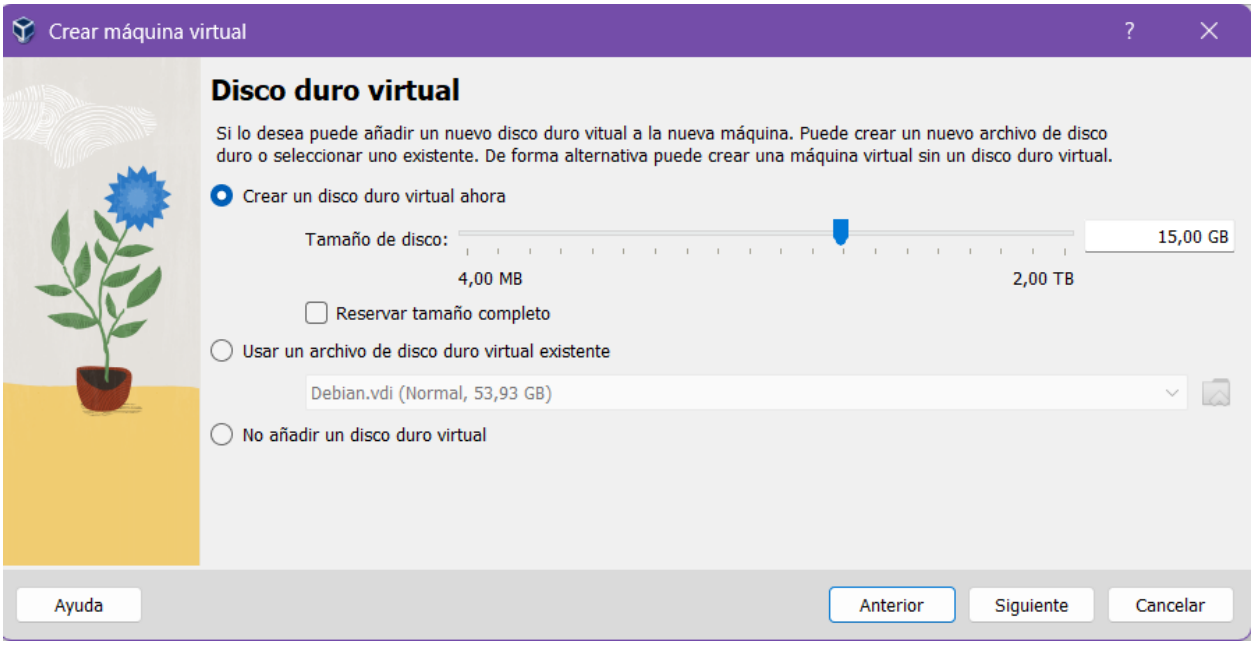
Instale 3 máquinas virtuales con el sistema operativo Debian 13, suponga que estas máquinas se llaman Lab1, Lab2, Lab3. Procure configurar la interfaz de red de su máquina virtual para que use la opción Bridge. Asegúrese que todas las máquinas virtuales tienen exactamente el mismo nombre de usuario.

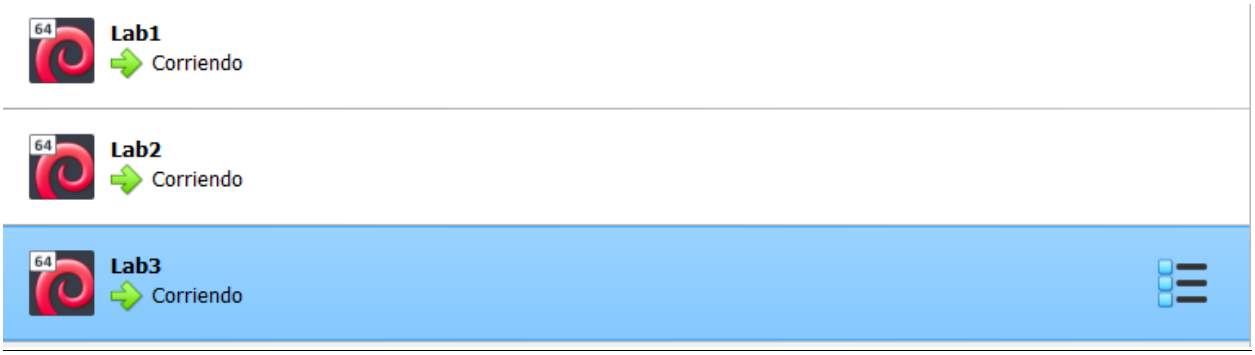
Se hace el procedimiento de instalación de las 3 máquinas virtuales, lo único que cambia es el nombre de cada una:


Crear máquina virtual
Nombre y sistema operativo de la máquina virtual
Seleccione un nombre descriptivo y carpeta destino para la nueva máquina virtual. El nombre que seleccione será usado por VirtualBox para identificar esta máquina. Adicionalmente, puede seleccionar una imagen ISO que puede ser usada para instalar el sistema operativo invitado.
Nombre: Lab1
Carpeta: C:\Users\lamad\VirtualBox VMs
Imagen ISO: C:\Users\lamad\Downloads\debian-13.1.0-amd64-netinst.iso
Edición:
Tipo: Linux
Versión: Debian (64-bit)
Omitir instalación desatendida
Tipo de SO detectado: Debian (64-bit). Este tipo de SO puede ser instalado de forma desatendida. La instalación se iniciará después de cerrar este asistente.
Ayuda
Modo experto
Anterior
Siguiente
Cancelar

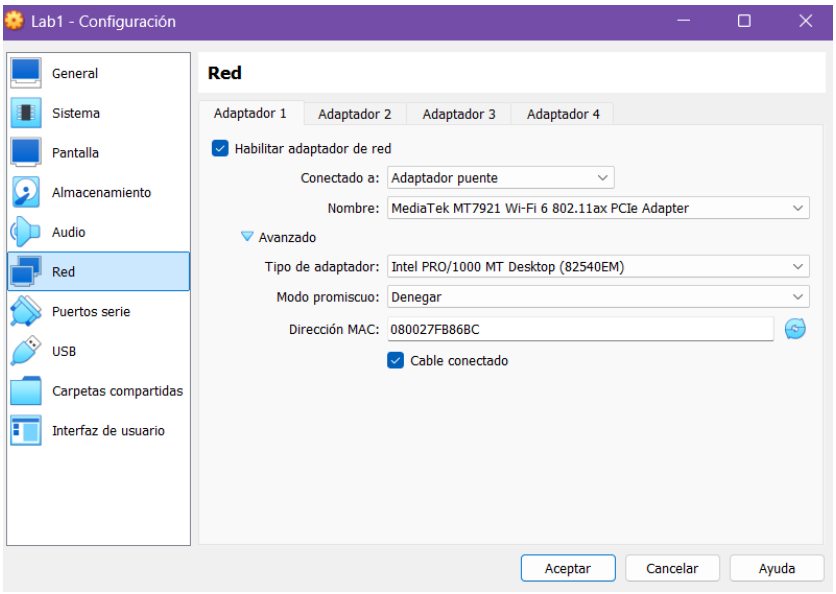

Crear máquina virtual
Configuración de instalación desatendida de SO invitado
Puede configurar la instalación desatendida del SO invitado modificando el usuario, contraseña y nombre de máquina. Adicionalmente puede habilitar la instalación de los complementos del invitado. Para los invitados Windows es posible proporcionar una clave de producto.
Usuario y contraseña
Nombre de usuario: laboratorio
Contraseña: •••••
Repetir contraseña: •••••
Opciones adicionales
Clave de prodcuto: #####-#####-#####-#####-#
Nombre de máquina: Lab1
Nombre de dominio: myguest.virtualbox.org
Instalar en segundo plano
Complementos del invitado
ISO de complementos del invitado: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso
Ayuda
Anterior
Siguiente
Cancelar


