

## Laboratorio 9

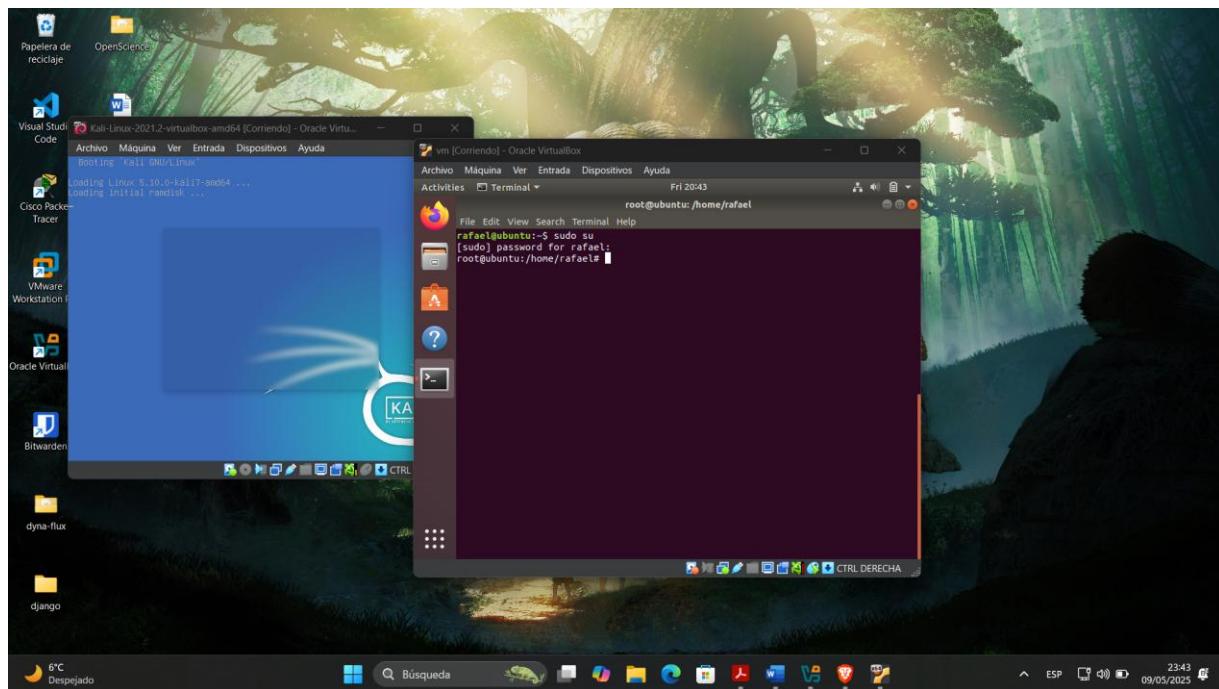
**Nombre:** Rafael Antonio Patricio Ayllón

