

PRÁCTICA 2 (almellonesfernandez-practica2)

U.D.1. SSH. AUTENTICACIÓN. CONTROL DE ACCESO Y SEGURIDAD. (PARTE Nº 2)

CIFRADO ASIMÉTRICO: AUTENTICACIÓN MEDIANTE CIFRADO ASIMÉTRICO

Relacionado con el servidor SSHD de Ubuntu Server, realice las siguientes operaciones:

1. Genere un único par de llaves (XXxx, XXxx.pub, **será usado por usted durante todo el curso**) en el S.O. Ubuntu Server, de 2048 bits, sin contraseñas y las guarda inicialmente en el directorio /root/keys/ e introduzca dicha llave pública para poder realizar conexiones SSH a este servidor Ubuntu Server (`cat XXxx.pub >> /root/.ssh/authorized_keys`, `cat XXxx.pub >>/home/XXxx/.ssh/authorized_keys`). (0,5 puntos cada uno). Compruebe que puede conectarse al servidor Ubuntu server, usando la llave privada, desde:

```
root@ubuntu-server-bastionado:~# cd keys/
root@ubuntu-server-bastionado:~/keys# ssh-keygen -t rsa -b 2048 -f /root/keys/almellonesfernandez -N ""
Generating public/private rsa key pair.
Your identification has been saved in /root/keys/almellonesfernandez
Your public key has been saved in /root/keys/almellonesfernandez.pub
The key fingerprint is:
SHA256:DvXsxv1lRUUsZRD4Kfu9LAhNttRepFb21lK3ds root@ubuntu-server-bastionado
The key's randomart image is:
+---[RSA 2048]-----+
|      .o+B0|
|      .+++|
|      .o+o|
|      .o.o.=|
|      .S.o.=*|
|      o.o.o.=0|
|      .B.O.++E|
|      o.B.O.o|
|      .+o|
+-----[SHA256]-----+
root@ubuntu-server-bastionado:~/keys# ls
almellonesfernandez  almellonesfernandez.pub
```

```
almellonesfernandez@ubuntu-server-bastionado:~/ssh$ sudo su
root@ubuntu-server-bastionado:/home/almellonesfernandez/.ssh# cat /root/keys/almellonesfernandez.pub >> /root/.ssh/authorized_keys
root@ubuntu-server-bastionado:/home/almellonesfernandez/.ssh# cat /root/keys/almellonesfernandez.pub >>/home/almellonesfernandez/.ssh/authorized_keys
```

- a. Localhost. (No es necesario copiar la llave privada en ningún lugar, ya que la tenemos), tanto como usuario XXxx como root (`ssh -i /root/keys/llaveprivada XXxx@localhost`, `ssh -i /root/keys/llaveprivada root@localhost`) (`netstat -putan |grep ESTABLISHED`)

```
almellonesfernandez@ubuntu-server-bastionado:~$ sudo ssh -i /root/keys/almellonesfernandez root@localhost
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

Álvaro Almellones Fernández

```
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo ssh -i /root/keys/almellonesfernandez almellonesfernandez@localhost
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la
conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

root@Ubuntu-server-bastionado:~# netstat -putan | grep ESTABLISHED
tcp        0      0 127.0.0.1:45226      127.0.0.1:22        ESTABLISHED 1191/ssh
tcp        0      0 127.0.0.1:57820     127.0.0.1:22        ESTABLISHED 2192/ssh
tcp        0      0 127.0.0.1:22        127.0.0.1:57820     ESTABLISHED 2193/sshd: root@pts
tcp        0      0 127.0.0.1:22        127.0.0.1:45226     ESTABLISHED 1192/sshd: almellon
tcp        0      0 127.0.0.1:60714     127.0.0.1:22        ESTABLISHED 1857/ssh
tcp        0      0 192.168.1.107:22    192.168.1.106:50366 ESTABLISHED 957/sshd: almellone
tcp        0      0 127.0.0.1:22        127.0.0.1:60714     ESTABLISHED 1858/sshd: almellon
root@Ubuntu-server-bastionado:~#
```

b. Cliente Microsoft Windows mediante comando. Recuerde que previamente hay que copiar la llave privada en Windows) (#scp XXxx.pub root@IP:/root/keys/llaveprivada c:\Usuarios\Desktop\MisKeys\llaveprivada)

```
Microsoft Windows [Versión 10.0.22631.4317]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alvar>scp root@192.168.1.107:/root/keys/almellonesfernandez C:\Users\alvar\Desktop\MisKeys
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de
este sistema informático
root@192.168.1.107's password:
almellonesfernandez 100% 1843 163.6KB/s 00:00

C:\Users\alvar>

almellonesfernandez@Ubuntu
C:\Users\alvar>ssh -i Desktop\MisKeys\almellonesfernandez almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de
este sistema informático
Ubuntu 24.04.1 LTS
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

System information as of Sun Oct 27 07:11:39 PM UTC 2024

System load:  0.0          Processes:            109
Usage of /:   13.2% of 24.44GB Users logged in:          1
Memory usage: 27%          IPv4 address for enp0s3: 192.168.1.107
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.

44 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

Last login: Sun Oct 27 18:59:07 2024 from 192.168.1.106
almellonesfernandez@Ubuntu-server-bastionado:~$
```

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastion: ~  
C:\Users\alvar>ssh -i Desktop\MisKeys\almellonesfernandez root@192.168.1.107  
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático  
Ubuntu 24.04.1 LTS  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Sun Oct 27 07:15:04 PM UTC 2024  
  
System load:  0.05          Processes:           113  
Usage of /:   13.2% of 24.44GB Users logged in:      1  
Memory usage: 28%          IPv4 address for enp0s3: 192.168.1.107  
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.  
  
44 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  
  
Last login: Sun Oct 27 19:15:04 2024 from 192.168.1.106  
root@Ubuntu-server-bastionado:~#
```

c. Cliente Microsoft Windows (GUI) (Mobaterm) desde usuario root. Recuerde que tiene que importar la llave privada en la aplicación GUI Mobaterm.

```
C:\Users\alvar>scp C:\Users\alvar\Desktop\MisKeys\almellonesfernandez C:\Users\alvar\AppData\Roaming\MobaXterm\home\MisKeys  
1 archivo(s) copiado(s).  
  
C:\Users\alvar>  
  
[2024-10-27 21:08:06] ~  
[alvar.LAPTOP-BK7DSVDP] > ssh -i "C:\Users\alvar\AppData\Roaming\MobaXterm\home\MisKeys\almellonesfernandez" al  
mellonesfernandez@192.168.1.107  
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está pro  
hibida la conexión si no es Administrador de este sistema informático  
Ubuntu 24.04.1 LTS  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
System information as of Sun Oct 27 08:08:14 PM UTC 2024  
  
System load:  0.0          Processes:           106  
Usage of /:   13.2% of 24.44GB Users logged in:      1  
Memory usage: 29%          IPv4 address for enp0s3: 192.168.1.107  
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.  
  
44 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  
  
MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
```

Álvaro Almellones Fernández

```

root@Ubuntu-server-bastionado: ~
[2024-10-27 21:10:20] ~
[alvar.LAPTOP-BK7DSVDP] ▶ ssh -i "C:\Users\alvar\AppData\Roaming\MobaXterm\home\MisKeys\almellonesfernandez" ro
ot@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está pro
hibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

System information as of Sun Oct 27 08:10:33 PM UTC 2024

System load:  0.0           Processes:            113
Usage of /:   13.2% of 24.44GB    Users logged in:     1
Memory usage: 29%           IPv4 address for enp0s3: 192.168.1.107
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.

44 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

root MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```

También se puede importar en una sesión y conectarte automáticamente sin tener que poner el comando ssh manualmente

Session settings

SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL

Basic SSH settings

Remote host: 192.168.1.107 Specify username: almallonesfernandez Port: 22

Advanced SSH settings Terminal settings Network settings Bookmark settings

☒ X11-Forwarding ☒ Compression Remote environment: Interactive shell

Execute command: Do not exit after command ends

SSH-browser type: SFTP protocol Follow SSH path (experimental)

☒ Use private key: me\MisKeys\almallonesfernandez Expert SSH settings

Execute macro at session start: <none>

OK Cancel

Aceptas usar private key y pegas la dirección en la que se encuentra la key

```
2. 192.168.1.107 (almellonesfernandez)
Pre-authentication banner message from server:
| Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del a
> lumno almellonesfernandez. Está prohibida la conexión si no es Administrador
> de este sistema informático
| Ubuntu 24.04.1 LTS
End of banner message from server
Authenticating with public key "root@Ubuntu-server-bastionado"

• MobaXterm Personal Edition v24.2 •
(SSH client, X server and network tools)

► SSH session to almellonesfernandez@192.168.1.107
• Direct SSH : ✓
• SSH compression : ✓
• SSH-browser : ✓
• X11-forwarding : ✓ (remote display is forwarded through SSH)

► For more info, ctrl+click on help or visit our website.

Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

System information as of Sat Nov 2 03:36:42 PM CET 2024
```

d. Cliente Ubuntu Desktop en modo comando. Recuerde que previamente hay que copiar la llave privada en algún directorio de Ubuntu Desktop (le recomiendo /root/MisKeys/)

```
root@almellonesfernandez-VirtualBox: ~/miskeys
root@almellonesfernandez-VirtualBox:~/miskeys# echo "antes del scp" && ls && scp root@192.168.1.107:/root/keys/almellone
sfernandez /root/miskeys && echo "despues del scp" && ls
antes del scp
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida l
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
root@192.168.1.107's password:
almellonesfernandez 100% 1843 19.6KB/s 00:00
despues del scp
almellonesfernandez
root@almellonesfernandez-VirtualBox:~/miskeys#
```

```
root@almellonesfernandez-VirtualBox:~/miskeys# ssh -i /root/miskeys/almellonesfernandez root@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida l
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)
```

```
root@almellonesfernandez-VirtualBox:~/miskeys# ssh -i /root/miskeys/almellonesfernandez almellonesfernandez@192.168.1.10
7
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida l
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)
```

```
root@almellonesfernandez-VirtualBox:~/miskeys# hostname -I
192.168.1.108
```

```
almellonesfernandez@Ubuntu-server-bastionado:~$ sudo netstat -putan |grep ESTABLISHED
tcp        0      52 192.168.1.107:22      192.168.1.108:42030  ESTABLISHED 1692/sshd: almellon
tcp        0      0 192.168.1.107:22      192.168.1.106:64539 ESTABLISHED 1053/sshd: almellon
tcp        0      0 192.168.1.107:22      192.168.1.106:64540 ESTABLISHED 1055/sshd: almellon
```

Álvaro Almellones Fernández

e. Cliente APP de su smartphone (Juice SSH, o la que desee) desde usuario XXxx. Recuerde que tiene que importar la llave privada en la aplicación de su APP.

La versión gratuita de termux no me permitia cambiar el fondo a blanco con letras en negro

```
17:38
$ scp root@192.168.1.107:/root/keys almellonesfernandez
/data/data/com.termux/files/home
Bienvenido al servidor Ubuntu server del modulo de Basti
onaje de redes, del alumno almellonesfernandez. Está pro
hibida la conexión si no es Administrador de este siste
ma informático
Ubuntu 24.04.1 LTS
almellonesfernandez 100% 1843 133.0KB/s 00:00
```

```
17:42
$ ssh -i /data/data/com.termux/files/home/almellonesfe
rnandez almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del modulo de Basti
onaje de redes, del alumno almellonesfernandez. Está pro
hibida la conexión si no es Administrador de este siste
ma informático
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generi
c x86_64)

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

System information as of Sat Nov  2 05:42:41 PM CET 202
4

System load: 0.16          Processes:
119
Usage of /:  14.6% of 24.44GB Users logged in:
1
Memory usage: 34%          IPv4 address for enp0
s3: 192.168.1.107
Swap usage:  0%

* Strictly confined Kubernetes makes edge and IoT secur
e. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8
s cluster deployment.

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

Expanded Security Maintenance for Applications is not en
abled.

57 updates can be applied immediately.
13 of these updates are standard security updates.
To see these additional updates run: apt list --upgradab
le

Enable ESM Apps to receive additional future security up
dates.
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 set
tings

Last login: Sat Nov  2 17:30:45 2024 from 192.168.1.66
almellonesfernandez@Ubuntu-server-bastionado:~$
```

```
17:39 ...
$ ifconfig
Warning: cannot open /proc/net/dev (Permission denied).
Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
    txqueuelen 1000 (UNSPEC)

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.66 netmask 255.255.255.0 broadcast 192.168.1.255
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
    txqueuelen 3000 (UNSPEC)

$
```

```
root@Ubuntu-server-bastionado:/home/almellonesfernandez# netstat -putan | grep ESTABLISHED
tcp        0      0 192.168.1.107:22    192.168.1.66:58956  ESTABLISHED 3298/sshd: almallor
tcp        0      0 192.168.1.107:22    192.168.1.108:42030 ESTABLISHED 1692/sshd: almellon
tcp        0    48 192.168.1.107:22    192.168.1.106:64539 ESTABLISHED 1053/sshd: almellon
tcp        0      0 192.168.1.107:22    192.168.1.106:64540 ESTABLISHED 1055/sshd: almellon
root@Ubuntu-server-bastionado:/home/almellonesfernandez#
```


2. A continuación, vamos a dotar a todos los demás S.O del servicio SSHD, además del servidor Ubuntu Server. Para ello, usaremos la misma llave pública (y por tanto la misma llave privada para poder autenticarnos). Instale SSHD y modifique el fichero `authorized_keys` (de la forma que cree oportuno), para que podamos conectarnos mediante un cliente a los servidores siguiente.

a. Servidor SSHD en Ubuntu Desktop (1 punto)

```
root@Ubuntu-server-bastionado:~/keys# ls
almellonesfernandez almellonesfernandez.pub
root@Ubuntu-server-bastionado:~/keys# ssh-copy-id -i /root/keys/almellonesfernandez.pub almellonesfernandez@192.168.1.108
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/keys/almellonesfernandez.pub"
The authenticity of host '192.168.1.108 (192.168.1.108)' can't be established.
ED25519 key fingerprint is SHA256:eyDuJ2HWPCvuV1sWi7NyOWQiK08JK4S/XYotm/yeaYY.
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 prompted now it is to install the new keys
almellonesfernandez@192.168.1.108's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'almellonesfernandez@192.168.1.108'"
and check to make sure that only the key(s) you wanted were added.
```

```
almellonesfernandez@almellonesfernandez-VirtualBox: ~/.ssh
almellonesfernandez@almellonesfernandez-VirtualBox:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-11-02 22:35:46 CET; 52min ago
 TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
        man:sshd_config(5)
   Process: 1068 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1083 (sshd)
     Tasks: 1 (limit: 4388)
    Memory: 2.1M (peak: 2.3M)
       CPU: 25ms
   CGroup: /system.slice/ssh.service
           └─1083 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

