

Laboratorio 2

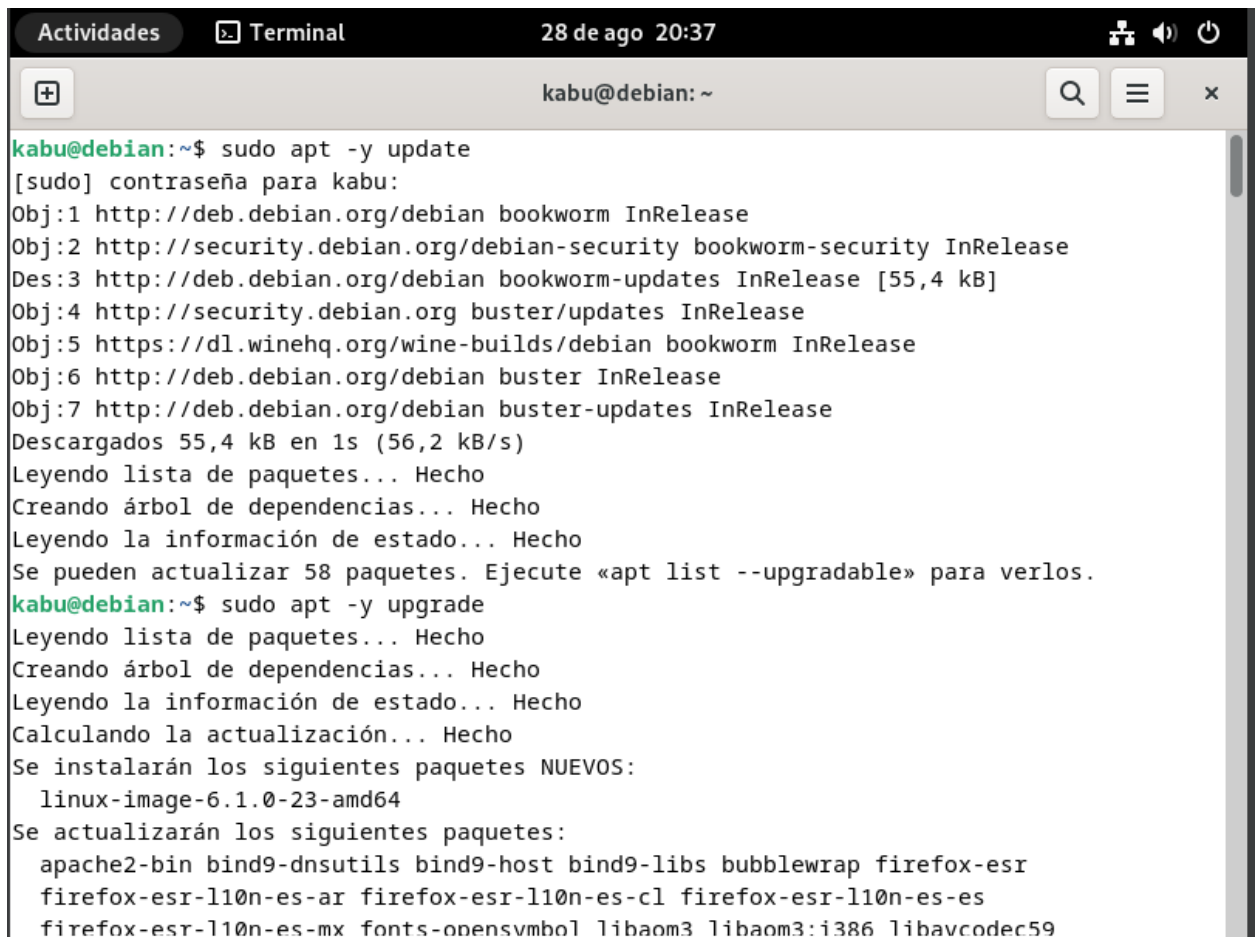
Nombre: Hugo Armijos

Fecha: 28/08/2024

1. Actualizamos los paquetes con los comandos “**sudo apt -y update**” y “**sudo apt -y upgrade**” esto nos permite tener nuestro sistema operativo actualizado y evitarnos problemas, siendo generalmente actualizados desde el repositorio de Linux.

Ilustración 1

Actualización del sistema



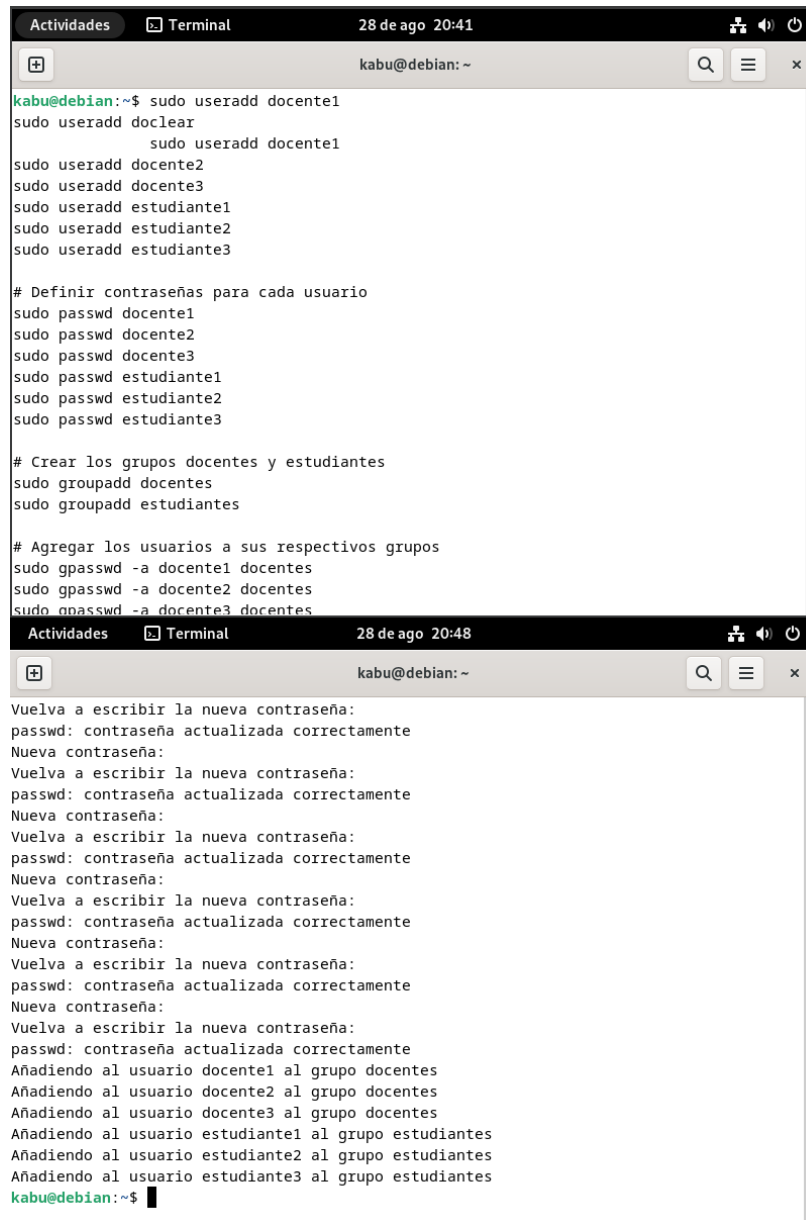
```
kabu@debian: ~$ sudo apt -y update
[sudo] contraseña para kabu:
Obj:1 http://deb.debian.org/debian bookworm InRelease
Obj:2 http://security.debian.org/debian-security bookworm-security InRelease
Des:3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Obj:4 http://security.debian.org buster/updates InRelease
Obj:5 https://dl.winehq.org/wine-builds/debian bookworm InRelease
Obj:6 http://deb.debian.org/debian buster InRelease
Obj:7 http://deb.debian.org/debian buster-updates InRelease
Descargados 55,4 kB en 1s (56,2 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 58 paquetes. Ejecute «apt list --upgradable» para verlos.
kabu@debian:~$ sudo apt -y upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  linux-image-6.1.0-23-amd64
Se actualizarán los siguientes paquetes:
  apache2-bin bind9-dnsutils bind9-host bind9-libs bubblewrap firefox-esr
  firefox-esr-l10n-es-ar firefox-esr-l10n-es-cl firefox-esr-l10n-es-es
  firefox-esr-l10n-es-mx fonts-opensymbol libaom3 libaom3:i386 libavcodec59
```

Nota autoría propia

2. Usamos el comando “**sudo useradd <nombre_usuario>**” para crear un nuevo usuario, luego con el comando “**sudo passwd <nombre_usuario>**” para agregar contraseñas a cada usuario y finalmente lo agregamos al grupo usando el comando “**sudo gpasswd -a <nombre_usuario> <nombre_grupo>**”.

