Práctica de Evaluación 9 – SSH
Fecha: 30 de noviembre de 2023
Resultados de aprendizaje y Criterios de evaluación que se evalúan: RA 3: e, f, g

---

¿Qué es SSH?

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.
Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

Más información

https://www.hostinger.es/tutoriales/que-es-ssh#¿Que_es_SSH

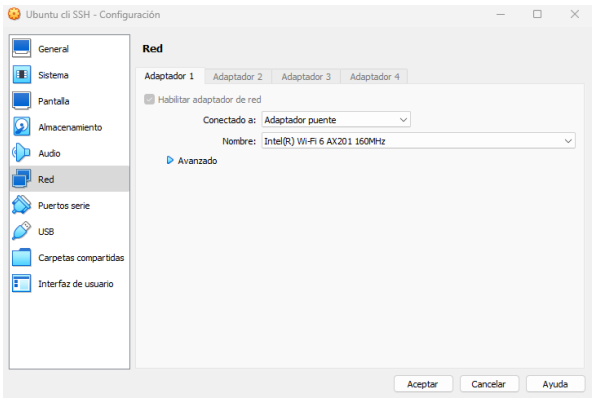
Los mejores clientes SSH para Windows (Putty)

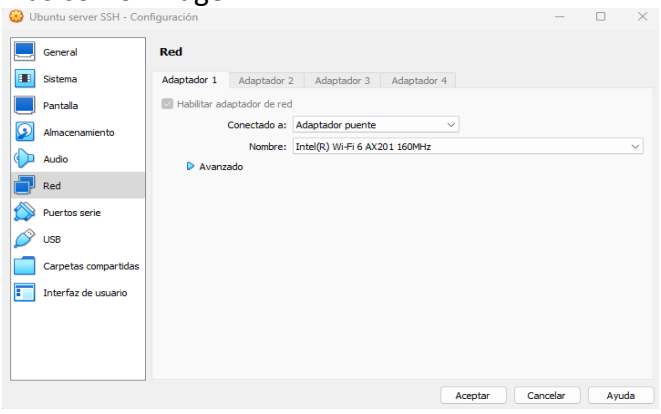
https://www.redeszone.net/tutoriales/servidores/mejores-clientes-ssh-windows/

Descripción de la actividad

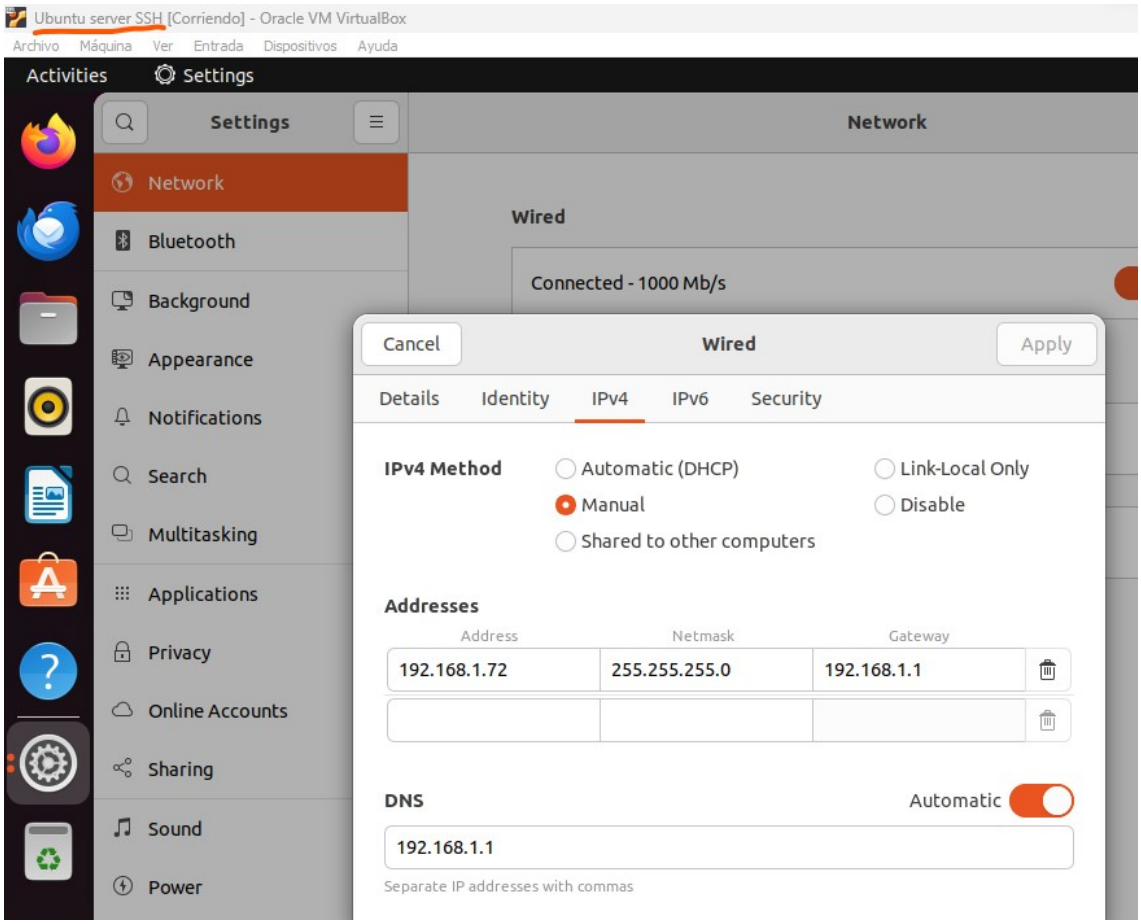
Realiza un documento en .pdf donde expliques paso a paso como has realizado la comunicación vía SSH con el servidor,. El documento debe tener capturas de pantalla de cada uno de los pasos a realizar y deberá incluir todos los puntos que se piden. NO REALICES LA PRÁCTICA A LA PRISA Y CON POCA JUSTIFICACIÓN O INFORMACIÓN, cada falta o error de la práctica quita -0,5. La puntuación total de la práctica es de 10.