**CI:** 10473854

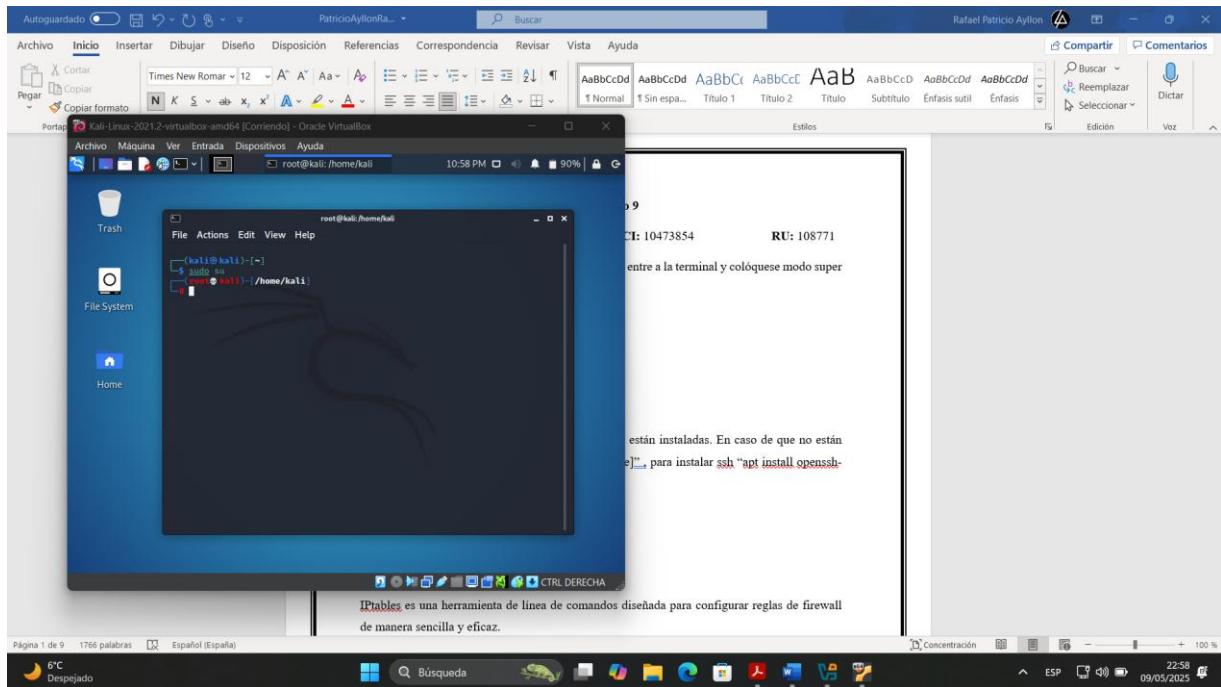
**RU:** 108771

**PASO 1:** Acceda a la máquina virtual Ubuntu y Kali entre a la terminal y colóquese modo super usuario.

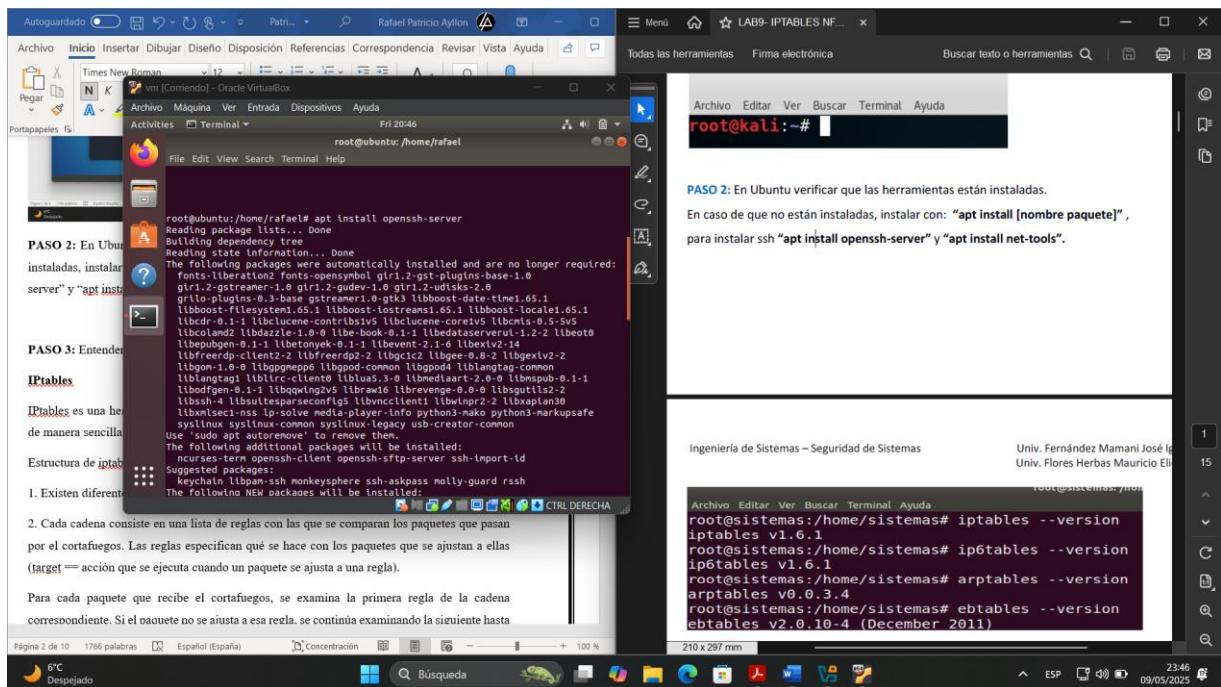
### Ubuntu

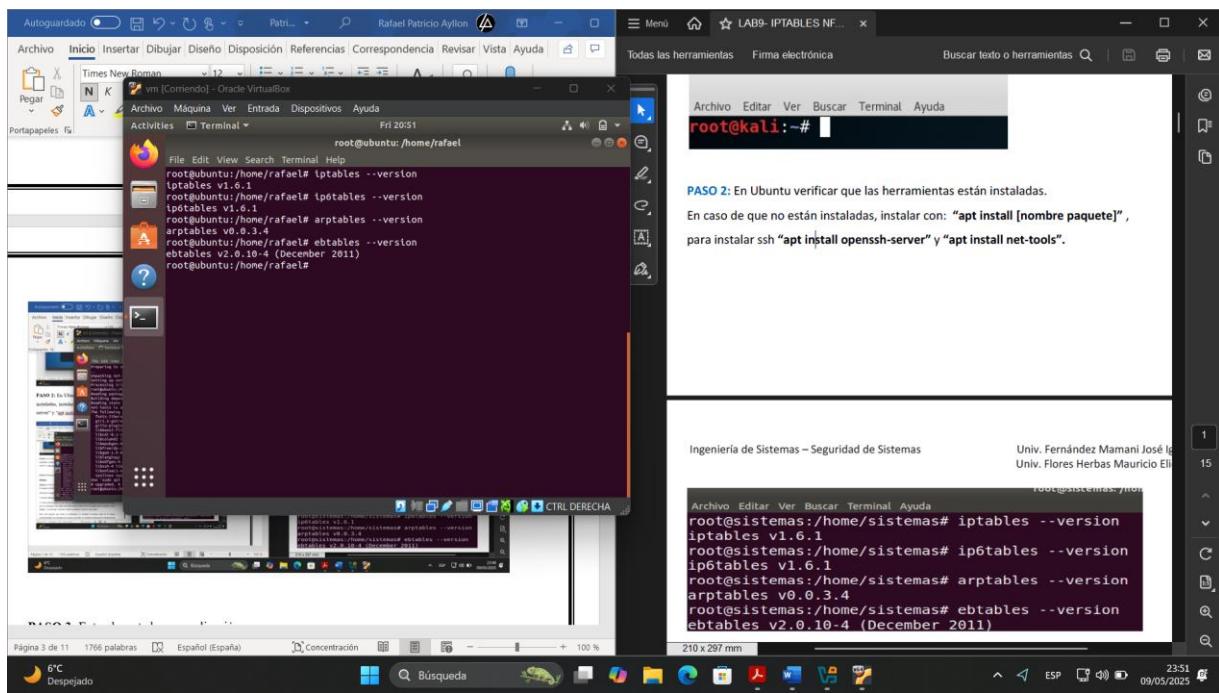
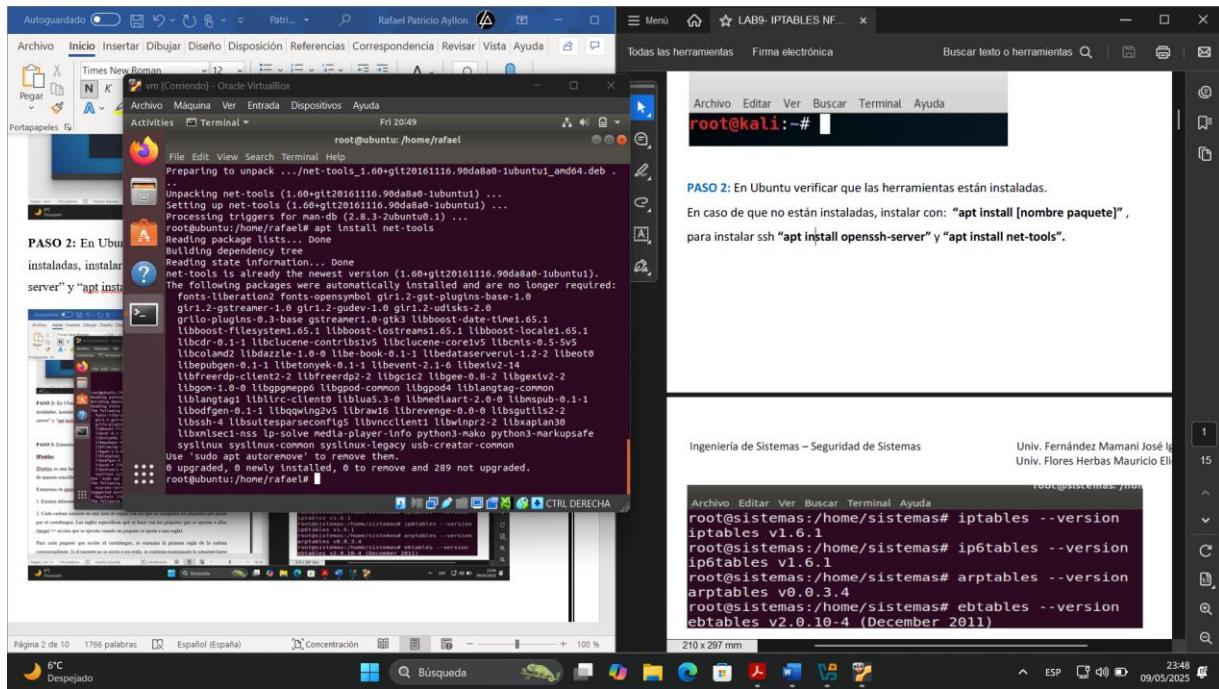


### Kali



**PASO 2:** En Ubuntu verificar que las herramientas están instaladas. En caso de que no están instaladas, instalar con: “apt install [nombre paquete]” , para instalar ssh “apt install openssh-server” y “apt install net-tools”.





**PASO 3:** Entender esta breve explicación:

## IPtables

IPtables es una herramienta de línea de comandos diseñada para configurar reglas de firewall de manera sencilla y eficaz.

