

<b>Universidad Autónoma Tomás Frías</b>	<b>Nota</b>
<b>Ingeniería de Sistemas</b>	
<b>SIS 737 – SEGURIDAD DE SISTEMAS</b>	
<b>DOCENTE: ING. ALEXANDER DURÁN</b>	
<b>NOMBRE: UNIV. SAAVEDRA MARCA PATRICIA EMILIA</b>	<b>RU: 109457</b>
<b>LABORATORIO 9: IPTABLES / NFTABLES</b>	

## PROPOSITO

Aprender a configurar reglas de firewall utilizando IPtables y NFtables.

## COMPETENCIA

La seguridad es esencial en toda organización. Este laboratorio permite desarrollar conocimientos básicos sobre la configuración de reglas de firewall a nivel del kernel de Linux con las herramientas IPtables y NFtables, que permiten implementar mecanismos de protección ante accesos no autorizados.

## DESCRIPCIÓN

Implementar dos escenarios:

1. Introducción a comandos, sintaxis y funcionamiento básico de IPtables y NFtables.
  2. Simulación de un entorno educativo con restricción de acceso a páginas web y por direcciones MAC.
- 

## RECURSOS

- Máquina Virtual Ubuntu 18
  - Máquina Virtual Kali Linux
  - Todas deben estar en el mismo segmento de red.
- 

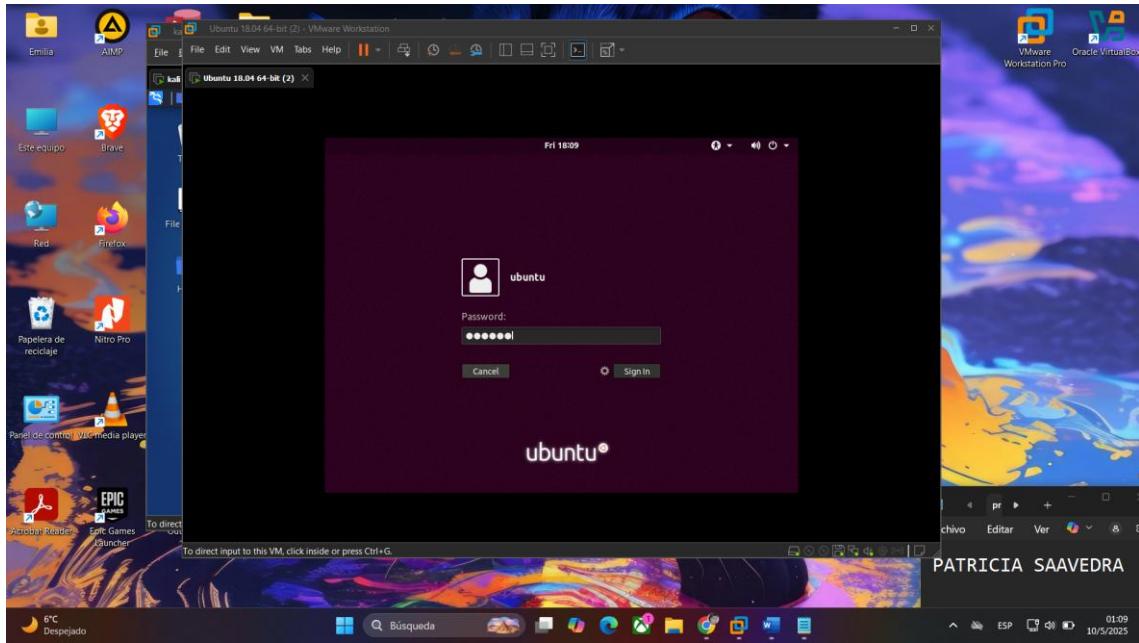
## PASOS PREVIOS

**PASO 1: Acceder a la terminal de Ubuntu y Kali como superusuario.**

**Credenciales:**

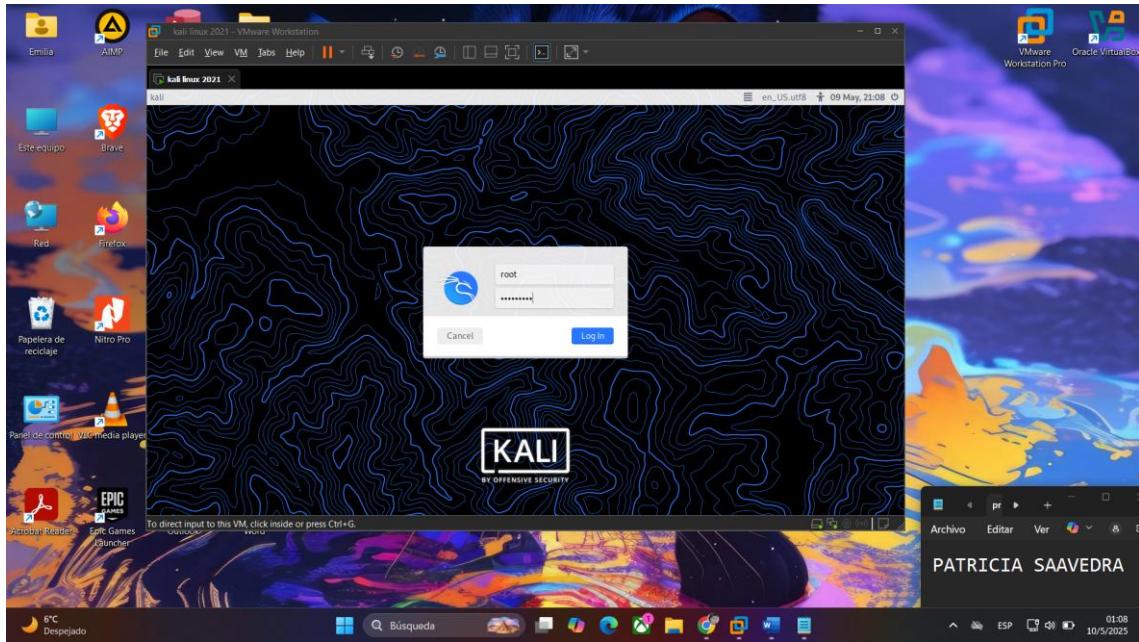
- **Ubuntu:**

- Usuario: ubuntu
- Password: ubuntu



- **Kali Linux:**

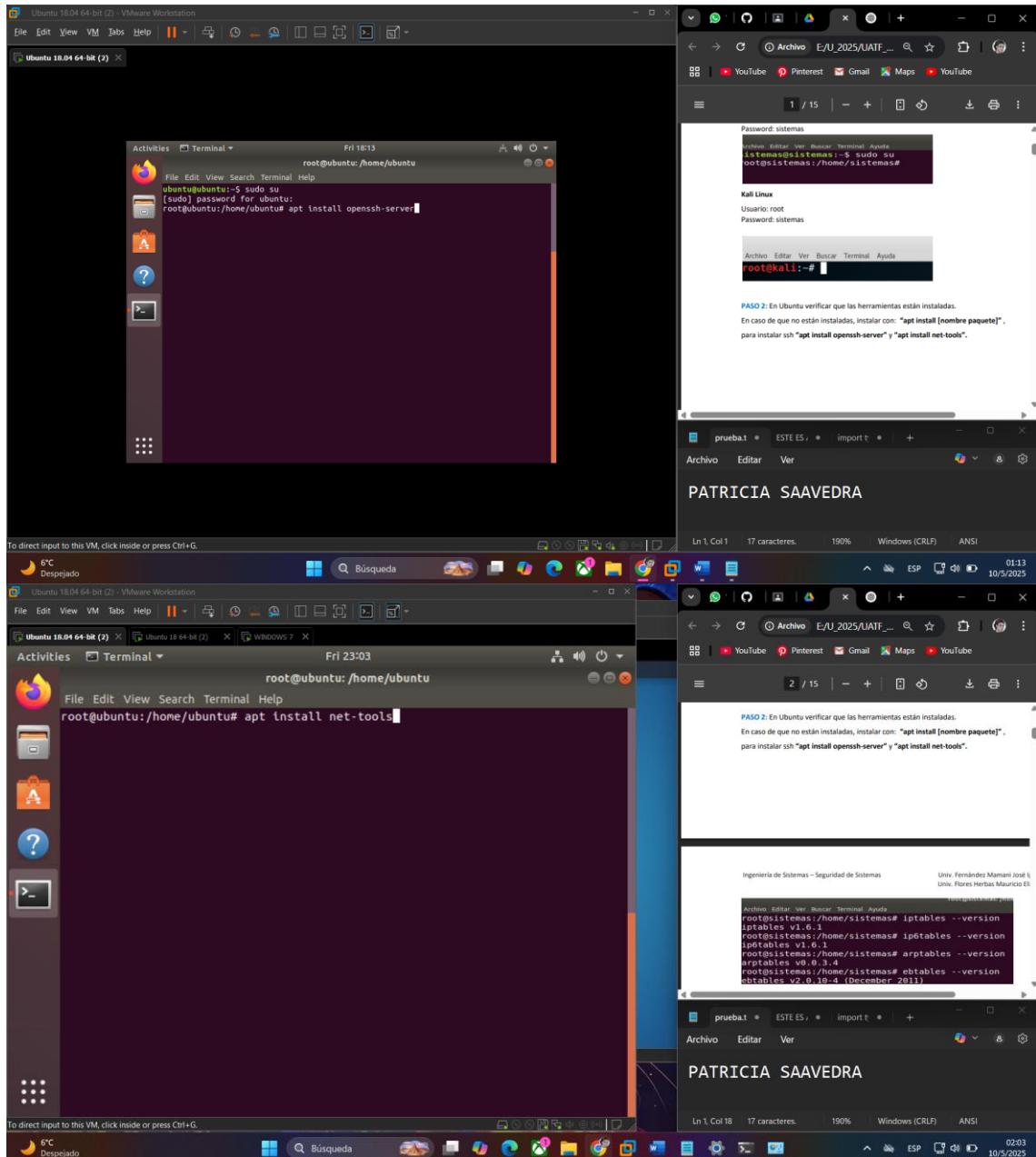
- Usuario: kali
- Password: kali



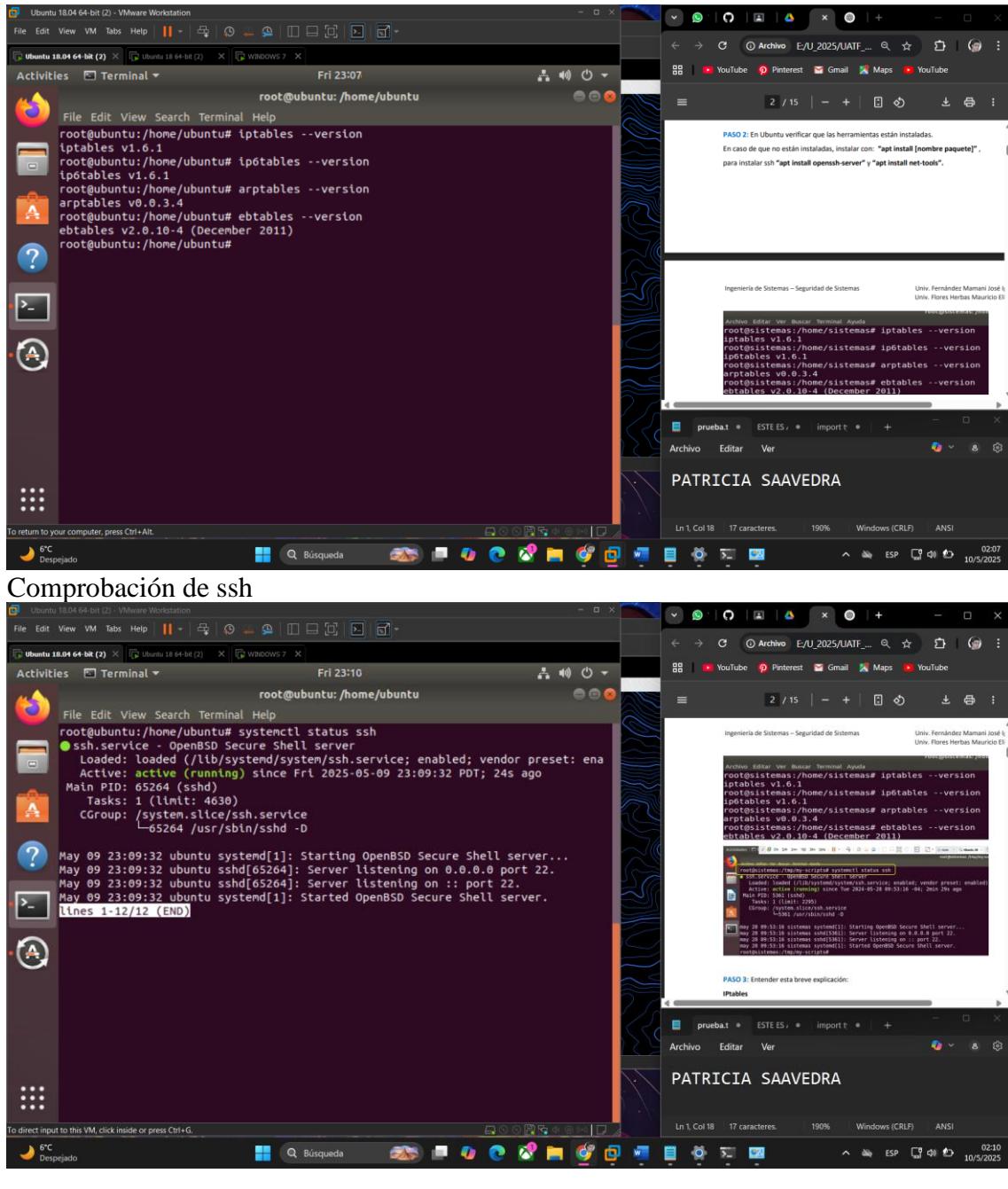
## PASO 2: Verificar que las herramientas necesarias estén instaladas.

Si no están instaladas, ejecutar:

```
apt install [nombre paquete]
apt install openssh-server
apt install net-tools
```



Comprobación de versiones



# **EXPLICACIÓN BÁSICA DE IPTABLES**

IPtables es una herramienta de línea de comandos para configurar reglas de firewall.

## Estructura:

- Las reglas están organizadas en **tablas** y **cadenas (chains)**.
  - Cada cadena contiene una lista de reglas que filtran los paquetes.
  - Cada regla tiene un objetivo (target):
    - DROP: descarta el paquete.
    - ACCEPT: permite el paso del paquete.

## Tablas comunes:

- filter (usada en este laboratorio)
- nat
- mangle

## Cadenas en la tabla filter:

- INPUT: paquetes dirigidos al sistema.
- FORWARD: paquetes reenviados.
- OUTPUT: paquetes generados por el sistema.
- (también existen PREROUTING y POSTROUTING en otras tablas)

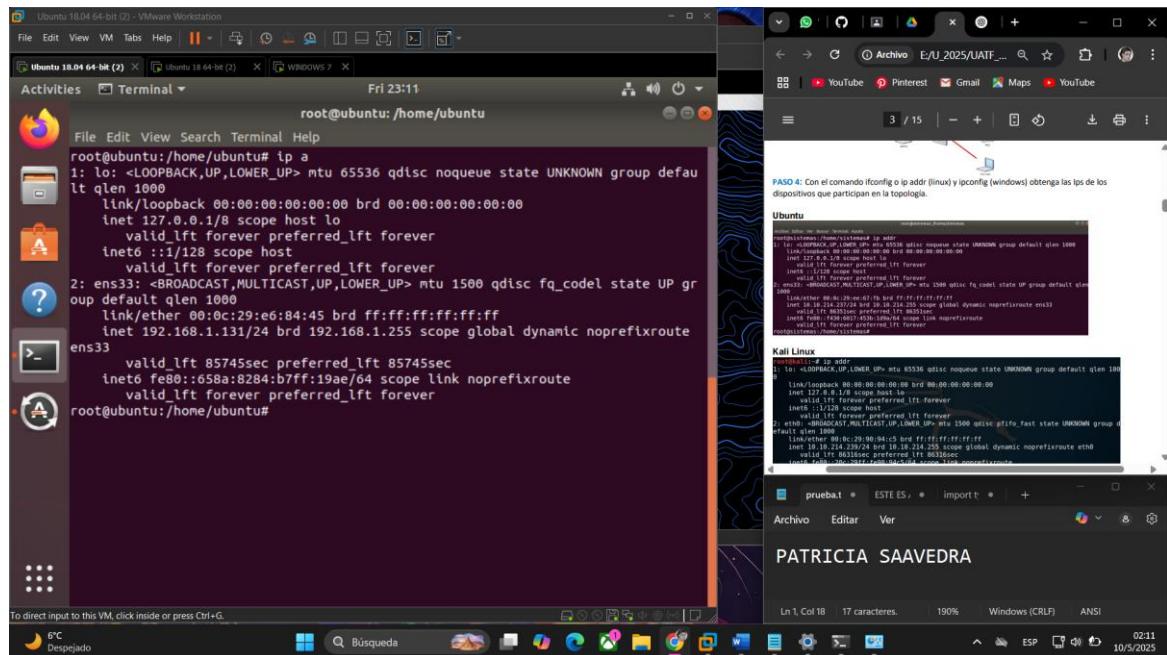
## Sintaxis básica:

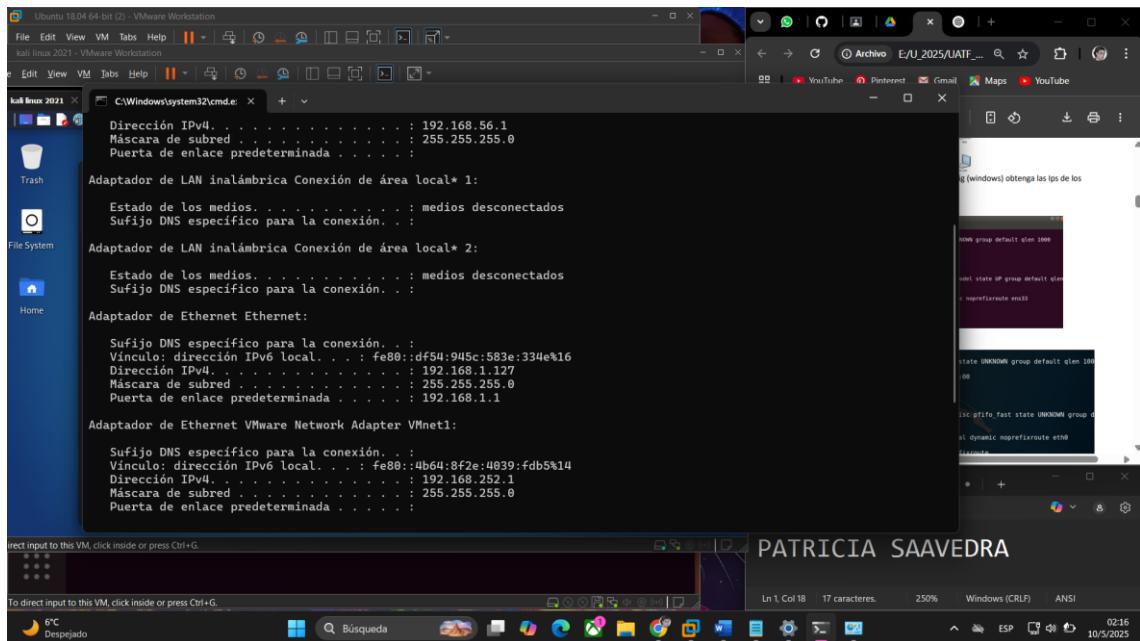
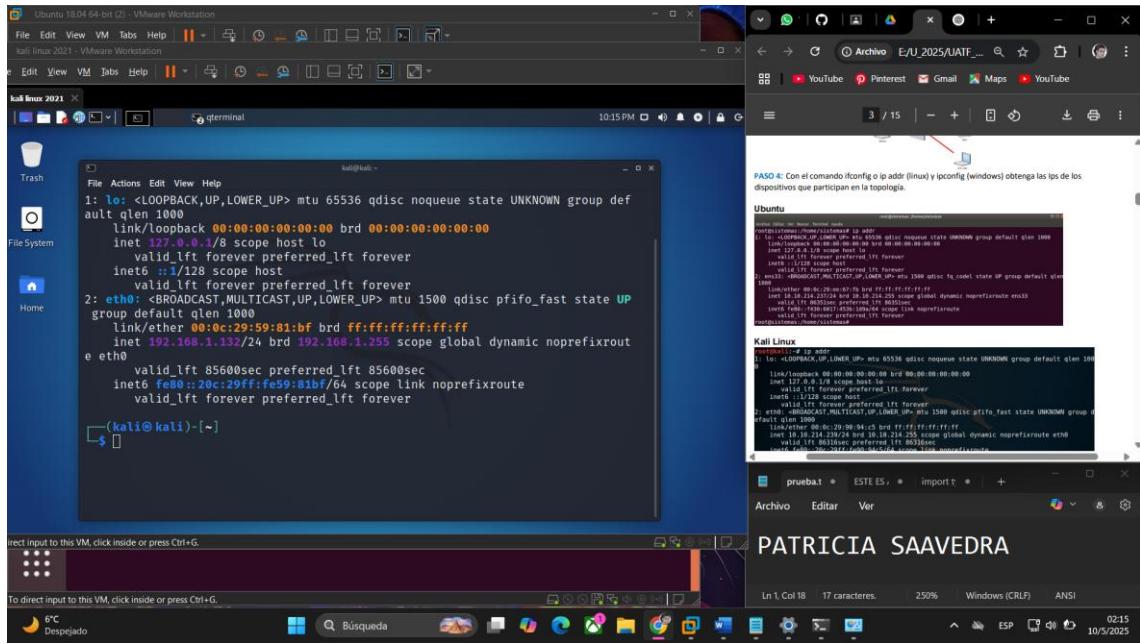
```
bash
CopiarEditar
iptables [-t tabla] -[opciones] [chain/regla]
```

## PASO 4: Obtener direcciones IP de las máquinas

Usar:

- ifconfig o ip addr en Linux
- ipconfig en Windows





### Tabla de direcciones IP:

Máquina virtual o dispositivo	Dirección IP
Ubuntu	192.168.1.131 /24
Kali Linux	192.168.1.132 /24
Windows (Máquina física)	192.168.1.127 /24

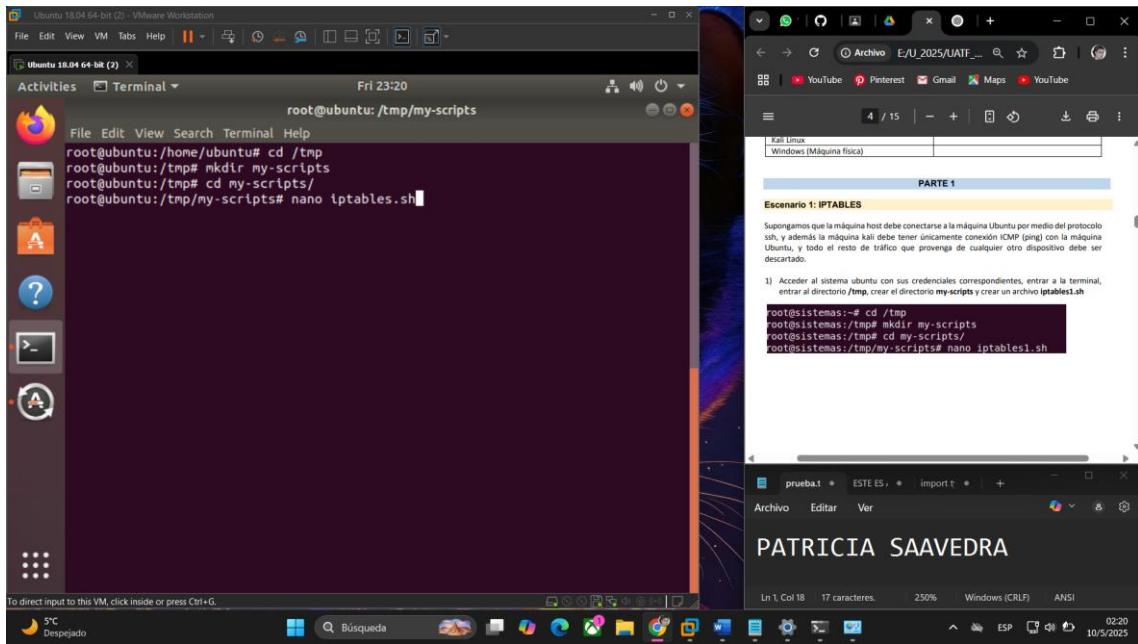
# PARTE 1 – Escenario 1: IPTABLES

## Objetivo:

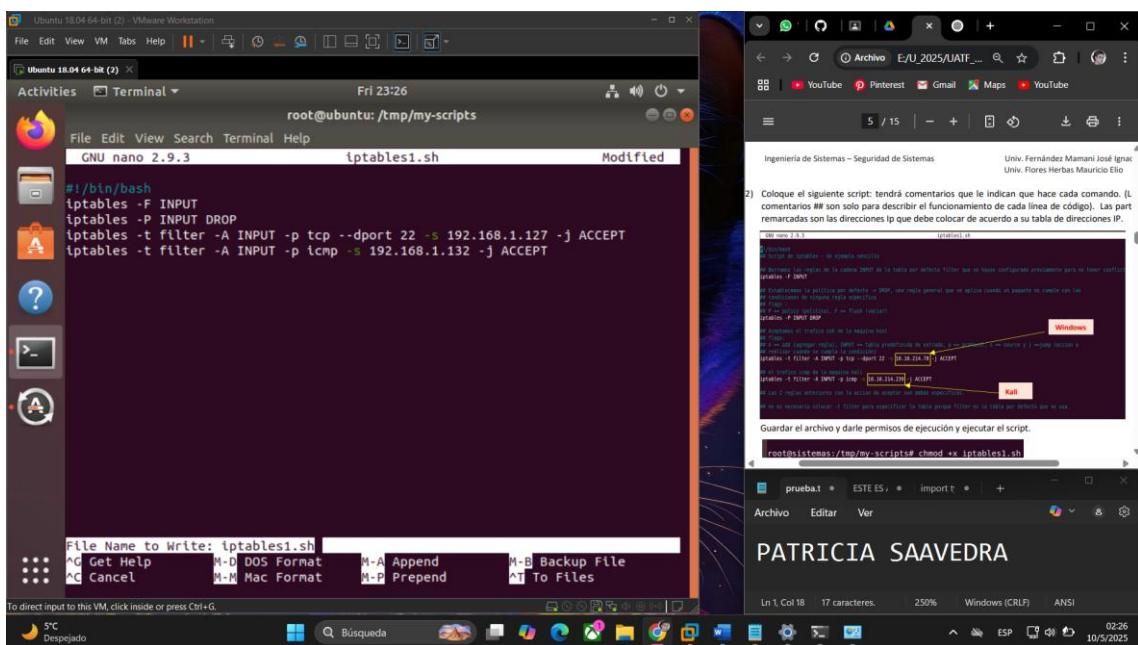
- Host → Ubuntu (SSH)
- Kali → Ubuntu (solo ICMP/ping)
- Todo otro tráfico → descartado

## Procedimiento:

1. Iniciar sesión en Ubuntu.
2. Crear directorio y archivo en /tmp/my-scripts/iptables1.sh.

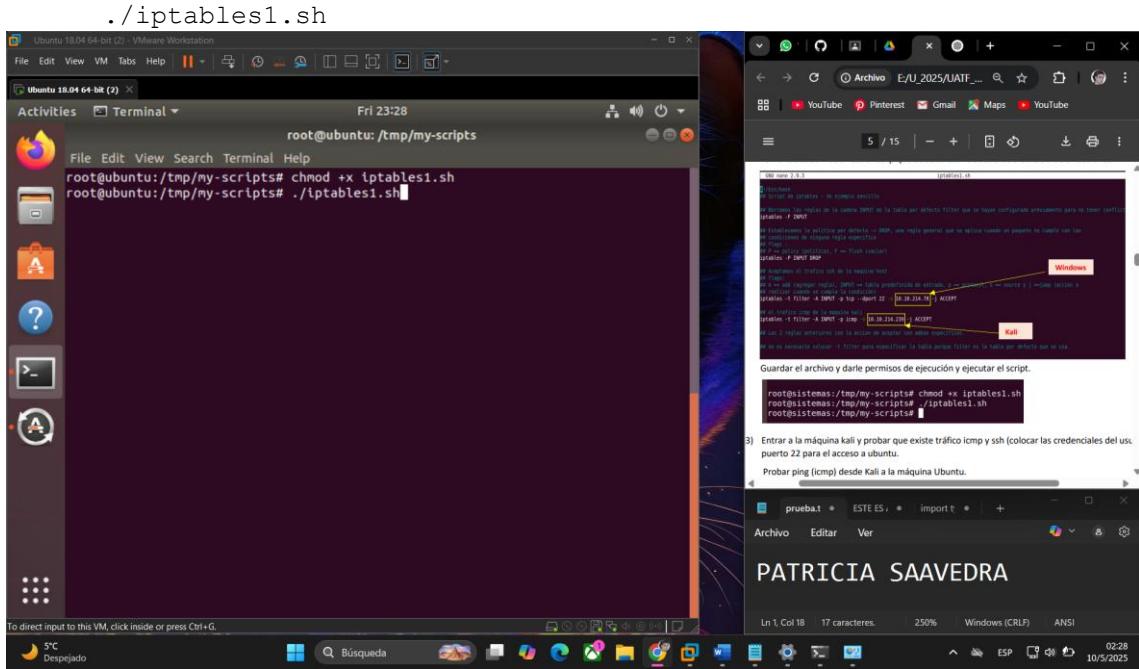


3. Insertar el script con comentarios descriptivos.



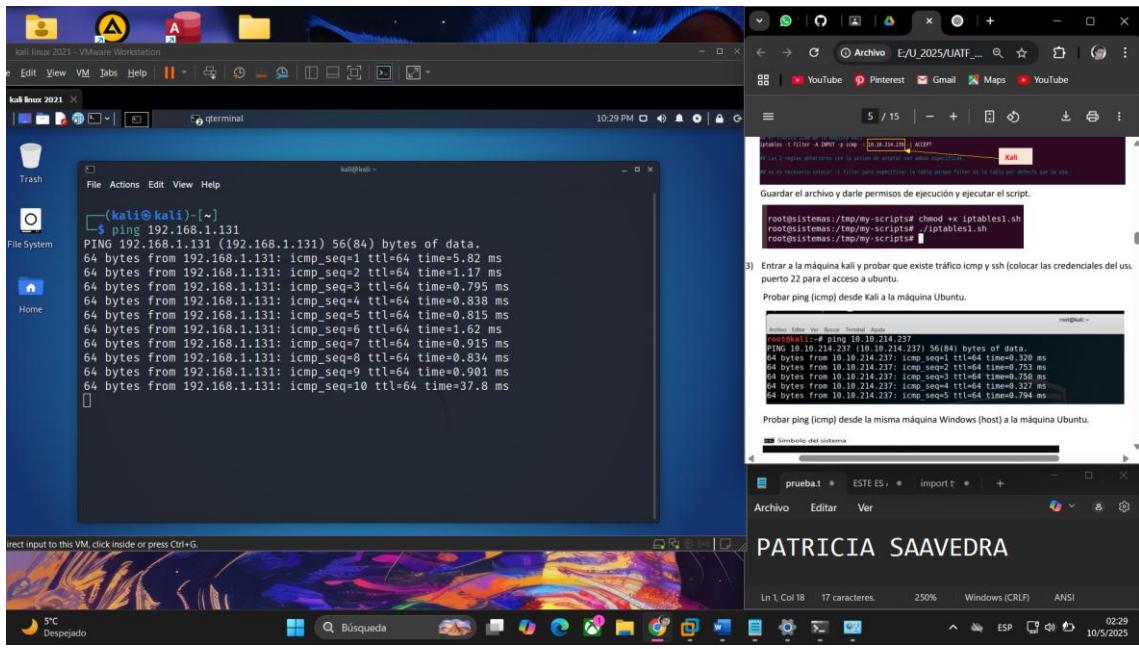
4. Dar permisos de ejecución:

```
chmod +x iptables1.sh
```



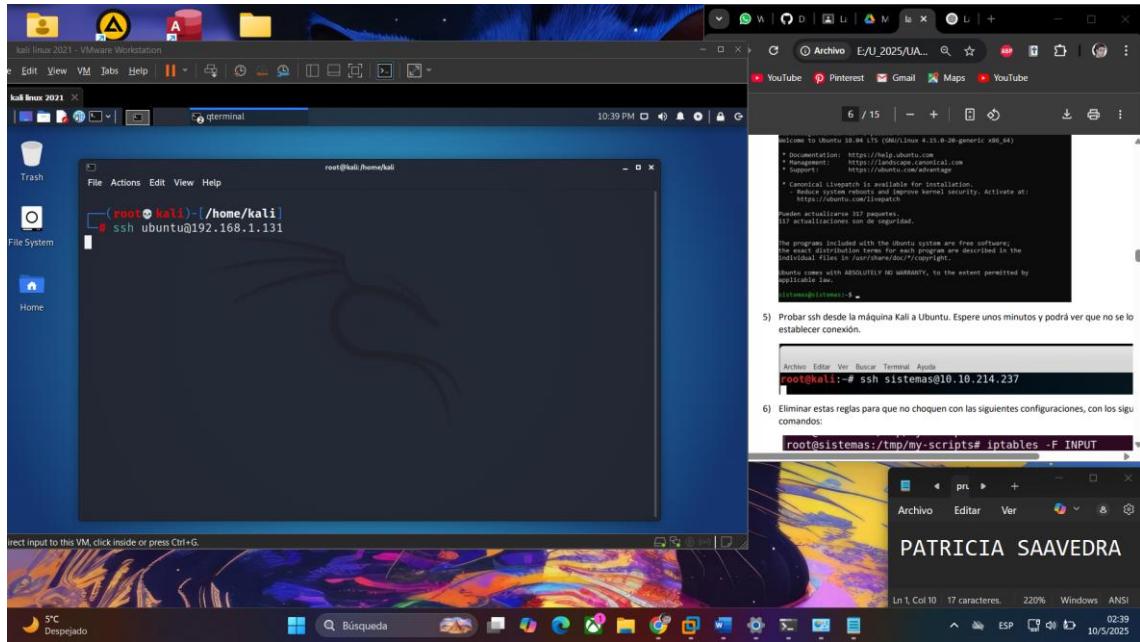
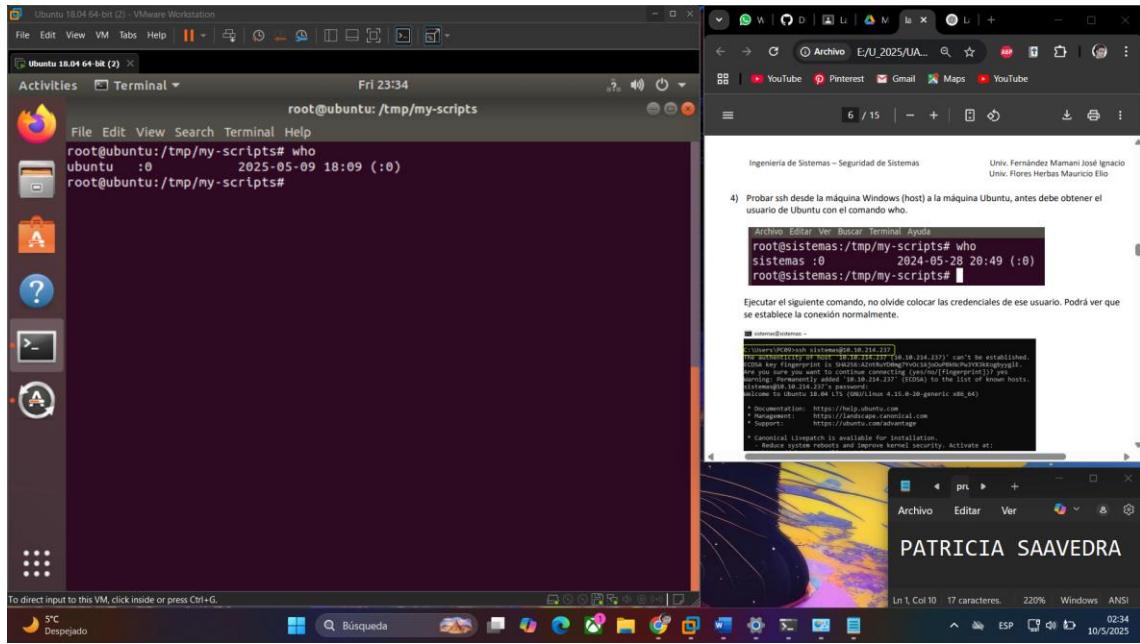
## 5. Verificar tráfico:

- o Kali → ping a Ubuntu ✓

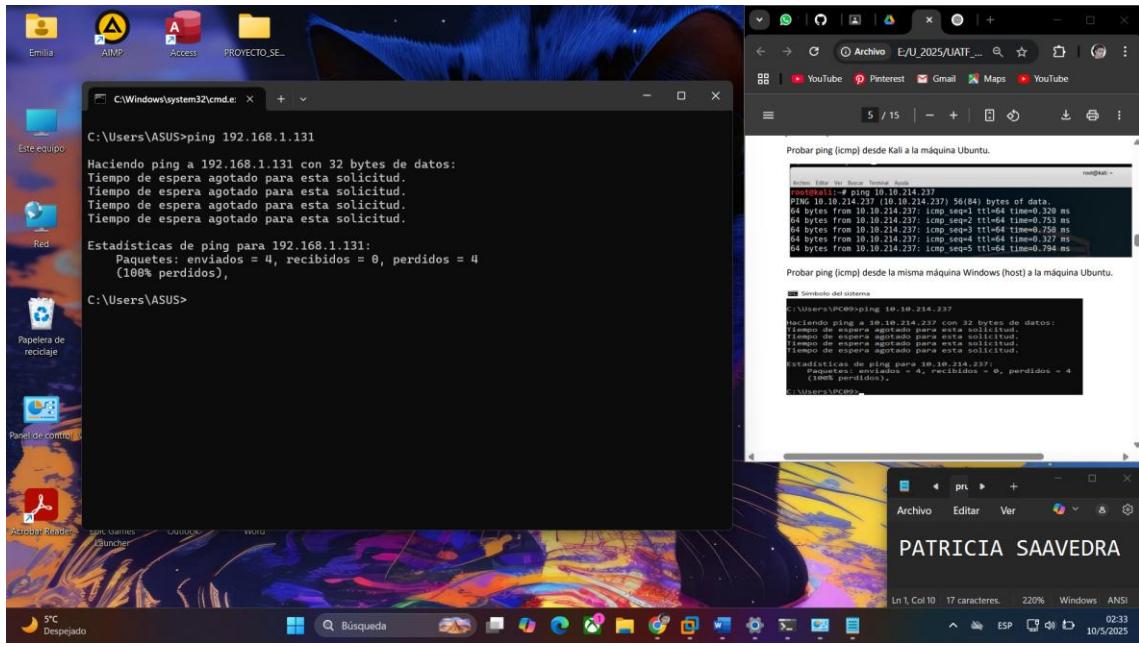


- o Kali → SSH a Ubuntu ✗

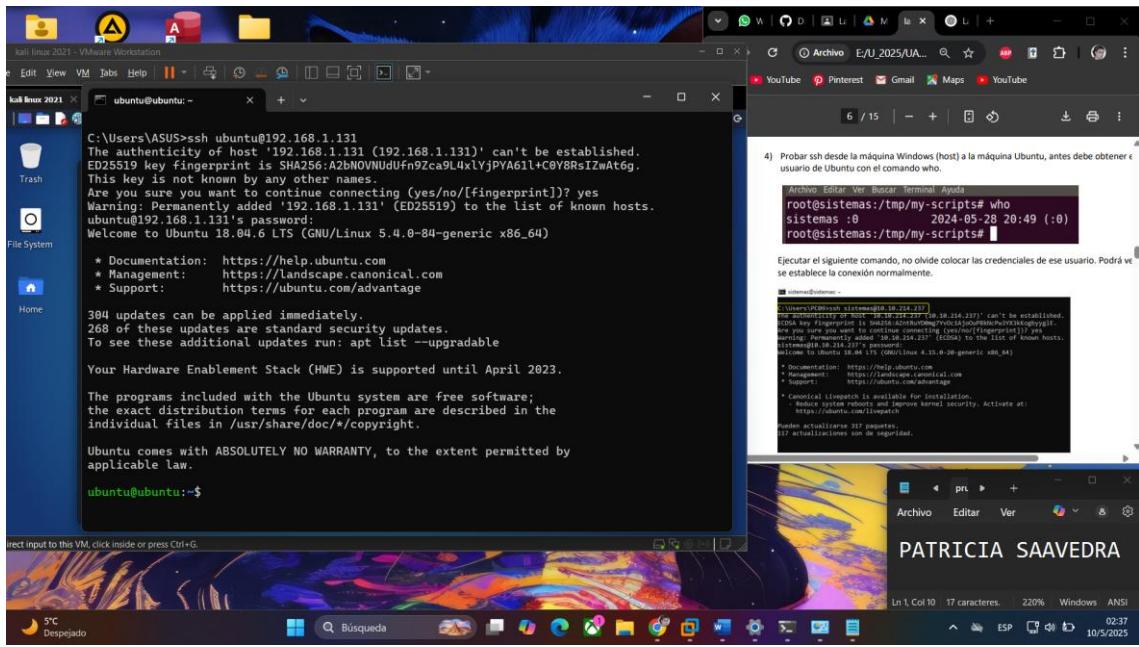
Who en Ubuntu:



- o Windows → ping a Ubuntu X



- Windows → SSH a Ubuntu ✓



6. Eliminar las reglas anteriores y ver resultados:

```
iptables -F INPUT  
iptables -P INPUT ACCEPT  
iptables -L
```

Ubuntu 18.04 64-bit (2) - VMware Workstation

Activities Terminal Fri 23:41

```
root@ubuntu:/tmp/my-scripts#
File Edit View Search Terminal Help
root@ubuntu:/tmp/my-scripts# who
ubuntu :0 2025-05-09 18:09 (:0)
root@ubuntu:/tmp/my-scripts# iptables -F INPUT
root@ubuntu:/tmp/my-scripts# iptables -P INPUT ACCEPT
root@ubuntu:/tmp/my-scripts# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@ubuntu:/tmp/my-scripts#
```

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

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

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
Verificar las reglas configuradas, con el siguiente comando:
root@sistemas:/tmp/my-scripts# iptables -L
```

## Escenario 2: NFTABLES

NFtables es una versión más moderna, con sintaxis simplificada.

### Instalación y Configuración:

#### 1. Actualizar sistema e instalar nftables:

```
sudo apt-get update
sudo apt-get install nftables
```

Ubuntu 18.04 64-bit (2) - VMware Workstation

Activities Terminal Fri 23:43

```
root@ubuntu:/tmp/my-scripts#
File Edit View Search Terminal Help
root@ubuntu:/tmp/my-scripts# sudo apt-get update
```

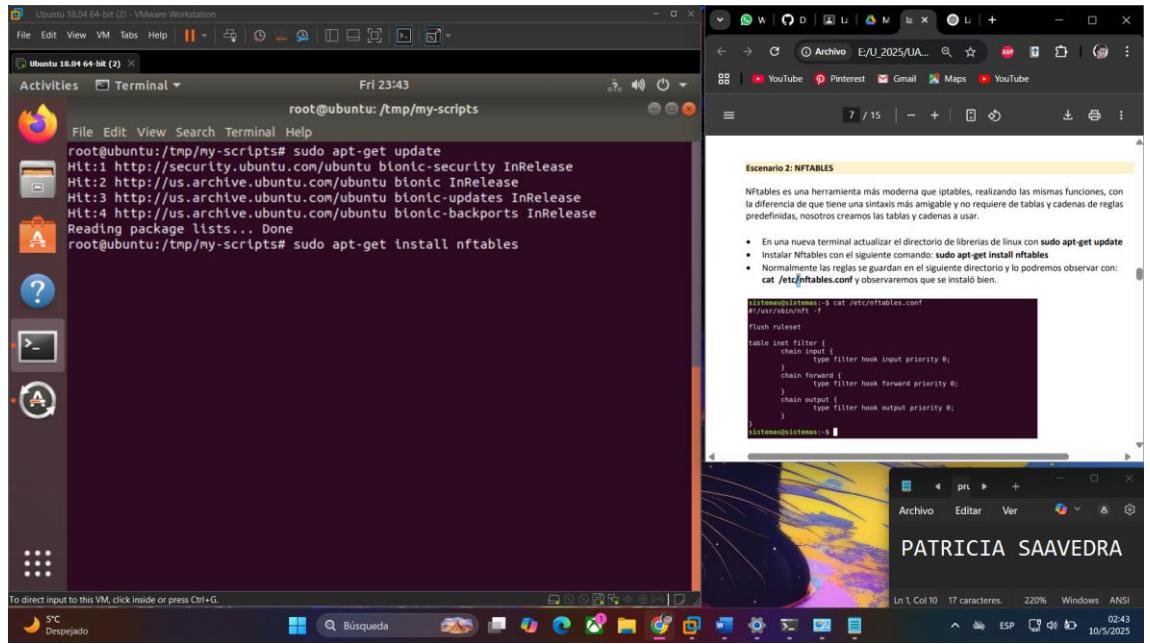
To direct input to this VM, click inside or press Ctrl+G.

Escenario 2: NFTables

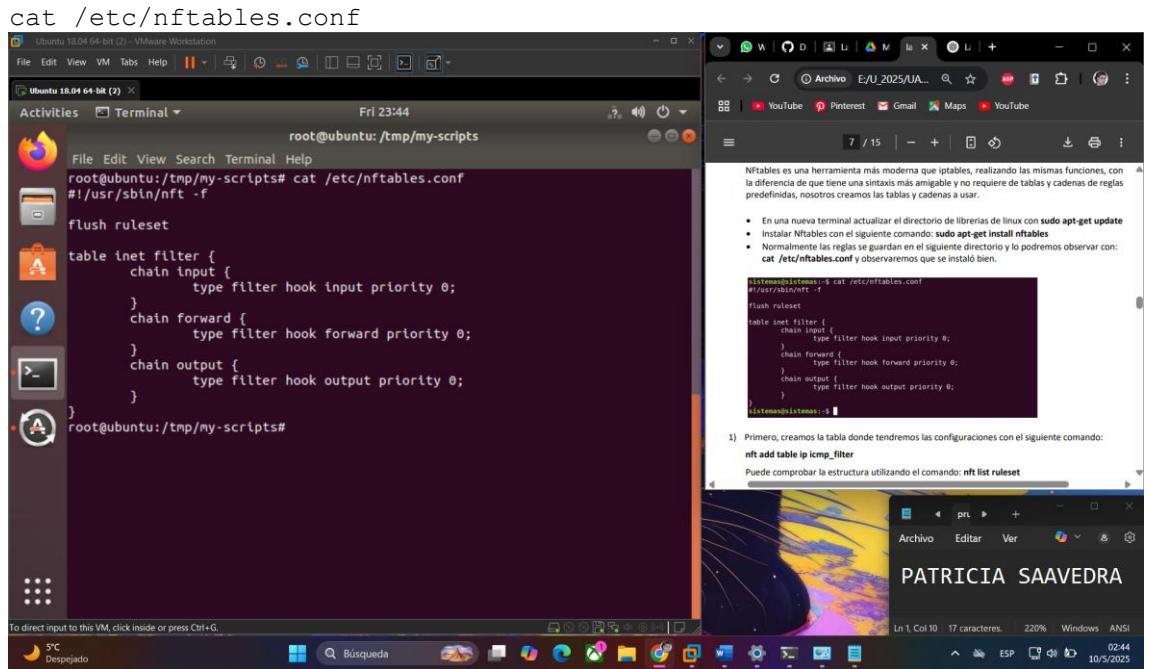
NFTables es una herramienta más moderna que iptables, realizando las mismas funciones, con la diferencia de que tiene una sintaxis más amigable y no requiere de tablas y cadenas de reglas predefinidas, nosotros creamos las tablas y cadenas a usar.

- En una nueva terminal actualizar el directorio de librerías de linux con `sudo apt-get update`
- Instalar Nftables con el siguiente comando: `sudo apt-get install nftables`
- Normalmente las reglas se guardan en el siguiente directorio y lo podemos observar con: `cat /etc/nftables.conf` y observaremos que se instaló bien.

```
#!/usr/sbin/nft -f
flush ruleset
table inet filter {
    chain input {
        type filter hook input priority 0;
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}
```



## 2. Verificar configuración:



## 3. Crear tabla y cadena:

```

nft add table ip icmp_filter
nft list ruleset

```

```

root@ubuntu:/tmp/my-scripts# nft add table ip icmp_filter
root@ubuntu:/tmp/my-scripts# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority 0; policy accept;
    }
    chain forward {
        type filter hook forward priority 0; policy accept;
    }
    chain output {
        type filter hook output priority 0; policy accept;
    }
}
table ip icmp_filter {
}
root@ubuntu:/tmp/my-scripts#

```

1) Primero, creamos la tabla donde tendremos las configuraciones con el siguiente comando:  
`nft add table ip icmp_filter`

Puede comprobar la estructura utilizando el comando: `nft list ruleset`

```

root@sistemas:~# nft add table ip icmp_filter
root@sistemas:~# nft list ruleset
root@sistemas:~# 

```

`nft add chain ip icmp_filter INPUT '{ type filter hook input priority 0; policy drop; }'`

```

root@ubuntu:/tmp/my-scripts# nft add chain ip icmp_filter INPUT '{ type filter hook input priority 0; policy drop; }'
root@ubuntu:/tmp/my-scripts# nft list ruleset
table ip icmp_filter {
    chain INPUT {
        type filter hook input priority 0; policy drop;
    }
}
root@ubuntu:/tmp/my-scripts#

```

Ingeniería de Sistemas – Seguridad de Sistemas  
Univ. Fernández Mamani José Ignacio  
Univ. Flores Herbas Mauricio Elío

2) Ahora agregamos el grupo de acceso o chain donde se implementarán las reglas:  
`nft add chain ip icmp_filter INPUT '{ type filter hook input priority 0; policy drop; }'`

```

root@sistemas:~# nft add chain ip icmp_filter INPUT '{ type filter hook input priority 0; policy drop; }'
root@sistemas:~# nft list ruleset
table ip icmp_filter {
    chain INPUT {
        type filter hook input priority 0; policy drop;
    }
}
root@sistemas:~# 

```

**typefilter:** Indica que la cadena se utilizará para filtrar paquetes según las reglas que establezcas.  
**hook input:** Indica que la cadena estará conectada al punto de enganche de entrada, lo que significa que manejará los paquetes que ingresan al sistema.  
**priority 0:** Establece la prioridad de la Cadena. Una prioridad de 0 indica que esta cadena se procesa antes que otras cadenas con una prioridad mayor.

#### 4. Agregar reglas:

```

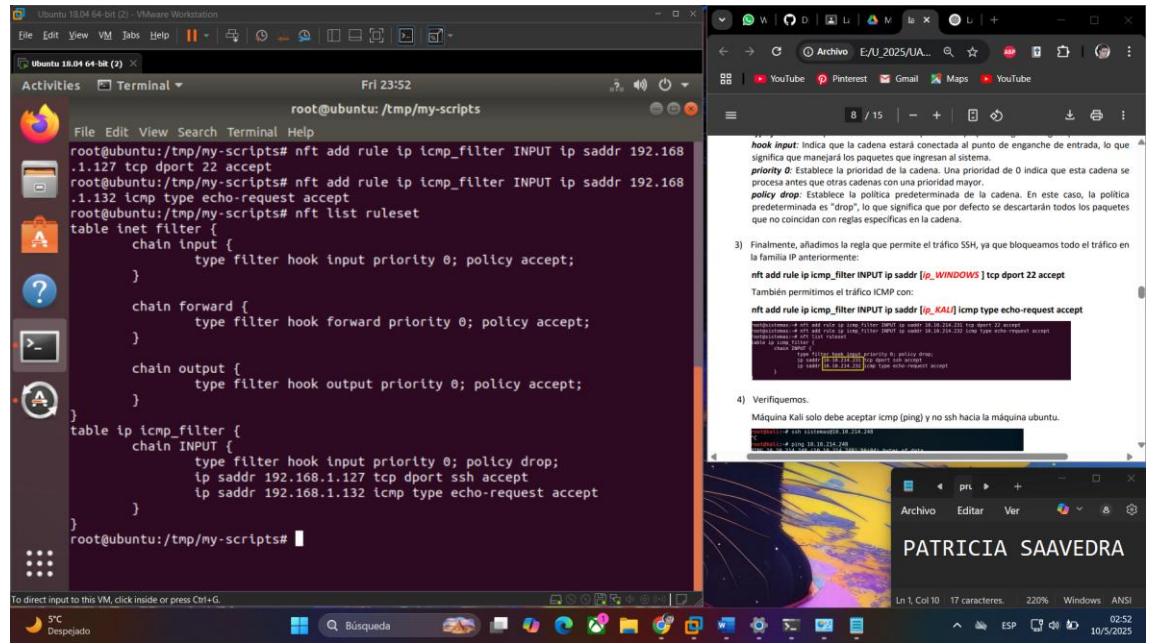
nft add rule ip icmp_filter INPUT ip saddr [ip_WINDOWS] tcp dport
22 accept

```