1. Crea dos máquinas con UBUNTU. Una de ellas hará de Servidor SSH y otra de cliente SSH.
2. Establece las tarjetas de red de las máquinas como Bridge.





3. Deberás configurar la tarjeta de red de la máquina servidora del servicio SSH con una IP FIJA.



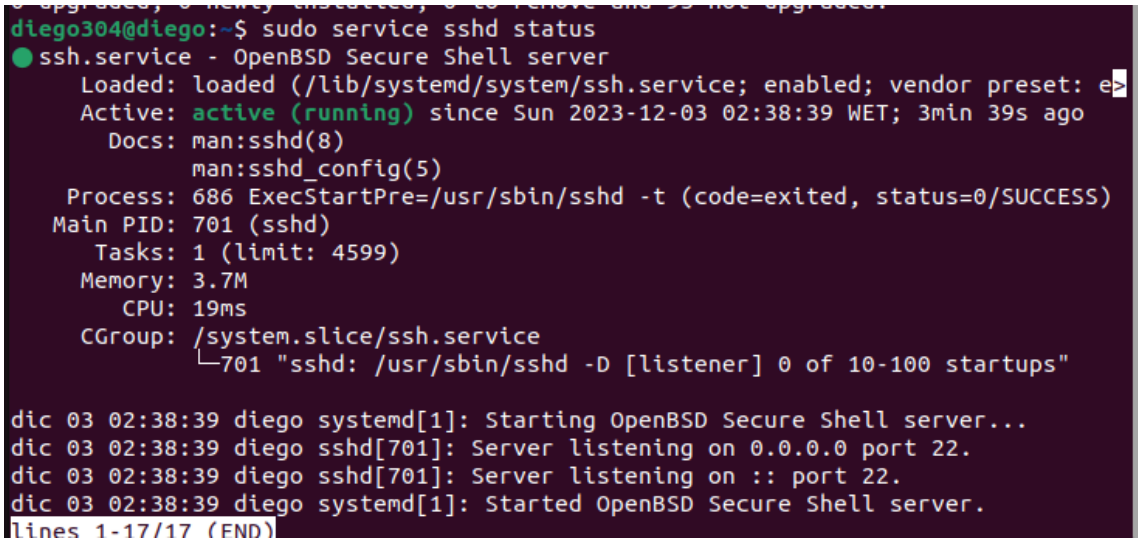
4. Realiza las instalaciones y configuraciones SSH en cada uno de los UBUNTU.