Estructura de iptables:

1. Existen diferentes tablas (tables) dentro de las cuales puede haber varias cadenas (chains).
2. Cada cadena consiste en una lista de reglas con las que se comparan los paquetes que pasan por el cortafuegos. Las reglas especifican qué se hace con los paquetes que se ajustan a ellas (target == acción que se ejecuta cuando un paquete se ajusta a una regla).

Para cada paquete que recibe el cortafuegos, se examina la primera regla de la cadena correspondiente. Si el paquete no se ajusta a esa regla, se continúa examinando la siguiente hasta que se ajusta con alguna. En ese momento se ejecuta el target, los targets o acciones pueden ser 2:

1. DROP: descartar paquete.
2. ACCEPT: paquete continúe su camino.

## tablas

En iptables existen tablas preinstaladas que son: filter, nat y mangle. Por cuestiones de tiempo solo usaremos la tabla filter en este laboratorio.

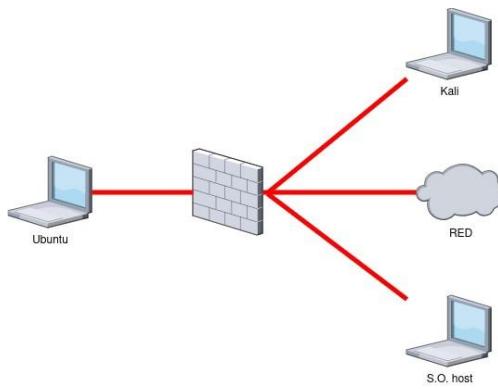
La tabla filter contiene las siguientes cadenas predefinidas que son:

- INPUT: para los paquetes que van dirigidos al cortafuegos.
- FORWARD: paquetes enrutados que vienen de un destino remoto a nuestro equipo.
- OUTPUT: paquetes generados localmente y que deben salir.
- PREROUTING: Modifica paquetes antes de ser enrutados. Se utiliza para tareas como el enmascaramiento de IP y la configuración de NAT.
- POSTROUTING: Modifica los paquetes justo antes de abandonar el sistema. Permite realizar tareas como el marcado de paquetes y la configuración de QoS.

Estructura básica de una maquina regla :

iptables [-t tabla] -[opciones] [chain/regla]

Crearemos diferentes escenarios para aprender con la práctica y que este paso sea sencillo y todo se ejecutara en un entorno que respete la siguiente topología de red:



**PASO 4:** Con el comando ifconfig o ip addr (linux) y ipconfig (windows) obtenga las Ips de los dispositivos que participan en la topología.

## Ubuntu

```

PASO 4: Con el comando ifconfig o ip addr (linux) y ipconfig (windows) obtenga las ips de dispositivos que participan en la topología.

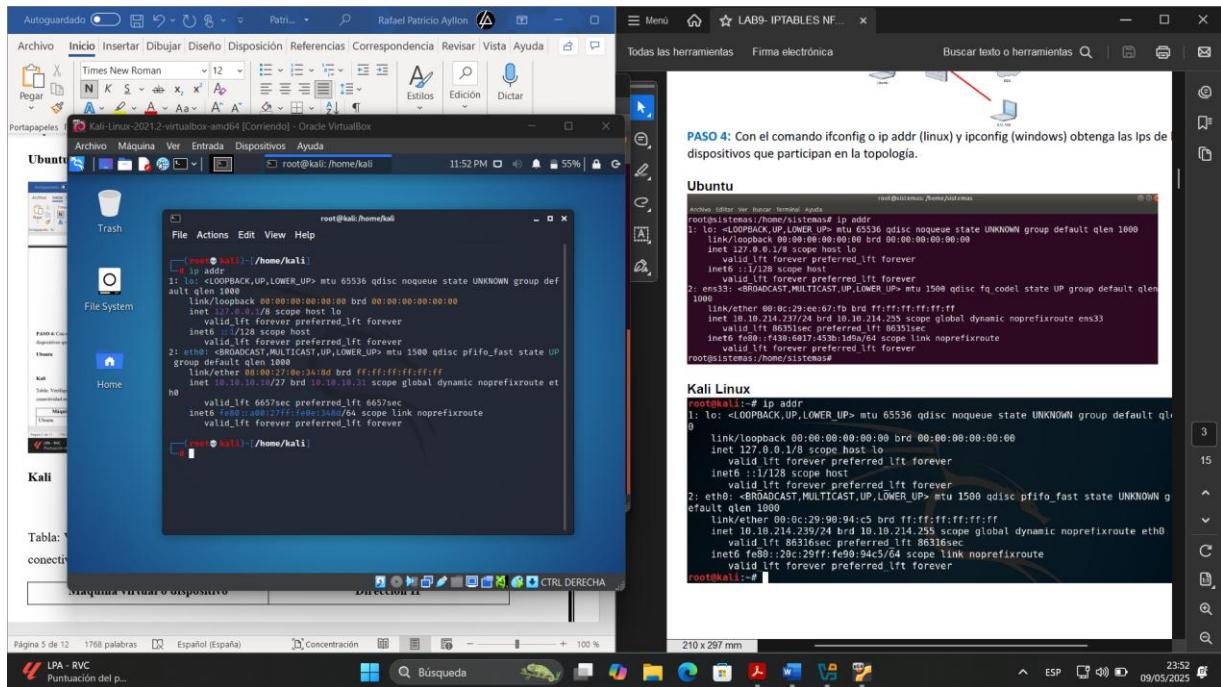
Ubuntu
root@ubuntu:/home/rafael# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3e:c5:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.12/27 brd 10.10.10.31 scope global dynamic noprefixroute eth0
        valid_lft 65525s preferred_lft 65525s
    inet6 fe80::1f2f:30e2:4318/64 brd ff:ff:ff:ff:ff:ff scope link noprefixroute
        valid_lft forever preferred_lft forever
root@ubuntu:/home/rafael# 

PASO 4: Con el comando ifconfig o ip addr (linux) y ipconfig (windows) obtenga las ips de dispositivos que participan en la topología.

Kali
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:ee:67:f0 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.12/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0
        valid_lft 65525s preferred_lft 65525s
    inet6 fe80::f43b:6917:459b:1d9a/64 brd ff:ff:ff:ff:ff:ff scope link noprefixroute
        valid_lft forever preferred_lft forever
root@kali:~#