Ilustración 2

Creación usuarios



The image shows two screenshots of a terminal window on a Debian system. The top screenshot, taken at 20:41, shows the execution of commands to create users and groups. The bottom screenshot, taken at 20:48, shows the password setting process for the created users.

```
kabu@debian: ~  
kabu@debian:~$ sudo useradd docente1  
sudo useradd doclear  
          sudo useradd docente1  
sudo useradd docente2  
sudo useradd docente3  
sudo useradd estudiante1  
sudo useradd estudiante2  
sudo useradd estudiante3  
  
# Definir contraseñas para cada usuario  
sudo passwd docente1  
sudo passwd docente2  
sudo passwd docente3  
sudo passwd estudiante1  
sudo passwd estudiante2  
sudo passwd estudiante3  
  
# Crear los grupos docentes y estudiantes  
sudo groupadd docentes  
sudo groupadd estudiantes  
  
# Agregar los usuarios a sus respectivos grupos  
sudo gpasswd -a docente1 docentes  
sudo gpasswd -a docente2 docentes  
sudo gpasswd -a docente3 docentes
```

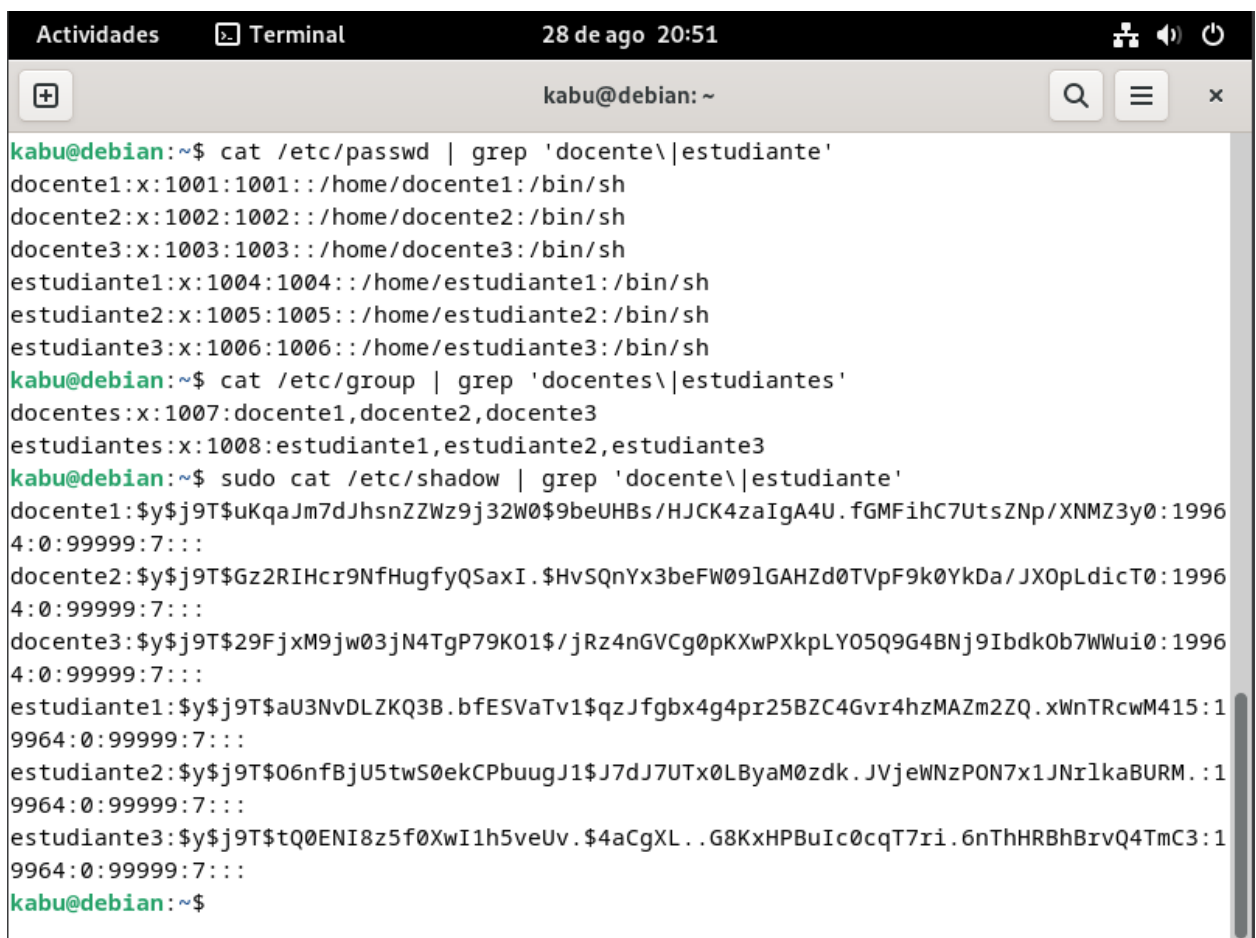
```
kabu@debian: ~  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
Nueva contraseña:  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
Nueva contraseña:  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
Nueva contraseña:  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
Nueva contraseña:  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
Nueva contraseña:  
Vuelva a escribir la nueva contraseña:  
passwd: contraseña actualizada correctamente  
Añadiendo al usuario docente1 al grupo docentes  
Añadiendo al usuario docente2 al grupo docentes  
Añadiendo al usuario docente3 al grupo docentes  
Añadiendo al usuario estudiante1 al grupo estudiantes  
Añadiendo al usuario estudiante2 al grupo estudiantes  
Añadiendo al usuario estudiante3 al grupo estudiantes  
kabu@debian:~$
```

Nota autoría propia

- Se verifican la creación de usuarios y de los grupos, usando los comandos “**cat /etc/passwd | grep '<nombre>'**” esta muestra la información básica de los usuarios, “**cat /etc/group | grep '<nombre_grupo>'**”, esta almacena información de todos los grupos del sistema, “**sudo cat /etc/shadow | grep '<nombre_usuario>'**” contiene las contraseñas encriptadas.

Ilustración 3

Verificación de grupos



```
Actividades Terminal 28 de ago 20:51
kabu@debian: ~
kabu@debian:~$ cat /etc/passwd | grep 'docente\|estudiante'
docente1:x:1001:1001::/home/docente1:/bin/sh
docente2:x:1002:1002::/home/docente2:/bin/sh
docente3:x:1003:1003::/home/docente3:/bin/sh
estudiante1:x:1004:1004::/home/estudiante1:/bin/sh
estudiante2:x:1005:1005::/home/estudiante2:/bin/sh
estudiante3:x:1006:1006::/home/estudiante3:/bin/sh
kabu@debian:~$ cat /etc/group | grep 'docentes\|estudiantes'
docentes:x:1007:docente1,docente2,docente3
estudiantes:x:1008:estudiante1,estudiante2,estudiante3
kabu@debian:~$ sudo cat /etc/shadow | grep 'docente\|estudiante'
docente1:$y$j9T$uKqaJm7dJhsnZZWz9j32W0$9beUHBs/HJCK4zaIgA4U.fGMFihC7UtsZNP/XNMZ3y0:19964:0:99999:7:::
docente2:$y$j9T$Gz2RIHcr9NfHugfyQSaxI.$HvSQnYx3beFW09lGAHZd0TVpF9k0YkDa/JX0pLdicT0:19964:0:99999:7:::
docente3:$y$j9T$29FjxM9jw03jN4TgP79K01$/jRz4nGVCg0pKXwPXkpLY05Q9G4BNj9Ibdk0b7WWui0:19964:0:99999:7:::
estudiante1:$y$j9T$aU3NvDLZKQ3B.bfESVaTv1$qzJfgbx4g4pr25BZC4Gvr4hzMAZm2ZQ.xWnTRcwM415:19964:0:99999:7:::
estudiante2:$y$j9T$06nfBjU5twS0ekCPbuugJ1$J7dJ7UTx0LByaM0zdk.JVjeWNzPON7x1JNrlkaBURM.:19964:0:99999:7:::
estudiante3:$y$j9T$tQ0ENI8z5f0XwI1h5veUv.$4aCgXL..G8KxHPBuIc0cqT7ri.6nThHRBhBrvQ4TmC3:19964:0:99999:7:::
kabu@debian:~$
```