Crear máquina virtual
Hardware
Puede modificar el hardware de la máquina virtual cambiando la cantidad de RAM y número de CPU virtuales. También es posible habilitar EFI.
Memoria base: 2048 MB
4 MB
16384 MB
Procesadores: 1
1 CPU
12 CPUs
Habilitar EFI (sólo SO especiales)
Ayuda
Anterior
Siguiente
Cancelar





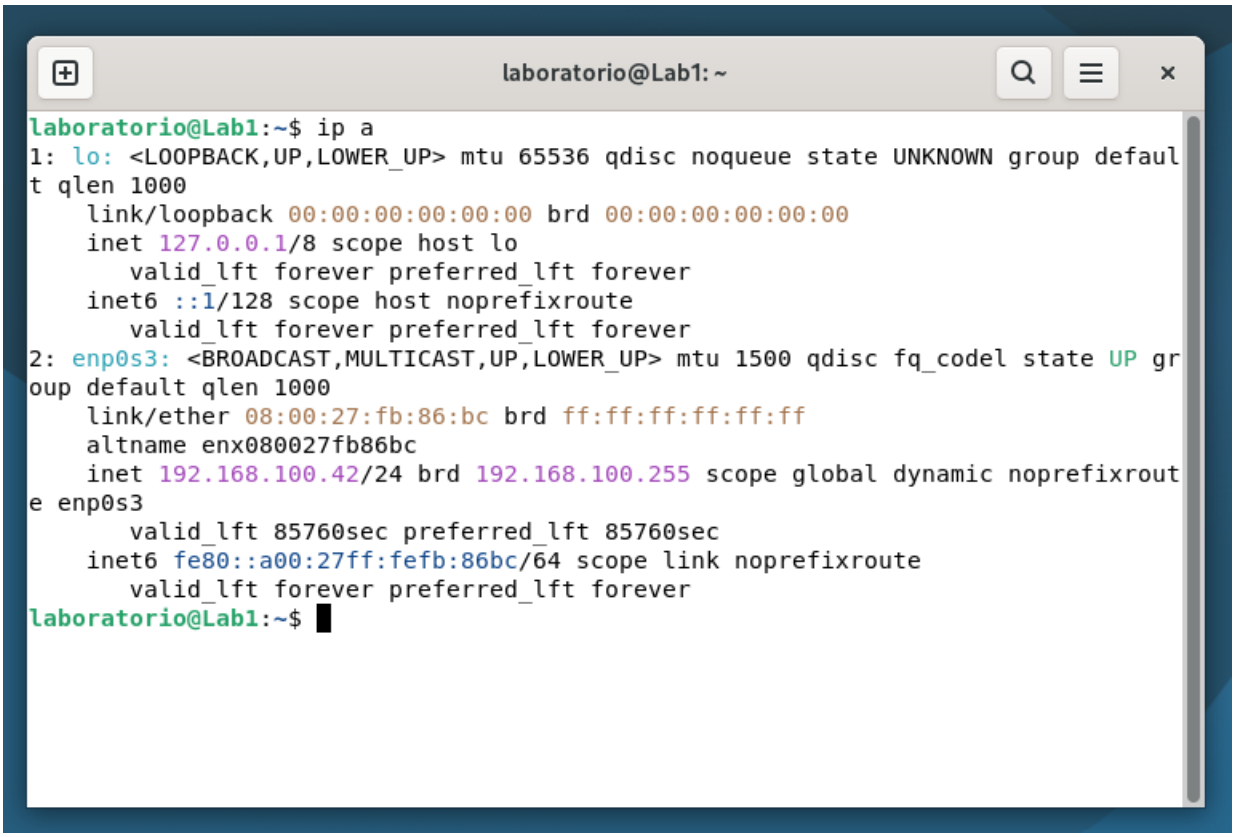
Se configuró en las 3 máquinas virtuales la opción de Bridged Adapter