```

## Kali



## Windows

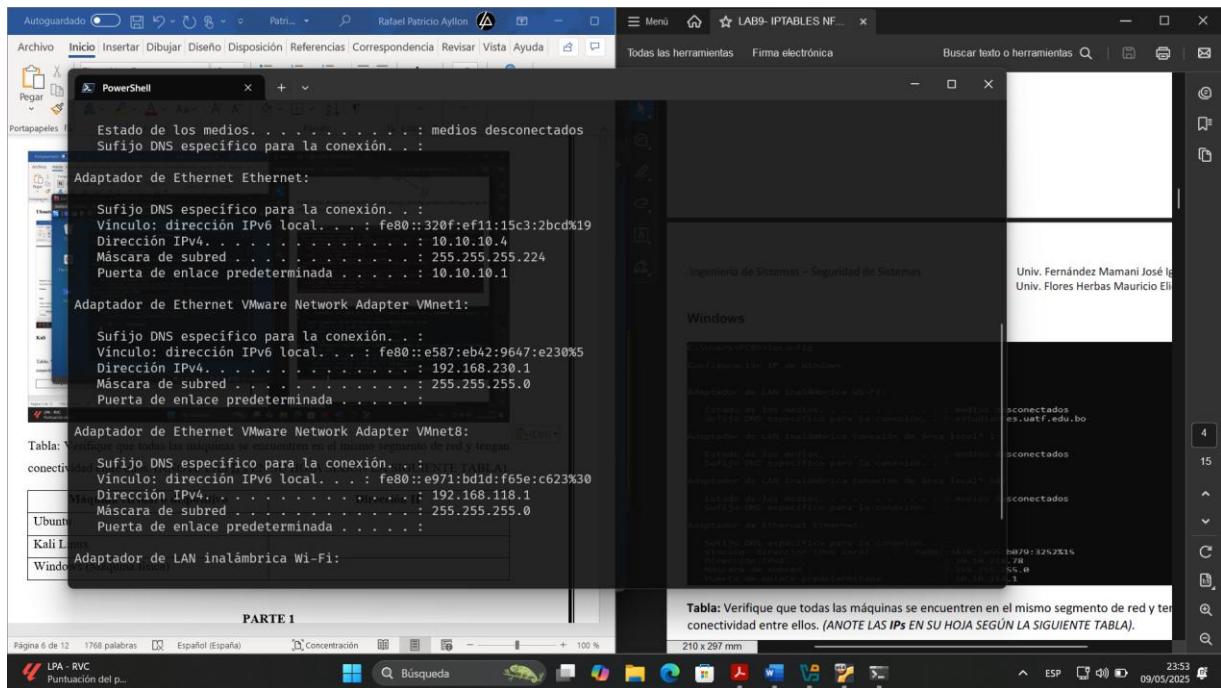


Tabla: Verifique que todas las máquinas se encuentren en el mismo segmento de red y tengan conectividad entre ellos. (ANOTE LAS IPs EN SU HOJA SEGÚN LA SIGUIENTE TABLA).