SERVER:

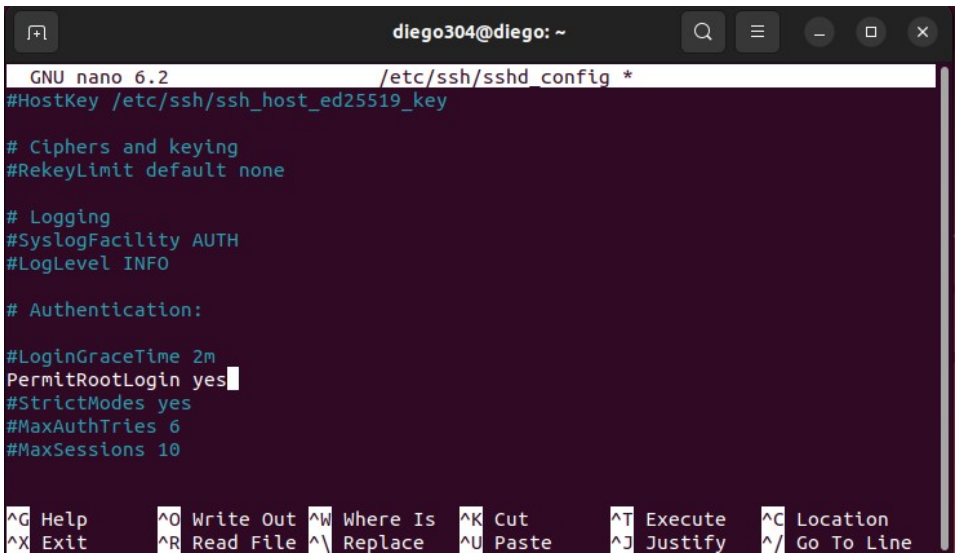
Primero instalares ssh en la maquina servidor.

```
diego304@diego:~$ sudo apt install openssh-server
[sudo] password for diego304:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.4).
0 upgraded, 0 newly installed, 0 to remove and 95 not upgraded.
```

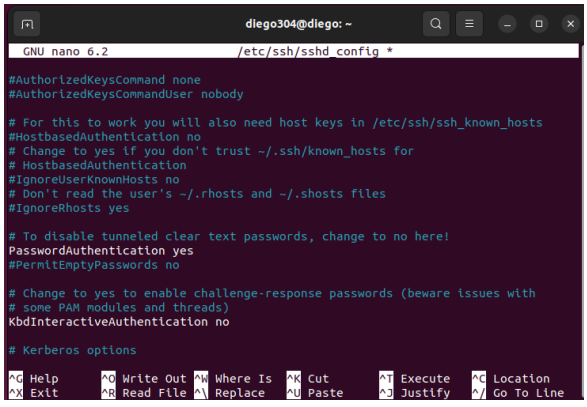
Comprobamos que el estado del servicio funciona correctamente



Ahora configuraremos en el archivo “sshd_config” el apartado PERMITROOTLOGIN poniéndolo en yes para que permita hacer login a los usuarios root.



Y también ponemos el yes en el apartado para que nos pida autorización con contraseña al loguearnos.



