

Universidad Autónoma de Baja California



Facultad de Ciencias Químicas e Ingeniería

GESTIÓN Y SEGURIDAD EN REDES

Meta 3.4

SERVICIO SSH

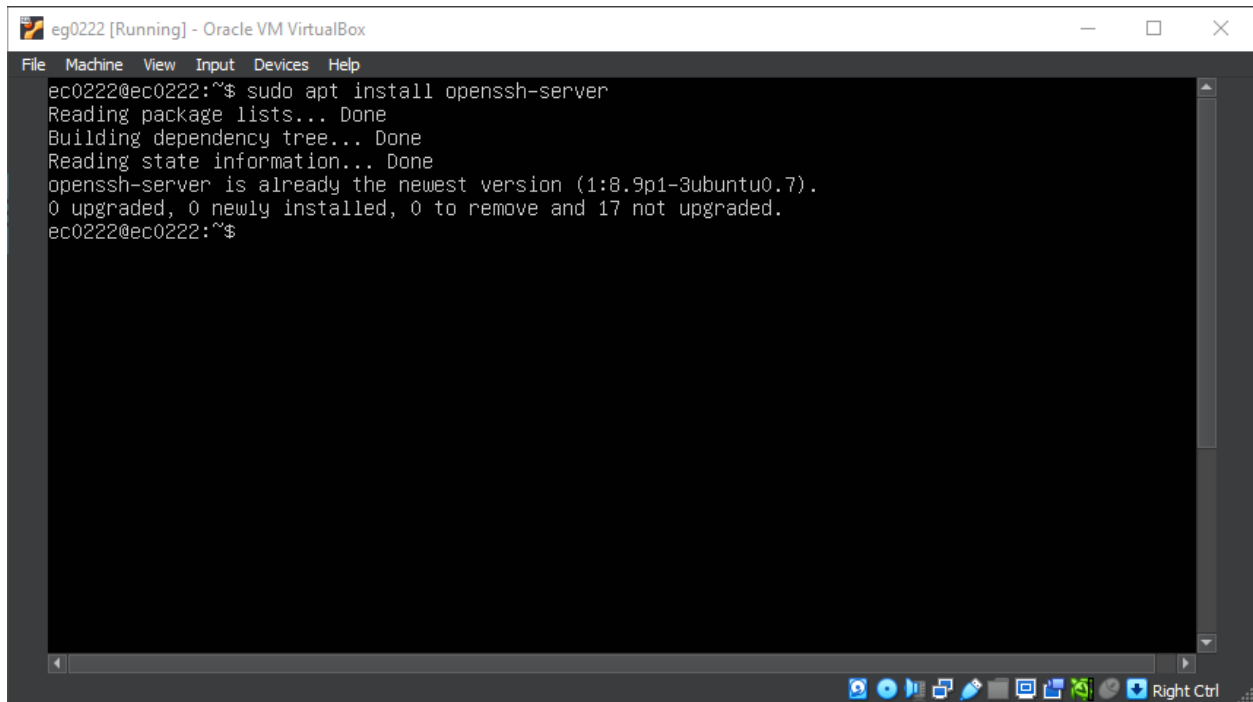
Docente: ALVAREZ SALGADO, CARLOS FRANCISCO

Alumno: Gómez Cárdenas, Emmanuel Alberto

Matricula: 01261509

Instalar SSH para servidor

Al instalar Ubuntu server openssh para servidor ya venía incluido.