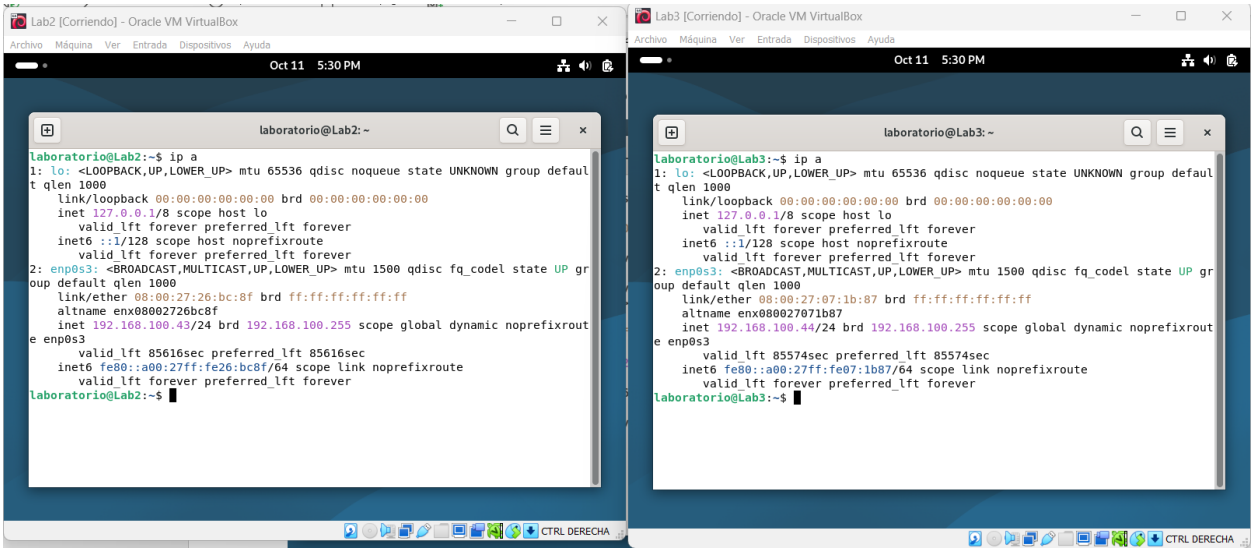


Investigue cómo autenticarse por SSH sin contraseña (intercambiando llaves) y configure su ambiente de forma que pueda desde Lab1 autenticarse sin contraseña en Lab2 y Lab3. Explique paso a paso su proceso, incluya capturas de pantalla. (50 puntos)

Se utilizó el paso a paso de la autenticación a partir de lo encontrado en Linuxize. 2019 y ChigozieCO, 2024.