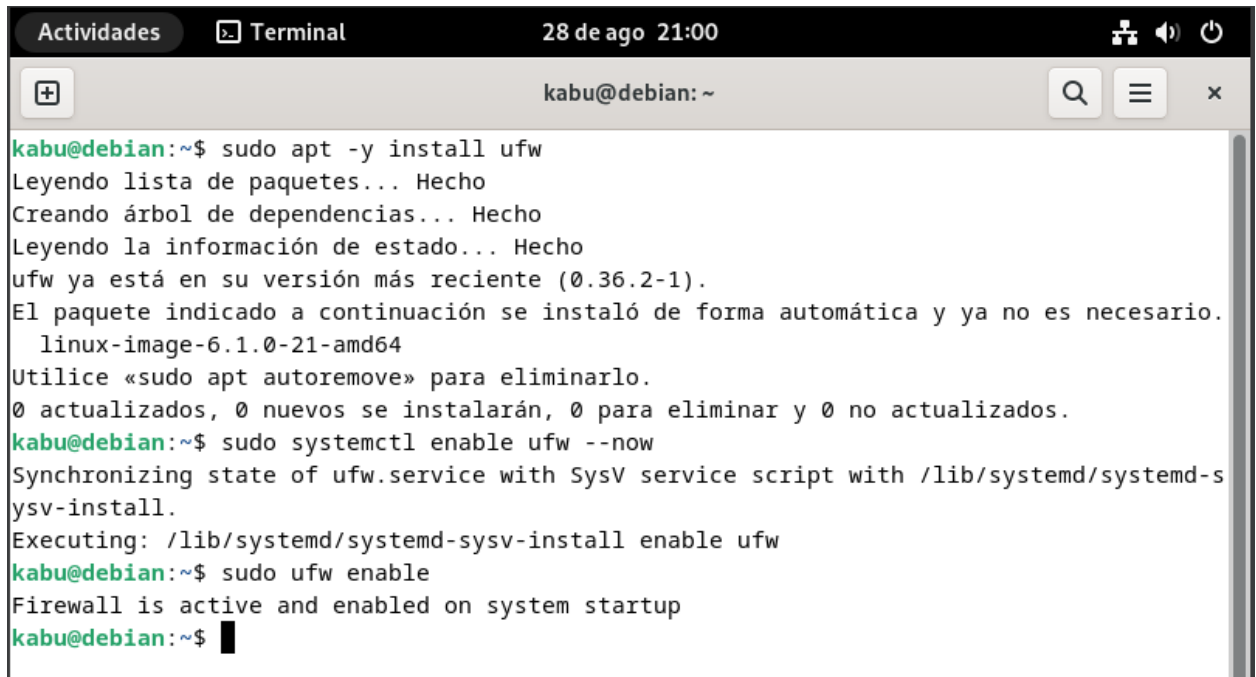
Nota autoría propia

- “**sudo apt -y install ufw**” con este comando instalamos el comando ufw, para luego habilitarlo con el comando “**sudo systemctl enable ufw --now**”, esto nos permite iniciar

el comando automáticamente, “**sudo ufw enable**”, activa el firewall que comienza filtrar el tráfico.

Ilustración 4

Configuración ufw

A screenshot of a Linux terminal window. The window title bar shows 'Actividades', 'Terminal', and the date/time '28 de ago 21:00'. The terminal prompt is 'kabu@debian: ~'. The user enters the command 'sudo apt -y install ufw'. The output shows that ufw is already installed and up-to-date. Then, the user enters 'sudo systemctl enable ufw --now', and the output shows the service being enabled. Finally, the user enters 'sudo ufw enable', and the output shows the firewall is active and enabled on system startup. The terminal ends with the prompt 'kabu@debian:~\$' and a cursor.

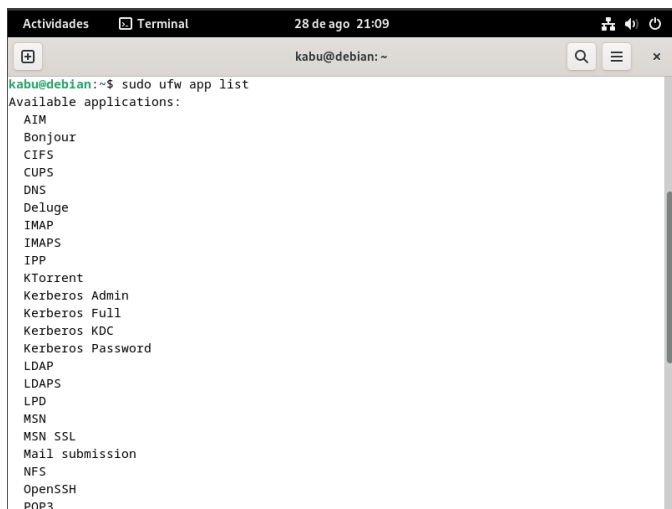
```
kabu@debian:~$ sudo apt -y install ufw
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
ufw ya está en su versión más reciente (0.36.2-1).
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  linux-image-6.1.0-21-amd64
Utilice «sudo apt autoremove» para eliminarlo.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
kabu@debian:~$ sudo systemctl enable ufw --now
Synchronizing state of ufw.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ufw
kabu@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
kabu@debian:~$
```

Nota autoría propia

5. Usamos el comando “**sudo ufw app list**” nos muestra la aplicaciones o servicios que ufw reconoce y tiene reglas de firewall.

Ilustración 5

Mostrar lista



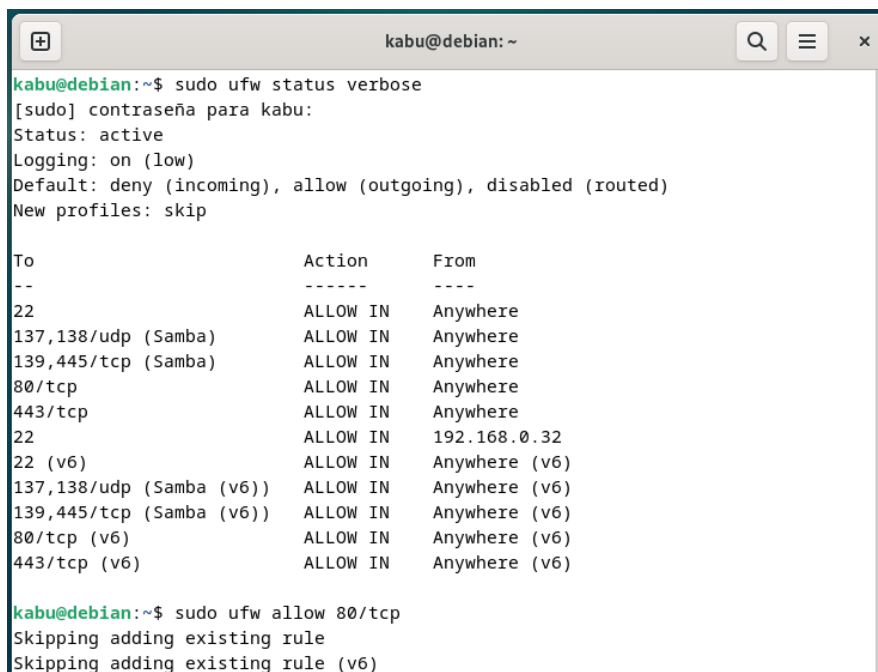
```
Actividades Terminal 28 de ago 21:09
kabu@debian: ~
kabu@debian:~$ sudo ufw app list
Available applications:
AIM
Bonjour
CIFS
CUPS
DNS
Deluge
IMAP
IMAPS
IPP
KTorrent
Kerberos Admin
Kerberos Full
Kerberos KDC
Kerberos Password
LDAP
LDAPS
LPD
MSN
MSN SSL
Mail submission
NFS
OpenSSH
POP3
```

Nota autoría propia

6. Para obtener un estado detallado sobre el firewall usamos el comando “**sudo ufw status verbose**”, una vez analizado el firewall podemos permitir que el trafico entre mediante el puerto 80 con el comando “**sudo ufw allow 80/tcp**”

Ilustración 6

Análisis de firewall y activación de puerto



```
kabu@debian: ~
kabu@debian:~$ sudo ufw status verbose
[sudo] contraseña para kabu:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22 ALLOW IN Anywhere
137,138/udp (Samba) ALLOW IN Anywhere
139,445/tcp (Samba) ALLOW IN Anywhere
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
22 ALLOW IN 192.168.0.32
22 (v6) ALLOW IN Anywhere (v6)
137,138/udp (Samba (v6)) ALLOW IN Anywhere (v6)
139,445/tcp (Samba (v6)) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
443/tcp (v6) ALLOW IN Anywhere (v6)

kabu@debian:~$ sudo ufw allow 80/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
```

Nota autoría propia

7. Para permitir el tráfico desde diferentes puntos de red tenemos los comandos “**sudo ufw allow 443/tcp**” este nos permite admitir tráfico desde el puerto 443, también podemos permitir tráfico por 1 puerto en específico desde 1 sola ip con el comando “**sudo ufw allow from <dirección_IP> to any port 22**”, este mismo comando también se puede aplicar para una subred con un ligero cambio “**sudo ufw allow from <subred>/<máscara> to any port 22**”, también con los comandos “**sudo ufw allow from <subred>/<máscara> to any port 22**,” **sudo ufw default deny incoming**” y “**sudo ufw default deny outgoing**”, podemos permitir la salida de tráfico, denegar la entrada de tráfico y denegar todo el tráfico saliente.