nov 02 22:35:46 almellonesfernandez-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
nov 02 22:35:46 almellonesfernandez-VirtualBox sshd[1083]: Server listening on :: port 22.
nov 02 22:35:46 almellonesfernandez-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
almellonesfernandez@almellonesfernandez-VirtualBox:~$ cd .ssh
almellonesfernandez@almellonesfernandez-VirtualBox:~/.ssh$ ls
authorized_keys
almellonesfernandez@almellonesfernandez-VirtualBox:~/.ssh$ cat authorized_keys
almellonesfernandez@almellonesfernandez-VirtualBox:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCCcD3bCVqScitx1ATf50Zl0Ebc+PKo0/+7WERq4K8kEnZrlyRaby+1MyE8j/PgEQhHSvJLeil0+gDPJ1gM22YlK93enAki6en6jKuAi/xgnaIK0YgeNz/smaeutq/f9cmUug+ieSFCBMPHaMA7zYLZoDpZDp7PI94nQy10Vvj6ZULD5yDaW1YF2k1PN69M7H/yp2uJW2BQp6HOXUkcTGTnxWYmMUsPUS8diIfzQPcQGxvu7kwJ7fkfYKELkyNRK3eKzoE22eZTNyCsNyygAdTWyU9sAa+YWU3RqRnmwshXbdS6EW8I2cnlaYFQLmrhXQ8goIse4W7RYtTouQI1x root@Ubuntu-server-bastionado
almellonesfernandez@almellonesfernandez-VirtualBox:~/.ssh$
```


Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-VirtualBox: ~/.ssh$ scp /home/almellonesfernandez/.ssh/authorized_keys root@localhost:/root/.ssh/authorized_keys
root@localhost's password:
authorized_keys                               100% 411      8.4KB/s   00:00
almellonesfernandez@almellonesfernandez-VirtualBox: ~/.ssh$ sudo su
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCCcD3bCVqSqcitx1ATf50Zl0Ebc+PKo0/+7WERq4K8kEnZriyRaby+1MyxE8j/PgEQhHSvJLeil0+gDPJ1g
M22YlK93enAki6en6jKuAi/xgnaik0YgeNz/smaeutq/f9cmUug+ieSFCBMPHaMA7zYLZoDpZDp7PI94nQy10Vvj6ZULD5yDaW1YF2k1PN69M7H/yp2uJW2B
Qp6H0XUkcTGTnxWYmMUSPUS8diIifzQPcQGxvu7kwJ7fkfYKELkyNRK3eKzoE22eZTNycsNyygAdTWyU9sAa+YWU3RqRnmwshXbdS6EW8I2cnlaYFQLmrhX
Q8qoIse4W7RYtTouQI1x root@Ubuntu-server-bastionado
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/.ssh#
```

```
root@Ubuntu-server-bastionado:/home/almellonesfernandez# ssh -i /root/keys/almellonesfernandez almellonesfernandez@192.168.1.108
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-48-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 48 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

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

Last login: Sun Nov  3 00:02:48 2024 from 192.168.1.107
almellonesfernandez@almellonesfernandez-VirtualBox:~$ exit
logout
Connection to 192.168.1.108 closed.
root@Ubuntu-server-bastionado:/home/almellonesfernandez# ssh -i /root/keys/almellonesfernandez root@192.168.1.108
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-48-generic x86_64)

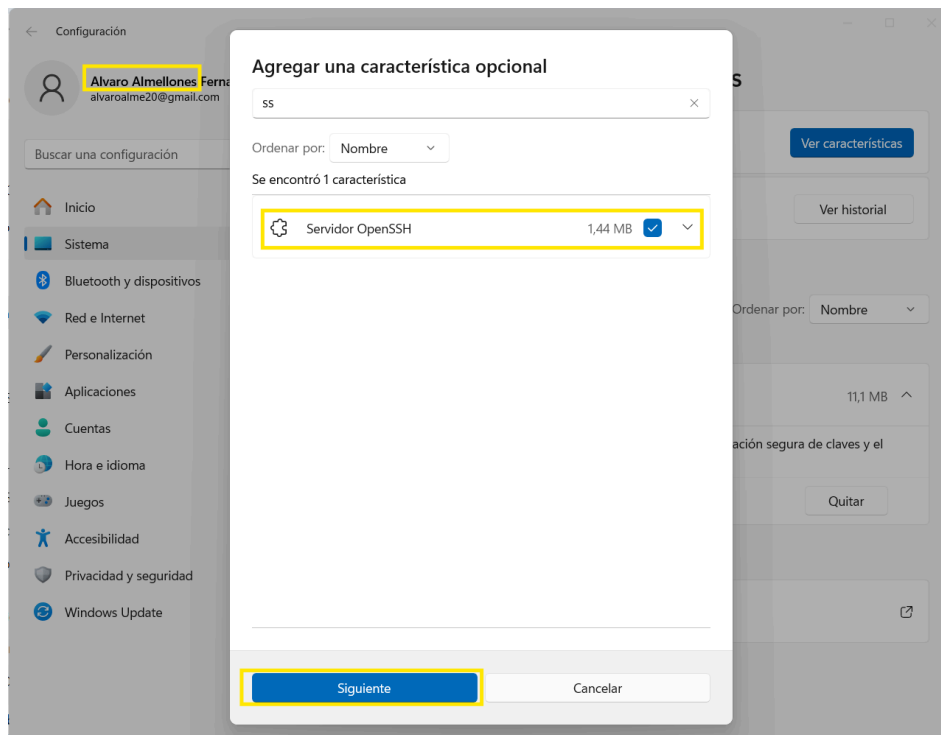
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 48 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
```

Activar Windows
Ve a Configuración para activar Windows.

b. Servidor SSHD de Windows. (1,5 punto)



Acciones recientes



Servidor OpenSSH

Agregada

Administrador: Windows PowerShell

Windows PowerShell

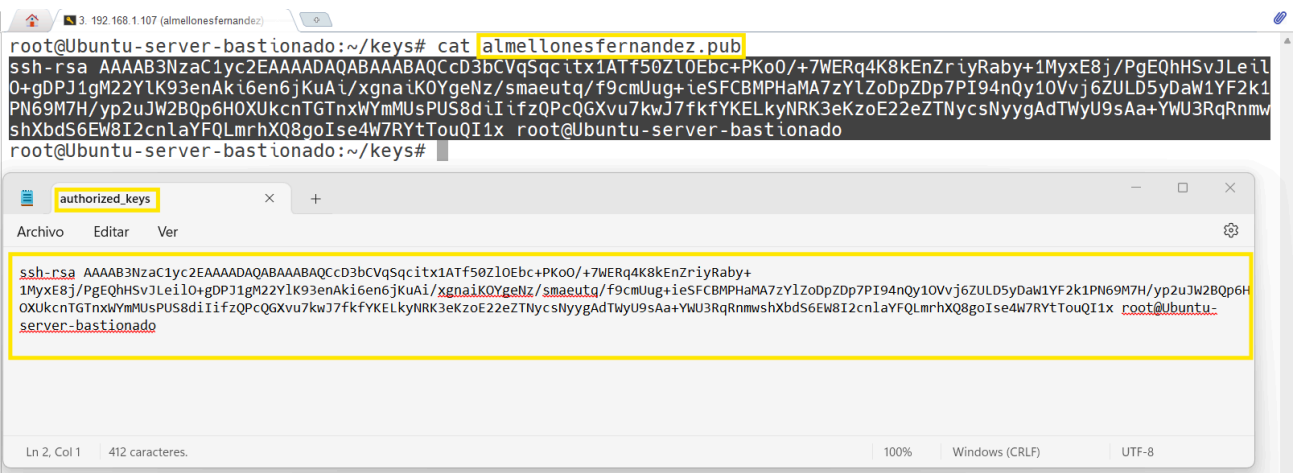
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. <https://aka.ms/PSWindows>

```
PS C:\WINDOWS\system32> Start-Service sshd
```

```
PS C:\WINDOWS\system32> Set-Service -Name sshd -StartupType 'Automatic'
```

```
PS C:\WINDOWS\system32>
```



Ejercicio no terminado porque no he conseguido acceder al usuario de windows por ssh , me daba permiso denegado y tenía la clave pública en

authorized_keys

c. Smartphone. (1 punto).

