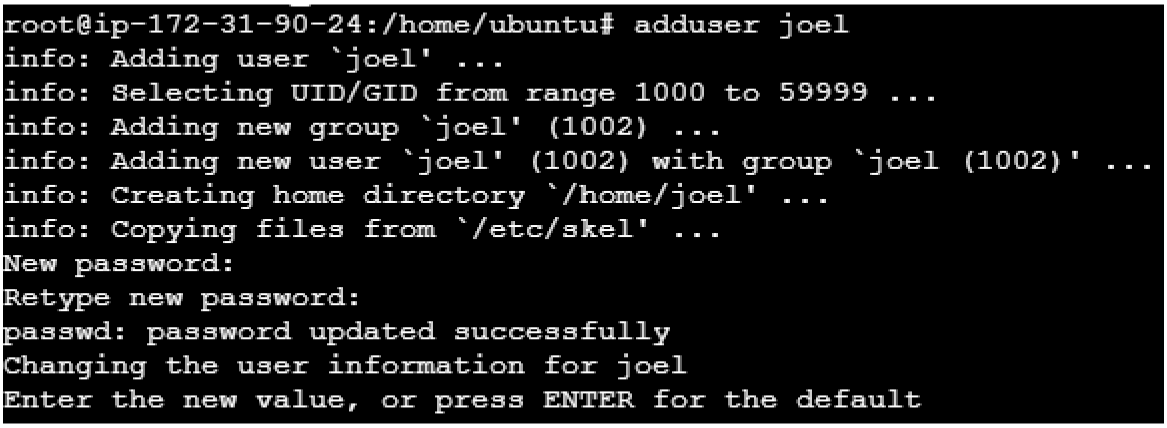
PROJECTE M12 LINKEDIN

Configuració servidor SSH 2
Fitxer de configuració SSH 2
fail2ban 3
Instal·lem fail2ban 3
Funcionament de la regla 4
RMIAS DEL SERVIDOR 4
CLIENT 5
figurem la connexió al client 5
comprovem si hi ha connexió per SSH 5
Generem dos claus rsa al client s'ha generat una keys pública que serà per al servidor i una keys privada 6
Per via SSH enviarem la nostra clau publica al servidor per poder entrar sense contraseña 6

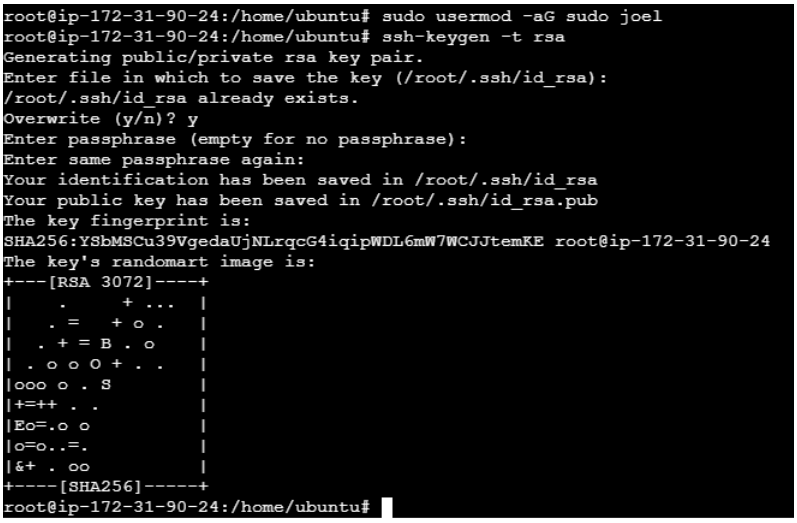
Configuració servidor SSH

creació d’usuari SSH



```
root@ip-172-31-90-24:/home/ubuntu# adduser joel
info: Adding user `joel' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `joel' (1002) ...
info: Adding new user `joel' (1002) with group `joel (1002)' ...
info: Creating home directory `/home/joel' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for joel
Enter the new value, or press ENTER for the default
```

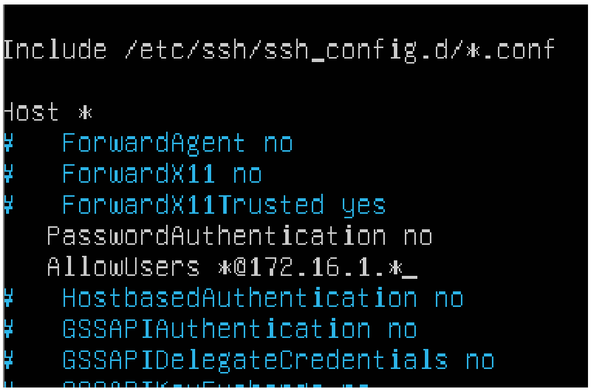
Generem claus rsa



```
root@ip-172-31-90-24:/home/ubuntu# sudo usermod -aG sudo joel
root@ip-172-31-90-24:/home/ubuntu# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:YSbMSCu39VgedaUjNLrqcG4iqipWDL6mW7WCJJtemKE root@ip-172-31-90-24
The key's randomart image is:
+---[RSA 3072]----+
|    .     + ...  |
|   . =   + o .   |
|  . + = B . o    |
| . o o O + . .   |
|ooo o . S        |
|+=++ . .         |
|Eo=.o o          |
|o=o..=.          |
|&+ . oo          |
+----[SHA256]-----+
root@ip-172-31-90-24:/home/ubuntu#
```

Fitxer de configuració SSH

Deshabilitarem la connexió per contrasenya solament per claus i solament es podran connectar els usuaris del mateix rang IP

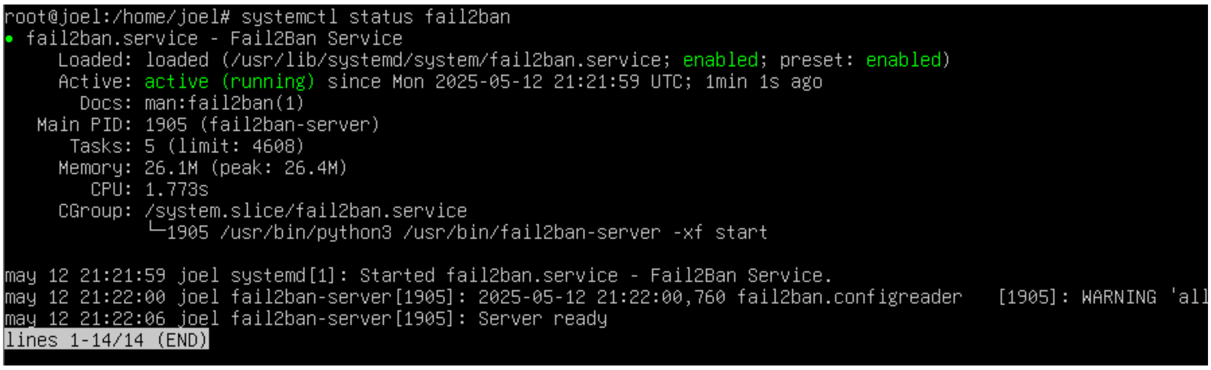


```
Include /etc/ssh/ssh_config.d/*.conf

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
    PasswordAuthentication no
    AllowUsers *@172.16.1.*_
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
```

fail2ban

“Fail2ban és una eina que se sol utilitzar contra atacs de força bruta al servidor Linux bloquejant IP de manera temporal o permanent”.

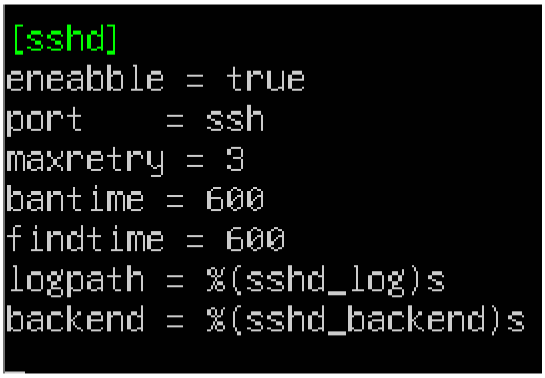
Instal·lem fail2ban



```
root@joel:/home/joel# systemctl status fail2ban
• fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-05-12 21:21:59 UTC; 1min 1s ago
       Docs: man:fail2ban(1)
   Main PID: 1905 (fail2ban-server)
      Tasks: 5 (limit: 4608)
     Memory: 26.1M (peak: 26.4M)
        CPU: 1.773s
     CGroup: /system.slice/fail2ban.service
             └─1905 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

may 12 21:21:59 joel systemd[1]: Started fail2ban.service - Fail2Ban Service.
may 12 21:22:00 joel fail2ban-server[1905]: 2025-05-12 21:22:00,760 fail2ban.configreader   [1905]: WARNING 'all
may 12 21:22:06 joel fail2ban-server[1905]: Server ready
lines 1-14/14 (END)
```