También crearemos un par de claves para nuestra maquina servidor para poder diferenciar las claves de cliente y servidor como veremos mas adelante.

```
diego304@diego:/etc/ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/diego304/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/diego304/.ssh/id_rsa
Your public key has been saved in /home/diego304/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:5xm4JeDKHRdN4RpprUs2ZpTNAAd75Gbzrlpyy9TLnT8 diego304@diego
The key's randomart image is:
+---[RSA 3072]----+
|       oo+ o.    |
|        = @      |
|       o & *     |
|      . B O      |
|       o S =     |
|    . o B @ o    |
|     o o * =     |
|        * + o .E |
|       ..+ o o... |
+----[SHA256]-----+
diego304@diego:/etc/ssh$
```

```
diego304@diego:~/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQoJVsOId8xk2PNQCufyO2hVXL1OMSCB2ASjd4Oiz9EItPTVi62l69k3HGaq9CC2WMixrKFPCEq8g1+wweShLbzBEMq4ZrOLh4Luj2aGRryrt3aWe+0MElJWv/xUpBm6tvspPJINc1pfcvWAdfl0Y2jY/jLr9VBbzVAVs9
7QwZk6OobDz8YUdlaaGMzxKlcoXNcV/zxOQUUJPiCDZ6WlqMNqsACcIM0cU7WkjnPju7BP7DXit7nCw9JlSUcWvG6cwa3dlgsSeBwCjTF8ufLHUVqvgip//7YMdaDctXTVfOFQrO7YWcMCpVN4xhwWW5zm8REMTACue/oKkRdRPxEboLZqA78aYdI3slntGSGuEpN2aSc2ST
bSbWkDBmu2NBF/6ZvdJTvbmy+KSWsuSdhHVWDeEDijlNnFds+QUBLLEbDwSD6idfdEVSSETafWyj+86JNYnnpf2W/X3NnXhlhZVXBj1PnkzSF+t3HLH1xZih8YB7klAgHT0hQopVXIvuw6E= diego304@diego
diego304@diego:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA0KCVbDiHQcZNjzUArn8jtoVVy9TjOQgdgEo3eDtc/RCLT01Yutou
vZNxxmqvQgtljIsayhTwhKvINfsMHuYS28wRDKuGazl4eC7o9mhka8q7d2lnvtDBIlVr/8
VKQZurb7KTySDXNaX3L1gHX5dGNoZP4y6/VQW81QFbPe0MGZOjqGw8/GFHYmnhjM8SpXKF
zXfT8QBFCTyHA2elpajDarAAnCDWFO1pISz47uwT+wi4re5wsPS2UlWFrxunNGt3YoL
EngCAo0xfLnyx1Far4Iqf/+2DHWg3LV01XzhUKzu2FnDAqVTePMYcFluc5VERDEwArnv6Cp
EXUT8RG6C2agO/GmHSN7JZ7RkhrhKTdmknNkk2+W1pAwZrtjQRf+mb3SU725svluVrLknY
R1Vg3hA4o4jZxXbPkFASyxGw8Eg+onX3RFUkhE2n1so/vOlTWJp6X9lv19zZ14YoWVWY9
T55M0hfrdxyx9cWdYfGAeSJQIB09IUKKVVyL7sOhAAAFlDGG768xhu+vAAAAB3NzaC1yc2
EAAAGBANCglWv4h0HGTY81AKS/I7aFVcvU4zkIHY8K9J3g7XP0Ql09NkLraLr2TccZqr01L
ZYyLGsoUBISryDX7DB7MEtvMEQyrhms4uHgu6PZoZGvKu3dpZ77QwSIla//FSkCbq2+yk8
kg1zWl9y9YB1+XRjaNj+Muv1UFvNUBWz3tDBmTo6hsPPxhR2JpoYzPEqVyhc1xX/PENBRQ
k8hwNnpaWow2qwAJwgzRxTtaSOc+O7sE/sNeK3ucLD0mVJRxa8bpzBrd2KCxJ4HAKNMXyS
8sdRWq+CKn//tgx1oNyidNV84VCs7thZwwKlU3jGHBZbnObxEQxMAKS7+gqRFiE/ERugtn
oOvxph0jeyWe0ZIa45k3ZpJzZJNvltaQMGa7YBEX/pm9Ol9ubL4rlay5J2EdVYN4QOKOI
2cV2z5BQEssRsPBIPqJ198RVJIRNp9bKP7zok1iael/Zb9fc2deGKFlVcGPU+eTNIX63cc
sfXFnWHxgHuSUCAdPSFCilVci+7DoQAAAAMBAAEAAAGADGgRTLnNmtTta7PO5CGfzMDP/+
argsqrkPOQ6gWrN2oog601hqqXCxtpoZ9aZ+C8P6vtyljNjxE1XzbsQwn18xbXCHgqjqWl
TDHbdRxTBPk91dmDA7UfuB1uN0wK6P0GOFav/M7m92v0x7gqGSZYFNJNPUkMVCS6xJa/n5
6ROLPnwIo7w/UvwN+n3ZNaoHO/lt6cMmePcooSaMH6DmOBRRtySrYd1+PxYQDC6zv/YrU2
xoTbDH82fWYwk1GNo4sHhnulZUauaARZ5D+5Cd8NDuWeKuvErb75sQNEnk9eubEssGMgd5
mUeDIR4fDLjKptZkS3MaaZvAbIMZr9KCT3h6V5eZuvzSkSRjlPG4hjhAl2xhEPIK2g3Iec
+KAIAv3GQWXg2KzX1m3QbdIPviQ0ZdokuGn5lleSp09pktDvR+Rgh0Ccaorrn/LxNu/8PD
Lr8vkT2eth0FSW3C5fxWqbMcNDVP1EwYUql9OP6j7+dQuXWbsYNaXY68BOsF/f9RuRAAAA
wQCDZhSKnNgZyBKnSnjg0Q93fKK+zPM9YLk6lJzgmC2YKNbynNFSTbmE3pc44VzSrve72b
q4+phTo0OZYR1km8aIoarhPUltUtCNYfrj8+q2N2q7mLbAAjvM4tpyub+7O1JA1cQUeTb
p1/WIhsmwZZoHuGkCBgtTn3AFfl2MnfgnOgTnI19PDdYZuWI/42yDQXw2DUNNh4gZgnGWL
rLR2A+lrjrO4YzZ3FY8/DkmLYQ/l8/MSsD/Q4ipqEdCSeUfvQAAADBANXo9/imU3g7fDnD
VGTofGeGZ2x84GF0cR/8hEUfB/KvOLjFgnZAv28tWRuDbf+rUINQm/5PirrLo9ds5zeKe
qES7EtjlMll2ArXORCO466HWyDYHOzw+b9VZp8bmbuPcefTLk0BjZVvIGgVqoFKybkwO0P
yGLJXuzXTc7HjwgoYS9kUSt/v7xp1ikZFZsSvijpKHbUTD8yuXIgeCN17+NOEstxzAnAz7
FsNgSnnbuYWf7sfaGKAn6oY/rYaimJ8QAAAMEA+a2DZmu2NwOELthOFzzP56CWzSvLVk4y
dECZ+nkX7NgRuWtayuViGlklNz3Zalq9KWGpfuzqrc72ce/ZSA27kHTB7cShBDCg4yoafW
k9YHDCr7R7vVGdZjgSYXXbavU7rgUa8sr53Tn3fJYQ659XlJsZrAIsuC1JFklGTMm/+od2
u6UrRSAsNb6J f8whIIoIrXClW1Oh6k/LPC1wogaLqpx+XVzxYfxQe1nefwe50IHoRe0sxL
ebRQeDYdT+WKSxAAAADmRpZWdvMzA0QGRpZWdvAQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

CLIENTE:

En nuestra maquina cliente instalaremos la versión cliente de ssh