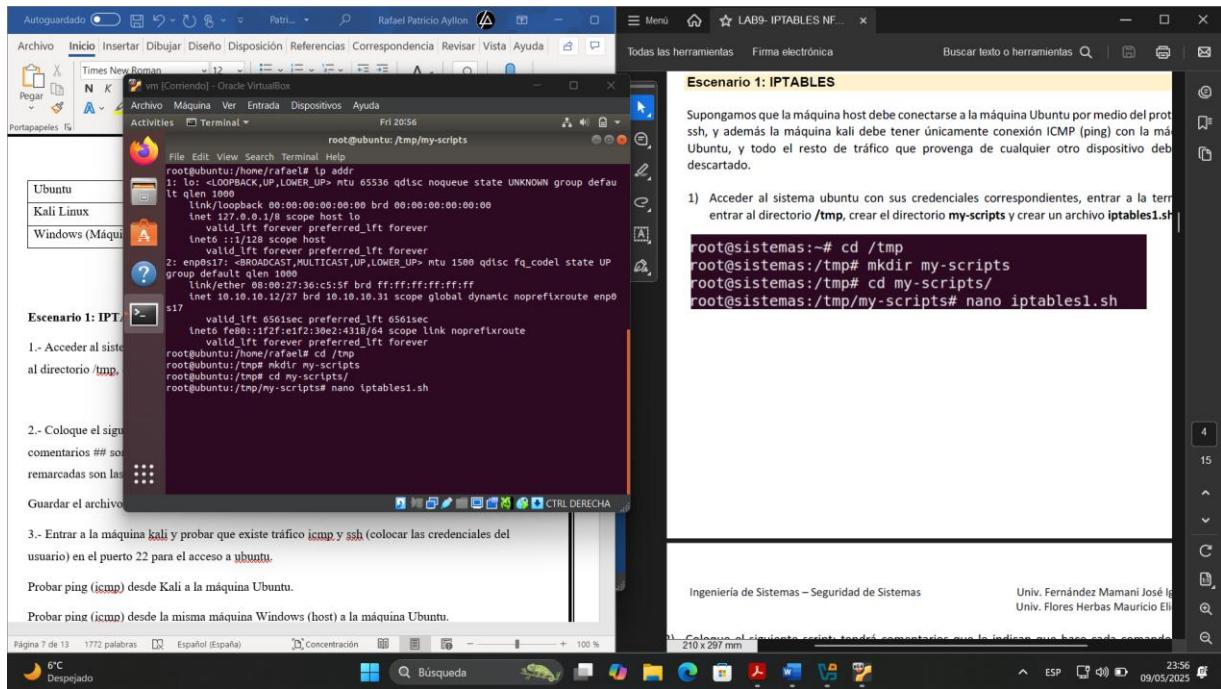
Máquina virtual o dispositivo	Dirección IP
-------------------------------	--------------

Ubuntu	10.10.10.12/27
Kali Linux	10.10.10.10/27
Windows (Máquina física)	10.10.10.4/27