```

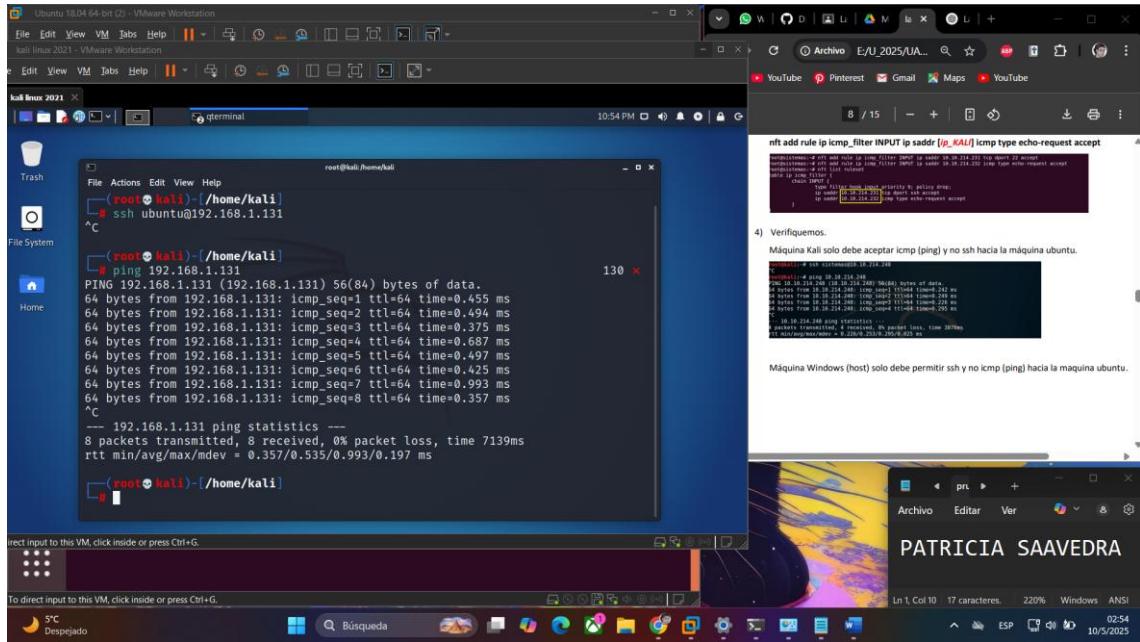
nft add rule ip icmp_filter INPUT ip saddr [ip_KALI] icmp type
echo-request accept

```

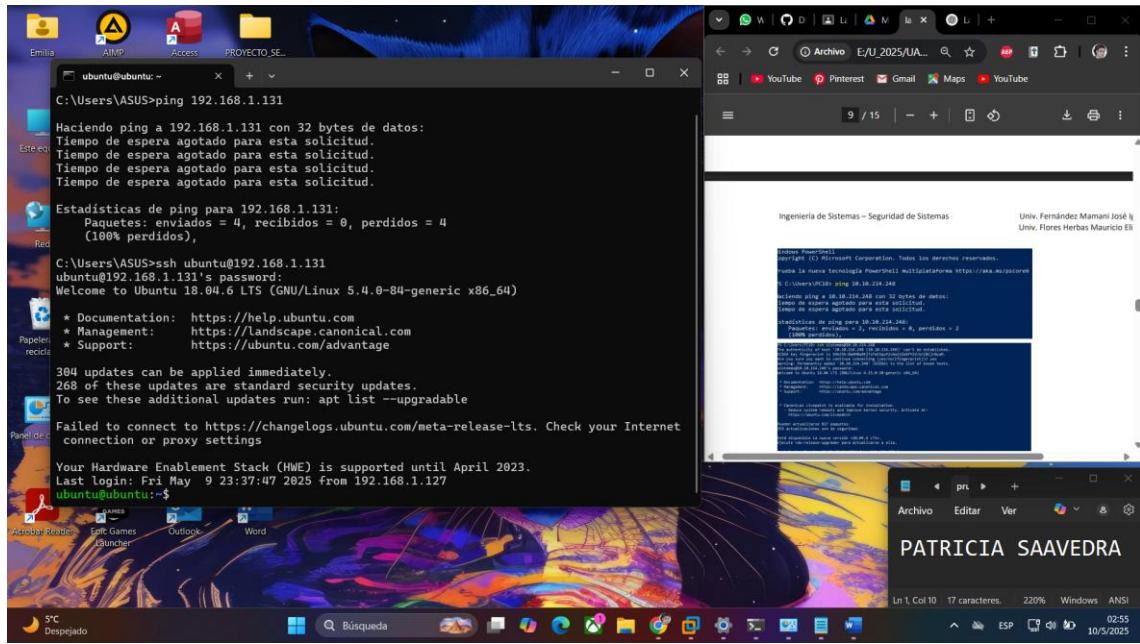


## 5. Verificar:

- Kali → SSH (✗), ICMP (✓).



- Windows → ICMP (X), SSH (✓).



## 6. Eliminar reglas:

```
nft delete table ip icmp_filter
nft list ruleset
```

```
File Edit View Search Terminal Help
root@ubuntu:/tmp/my-scripts# nft delete table ip icmp_filter
root@ubuntu:/tmp/my-scripts# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority 0; policy accept;
    }
    chain forward {
        type filter hook forward priority 0; policy accept;
    }
    chain output {
        type filter hook output priority 0; policy accept;
    }
}
root@ubuntu:/tmp/my-scripts#
```

```
iptables -F INPUT
iptables -P INPUT ACCEPT
iptables -L
```

5) Finalmente, si desea guardar las reglas configuradas permanentemente, **en este caso NO ejecute el comando**  
 "nft list ruleset > /etc/nftables.conf" (No ejecutar)  
 Tenga en cuenta que, si no ejecuta este comando, las reglas configuradas no se guardarán y se perderán después de reiniciar la máquina.

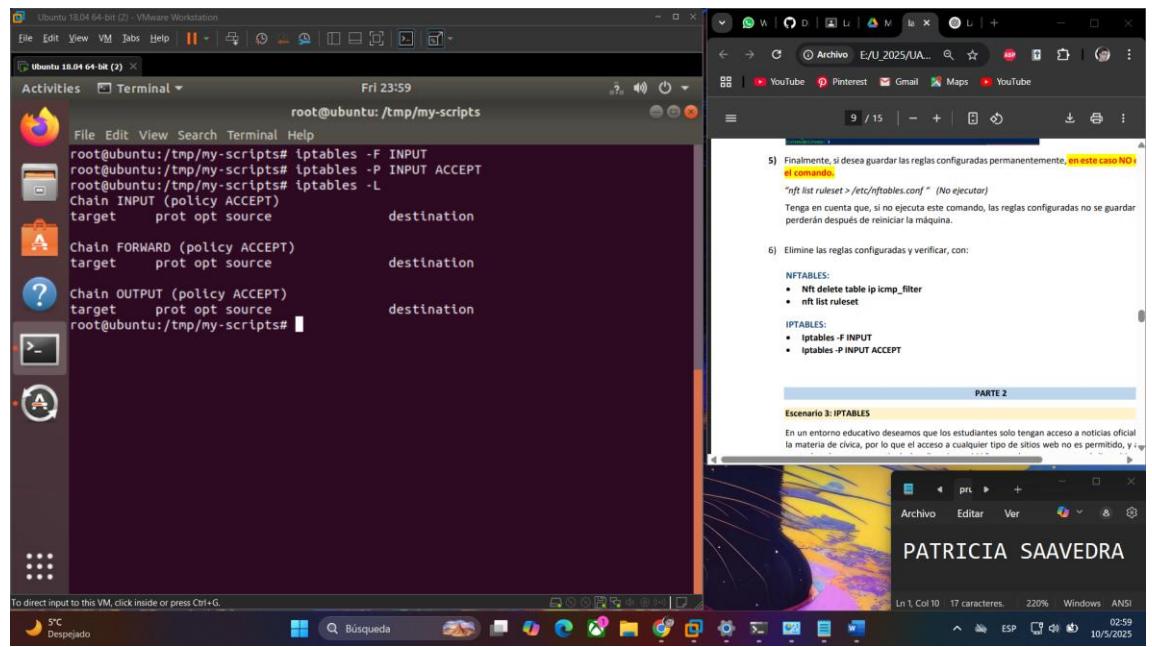
6) Elimine las reglas configuradas y verificar, con:

- NFTABLES:
  - nft delete table ip icmp\_filter
  - nft list ruleset
- IPTABLES:
  - iptables -F INPUT
  - iptables -P INPUT ACCEPT

PARTE 2

Escenario 3: IPTABLES

En un entorno educativo deseamos que los estudiantes solo tengan acceso a noticias oficiales para la materia de cívica, por lo que el acceso a cualquier tipo de sitios web no es permitido, y además



## PARTE 2 – Escenario 3: IPTABLES con restricción web y MAC

### Objetivo:

Permitir acceso solo a sitios web oficiales (por IP) y restringir acceso por MAC.

#### Escenario

#### 3:

#### IPTABLES

En un entorno educativo deseamos que los estudiantes solo tengan acceso a noticias oficiales para la materia de cívica, por lo que el acceso a cualquier tipo de sitios web no es permitido, y además controlar el acceso a partir de las direcciones MAC para el acceso remoto al dispositivo de los estudiantes.

La siguiente tabla de direcciones IP permitidas de los dominios que solo se podrán acceder:

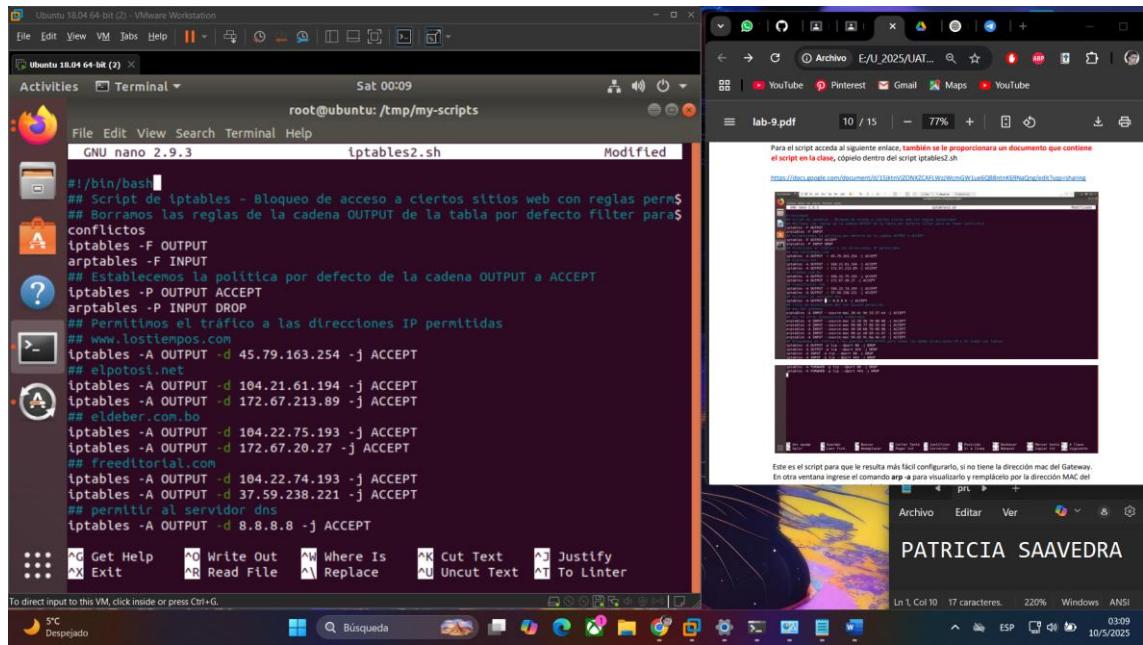
Dominios	Dirección IP
lostiempos.com	45.79.163.254
elpotosi.net	104.21.61.194
	172.67.213.89
eldeber.com.bo	104.22.75.193
	104.22.74.193
	172.67.20.27
freeditorial.com	37.59.238.221

Tabla de direcciones MAC permitida:

Dispositivo	MAC
Kali	12:34:56:78:90:00

Dispositivo	MAC
Kali	99:88:77:66:55:44
Kali	40:50:60:70:80:90

- Crear otro script con el nombre `iptables2.sh` en la misma carpeta `/tmp/my-scripts` y colocar el siguiente script.

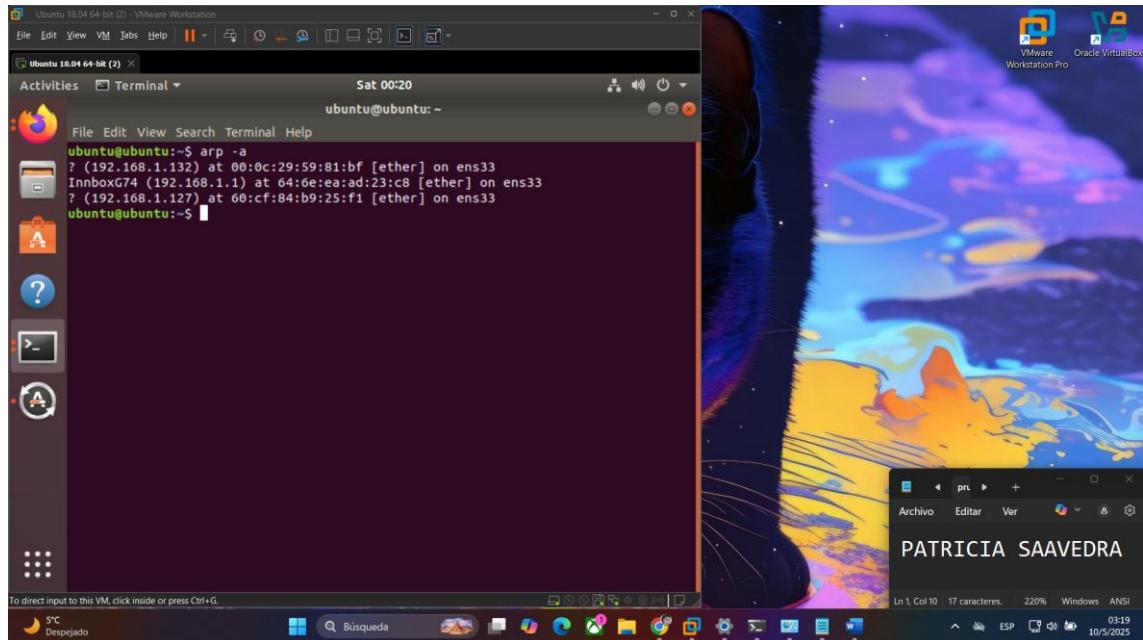


```

#!/bin/bash
## Script de iptables - Bloqueo de acceso a ciertos sitios web con reglas permisivas
## Borramos las reglas de la cadena OUTPUT de la tabla por defecto filter para no conflictar
iptables -F OUTPUT
arptables -F INPUT
## Establecemos la politica por defecto de la cadena OUTPUT a ACCEPT
iptables -P OUTPUT ACCEPT
arptables -P INPUT DROP
## Permitimos el trafico a las direcciones IP permitidas
## www.lostiempos.com
iptables -A OUTPUT -d 45.79.163.254 -j ACCEPT
## elpotosi.net
iptables -A OUTPUT -d 104.21.61.194 -j ACCEPT
iptables -A OUTPUT -d 172.67.213.89 -j ACCEPT
## eldeber.com.bo
iptables -A OUTPUT -d 104.22.75.193 -j ACCEPT
iptables -A OUTPUT -d 172.67.20.27 -j ACCEPT
## freedmortal.com
iptables -A OUTPUT -d 104.22.74.193 -j ACCEPT
iptables -A OUTPUT -d 37.59.238.221 -j ACCEPT
## permitir al servidor dns
iptables -A OUTPUT -d 8.8.8.8 -j ACCEPT

```

Este es el script para que le resulte más fácil configurarlo, si no tiene la dirección MAC del Gateway. En otra ventana ingrese el comando `arp -a` para visualizarlo y reemplácelo por la dirección MAC del script en caso de que no sea el mismo.