```
diego4@diegocli:~$ sudo apt-get install openssh-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-client is already the newest version (1:8.9p1-3ubuntu0.4).
openssh-client set to manually installed.
The following packages were automatically installed and are no longer required:
  ncurses-term openssh-sftp-server ssh-import-id
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 95 not upgraded.
diego4@diegocli:~$
```

Y comprobamos que ambas maquinas tengan conexión entre ellas

```
diego4@diegocli:~$ ping 192.168.1.72
PING 192.168.1.72 (192.168.1.72) 56(84) bytes of data.
64 bytes from 192.168.1.72: icmp_seq=1 ttl=64 time=0.025 ms
64 bytes from 192.168.1.72: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 192.168.1.72: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from 192.168.1.72: icmp_seq=4 ttl=64 time=0.039 ms
64 bytes from 192.168.1.72: icmp_seq=5 ttl=64 time=0.035 ms
64 bytes from 192.168.1.72: icmp_seq=6 ttl=64 time=0.058 ms
64 bytes from 192.168.1.72: icmp_seq=7 ttl=64 time=0.059 ms
64 bytes from 192.168.1.72: icmp_seq=8 ttl=64 time=0.025 ms
64 bytes from 192.168.1.72: icmp_seq=9 ttl=64 time=0.058 ms
64 bytes from 192.168.1.72: icmp_seq=10 ttl=64 time=0.045 ms
64 bytes from 192.168.1.72: icmp_seq=11 ttl=64 time=0.052 ms
64 bytes from 192.168.1.72: icmp_seq=12 ttl=64 time=0.038 ms
64 bytes from 192.168.1.72: icmp_seq=13 ttl=64 time=0.055 ms
64 bytes from 192.168.1.72: icmp_seq=14 ttl=64 time=0.052 ms
64 bytes from 192.168.1.72: icmp_seq=15 ttl=64 time=0.053 ms
64 bytes from 192.168.1.72: icmp_seq=16 ttl=64 time=0.042 ms
^C
--- 192.168.1.72 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15360ms
rtt min/avg/max/mdev = 0.025/0.044/0.059/0.010 ms
diego4@diegocli:~$
```

5. La máquina que hará de server tendrá dos usuarios, "homer" que será el usuario administrador y otro que será "peter" que tendrá simples privilegios de usuario. Desde la máquina cliente lo que haremos será manejar la máquina server de manera remota...Esto lo haremos en el punto 6 y 7 con dos de las maneras de autenticarse en SSH.

Creamos el usuario homer