Ilustración 7

Configuración de puertos

```
kabu@debian:~$ sudo ufw allow 443/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
kabu@debian:~$ sudo ufw allow from 190.162.0.32 to any port 22
Rule added
kabu@debian:~$ sudo ufw allow from 190.162.0.32/24 to any port 22
WARN: Rule changed after normalization
Rule added
kabu@debian:~$ sudo ufw allow out 443/tcp
Rule added
Rule added (v6)
kabu@debian:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
kabu@debian:~$ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
kabu@debian:~$
```

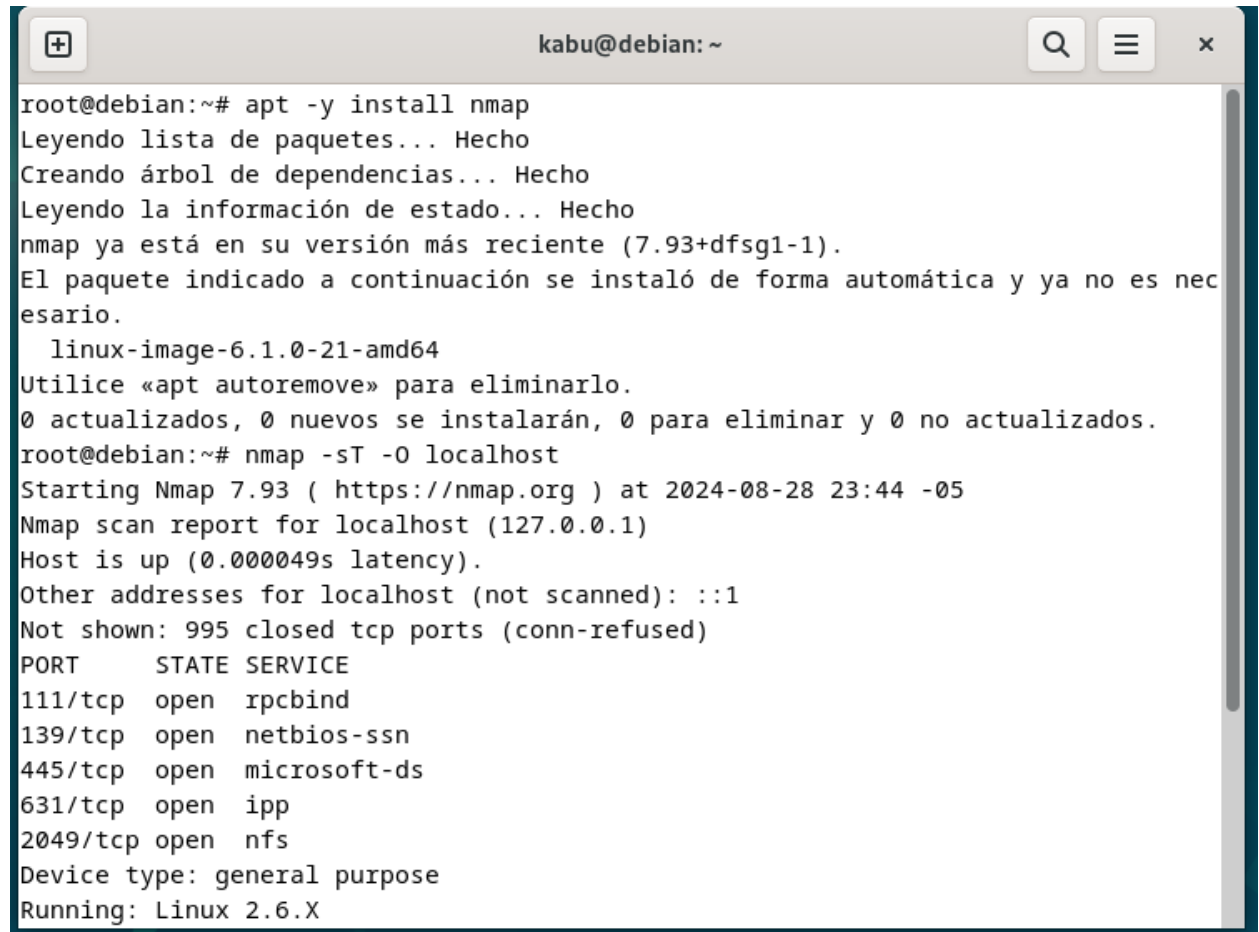
Nota autoría propia

8. Para instalar nmap, usamos el comando “**sudo apt -y install nmap**”, la cual es una herramienta para escanear redes e identificar los puertos abiertos, para esta tarea usamos

el comando “**nmap -sT -O localhost**”, el cual realiza un escaneo de los puertos detectados en el SO.

Ilustración 8

Instalación y escaneo de nmap



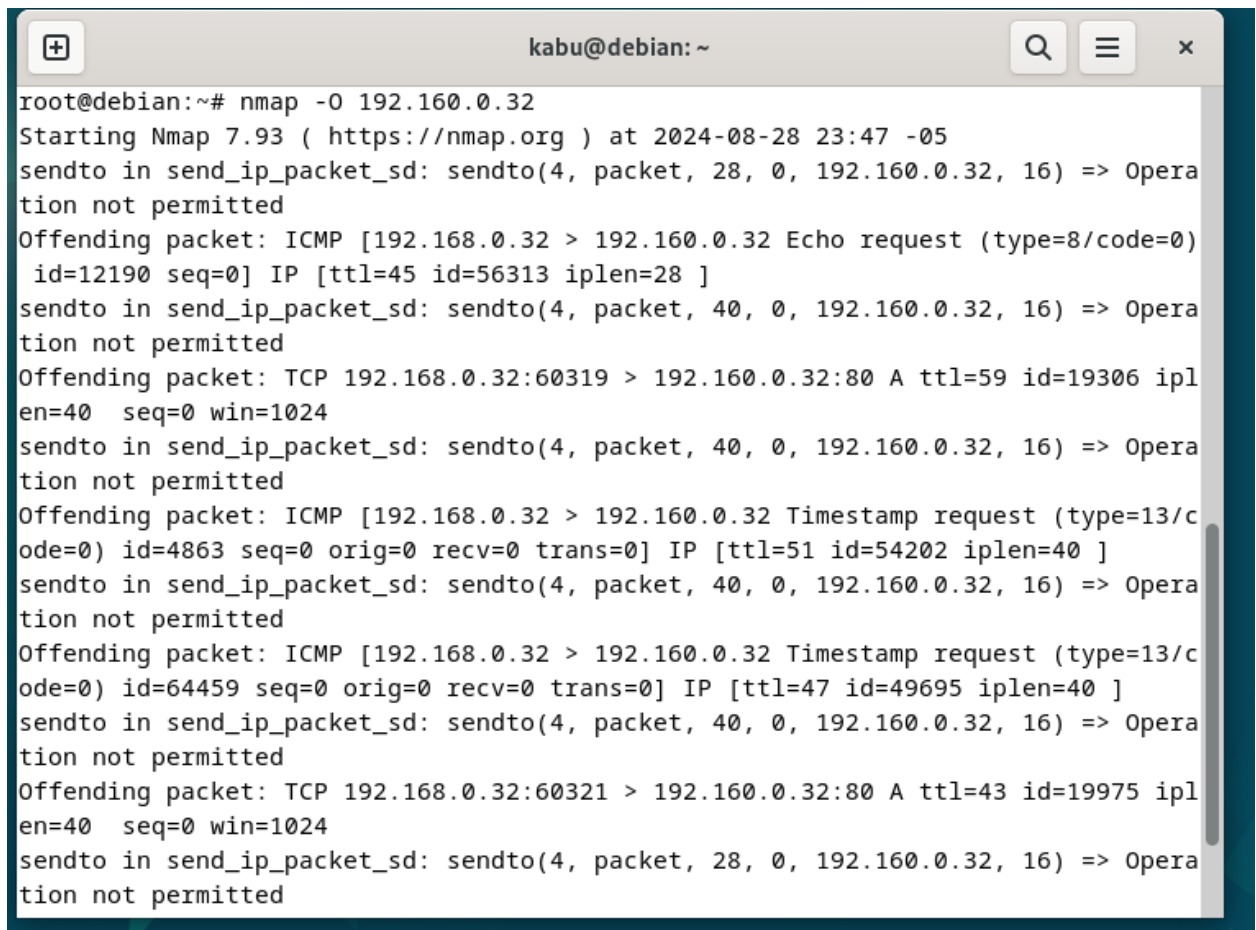
```
kabu@debian: ~  
root@debian:~# apt -y install nmap  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
nmap ya está en su versión más reciente (7.93+dfsg1-1).  
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.  
  linux-image-6.1.0-21-amd64  
Utilice «apt autoremove» para eliminarlo.  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
root@debian:~# nmap -sT -O localhost  
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-28 23:44 -05  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000049s latency).  
Other addresses for localhost (not scanned): ::1  
Not shown: 995 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
631/tcp   open  ipp  
2049/tcp  open  nfs  
Device type: general purpose  
Running: Linux 2.6.X
```