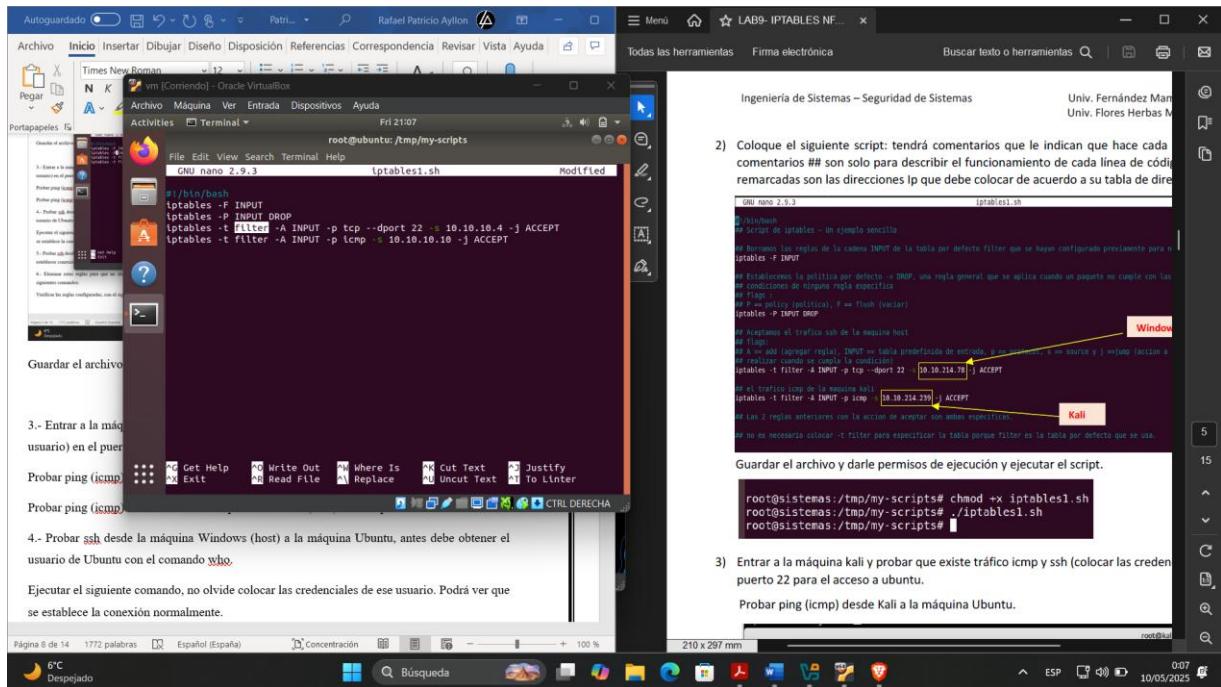
## PARTE 1

### Escenario 1: IPTABLES

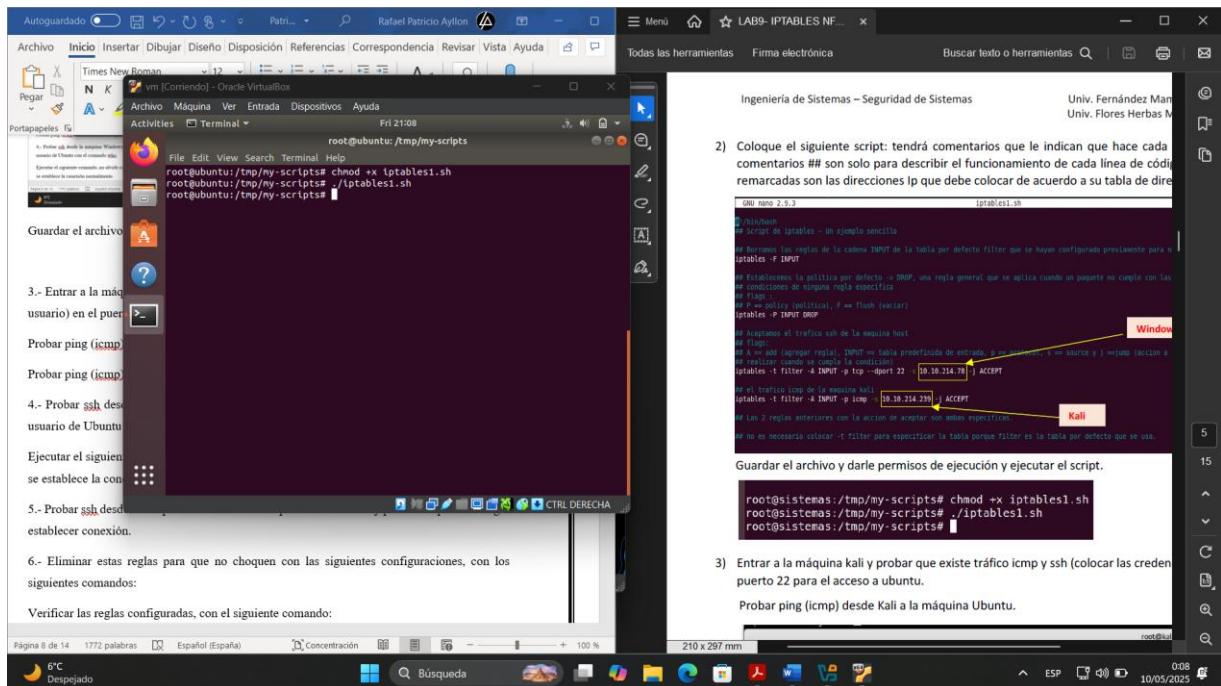
- 1.- Acceder al sistema ubuntu con sus credenciales correspondientes, entrar a la terminal, entrar al directorio /tmp, crear el directorio my-scripts y crear un archivo iptables1.sh



- 2.- Coloque el siguiente script: tendrá comentarios que le indican que hace cada comando. (Los comentarios ## son solo para describir el funcionamiento de cada línea de código). Las partes remarcadas son las direcciones Ip que debe colocar de acuerdo a su tabla de direcciones IP.