```
diego304@diego:~$ sudo adduser homer
Adding user `homer' ...
Adding new group `homer' (1003) ...
Adding new user `homer' (1003) with group `homer' ...
Creating home directory `/home/homer' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
Changing the user information for homer
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
diego304@diego:~$
```

Y le damos privilegios de administrador

```
diego304@diego:~$ sudo usermod -aG sudo homer
diego304@diego:~$
```

Haremos lo mismo con el usuario peter pero a este no le daremos estos permisos.

```
diego304@diego:~$ sudo adduser peter
Adding user `peter' ...
Adding new group `peter' (1004) ...
Adding new user `peter' (1004) with group `peter' ...
Creating home directory `/home/peter' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
Changing the user information for peter
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
diego304@diego:~$
```

6. Realiza las configuraciones pertinentes para que desde tu máquina cliente puedas conectarte con los usuarios root, homer y peter al servidor ssh usando únicamente como control de acceso un login y un password.

En primera instancia para que nos deje loguear con sudo deberemos restablecer la contraseña ya que si no nos dará un fallo al tratar de entrar

```
diego304@diego:~$ sudo usermod -aG sudo root
diego304@diego:~$ sudo passwd root
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
diego304@diego:~$
```

Ya desde el cliente después de las configuraciones dichas anteriormente ejecutamos el comando “ssh usuario@IP_SERVIDOR” para iniciar sesión poniendo la contraseña que en nuestro caso es “qwerty1234”.

```
diego4@diegocli:~$ ssh root@192.168.1.73
The authenticity of host '192.168.1.73 (192.168.1.73)' can't be established.
ED25519 key fingerprint is SHA256:Cfqf+rcO76i3hc1G73hIA+MJCaeDQhKDzAi7BTlEdGw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.73' (ED25519) to the list of known hosts.
root@192.168.1.73's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-35-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***
Last login: Sun Dec  3 21:11:37 2023 from 192.168.1.72
root@diego:~# exit
logout
Connection to 192.168.1.73 closed.
diego4@diegocli:~$
```

Y hacemos lo mismo con los otros dos usuarios para comprobar que funciona correctamente

```
diego4@diegocli:~$ ssh homer@192.168.1.73
homer@192.168.1.73's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-35-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

homer@diego:~$ exit
logout
Connection to 192.168.1.73 closed.
diego4@diegocli:~$
```

```
diego4@diegocli:~$ ssh peter@192.168.1.73
peter@192.168.1.73's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-35-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

peter@diego:~$ exit
logout
Connection to 192.168.1.73 closed.
diego4@diegocli:~$
```

7. Realiza las configuraciones pertinentes para que desde tu máquina cliente puedas conectarte con los usuarios root, homer y peter al servidor ssh usando únicamente como control de acceso una clave pública SSH.

Empezamos creando las claves en la maquina cliente ya que estas las usaremos para confirmar la conexión con el servidor. Para que no nos requiera ningún tipo de contraseña para loguear no le pondremos contraseña a las claves y la conexión la autenticara el servidor.

