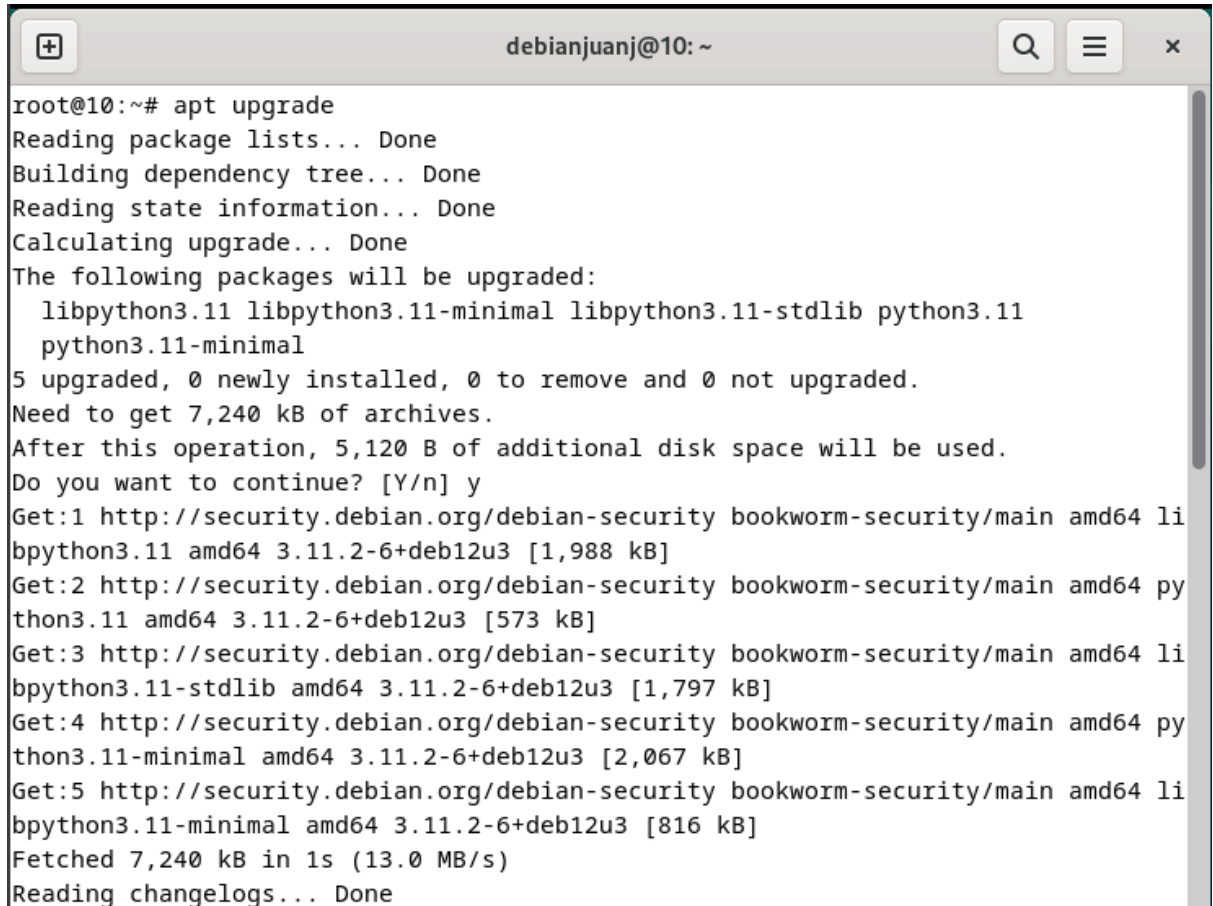


Laboratorio 2_U3

Nombre: Juan Jiménez

Fecha: 27/08/2024

1. Emplear el comando de actualización del sistema y aplicaciones:



```
root@10:~# apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  libpython3.11 libpython3.11-minimal libpython3.11-stdlib python3.11
  python3.11-minimal
5 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 7,240 kB of archives.
After this operation, 5,120 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://security.debian.org/debian-security bookworm-security/main amd64 li
bpython3.11 amd64 3.11.2-6+deb12u3 [1,988 kB]
Get:2 http://security.debian.org/debian-security bookworm-security/main amd64 py
thon3.11 amd64 3.11.2-6+deb12u3 [573 kB]
Get:3 http://security.debian.org/debian-security bookworm-security/main amd64 li
bpython3.11-stdlib amd64 3.11.2-6+deb12u3 [1,797 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main amd64 py
thon3.11-minimal amd64 3.11.2-6+deb12u3 [2,067 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 li
bpython3.11-minimal amd64 3.11.2-6+deb12u3 [816 kB]
Fetched 7,240 kB in 1s (13.0 MB/s)
Reading changelogs... Done
```

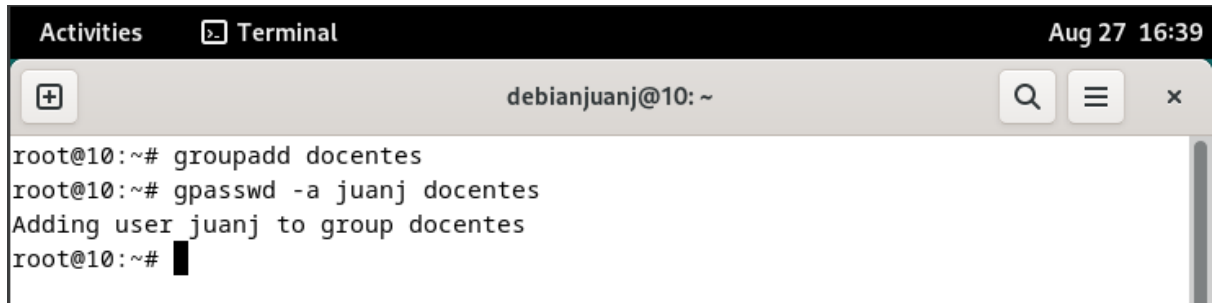
Para empezar la actividad se realizo la actualizacion de los repositorios de apt con los comandos “apt update” y “apt upgrade” estos 2 realizados mediante root.