```

ubuntu@ubuntu:~$ arp -a
? (192.168.1.132) at 00:0c:29:59:81:bf [ether] on ens3
InnbboxG74 (192.168.1.1) at 64:6e:ea:ad:23:c8 [ether] on ens3
? (192.168.1.127) at 60:cf:b9:25:f1 [ether] on ens3
ubuntu@ubuntu:~$ 

```

```

Ubuntu 18.04 64-bit (2) - VMware Workstation
Activities Terminal Sat 02:44
root@ubuntu:/tmp/my-scripts
File Edit View Search Terminal Help
GNU nano 2.9.3 iptables2.sh Modified
## mac del gateway
arpTables -A INPUT --source-mac 64:de:ea:ad:23:c8 -j ACCEPT
## mac de otros dispositivos simulados
arpTables -A INPUT --source-mac 12:34:56:78:90:00 -j ACCEPT
arpTables -A INPUT --source-mac 99:88:77:66:55:44 -j ACCEPT
arpTables -A INPUT --source-mac 40:58:60:70:88:90 -j ACCEPT
arpTables -A INPUT --source-mac 00:ac:e0:b9:ce:d7 -j ACCEPT
arpTables -A INPUT --source-mac 94:65:9c:6a:4e:c9 -j ACCEPT
## Bloqueamos el tráfico a los puertos HTTP/HTTPS para todas las demás direcciones en todas las tablas
iptables -A OUTPUT -p tcp --dport 80 -j DROP
iptables -A OUTPUT -p tcp --dport 443 -j DROP
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP
iptables -A FORWARD -p tcp --dport 80 -j DROP
iptables -A FORWARD -p tcp --dport 443 -j DROP

```

Get Help Write Out Where Is Cut Text Justify Exit Read File Replace Uncut Text To Linter

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

5°C Despejado

Búsqueda

Archivo Editar Ver

PATRICIA SAAVEDRA

Ln 1 Col 10 17 caracteres 220% Windows ANSI

03:24 10/5/2025

## 2. Darle permisos de ejecución al script y ejecutarlo.

```
chmod +x /tmp/my-scripts/iptables2.sh
```

```
sudo /tmp/my-scripts/iptables2.sh
```

```

Ubuntu 18.04 64-bit (2) - VMware Workstation
Activities Terminal Sat 02:49
root@ubuntu:/tmp/my-scripts
File Edit View Search Terminal Help
root@ubuntu:/tmp/my-scripts# chmod +x iptables2.sh
root@ubuntu:/tmp/my-scripts# chmod +x iptables2.sh
root@ubuntu:/tmp/my-scripts# ./iptables2.sh
root@ubuntu:/tmp/my-scripts#

```

2) darle permisos de ejecución al script y ejecutarlo.

```
C:\Users\PC09\ping 10.10.214.237
Haciendo ping a 10.10.214.237 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
```

3) Entrar a la máquina Windows host y realizar ping a ubuntu, el mismo paso en Kali Linux. Ambos deben fallar ya que tienen direcciones MAC que no pertenecen a la lista.

4) Símbolo del sistema - ping 10.10.214.237

```
C:\Users\PC09\ping 10.10.214.237
Haciendo ping a 10.10.214.237 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
```

4) Trabajaremos con Kali para agregar direcciones mac, primero observe su dirección mac actual y su interfaz.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.214.237 brd 10.10.214.255 netmask 255.255.255.0 broadcast 10.10.214.255
      ...
```

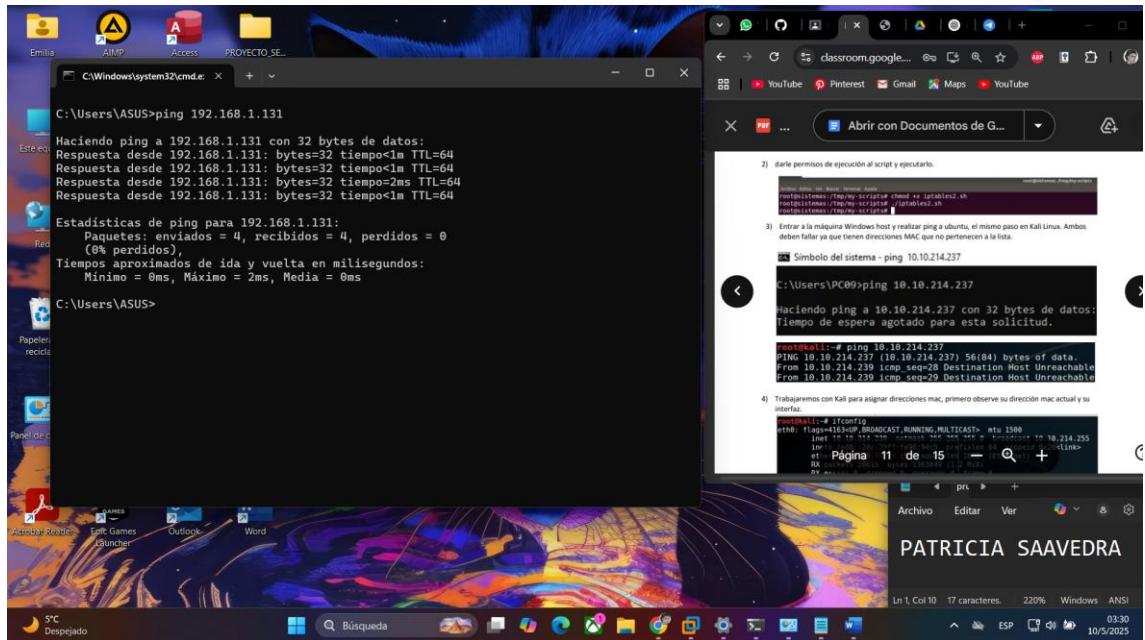
Patricia SAAVEDRA

Ln 1 Col 10 17 caracteres 220% Windows ANSI

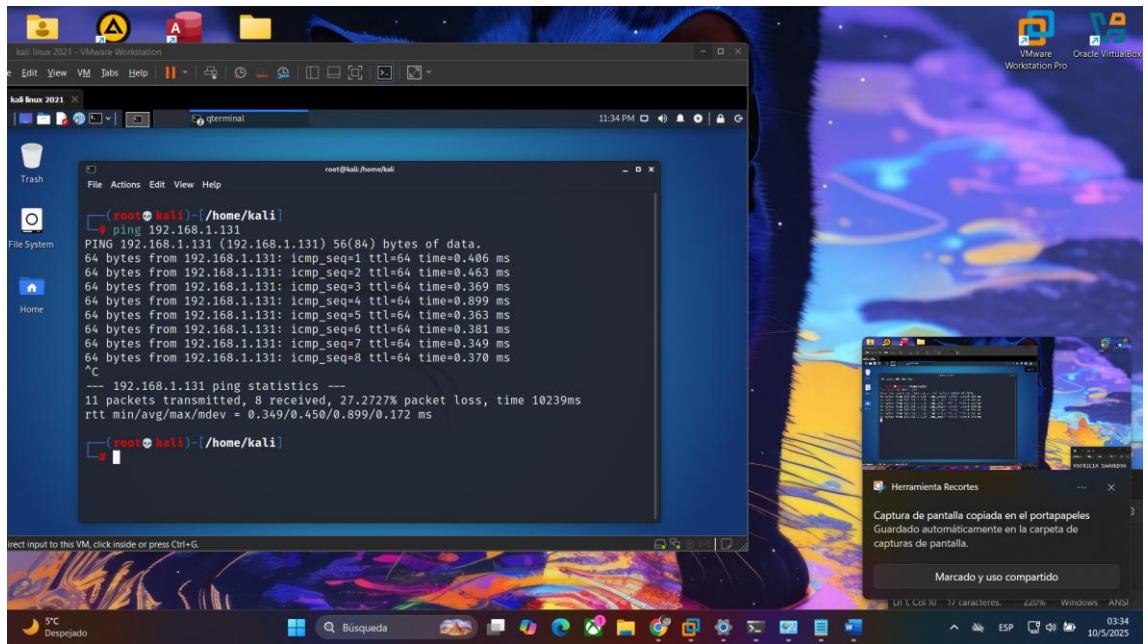
03:29 10/5/2025

## 3. Entrar a la máquina Windows host y realizar ping a Ubuntu, el mismo paso en Kali Linux. Ambos deben fallar ya que tienen direcciones MAC que no pertenecen a la lista. En mi caso ambos dieron ping con normalidad.

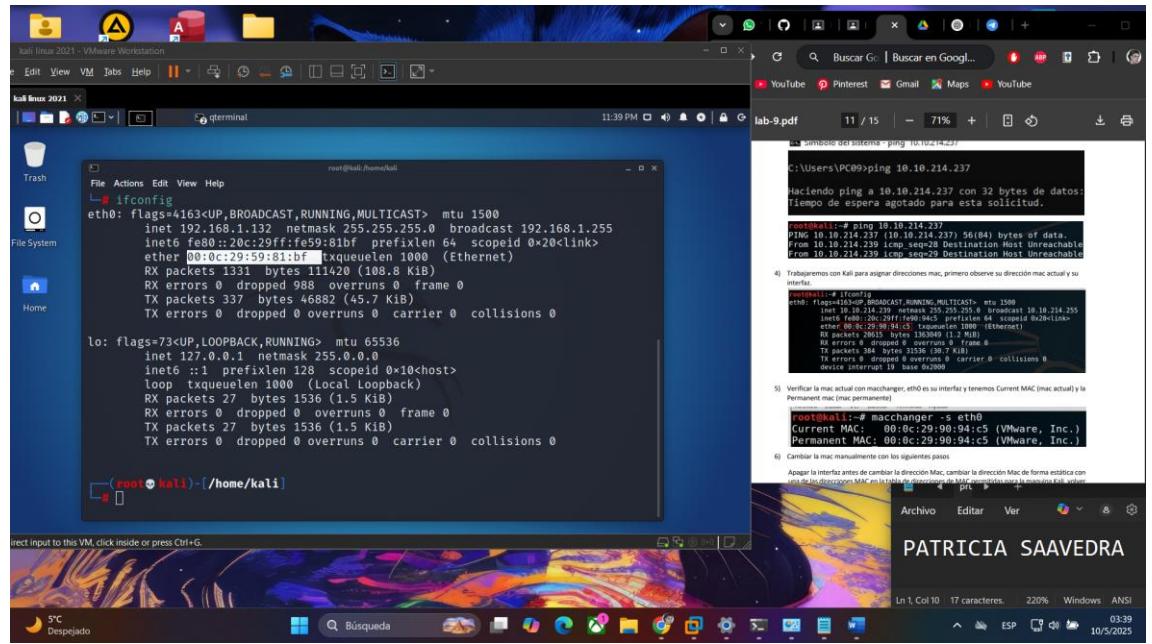
Host



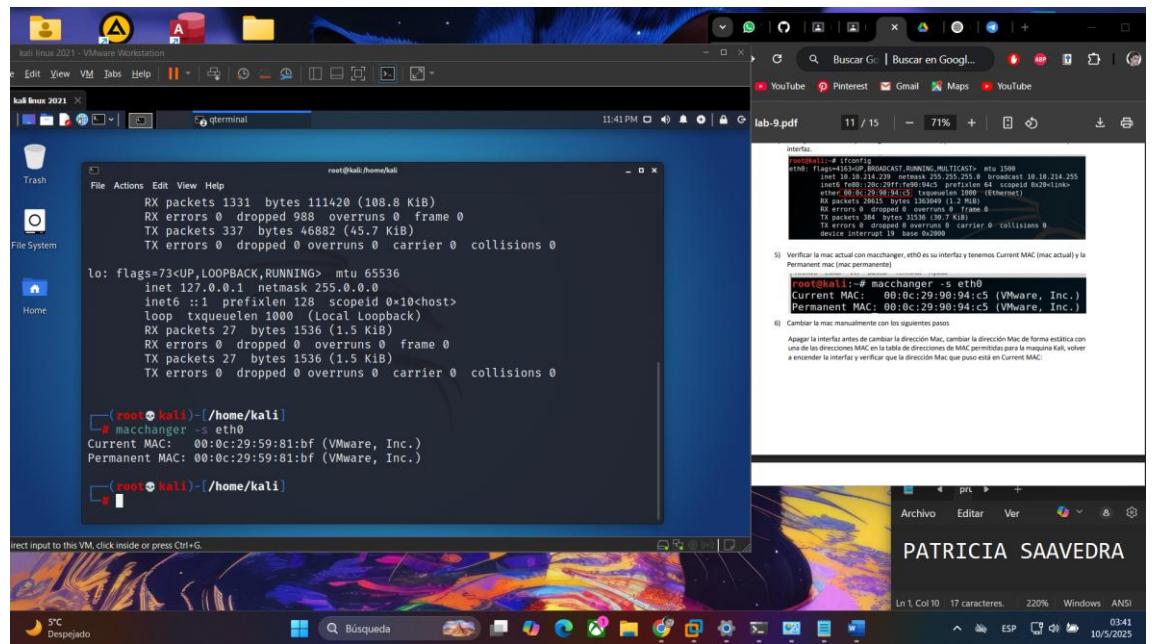
## Kali



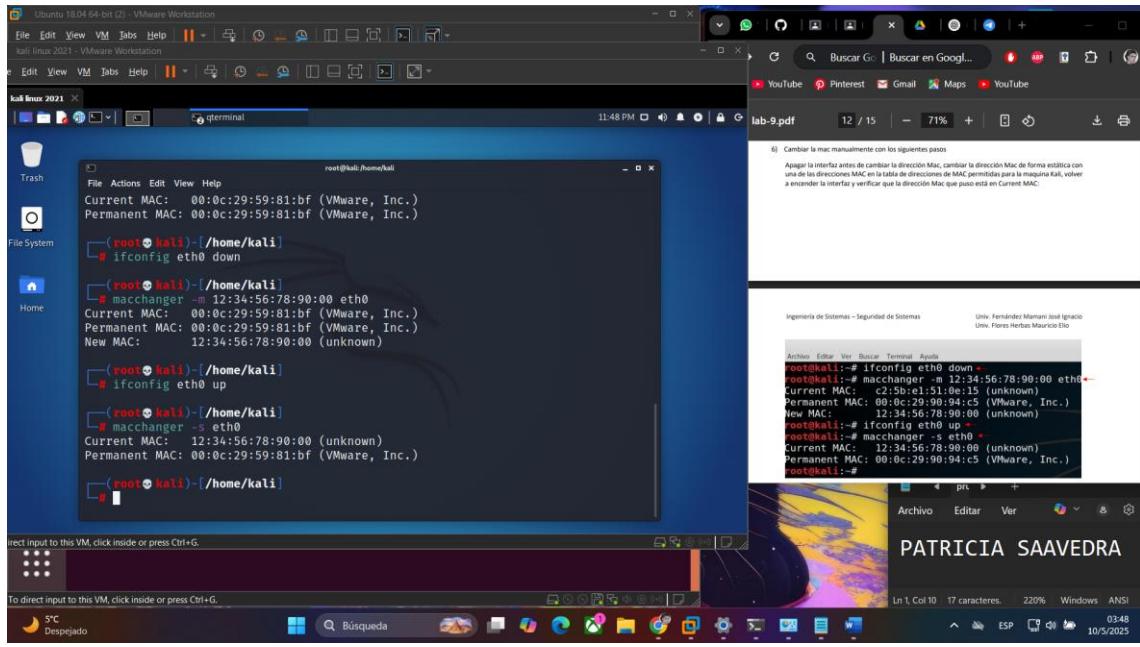
4. Trabajaremos con Kali para asignar direcciones MAC, primero observe su dirección MAC actual y su interfaz.



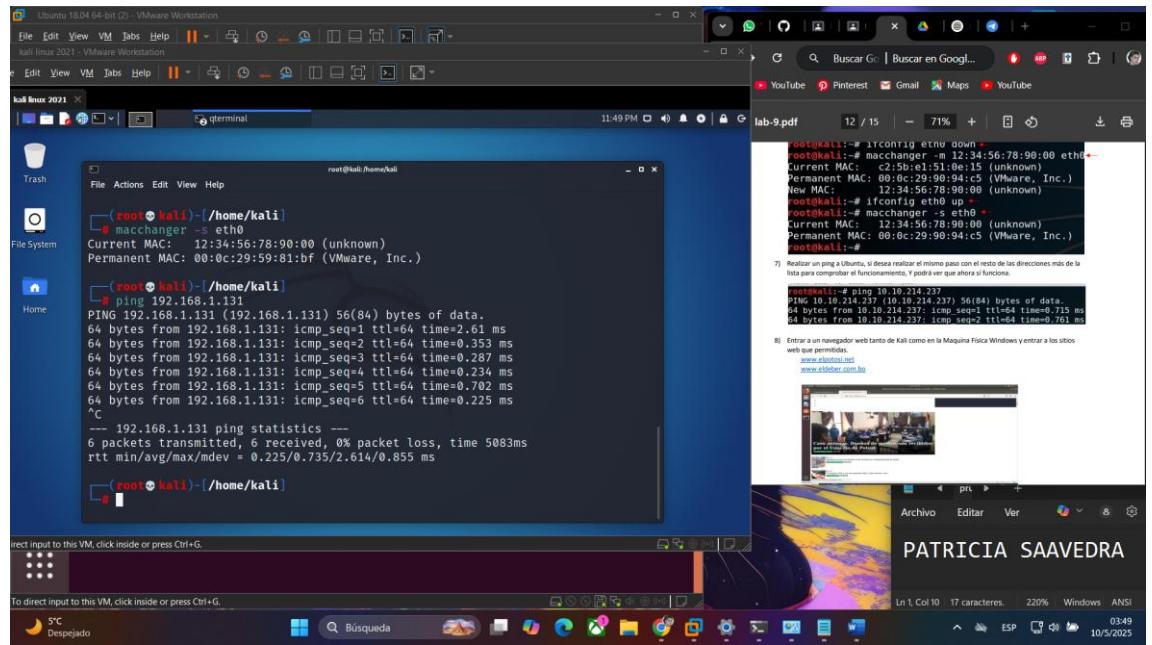
5. Verificar la MAC actual con `macchanger`, `eth0` es su interfaz y tenemos Current MAC (mac actual) y la Permanent MAC (mac permanente).