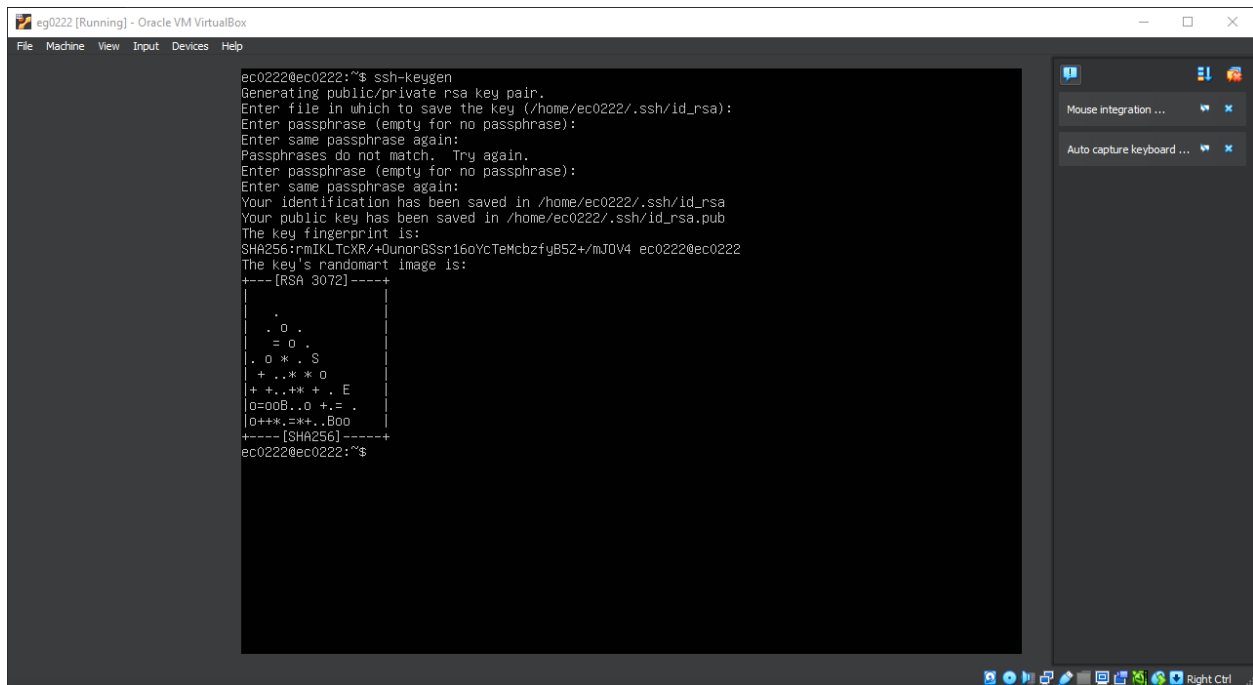
The screenshot shows a terminal window titled "eg0222 [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
ec0222@ec0222:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.7).
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
ec0222@ec0222:~$
```

Abriendo el puerto SSH

```
ec0222@ec0222:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
ec0222@ec0222:~$ _
```

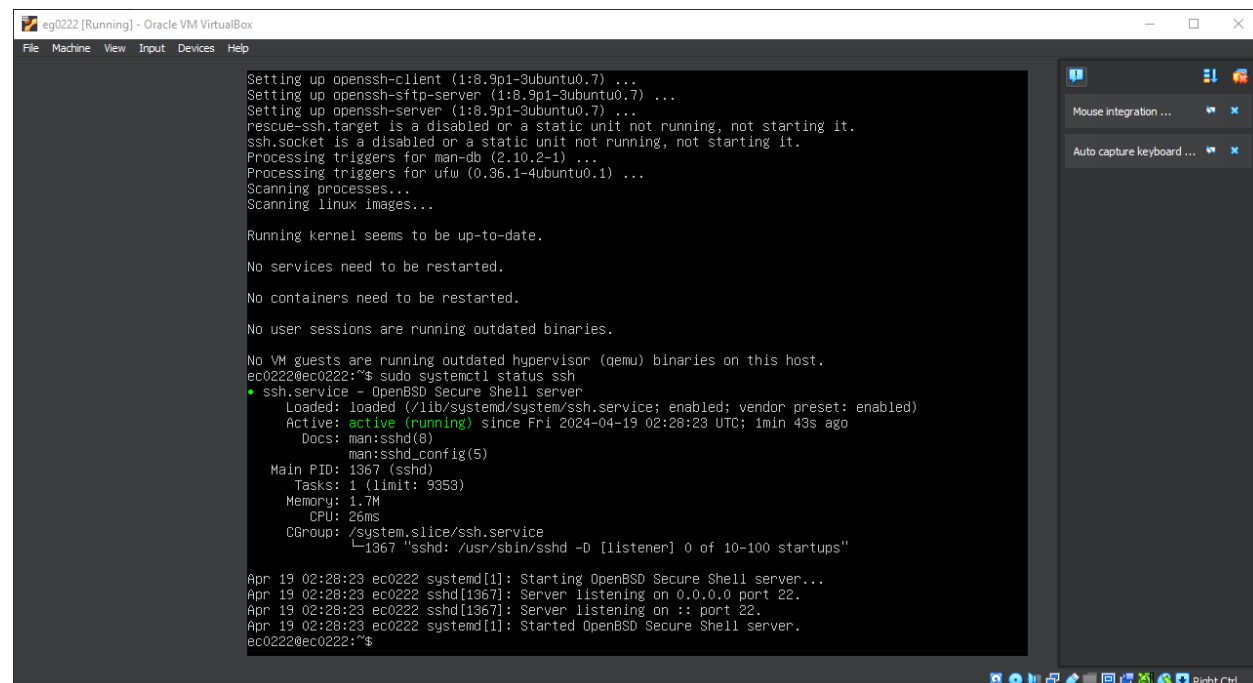
Crear un nuevo par de claves SSH



