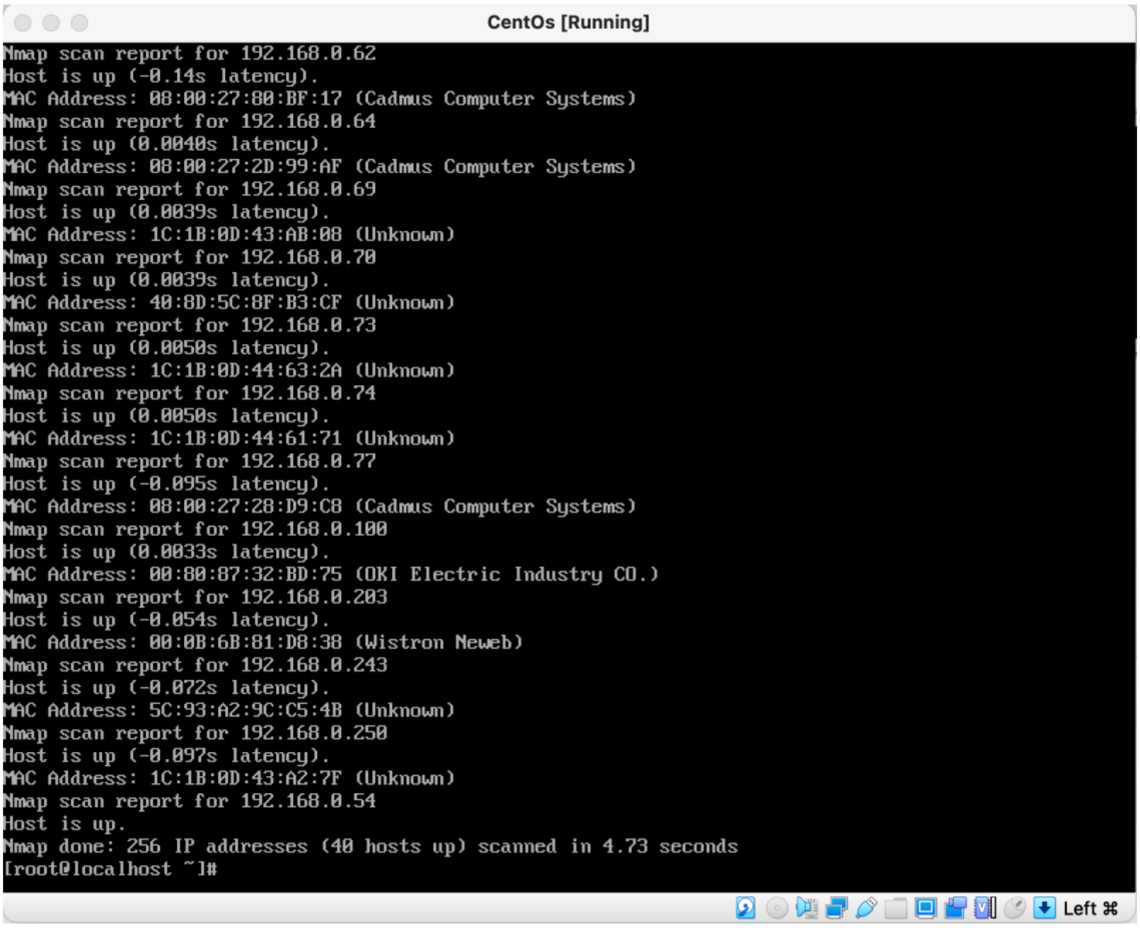
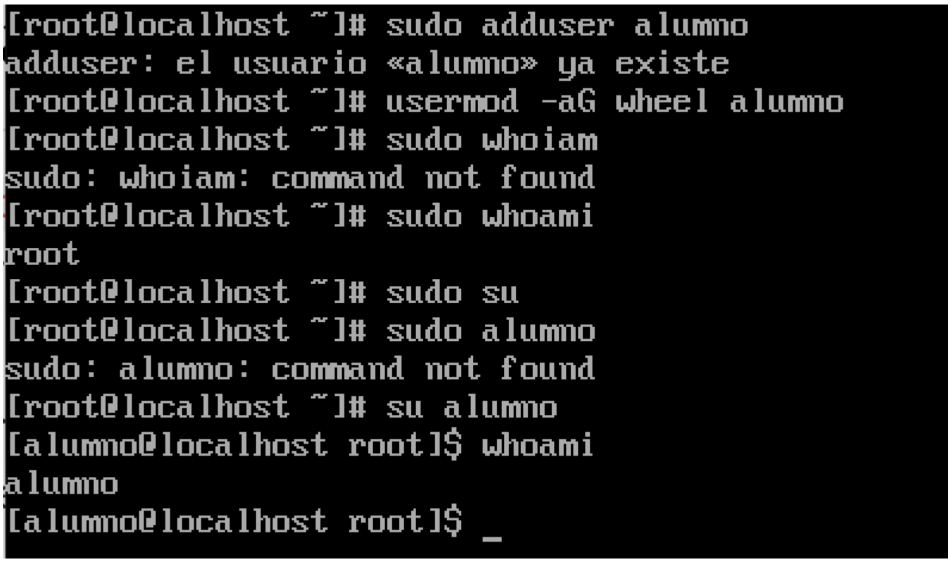
Primero hago el comando nmap -sP 192.168.0.0/24 para saber las ip que hay en mi red:



```
Nmap scan report for 192.168.0.62
Host is up (-0.14s latency).
MAC Address: 08:00:27:80:BF:17 (Cadmus Computer Systems)
Nmap scan report for 192.168.0.64
Host is up (0.0040s latency).
MAC Address: 08:00:27:2D:99:AF (Cadmus Computer Systems)
Nmap scan report for 192.168.0.69
Host is up (0.0039s latency).
MAC Address: 1C:1B:0D:43:AB:08 (Unknown)
Nmap scan report for 192.168.0.70
Host is up (0.0039s latency).
MAC Address: 40:8D:5C:8F:B3:CF (Unknown)
Nmap scan report for 192.168.0.73
Host is up (0.0050s latency).
MAC Address: 1C:1B:0D:44:63:2A (Unknown)
Nmap scan report for 192.168.0.74
Host is up (0.0050s latency).
MAC Address: 1C:1B:0D:44:61:71 (Unknown)
Nmap scan report for 192.168.0.77
Host is up (-0.095s latency).
MAC Address: 08:00:27:28:D9:C8 (Cadmus Computer Systems)
Nmap scan report for 192.168.0.100
Host is up (0.0033s latency).
MAC Address: 00:80:87:32:BD:75 (OKI Electric Industry CO.)
Nmap scan report for 192.168.0.203
Host is up (-0.054s latency).
MAC Address: 00:0B:6B:81:D8:38 (Wistron Neweb)
Nmap scan report for 192.168.0.243
Host is up (-0.072s latency).
MAC Address: 5C:93:A2:9C:C5:4B (Unknown)
Nmap scan report for 192.168.0.250
Host is up (-0.097s latency).
MAC Address: 1C:1B:0D:43:A2:7F (Unknown)
Nmap scan report for 192.168.0.54
Host is up.
Nmap done: 256 IP addresses (40 hosts up) scanned in 4.73 seconds
[root@localhost ~]#
```