2. Gestionar los usuarios:



```
root@10:~# useradd juanj
root@10:~# passwd juanj
New password:
Retype new password:
passwd: password updated successfully
root@10:~# █
```

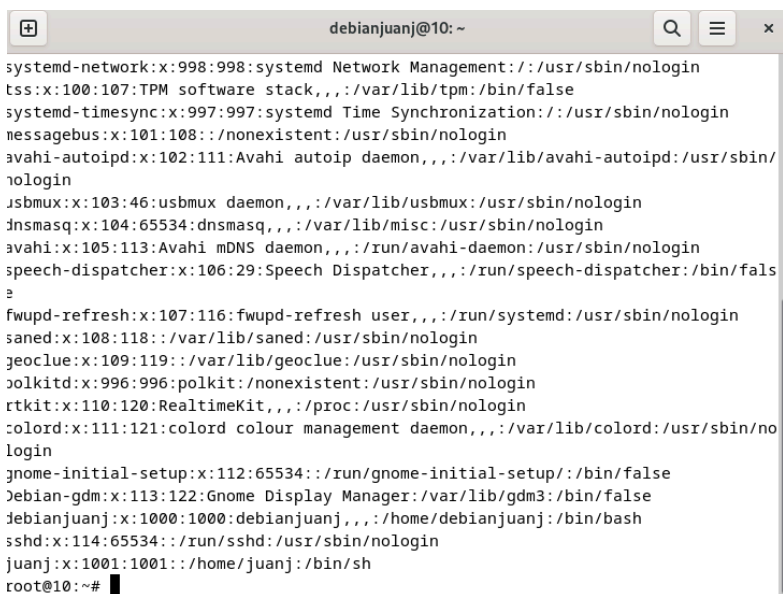
Se crea un usuario con el comando “useradd (nombreusuario)” y su respectiva contraseña con el comando “passwd (nombreusuario)” con este comando se coloca una contraseña a algún usuario que esté registrado.



```
root@10:~# groupadd docentes
root@10:~# gpasswd -a juanj docentes
Adding user juanj to group docentes
root@10:~#
```

Con el comando “groupadd (nombregrupo)” se agrega un grupo a la listas de grupos del equipo y con el comando “gpasswd -a (nombreusuario) (nombregrupo)” con este comando se agrega un usuario a un grupo.

3. Verificar en los archivos /etc/passwd, /etc/group y /etc/shadow , la creación de los usuarios, la definición de los grupos y las contraseñas encriptadas:



```
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
tss:x:100:107:TPM software stack,,:/var/lib/tpm:/bin/false
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
messagebus:x:101:108:/:nonexistent:/usr/sbin/nologin
avahi-autoipd:x:102:111:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:103:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:104:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:105:113:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:106:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:107:116:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
saned:x:108:118:/:/var/lib/saned:/usr/sbin/nologin
geoclue:x:109:119:/:/var/lib/geoclue:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:110:120:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:111:121:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:112:65534:/:/run/gnome-initial-setup:/bin/false
debian-gdm:x:113:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
debianjuanj:x:1000:1000:debianjuanj,,:/home/debianjuanj:/bin/bash
sshd:x:114:65534:/:/run/ssh:/usr/sbin/nologin
juanj:x:1001:1001:/:/home/juanj:/bin/sh
root@10:~#
```

```
debianjuan@10: ~  
systemd-timesync:x:997:  
messagebus:x:108:  
_ssh:x:109:  
ssl-cert:x:110:  
avahi-autoipd:x:111:  
bluetooth:x:112:  
avahi:x:113:  
lpadmin:x:114:  
pipewire:x:115:  
fwupd-refresh:x:116:  
scanner:x:117:saned  
saned:x:118:  
geoclue:x:119:  
polkitd:x:996:  
rtkit:x:120:  
colord:x:121:  
Debian-gdm:x:122:  
debianjuanj:x:1000:  
gnome-initial-setup:x:995:  
rdma:x:123:  
smbshare:x:994:  
juanj:x:1001:  
docentes:x:1002:juanj  
root@10:~#
```

```
debianjuanj@10: ~  
nobody:*:19927:0:99999:7:::  
systemd-network:!*:19927:::~:  
tss:!:19927:::~:  
systemd-timesync:!*:19927:::~:  
messagebus:!:19927:::~:  
avahi-autoipd:!:19927:::~:  
usbmux:!:19927:::~:  
dnsmasq:!:19927:::~:  
avahi:!:19927:::~:  
speech-dispatcher:!:19927:::~:  
fwupd-refresh:!:19927:::~:  
saned:!:19927:::~:  
geoclue:!:19927:::~:  
polkitd:!*:19927:::~:  
rtkit:!:19927:::~:  
colord:!:19927:::~:  
gnome-initial-setup:!:19927:::~:  
Debian-gdm:!:19927:::~:  
debianjuanj:$y$j9T$LR5xf7DZkHr9dNljz//u3/$eDLihEVU7PfytxGX5dXiXPBmbP2THDvvhW5ULJ  
fp0rA:19927:0:99999:7:::  
sshd:!:19927:::~:  
juanj:$y$j9T$PdUsj9Iszvz00w50LFu810$eBPydbewCjaVZ7YVzw/z8xnL5EFy2SJoGEN8KG5STY3:  
19962:0:99999:7:::  
root@10:~#
```

Con los comandos “cat /etc/passwd” se verifica los datos de las contraseñas de los diferentes usuarios que se encuentran en el equipo, con el comando “cat /etc/group” se verifican los grupos que se encuentran en el equipo y con el comando “cat /etc/shadow” este se mira las conexiones entre los usuarios y los grupos.

