

EXERCICIS SSH

1.1 – SECURE SHELL SENSE CONTRASENYA

- SERVER 1: ADAPTADOR PONT

```
user@userserver:~$ cat /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses:
        - 172.16.24.203/24
      routes:
        - to: default
          via: 172.16.24.254
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

- SERVER 2: XARXA NAT (Port forwarding)

Xarxa

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4

☒ Habilita l'adaptador de xarxa

Connectat a: **NAT**

Nom:

▼ **Avançat**

Tipus d'adaptador: **Xarxa paravirtualitzada (virtio-net)**

Mode promiscu: **Denega**

Adreça MAC:

☒ Cable connectat

Reenviament de ports

Nom	Protocol	IP de l'amfitrió	Port de l'amfitrió	IP del client	Port del client
Rule 1	TCP	127.0.0.1	2222		22

al server1". Comprova-ho des

h

stall figlet

actant :)

```
l server1
```

banner

```
user@userserver:/etc/ssh$ sudo nano sshd_config
# no default banner path
Banner /etc/ssh/banner

user@userserver:~$ sudo systemctl restart sshd
[sudo] password for user:
user@userserver:~$
```

Quan intentem accedir veurem el missatge:

```
aaroncano@aaroncano:~$ ssh user@172.16.24.203
Warning: Permanently added '172.16.24.203' (RSA) to the list of known hosts.
user@172.16.24.203's password:
```

Configura a Server2 el servei ssh. Comprova-ho des de el teu host. Recorda que al estar en NAT hauràs de fer una redirecció de ports

```
aaroncano@aaroncano:~$ ssh -p 2222 user@localhost
user@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)
```

Aarón Cano

Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari per defecte del servidor 1 sense tenir que posar cap contrasenya

Primer generem una clau a la nostra màquina real amb la comanda keygen:

```
aaroncano@aaroncano:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/aaroncano/.ssh/id_rsa):
/home/aaroncano/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

Ara la copiem al server1:

```
aaroncano@aaroncano:~$ scp .ssh/id_rsa.pub user@172.16.24.203:/home/user
Warning: Permanently added '172.16.24.203' (SSH-2.0-OpenSSH_8.9p1 Ubuntu-0ubuntu0.2) to the list of known hosts.
user@server1:~$
```

Ara l'afegim al fitxer authorized_keys:

```
user@userserver:~$ cat id_rsa.pub >> .ssh/authorized_keys
```

Ara si intentem iniciar sessió no demanarà contrasenya:

```
aaroncano@aaroncano:~$ ssh user@172.16.24.203
Warning: Permanently added '172.16.24.203' (SSH-2.0-OpenSSH_8.9p1 Ubuntu-0ubuntu0.2) to the list of known hosts.
user@server1:~$
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)
```

Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari root del servidor 1 sense tenir que posar cap contrasenya

Primer hem d'habilitar l'usuari root canviant la seva contrasenya:

```
user@userserver:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
```

També haurem de modificar el fitxer /etc/ssh/sshd_config i permetre que pugui iniciar sessió:

```
GNU nano 6.2 /etc/ssh/sshd_config
# Authentication:

PermitRootLogin yes
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Reiniciem els serveis i després copiarem la mateixa clau d'abans a l'usuari root:

```
user@userserver:~$ sudo systemctl restart sshd
user@userserver:~$ sudo systemctl restart ssh
```

```
aaroncano@aaroncano:~$ scp .ssh/id_rsa.pub root@172.16.24.203:/root
Warning: Permanently added '172.16.24.203' (RSA) to the list of known hosts.
server
id_rsa.pub 100% 573 1.6MB/s 00:00
aaroncano@aaroncano:~$
```

Com abans l'afegim a l'authorized_keys:

```
aaroncano@aaroncano:~$ ssh root@172.16.24.203
```

```
[root@userserver ~]#
```

```
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)
```

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

```
System information as of dimecres, 28 de febrer de 2024, 13:10:43 UTC
```

```
System load:   0.0          Processes:           115
Usage of /:    46.4% of 11.21GB Users logged in:      0
Memory usage:  12%         IPv4 address for enp0s3: 172.16.24.203
Swap usage:    0%
```

```
Expanded Security Maintenance for Applications is not enabled.
```

```
Es poden aplicar immediatament 24 actualitzacions.
Per veure aquestes actualitzacions addicionals, executeu: apt list --upgradable
```

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

```
Last login: Wed Feb 28 13:01:11 2024 from 172.16.24.3
root@userserver:~# █
```

Utilitzant la mateixa clau la passarem al server2 de la mateixa forma però indicant el port i anant a localhost.

6

Aarón Cano

L'afegim a `authorized_keys`:

```
user@userserver:~$ cat id_rsa.pub >> .ssh/authorized_keys
```

```
aaroncano@aaroncano:~$ ssh -p 2222 user@localhost
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