6. Cambiar la MAC manualmente con los siguientes pasos:  
Apagar la interfaz antes de cambiar la dirección MAC, cambiar la dirección MAC de forma estática con una de las direcciones MAC en la tabla de direcciones de MAC permitidas para la máquina Kali, volver a encender la interfaz y verificar que la dirección MAC que puso está en Current MAC.

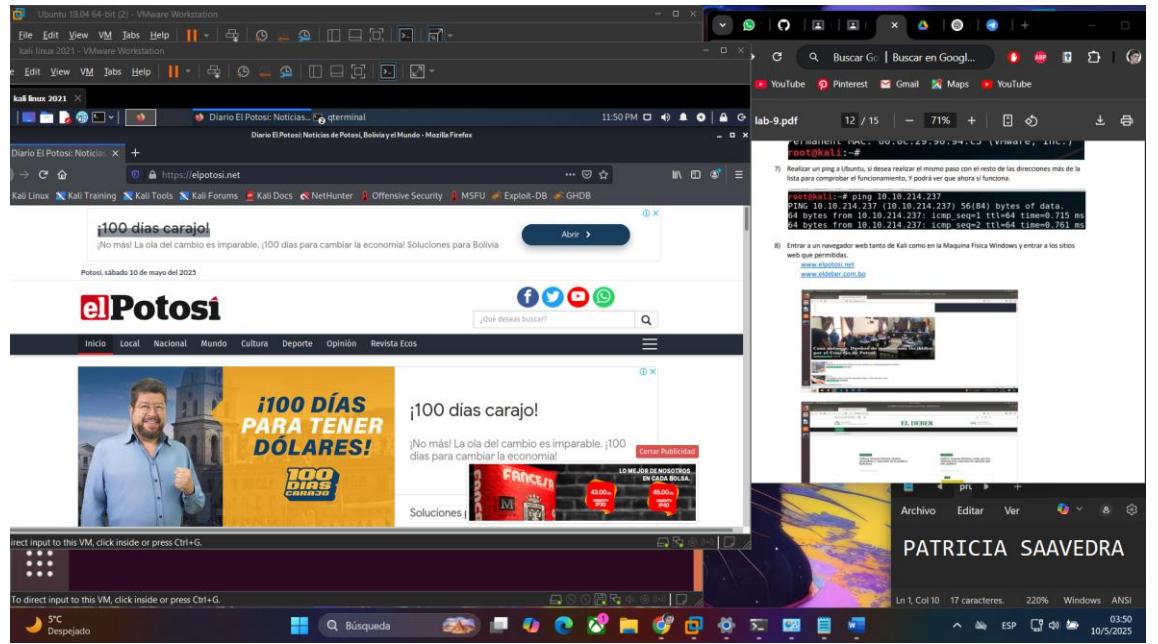


- Realizar un ping a Ubuntu, si desea realizar el mismo paso con el resto de las direcciones MAC de la lista para comprobar el funcionamiento, podrá ver que ahora sí funciona.

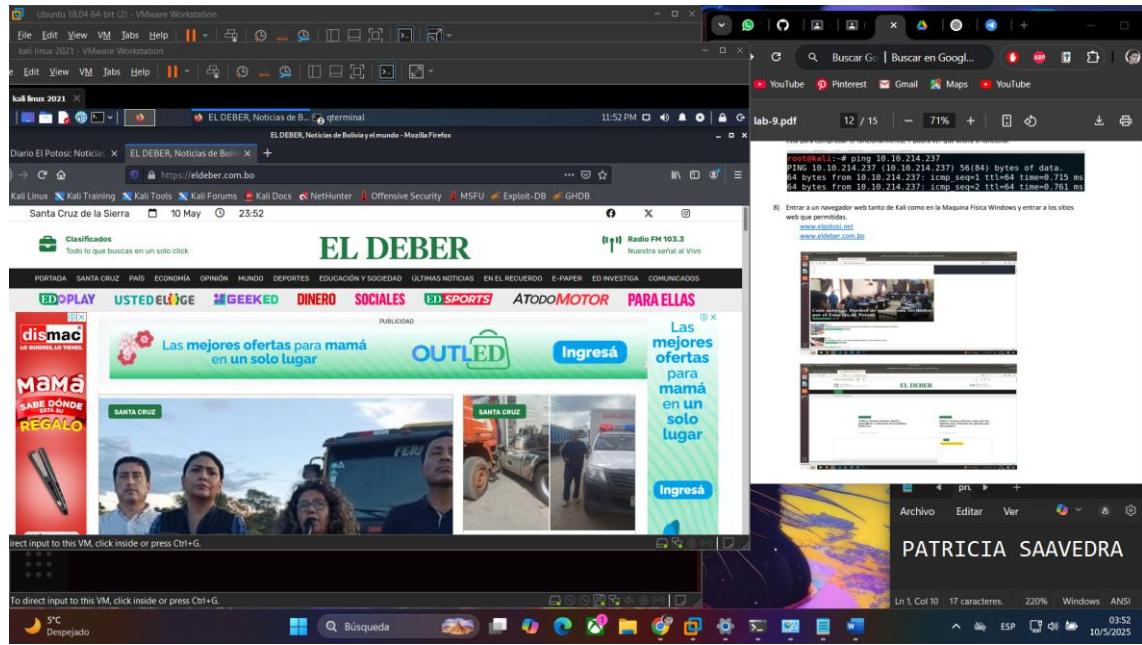


- Entrar a un navegador web tanto de Kali como en la Máquina Física Windows y entrar a los sitios web permitidos:

- [www.elpotosi.net](http://www.elpotosi.net)

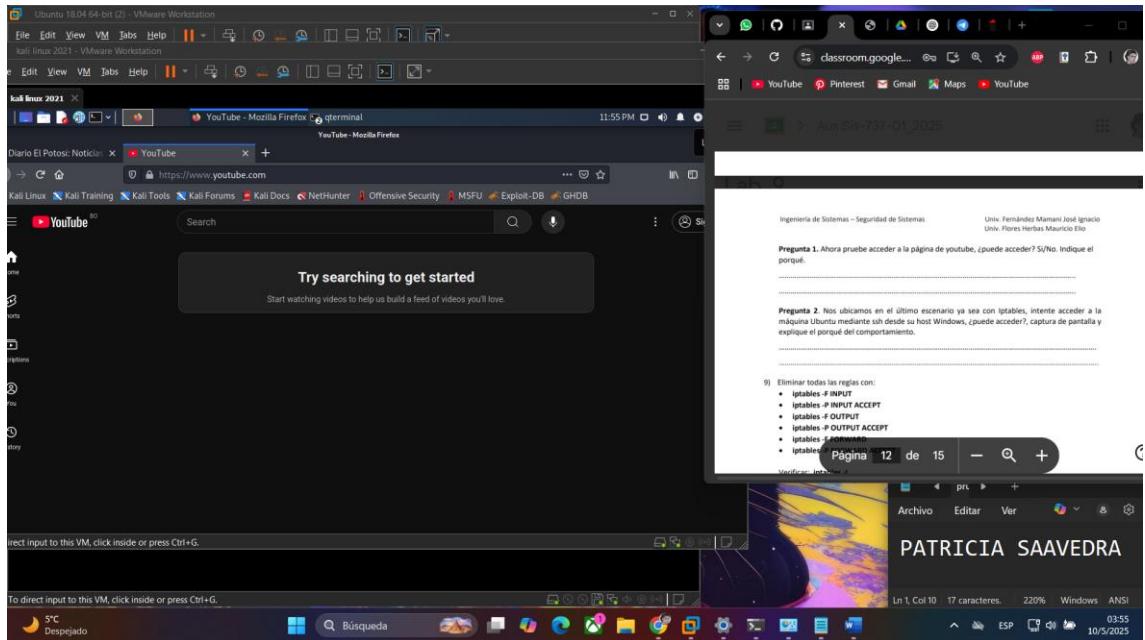


[www.eldeber.com.bo](http://www.eldeber.com.bo)

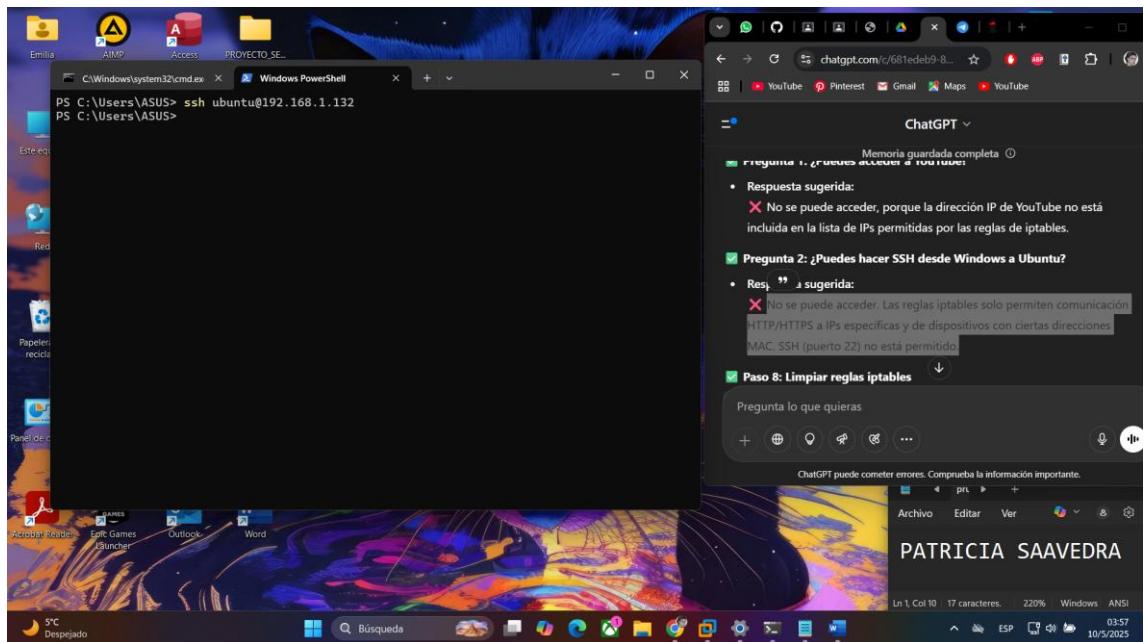


**Pregunta 1.** Ahora pruebe acceder a la página de YouTube, ¿puede acceder? ¿Sí/No?  
Indique el porqué.

No se puede acceder, porque la dirección IP de YouTube no está incluida en la lista de IPs permitidas por las reglas de iptables, pero... qué crees?, no sé algo hice mal acá.



**Pregunta 2.** Nos ubicamos en el último escenario ya sea con Iptables, intente acceder a la máquina Ubuntu mediante SSH desde su host Windows, ¿puede acceder?, captura de pantalla y explique el porqué del comportamiento. No se puede acceder. Las reglas iptables solo permiten comunicación HTTP/HTTPS a IPs específicas y de dispositivos con ciertas direcciones MAC. SSH (puerto 22) no está permitido.

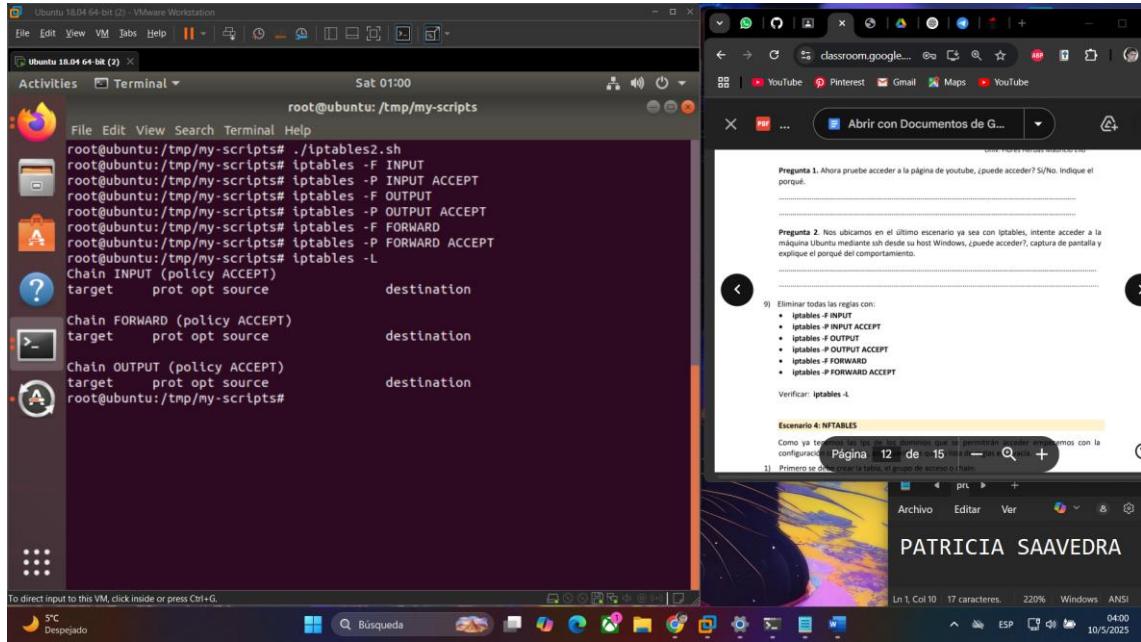


## 9. Eliminar todas las reglas con:

```
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:

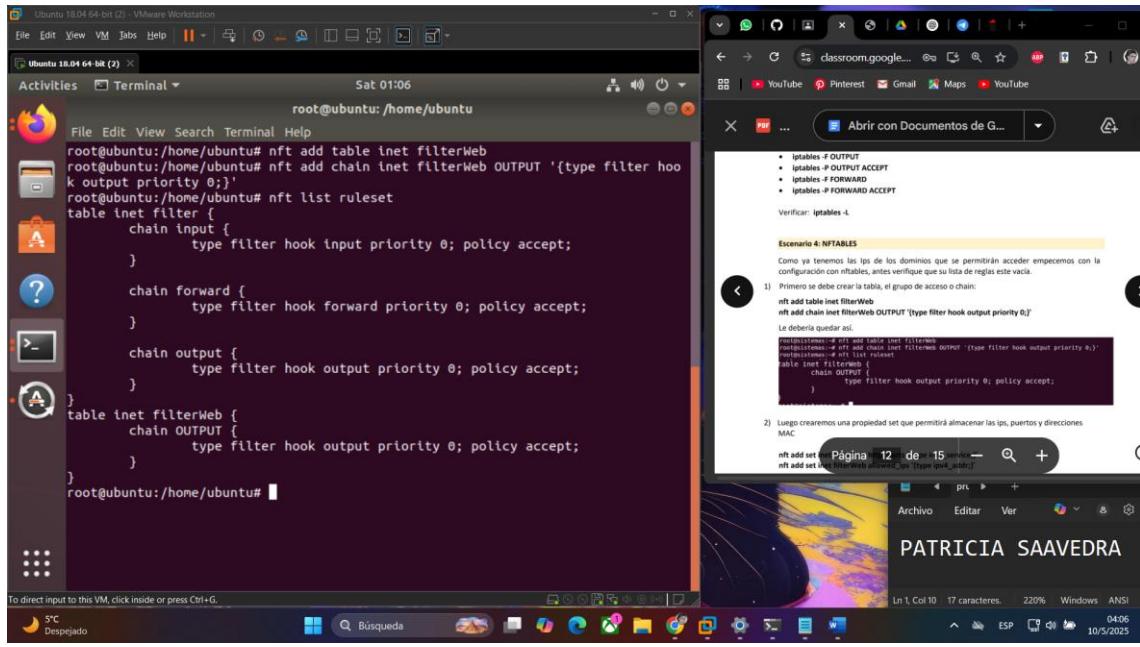
## NFTABLES

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 esté vacía.

Con `nft list ruleset`

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

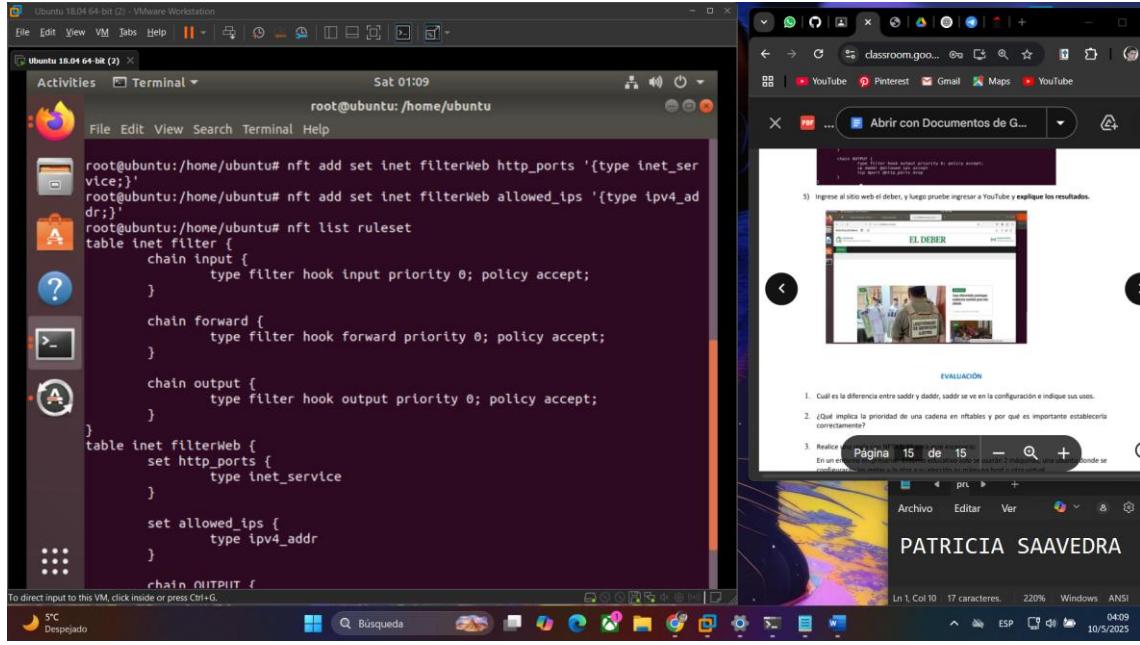
```
nft add table inet filterWeb
nft add chain inet filterWeb OUTPUT '{type filter hook output priority
0;}'
```



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_ips '{type ipv4_addr;}'
```