4. Eliminar un usuario:

```
debianjuanj@10: ~  
root@10:~# useradd sora  
root@10:~# userdel -r sora  
userdel: sora mail spool (/var/mail/sora) not found  
userdel: sora home directory (/home/sora) not found  
root@10:~#
```

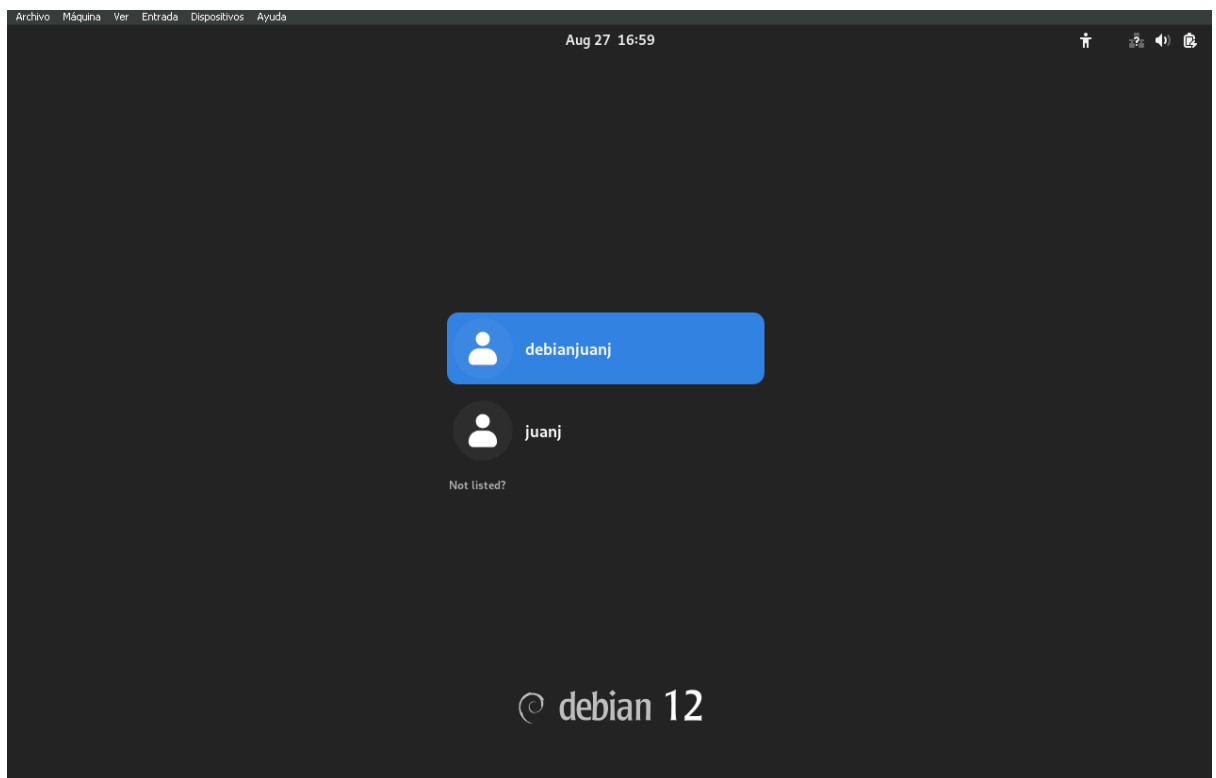
Con el comando “userdel -r (nombreusuario)” se eliminan usuarios del grupo de usuarios del equipo.

5. Bloquear un usuario:

```
debianjuanj@10: ~  
root@10:~# passwd -l sora  
passwd: password changed.  
root@10:~#
```

Con el comando “passwd -l (nombreusuario)” se bloquea la cuenta de un usuario que esté ingresado.

6. Verificar que el usuario está bloqueado cambiando de sesión:



Se logra ver que el usuario “sora” desapareció de la lista de usuarios.

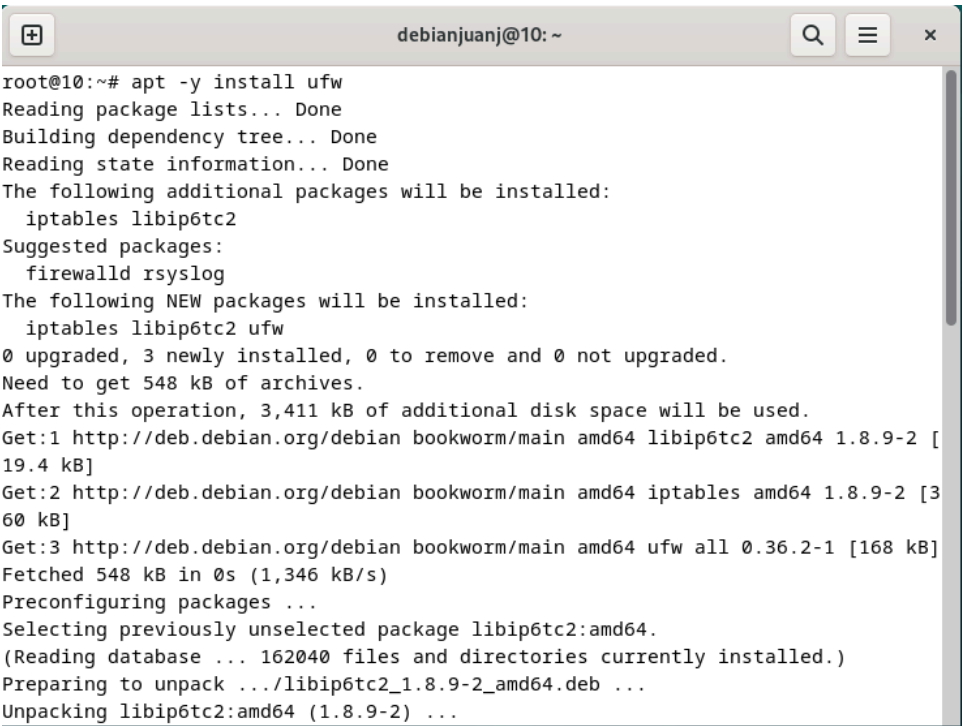
7. Desbloquear al usuario:

A terminal window titled 'debianjuan@10: ~' with search, menu, and close icons. It shows the command 'passwd -u sora' being executed, resulting in 'passwd: password changed.' and returning to the root prompt.

```
root@10:~# passwd -u sora
passwd: password changed.
root@10:~#
```

con el comando “passwd -y (nombreusuario)” con este comando se realiza la función de desbloquear un usuario especificado.

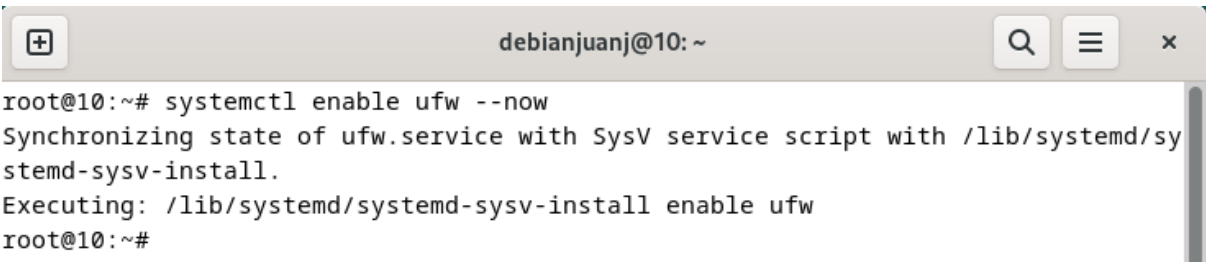
8. Instalar el firewall ufw en Linux:

A terminal window titled 'debianjuan@10: ~' showing the installation of ufw. It lists additional packages (iptables, libip6tc2), suggested packages (firewalld, rsyslog), and disk space requirements. It shows the download progress for libip6tc2, iptables, and ufw.

```
root@10:~# apt -y install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  iptables libip6tc2
Suggested packages:
  firewalld rsyslog
The following NEW packages will be installed:
  iptables libip6tc2 ufw
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 548 kB of archives.
After this operation, 3,411 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 libip6tc2 amd64 1.8.9-2 [19.4 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 ufw all 0.36.2-1 [168 kB]
Fetched 548 kB in 0s (1,346 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libip6tc2:amd64.
(Reading database ... 162040 files and directories currently installed.)
Preparing to unpack .../libip6tc2_1.8.9-2_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.9-2) ...
```

Se instala el firewall ufw con el comando “apt -y install ufw” y genera un montón de líneas de comandos que instalan el ufw.

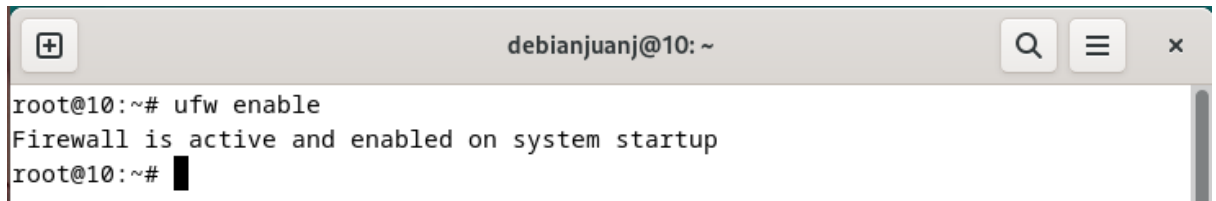
9. Habilitar e instalar el servicio ufw:

A terminal window titled 'debianjuan@10: ~' showing the command 'systemctl enable ufw --now' being executed. It shows the process of synchronizing the service state and installing the systemd-sysv script.

```
root@10:~# systemctl enable ufw --now
Synchronizing state of ufw.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ufw
root@10:~#
```

Con el comando “systemctl enable ufw --now” se habilita el servicio de ufw.

10. Habilitar el firewall:



```
debianjuanj@10: ~  
root@10:~# ufw enable  
Firewall is active and enabled on system startup  
root@10:~#
```

Con el comando “ufw enable” se habilita el funcionamiento del firewall de ufw.