La versión gratuita de termux no me permitia cambiar el fondo a blanco con letras en negro

```
17:06
$ whoami
u0_a434
$ ifconfig
Warning: cannot open /proc/net/dev (Permission denied).
Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
    txqueuelen 1000 (UNSPEC)

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.66 netmask 255.255.255.0 broadcast 192.168.1.255
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
    txqueuelen 3000 (UNSPEC)

$ sshd
$ cat $PREFIX/etc/ssh/sshd_config | grep Port
Port 8022
#GatewayPorts no
$ psswd
No command psswd found, did you mean:
  Command passwd in package termux-auth
$ passwd
New password:
Retype new password:
New password was successfully set.
$
```

```
4. 192.168.1.107 almellonesfernandez
5. 192.168.1.108 (almellonesfernandez)
root@Ubuntu-server-bastionado:/home/almellonesfernandez# ssh-copy-id -i /root/keys/almellonesfernandez.pub
-p 8022 u0_a434@192.168.1.66
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/keys/almellonesfernandez.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
u0_a434@192.168.1.66's password:
SELinux: Loaded file_contexts

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p 8022 'u0_a434@192.168.1.66'"
and check to make sure that only the key(s) you wanted were added.

root@Ubuntu-server-bastionado:/home/almellonesfernandez# ssh -i /root/keys/almellonesfernandez -p 8022 u0_a
434@192.168.1.66
Welcome to Termux

Docs:      https://doc.termux.com
Community: https://community.termux.com

Working with packages:
- Search: pkg search <query>
- Install: pkg install <package>
- Upgrade: pkg upgrade

Report issues at https://bugs.termux.com
~ $ ^C
~ $ exit
logout
Connection to 192.168.1.66 closed.
```

Álvaro Almellones Fernández

Aclaración: Es la primera tarea que hay contenidos no explicados en clase (instalación de servidor SSHD en Windows y smartphone), pero en la mayoría de los casos es muy fácil realizarlo. El fichero de configuración se suele llamar de igual forma.

Para evidenciar este ejercicio, elija las capturas que crea oportuno para demostrar que:

- Se ha instalado correctamente. (netstat, ss, systemctl, etc.)
- Podemos loguearnos mediante usuario/contraseña (tcpdump, netstat, iptraf, etc.)
- Se ha introducido correctamente el contenido de la llave pública en authorized_keys del servidor en cuestión
- Se ha hecho una conexión desde otro cliente (comando, GUI) para probar que funciona la autenticación mediante llave privada.

****** Tendrá que realizar esta operación cada vez que tengamos un nuevo servidor en este curso. Puede usar el comando ssh-copy-id desde Ubuntu Server, para meter la clave pública en cada uno de estos nuevos servidores SSHD. Aunque se recuerda que hay muchas más formas (scp, winscp, cat)..**

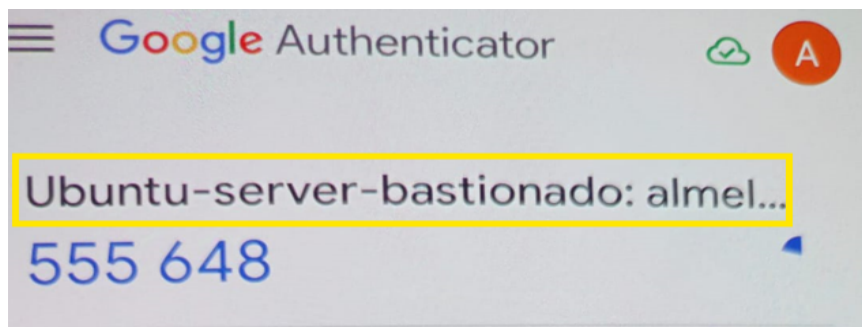
CIFRADO ASIMÉTRICO: AUTENTIFICACIÓN MEDIANTE LLAVES Y DOBLE FACTOR DE AUTENTIFICACIÓN (2FA)

3. Realice todo lo necesario para que se pueda entrar al servidor SSHD, usando a la vez llave privada y usando doble Autenticación (TOTP, contraseña de un sólo uso por tiempo), usando para ello la herramienta Google Authenticator (**KbdInteractiveAuthentication yes**).

Se deja al estudiante que elija las capturas necesarias para demostrar que le funciona correctamente. Se recomienda que siga los pasos del material proporcionado al alumno.

(0,5 punto)

```
almellonesfernandez@Ubuntu-server-bastionado:~$ grep -E '#@include common-auth|auth required pam_google_authenti
cator.so' /etc/pam.d/sshd
#@include common-auth
auth required pam_google_authenticator.so
almellonesfernandez@Ubuntu-server-bastionado:~$ grep -E 'ChallengeResponseAuthentication|PubkeyAuthentication|Use
ePAM|AuthenticationMethods publickey.keyboard-interactive' /etc/ssh/sshd_config
PubkeyAuthentication yes
AuthenticationMethods publickey,keyboard-interactive
ChallengeResponseAuthentication yes
UsePAM yes
almellonesfernandez@Ubuntu-server-bastionado:~$
```



```
C:\Users\alvar> ssh -i "C:\Users\alvar\Desktop\MisKeys\almellonesfernandez" almellonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de
este sistema informático
Ubuntu 24.04.1 LTS
(almellonesfernandez@192.168.1.107) Verification code:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

System information as of Sat Nov  2 08:23:26 PM CET 2024

System load:  0.61               Processes:    119
Usage of /:   14.6% of 24.44GB    Users logged in: 1
Memory usage: 33%               IPv4 address for enp0s3: 192.168.1.107
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.

57 updates can be applied immediately.
13 of these updates are standard security updates.
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

Last login: Sat Nov  2 20:00:47 2024 from 192.168.1.106
almellonesfernandez@Ubuntu-server-bastionado:~$
```

REDUCIENDO LAS PROBABILIDADES DE EXPOSICIÓN ATAQUES. CONEXIÓN CLIENTE SERVIDOR

4. Cambie (sólo en el servidor Ubuntu Server) para que se pueda únicamente autentificar mediante el uso de cifrado asimétrico, no por usuario/contraseña (demuestre que no se puede). A partir de ahora, no se puede entrar con usuario/contraseña en todo el curso.

(PasswordAuthentication no) (0,5 puntos)

```
almellonesfernandez@Ubuntu-server-bastionado:~$ grep -E 'ChallengeResponseAuthentication|PubkeyAuthentication|AuthenticationMethods publickey|PasswordAuthentication no' /etc/ssh/sshd_config
PubkeyAuthentication yes
PasswordAuthentication no
AuthenticationMethods publickey
ChallengeResponseAuthentication no
almellonesfernandez@Ubuntu-server-bastionado:~$
```

```
root@Ubuntu-server-bastionado:~$ ssh almallonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almallonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
almellonesfernandez@192.168.1.107: Permission denied (publickey).

C:\Users\alvar>ssh root@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almallonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
root@192.168.1.107: Permission denied (publickey).

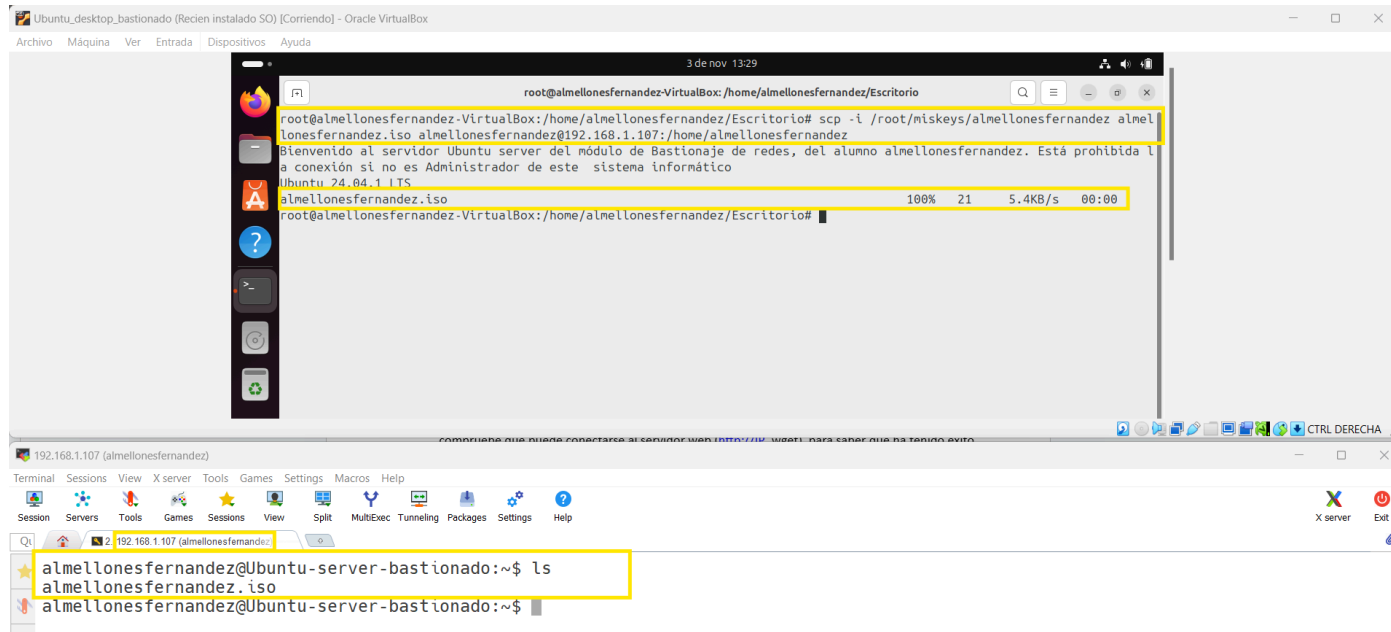
C:\Users\alvar>ssh -i "C:\Users\alvar\Desktop\MisKeys\almellonesfernandez" almallonesfernandez@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almallonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Last login: Sat Nov 2 20:23:26 2024 from 192.168.1.106
almellonesfernandez@Ubuntu-server-bastionado:~$ ^C
almellonesfernandez@Ubuntu-server-bastionado:~$ exit
logout
Connection to 192.168.1.107 closed.

C:\Users\alvar>ssh -i "C:\Users\alvar\Desktop\MisKeys\almellonesfernandez" root@192.168.1.107
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almallonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Last login: Sat Nov 2 17:40:53 2024 from 192.168.1.66
root@Ubuntu-server-bastionado:~#
```

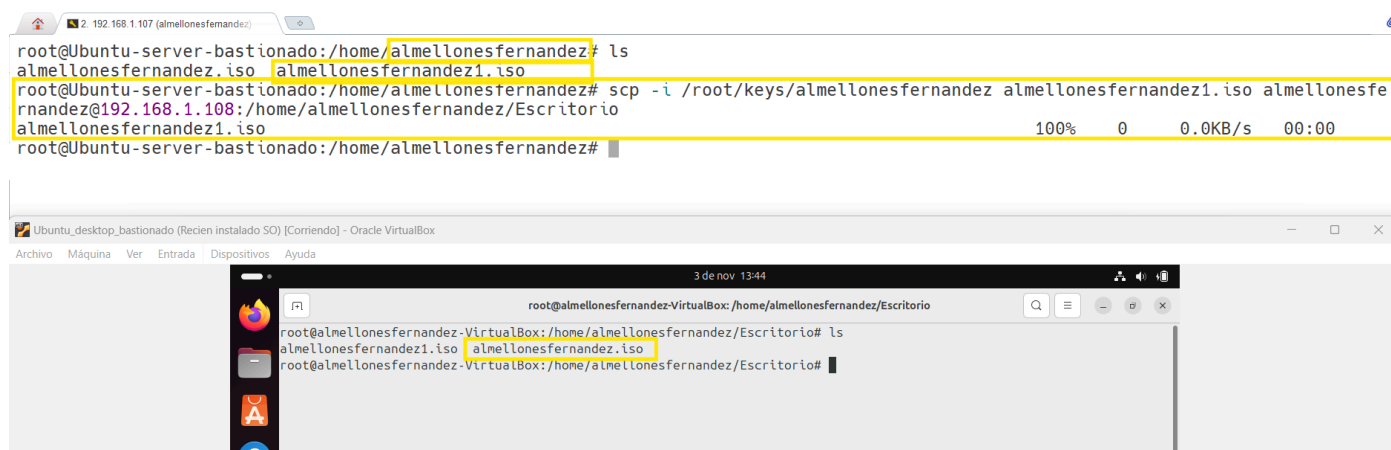
SACANDO PROVECHO A HERRAMIENTAS VARIAS RELACIONADAS CON CLIENTE SSH.

5. Realice las siguientes comprobaciones desde cliente SSH Ubuntu Desktop en modo comando conectándose al servidor SSHD de Ubuntu Server, usando **siempre** autenticación por cifrado asimétrico. (0,25 puntos cada uno)

a. Compruebe que puede copiar (*# scp -i llaveprivada*) un archivo desde un cliente al servidor (XXxx.iso).



b. Compruebe que puede copiar (*# scp -i llaveprivada*) un archivo desde el servidor al cliente (XX.xx 1.iso). Al revés, que en el ejercicio anterior.



c. Realice la actualización de fuentes, actualizar el S.O, instalar apache2 y reiniciar el servicio de apache2, sin tener que entrar al sistema operativo, usando un único comando (&&). Posteriormente, compruebe que puede conectarse al servidor web (<http://IP>, wget), para saber que ha tenido éxito

Álvaro Almellones Fernández

Estoy usando la terminal de ubuntu desktop(está marcada la ip de ubuntu desktop en la captura) desde moba para que se vea mejor y así me permite copiar y pegar los comandos .

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# ssh -i /root/miskeys/almellonesfernandez root@192.168.1.107 "sudo apt update && sudo apt upgrade -y && sudo apt install apache2 -y && sudo systemctl restart apache2"
```

Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida la conexión si no es Administrador de este sistema informático

Ubuntu 24.04.1 LTS

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

```
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [114 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [305 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7208 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:13 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:14 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
Get:15 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [21.2 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 880 kB in 3s (260 kB/s)
Reading package lists...
Building dependency tree...
Reading state information...
40 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# wget --spider http://192.168.1.107
Modo arácnido activado. Comprobar si el fichero remoto existe.
--2024-11-03 14:32:21-- http://192.168.1.107/
Conectando con 192.168.1.107:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 10671 (10K) [text/html]
El archivo remoto existe y podría contener vínculos adicionales,
pero la recursividad está desactivada -- no se recupera.

root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#
```

d. Compruebe que puede montar mediante sshfs el sistema de archivos completo del servidor Ubuntu Server. (`ls -al`, `ll`, y `df -ah`, `cat /etc/mtab`). Desmonte el sistema de archivo montado en el apartado anterior y vuelva a comprobar.

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# sudo apt update && sudo apt install sshfs -y
Obj:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:2 http://archive.ubuntu.com/ubuntu noble InRelease
Obj:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 51 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  sshfs
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 51 no actualizados.
Se necesita descargar 45,3 kB de archivos.
Se utilizarán 125 kB de espacio de disco adicional después de esta operación.
Des:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 sshfs amd64 3.7.3-1.1build3 [45,3 kB]
Descargados 45,3 kB en 0s (91,4 kB/s)
Seleccionando el paquete sshfs previamente no seleccionado.
(Leyendo la base de datos ... 151328 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../sshfs_3.7.3-1.1build3_amd64.deb ...
Desempaquetando sshfs (3.7.3-1.1build3) ...
Configurando sshfs (3.7.3-1.1build3) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez#

root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez# pwd
/root/mnt/servidor-almellonesfernandez
root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez# sshfs -o IdentityFile=/root/miskeys
/almellonesfernandez almellonesfernandez@192.168.1.107:/ ~/mnt/servidor-almellonesfernandez

root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez# echo "comprobacion de que se ha mon
tado el sistema de archivos: " && ls -al && ll && df -ah && cat /etc/mtab
comprobacion de que se ha montado el sistema de archivos:
total 8
drwxr-xr-x 2 root root 4096 nov  3 16:20 .
drwxr-xr-x 3 root root 4096 nov  3 16:20 ..
total 8
drwxr-xr-x 2 root root 4096 nov  3 16:20 ./
drwxr-xr-x 3 root root 4096 nov  3 16:20 ../
S.ficheros
Tamaño Usados  Disp  Uso%  Montado en
sysfs      0          0      0    -  /sys
proc        0          0      0    -  /proc
udev       1,8G        0    1,8G    0%  /dev
devpts      0          0      0    -  /dev/pts
tmpfs      373M       1,5M    372M    1%  /run
/dev/sda3   14G        7,6G    5,7G    58%  /
securityfs  0          0      0    -  /sys/kernel/security
tmpfs      1,9G        0    1,9G    0%  /dev/shm
tmpfs      5,0M        8,0K    5,0M    1%  /run/lock
cgroup2     0          0      0    -  /sys/fs/cgroup
pstore     0          0      0    -  /sys/fs/pstore
bpf         0          0      0    -  /sys/fs/bpf
systemd-1   -          -      -    -  /proc/sys/fs/binfmt_misc
hugetlbfs  0          0      0    -  /dev/hugepages
mqueue     0          0      0    -  /dev/mqueue
debugfs     0          0      0    -  /sys/kernel/debug
tracefs     0          0      0    -  /sys/kernel/tracing
configfs    0          0      0    -  /sys/kernel/config
fusectl     0          0      0    -  /sys/fs/fuse/connections
/dev/loop1  128K       128K    0  100%  /snap/bare/5
/dev/loop2  74M        74M    0  100%  /snap/core22/1663
/dev/loop0  75M        75M    0  100%  /snap/core22/1564
```

```
4. 192.168.1.107 (almellonesfernandez) 5. 192.168.1.108 (almellonesfernandez)
/dev/loop3 270M 270M 0 100% /snap/firefox/4793
/dev/loop4 11M 11M 0 100% /snap/firmware-updater/127
/dev/loop5 12M 12M 0 100% /snap/firmware-updater/147
/dev/loop7 92M 92M 0 100% /snap/gtk-common-themes/1535
/dev/loop6 506M 506M 0 100% /snap/gnome-42-2204/176
/dev/loop8 11M 11M 0 100% /snap/snap-store/1173
/dev/loop9 11M 11M 0 100% /snap/snap-store/1218
/dev/loop10 39M 39M 0 100% /snap/snapd/21759
/dev/loop11 512K 512K 0 100% /snap/snapd-desktop-integration/178
binfmt_misc 0 0 0 - /proc/sys/fs/binfmt_misc
tmpfs 373M 116K 373M 1% /run/user/1000
portal 0,0K 0,0K 0,0K - /run/user/1000/doc
tmpfs 373M 1,5M 372M 1% /run/snapd/ns
nsfs 0 0 0 - /run/snapd/ns/snapd-desktop-integration.mnt
gvfsd-fuse 0,0K 0,0K 0,0K - /run/user/1000/gvfs
almellonesfernandez@192.168.1.107:/ 25G 3,9G 20G 17% /root/mnt/servidor-almellonesfernandez
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,relatime,size=1872364k,nr_inodes=468091,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,noexec,relatime,size=381592k,mode=755,inode64 0 0
/dev/sda3 / ext4 rw,relatime 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev,inode64 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k,inode64 0 0
cgroup2 /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
bpf /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=32,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,p
ipe_ino=3183 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,nosuid,nodev,relatime,pagesize=2M 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
```

```
4. 192.168.1.107 (almellonesfernandez) 5. 192.168.1.108 (almellonesfernandez)
bpf /sys/fs/bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=32,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,p
ipe_ino=3183 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,nosuid,nodev,relatime,pagesize=2M 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,nosuid,nodev,noexec,relatime 0 0
tracefs /sys/kernel/tracing tracefs rw,nosuid,nodev,noexec,relatime 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
fusectl /sys/fs/fuse/connections fusectl rw,nosuid,nodev,noexec,relatime 0 0
/dev/loop1 /snap/bare/5 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop2 /snap/core22/1663 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop0 /snap/core22/1564 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop3 /snap/firefox/4793 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop4 /snap/firmware-updater/127 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop5 /snap/firmware-updater/147 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop7 /snap/gtk-common-themes/1535 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop6 /snap/gnome-42-2204/176 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop8 /snap/snap-store/1173 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop9 /snap/snap-store/1218 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop10 /snap/snapd/21759 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop11 /snap/snapd-desktop-integration/178 squashfs ro,nodev,relatime,errors=continue,threads=single 0
0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /run/user/1000 tmpfs rw,nosuid,nodev,relatime,size=381588k,nr_inodes=95397,mode=700,uid=1000,gid=1000
,inode64 0 0
portal /run/user/1000/doc fuse.portal rw,nosuid,nodev,relatime,user_id=1000,group_id=1000 0 0
tmpfs /run/snapd/ns tmpfs rw,nosuid,nodev,noexec,relatime,size=381592k,mode=755,inode64 0 0
nsfs /run/snapd/ns/snapd-desktop-integration.mnt nsfs rw 0 0
gvfsd-fuse /run/user/1000/gvfs fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=1000,group_id=1000 0 0
almellonesfernandez@192.168.1.107:/ /root/mnt/servidor-almellonesfernandez fuse.sshfs rw,nosuid,nodev,relat
ime,user_id=0,group_id=0 0
root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez#
```

Una vez ejecutados los comandos demandados para comprobar que se monta el sistema de ficheros del server procedemos a desmontarlo y volver a ejecutarlos para comprobar que se desmonta correctamente

```
4. 192.168.1.107 (almellonesfernandez) 5. 192.168.1.108 (almellonesfernandez)
root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez# cd ..
root@almellonesfernandez-VirtualBox:~/mnt# cd ..
root@almellonesfernandez-VirtualBox:~# cd ..
root@almellonesfernandez-VirtualBox:~# fusermount -u ~/mnt/servidor-almellonesfernandez
```

```
root@almellonesfernandez-VirtualBox:/# cd ~/mnt/servidor-almellonesfernandez
root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez# echo "comprobacion de que se ha des
comprobacion de que se ha desmontado el sistema de archivos:
total 8
drwxr-xr-x 2 root root 4096 nov  3 16:20 .
drwxr-xr-x 3 root root 4096 nov  3 16:20 ..
total 8
drwxr-xr-x 2 root root 4096 nov  3 16:20 ./
drwxr-xr-x 3 root root 4096 nov  3 16:20 ../
S.ficheros      Tamaño Usados  Disp Uso% Montado en
sysfs           0         0      0  - /sys
proc            0         0      0  - /proc
udev            1,8G      0  1,8G  0% /dev
devpts          0         0      0  - /dev/pts
tmpfs           373M      1,5M  372M  1% /run
/dev/sda3       14G      7 6G  5 9% /

/dev/loop0      75M      75M    0 100% /snap/core22/1564
/dev/loop3      270M     270M    0 100% /snap/firefox/4793
/dev/loop4       11M      11M    0 100% /snap/firmware-updater/127
/dev/loop5       12M      12M    0 100% /snap/firmware-updater/147
/dev/loop7       92M      92M    0 100% /snap/gtk-common-themes/1535
/dev/loop6      506M     506M    0 100% /snap/gnome-42-2204/176
/dev/loop8       11M      11M    0 100% /snap/snap-store/1173
/dev/loop9       11M      11M    0 100% /snap/snap-store/1218
/dev/loop10      39M      39M    0 100% /snap/snapd/21759
/dev/loop11     512K     512K    0 100% /snap/snapd-desktop-integration/178
binfmt_misc      0         0      0  - /proc/sys/fs/binfmt_misc
tmpfs           373M     116K  373M  1% /run/user/1000
portal          0,0K     0,0K    0,0K  - /run/user/1000/doc
tmpfs           373M     1,5M  372M  1% /run/snapd/ns
nsfs            0         0      0  - /run/snapd/ns/snapd-desktop-integration.mnt
gvfsd-fuse       0,0K     0,0K    0,0K  - /run/user/1000/gvfs
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,nosuid,relatime,size=1872364k,nr_inodes=468091,mode=755,inode64 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,noexec,relatime,size=381592k,mode=755,inode64 0 0
/dev/sda3 / ext4 rw,relatime 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
cgroup2 /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
bpfs /sys/fs/bpfs bpfs rw,nosuid,nodev,noexec,relatime,mode=700 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=32,prgrp=1,timeout=0,minproto=5,maxproto=5,direct,po
tpe_ino=3183 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,nosuid,nodev,relatime,pagesize=2M 0 0
mqueue /dev/mqueue mqueue rw,nosuid,nodev,noexec,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,nosuid,nodev,noexec,relatime 0 0
tracefs /sys/kernel/tracing tracefs rw,nosuid,nodev,noexec,relatime 0 0
configfs /sys/kernel/config configfs rw,nosuid,nodev,noexec,relatime 0 0
fusectl /sys/fs/fuse/connections fusectl rw,nosuid,nodev,noexec,relatime 0 0
/dev/loop1 /snap/bare/5 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop2 /snap/core22/1663 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop0 /snap/core22/1564 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop3 /snap/firefox/4793 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop4 /snap/firmware-updater/127 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop5 /snap/firmware-updater/147 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop7 /snap/gtk-common-themes/1535 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop6 /snap/gnome-42-2204/176 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop8 /snap/snap-store/1173 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop9 /snap/snap-store/1218 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop10 /snap/snapd/21759 squashfs ro,nodev,relatime,errors=continue,threads=single 0 0
/dev/loop11 /snap/snapd-desktop-integration/178 squashfs ro,nodev,relatime,errors=continue,threads=single 0
0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /run/user/1000 tmpfs rw,nosuid,nodev,relatime,size=381588k,nr_inodes=95397,mode=700,uid=1000,gid=1000
,inode64 0 0
portal /run/user/1000/doc fuse.portal rw,nosuid,nodev,relatime,user_id=1000,group_id=1000 0 0
tmpfs /run/snapd/ns tmpfs rw,nosuid,nodev,noexec,relatime,size=381592k,mode=755,inode64 0 0
nsfs /run/snapd/ns/snapd-desktop-integration.mnt nsfs rw 0 0
gvfsd-fuse /run/user/1000/gvfs fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=1000,group_id=1000 0 0
root@almellonesfernandez-VirtualBox:~/mnt/servidor-almellonesfernandez#
```

Ya no aparece el sistema de ficheros porque lo hemos desmontado correctamente

PROBANDO TODO LO APRENDIDO CON HERRAMIENTAS DE SSH. AUTOMATIZACIÓN DE TAREAS (DEMONIO CROND). ATACANDO A MUCHOS EQUIPOS A LA VEZ.

6. Realice un script de Linux (/root/Bucle/XXxx-SSH.sh) que se ejecute en un S.O. Linux (por ejemplo, Ubuntu Desktop) que gestione como **mínimo** dos servidores (Ubuntu Server y crear otro S.O. para esta práctica) y que usando **siempre** autenticación por cifrado asimétrico (NO CONTRASEÑA) y usando un fichero de texto ipXXxx.txt, realice las siguientes tareas: **(0,25 puntos cada apartado)**

Video no realizado porque no me iba a dar tiempo realizar la entrega antes de la hora límite

```
5. 192.168.1.108 (almellonesfernandez)
root@almellonesfernandez-VirtualBox:~/bucle# ls
almellonesfernandez-SSH.sh ipalmellonesfernandez.txt
root@almellonesfernandez-VirtualBox:~/bucle# cat ipalmellonesfernandez.txt
192.168.1.107:aalmfer2001@g.educaand.es:ubuntu-server-bastionado1
192.168.1.109:aalmfer2001@g.educaand.es:ubuntu-server-bastionado2
```

```
GNU nano 7.2 almallonesfernandez-SSH.sh
# Archivo que contiene IPs y correos de los servidores
IP_FILE="ipalmellonesfernandez.txt"
# Clave privada SSH para autenticación
KEY="/root/miskeyes/almellonesfernandez"
# Archivo temporal para registro de la salida
LOG_FILE="/root/scripts/ssh_operationsalmellonesfernandez.log"

echo "creo las variables"

# Generación de claves SSH temporales para autenticación
TEMP_KEY="/root/.ssh/id_rsa_temp"

# Eliminar claves temporales por si no funciona el bucle
rm -f "$TEMP_KEY" "$TEMP_KEY.pub"

#ssh-keygen -t rsa -b 2048 -f "$TEMP_KEY" -N "" > /dev/null

echo "creo las key temporales"

# Bucle para cada línea en IPs.txt
for linea in $(cat $IP_FILE); do
    # Extracción de datos de cada línea
    IP=$(echo $linea | cut -d: -f1)
    correo=$(echo $linea | cut -d: -f2)
    nombre=$(echo $linea | cut -d: -f3)

    echo "Conectando con el servidor $nombre en la IP $IP"
    echo "----- almallonesfernandez -----" >> "$LOG_FILE"
done
```

rm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

a. Actualizará fuentes, actualizará los S.O y mostrará los dos últimos usuarios (/etc/passwd) que se han creados en ese S.O.

Álvaro Almellones Fernández

```
# a. Actualización del sistema y obtención de los dos últimos usuarios creados
ssh -o StrictHostKeyChecking=no -i "$KEY" root@"$IP" "
  apt update && apt upgrade -y;
  tail -n 2 /etc/passwd
">> "$LOG_FILE" 2>&1
```

b. Comprobará el tamaño de disco duro libre (únicamente del disco duro raíz, no otros) que tiene y la memoria RAM que está usando actualmente.

```
# b. Comprobar espacio libre en disco y memoria RAM
ssh -o StrictHostKeyChecking=no -i "$KEY" root@"$IP" "
  df -h / | grep -v 'Filesystem' | awk '{print \"Espacio libre en disco raíz:\", \"$4}';
  free -h | grep 'Mem:' | awk '{print \"Memoria RAM usada:\", \"$3 \" / \" \"$2}'
">> "$LOG_FILE" 2>&1
```

c. Copiará (#scp ...) desde el equipo que se ejecuta el script un fichero (por ejemplo, este mismo script) a esos S.O remotos.

```
# c. Copiar archivo local al servidor remoto
scp -o StrictHostKeyChecking=no -i "$KEY" /root/scripts/backup.txt root@"$IP":/root/backup.txt >> "$LOG_FILE" 2>&1
echo "Archivo backup.txt copiado correctamente al servidor $nombre." >> "$LOG_FILE"
```

```
root@almellonesfernandez-VirtualBox:~/scripts# ls
auth_192.168.1.107.log auth_192.168.1.109.log backup.txt ubuntu-server-bastionado1 ubuntu-server-bastionado2
root@almellonesfernandez-VirtualBox:~/scripts# cd ubuntu-server-bastionado1
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado1# ls
backup.txt keys scripts vboxpostinstall.sh
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado1# cd ..
root@almellonesfernandez-VirtualBox:~/scripts# cd ubuntu-server-bastionado2
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado2# ls
backup.txt keys scripts vboxpostinstall.sh
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado2#
```

d. Copiará (#scp) el fichero /var/log/auth de esos S.O. remotos a este S.O. (para que no machaque unos con otros hay que cambiar authIP.log)

```
# d. Copiar el archivo de autenticación del servidor remoto al equipo local
scp -o StrictHostKeyChecking=no -i "$KEY" root@"$IP":/var/log/auth.log "/root/scripts/auth_${IP}.log" >> "$LOG_FILE" 2>&1
```

```
root@almellonesfernandez-VirtualBox:~/scripts# ls
auth_192.168.1.107.log auth_192.168.1.109.log backup.txt ubuntu-server-bastionado1 ubuntu-server-bastionado2
root@almellonesfernandez-VirtualBox:~/scripts#
```

e. Montará (#sshfs) el directorio /root de cada uno de los S.O. remotos en el equipo que se ejecuta el script. Hay que crear el directorio con la IP (#mkdir 2>/dev/null) donde se montará dicho directorio remoto.

```
# e. Montar el directorio /root de cada servidor remoto en un directorio local
mkdir -p "/root/scripts/$nombre"
sshfs -o IdentityFile="$KEY" root@"$IP":/root "/root/scripts/$nombre" >> "$LOG_FILE" 2>&1
```

```
root@almellonesfernandez-VirtualBox:~/scripts# ls
auth_192.168.1.107.log auth_192.168.1.109.log backup.txt ubuntu-server-bastionado1 ubuntu-server-bastionado2
root@almellonesfernandez-VirtualBox:~/scripts# cd ubuntu-server-bastionado1
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado1# ls
backup.txt keys scripts vboxpostinstall.sh
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado1# cd ..
root@almellonesfernandez-VirtualBox:~/scripts# cd ubuntu-server-bastionado2
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado2# ls
backup.txt keys scripts vboxpostinstall.sh
root@almellonesfernandez-VirtualBox:~/scripts/ubuntu-server-bastionado2#
```