Le debería quedar de la siguiente forma:



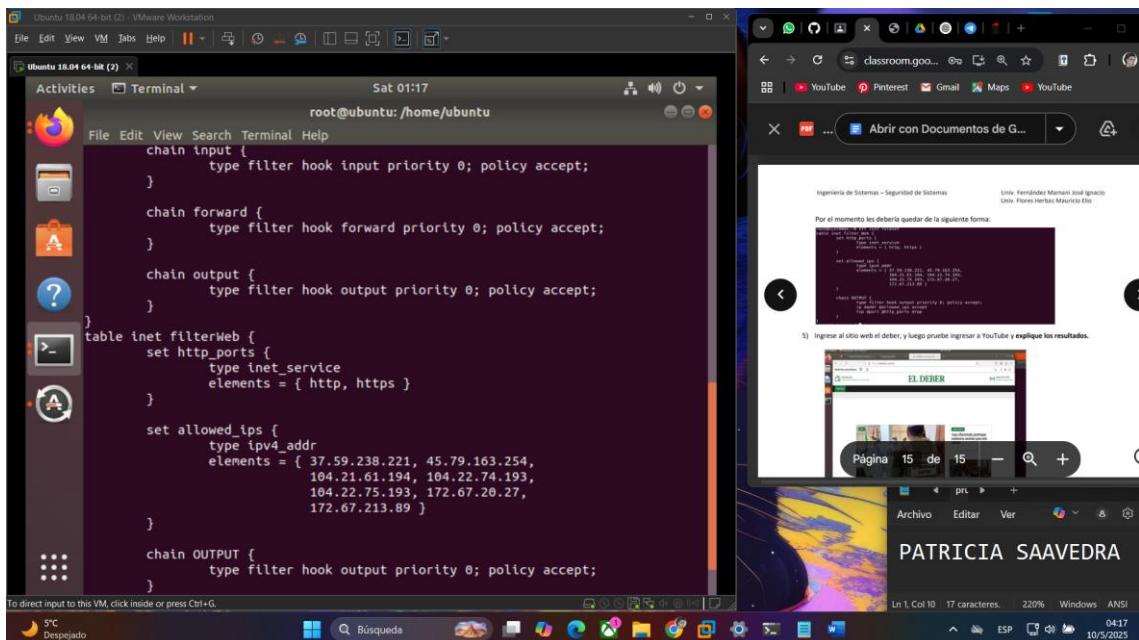
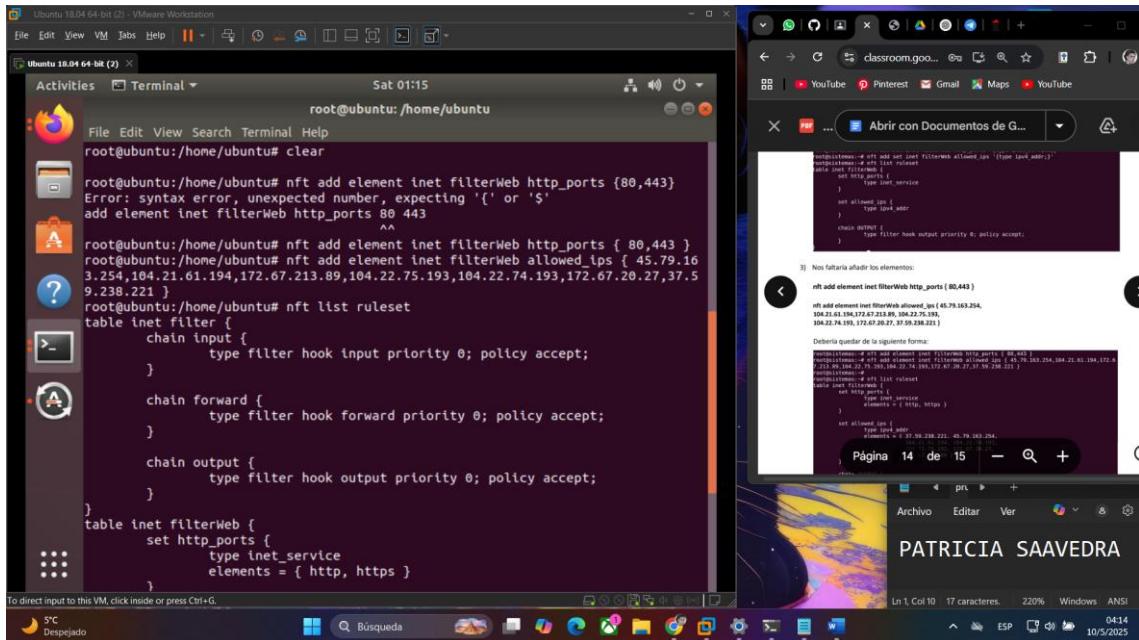
3. Nos faltaría añadir los elementos:

Dominios	Dirección IP
lostiempos.com	45.79.163.254
elpotosi.net	104.21.61.194
	172.67.213.89

eldeber.com.bo	104.22.75.193
	104.22.74.193
	172.67.20.27
freeditorial.com	37.59.238.221

```
nft add element inet filterWeb http_ports { 80,443 }
nft add element inet filterWeb allowed_ips { 45.79.163.254,
104.21.61.194, 172.67.213.89, 104.22.75.193,
172.67.20.27, 37.59.238.221 }
```

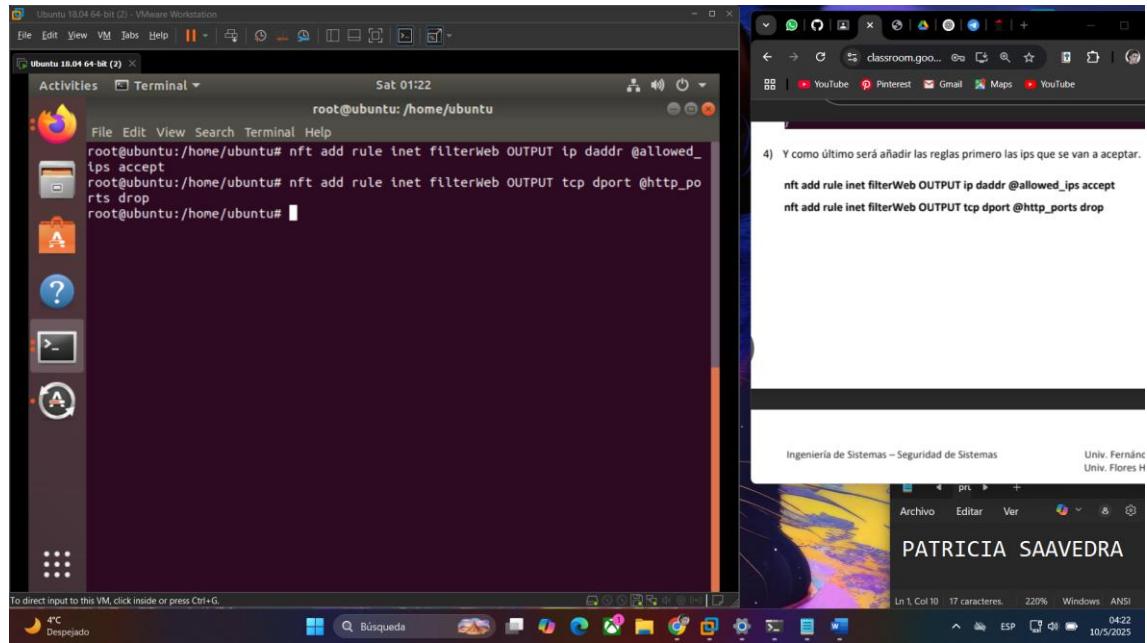
Debería quedar de la siguiente forma:



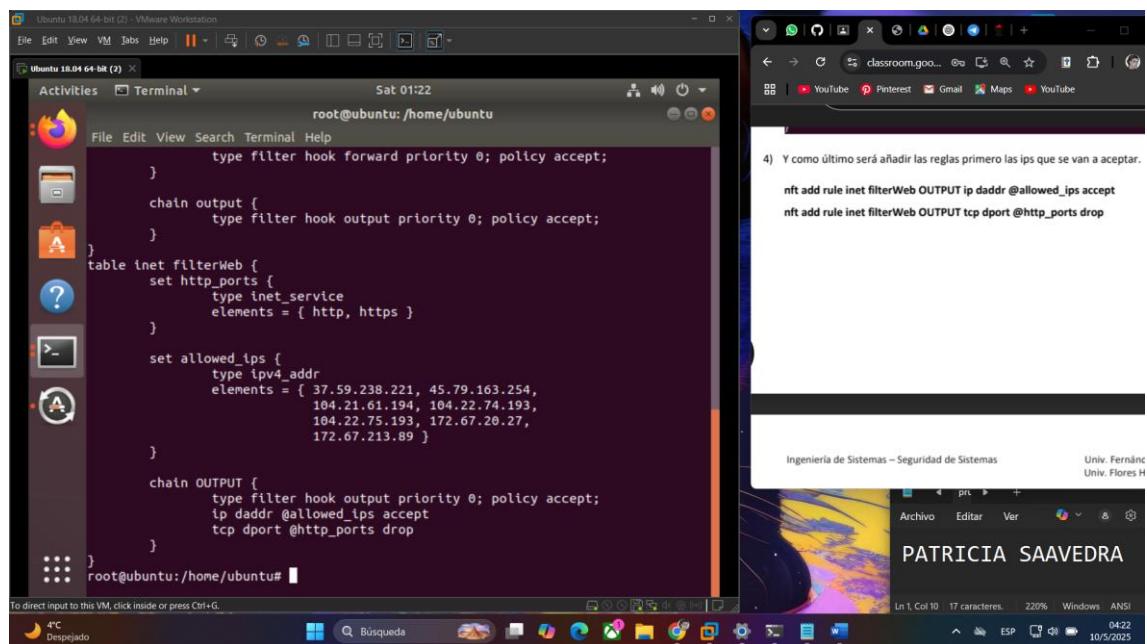
4. Y como último será añadir las reglas, primero las IPs que se van a aceptar:

```
nft add rule inet filterWeb OUTPUT ip daddr @allowed_ips accept
```

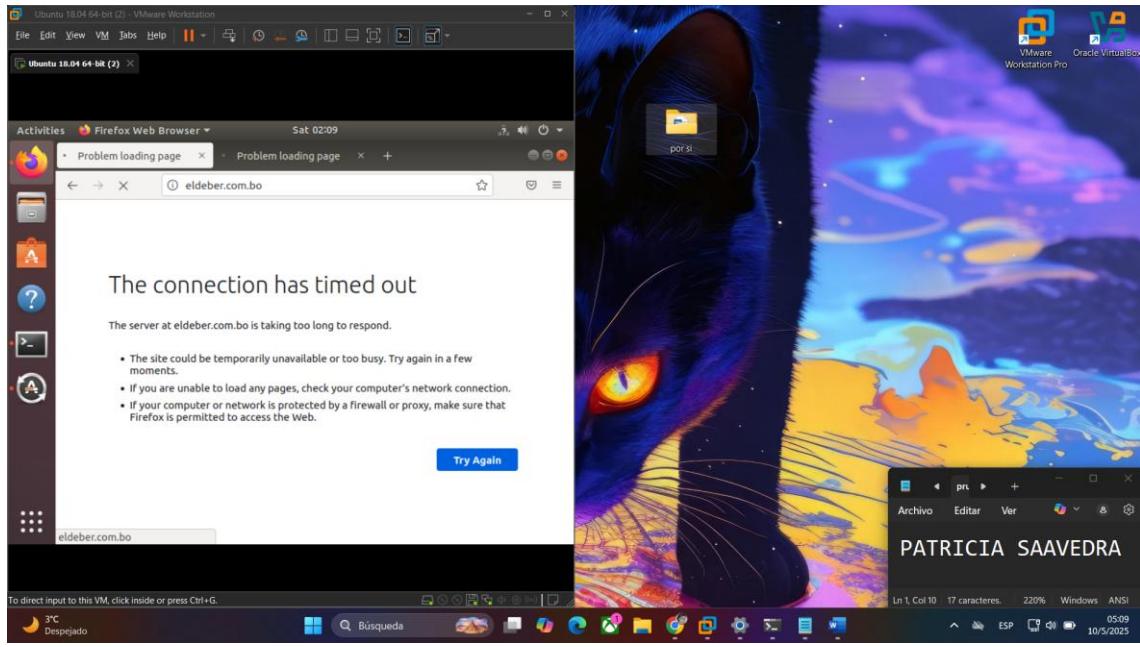
```
nft add rule inet filterWeb OUTPUT tcp dport @http_ports drop
```



Por el momento les debería quedar de la siguiente forma:

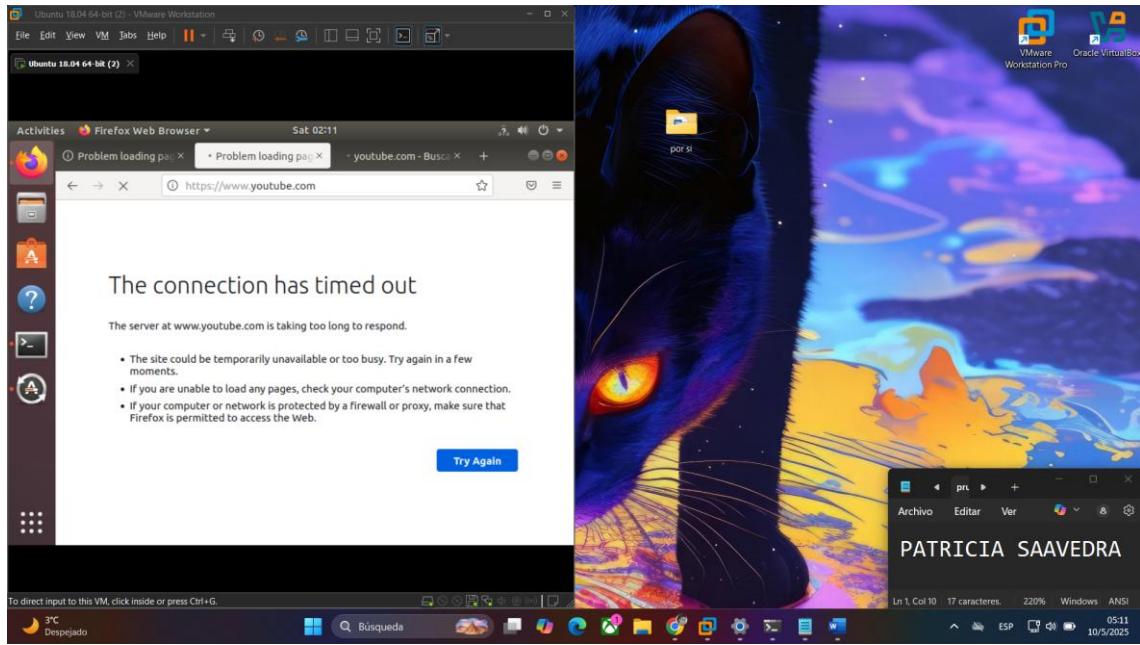


5. Ingrese al sitio web El Deber, y luego pruebe ingresar a YouTube y explique los resultados.



El deber no dio, aunque si debería porque está dentro de las ip permitidas.

Youtube no dio y no debería porque no está dentro de las ips permitidas, todo mal.



## EVALUACIÓN

1. ¿Cuál es la diferencia entre saddr y daddr, saddr se ve en la configuración e indique sus usos?

**saddr:** Dirección IP de origen del paquete.

**daddr:** Dirección IP de destino del paquete.

**Usos:** Se usan para filtrar tráfico basado en la IP de origen (saddr) o destino (daddr)

2. ¿Qué implica la prioridad de una cadena en nftables y por qué es importante establecerla correctamente?

La prioridad determina el orden de evaluación de las reglas en una cadena. Es importante para asegurarse de que las reglas se apliquen en el orden correcto, especialmente cuando hay reglas conflictivas.

3. Realice una regla con NFTABLES para este escenario:  
En un entorno empresarial. Entorno educativo solo se usarán 2 máquinas, una Ubuntu donde se configurarán las reglas y la otra a su elección (su máquina host u otra virtual).  
Estamos en un examen importante, pero por la gran importancia y complejidad se les permite usar computadores, para evitar la búsqueda de soluciones o trampas entre compañeros, solo se permite el acceso a una única página la: [www.mclibre.org](http://www.mclibre.org), que solo contiene fórmulas matemáticas necesarias, y como última condición sólo permitir paquetes de estado desde la máquina externa que esté usando a la máquina virtual Ubuntu, todo lo demás debe ser denegado.

## Paso 1: Eliminar las reglas previas

Primero, si tienes reglas previas en la tabla `inet filter`, puedes eliminarlas para empezar desde cero.