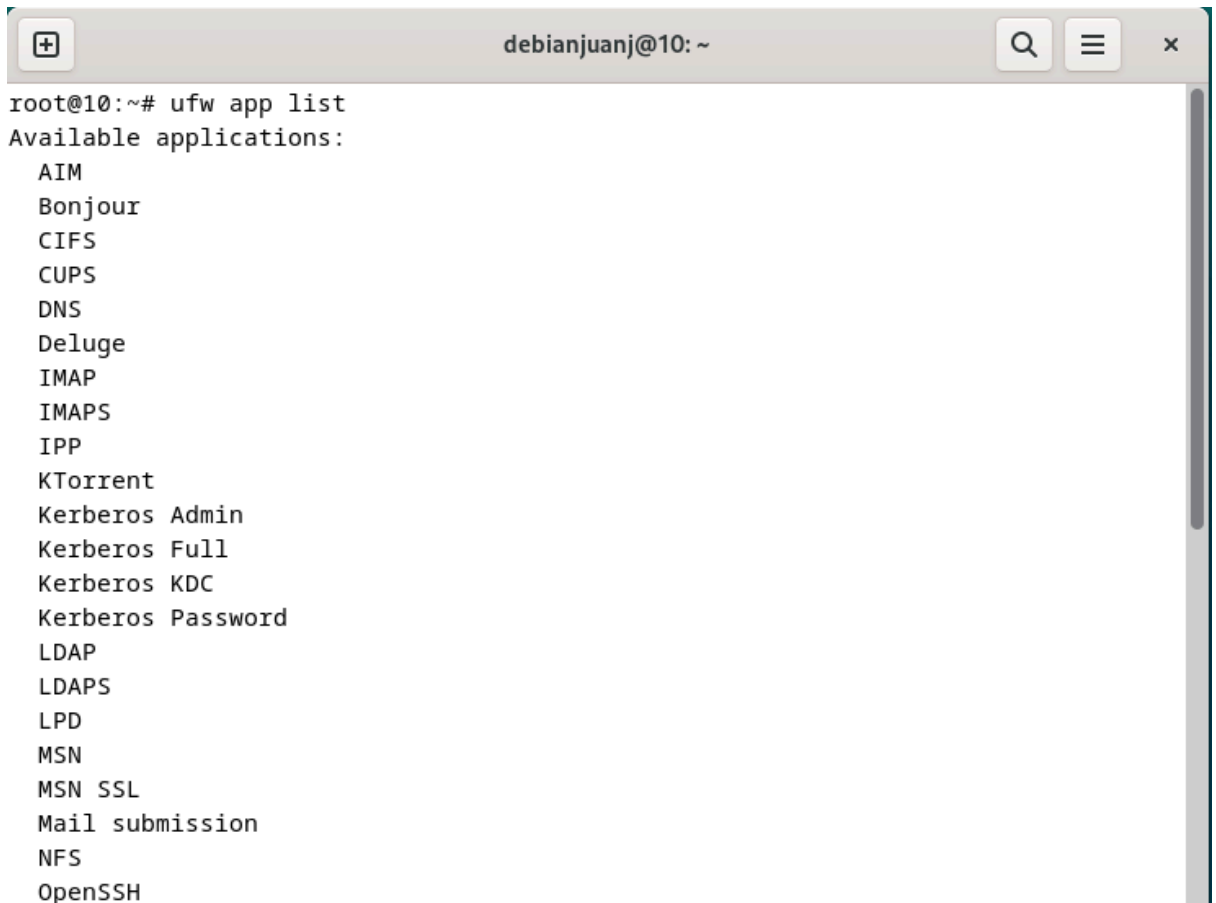
11. Revisar las zonas activas y las reglas asociadas a cada una:



```
debianjuanj@10: ~  
root@10:~# ufw status  
Status: active  
root@10:~#
```

Con el comando “ufw status” se muestra el estado del servicio ufw, en este caso muestra que se encuentra operativo.

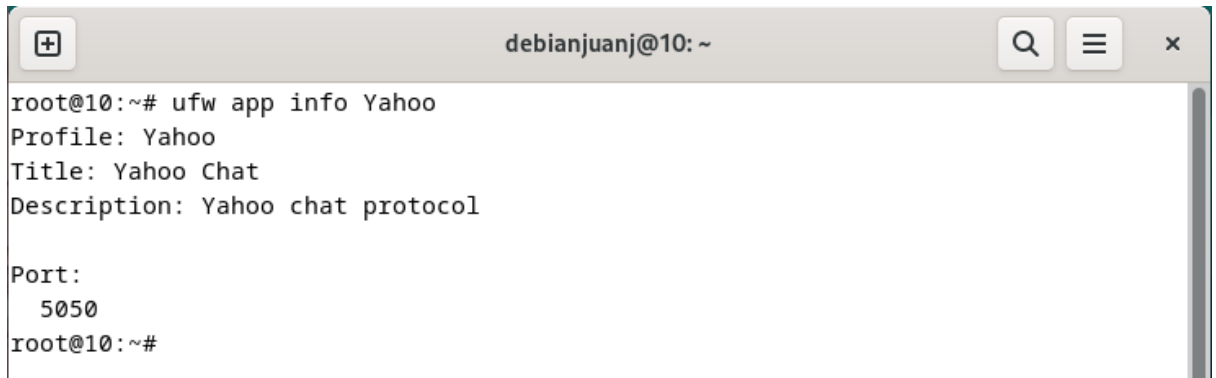
12. Observar las zonas del firewall:



```
debianjuanj@10: ~  
root@10:~# ufw app list  
Available applications:  
  AIM  
  Bonjour  
  CIFS  
  CUPS  
  DNS  
  Deluge  
  IMAP  
  IMAPS  
  IPP  
  KTorrent  
  Kerberos Admin  
  Kerberos Full  
  Kerberos KDC  
  Kerberos Password  
  LDAP  
  LDAPS  
  LPD  
  MSN  
  MSN SSL  
  Mail submission  
  NFS  
  OpenSSH
```

Con el comando “ufw app list” se muestra la lista de las aplicaciones en las que se encuentra habilitado el servicio de ufw.

13. Obtener información detallada sobre las reglas de una aplicación o servicio:

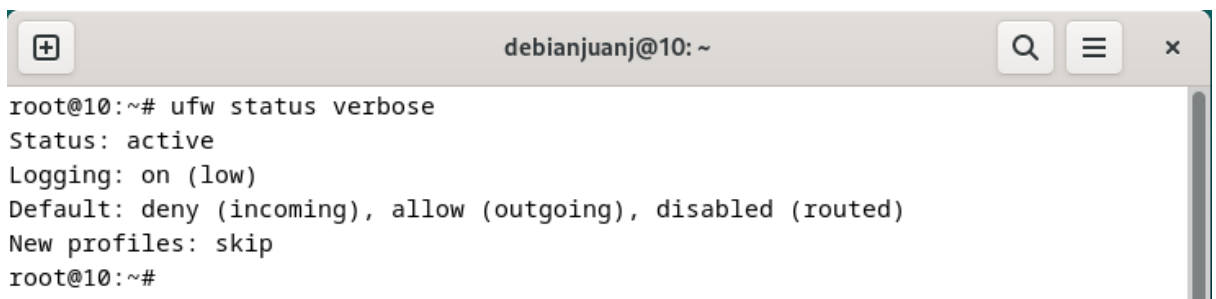


```
debianjuanj@10: ~
root@10:~# ufw app info Yahoo
Profile: Yahoo
Title: Yahoo Chat
Description: Yahoo chat protocol

Port:
  5050
root@10:~#
```

Con el comando “ufw app info (nombreAplicacion)” se muestra información sobre la aplicación que tenga compatibilidad con ufw.

14. Determinar de manera detallada el status de las zonas:



```
debianjuanj@10: ~
root@10:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
root@10:~#
```

con el comando “ufw status verbose” te muestra el estado del ufw con algo de información extra.

15. ACLs de red con ufw permitir tráfico entrante HTTP en el puerto 80:



```
debianjuanj@10: ~
root@10:~# ufw allow 80/tcp
Rule added
Rule added (v6)
root@10:~#
```

Con el comando “ufw allow 80/tcp” permite el trafico de los puertos 80 para servicios http.

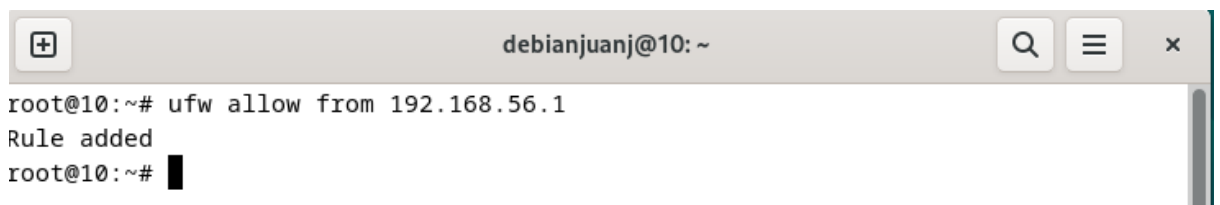
16. Permitir tráfico entrante HTTPS en el puerto 443:

A terminal window titled 'debianjuan@10: ~' with search, menu, and close icons. The command 'ufw allow 433/tcp' is entered, resulting in the output: 'Rule added', 'Rule added (v6)', and a new prompt 'root@10:~#'.

```
root@10:~# ufw allow 433/tcp
Rule added
Rule added (v6)
root@10:~#
```

Con el comando “ufw allow 433/tcp” permite las conexiones https de los puertos 443

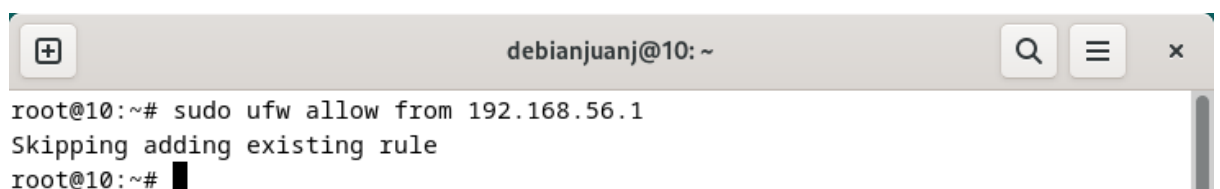
17. Permitir tráfico entrante SSH en el puerto 22 solo desde una dirección IP específica:

A terminal window titled 'debianjuan@10: ~' with search, menu, and close icons. The command 'ufw allow from 192.168.56.1' is entered, resulting in the output: 'Rule added' and a new prompt 'root@10:~#'.

```
root@10:~# ufw allow from 192.168.56.1
Rule added
root@10:~#
```

Con el comando “ufw allow from (ip deseada)” permite la conexion de algun puerto 22 para una ip en especifico.

18. Permitir tráfico entrante SSH en el puerto 22 solo desde una subred específica:

A terminal window titled 'debianjuan@10: ~' with search, menu, and close icons. The command 'sudo ufw allow from 192.168.56.1' is entered, resulting in the output: 'Skipping adding existing rule' and a new prompt 'root@10:~#'.

```
root@10:~# sudo ufw allow from 192.168.56.1
Skipping adding existing rule
root@10:~#
```

Con el comando “sudo ufw allow from (ip en específica)” permite la conexión de algún puerto de una subred.

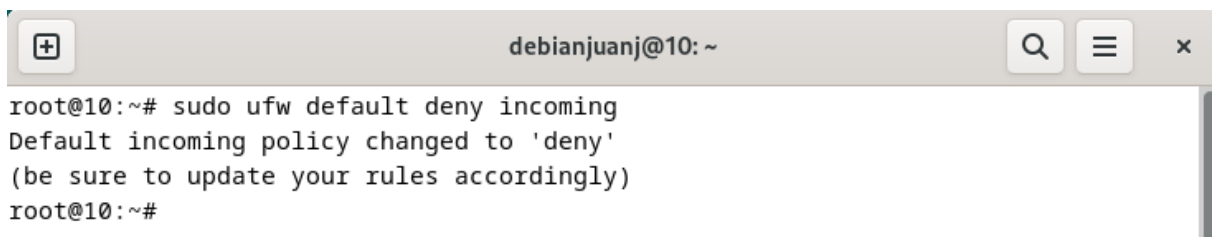
19. Permitir tráfico saliente HTTPS:



```
debianjuanj@10: ~
root@10:~# sudo ufw allow out 443/tcp
Rule added
Rule added (v6)
root@10:~#
```

Con el comando “sudo ufw allow out 443/tcp” este permite el tráfico saliente de los puertos https.