Álvaro Almellones Fernández

f. Cambiará una opción del fichero de configuración del servidor apache de los S.O. (por ejemplo, cambiar el puerto de escucha, reiniciar el sistema y comprobar que funciona en el nuevo puerto) (# sed XXXXXX).

```
# f. Cambiar el puerto del servidor Apache y reiniciar el servicio
ssh -o StrictHostKeyChecking=no -i "$KEY" root@"$IP" "
sed -i 's/^Listen 80$/Listen 8080/' /etc/apache2/ports.conf;
systemctl restart apache2;
systemctl status apache2 | grep 'active (running)'
">> "$LOG_FILE" 2>&1
```

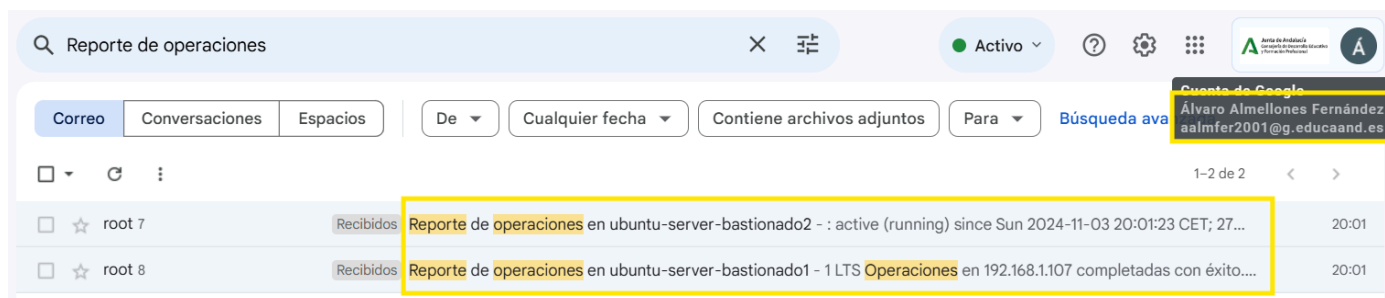
g. Como medida de seguridad adicional, cada vez que se ejecute este script se generará un par de keys/llaves (privada/pública) nuevas e incluirá la llave pública generada en el fichero authorized_keys de S.O. remoto (#ssh-id-copy....). Realice una nueva prueba para comprobar que se puede autenticar con la **nueva** llave privada generada.

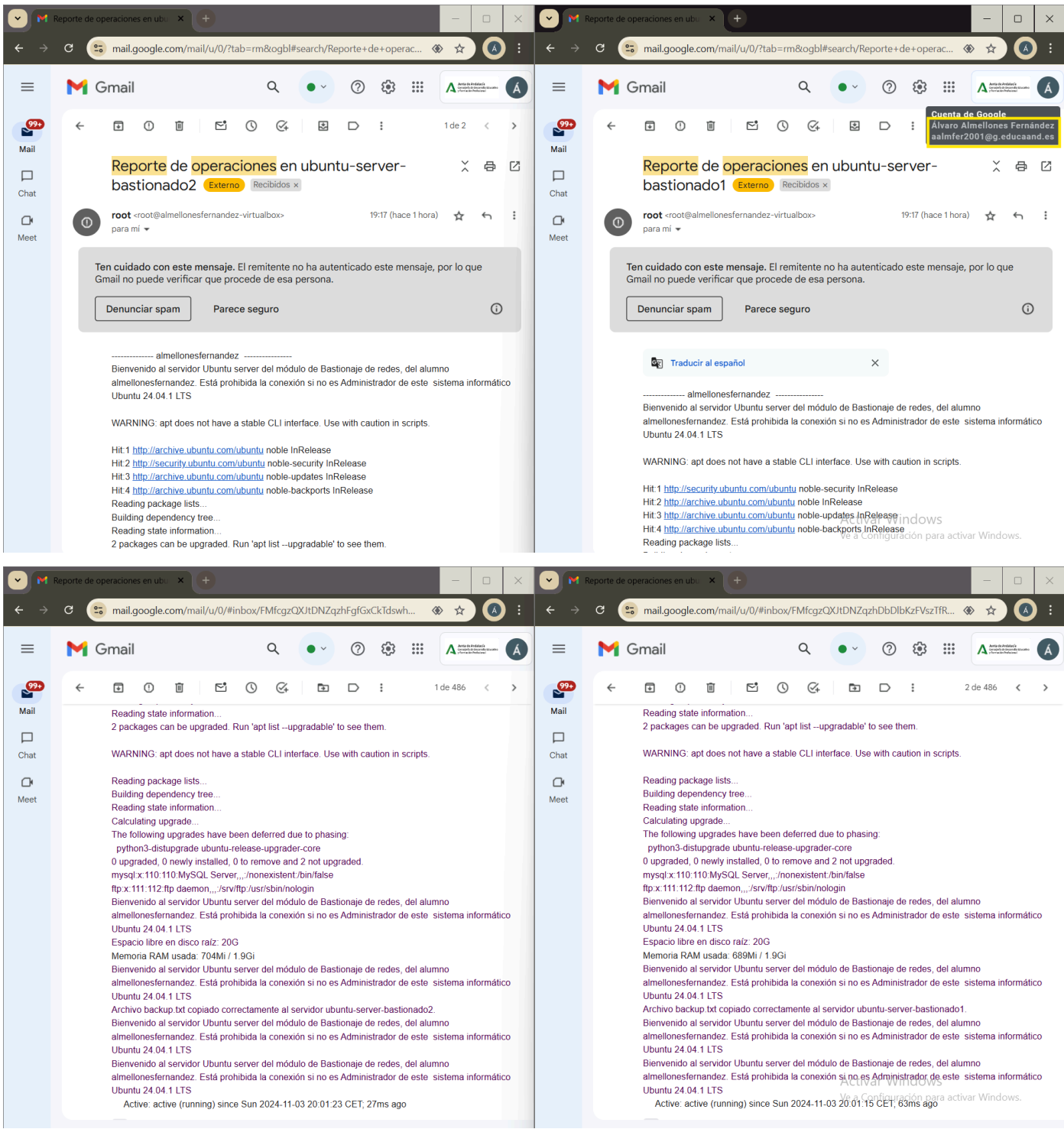
No he conseguido que me funcione

h. Enviará un mensaje de correo electrónico (estará en el fichero ipXXxx.txt) con lo que se ha realizado correctamente y con lo que no ha funcionado.

```
# h. Enviar un correo electrónico con el log de resultados
cat "$LOG_FILE" | mailx -s "Reporte de operaciones en $nombre" "$correo"

# Limpiar el log temporal antes de la próxima iteración
> "$LOG_FILE"
```





Se tendrá en cuenta para la nota de este ejercicio:

- Uso técnico en la explicación del script y Calidad del video explicativo (0,5 puntos)
- Claridad en el diseño del script, uso de variables, uso de mensajes

clarificadores, etc. Este ejercicio se corregirá montando un video (NO

grabado con móvil, use Canta) donde:

- El video tendrá **máximo 5 minutos** de grabación y el alumno debe explicar (tiene que escucharse) todas las comprobaciones que realiza el script.
- Aparezcan varios terminales donde se demuestre los resultados y comprobaciones. • Existen algunos “echo” en el script para explicar que se está realizando o que no se ha realizado.
- Introducir paradas (sleep) para que dé tiempo a ir explicando correctamente lo que va realizando. Hacer lo más personal (XXxx, etc.) posible el script.
- **En ningún momento** puede solicitar por pantalla al usuario, ya que supuestamente este script se ejecutará sin intervención de un usuario.
- Se debe intentar que las comprobaciones sean hechas en el mismo script, por ejemplo, cuando se monta por sshfs, que aparezca el df del servidor remoto, etc., haciendo uso de && y ||.