```
eg0222 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

ec0222@ec0222:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ec0222/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Passphrases do not match. Try again.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ec0222/.ssh/id_rsa
Your public key has been saved in /home/ec0222/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:rmIKLTcXR/+0unorBSSr16oYcTeMcbzfYB5Z+/mJ0V4 ec0222@ec0222
The key's randomart image is:
+---[RSA 3072]-----+
|
| . O .
| = O .
| . O * . S
| + . * * O
| + + . * * + . E
| O = O B . O + . = .
| O + * . = * + . B o o
+---[SHA256]-----+
ec0222@ec0222:~$
```

Comprobando si esta corriendo



```
eg0222 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Setting up openssh-client (1:8.9p1-3ubuntu0.7) ...
Setting up openssh-sftp-server (1:8.9p1-3ubuntu0.7) ...
Setting up openssh-server (1:8.9p1-3ubuntu0.7) ...
rescue-ssh.target is a disabled or a static unit not running, not starting it.
ssh.socket is a disabled or a static unit not running, not starting it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ec0222@ec0222:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-04-19 02:28:23 UTC; 1min 43s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1367 (sshd)
     Tasks: 1 (limit: 9353)
    Memory: 1.7M
       CPU: 26ms
   CGroup: /system.slice/ssh.service
           └─1367 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 19 02:28:23 ec0222 systemd[1]: Starting OpenBSD Secure Shell server...
Apr 19 02:28:23 ec0222 sshd[1367]: Server listening on 0.0.0.0 port 22.
Apr 19 02:28:23 ec0222 sshd[1367]: Server listening on :: port 22.
Apr 19 02:28:23 ec0222 systemd[1]: Started OpenBSD Secure Shell server.
ec0222@ec0222:~$
```

19/04/2024


GESTIÓN Y SEGURIDAD EN REDES

Gómez Cárdenas Emmanuel Alberto

INGENIERÍA EN COMPUTACIÓN

Instalar SSH-Client en windows

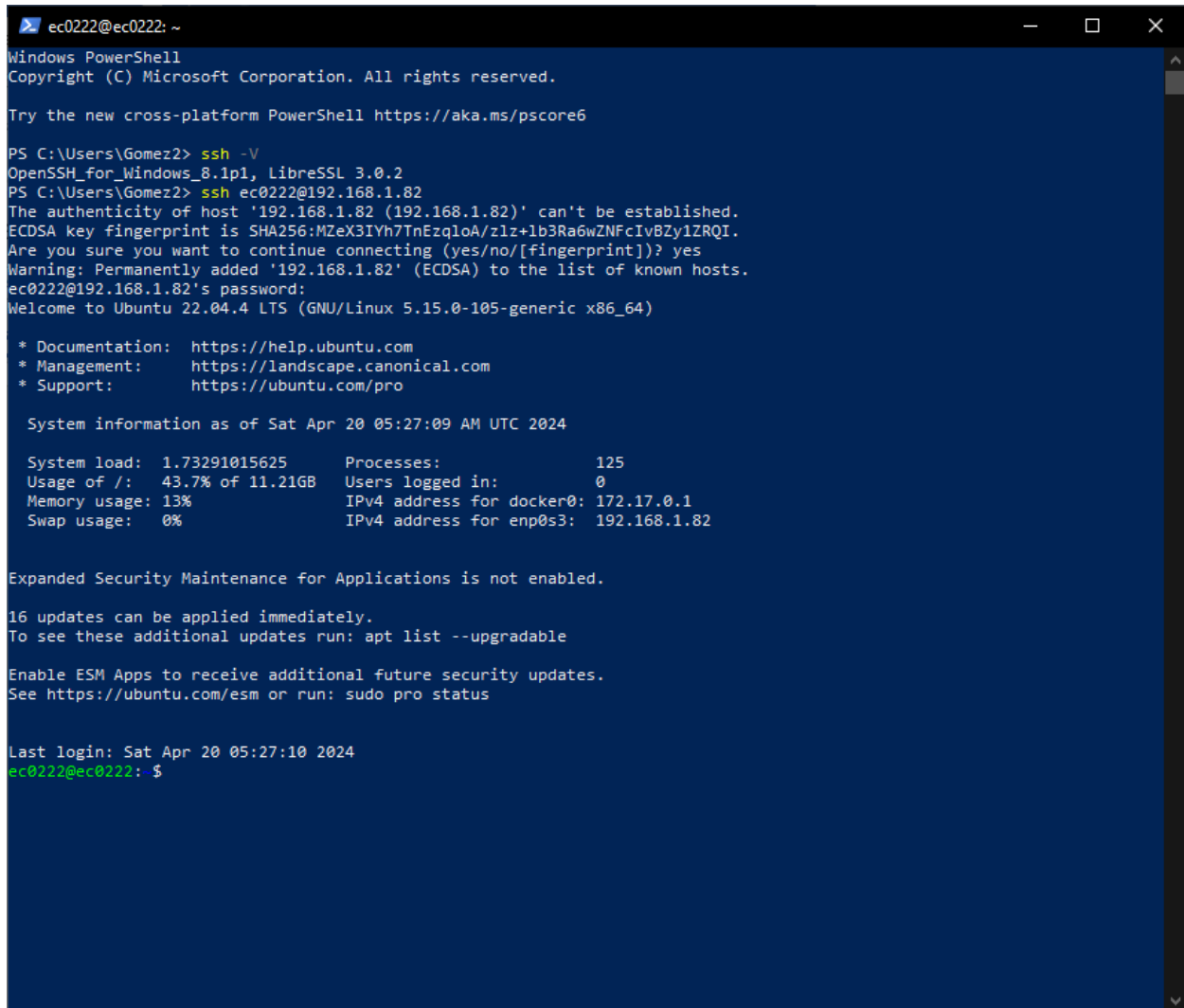
En mi caso, el cliente SSH también estaba instalado