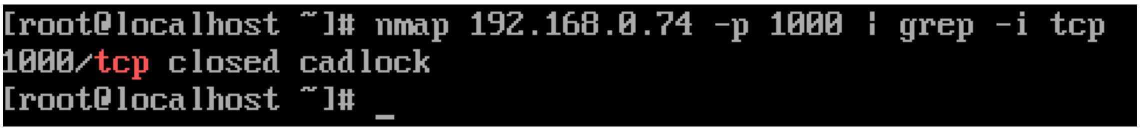
Después añado el usuario alumno al grupo Wheel para acceder como superusuario: con el comando usermod -aG Wheel alumno:

Entro como usuario alumno para comprobar que esta añadido como superusuario



```
[root@localhost ~]# sudo adduser alumno
adduser: el usuario «alumno» ya existe
[root@localhost ~]# usermod -aG wheel alumno
[root@localhost ~]# sudo whoiam
sudo: whoiam: command not found
[root@localhost ~]# sudo whoami
root
[root@localhost ~]# sudo su
[root@localhost ~]# sudo alumno
sudo: alumno: command not found
[root@localhost ~]# su alumno
[alumno@localhost root]$ whoami
alumno
[alumno@localhost root]$ _
```

Comprobar cada ip para saber que puertos que tienen abierto:
nmap (ip elegida) -p 1000 | grep -i tcp



```
[root@localhost ~]# nmap 192.168.0.74 -p 1000 | grep -i tcp
1000/tcp closed cadlock
[root@localhost ~]# _
```

En este caso el puerto 1000 lo tiene cerrado.

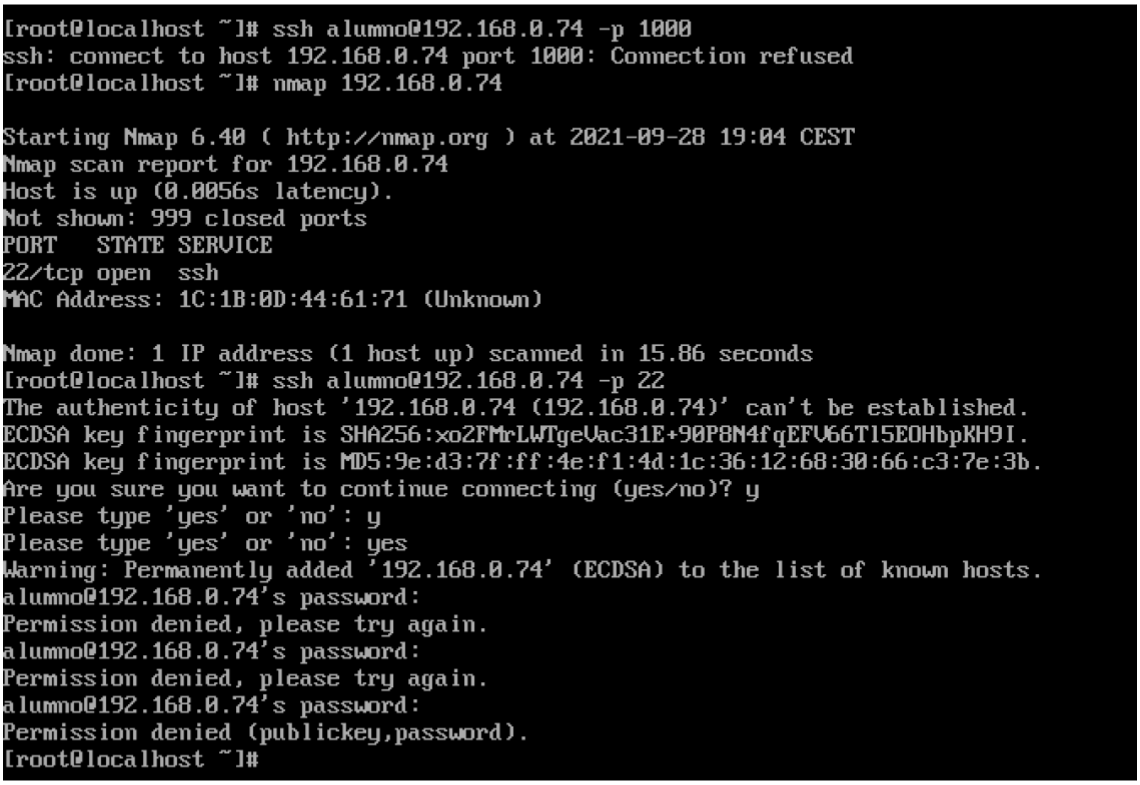
Uso el siguiente código para ver la nmap de la red que quiero atacar y que me de la información del puerto que tiene abierto.

nmap (la dirección que quiero atacar) **192.168.0.74**

He visto que el puerto que tiene abierto es el **22/tcp open ssh**.

Y este comando es para acceder a él
ssh alumno@192.168.0.74 -p 22

Una vez accedo a él me pide la contraseña, la he intentado poner pero se ve que la ha cambiado.



```
[root@localhost ~]# ssh alumno@192.168.0.74 -p 1000
ssh: connect to host 192.168.0.74 port 1000: Connection refused
[root@localhost ~]# nmap 192.168.0.74

Starting Nmap 6.40 ( http://nmap.org ) at 2021-09-28 19:04 CEST
Nmap scan report for 192.168.0.74
Host is up (0.0056s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 1C:1B:0D:44:61:71 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 15.86 seconds
[root@localhost ~]# ssh alumno@192.168.0.74 -p 22
The authenticity of host '192.168.0.74 (192.168.0.74)' can't be established.
ECDSA key fingerprint is SHA256:xo2FMrLWTgeVac31E+90P8N4fqEFV66Tl5EOHbpKH9I.
ECDSA key fingerprint is MD5:9e:d3:7f:ff:4e:f1:4d:1c:36:12:68:30:66:c3:7e:3b.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.0.74' (ECDSA) to the list of known hosts.
alumno@192.168.0.74's password:
Permission denied, please try again.
alumno@192.168.0.74's password:
Permission denied, please try again.
alumno@192.168.0.74's password:
Permission denied (publickey,password).
[root@localhost ~]#
```