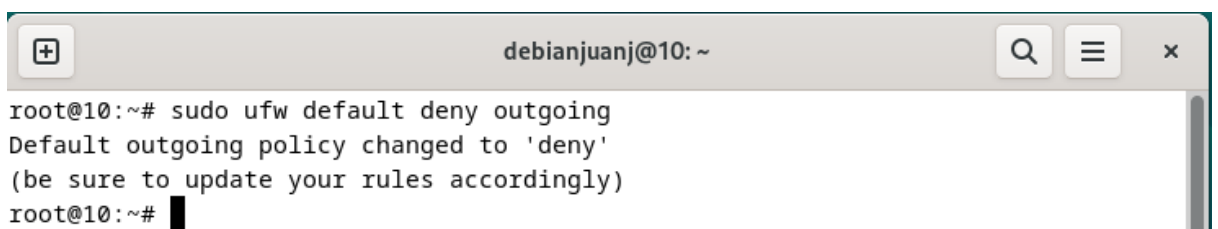
20. Denegar todo el tráfico entrante:



```
debianjuanj@10: ~
root@10:~# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@10:~#
```

Con el comando “sudo ufw default deny incoming” deniega el tráfico entrante al equipo.

21. Denegar todo el tráfico saliente:



```
debianjuanj@10: ~
root@10:~# sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
root@10:~#
```

Con el comando “sudo ufw default deny outgoing” este se encarga de bloquear o denegar todo el tráfico saliente del equipo.

22. Monitoreo de puertos:

```
debianjuanj@10: ~  
root@10:~# apt -y install nmap  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  liblinear4 libpcres lua-lpeg nmap-common  
Suggested packages:  
  liblinear-tools liblinear-dev ncat ndiff zenmap  
The following NEW packages will be installed:  
  liblinear4 libpcres lua-lpeg nmap nmap-common  
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.  
Need to get 6,468 kB of archives.  
After this operation, 27.3 MB of additional disk space will be used.  
Ign:1 http://deb.debian.org/debian bookworm/main amd64 liblinear4 amd64 2.3.0+dfsg-5  
Ign:2 http://deb.debian.org/debian bookworm/main amd64 libpcres amd64 2:8.39-15  
Ign:3 http://deb.debian.org/debian bookworm/main amd64 lua-lpeg amd64 1.0.2-2  
Ign:4 http://deb.debian.org/debian bookworm/main amd64 nmap-common all 7.93+dfsg1-1  
Ign:5 http://deb.debian.org/debian bookworm/main amd64 nmap amd64 7.93+dfsg1-1  
Ign:1 http://deb.debian.org/debian bookworm/main amd64 liblinear4 amd64 2.3.0+dfsg-5  
Ign:2 http://deb.debian.org/debian bookworm/main amd64 libpcres amd64 2:8.39-15  
Ign:3 http://deb.debian.org/debian bookworm/main amd64 lua-lpeg amd64 1.0.2-2
```

Con el comando “apt -y install nmap” se instala el servicio nmap para realizar la siguiente sección del laboratorio.

23. Revisar los puertos abiertos del sistema (localhost se puede reemplazar con una ip) :

```
debianjuanj@10: ~
root@10:~# nmap -sT -O localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:30 -05
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000075s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.58 seconds
root@10:~#
```

Con el comando “nmap -sT -O localhost” se revisa los puertos que estén abiertos del sistema.

24. Escaneo de puertos y detección de sistemas operativos:

```
debianjuanj@10: ~
root@10:~# nmap -O <192.168.56.1>
-bash: syntax error near unexpected token `newline'
root@10:~#
```

Con el comando “nmap -O <IP_Adress>” con este comando verificamos el escaneo y la detección de los SO.

25. Escaneo de puertos y detección de versiones de servicios:

```
debianjuanj@10: ~  
root@10:~# nmap -sV 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:34 -05  
Nmap scan report for 192.168.56.1 (192.168.56.1)  
Host is up (0.0027s latency).  
Not shown: 995 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH for_Windows_8.1 (protocol 2.0)  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds?   
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.47 seconds  
root@10:~#
```

Con el comando “nmap -sV (ip deseada)” se escanea los puertos y la detección de las versiones de los servicios.

26. Escaneo de puertos con detección de firewall:

```
debianjuanj@10: ~  
root@10:~# nmap -sA 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:35 -05  
Nmap scan report for 192.168.56.1 (192.168.56.1)  
Host is up (0.000083s latency).  
All 1000 scanned ports on 192.168.56.1 (192.168.56.1) are in ignored states.  
Not shown: 1000 unfiltered tcp ports (reset)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds  
root@10:~#
```