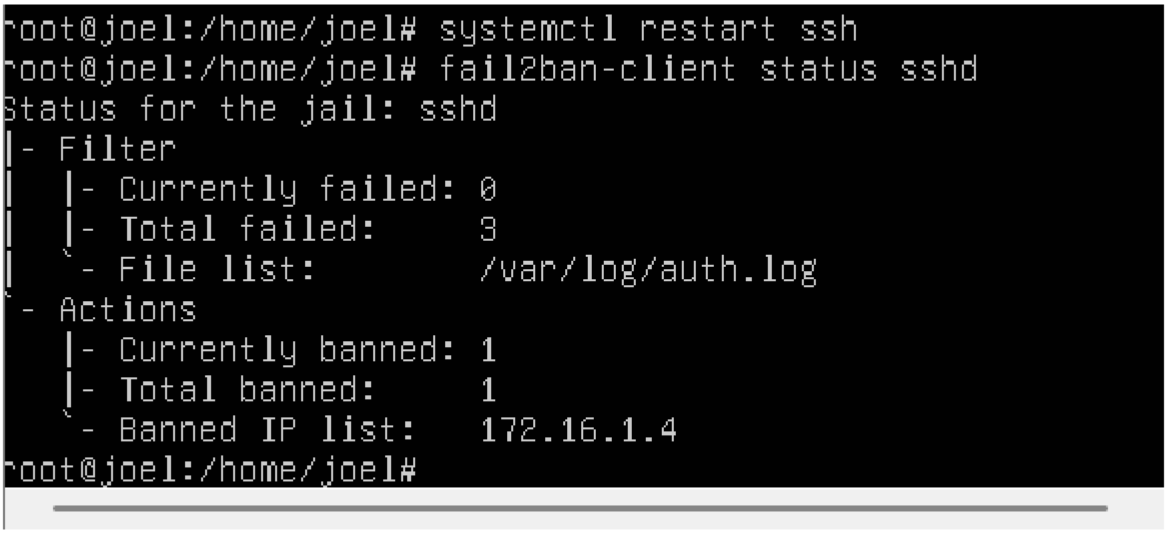
Nosaltres farem servir l’eina per millorar la seguretat per SSH

amb aquesta informació si un usuari falla tres intents de connexió estarà vetat 10 minuts del servidor.

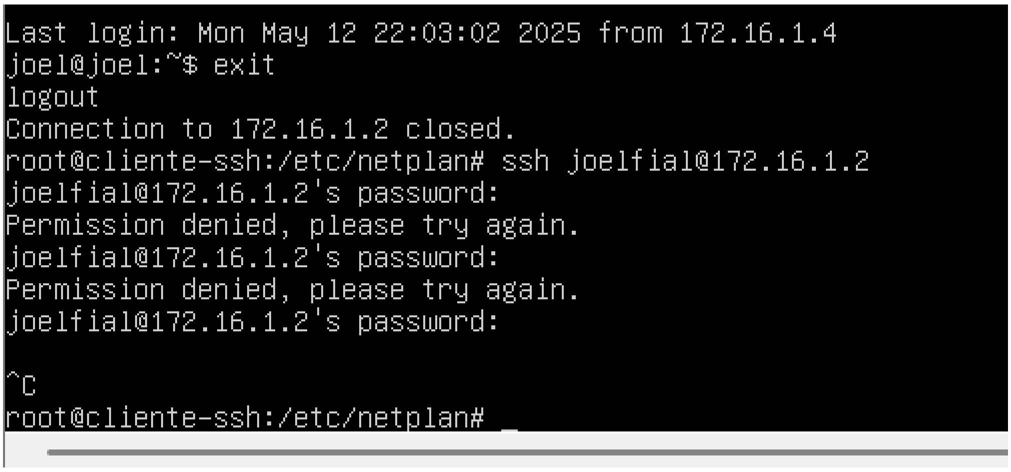


```
[sshd]
eneabble = true
port     = ssh
maxretry = 3
bantime = 600
findtime = 600
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Funcionament de la regla



```
root@joel:/home/joel# systemctl restart ssh
root@joel:/home/joel# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   172.16.1.4
root@joel:/home/joel#
```

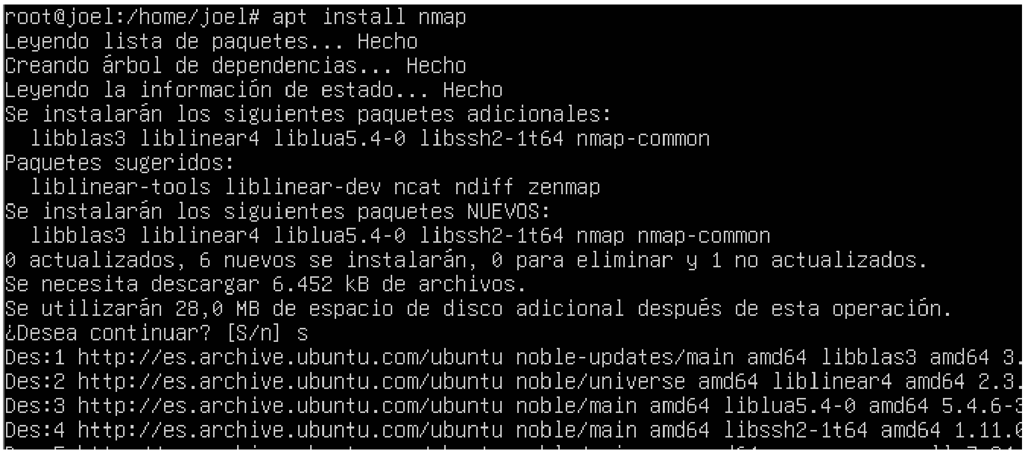


```
Last login: Mon May 12 22:03:02 2025 from 172.16.1.4
joel@joel:~$ exit
logout
Connection to 172.16.1.2 closed.
root@cliente-ssh:/etc/netplan# ssh joelfial@172.16.1.2
joelfial@172.16.1.2's password:
Permission denied, please try again.
joelfial@172.16.1.2's password:
Permission denied, please try again.
joelfial@172.16.1.2's password:

^C
root@cliente-ssh:/etc/netplan# _
```

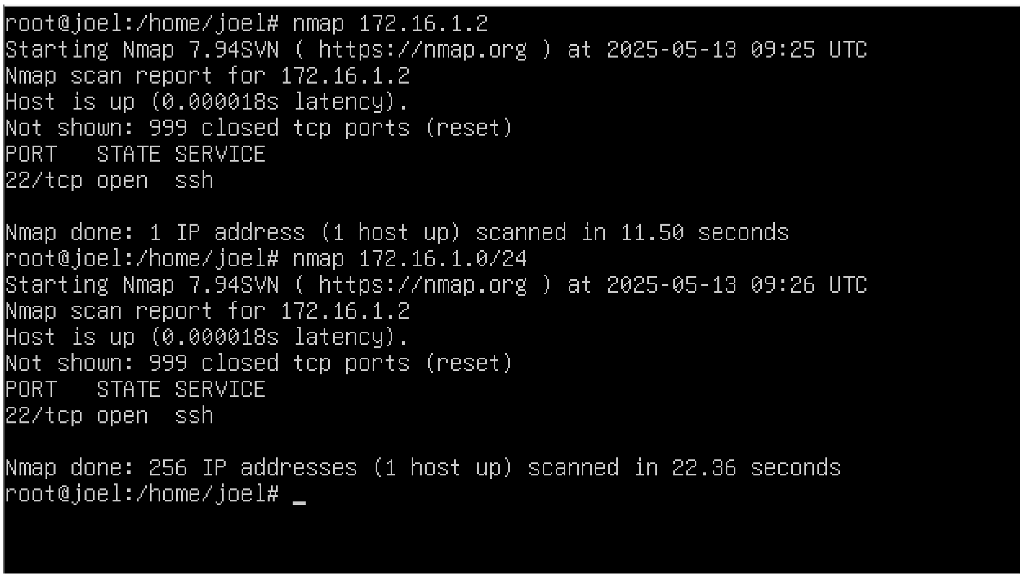
RMIAS DEL SERVIDOR

1. Avaluem els riscos

   Per poder identificar amenaces al servidor instal·lem l’eina nmap



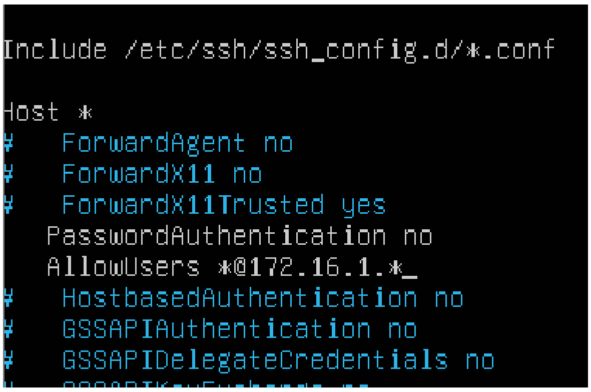
```
root@joel:/home/joel# apt install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap-common
Paquetes sugeridos:
  liblinear-tools liblinear-dev ncat ndiff zenmap
Se instalarán los siguientes paquetes NUEVOS:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap nmap-common
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 6.452 kB de archivos.
Se utilizarán 28,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3.
Des:2 http://es.archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.
Des:3 http://es.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3
Des:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0
```



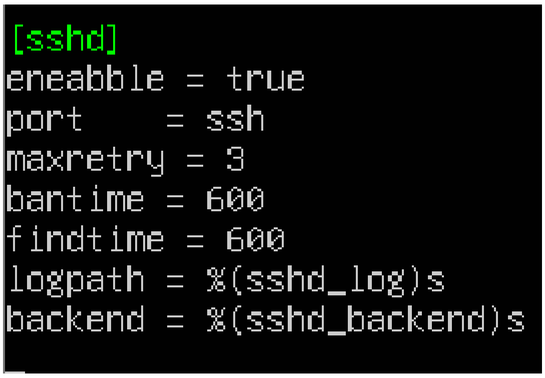
```
root@joel:/home/joel# nmap 172.16.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 09:25 UTC
Nmap scan report for 172.16.1.2
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
root@joel:/home/joel# nmap 172.16.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 09:26 UTC
Nmap scan report for 172.16.1.2
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (1 host up) scanned in 22.36 seconds
root@joel:/home/joel# _
```

2. Control d'accés

Hem implementat a la configuració de SSH que no es pot accedir per contrasenya sinó amb les keys rsa i solament amb , també amb l'eina de Fail2ban el ban de les IP de l'accés no autoritzat.



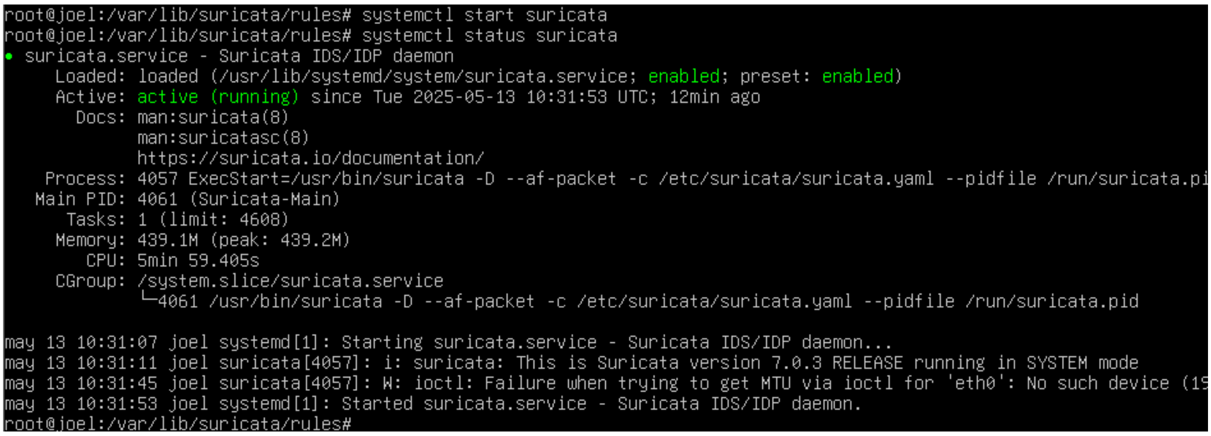
```
Include /etc/ssh/ssh_config.d/*.conf

