En esta práctica se utilizan dos MV:

- Servidor SSH: se ha instalado un Debian 12. Este sistema operativo ya incorpora el paquete “openssh-server” y tiene operativo el software de servidor ssh.

```
root@servidor:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sun 2023-10-01 08:29:22 CEST; 3 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 488 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 538 (sshd)
      Tasks: 1 (limit: 2285)
     Memory: 5.8M
        CPU: 694ms
     CGroup: /system.slice/ssh.service
             └─538 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct 01 08:43:16 servidor sshd[1152]: pam_unix(sshd:session): session opened for user mortadel
oct 01 08:43:16 servidor sshd[1152]: pam_env(sshd:session): deprecated reading of user enviro
```

- Cliente SSH: se ha instalado un Ubuntu 22.

Ambas máquinas comprobamos que trabajan en la misma red. Si se puede en RedNAT o si no en NAT.

1) Deberéis comprobar la dirección ip asignada a la tarjeta de red de cada máquina (con el comando “ipconfig” o con “ip a” y posteriormente comprobar que se conectan mediante el comando ping.

```
mortadelo@servidor:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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,DYNAMIC,UP,LOWER_UP> mtu 1500 qdisc fq_codel sta
te UP group default qlen 1000
    link/ether 08:00:27:8b:f5:a1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8b:f5a1/64 scope link
       valid_lft forever preferred_lft forever
mortadelo@servidor:~$
```

2) En la MV servidora tenemos un usuario llamado “doraemon” y de contraseña “nobita”.

Lo he creado desde el usuario root con el comando:

adduser doraemon -home /home/doraemon

```
root@servidor:~# adduser doraemon -home /home/doraemon
Añadiendo el usuario `doraemon' ...
Añadiendo el nuevo grupo `doraemon' (1001) ...
Adding new user `doraemon' (1001) with group `doraemon (1001)' ...
Creando el directorio personal `/home/doraemon' ...
Copiando los ficheros desde `/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para doraemon
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
 Nombre completo []:
 Número de habitación []:
 Teléfono del trabajo []:
 Teléfono de casa []:
 Otro []:
¿Es correcta la información? [S/n] s
Adding new user `doraemon' to supplemental / extra groups `users' ...
Añadiendo al usuario `doraemon' al grupo `users' ...
root@servidor:~#
```

Si vemos el contenido de la carpeta creada para el usuario “doraemon”:

```
root@servidor:~# ls -la /home/doraemon/
total 36
drwx------ 3 doraemon doraemon 4096 oct  1 08:54 .
drwxr-xr-x 4 root     root     4096 oct  1 08:49 ..
-rw------- 1 doraemon doraemon   23 oct  1 08:57 .bash_history
-rw-r--r-- 1 doraemon doraemon  220 oct  1 08:49 .bash_logout
-rw-r--r-- 1 doraemon doraemon 3526 oct  1 08:49 .bashrc
drwx------ 3 doraemon doraemon 4096 oct  1 08:54 .config
-rw-r--r-- 1 doraemon doraemon 5290 oct  1 08:49 .face
lrwxrwxrwx 1 doraemon doraemon    5 oct  1 08:49 .face.icon -> .face
-rw-r--r-- 1 doraemon doraemon  807 oct  1 08:49 .profile
root@servidor:~#
```

(OJO: No hay ninguna carpeta .ssh, porque no ha guardado ninguna clave pública ni privada ahí).

3) Conexión por SSH pero **autenticando al usuario con contraseña**. Vamos a comprobar el acceso desde la MV cliente Ubuntu al servidor. Para ello, desde un terminal tecleamos:

ssh doraemon@dir_ip_servidor

```
pikachu@cliente:~$ ssh doraemon@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ED25519 key fingerprint is SHA256:NrKiKELOwYRogLDI189P5L2EtOdagaysZGIMF2vdGeM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Escribimos “yes”.

```
Warning: Permanently added '10.0.2.7' (ED25519) to the list of known hosts.
doraemon@10.0.2.7's password:
```

A continuación nos indica que va a guardar como host conocido al que nos estamos conectando y después nos pide el password para el usuario “doraemon”, es decir “nobita”.

Tras indicársela nos muestra el siguiente mensaje de bienvenida al servidor y ya estaríamos dentro:

```
doraemon@10.0.2.7's password:
Linux servidor 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) 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: Sun Oct  1 08:55:11 2023 from 10.0.2.15
doraemon@servidor:~$
```

Recordad, en esta conexión en la MV cliente Ubuntu **se ha almacenado un fichero que contiene la clave pública del servidor SSH**. Este fichero se denomina **known_hosts** y está en una carpeta .ssh que se ha creado automáticamente en el home del usuario desde el que lancé la orden “ssh …”. En mi caso la conexión la hice desde el terminal de mi usuario pikachu (el único que había creado en mi MV Ubuntu):

```
pikachu@cliente:~$ ls -la .ssh
total 16
drwx------  2 pikachu pikachu 4096 oct  4 20:08 .
drwxr-x--- 15 pikachu pikachu 4096 oct  4 20:06 ..
-rw-------  1 pikachu pikachu  978 oct  4 20:08 known_hosts
-rw-r--r--  1 pikachu pikachu  142 oct  4 20:06 known_hosts.old
```

¿Qué aspecto tiene una clave pública?

```
pikachu@cliente:~$ cat .ssh/known_hosts
|1|kb74teXTosx73bc41c18/FhIhkQ=|kGjiooAbSb/V3OtY7sMVmzKNywY= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAA
AIKBcW423LQBnIeAWirKJiDrqOzcJKU9U74kY5mkD/vbR
|1|8fGGcaDyScIncWr8j430vChpchY=|F5WNhlYRP3POYaBjZkll4I1m0HM= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAA
BgQDaiHEwxhFBpcVvMk2AXvJi5XIpuooFBzj4XU/Rf0UTjoPtBRhJYaIeR0UF0N3zyqtRlPpojJm7ugkZl5Ywl9szKvWOjBb
AyTx0CwDVhSVKSPVNzsLBbP9f6z2qOC5KwYjdWyyuybOf+ANCQzTDRzgyDTfogQlObDezJ3BqUKsn5zZexX26ykxxaIaLOBI
fQIkUA5AA4MembqgwbmeT9fTJLuLA8Vf09SWSJpvW6SVQlIfcd5ynJ4RTAi7AFy/373/Ce2SasZmS7n+trjJ9edw/mtglQA6
upFTB95hqOPvr2mRk2nFrRF6AZgnnQ4MNnDjLZlSkakCO/ny0/EbV9VbvTp1lliCIDPTfs6XnQ6s7xtMwoRQ8B/zT66dyd4J
Fm0oaZGMkfULYDfq6nfIc++3fdynmwNU8h0OGn9HXlkFbhY2AfAwPkQpdrZPBy19ha4vfoRc2i2yEM7GZdGQxX1v9dSm/aan
5TSwqMaesfjK6NkoC0+ld3AeK7NhLeFxwMKk=
|1|JR/pqsW0u4CnoUK3fyL+lVHX0VY=|cjof1aEkAzMNWKfzB3HH1IIvuQk= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXN
oYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKjlM22J2Zpx8OwC9rDV1Dtauy2yhntOsEdGI2VA5dDjuEXwGzsBUs1cEkL
0GVpskbLGlI2ZeWi+xmlo486/ueM=
```

Sin embargo, en esta imagen no se ve una única clave pública sino tres. (Aquí se identifican porque empiezan por |1|).

¿Y dónde tenía esto almacenado el servidor SSH en la MV Debian?