Nota autoría propia

9. Escanea una IP específica y busca determinar el sistema operativo Host con el comando “**nmap -O <ip_address>**”.

Ilustración 9

Escaneo de ip específica

A terminal window titled 'kabu@debian: ~' showing the output of the command 'nmap -O 192.160.0.32'. The output displays the start of an Nmap scan at 2024-08-28 23:47 -05. It shows several failed attempts to send packets to 192.160.0.32: an ICMP Echo request (type=8/code=0), an ICMP Timestamp request (type=13/code=0), and a TCP packet (A ttl=59 id=19306 iplen=40 seq=0 win=1024). Each attempt results in 'sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted'.

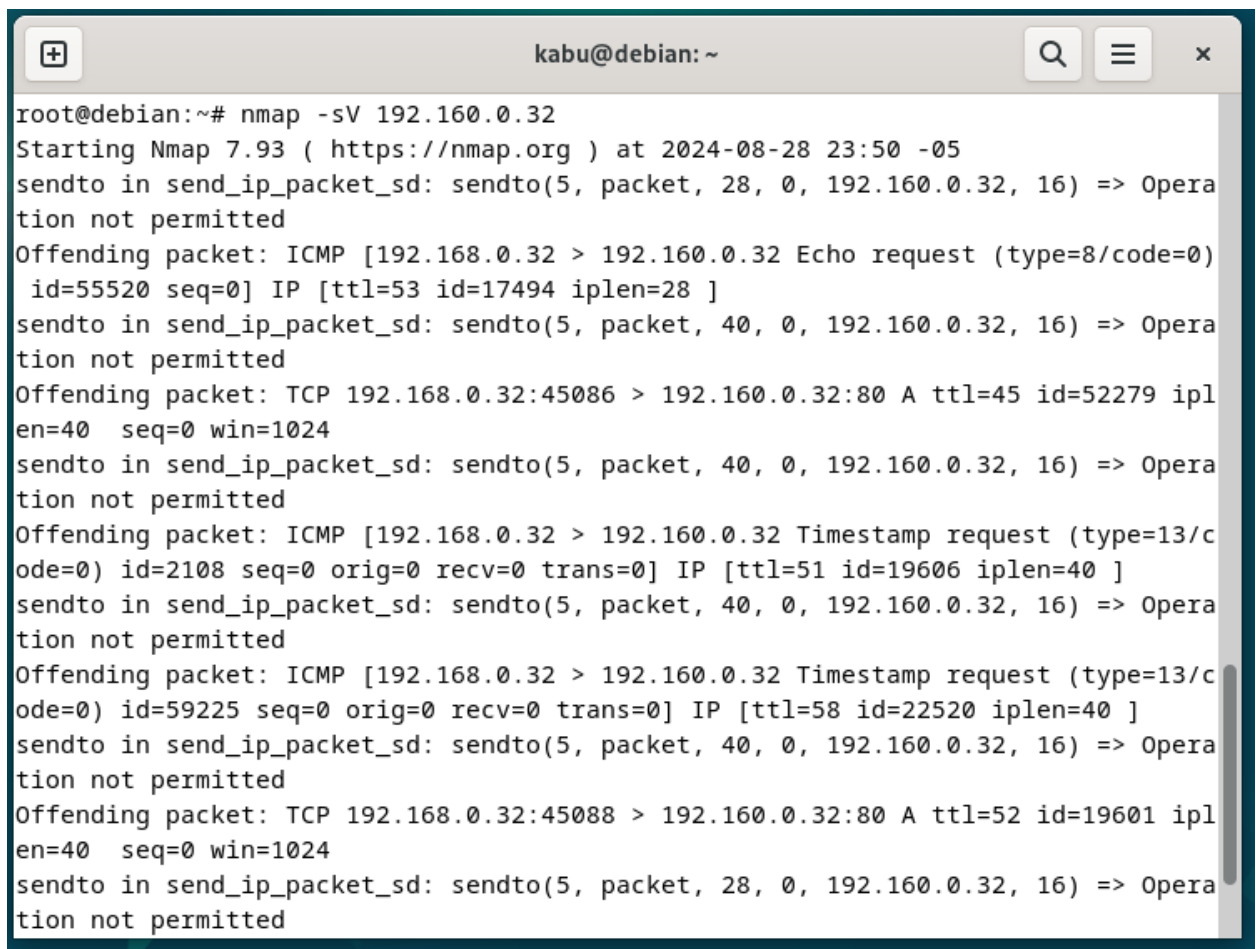
```
root@debian:~# nmap -O 192.160.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-28 23:47 -05
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Echo request (type=8/code=0) id=12190 seq=0] IP [ttl=45 id=56313 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:60319 > 192.160.0.32:80 A ttl=59 id=19306 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=4863 seq=0 orig=0 recv=0 trans=0] IP [ttl=51 id=54202 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=64459 seq=0 orig=0 recv=0 trans=0] IP [ttl=47 id=49695 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:60321 > 192.160.0.32:80 A ttl=43 id=19975 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
```

Nota autoría propia

10. Escanea una IP específica y busca determinar las versiones de los servicios que están corriendo en esos puertos “**nmap -sV <ip_address>**”.

Ilustración 10

Escaneo de servicios

A terminal window titled 'kabu@debian: ~' showing the output of the command 'nmap -sV 192.160.0.32'. The output indicates that Nmap 7.93 is starting at 2024-08-28 23:50 -05. It shows several failed attempts to send packets to the target IP. The first attempt is an ICMP Echo request (type=8/code=0) with id=55520 and seq=0, which fails with 'Operation not permitted'. The second attempt is a TCP packet (192.168.0.32:45086 to 192.160.0.32:80) with ttl=45, id=52279, and iplen=40, which also fails with 'Operation not permitted'. The third attempt is an ICMP Timestamp request (type=13/code=0) with id=2108, seq=0, orig=0, recv=0, and trans=0, which fails with 'Operation not permitted'. The fourth attempt is another ICMP Timestamp request (type=13/code=0) with id=59225, seq=0, orig=0, recv=0, and trans=0, which fails with 'Operation not permitted'. The fifth attempt is a TCP packet (192.168.0.32:45088 to 192.160.0.32:80) with ttl=52, id=19601, and iplen=40, which fails with 'Operation not permitted'.

```
root@debian:~# nmap -sV 192.160.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-28 23:50 -05
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Echo request (type=8/code=0) id=55520 seq=0] IP [ttl=53 id=17494 iplen=28 ]
sendto in send_ip_packet_sd: sendto(5, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:45086 > 192.160.0.32:80 A ttl=45 id=52279 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(5, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=2108 seq=0 orig=0 recv=0 trans=0] IP [ttl=51 id=19606 iplen=40 ]
sendto in send_ip_packet_sd: sendto(5, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=59225 seq=0 orig=0 recv=0 trans=0] IP [ttl=58 id=22520 iplen=40 ]
sendto in send_ip_packet_sd: sendto(5, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:45088 > 192.160.0.32:80 A ttl=52 id=19601 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(5, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
```

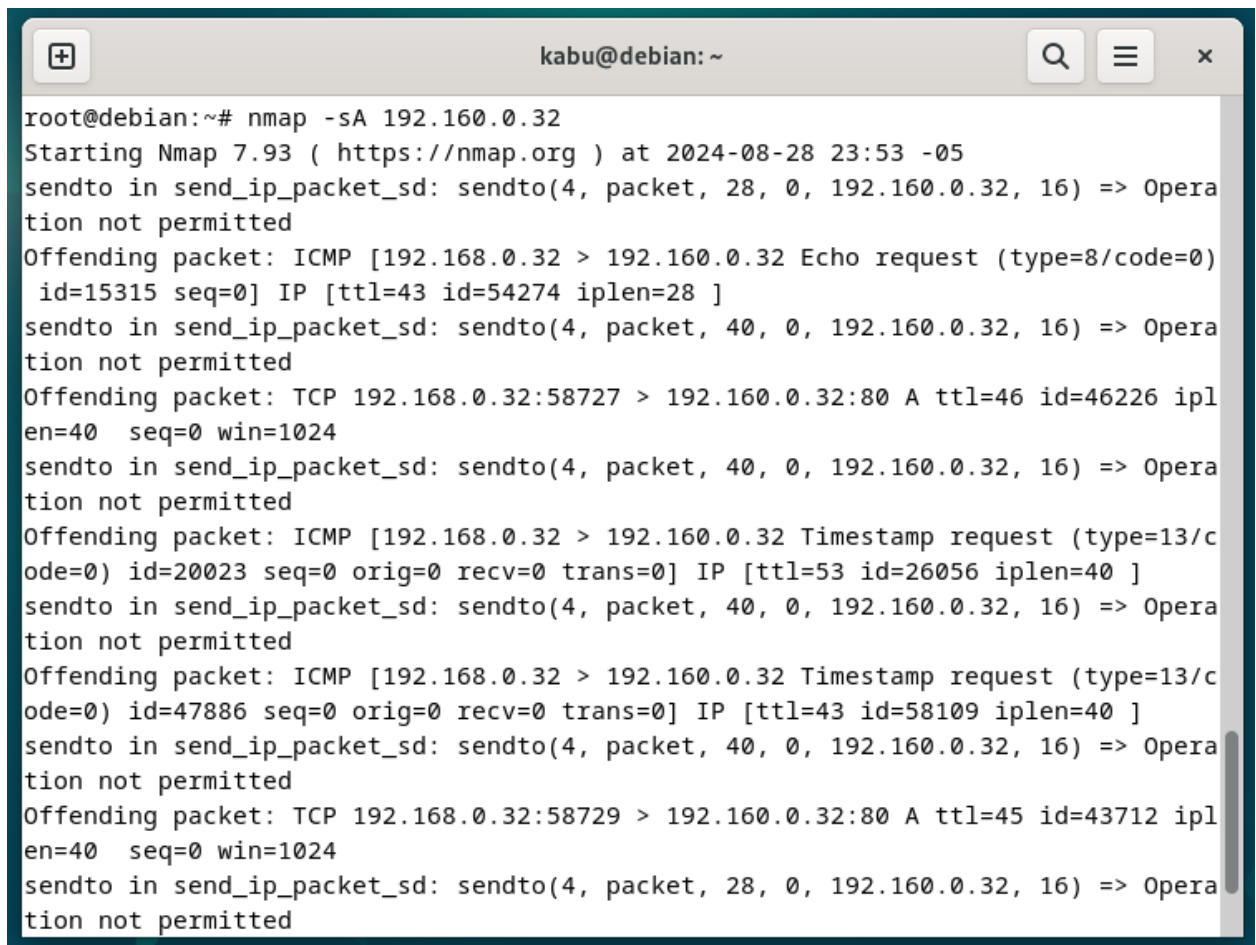
Nota autoría propia

11. Escanea una IP específica y busca determinar la presencia de firewalls y su configuración

“nmap -sA <ip_address>”

Ilustración 11

Escaneo de firewall

A terminal window titled 'kabu@debian: ~' showing the output of the command 'nmap -sA 192.160.0.32'. The output indicates that the scan is being performed at 2024-08-28 23:53 -05. It shows several attempts to send packets to the target IP, but all are blocked with the message 'Operation not permitted'. The blocked packets include ICMP Echo requests, ICMP Timestamp requests, and TCP SYN packets. The terminal text is as follows:

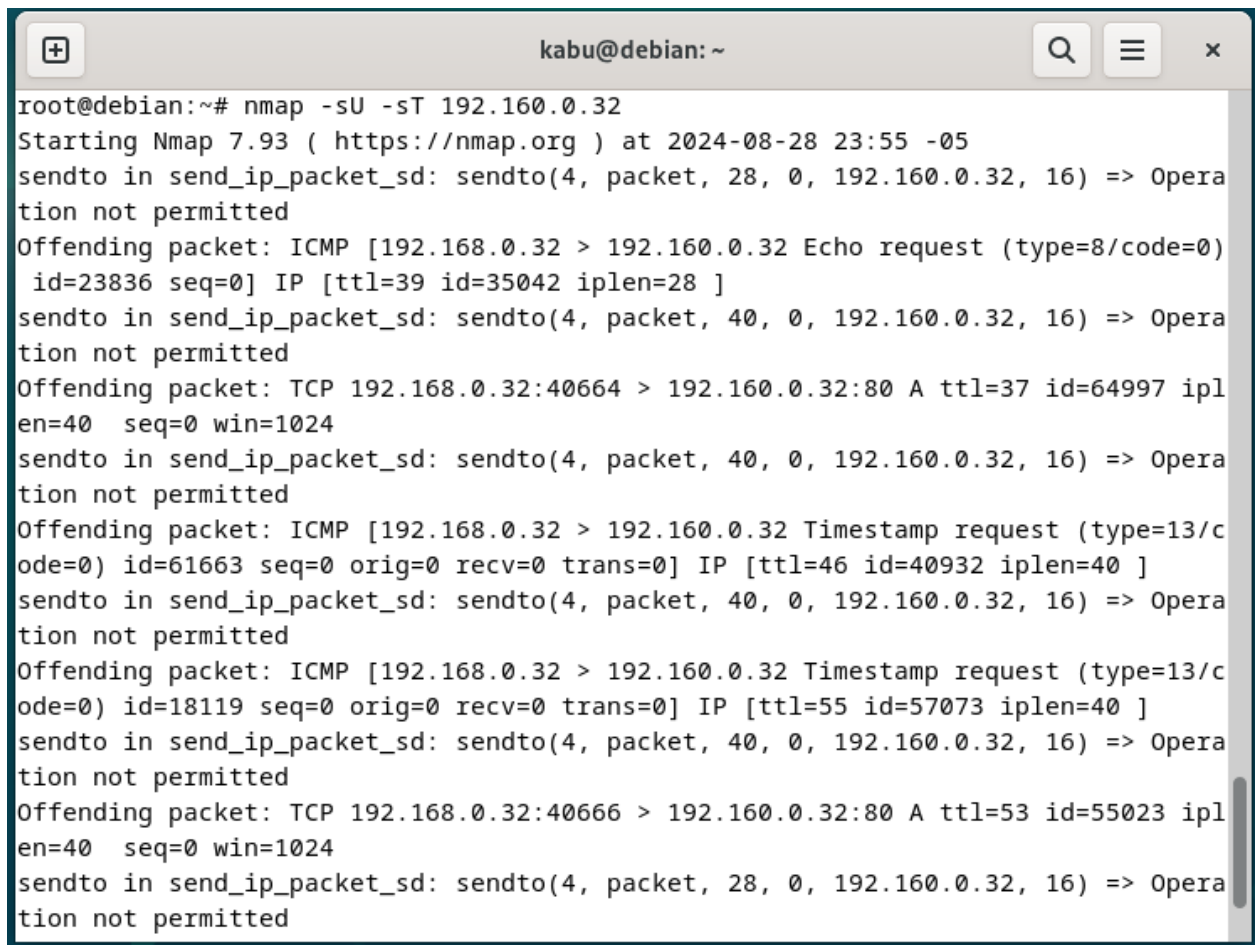
```
root@debian:~# nmap -sA 192.160.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-28 23:53 -05
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Echo request (type=8/code=0) id=15315 seq=0] IP [ttl=43 id=54274 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:58727 > 192.160.0.32:80 A ttl=46 id=46226 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=20023 seq=0 orig=0 recv=0 trans=0] IP [ttl=53 id=26056 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=47886 seq=0 orig=0 recv=0 trans=0] IP [ttl=43 id=58109 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:58729 > 192.160.0.32:80 A ttl=45 id=43712 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
```

Nota autoría propia

12. Escanea una IP específica, indagando en los puertos UDP y TCP “**nmap -sU -sT**
<ip_address>”

Ilustración 12

Escaneo de UDP y TCP



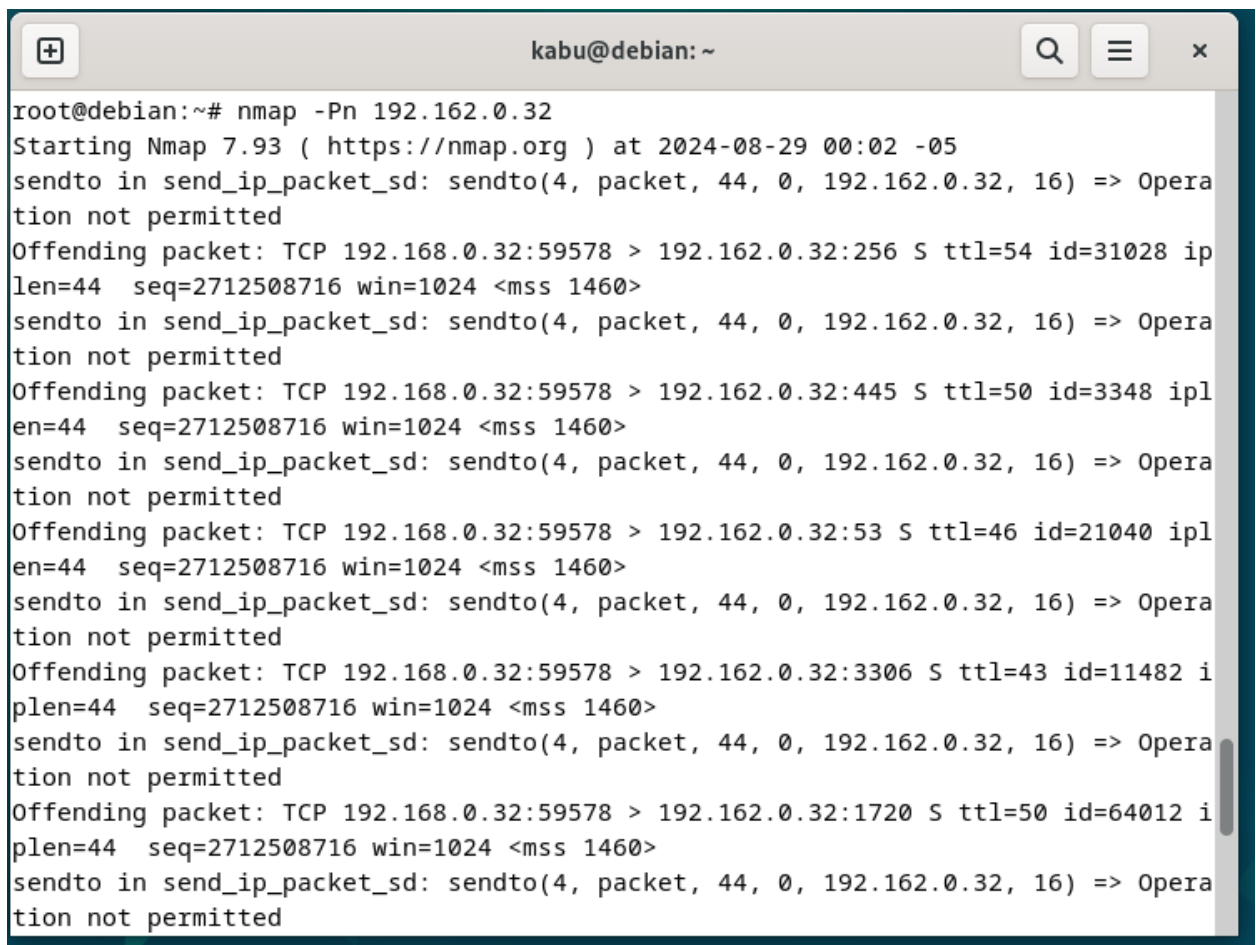
```
kabu@debian: ~
root@debian:~# nmap -sU -sT 192.160.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-28 23:55 -05
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Echo request (type=8/code=0) id=23836 seq=0] IP [ttl=39 id=35042 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:40664 > 192.160.0.32:80 A ttl=37 id=64997 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=61663 seq=0 orig=0 recv=0 trans=0] IP [ttl=46 id=40932 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=18119 seq=0 orig=0 recv=0 trans=0] IP [ttl=55 id=57073 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:40666 > 192.160.0.32:80 A ttl=53 id=55023 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
```

Nota autoría propia

13. Escanea una IP específica, sin enviar un ping antes “**nmap -Pn <ip_address>**”

Ilustración 13

Escaneo sin ping

A terminal window titled 'kabu@debian: ~' showing the output of the command 'nmap -Pn 192.162.0.32'. The output indicates that the operation is not permitted for several TCP ports (256, 445, 53, 3306, 1720) because the source IP (192.168.0.32) is not in the target's subnet (192.162.0.32).

```
root@debian:~# nmap -Pn 192.162.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 00:02 -05
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 192.162.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:59578 > 192.162.0.32:256 S ttl=54 id=31028 ip len=44 seq=2712508716 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 192.162.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:59578 > 192.162.0.32:445 S ttl=50 id=3348 ip len=44 seq=2712508716 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 192.162.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:59578 > 192.162.0.32:53 S ttl=46 id=21040 ip len=44 seq=2712508716 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 192.162.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:59578 > 192.162.0.32:3306 S ttl=43 id=11482 ip len=44 seq=2712508716 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 192.162.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:59578 > 192.162.0.32:1720 S ttl=50 id=64012 ip len=44 seq=2712508716 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 192.162.0.32, 16) => Operation not permitted
```

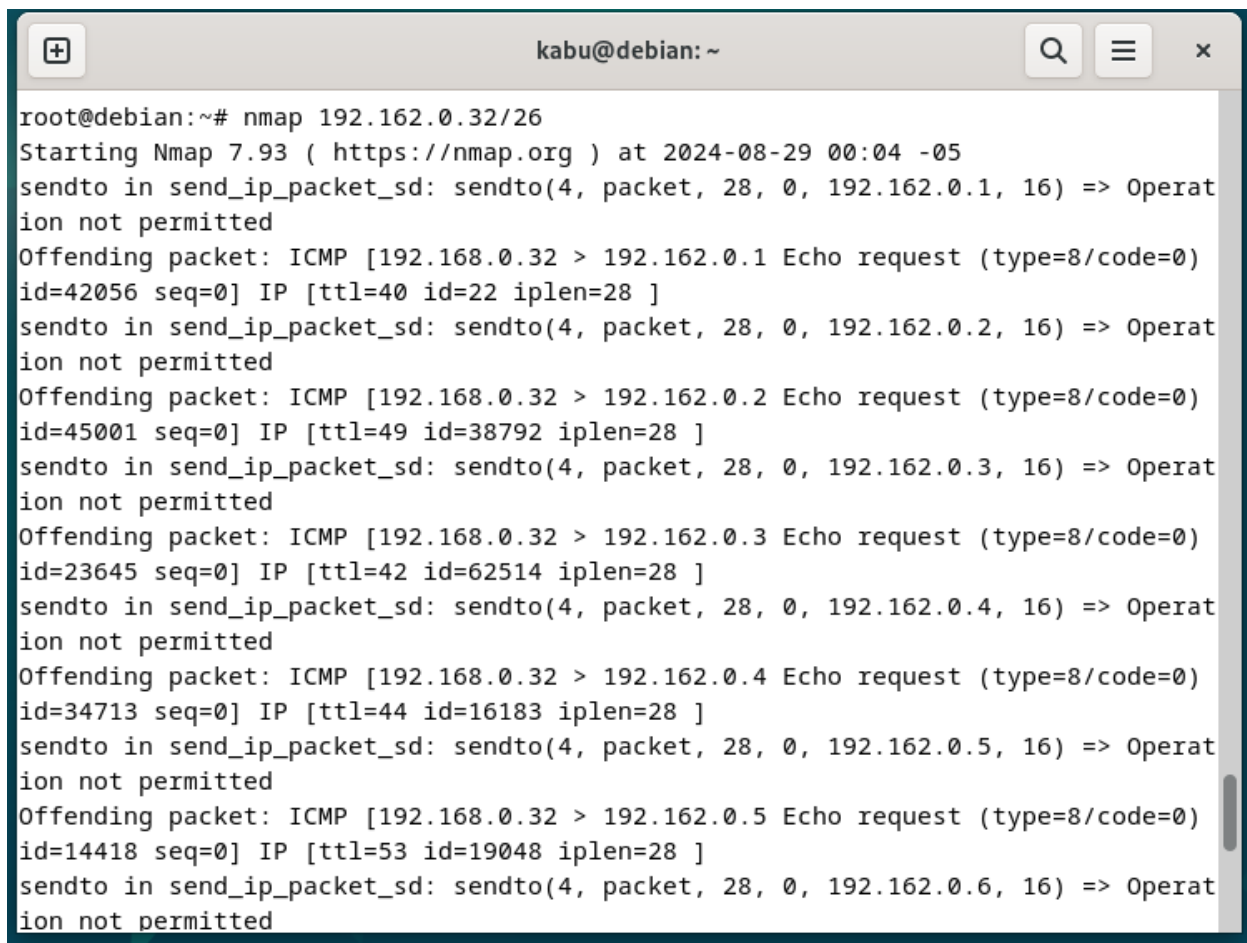
Nota autoría propia

14. Escanea todos los dispositivos en una subred específica “**nmap**

<network_address>/<subnet_mask>”

Ilustración 14

Escaneo de dispositivos

A terminal window titled 'kabu@debian: ~' showing the output of an nmap scan. The command 'nmap 192.162.0.32/26' was executed. The output shows the start of Nmap 7.93 at 2024-08-29 00:04 -05. It then displays a series of 'sendto' errors for ICMP Echo requests to various IP addresses in the 192.162.0.1 to 192.162.0.6 range, all resulting in 'Operation not permitted'. Each error message includes details about the packet, such as the source IP (192.168.0.32), destination IP, type (8), code (0), ID, sequence number, TTL, and IP length.

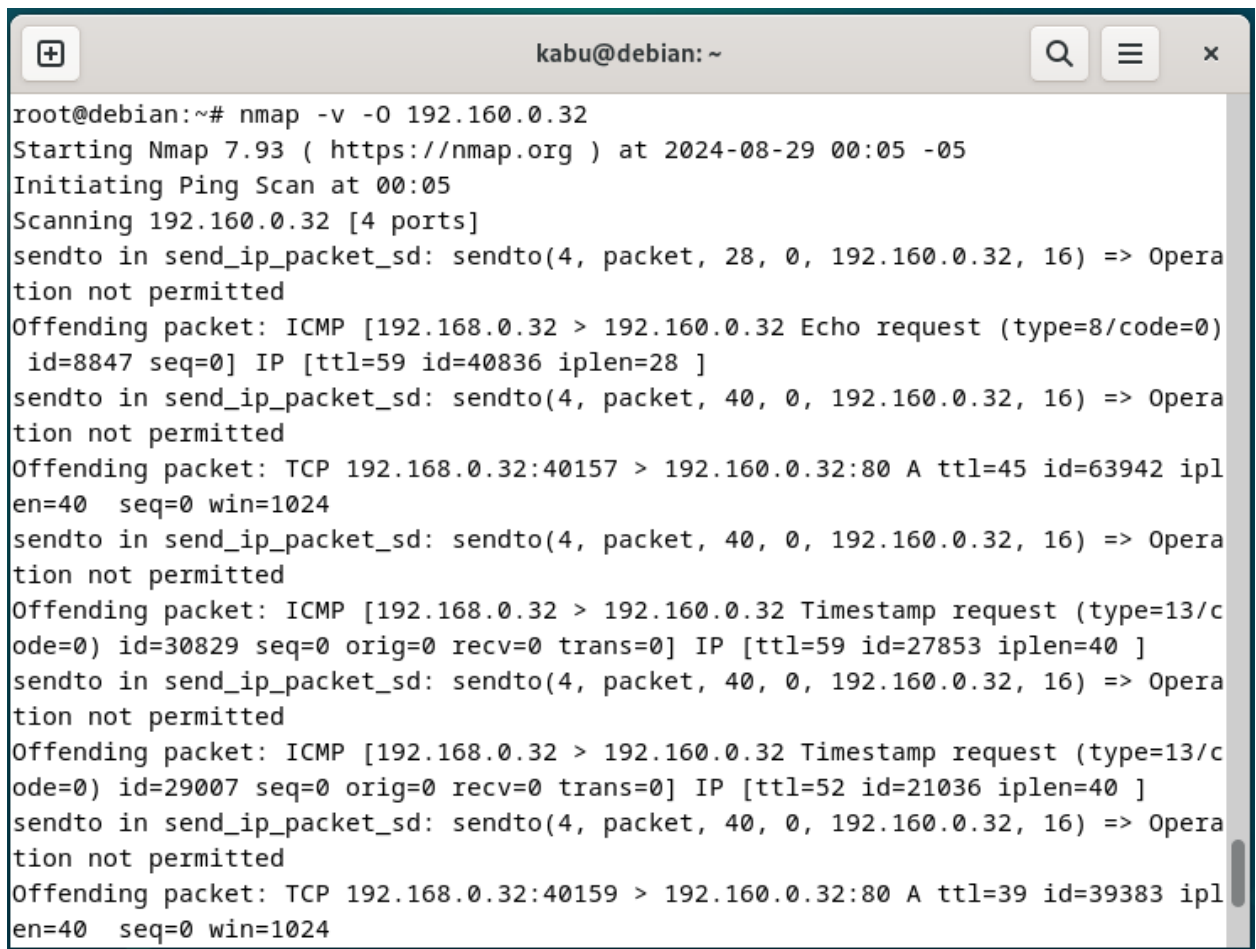
```
root@debian:~# nmap 192.162.0.32/26
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 00:04 -05
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.162.0.1, 16) => Operat
ion not permitted
Offending packet: ICMP [192.168.0.32 > 192.162.0.1 Echo request (type=8/code=0)
id=42056 seq=0] IP [ttl=40 id=22 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.162.0.2, 16) => Operat
ion not permitted
Offending packet: ICMP [192.168.0.32 > 192.162.0.2 Echo request (type=8/code=0)
id=45001 seq=0] IP [ttl=49 id=38792 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.162.0.3, 16) => Operat
ion not permitted
Offending packet: ICMP [192.168.0.32 > 192.162.0.3 Echo request (type=8/code=0)
id=23645 seq=0] IP [ttl=42 id=62514 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.162.0.4, 16) => Operat
ion not permitted
Offending packet: ICMP [192.168.0.32 > 192.162.0.4 Echo request (type=8/code=0)
id=34713 seq=0] IP [ttl=44 id=16183 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.162.0.5, 16) => Operat
ion not permitted
Offending packet: ICMP [192.168.0.32 > 192.162.0.5 Echo request (type=8/code=0)
id=14418 seq=0] IP [ttl=53 id=19048 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.162.0.6, 16) => Operat
ion not permitted
```

Nota autoría propia

15. Realiza un escaneo detallado con información extra “**nmap -v -O <ip_address>**”

Ilustración 15

Escaneo detallado

A terminal window titled 'kabu@debian: ~' showing the output of an nmap scan. The user is root@debian and has run 'nmap -v -O 192.160.0.32'. The output shows the scan starting at 2024-08-29 00:05, initiating a ping scan, and scanning 192.160.0.32 on 4 ports. It details several failed attempts to send ICMP Echo, TCP, and ICMP Timestamp requests due to 'Operation not permitted' errors. The terminal window has a standard Linux desktop interface with a title bar and window controls.

```
root@debian:~# nmap -v -O 192.160.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 00:05 -05
Initiating Ping Scan at 00:05
Scanning 192.160.0.32 [4 ports]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Echo request (type=8/code=0) id=8847 seq=0] IP [ttl=59 id=40836 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:40157 > 192.160.0.32:80 A ttl=45 id=63942 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=30829 seq=0 orig=0 recv=0 trans=0] IP [ttl=59 id=27853 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=29007 seq=0 orig=0 recv=0 trans=0] IP [ttl=52 id=21036 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:40159 > 192.160.0.32:80 A ttl=39 id=39383 iplen=40 seq=0 win=1024
```

Nota autoría propia

16. Realiza un escaneo detallado para detectar firewalls con información extra “**nmap -v -sA** **<ip_address>**”

Ilustración 16

Escaneo detallado

```
kabu@debian: ~
root@debian:~# nmap -v -sA 192.160.0.32
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 00:07 -05
Initiating Ping Scan at 00:07
Scanning 192.160.0.32 [4 ports]
sendto in send_ip_packet_sd: sendto(4, packet, 28, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Echo request (type=8/code=0) id=1198 seq=0] IP [ttl=41 id=13983 iplen=28 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:55021 > 192.160.0.32:80 A ttl=49 id=8587 iplen=40 seq=0 win=1024
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=54136 seq=0 orig=0 recv=0 trans=0] IP [ttl=43 id=2024 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: ICMP [192.168.0.32 > 192.160.0.32 Timestamp request (type=13/code=0) id=63237 seq=0 orig=0 recv=0 trans=0] IP [ttl=37 id=16643 iplen=40 ]
sendto in send_ip_packet_sd: sendto(4, packet, 40, 0, 192.160.0.32, 16) => Operation not permitted
Offending packet: TCP 192.168.0.32:55023 > 192.160.0.32:80 A ttl=39 id=2789 iplen=40 seq=0 win=1024
```

Nota autoría propia

17. Busca información sobre un puerto específico “**cat /etc/services | grep**

<número_de_puerto>”

Ilustración 17

Búsqueda puerto

```
root@debian:~# cat /etc/services | grep 22
ssh                22/tcp             # SSH Remote Login Protocol
xmpp-client        5222/tcp           jabber-client      # Jabber Client Connection
dcap               22125/tcp          # dCache Access Protocol
gsidcap            22128/tcp          # GSI dCache Access Protocol
wnn6               22273/tcp          # wnn6
root@debian:~#
```

Nota autoría propia

