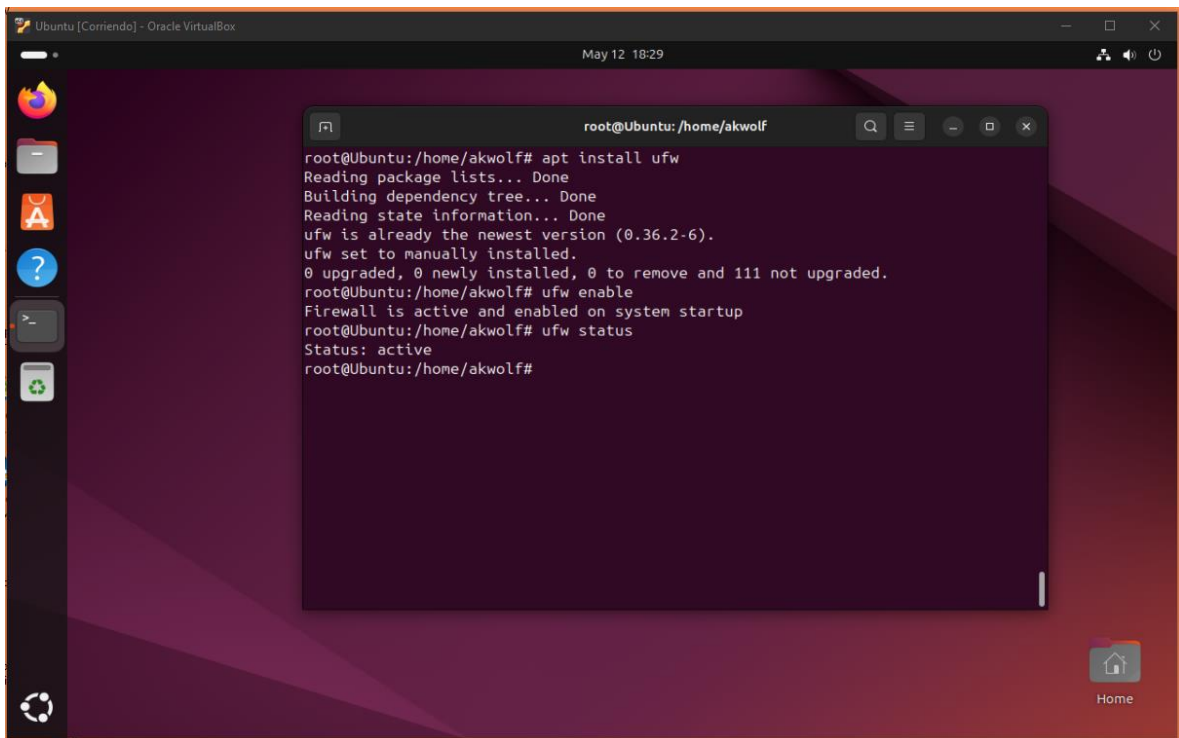
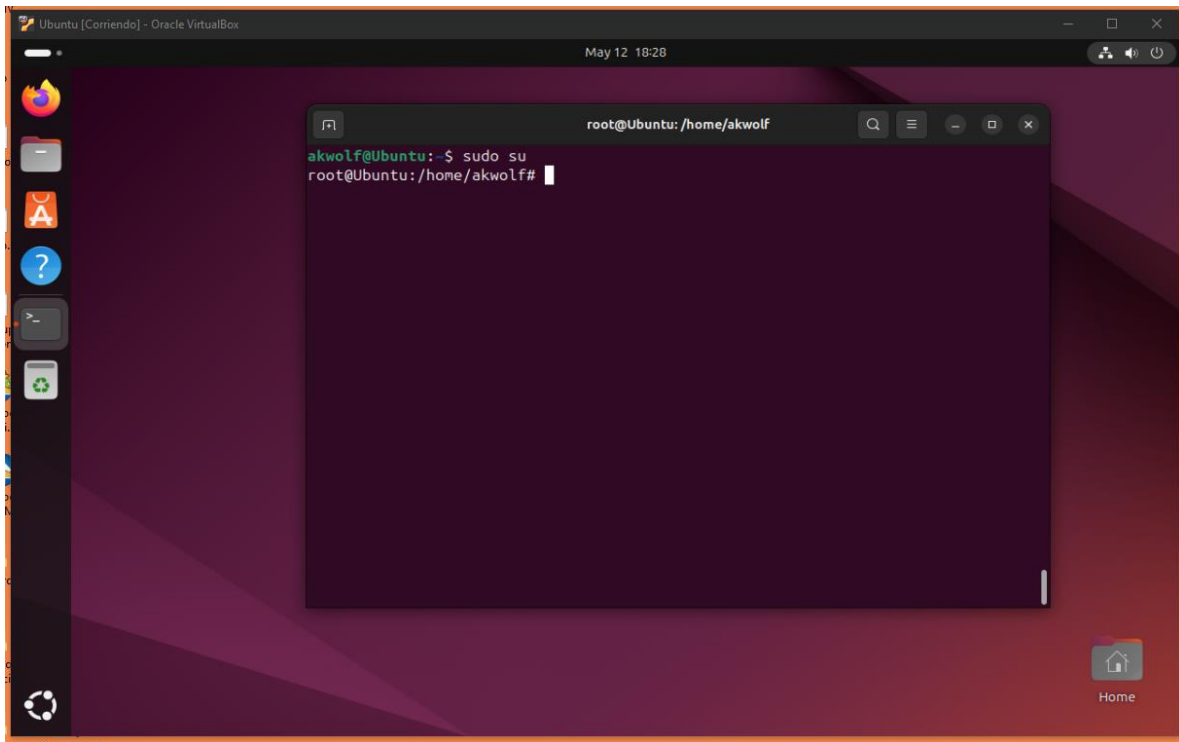


Lección - 7



```
Ubuntu [Corriendo] - Oracle VirtualBox
May 12 18:30
root@Ubuntu: /home/akwolf

root@Ubuntu:/home/akwolf# apt install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 111 not upgraded.
root@Ubuntu:/home/akwolf# iptables -L
Chain INPUT (policy DROP)
target    prot opt source                destination
ufw-before-logging-input all -- anywhere             anywhere
ufw-before-input all -- anywhere             anywhere
ufw-after-input all -- anywhere             anywhere
ufw-after-logging-input all -- anywhere             anywhere
ufw-reject-input all -- anywhere             anywhere
ufw-track-input all -- anywhere             anywhere

Chain FORWARD (policy DROP)
target    prot opt source                destination
ufw-before-logging-forward all -- anywhere             anywhere
ufw-before-forward all -- anywhere             anywhere
ufw-after-forward all -- anywhere             anywhere
ufw-after-logging-forward all -- anywhere             anywhere
ufw-reject-forward all -- anywhere             anywhere
ufw-track-forward all -- anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
ufw-before-logging-output all -- anywhere             anywhere
ufw-before-output all -- anywhere             anywhere
```

```
root@Ubuntu: /home/akwolf

root@Ubuntu:/home/akwolf# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@Ubuntu:/home/akwolf# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@Ubuntu:/home/akwolf#
```

```
root@Ubuntu: /home/akwolf
root@Ubuntu:/home/akwolf# iptables -P INPUT DROP
root@Ubuntu:/home/akwolf# iptables -P OUTPUT ACCEPT
root@Ubuntu:/home/akwolf#
```

```
root@Ubuntu: /home/akwolf
root@Ubuntu:/home/akwolf# ufw allow ssh
Rule added
Rule added (v6)
root@Ubuntu:/home/akwolf# ufw allow http
Rule added
Rule added (v6)
root@Ubuntu:/home/akwolf# ufw allow https
Rule added
Rule added (v6)
root@Ubuntu:/home/akwolf#
```

```
root@Ubuntu: /home/akwolf
root@Ubuntu:/home/akwolf# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@Ubuntu:/home/akwolf# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@Ubuntu:/home/akwolf# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
root@Ubuntu:/home/akwolf#
```

```
root@Ubuntu: /home/akwolf
root@Ubuntu:/home/akwolf# ufw status numbered
Status: active

      To Action From
      --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 5] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 443 (v6) ALLOW IN Anywhere (v6)

root@Ubuntu:/home/akwolf#
```

```

root@Ubuntu:/home/akwolf# iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ufw-before-logging-input  all  --  anywhere              anywhere
ufw-before-input          all  --  anywhere              anywhere
ufw-after-input           all  --  anywhere              anywhere
ufw-after-logging-input   all  --  anywhere              anywhere
ufw-reject-input          all  --  anywhere              anywhere
ufw-track-input           all  --  anywhere              anywhere
ACCEPT      tcp  --  anywhere              anywhere            tcp dpt:ssh
ACCEPT      tcp  --  anywhere              anywhere            tcp dpt:ssh
ACCEPT      tcp  --  anywhere              anywhere            tcp dpt:http
ACCEPT      tcp  --  anywhere              anywhere            tcp dpt:https

Chain FORWARD (policy DROP)
target     prot opt source                destination
ufw-before-logging-forward all  --  anywhere              anywhere
ufw-before-forward        all  --  anywhere              anywhere
ufw-after-forward         all  --  anywhere              anywhere
ufw-after-logging-forward all  --  anywhere              anywhere
ufw-reject-forward        all  --  anywhere              anywhere
ufw-track-forward         all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

```

```

root@Ubuntu:/home/akwolf# ufw allow from 192.168.1.1
Rule added
root@Ubuntu:/home/akwolf# ufw deny from 192.168.1.1
Rule updated
root@Ubuntu:/home/akwolf# ufw status numbered
Status: active

    To Action From
    --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 80/tcp ALLOW IN Anywhere
[ 3] 443 ALLOW IN Anywhere
[ 4] Anywhere DENY IN 192.168.1.1
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 443 (v6) ALLOW IN Anywhere (v6)

root@Ubuntu:/home/akwolf#

```

```

root@Ubuntu: /home/akwolf
num target      prot opt source      destination      ctstate NEW
2 ACCEPT      udp  -- anywhere    anywhere         ctstate NEW

Chain ufw-user-forward (1 references)
num target      prot opt source      destination
Chain ufw-user-input (1 references)
num target      prot opt source      destination      tcp dpt:ssh
2 ACCEPT      tcp  -- anywhere    anywhere         tcp dpt:http
3 ACCEPT      tcp  -- anywhere    anywhere         tcp dpt:https
4 ACCEPT      udp  -- anywhere    anywhere         udp dpt:https
5 DROP        all  -- 192.168.1.1  anywhere

Chain ufw-user-limit (0 references)
num target      prot opt source      destination      limit: avg 3/min burst 5 LO
1 LOG         all  -- anywhere    anywhere
G level warn prefix "[UFW LIMIT BLOCK] "
2 REJECT      all  -- anywhere    anywhere         reject-with icmp-port-unrea
chable

Chain ufw-user-limit-accept (0 references)
num target      prot opt source      destination
1 ACCEPT      all  -- anywhere    anywhere

```

Commandos:

- sudo su (inicio de sesión)
- apt install ufw -Y
- ufw enable
- ufw status
- apt install iptables -Y
- iptables -L
- ufw default deny incoming
- ufw default allow outgoing
- iptables -P INPUT DROP
- iptables -P OUTPUT ACCEPT
- ufw allow ssh
- ufw allow http
- ufw allow https
- iptables -A INPUT -P tcp --dport 22 -j ACCEPT
- iptables -A INPUT -P tcp --dport 80 -j ACCEPT
- iptables -A INPUT -P tcp --dport 443 -j ACCEPT
- ufw status numbered
- iptables -L
- ufw allow from 192.168.1.1
- ufw deny from 192.168.1.1
- iptables -A INPUT -s 192.168.1.2 -j ACCEPT
- iptables -L --line-numbers
- iptables -D INPUT 9

- iptables -L --line-numbers
- ufw deny from any to any port 8080
- iptables -A INPUT -p tcp --dport 8080 -j DROP