System information as of dimecres, 28 de febrer de 2024, 13:18:12 UTC

System load:  0.0                Processes:           115
Usage of /:   46.4% of 11.21GB   Users logged in:    1
Memory usage: 12%                IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

Es poden aplicar immediatament 24 actualitzacions.
Per veure aquestes actualitzacions addicionals, executeu: apt list --upgradable

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Feb 28 12:15:03 2024 from 10.0.2.2
user@userserver:~$
```

Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari root del servidor 2 sense tenir que posar cap contrasenya

Seguirem els passos anteriors però tenint en compte el port forwarding:

```
user@userserver:~$ sudo passwd root
[sudo] password for user:
New password:
Retype new password:
passwd: password updated successfully
user@userserver:~$
```

```
GNU nano 6.2 /etc/ssh/sshd_config
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
user@userserver:~$ sudo systemctl restart sshd
user@userserver:~$ sudo systemctl restart ssh
user@userserver:~$
```

```
aaroncano@aaroncano:~$ scp -P 2222 .ssh/id_rsa.pub root@localhost:/root
```

L'afegim a authorized_keys:

```
root@userserver:~# cat id_rsa.pub >> .ssh/authorized_keys
```

```
aaroncano@aaroncano:~$ ssh -p 2222 root@localhost
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

System information as of dimecres, 28 de febrer de 2024, 13:23:23 UTC

System load:  0.078125      Processes:           119
Usage of /:   46.4% of 11.21GB Users logged in:       1
Memory usage: 12%          IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

Es poden aplicar immediatament 24 actualitzacions.
Per veure aquestes actualitzacions addicionals, executeu: apt list --upgradable

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

root@userserver:~#
```


1.2 – EXERCICI 2: scp + login sense contrasenya

SERVER 1: Adaptador pont

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses:
        - 172.16.26.203/24
      routes:
        - to: default
          via: 172.16.26.254
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

SERVER 2: NAT amb Port Forwarding



1. Configura a Server1 i server 2 el servei ssh amb el banner "Benvingut al server no X" on X és el número de servidor. Comprova-ho des de el teu host

SERVER 1:

```
aaron1@server1:~$ figlet Benvingut al server1
```

Benvingut al server1

server1

```
aaron1@server1:~$
```

```
sudo nano /etc/ssh/banner
```

[illegible]

```
sudo nano /etc/ssh/sshd_config
```

```
GNU nano 6.2 /etc/ssh/sshd_config
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
Banner /etc/ssh/banner
```

```
sudo systemctl restart ssh
```

```
sudo systemctl restart sshd
```

```
aaroncano@aaroncano:~$ ssh aaron1@172.16.26.203
Benvingut al
server
aaron1@172.16.26.203's password:
```


SERVER 2:

```
aaron2@server2:~$ figlet Benvingut al server 2
Benvingut al
server 2
```

```
GNU nano 6.2 /etc/ssh/banner
Benvingut al
server 2
```


2. Fes un scp desde el teu host per a copiar a.txt a la home de l'usuari per defecte de Server1 i comprova que s'ha pujat.

```
aaroncano@aaroncano:~$ scp a.txt aaron1@172.16.26.203:/home/aaron1
```



```
aaron1@172.16.26.203's password:
```

```
a.txt 100% 5 7.8KB/s 00:00
```

```
aaron1@server1:~$ cat a.txt
```

```
hola
```

3. Fes un scp desde el teu host per a copiar a.txt a la home de l'usuari per defecte de Server2 i comprova que s'ha pujat.

```
aaroncano@aaroncano:~$ scp -P 3333 a.txt aaron2@localhost:/home/aaron2
```



```
aaron2@localhost's password:
```

```
a.txt 100% 5 15.3KB/s 00:00
```

```
aaroncano@aaroncano:~$
```

```
aaron2@server2:~$ cat a.txt
```

```
hola
```

4. Edita a.txt a Server1 i fes que el contingut sigui "adeu". Des de el teu host descarrega a.txt del Server1 i comprova que ha canviat

```
aaron1@server1:~$ cat a.txt
adeu
```

```
aaroncano@aaroncano:~$ scp aaron1@172.16.26.203:/home/aaron1/a.txt .
```

```
Benvenuto a
```

```
Server1
```

```
aaron1@172.16.26.203's password:
```

```
a.txt
```

```
100% 5 9.0KB/s 00:00
```

```
aaroncano@aaroncano:~$ cat a.txt
```

```
adeu
```

5. Desde el teu host fes un scp del fitxer a.txt entre Server1 i Server 2 i comprova que ha funcionat.

```
aaron1@server1:~$ scp -P 3333 a.txt aaron2@localhost:/home/aaron2/
```

```
aaron2@server2:~$ cat a.txt
adeu
```

6. Edita el fitxer a server2 amb el nou missatge "Hola de nou" i ara copia de server 2 a server 1 executant el scp al teu host. Comprova que ha canviat.