## Resumen dConfiguración correcta de tabla y cadenas con hook (solo una vez por cadena principal)

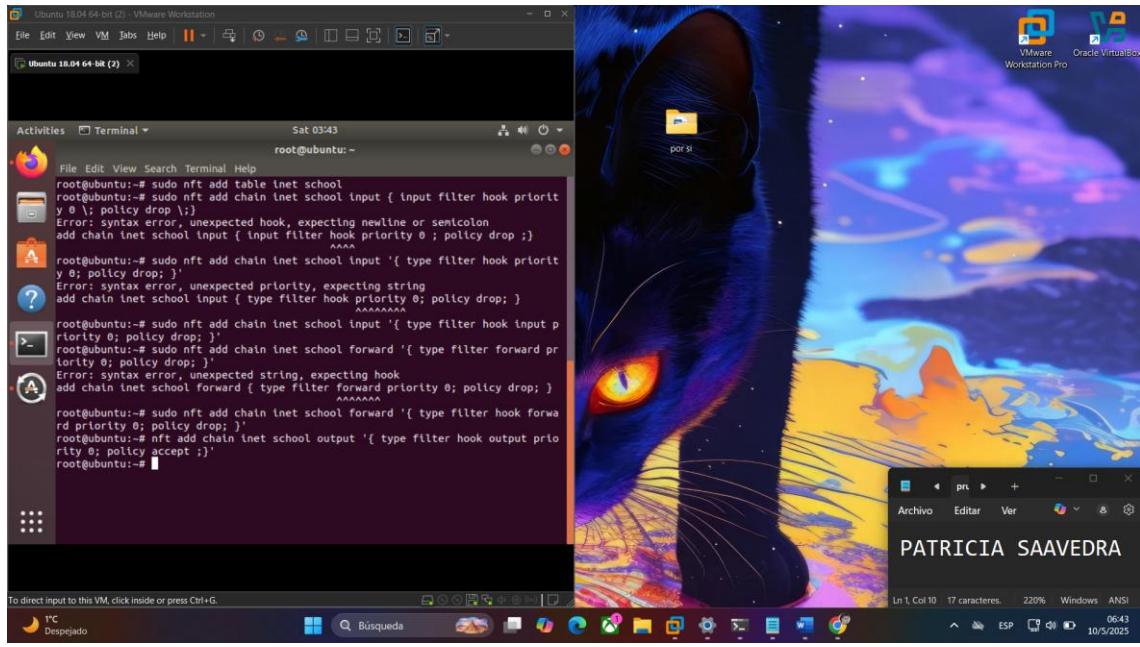
```
# Limpiar reglas anteriores
sudo nft flush ruleset

# Crear tabla llamada school
sudo nft add table inet school

# Crear cadena INPUT con hook y política predeterminada
sudo nft add chain inet school input '{ type filter hook input
priority 0 ; policy drop ; }'

# Crear cadena FORWARD con hook
sudo nft add chain inet school forward '{ type filter hook forward
priority 0 ; policy drop ; }'

# Crear cadena OUTPUT con hook
sudo nft add chain inet school output '{ type filter hook output
priority 0 ; policy accept ; }'
```



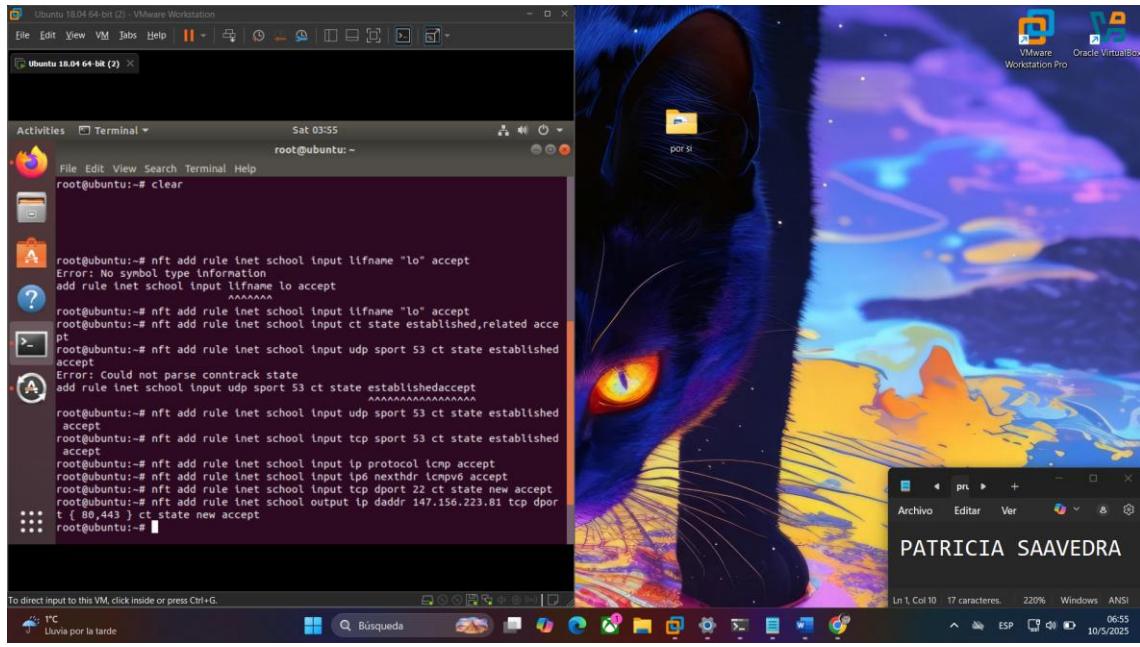
## Reglas a añadir en la tabla school

```
# Permitir conexiones ya establecidas/relacionadas
sudo nft add rule inet school input ct state established,related
accept
sudo nft add rule inet school output ct state established,related
accept

# Permitir PING (ICMP) solo a 192.168.1.133 y a mclibre.org
(147.156.223.81)
sudo nft add rule inet school output ip daddr 192.168.1.133 ip
protocol icmp type echo-request accept
sudo nft add rule inet school input ip saddr 192.168.1.133 ip protocol
icmp type echo-reply accept

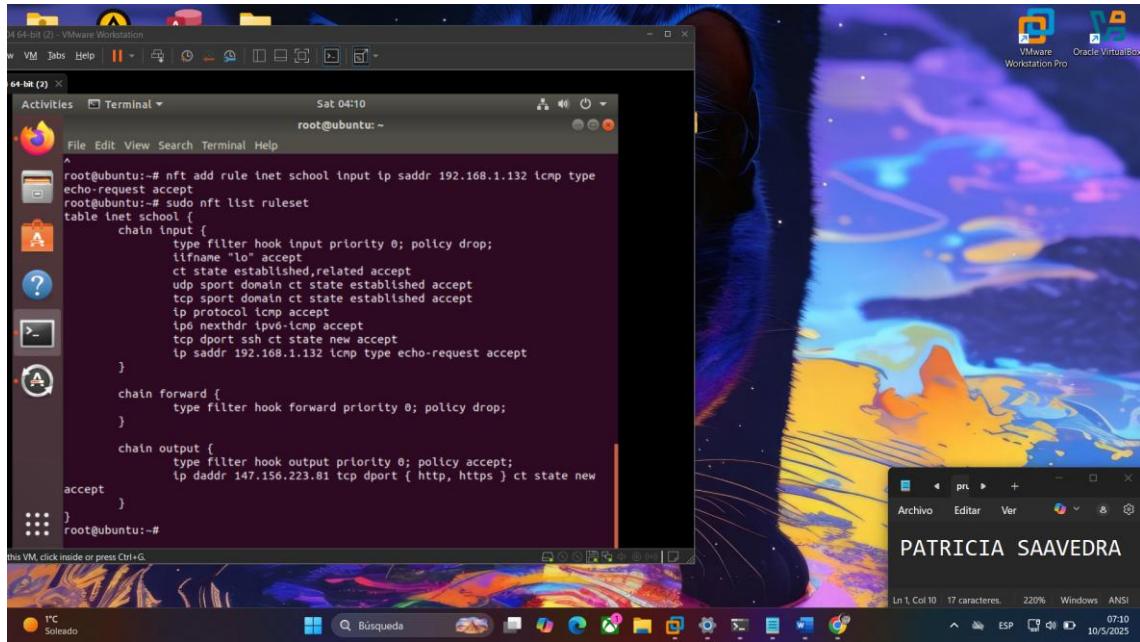
sudo nft add rule inet school output ip daddr 147.156.223.81 ip
protocol icmp type echo-request accept
sudo nft add rule inet school input ip saddr 147.156.223.81 ip
protocol icmp type echo-reply accept

# Permitir solo navegación web a www.mclibre.org (HTTP y HTTPS)
sudo nft add rule inet school output ip daddr 147.156.223.81 tcp dport
{80,443} ct state new accept .
```



## Verifica las reglas

sudo nft list ruleset



## Resumen de las reglas:

1. **Eliminar reglas anteriores** (si es necesario).
2. **Crear la tabla `inet filter`** y la cadena de entrada.
3. **Permitir tráfico relacionado y establecido.**
4. **Permitir acceso solo a [www.mclibre.org](http://www.mclibre.org).**
5. **Permitir tráfico solo desde la máquina externa 192.168.1.133.**

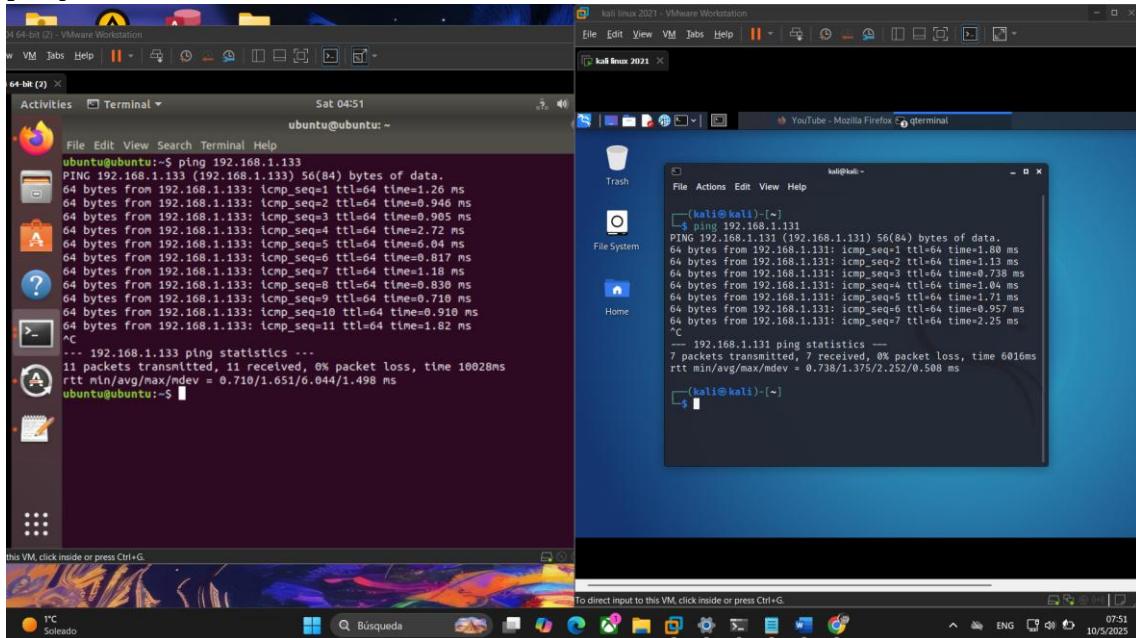
## 6. Denegar todo el tráfico restante.

### 1. Permitir solo paquetes establecidos y relacionados

Prueba:

Desde la **máquina externa**, inicia un **ping** o una conexión **después** de haber sido iniciada desde Ubuntu.

```
# En Ubuntu  
ping 192.168.1.133  
# En máquina kali  
ping 192.168.1.131
```



Resultado esperado:

- Si el tráfico ya fue iniciado desde Ubuntu, la respuesta del **ping** será exitosa en la máquina externa.
- Si el tráfico se inicia desde la máquina externa y no está permitido aún, se bloquea (salvo que lo permita otra regla).

Con Windows y Ubuntu no debería dar como acá.

---

### 2. Permitir solo acceso a [www.mclibre.org](http://www.mclibre.org) (IP 147.156.223.81)

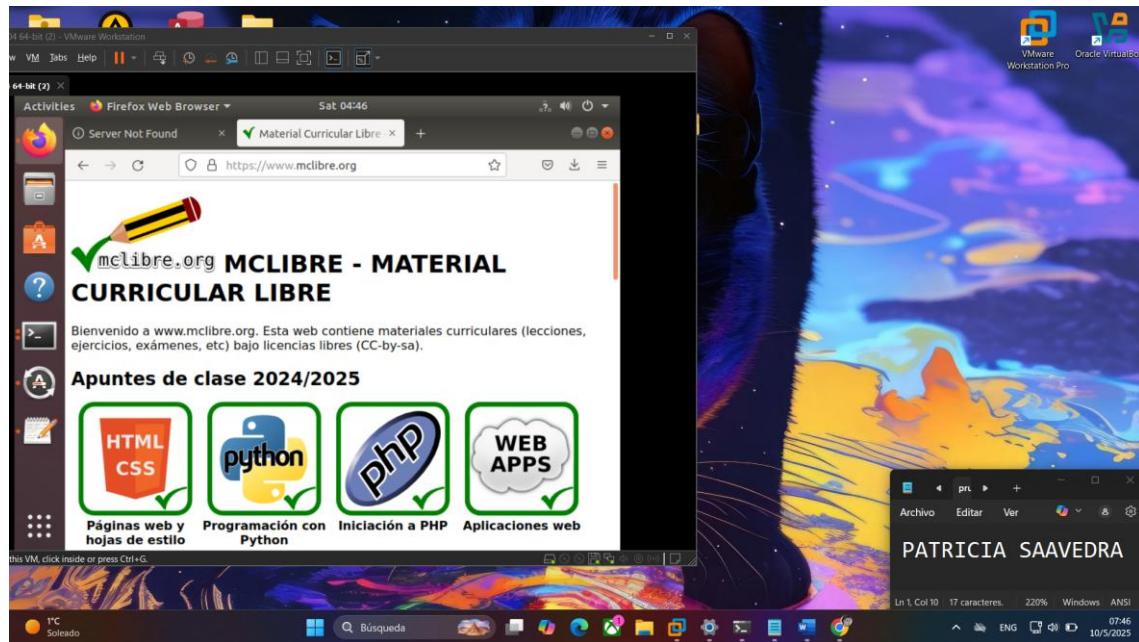
### Prueba:

Desde Ubuntu, intenta acceder a [www.mclibre.org](http://www.mclibre.org) usando ping.

```
ping http://147.156.223.81
```

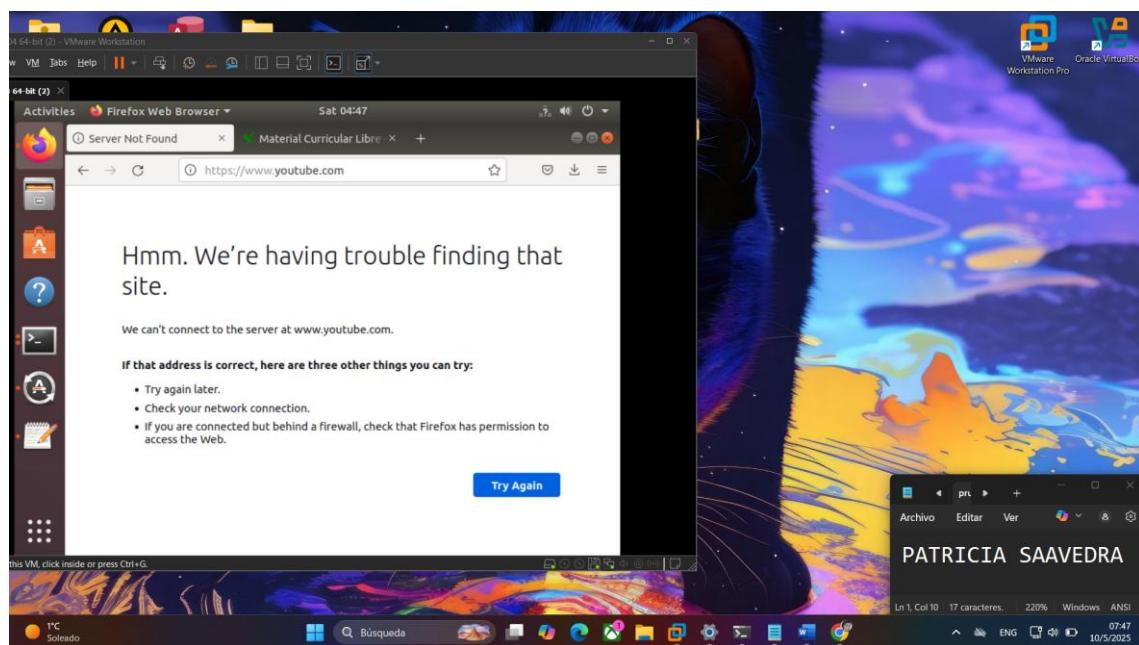
O directamente:

Ir al navegador <http://www.mclibre.org>



### Prueba negativa:

Prueba acceder a otro sitio web, por ejemplo youtube:



Resultado esperado:

- Acceso a [www.mclibre.org](http://www.mclibre.org) debe funcionar.
  - Acceso a otros sitios web **debe fallar** (bloqueado por firewall).
- 

3. Permitir solo acceso desde la máquina externa (192.168.1.133)

Prueba:

Desde otra máquina externa (Windows), intenta hacer ping a Ubuntu:

```
ping 192.168.1.127
```

Prueba negativa:

