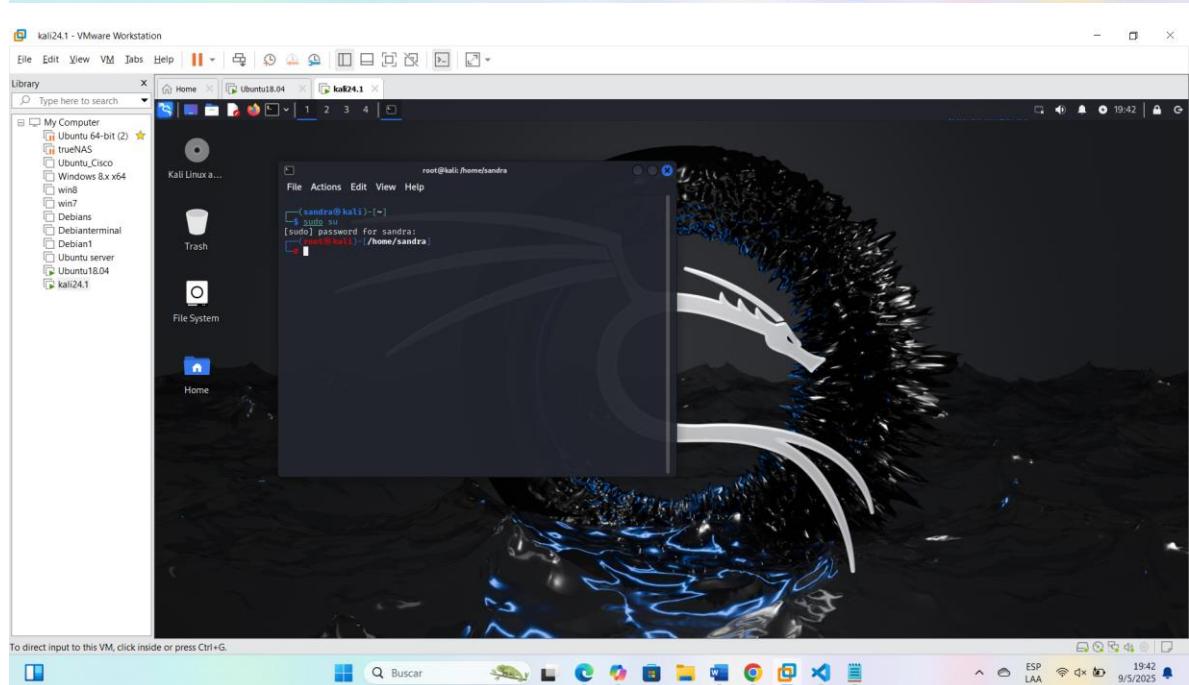
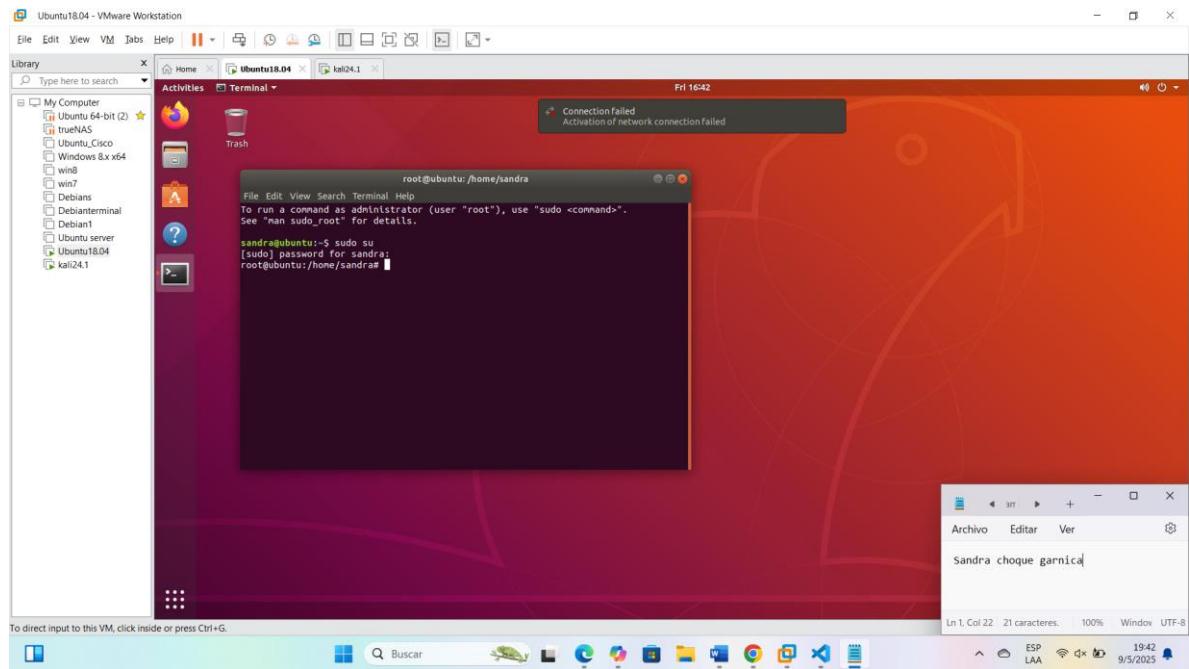


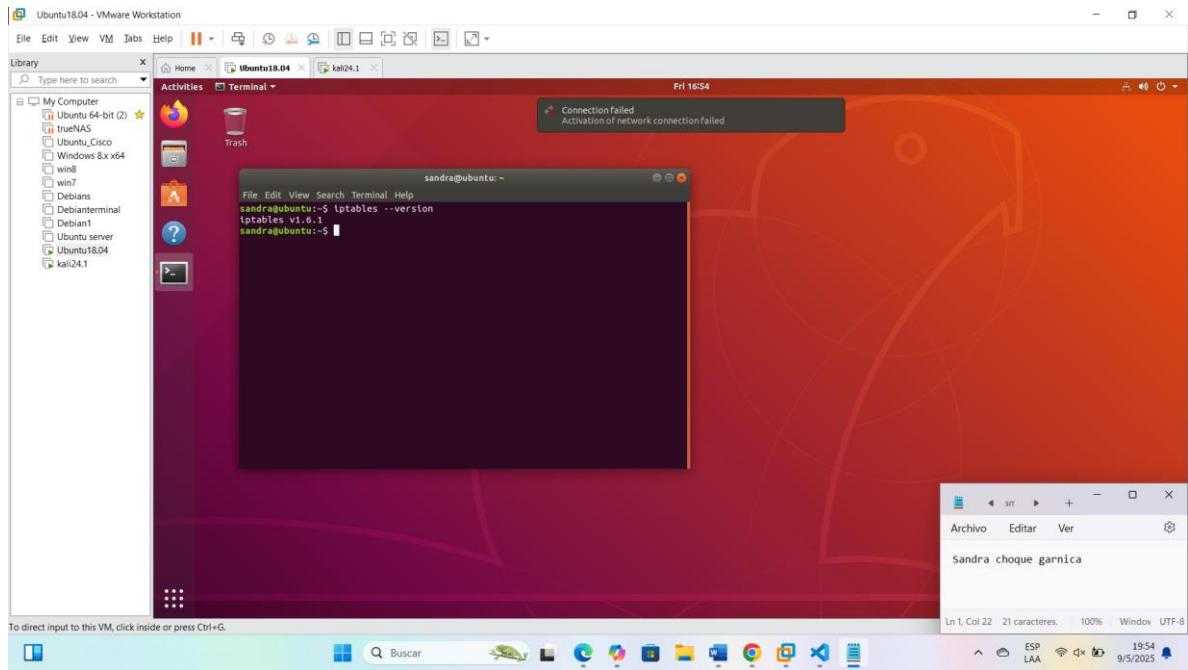
NOMBRE:SANDRA CHOQUE GARNICA

LAB 9

Paso 1



Paso 2



Paso 3

Autoguardado

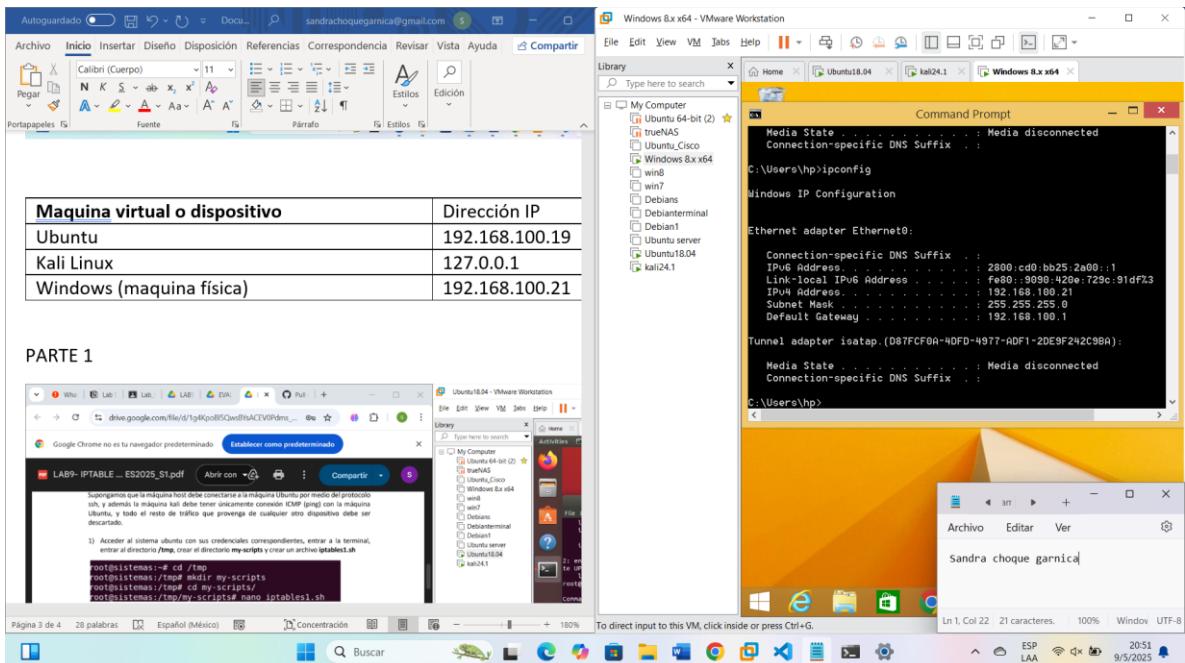
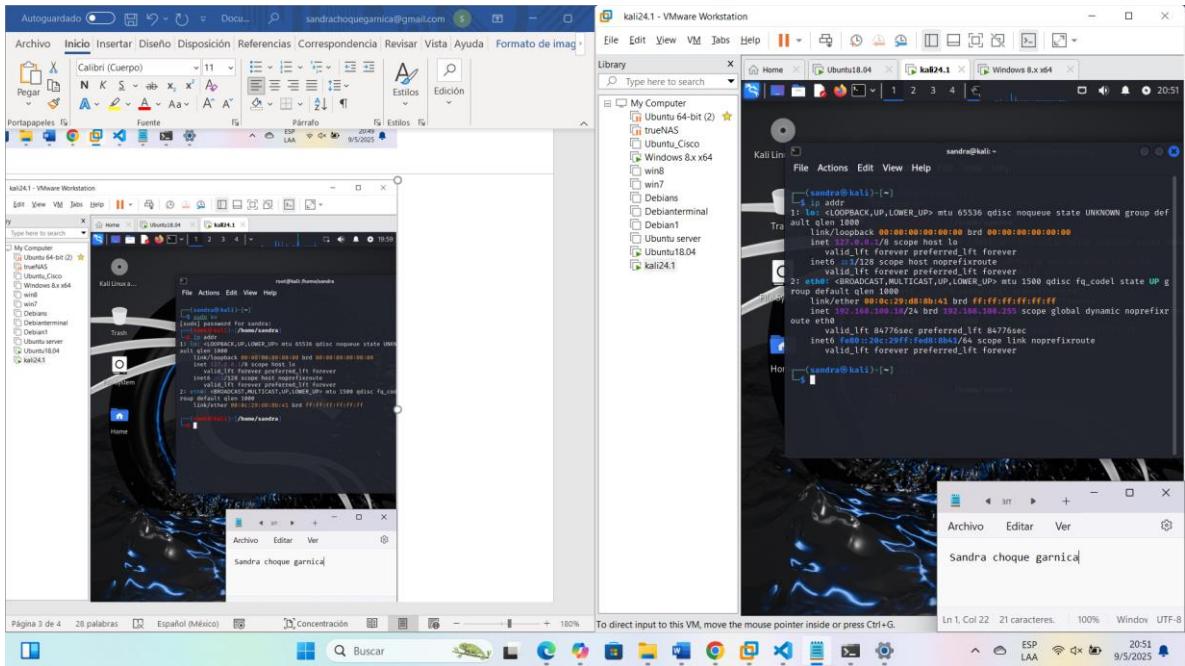
Maquina virtual o dispositivo	Dirección IP
Ubuntu	192.168.100.19
Kali Linux	127.0.0.1
Windows (maquina física)	192.168.100.21

PARTE 1

To direct input to this VM, click inside or press Ctrl+G.

File Edit View Search Terminal Help

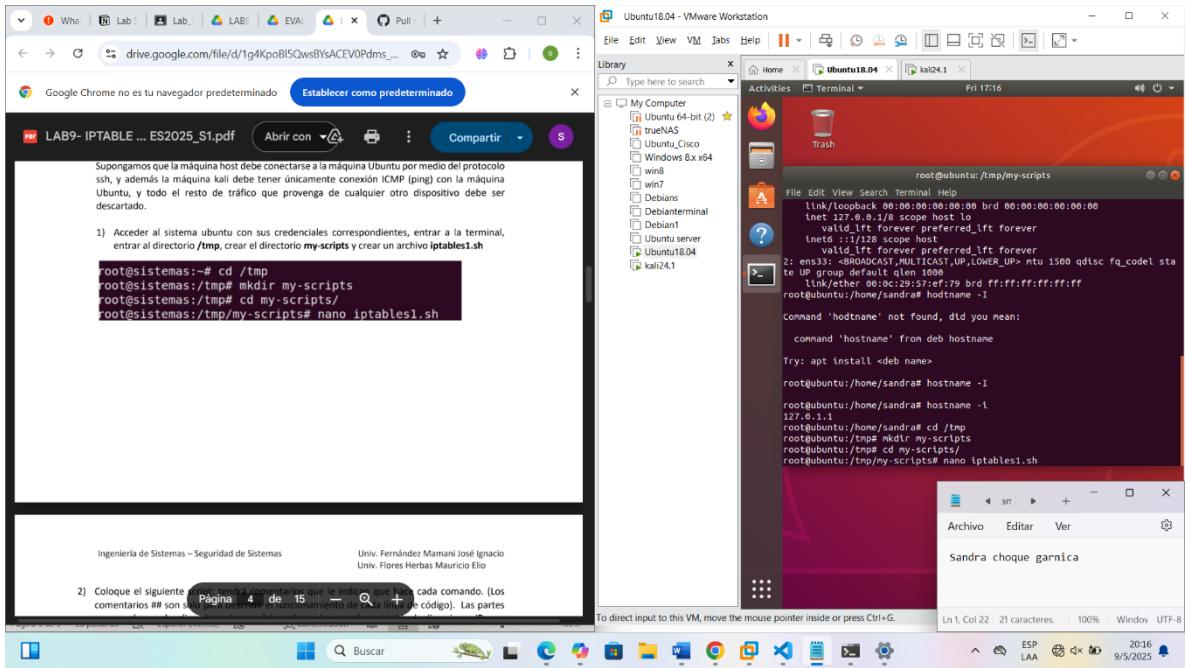
```
sandra@ubuntu:~$ sudo su
[sudo] password for sandra:
root@ubuntu:/home/sandra# hostname -c
127.0.1.1
root@ubuntu:/home/sandra# ip addr
1: lo <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    brd 00:00:00:00:00:00
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: ens33: <>BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP qlen 1000
    brd 192.168.100.255
        link/ether 00:0c:29:57:ef:79 brd ff:ff:ff:ff:ff:ff
        inet 192.168.100.19/24 brd 192.168.100.255 scope global dynamic noprefixroute
            valid_lft 899sec preferred_lft 899sec
            inet6 fe80::20c:29ff:fe57:ef79/64 brd fe80::ff:ff:ff:ff:ff:ff scope link noprefixroute
                valid_lft forever preferred_lft forever
root@ubuntu:/home/sandra# cd /tmp
root@ubuntu:/tmp# mkdir my-scripts
root@ubuntu:/tmp# cd my-scripts/
root@ubuntu:/tmp/my-scripts# nano iptables1.sh
root@ubuntu:/tmp/my-scripts# nano iptables1.sh
root@ubuntu:/tmp/my-scripts# 
```



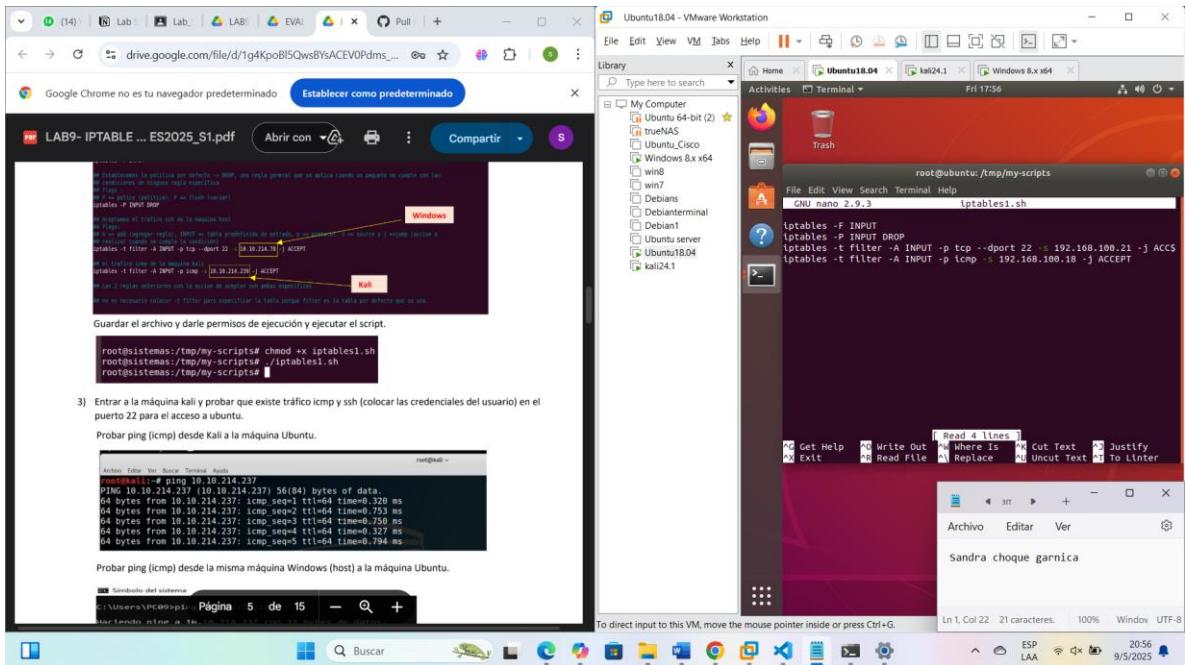
Maquina virtual o dispositivo	Dirección IP
Ubuntu	192.168.100.19
Kali Linux	127.0.0.1
Windows (maquina física)	192.168.100.21

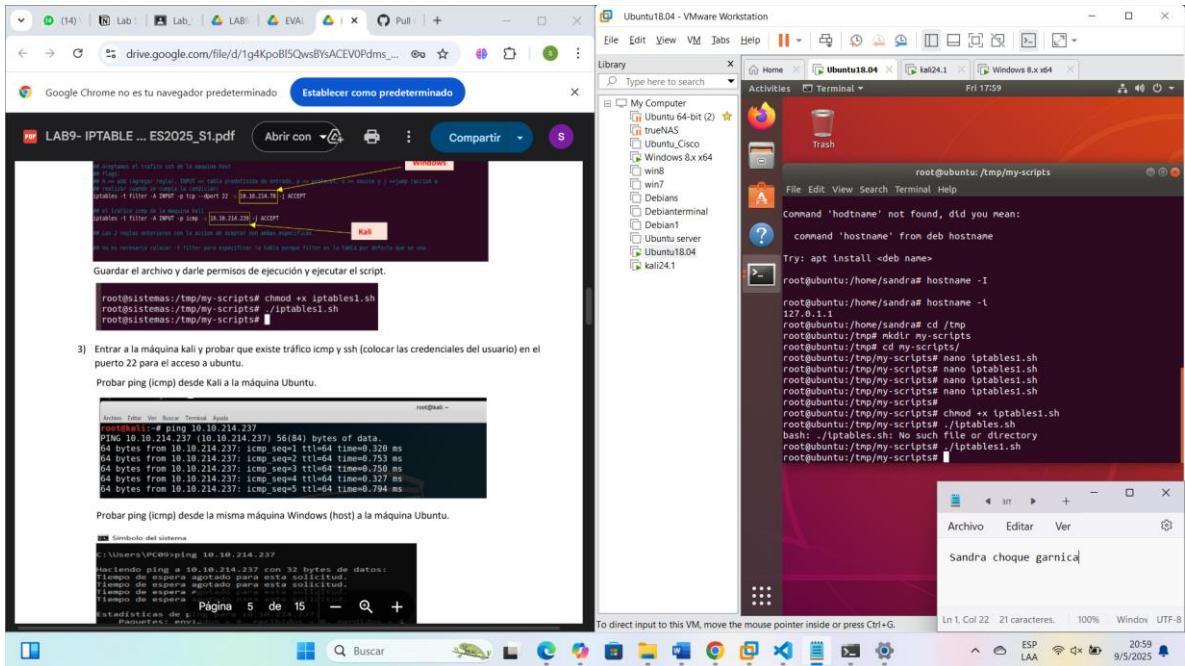
PARTE 1

1)

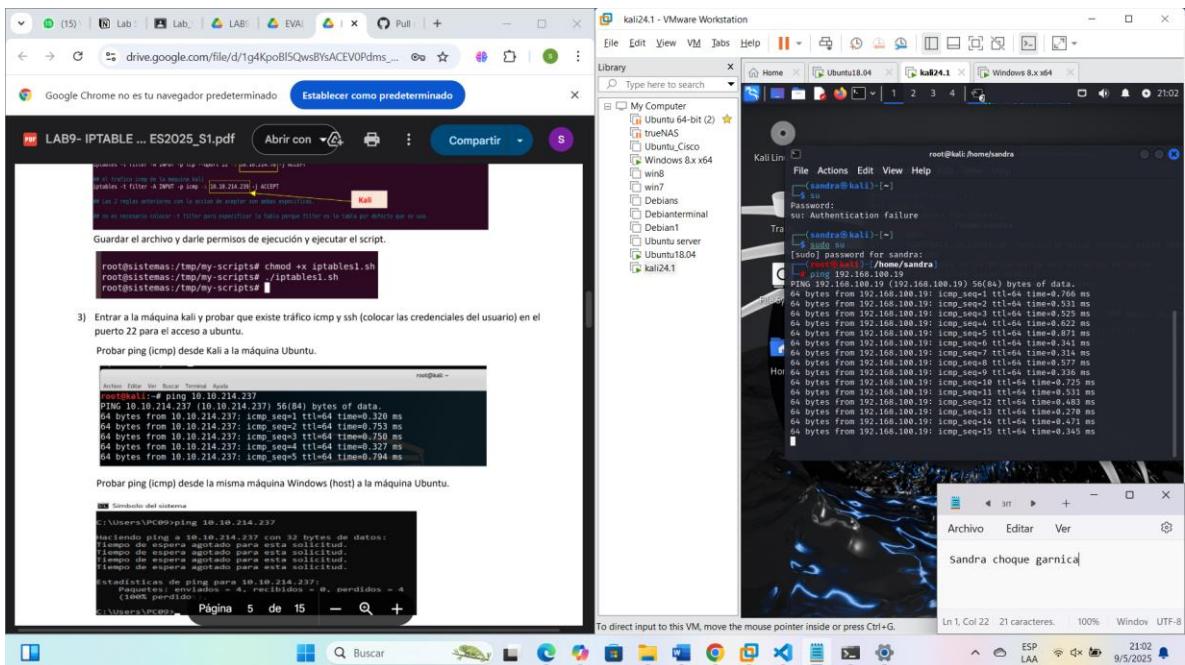


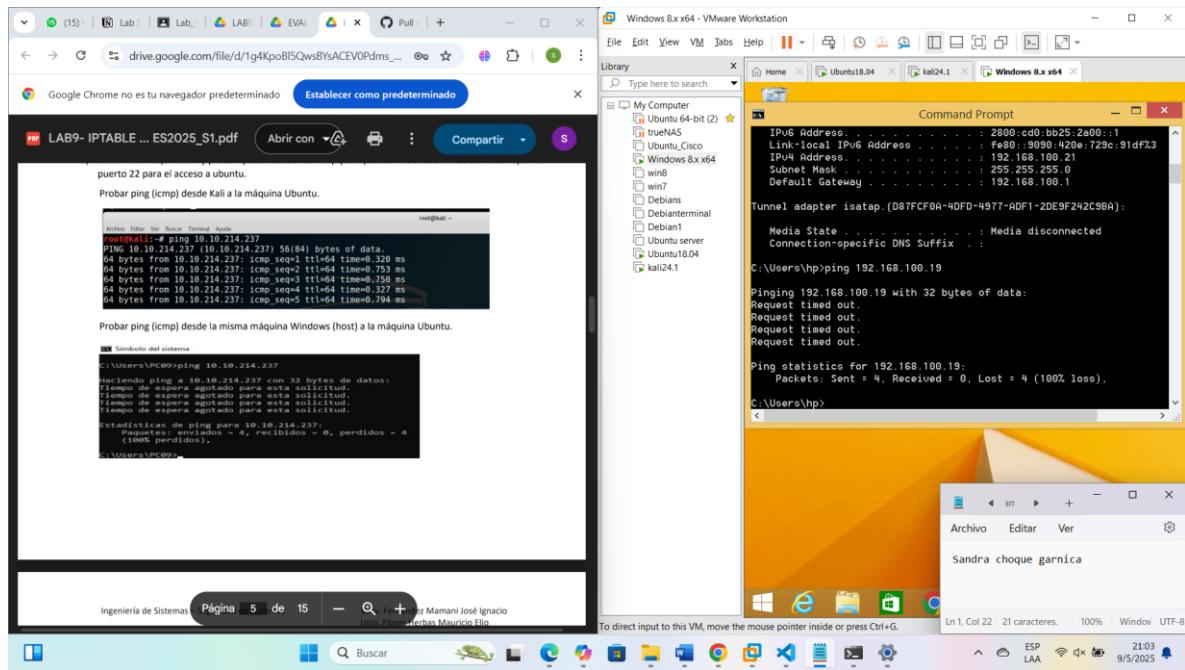
2)



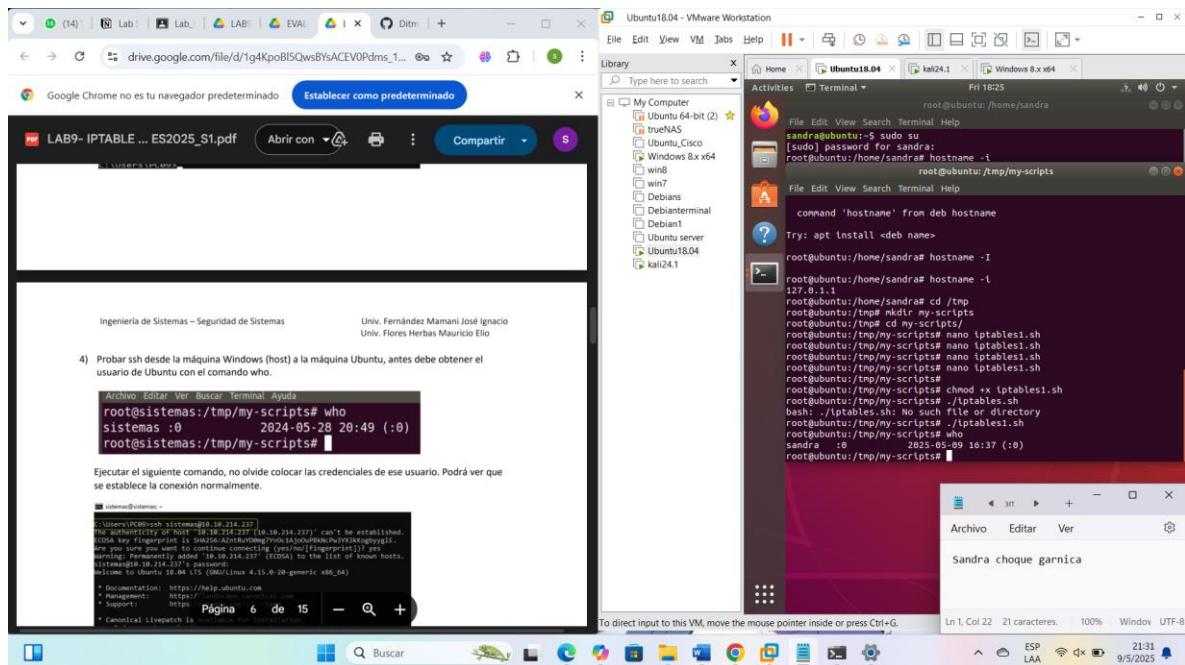


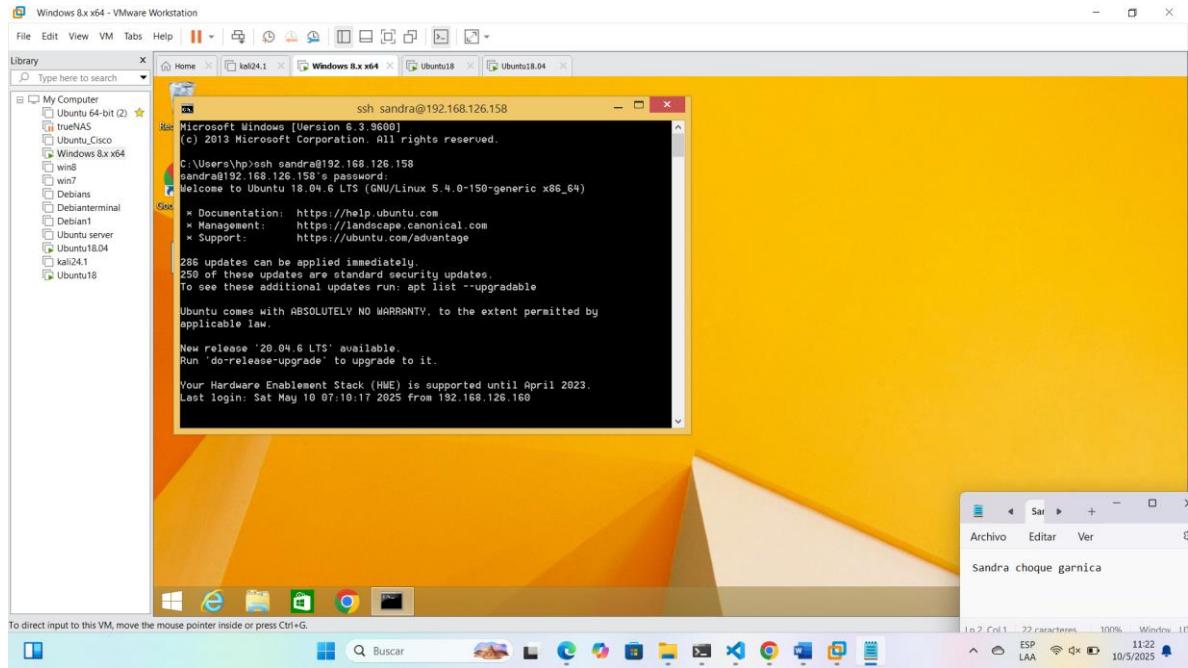
3)





4)





5)

drive.google.com/file/d/1g4KpoBf5QwsByACEVOp... Establecer como predeterminado

Google Chrome no es tu navegador predeterminado

LAB- IPTABLE ... ES2025_S1.pdf

5) Probar ssh desde la máquina Kali a Ubuntu. Espere unos minutos y podrá ver que no logra establecer conexión.

root@sistemas:~# ssh sistemas@10.10.214.237

6) Eliminar estas reglas para que no choquen con las siguientes configuraciones, con los siguientes comandos:

```
root@sistemas:/tmp/my-scripts# iptables -F INPUT
root@sistemas:/tmp/my-scripts# iptables -P INPUT ACCEPT
root@sistemas:/tmp/my-scripts# iptables -L
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Archivo Editar Ver Buscar Terminal Ayuda

sandra@sandra-kali:~\$

File Actions Edit View Help

sandra@sandra-kali:~\$ ssh sandra@192.168.126.158

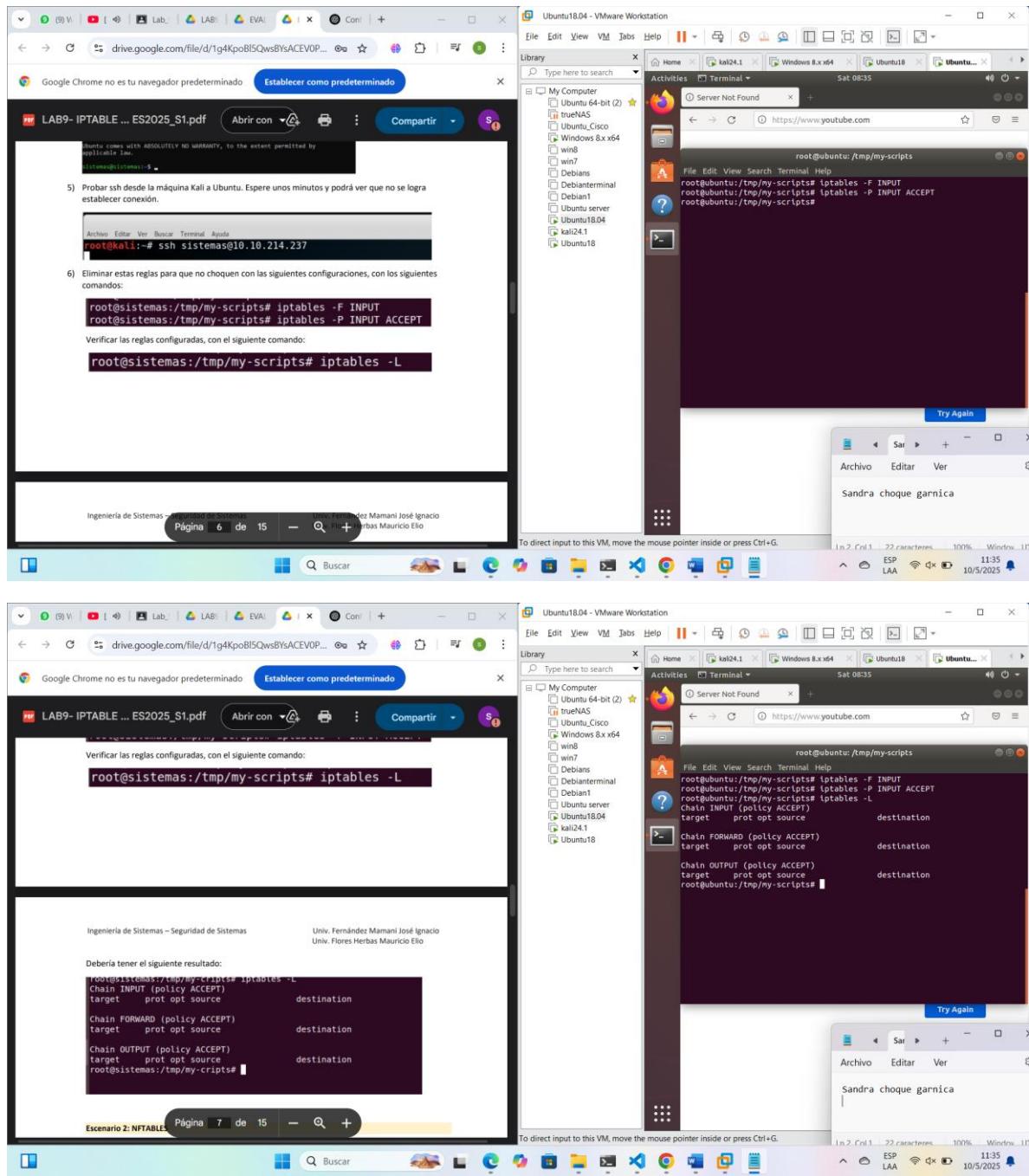
Archivo Editar Ver

Sandra cheque garnica

In 2, Col 1 22 caracteres 100% Window... UP

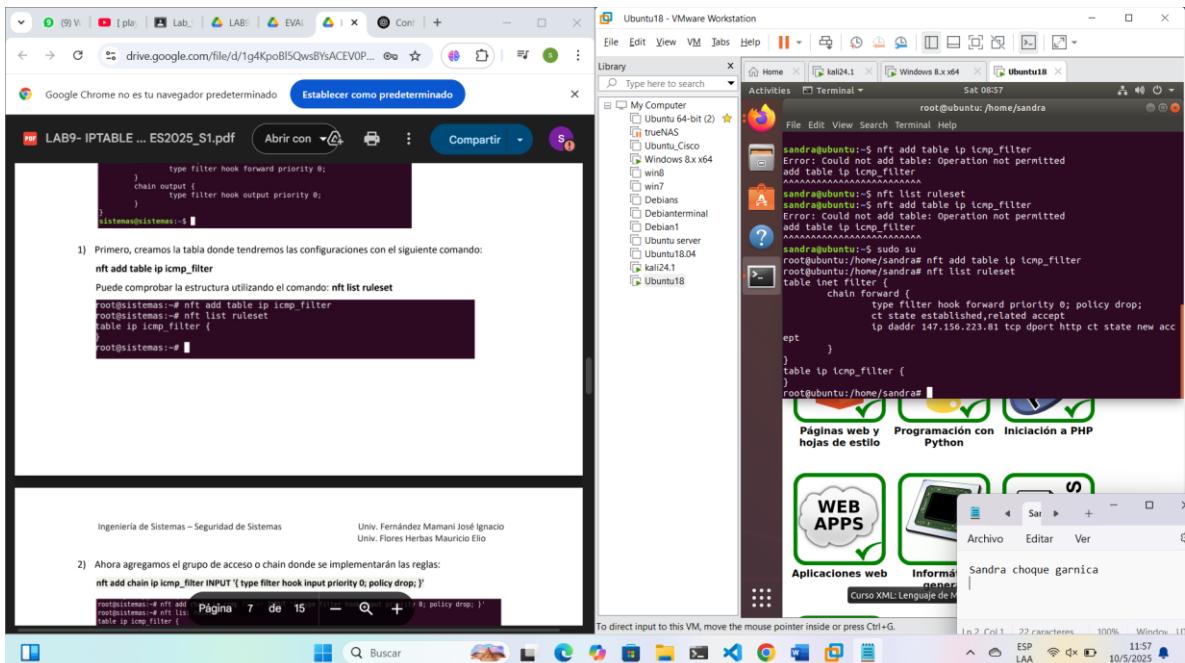
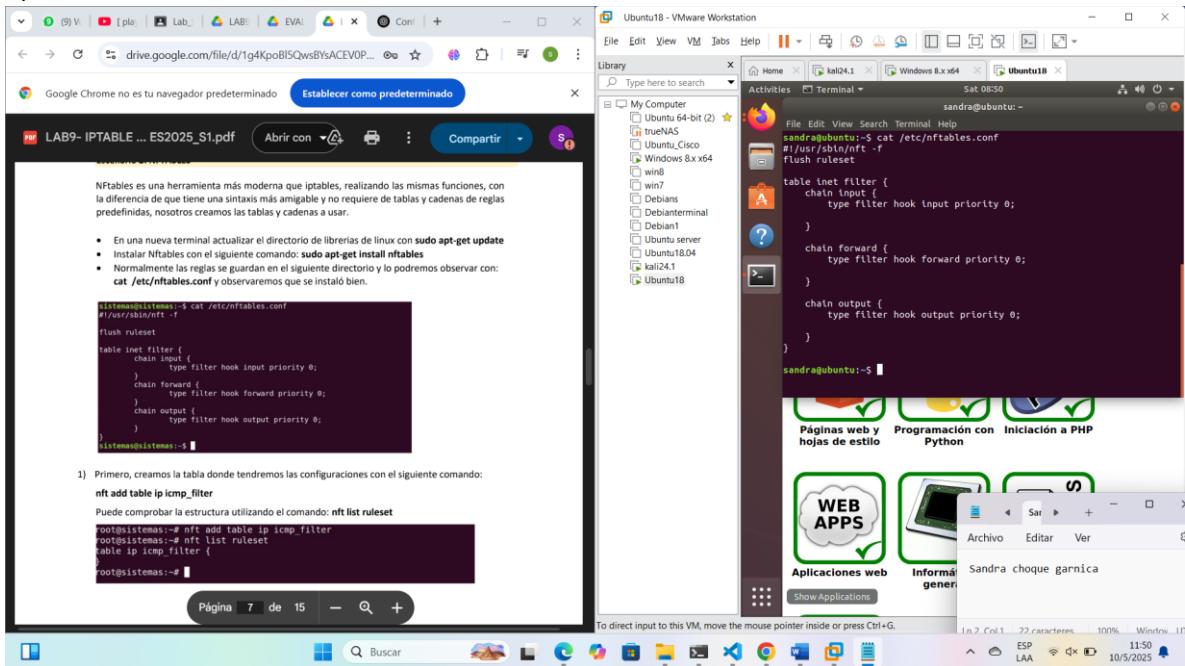
ESP LAA 1128 10/5/2025

6)

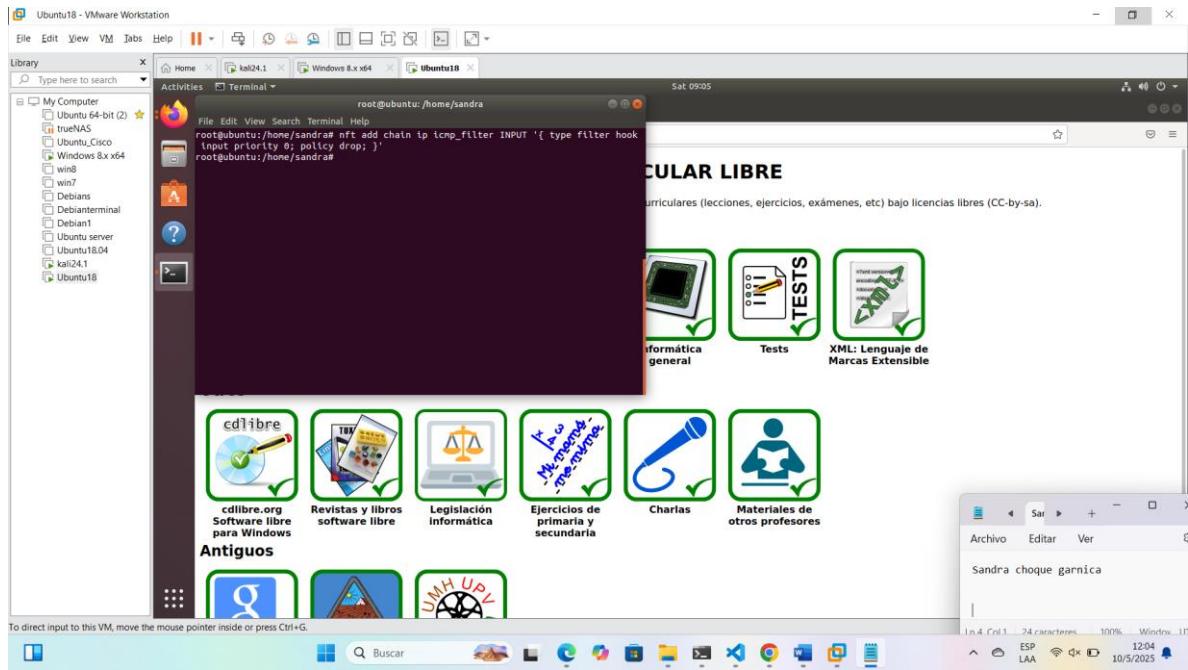


Escenario nftables

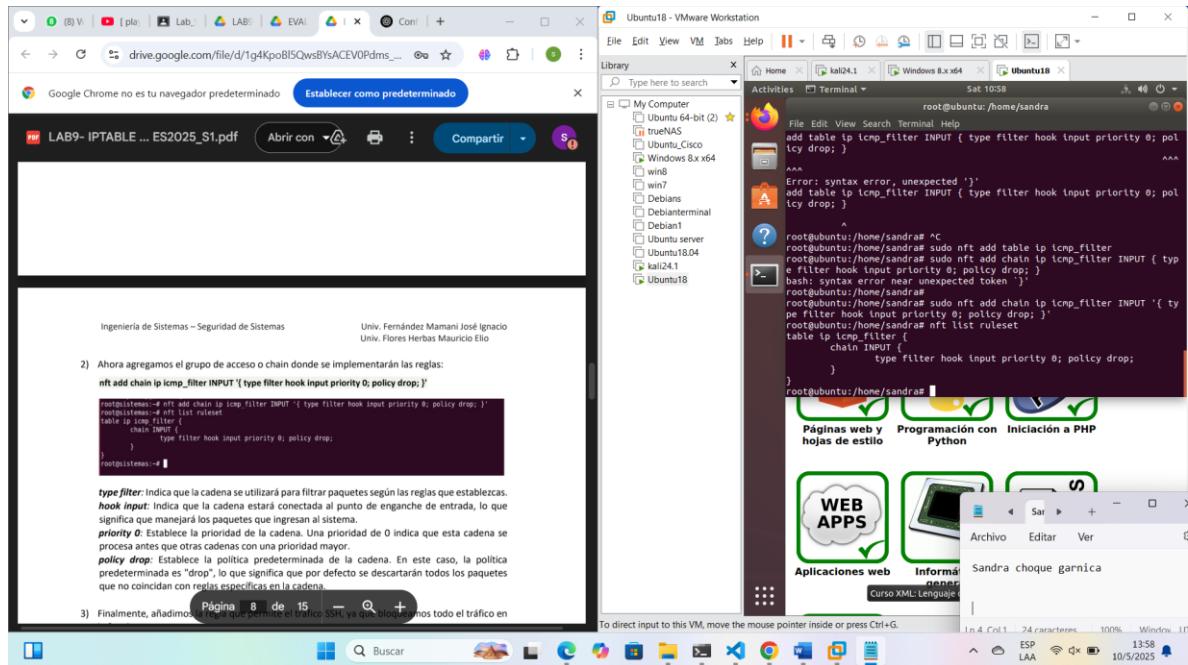
1)



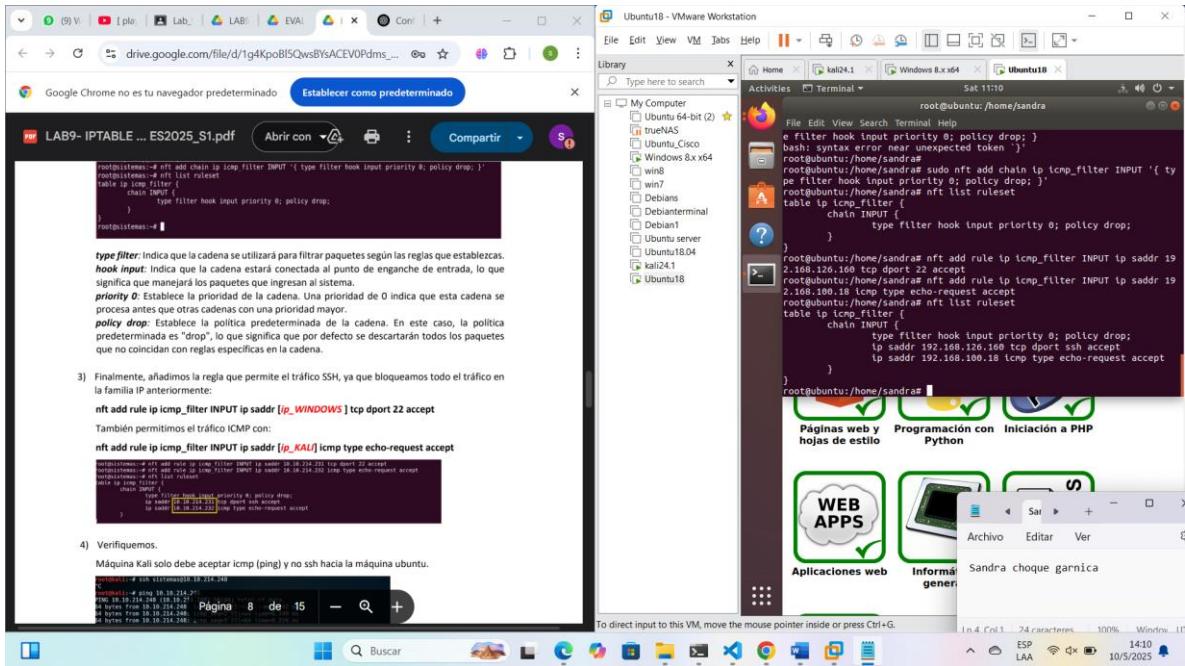
2)



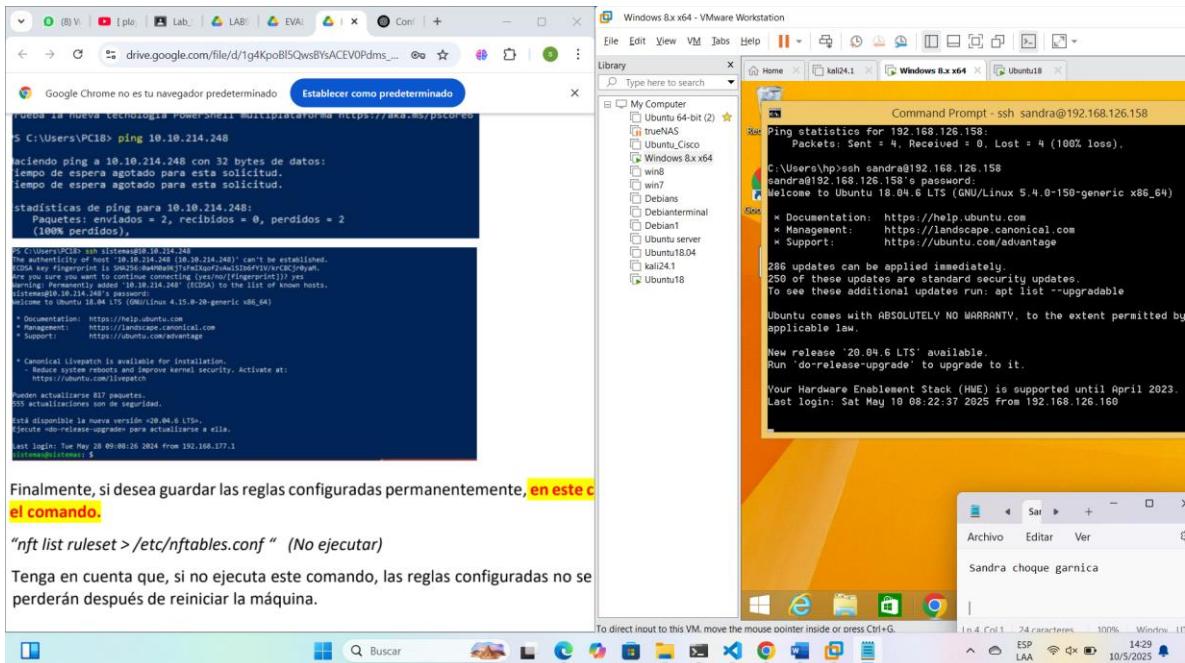
2)



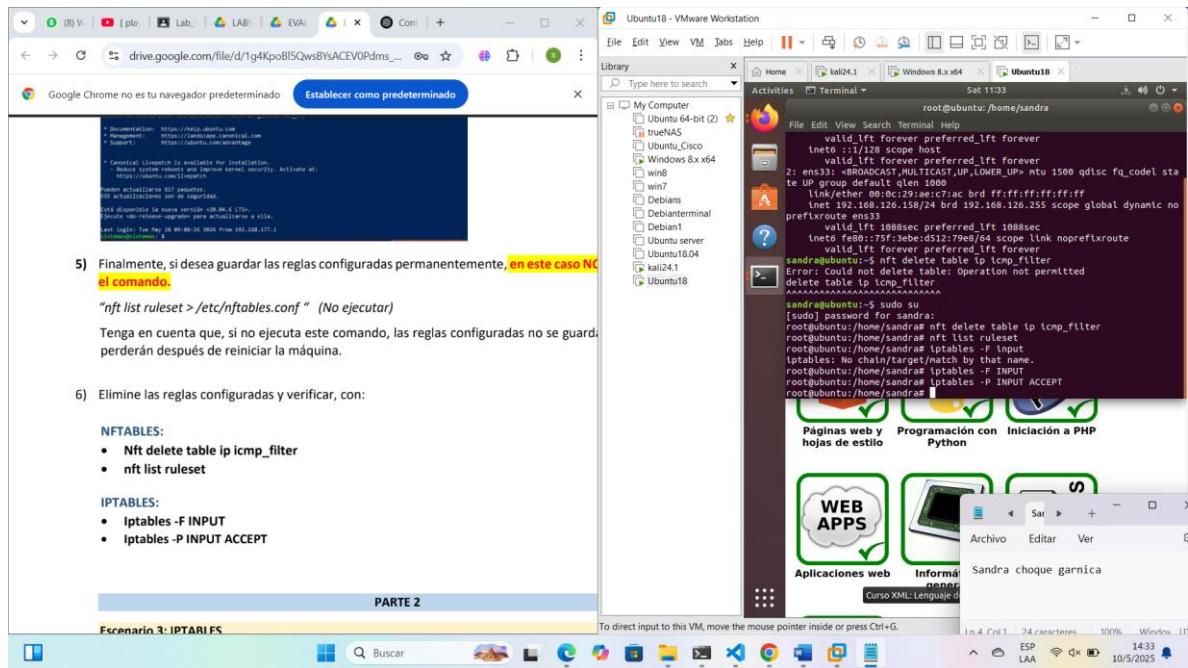
3)



4)

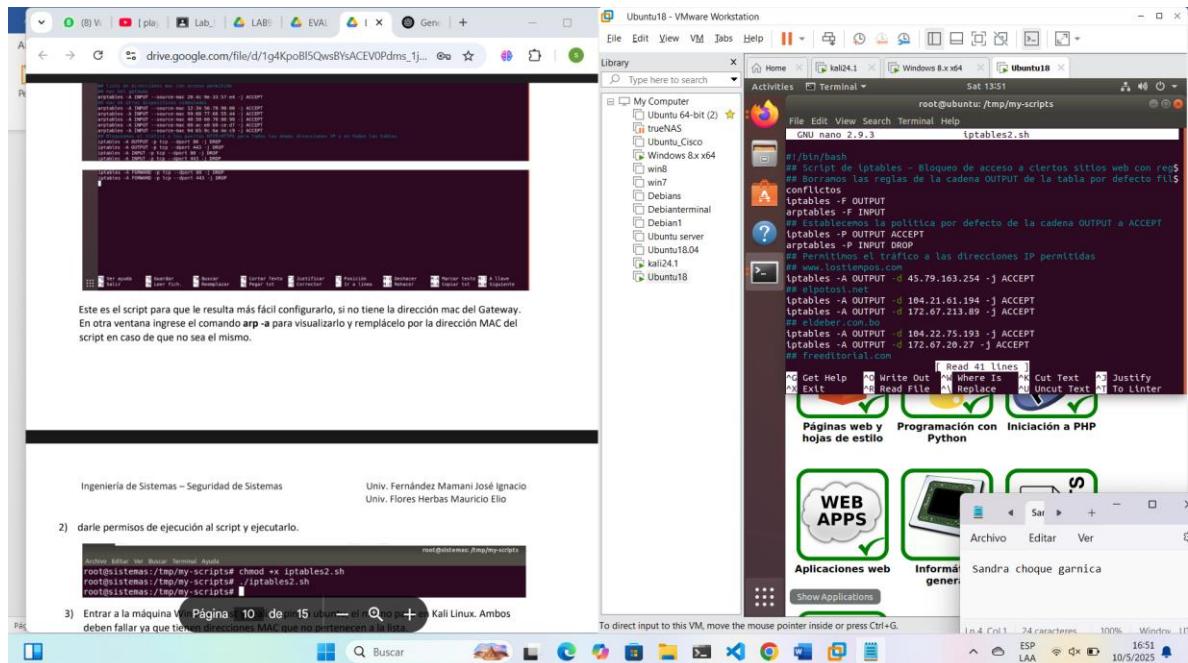


6)

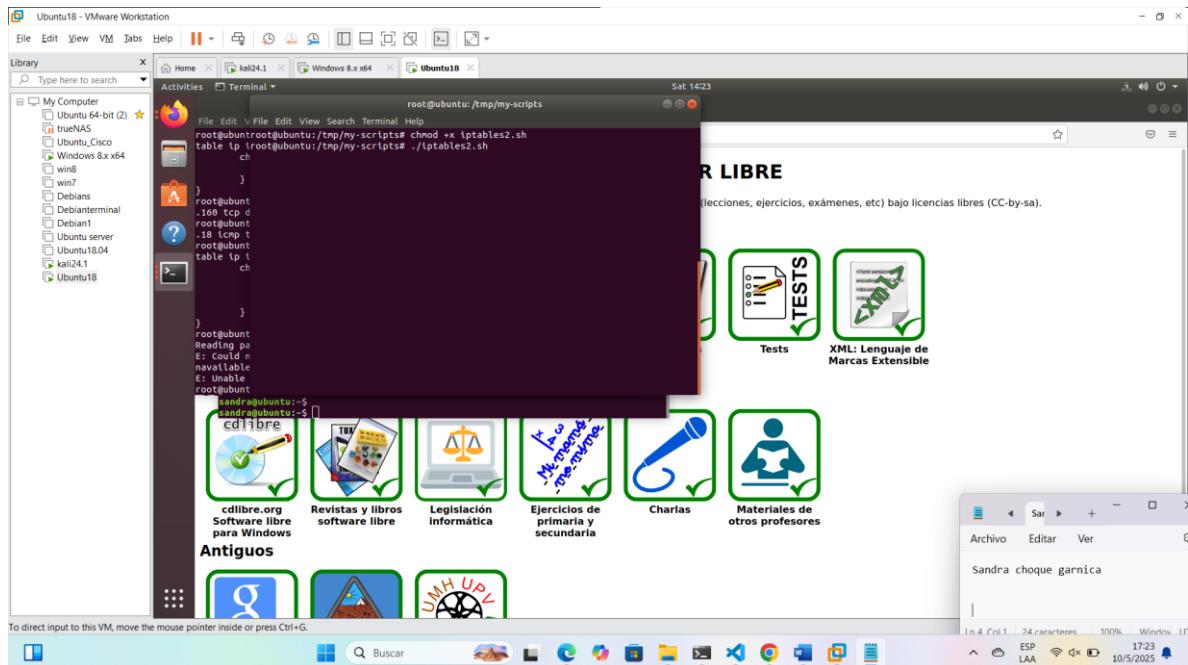


PARTE 2

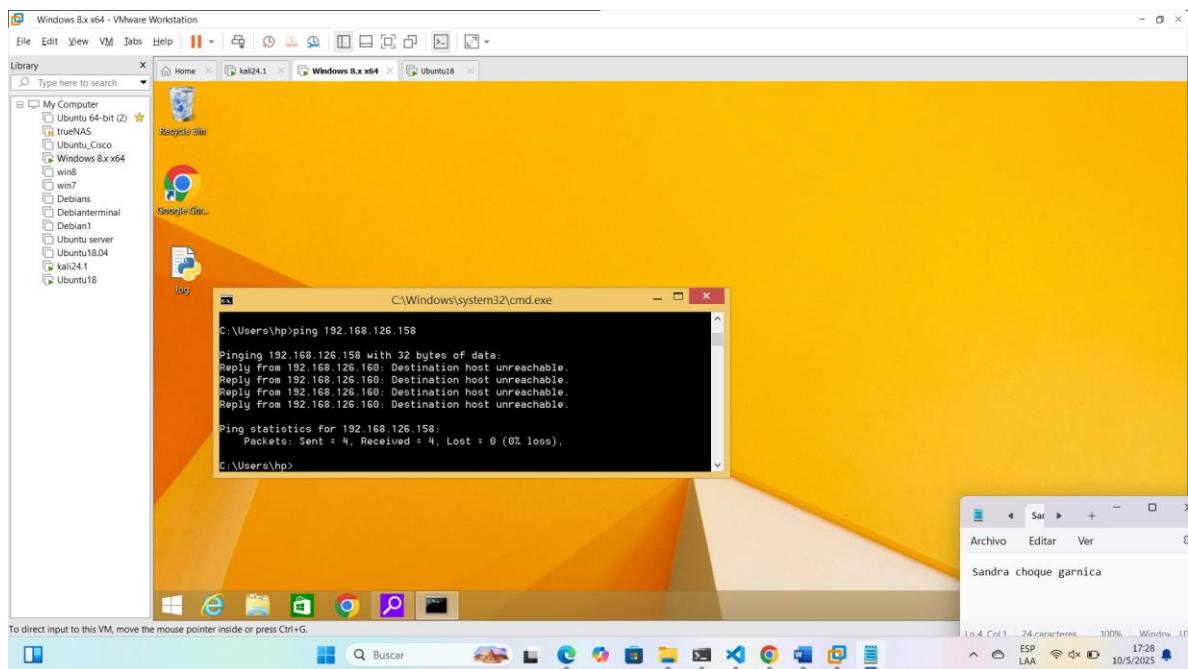
1)

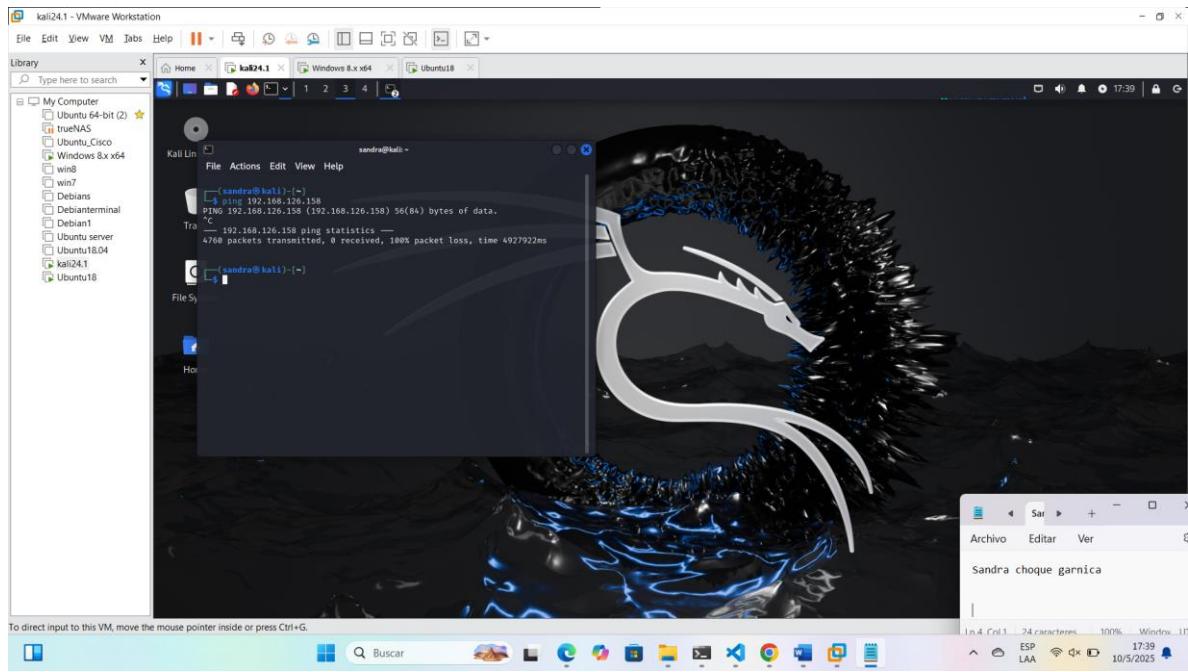


2)

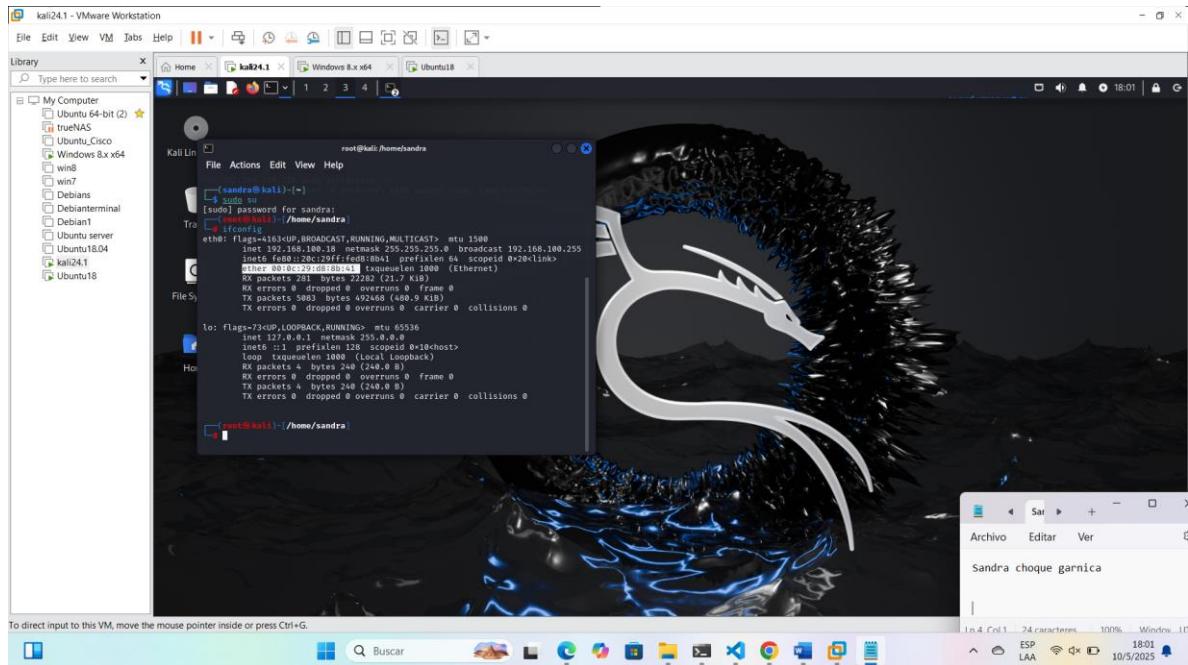


3)

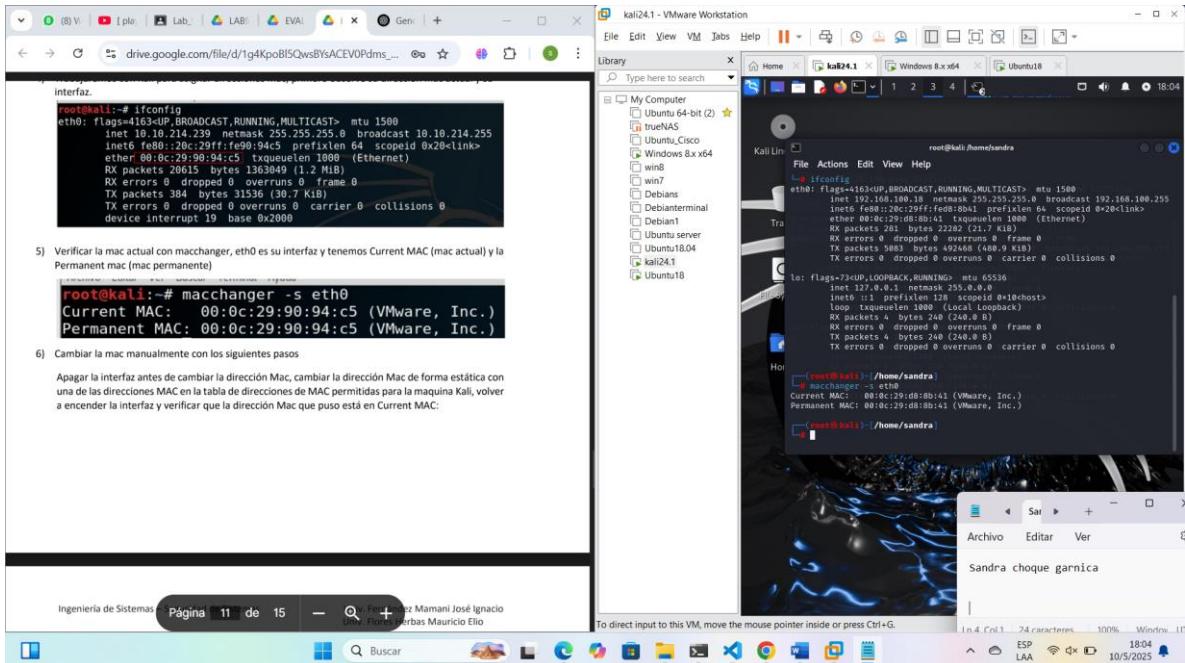




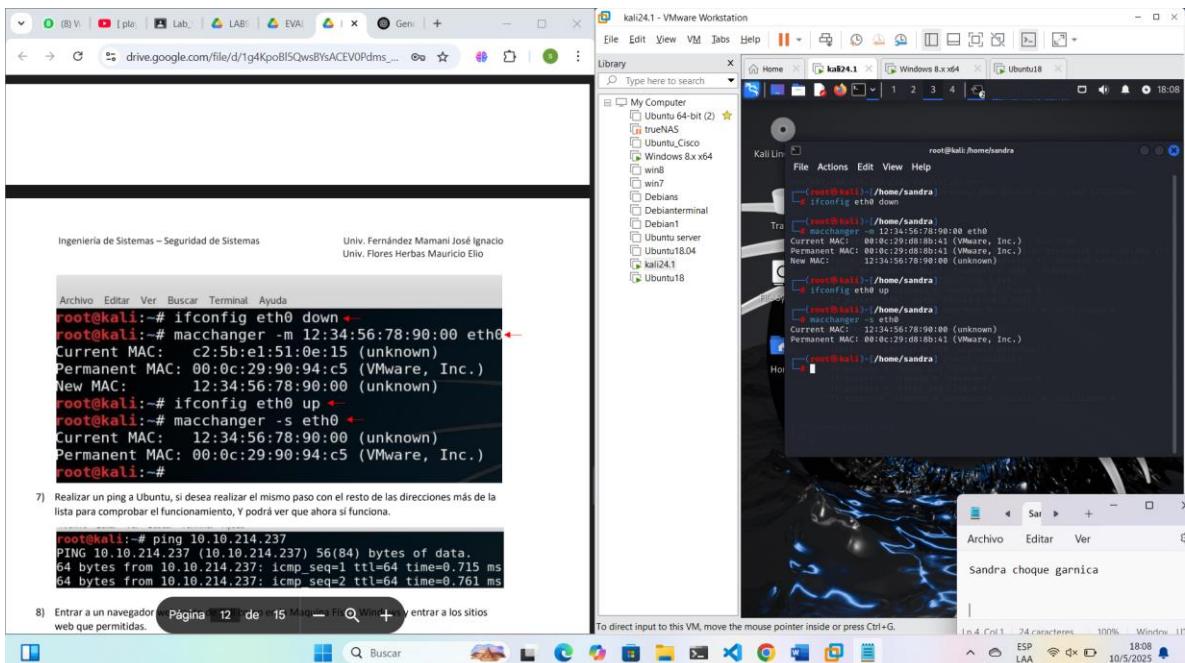
4)



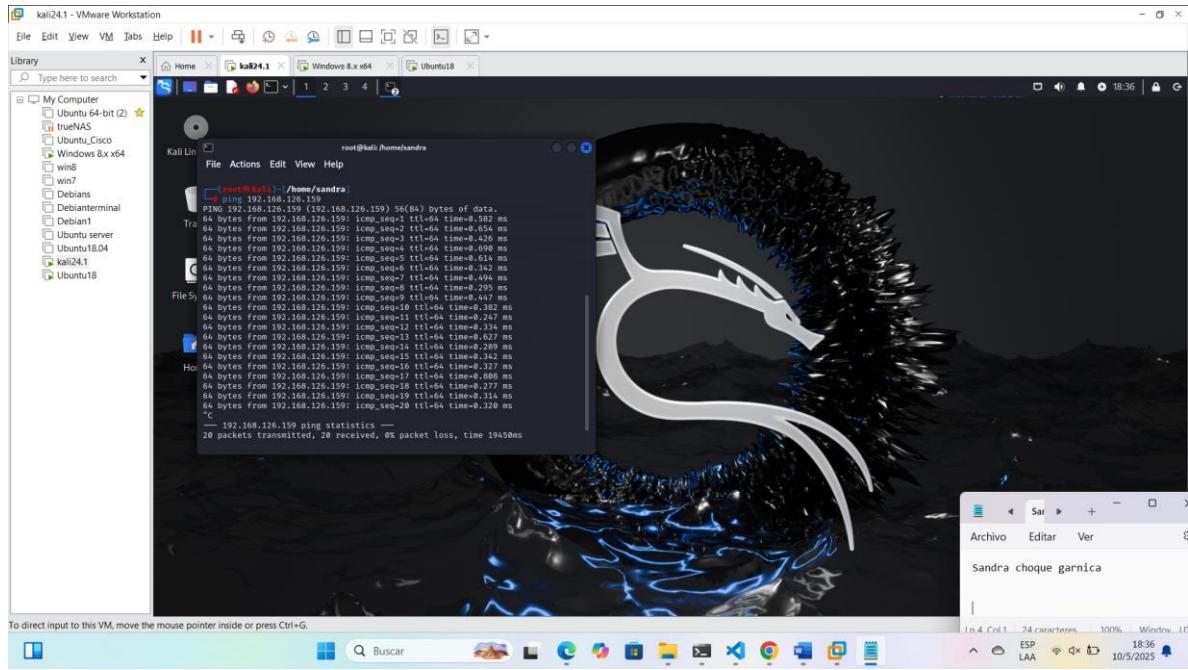
5)



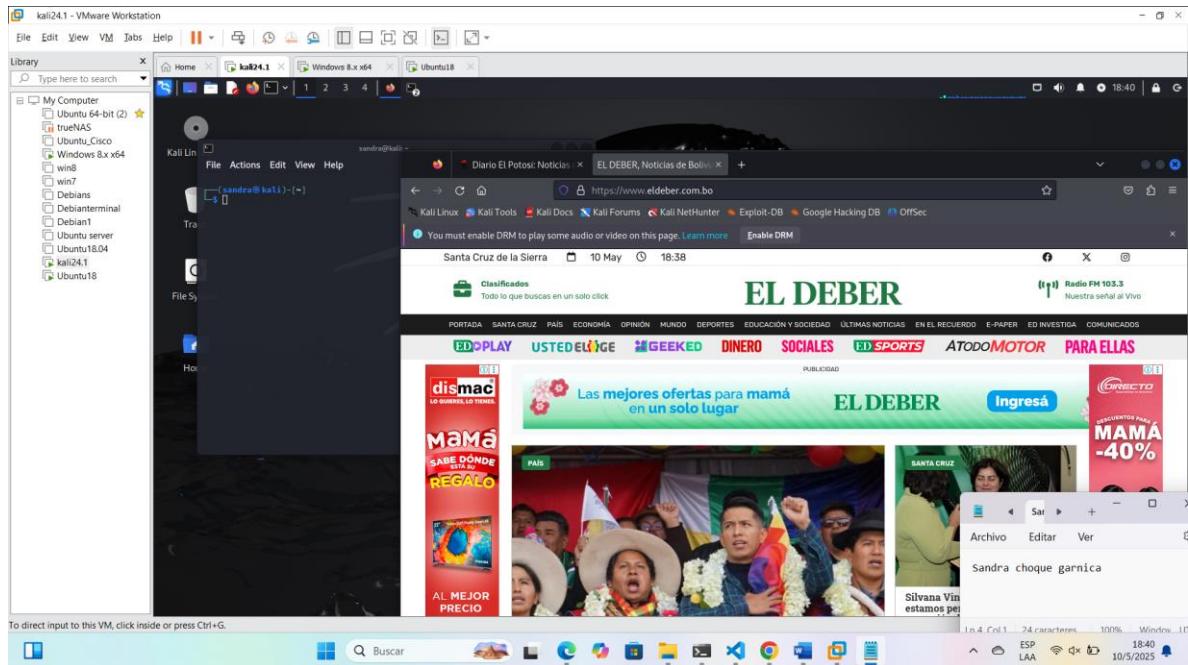
6)

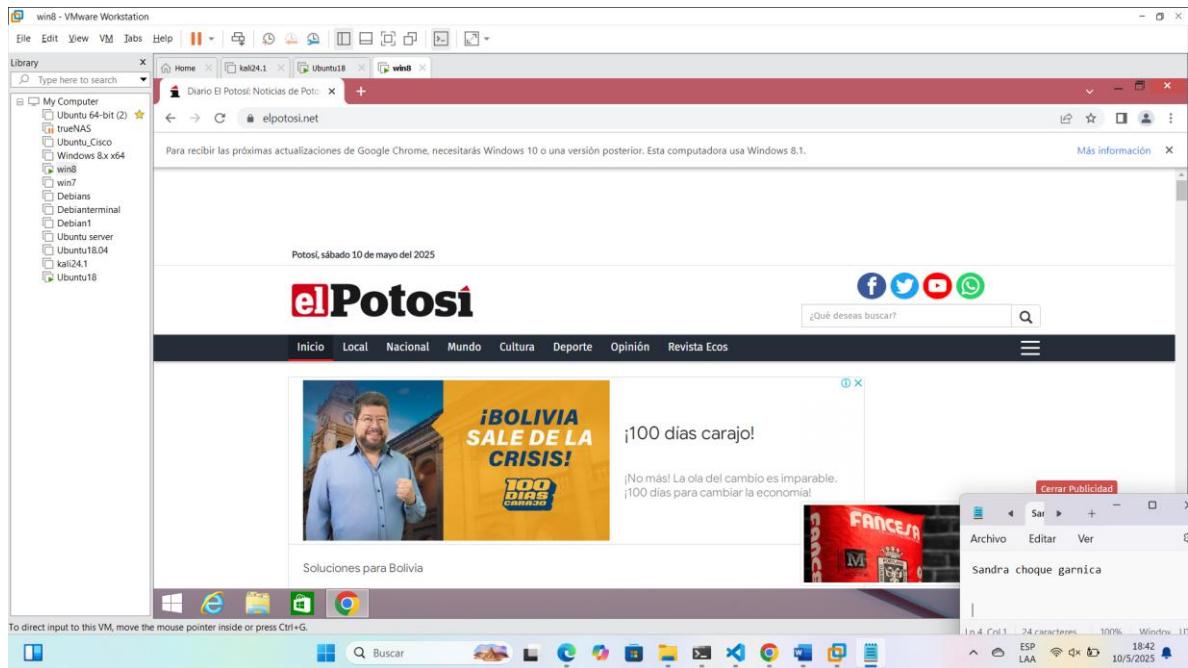


7)



8)





Respuesta pregunta 1

No, porque solo algunas páginas están permitidas para acceder como se puede ver en nano iptables2.sh

2.

La conexión desde Windows hacia Ubuntu se puede establecer, pero no al sitio web de Ubuntu debió a que estamos trabajando con algunas MAC permitidas en Kali; la que nos deja ingresar a sitios web

9)

9) Eliminar todas las reglas con:

- iptables -F INPUT
- iptables -P INPUT ACCEPT
- iptables -F OUTPUT
- iptables -P OUTPUT ACCEPT
- iptables -F FORWARD
- iptables -P FORWARD ACCEPT

Verificar: `iptables -L`

Escenario 4: NFTABLES

Como ya tenemos las ips de los dominios que se permitirán acceder empecemos con la configuración con nftables, antes verifique que su lista de reglas este vacía.

- 1) Primero se debe crear la tabla, el grupo de acceso o chain:

```
nft add table inet filterWeb
nft add chain inet filterWeb OUTPUT '{type filter hook output priority 0;}'
```

Le debería quedar así.

```
root@sistemas:~# nft add table inet filterWeb
root@sistemas:~# nft add chain inet filterWeb OUTPUT '{type filter hook output priority 0;}'` 
root@sistemas:~# nft list ruleset
table inet filterWeb {
    chain OUTPUT {
        type filter hook output priority 0; policy accept;
    }
}
```
- 2) Luego crearemos una propiedad set que permitirá almacenar las ips, puertos y direcciones MAC

```
nft add set inet filterWeb http_ports '{type inet_service;}'` 
nft add set inet filterWeb allowed_ip '{type ipv4_addr;}'`
```

Escenario 4 nf tables

1)

9) Eliminar todas las reglas con:

- iptables -F INPUT
- iptables -P INPUT ACCEPT
- iptables -F OUTPUT
- iptables -P OUTPUT ACCEPT
- iptables -F FORWARD
- iptables -P FORWARD ACCEPT

Verificar: `iptables -L`

Escenario 4: NFTABLES

Como ya tenemos las ips de los dominios que se permitirán acceder empecemos con la configuración con nftables, antes verifique que su lista de reglas este vacía.

- 1) Primero se debe crear la tabla, el grupo de acceso o chain:

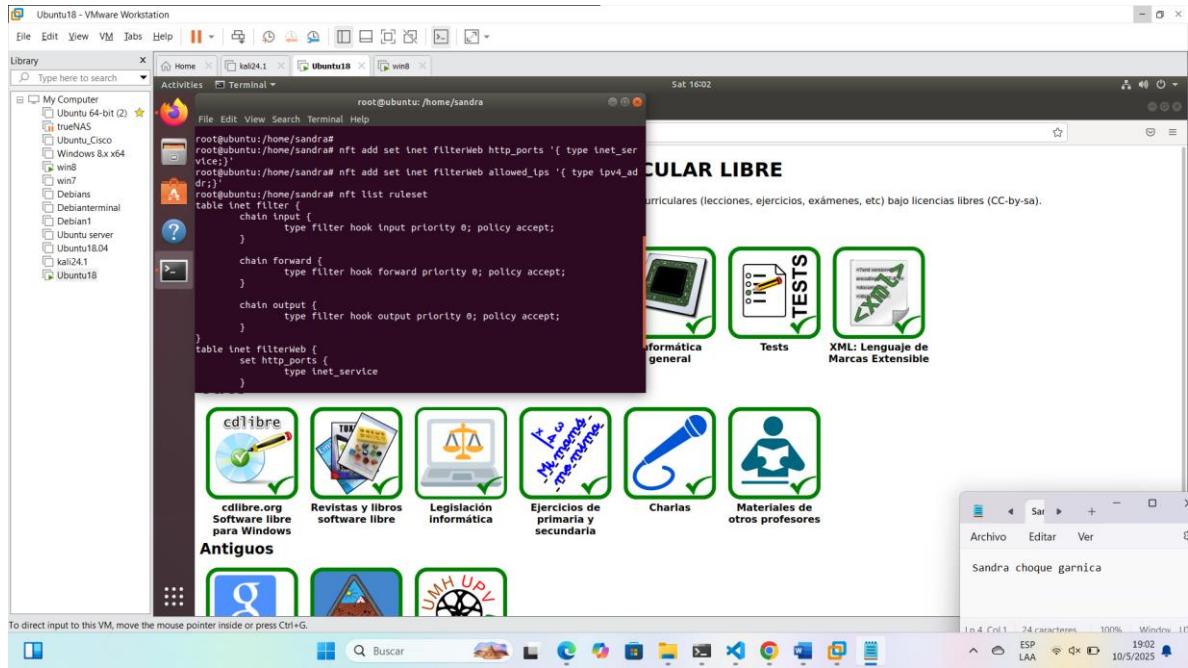
```
nft add table inet filterWeb
nft add chain inet filterWeb OUTPUT '{type filter hook output priority 0;}'`
```

Le debería quedar así.

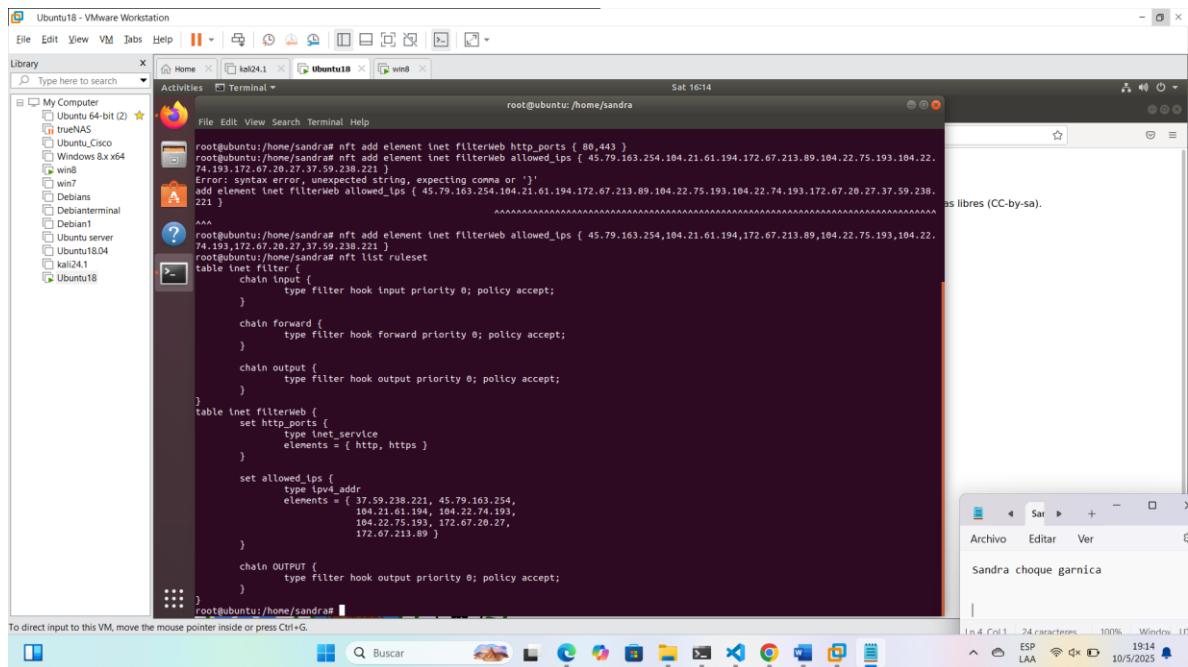
```
root@sistemas:~# nft add table inet filterWeb
root@sistemas:~# nft add chain inet filterWeb OUTPUT '{type filter hook output priority 0;}'` 
root@sistemas:~# nft list ruleset
table inet filterWeb {
    chain OUTPUT {
        type filter hook output priority 0; policy accept;
    }
}
```
- 2) Luego crearemos una propiedad set que permitirá almacenar las ips, puertos y direcciones MAC

```
nft add set inet filterWeb http_ports '{type inet_service;}'` 
nft add set inet filterWeb allowed_ip '{type ipv4_addr;}'`
```

2)



3)



4)

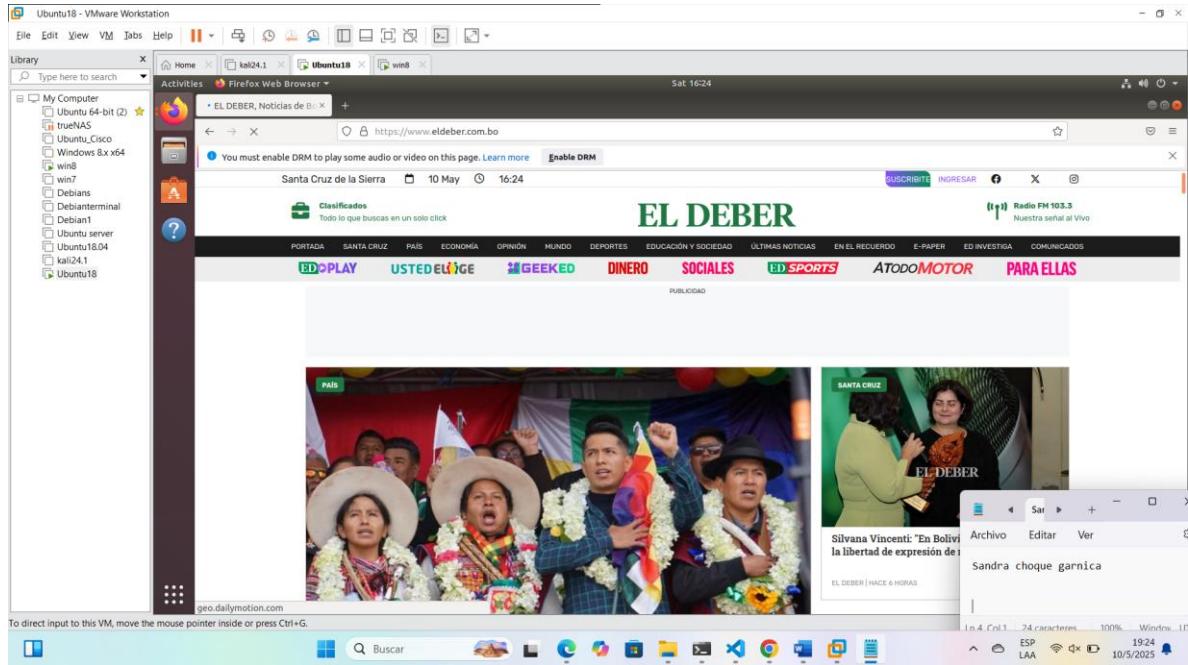
```

root@ubuntu:~# nft add rule inet filterWeb OUTPUT ip daddr @allowed_ips accept
root@ubuntu:~# nft add rule inet filterWeb OUTPUT tcp dport @http_ports drop
root@ubuntu:~# nft list ruleset
table inet filter {
    chain output {
        type filter hook output priority 0; policy accept;
    }
    chain forward {
        type filter hook forward priority 0; policy accept;
    }
    chain INPUT {
        type filter hook input priority 0; policy accept;
    }
}
table inet filterWeb {
    set http_ports {
        type Inet_service
        elements = [ http, https ]
    }
    set allowed_ips [
        typeIpv4_addr
        elements = [ 37.59.238.221, 45.79.163.254,
                    104.21.61.194, 104.22.74.193,
                    104.22.75.193, 172.67.20.27,
                    172.67.213.89 ]
    ]
    chain OUTPUT {
        type filter hook output priority 0; policy accept;
        ip daddr @allowed_ips accept
        tcp dport @http_ports drop
    }
}

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5)



En este caso el acceso a YouTube no funciona debio a que las ip habilitados son de otras paginas web y no haci de YouTube como se puede ver en la captura

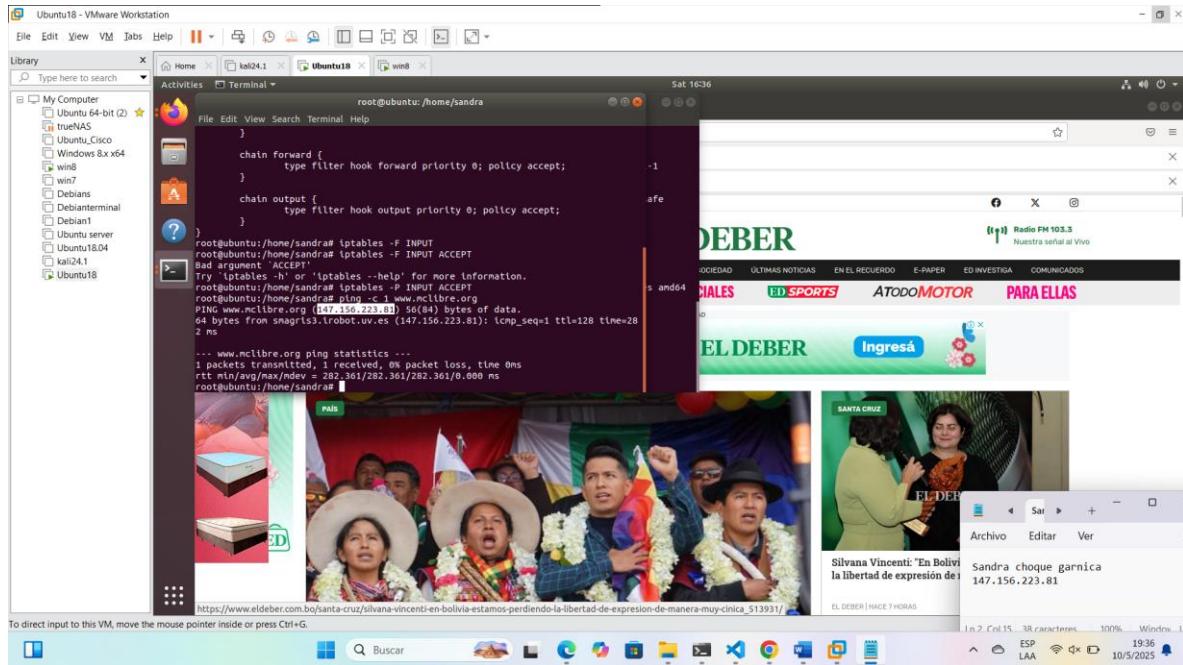
EVALUACION

1.- Saddr es la dirección de origen y la daddr es la dirección destino en este caso la saddr como se puede ver es la que identifica el dispositivo que envía el paquete, filtra el tráfico de red

2.- Es importante porque se garantiza que las reglas de cadena se procesen en el orden correcto por ej si una cadena tiene una prioridad alta por la cual se procesaran las reglas de la primera cadena con nft add chain filter priority 5 la prioridad de la cadena será 5 con en este caso

3.-

1) obtener ip



2.