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
    PasswordAuthentication no
    AllowUsers *@172.16.1.*_
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
```



```
[sshd]
eneabble = true
port     = ssh
maxretry = 3
bantime = 600
findtime = 600
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

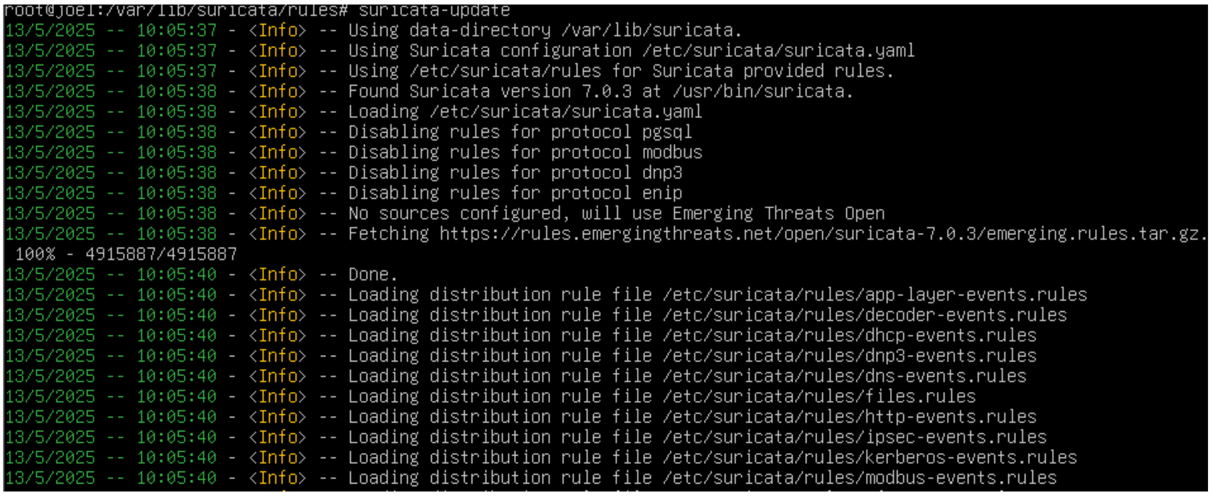
3. Monitoratge d’intrusos al servidor

Per poder aconseguir el monitoratge a temps real utilitzaré l’eina de suricata aquesta eina analitza i detecta a la xarxa del servidor



```
root@joel:/var/lib/suricata/rules# systemctl start suricata
root@joel:/var/lib/suricata/rules# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-05-13 10:31:53 UTC; 12min ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 4057 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pi
   Main PID: 4061 (Suricata-Main)
      Tasks: 1 (limit: 4608)
     Memory: 439.1M (peak: 439.2M)
        CPU: 5min 59.405s
     CGroup: /system.slice/suricata.service
             └─4061 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

may 13 10:31:07 joel systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
may 13 10:31:11 joel suricata[4057]: i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
may 13 10:31:45 joel suricata[4057]: W: ioctl: Failure when trying to get MTU via ioctl for 'eth0': No such device (19
may 13 10:31:53 joel systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
root@joel:/var/lib/suricata/rules#
```

Descarreguem les regles de suricata

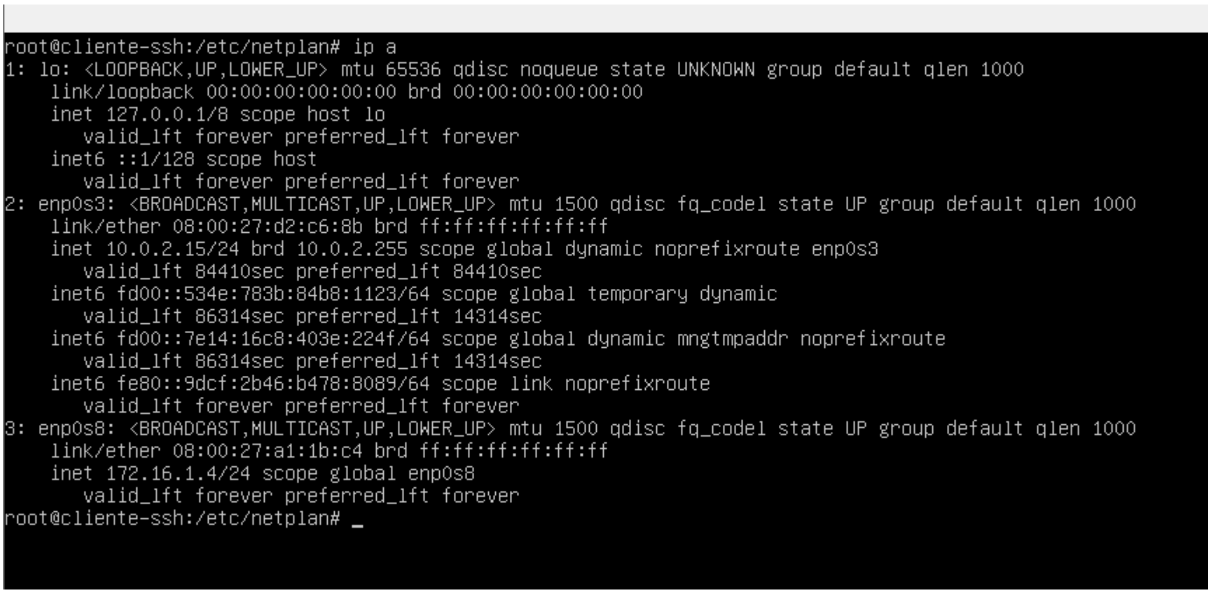


```
root@joel:/var/lib/suricata/rules# suricata-update
13/5/2025 -- 10:05:37 - <Info> -- Using data-directory /var/lib/suricata.
13/5/2025 -- 10:05:37 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
13/5/2025 -- 10:05:37 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
13/5/2025 -- 10:05:38 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suricata.
13/5/2025 -- 10:05:38 - <Info> -- Loading /etc/suricata/suricata.yaml
13/5/2025 -- 10:05:38 - <Info> -- Disabling rules for protocol pgsql
13/5/2025 -- 10:05:38 - <Info> -- Disabling rules for protocol modbus
13/5/2025 -- 10:05:38 - <Info> -- Disabling rules for protocol dnp3
13/5/2025 -- 10:05:38 - <Info> -- Disabling rules for protocol enip
13/5/2025 -- 10:05:38 - <Info> -- No sources configured, will use Emerging Threats Open
13/5/2025 -- 10:05:38 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.3/emerging.rules.tar.gz.
 100% - 4915887/4915887
13/5/2025 -- 10:05:40 - <Info> -- Done.
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
13/5/2025 -- 10:05:40 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
```

Para detectar els últims logs al servidor afegim una comanda amb un tal al i -f per veure’l a temps real al fitxer logs de suricata

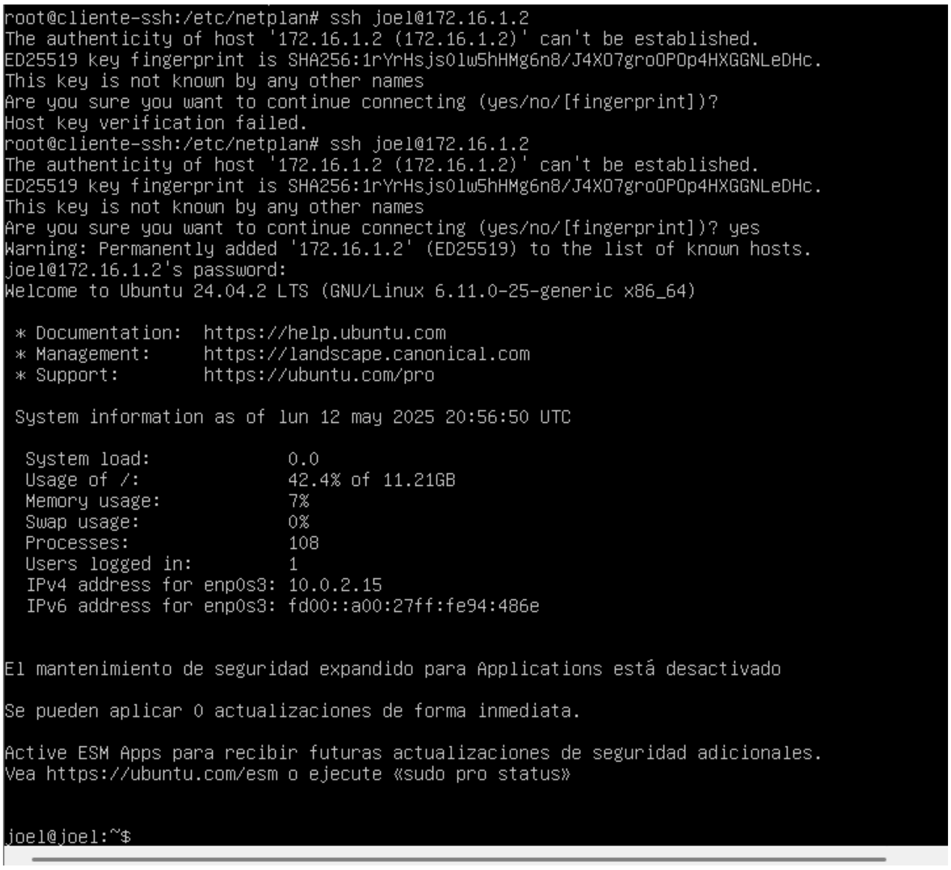
CLIENT

figurem la connexió al client



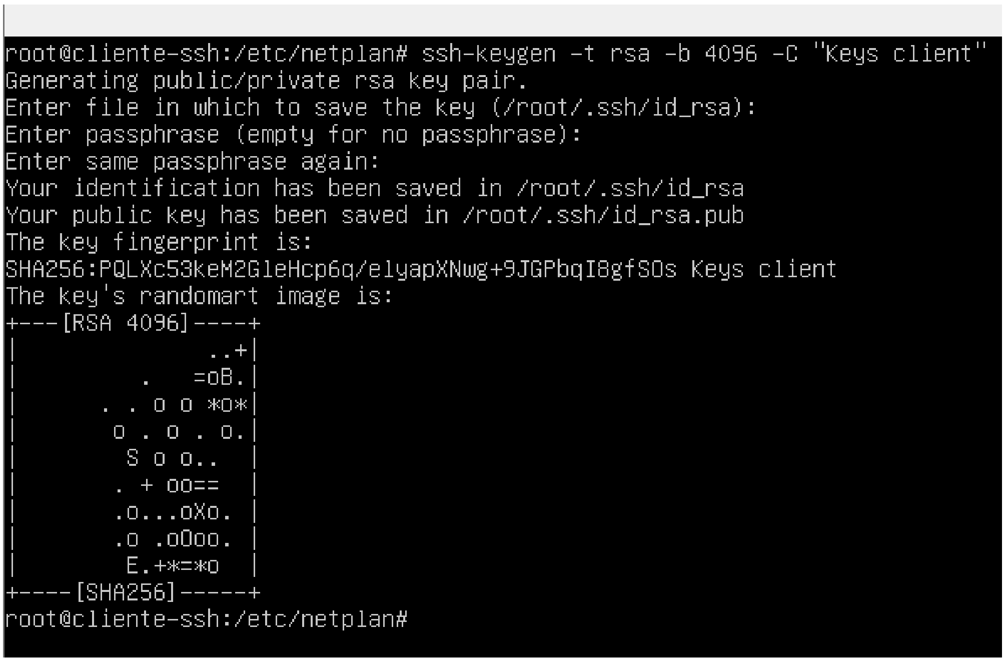
```
root@cliente-ssh:/etc/netplan# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:c6:8b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 84410sec preferred_lft 84410sec
    inet6 fd00::534e:783b:84b8:1123/64 scope global temporary dynamic
       valid_lft 86314sec preferred_lft 14314sec
    inet6 fd00::7e14:16c8:403e:224f/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86314sec preferred_lft 14314sec
    inet6 fe80::9dcf:2b46:b478:8089/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a1:1b:c4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.4/24 scope global enp0s8
       valid_lft forever preferred_lft forever
root@cliente-ssh:/etc/netplan# _
```