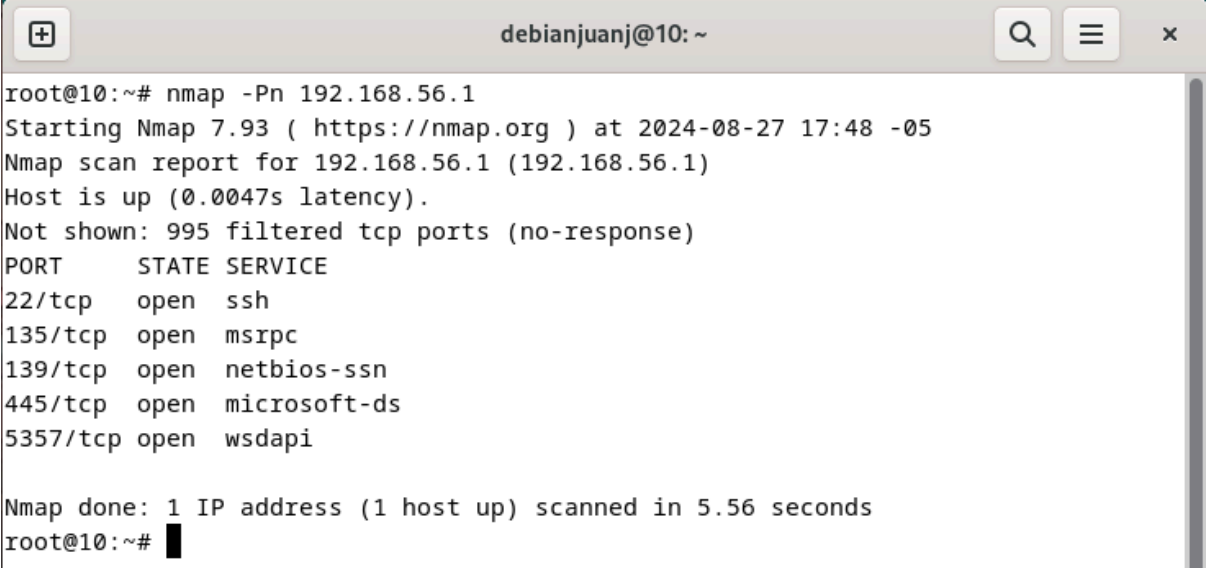
Con el comando “nmap -sA (ip deseada)” con este comando se realiza el escaneo de los puertos que tengan una detección de firewall.

27. Escaneo de puertos TCP y UDP:

```
debianjuanj@10: ~  
root@10:~# nmap -sU -sT 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:41 -05  
  
root@10:~#
```

Con el comando “nmap -sU -sT (ip deseada)” se escanea los puertos tcp y udp.

28. Escaneo de puertos sin ping:


A terminal window titled 'debianjuan@10: ~' showing the output of an nmap scan. The command executed is 'nmap -Pn 192.168.56.1'. The output indicates the host is up and lists several open ports with their corresponding services.

```
root@10:~# nmap -Pn 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:48 -05
Nmap scan report for 192.168.56.1 (192.168.56.1)
Host is up (0.0047s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsapi

Nmap done: 1 IP address (1 host up) scanned in 5.56 seconds
root@10:~#
```

Con el comando “nmap -Pn (ip deseada)” se verifica los puertos que no tengan ping en la conexión.

29. Escaneo de puertos en una subred:

A terminal window titled 'debianjuan@10: ~' showing an nmap command for a subnet. The command is 'nmap 192.168.1.15/192.168.1.15', which is incorrect for scanning a range of IP addresses. The output shows a warning and that no targets were scanned.

```
root@10:~# nmap 192.168.1.15/192.168.1.15
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:52 -05
Unable to split netmask from target expression: "192.168.1.15/192.168.1.15"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@10:~#
```

Con el comando “nmap (ip 1)/(ip 2)” para realizar un escaneo de los puertos en una subred.

30. Escaneo de puertos y detección de sistemas operativos con detalles detallados:

```
debianjuanj@10: ~
root@10:~# nmap -v -O 191.168.1.15
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:50 -05
Initiating Ping Scan at 17:50
Scanning 191.168.1.15 [4 ports]
Completed Ping Scan at 17:50, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:50
Completed Parallel DNS resolution of 1 host. at 17:50, 0.48s elapsed
Initiating SYN Stealth Scan at 17:50
Scanning 15.1.168.191.isp.timbrasil.com.br (191.168.1.15) [1000 ports]
Completed SYN Stealth Scan at 17:50, 4.43s elapsed (1000 total ports)
Initiating OS detection (try #1) against 15.1.168.191.isp.timbrasil.com.br (191.168.1.15)
Retrying OS detection (try #2) against 15.1.168.191.isp.timbrasil.com.br (191.168.1.15)
Nmap scan report for 15.1.168.191.isp.timbrasil.com.br (191.168.1.15)
Host is up (0.0022s latency).
All 1000 scanned ports on 15.1.168.191.isp.timbrasil.com.br (191.168.1.15) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Con el comando “nmap -v -O (ip deseada)” con este comando se realiza el escaneo y la verificación entre las conexiones de los SO.

31. Escaneo de puertos con detección de firewall y detalles

destacados:

```
debianjuanj@10: ~
root@10:~# nmap -v -sA 192.168.1.15
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 17:54 -05
Initiating Ping Scan at 17:54
Scanning 192.168.1.15 [4 ports]
Completed Ping Scan at 17:54, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:54
Completed Parallel DNS resolution of 1 host. at 17:54, 0.00s elapsed
Initiating ACK Scan at 17:54
Scanning 192.168.1.15 (192.168.1.15) [1000 ports]
Completed ACK Scan at 17:54, 0.28s elapsed (1000 total ports)
Nmap scan report for 192.168.1.15 (192.168.1.15)
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.15 (192.168.1.15) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
root@10:~#
```

Con el comando `nmap -v -sA (ip deseada)` con este comando se escanea los puertos de detección firewall y detalles varios.

32. Determinar la información de un puerto (port = número de puerto):

```
debianjuanj@10: ~
root@10:~# cat /etc/services | grep 661
root@10:~#
```

Con el comando `cat /etc/services grep 661` se realiza el obtencion de informacion de un puerto que se designa por el usuario.