```
root@servidor:~# ls -la /etc/ssh/*.pub
-rw-r--r-- 1 root root 175 sep 29 09:26 /etc/ssh/ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root  95 sep 29 09:26 /etc/ssh/ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 567 sep 29 09:26 /etc/ssh/ssh_host_rsa_key.pub
```

NOTA: Al instalar el paquete openssh-server, ya preinstalado, se crean tres pares de claves pública-privada: una con RSA, otra con ECDSA y otra con ED25519. Estos son distintos algoritmos para crear claves asimétricas.

Si veo el contenido de uno de ellos identificaré alguna de las cadenas mostradas en la pantalla del cliente.

```
root@servidor:~# cat /etc/ssh/ssh_host_ed25519_key.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKBcW423LQBnIeAWirKJiDrqOzcJKU9U74kY5mkD/vbR root@servidor
```

4) Conexión por SSH autenticando al usuario con clave pública.

Ahora se necesita crear el mismo usuario con el que nos queremos conectar al servidor SSH.

He creado en el cliente un usuario doraemon para conectarme luego desde remoto al servidor y le incluyo como administrador de la máquina local MV Ubuntu:

sudo adduser doraemon –home */home*/doraemon

sudo usermod -aG sudo doraemon

Inicio sesión con este usuario mortadelo: su doraemon

```
doraemon@cliente:~$ pwd
/home/doraemon
doraemon@cliente:~$ ls -la
total 20
drwxr-x--- 2 doraemon doraemon 4096 oct  4 20:26 .
drwxr-xr-x 5 root     root     4096 oct  4 20:26 ..
-rw-r--r-- 1 doraemon doraemon  220 oct  4 20:26 .bash_logout
-rw-r--r-- 1 doraemon doraemon 3771 oct  4 20:26 .bashrc
-rw-r--r-- 1 doraemon doraemon  807 oct  4 20:26 .profile
```

Genero el par de claves rsa para doraemon

ssh-keygen -t rsa -b 4096

Cuando me pregunte el nombre del fichero a almacenar le digo "/home/doraemon/.ssh/doraemon" así luego es más fácil para mí distinguirlo en el anillo de claves.

```
doraemon@cliente:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/doraemon/.ssh/id_rsa): /home/doraemon/.ssh/doraemon
Created directory '/home/doraemon/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/doraemon/.ssh/doraemon
Your public key has been saved in /home/doraemon/.ssh/doraemon.pub
The key fingerprint is:
SHA256:JymyBc/WtG9VRyujWFEGiZDo5+Dqu3jmyigmwZgzDVw doraemon@cliente
The key's randomart image is:
+---[RSA 4096]----+
|      ..o .o+o  .|
|   E . . . .o  ..|
|. . o   .  . o...|
|..   * + oo ..o. |
|o+  o X S....    |
|*..  * o + .     |
| +  o    o       |
|=..+     .       |
|=+*=o            |
+----[SHA256]-----+
doraemon@cliente:~$
```

Nos ha creado una carpeta .ssh y dos ficheros, uno con la clave pública (.pub) y otro con la clave privada:

```
doraemon@cliente:~$ ls -la .ssh/
total 16
drwx------ 2 doraemon doraemon 4096 oct  4 20:30 .
drwxr-x--- 3 doraemon doraemon 4096 oct  4 20:29 ..
-rw------- 1 doraemon doraemon 3434 oct  4 20:30 doraemon
-rw-r--r-- 1 doraemon doraemon  742 oct  4 20:30 doraemon.pub
doraemon@cliente:~$
```

Para poder conectarnos sin contraseña al servidor ssh deberemos copiar allí la clave pública del usuario “doraemon”. El proceso que se encargará de copiarlo desde aquí y guardarlo allí se denomina “ssh-agent”

Compruebo en la MV cliente si está lanzado desde mi usuario el proceso ssh-agent:

ps -ef| grep ssh-agent

si no está lo lanzo con este comando: eval "$(ssh-agent)"