```
Windows PowerShell
PS C:\Users\Gomez2> ssh -V
OpenSSH_for_Windows_8.1p1, LibreSSL 3.0.2
PS C:\Users\Gomez2>
```

Conectarse al servidor desde el cliente

Al ser la primera vez que me conecto me dará un aviso



```
ec0222@ec0222: ~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Gomez2> ssh -V
OpenSSH_for_Windows_8.1p1, LibreSSL 3.0.2
PS C:\Users\Gomez2> ssh ec0222@192.168.1.82
The authenticity of host '192.168.1.82 (192.168.1.82)' can't be established.
ECDSA key fingerprint is SHA256:MZeX3IYh7TnEzql0A/z1z+1b3Ra6wZNfcIv8Zy1ZRQI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.82' (ECDSA) to the list of known hosts.
ec0222@192.168.1.82's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-105-generic x86_64)

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

System information as of Sat Apr 20 05:27:09 AM UTC 2024

System load:  1.73291015625      Processes:           125
Usage of /:   43.7% of 11.21GB   Users logged in:    0
Memory usage: 13%              IPv4 address for docker0: 172.17.0.1
Swap usage:   0%                IPv4 address for enp0s3: 192.168.1.82

Expanded Security Maintenance for Applications is not enabled.

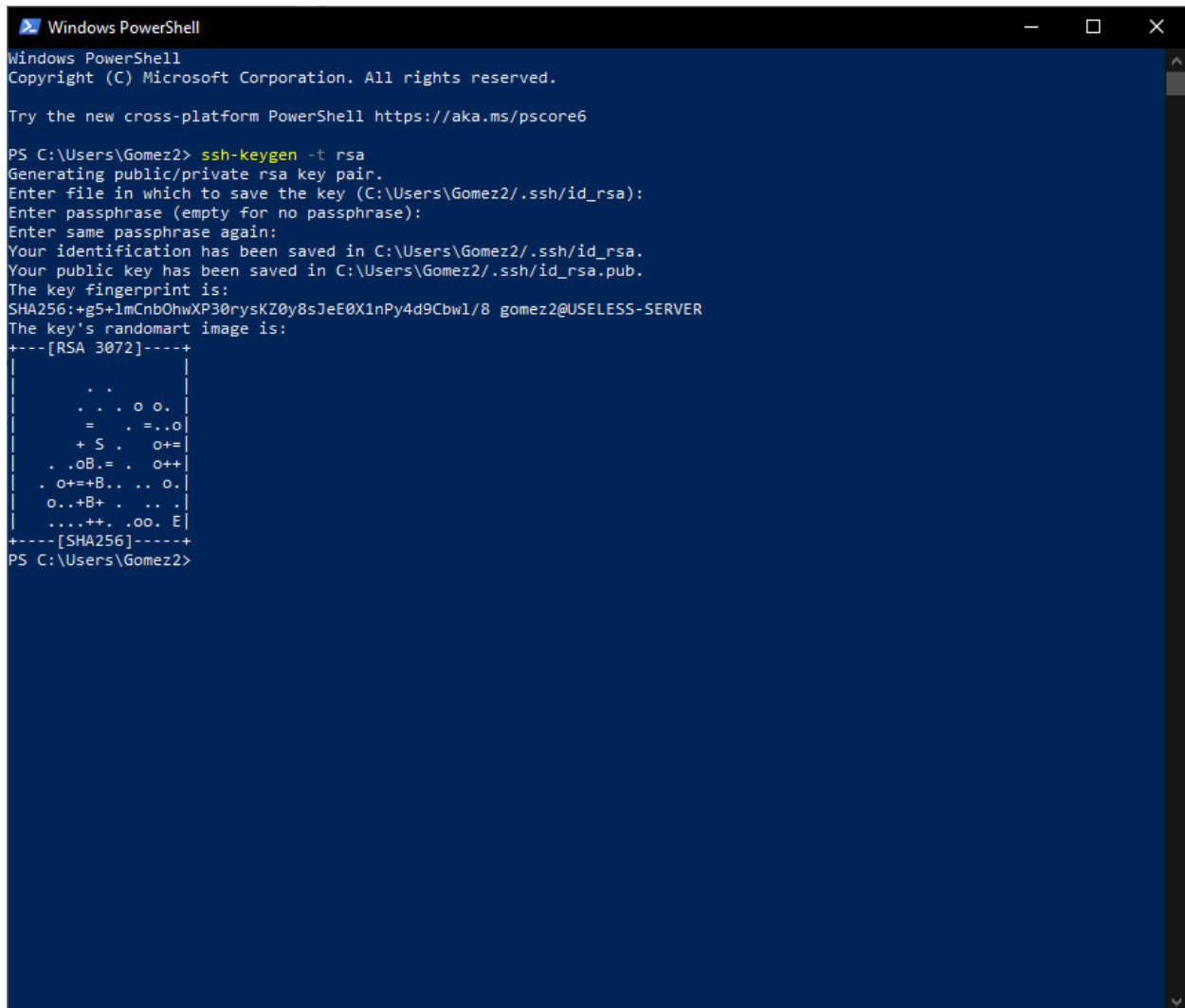
16 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Last login: Sat Apr 20 05:27:10 2024
ec0222@ec0222: $
```

PARTE 2 – Conectarse con el uso de llaves

Generar las llaves



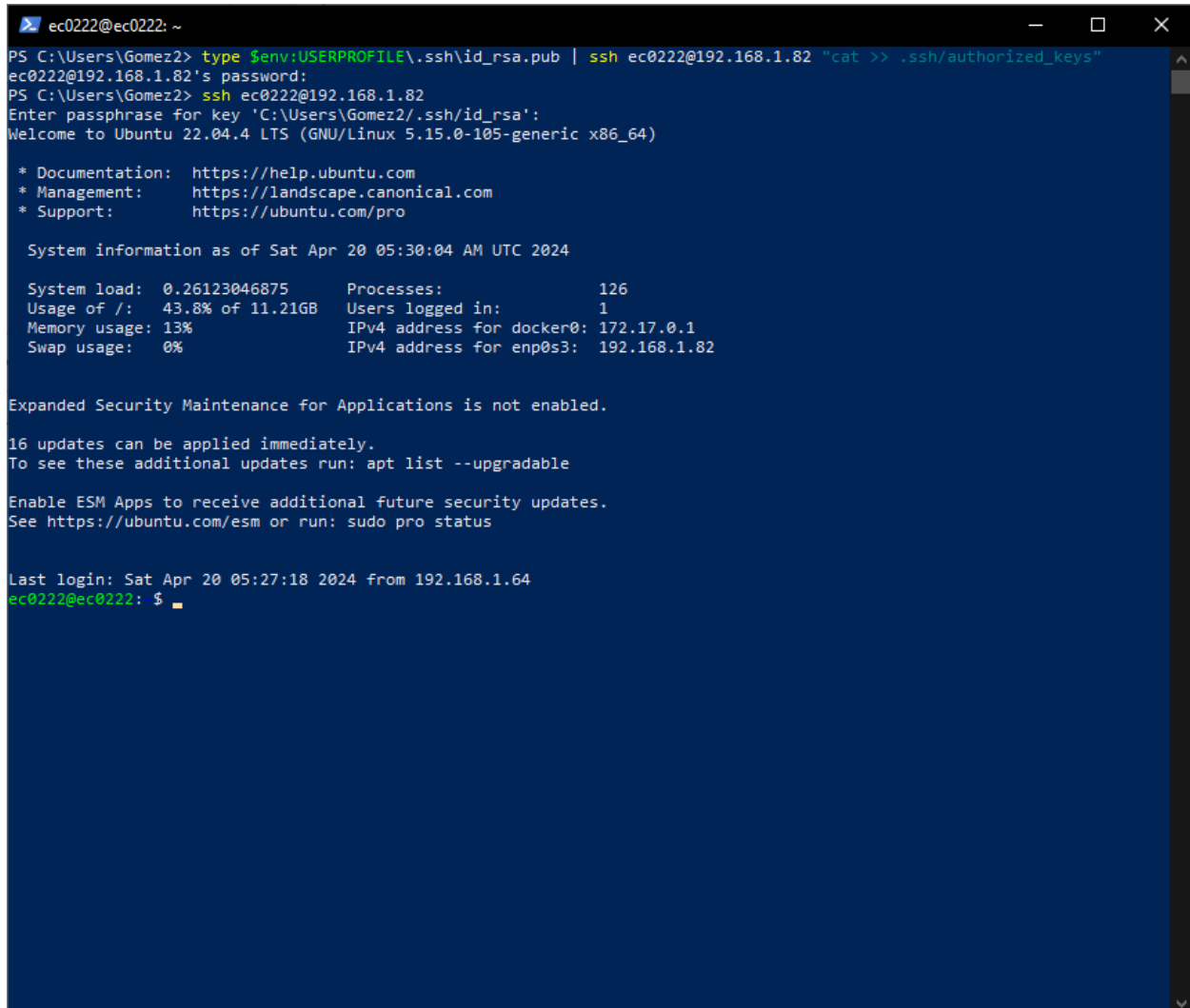
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Gomez2> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Gomez2\.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Gomez2\.ssh/id_rsa.
Your public key has been saved in C:\Users\Gomez2\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:+g5+lmCnb0hwXP30ryskZ0y8sJeE0X1nPy4d9Cbwl/8 gomez2@USELESS-SERVER
The key's randomart image is:
+----[RSA 3072]-----+
|
|   .
|  . . o o
| = . =..o
| + S . o+=
| . .oB.= . o++
| . o+=+B.. .. o.
| o..+B+ . .. .
| .....+. .oo. E
+-----[SHA256]-----+
PS C:\Users\Gomez2>
```