comprovem si hi ha connexió per SSH



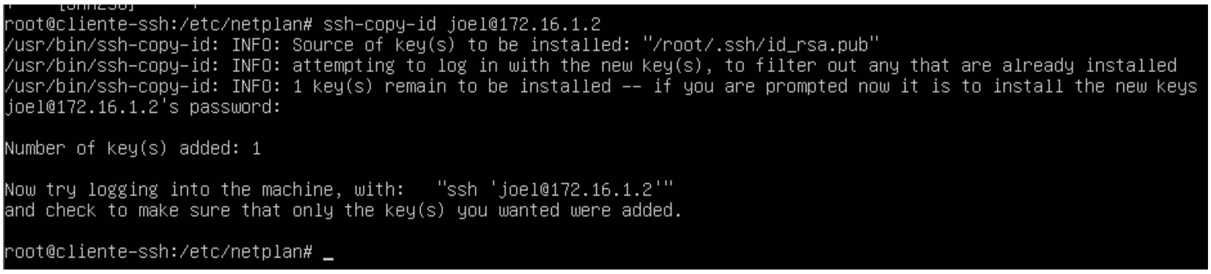
```
root@cliente-ssh:/etc/netplan# ssh joel@172.16.1.2
The authenticity of host '172.16.1.2 (172.16.1.2)' can't be established.
ED25519 key fingerprint is SHA256:1rYrHsjsOlw5hHMg6n8/J4XO7groOPOp4HXGGNLeDHc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
root@cliente-ssh:/etc/netplan# ssh joel@172.16.1.2
The authenticity of host '172.16.1.2 (172.16.1.2)' can't be established.
ED25519 key fingerprint is SHA256:1rYrHsjsOlw5hHMg6n8/J4XO7groOPOp4HXGGNLeDHc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.2' (ED25519) to the list of known hosts.
joel@172.16.1.2's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

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

 System information as of lun 12 may 2025 20:56:50 UTC

  System load:             0.0
  Usage of /:              42.4% of 11.21GB
  Memory usage:            7%
  Swap usage:              0%
  Processes:               108
  Users logged in:         1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd00::a00:27ff:fe94:486e


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

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


joel@joel:~$
```

Generem dos claus rsa al client s’ha generat una keys pública que serà per al servidor i una keys privada.

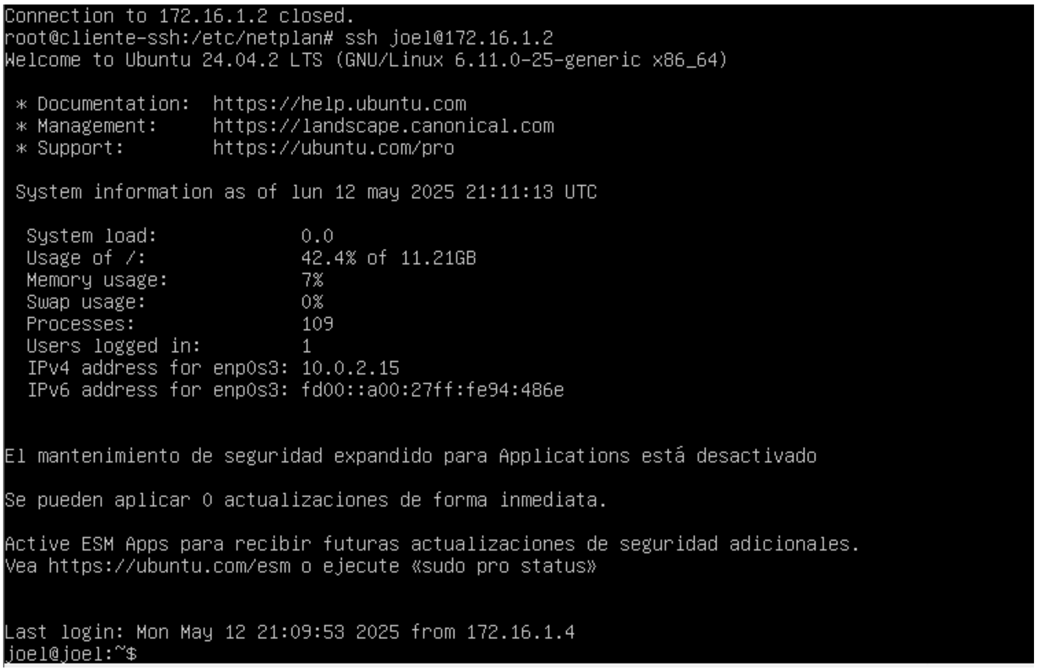


```
root@cliente-ssh:/etc/netplan# ssh-keygen -t rsa -b 4096 -C "Keys client"
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:PQLXc53keM2GleHcp6q/elyapXNwg+9JGPbqI8gfSOs Keys client
The key's randomart image is:
+---[RSA 4096]----+
|              ..+|
|         .   =oB.|
|      . . o o *o*|
|       o . o . o.|
|        S o o..  |
|       . + oo==  |
|       .o...oXo. |
|       .o .oOoo. |
|        E.+*=*o  |
+----[SHA256]-----+
root@cliente-ssh:/etc/netplan#
```

Per via SSH enviarem la nostra clau publica al servidor per poder entrar sense contraseña



```
root@cliente-ssh:/etc/netplan# ssh-copy-id joel@172.16.1.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.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 prompted now it is to install the new keys
joel@172.16.1.2's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'joel@172.16.1.2'"
and check to make sure that only the key(s) you wanted were added.

root@cliente-ssh:/etc/netplan# _
```



```
Connection to 172.16.1.2 closed.
root@cliente-ssh:/etc/netplan# ssh joel@172.16.1.2
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

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

 System information as of lun 12 may 2025 21:11:13 UTC

  System load:             0.0
  Usage of /:              42.4% of 11.21GB
  Memory usage:            7%
  Swap usage:              0%
  Processes:               109
  Users logged in:         1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd00::a00:27ff:fe94:486e


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

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


Last login: Mon May 12 21:09:53 2025 from 172.16.1.4
joel@joel:~$
```