Se puso el comando ip a para saber las direcciones de cada una

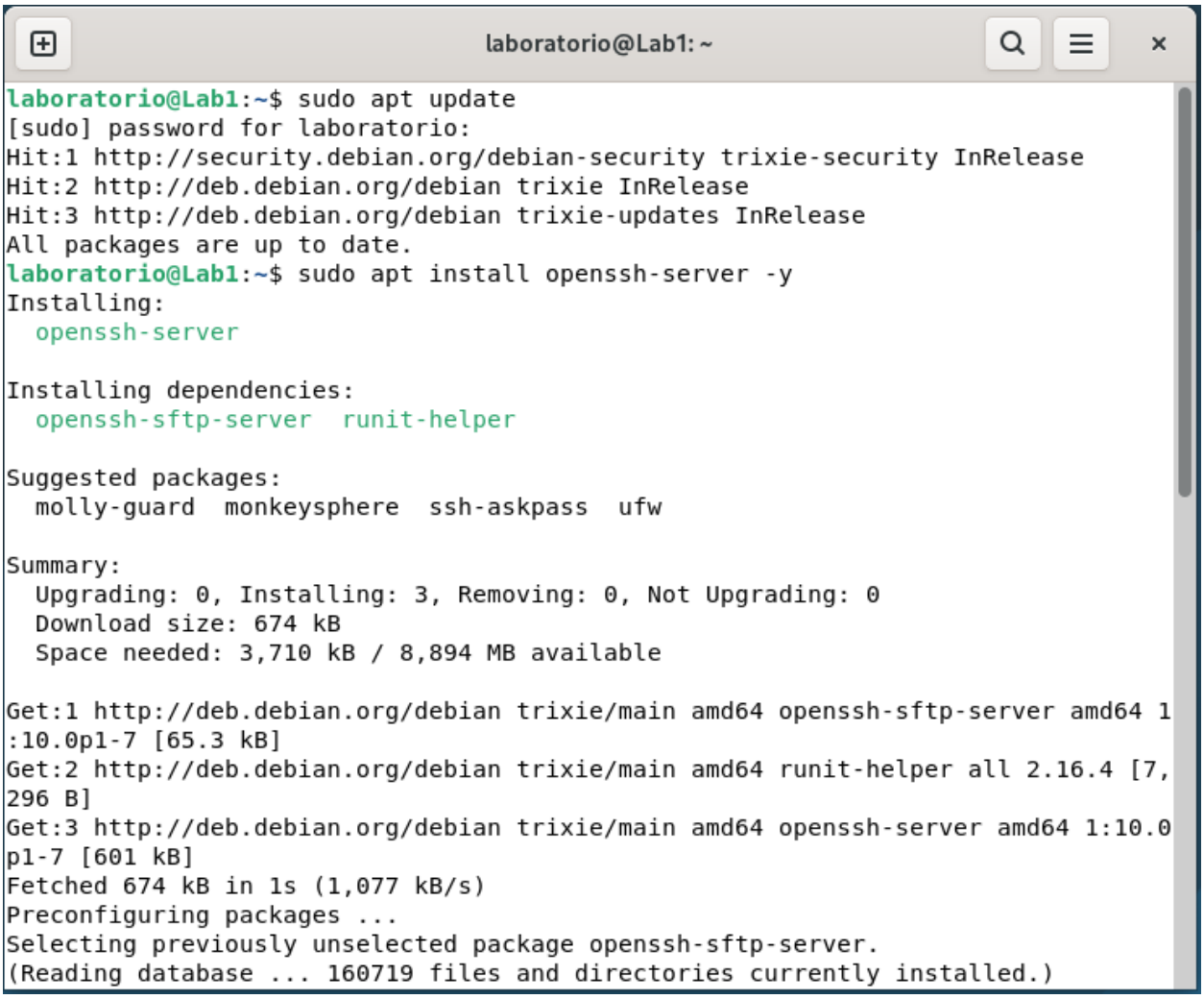


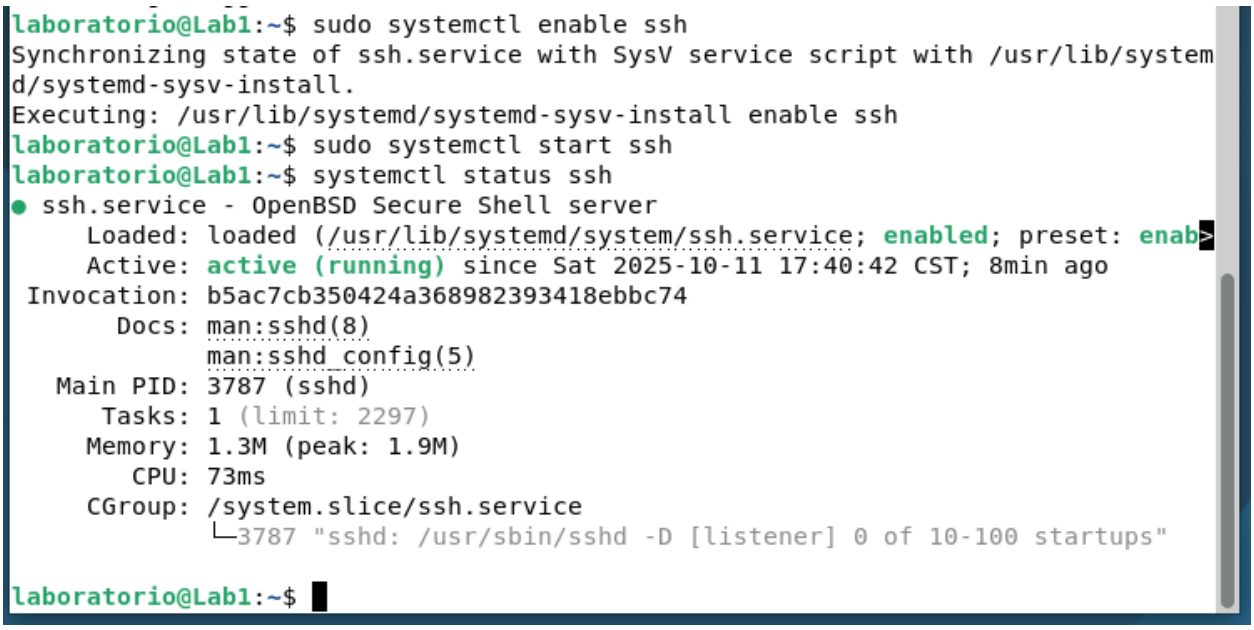


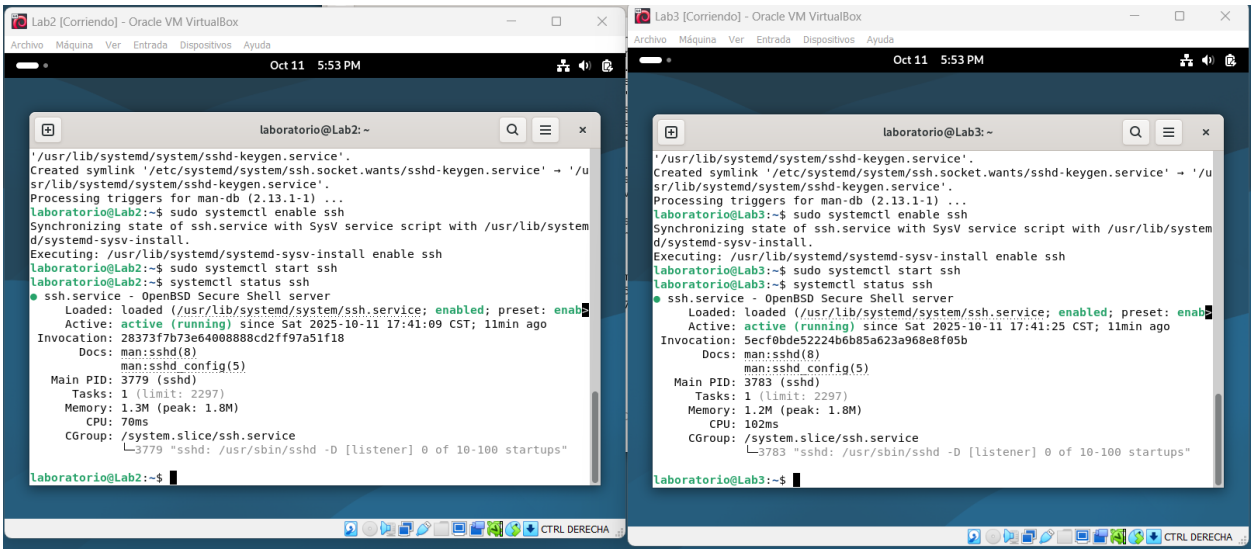
Se verificó que hubiera conexión con las otras dos máquinas virtuales

```
laboratorio@Lab1:~$ ping 192.168.100.43
PING 192.168.100.43 (192.168.100.43) 56(84) bytes of data.
64 bytes from 192.168.100.43: icmp_seq=1 ttl=64 time=4.73 ms
64 bytes from 192.168.100.43: icmp_seq=2 ttl=64 time=1.52 ms
64 bytes from 192.168.100.43: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 192.168.100.43: icmp_seq=4 ttl=64 time=2.10 ms
64 bytes from 192.168.100.43: icmp_seq=5 ttl=64 time=2.52 ms
^C
--- 192.168.100.43 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.242/2.421/4.730/1.236 ms
laboratorio@Lab1:~$ ping 192.168.100.44
PING 192.168.100.44 (192.168.100.44) 56(84) bytes of data.
64 bytes from 192.168.100.44: icmp_seq=1 ttl=64 time=11.5 ms
64 bytes from 192.168.100.44: icmp_seq=2 ttl=64 time=0.794 ms
64 bytes from 192.168.100.44: icmp_seq=3 ttl=64 time=1.14 ms
64 bytes from 192.168.100.44: icmp_seq=4 ttl=64 time=1.34 ms
^C
--- 192.168.100.44 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.794/3.689/11.486/4.505 ms
laboratorio@Lab1:~$
```

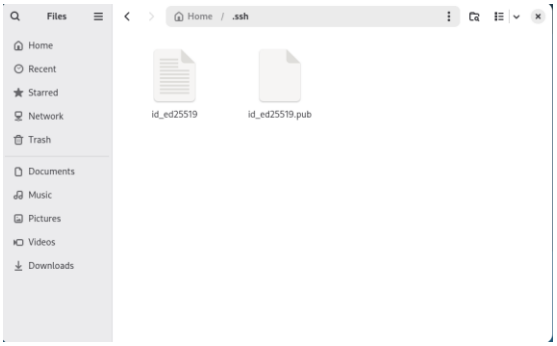
Se instaló openssh-server en las 3 máquinas virtuales, se habilitó, se le dio start y se verificó que estuviera activo


laboratorio@Lab1: ~
laboratorio@Lab1:~$ sudo apt update
[sudo] password for laboratorio:
Hit:1 http://security.debian.org/debian-security trixie-security InRelease
Hit:2 http://deb.debian.org/debian trixie InRelease
Hit:3 http://deb.debian.org/debian trixie-updates InRelease
All packages are up to date.
laboratorio@Lab1:~$ sudo apt install openssh-server -y
Installing:
openssh-server
Installing dependencies:
openssh-sftp-server runit-helper
Suggested packages:
molly-guard monkeysphere ssh-askpass ufw
Summary:
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 0
Download size: 674 kB
Space needed: 3,710 kB / 8,894 MB available
Get:1 http://deb.debian.org/debian trixie/main amd64 openssh-sftp-server amd64 1
:10.0p1-7 [65.3 kB]
Get:2 http://deb.debian.org/debian trixie/main amd64 runit-helper all 2.16.4 [7,
296 B]
Get:3 http://deb.debian.org/debian trixie/main amd64 openssh-server amd64 1:10.0
p1-7 [601 kB]
Fetched 674 kB in 1s (1,077 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 160719 files and directories currently installed.)


laboratorio@Lab1:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/system
d/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
laboratorio@Lab1:~$ sudo systemctl start ssh
laboratorio@Lab1:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab
Active: active (running) since Sat 2025-10-11 17:40:42 CST; 8min ago
Invocation: b5ac7cb350424a368982393418ebbc74
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 3787 (sshd)
Tasks: 1 (limit: 2297)
Memory: 1.3M (peak: 1.9M)
CPU: 73ms
CGroup: /system.slice/ssh.service
└─3787 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
laboratorio@Lab1:~$