Copiar llaves del servidor

Ahora cada que me quiera conectar solo me pedirá la passphrase de la llave en vez de la contraseña del servidor

A terminal window titled 'ec0222@ec0222: ~' showing a Windows command prompt session. The user runs 'type \$env:USERPROFILE\.ssh\id_rsa.pub | ssh ec0222@192.168.1.82 "cat >> .ssh/authorized_keys"', which successfully copies the public key to the server. The terminal then shows the SSH login process, including the passphrase prompt and the Ubuntu 22.04.4 LTS welcome message. System information is displayed, showing system load, memory usage, and network addresses. A security update notification is also visible.

```
ec0222@ec0222: ~
PS C:\Users\Gomez2> type $env:USERPROFILE\.ssh\id_rsa.pub | ssh ec0222@192.168.1.82 "cat >> .ssh/authorized_keys"
ec0222@192.168.1.82's password:
PS C:\Users\Gomez2> ssh ec0222@192.168.1.82
Enter passphrase for key 'C:\Users\Gomez2\.ssh\id_rsa':
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-105-generic x86_64)

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

System information as of Sat Apr 20 05:30:04 AM UTC 2024

System load:  0.26123046875   Processes:            126
Usage of /:   43.8% of 11.21GB Users logged in:          1
Memory usage: 13%           IPv4 address for docker0: 172.17.0.1
Swap usage:   0%             IPv4 address for enp0s3:  192.168.1.82

Expanded Security Maintenance for Applications is not enabled.

16 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: Sat Apr 20 05:27:18 2024 from 192.168.1.64
ec0222@ec0222: $
```

Conclusión:

SSH es una herramienta muy importante ya que permite la conexión cifrada entre el servidor y un cliente dando posibilidad de un medio seguro para la autenticación, la comunicación y la transferencia de datos.