```
doraemon@cliente:~$ eval "$(ssh-agent)"
Agent pid 93217
doraemon@cliente:~$ ps -ef|grep ssh-agent
doraemon   93217     673  0 20:35 ?        00:00:00 ssh-agent
doraemon   93407   79815  0 20:36 pts/0    00:00:00 grep --color=auto ssh-agent
```

Compruebo las claves públicas registradas por ssh-agent en mi máquina:

ssh-add -l

```
doraemon@cliente:~$ ssh-add -l
The agent has no identities.
```

** Si está vacío, añado la clave pública de mortadelo al anillo de claves públicas de la máquina:

ssh-add /home/doraemon/.ssh/doraemon

Aparecerá el mensaje: "Identity added: ….:

```
doraemon@cliente:~$ ssh-add /home/doraemon/.ssh/doraemon
Enter passphrase for /home/doraemon/.ssh/doraemon:
Identity added: /home/doraemon/.ssh/doraemon (doraemon@cliente)
doraemon@cliente:~$ ssh-add -l
4096 SHA256:JymyBc/WtG9VRyujWFEGiZDo5+Dqu3jmyigmwZgzDVw doraemon@cliente (RSA)
doraemon@cliente:~$
```

(El password que pide es el que introdujistéis al generar el par de claves).

Se pueden borrar las ya registradas con el comando "ssh-add -D".

Copiamos al servidor esta clave pública con la utilidad:

ssh-copy-id doraemon@10.0.2.7

```
doraemon@cliente:~$ ssh-copy-id doraemon@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ED25519 key fingerprint is SHA256:NrKiKELOwYRogLDI189P5L2EtOdagaysZGIMF2vdGeM.
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
nstalled
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are promp
e new keys
doraemon@10.0.2.7's password:
Permission denied, please try again.
doraemon@10.0.2.7's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'doraemon@10.0.2.7'"
and check to make sure that only the key(s) you wanted were added.

doraemon@cliente:~$
```

Si miramos en la MV Servidora SSH, habrá creado una carpeta /home/doraemon/.ssh con un

```
root@servidor:~# ls -la /home/doraemon/.ssh
total 12
drwx------ 2 doraemon doraemon 4096 oct  4 20:40 .
drwx------ 4 doraemon doraemon 4096 oct  4 20:40 ..
-rw------- 1 doraemon doraemon  742 oct  4 20:40 authorized_keys
root@servidor:~#
```

fichero authorized_keys que contiene la clave recién copiada :

```
root@servidor:~# cat /home/doraemon/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC7F2tVx4zcoqwYmY6u6iJvVg2PJc0t2hYBv
4RuYrX5M3ZWIyidVeE4rMW5AXVncn0oa/MCoUJIZYIsfU9T3G9VhDw0tIVItNyrReR5rfuaQj
e3CXElBf9GuBIFIbtKPZIvbGG+oRoTRDpBqi5O7IG+WPNXtB/phD8go82xgS0sF+YbyhFMWrc
XOsb1Wj4PJRPZUYwraREZs2ifP7wDOJ1l0ls+KgGLqlR8WXhue/SMszwB2gtfHiv7s5SV3aM+
+tP6gAQZT5FkL/uFnXHFHUdrXMSUlygmAJ4edYVlcRE1lJ00y189ZnF6nkquv4+/6SwavBp5W
PsIxKax6V9XRtoerYiTzFXq79wcfyysi+NsYhNCVurD9jB9e5ArzVGBN1TZzwbI926wTh2m9H
Xkp3DSQIrm73SEaSyFluGJBVuN7Ss3WuHbm9eZAn7aBPyRtuxC59ryKPXUk7UglQPAN0l8u3r
UCJxN2XUWTlT6a6JBq1YrMqP9+PFlOS1REqQ== doraemon@cliente
```

Para finalizar realizamos la conexión desde la MV cliente Ubuntu:

ssh doraemon@dir_ip_servidor