Se generó la llave SSH



Desde Lab1 se envió a Lab2 y Lab3 la copia de la llave SSH

```
laboratorio@Lab1:~$ ssh-copy-id laboratorio@192.168.100.43
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
The authenticity of host '192.168.100.43 (192.168.100.43)' can't be established.
ED25519 key fingerprint is SHA256:DaSrJqGjEsH9EKJwA9bo23UQYyI0haHgeYTLNx7OzLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
laboratorio@192.168.100.43's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'laboratorio@192.168.100.43'"
and check to make sure that only the key(s) you wanted were added.
```

```
laboratorio@Lab1:~$ ssh-copy-id laboratorio@192.168.100.44
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
The authenticity of host '192.168.100.44 (192.168.100.44)' can't be established.
ED25519 key fingerprint is SHA256:qyZ3HK1SnfO7CJRwKYlqvcmjWojpUwjVy9QACIjZ4vI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
laboratorio@192.168.100.44's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'laboratorio@192.168.100.44'"
and check to make sure that only the key(s) you wanted were added.
```

Se ingresó sin contraseña a Lab2 y Lab3. Se puede ver en la captura de pantalla que incluso se intentó ingresar a Lab3 desde Lab2 y daba el error que pedía una contraseña.

```
laboratorio@Lab1:~$ ssh laboratorio@192.168.100.43
Linux Lab2 6.12.48+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.48-1 (2025-09-
20) 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.
laboratorio@Lab2:~$ ssh laboratorio@192.168.100.44
The authenticity of host '192.168.100.44 (192.168.100.44)' can't be established.
ED25519 key fingerprint is SHA256:qyZ3HK1SnfO7CJRwKYlqvcmjWojpUwjVy9QACIjZ4vI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? no
Host key verification failed.
laboratorio@Lab2:~$ exit
logout
Connection to 192.168.100.43 closed.
laboratorio@Lab1:~$ ssh laboratorio@192.168.100.44
Linux Lab3 6.12.48+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.48-1 (2025-09-
20) 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.
laboratorio@Lab3:~$ exit
logout
Connection to 192.168.100.44 closed.
laboratorio@Lab1:~$
```

Citas y Referencias

Bhatt, H. (2024, 4 marzo). ¿Qué es RSA? ¿cómo funciona un RSA? *Encryption Consulting*.

https://www.encryptionconsulting.com/education-center/what-is-rsa/

ChigozieCO. (2024, 19 de febrero). Remotely accessing a virtual machine using SSH key pair. Dev Community. https://dev.to/chigozieco/remotely-accessing-a-virtual-machine-ssh-key-pair-4en4

Cloudflare. (s. f.-a). *What is SSH (Secure Shell)?* Cloudflare. Recuperado el 11 de octubre de 2025, de https://www.cloudflare.com/learning/access-management/what-is-ssh/

Cloudflare. (s. f.-b). *What is SSL (Secure Sockets Layer)?* Cloudflare. Recuperado el 11 de octubre de 2025, de https://www.cloudflare.com/learning/ssl/what-is-ssl/

Equipo editorial de IONOS. (2022, 1 marzo). *¿Cómo funcionan las claves RSA?* IONOS Digital Guide. https://www.ionos.com/es-us/digitalguide/servidores/seguridad/claves-rsa/

Gitlan, D. (2025, 11 marzo). *Cifrado RSA vs AES: Explicación de las diferencias entre claves*. SSL Dragon. https://www.ssldragon.com/es/blog/rsa-aes-cifrado/

Linuxize. (2019, 19 de febrero). How to Set Up SSH Key-Based Authentication on Linux. Linuxize. https://linuxize.com/post/how-to-setup-passwordless-ssh-login/

Panda Security. (2023, 27 julio). *¿Qué es el cifrado AES? Una guía sobre el Advanced Encryption Standard*. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/cifrado-aes-guia/