```
aaron2@server2:~$ cat a.txt
Hola de nou
```


8. Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari per defecte del servidor 1 sense tenir que posar cap contrasenya

```
aaroncano@aaroncano:~$ ssh-copy-id -i .ssh/id_rsa.pub aaron1@172.16.26.203
```

```
aaroncano@aaroncano:~$ ssh aaron1@172.16.26.203
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

System information as of divendres, 8 de març de 2024, 08:31:24 UTC

System load:  0.0               Processes:    105
Usage of /:   53.8% of 11.21GB   Users logged in: 1
Memory usage: 26%              IPv4 address for enp0s3: 172.16.26.203
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

Es poden aplicar immediatament 70 actualitzacions.
9 d'aquestes actualitzacions són actualitzacions de seguretat.
Per veure aquestes actualitzacions addicionals, executeu: 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: Fri Mar  8 07:34:29 2024 from 172.16.26.28
aaron1@server1:~$
```

9. Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari root del servidor 1 sense tenir que posar cap contrasenya

```
aaron1@server1:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
```

```
GNU nano 6.2 /etc/ssh/sshd_config
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```



```
aaron1@server1:~$ sudo systemctl restart ssh
aaron1@server1:~$ sudo systemctl restart sshd
```

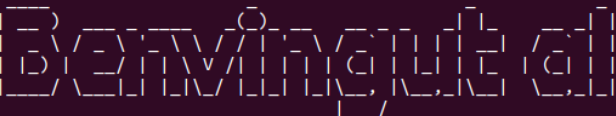

```
aaroncano@aaroncano:~$ ssh-copy-id -i .ssh/id_rsa.pub root@172.16.26.203
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already in
stalled
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the
new keys

root@172.16.26.203's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@172.16.26.203'"
and check to make sure that only the key(s) you wanted were added.
```

```
aaroncano@aaroncano:~$ ssh root@172.16.26.203


Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

System information as of divendres, 8 de març de 2024, 08:46:37 UTC

System load:  0.080078125      Processes:           111
Usage of /:   53.8% of 11.21GB  Users logged in:    1
Memory usage: 26%              IPv4 address for enp0s3: 172.16.26.203
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

Es poden aplicar immediatament 70 actualitzacions.
9 d'aquestes actualitzacions són actualitzacions de seguretat.
Per veure aquestes actualitzacions addicionals, executeu: 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 ***
root@server1:~#
```

10. Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari per defecte del servidor 2 sense tenir que posar cap contrasenya

```
aaroncano@aaroncano:~$ ssh-copy-id -p 3333 -i .ssh/id_rsa.pub aaron2@localhost
```

```
aaroncano@aaroncano:~$ ssh -p 3333 aaron2@localhost
```

Evangelical Christianity

```
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)
```

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

System information as of divendres, 8 de març de 2024, 08:35:07 UTC

```
System load: 0.0      Processes:            104
Usage of /:  44.8% of 11.21GB
Memory usage: 26%     Users logged in:    0
Swap usage:  0%       IPv4 address for enp0s3: 10.0.2.15
```

Expanded Security Maintenance for Applications is not enabled.

Es poden aplicar immediatament 24 actualitzacions.

Per veure aquestes actualitzacions addicionals, executeu: `apt list --upgradable`

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

```
Last login: Fri Mar  8 08:12:31 2024 from 10.0.2.2
```

```
aaron2@server2:~$
```

11. Configura els serveis per a que el teu usuari del teu host pugui accedir a l'usuari root del servidor 2 sense haver de posar cap contrasenya


```
GNU nano 6.2 /etc/ssh/sshd_config
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
aaron2@server2:~$ sudo systemctl restart ssh
aaron2@server2:~$ sudo systemctl restart sshd
```

```
aaroncano@aaroncano:~$ ssh-copy-id -p 3333 -i .ssh/id_rsa.pub root@localhost
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_rsa.pub"
/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
Warning: Permanently added 'localhost' (rsa) to the list of known hosts.
root@localhost's password:
Number of key(s) added: 1
Now try logging into the machine, with: "ssh -p '3333' 'root@localhost'"
```

```
aaroncano@aaroncano:~$ ssh -p 3333 root@localhost
```



```
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic x86_64)

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

System information as of divendres, 8 de març de 2024, 08:57:23 UTC

System load:   0.0          Processes:            105
Usage of /:    44.8% of 11.21GB Users logged in:      0
Memory usage:  26%         IPv4 address for enp0s3: 10.0.2.15
Swap usage:    0%
```

```
Expanded Security Maintenance for Applications is not enabled.

Es poden aplicar immediatament 24 actualitzacions.
Per veure aquestes actualitzacions addicionals, executeu: apt list --upgradable

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

```
root@server2:~#
```