```
diego4@diegocli:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/diego4/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/diego4/.ssh/id_rsa
Your public key has been saved in /home/diego4/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:KrzxQzcQfEpWVw/tGKWEKp5HA4y2oj1gXzTHLAIzHGg diego4@diegocli
The key's randomart image is:
+---[RSA 3072]----+
|o=o  +o.. .o+o.  |
|.Eo.o+B+.....+.  |
|.  .o++= .  .+.  |
|... ..+ +   . .  |
|.+.... =S.       |
|. oo  +.+        |
|   .+..o .       |
|     =.          |
|    . ..         |
+----[SHA256]-----+
diego4@diegocli:~$
```

Copiamos las claves desde los usuarios del cliente al servidor poniendo el usuario que se autentica y la ip del servidor. Esto lo hacemos con todos los usuarios

```
diego4@diegocli:~$ ssh-copy-id root@192.168.1.73
/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
root@192.168.1.73's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.1.73'"
and check to make sure that only the key(s) you wanted were added.

diego4@diegocli:~$
```

```
diego4@diegocli:~$ ssh-copy-id homer@192.168.1.73
/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
homer@192.168.1.73's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'homer@192.168.1.73'"
and check to make sure that only the key(s) you wanted were added.

diego4@diegocli:~$
```

```
diego4@diegocli:~$ ssh-copy-id peter@192.168.1.73
/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
peter@192.168.1.73's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'peter@192.168.1.73'"
and check to make sure that only the key(s) you wanted were added.

diego4@diegocli:~$
```

Probamos a conectarnos igual que antes pero ahora ya que nos registra por la clave no nos pide ningún tipo de contraseña con ninguno de los 3 usuarios.

```
diego4@diegocli:~$ ssh root@192.168.1.73
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-35-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

*** System restart required ***
Last login: Sun Dec  3 21:13:44 2023 from 192.168.1.72
root@diego:~# exit
logout
Connection to 192.168.1.73 closed.
diego4@diegocli:~$
```

```
diego4@diegocli:~$ ssh homer@192.168.1.73
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-35-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***
Last login: Sun Dec  3 21:14:31 2023 from 192.168.1.72
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

homer@diego:~$ exit
logout
Connection to 192.168.1.73 closed.
diego4@diegocli:~$
```

```
diego4@diegocli:~$ ssh peter@192.168.1.73
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-35-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

32 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***
Last login: Sun Dec  3 21:15:48 2023 from 192.168.1.72
peter@diego:~$ exit
logout
Connection to 192.168.1.73 closed.
diego4@diegocli:~$
```

Para comprobar que se paso correctamente en la maquina servidor en el archivo /home/diego304/.ssh/authorized_keys podremos ver que nos llego correcta mente la clave autorizada desde diego@diegocli que es nuestro cliente.

```
diego304@diego:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
diego304@diego:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCzRcFR58xJc2b2EeAY83TpnE0TtM54pbJeOJZYOLtnUNwRCfNBLkZ4OcLFsbXfcrUWjNBUbgEdwluCVsxShu3XT0Ahb9lsl9PtxtLQ7cezCzwWYXm3bf+/OVAxxjWcoWLXkEjXTKRJ1NELGvywsqAGNoS/6CzZBA/qMPlj
QKM07omaV4eGyBT5j3RzpThXpgT5DSaQKDxRWBbLGUMgEfQ66yLHR/i8Y1SnUvLBa/Zw7Rluf/FRXgskutdWB2sF3jVcpIA2s/T7lZNObKUFa/S5oEvRVBBDBom3fbRSjsG3OE9JpFZjYbrluW+S4MFHcTI1qTPpS/O3qAGcfm6t2oL0mr75ECqK6/918u2NIUrW3KkPU98N
QmpfwpVKjqLVQ9R2dAp+BjecCmaWVfJEz/7EUVGQrVcM58nTtPEdb4yHfdn/hM4cHZOsKtB/vlIKvKAdujk9b7MCCfUUFAsJRr6O62TUVKVedKbn7q5l8AVK+4kELDaokhWvWrvGH1Od+DE= diego4@diegocli
diego304@diego:~/.ssh$
```

8. ¿Qué método recomiendan como método de autenticación en SSH? ¿Por qué?

Principalmente yo recomendaría el método de autenticación por clave publica que ya es mas seguro a la hora de transmitir información ademas de tener un login mas ameno al no pedir contraseña.
Esto lo puede llegar a ser un problema de seguridad ya que si consiguen la clave podrían entrar pero igualmente recomendaría el método de claves ya que la autenticación por login el vulnerable a ataques por diccionario sobre todo usando el usuario root que es conocido por la mayoría de usuarios.