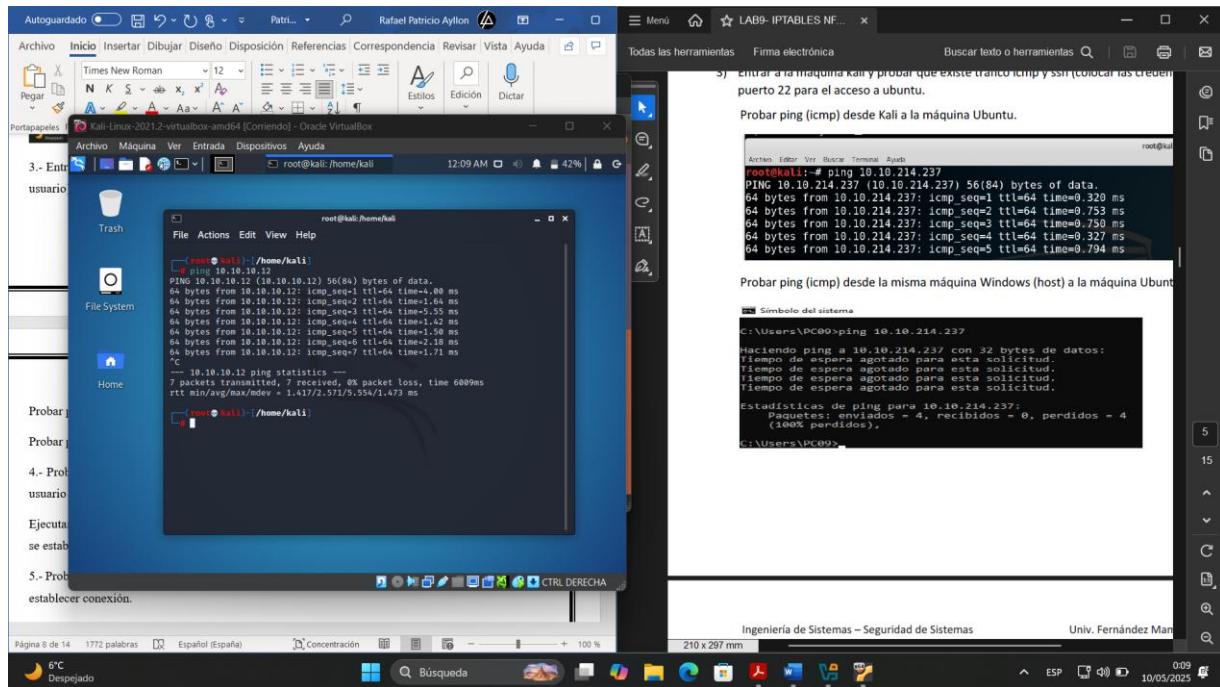


Guardar el archivo y darle permisos de ejecución y ejecutar el script.

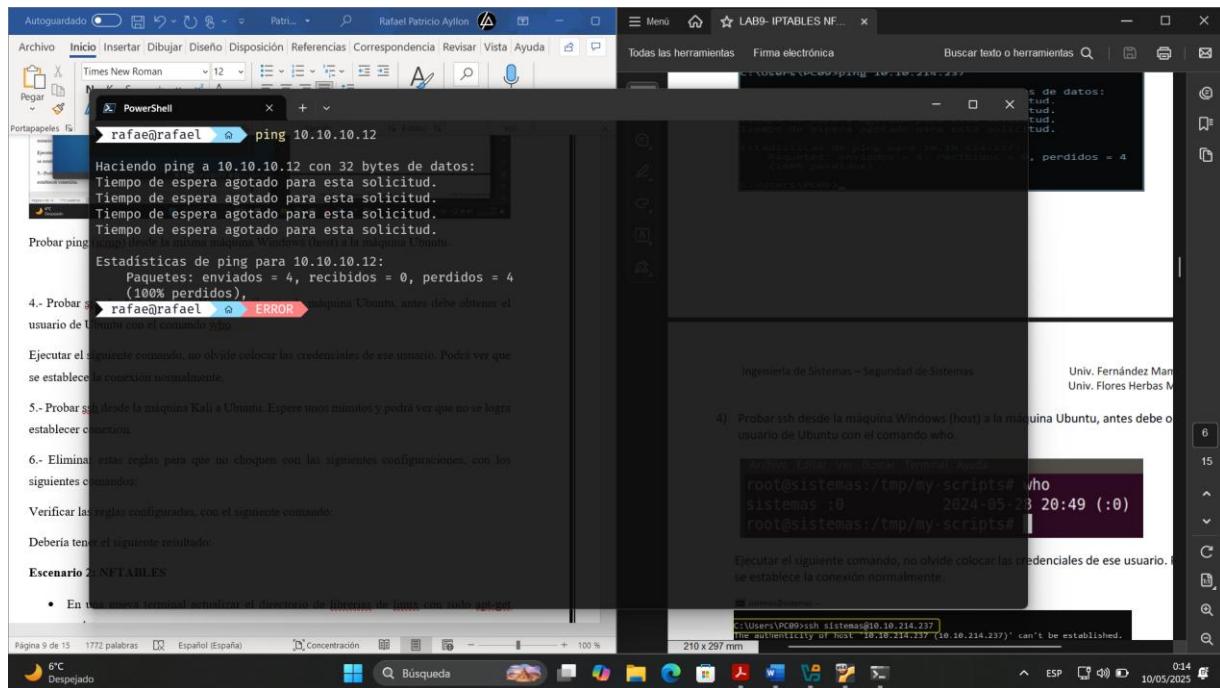


3.- Entrar a la máquina kali y probar que existe tráfico icmp y ssh (colocar las credenciales del usuario) en el puerto 22 para el acceso a ubuntu.

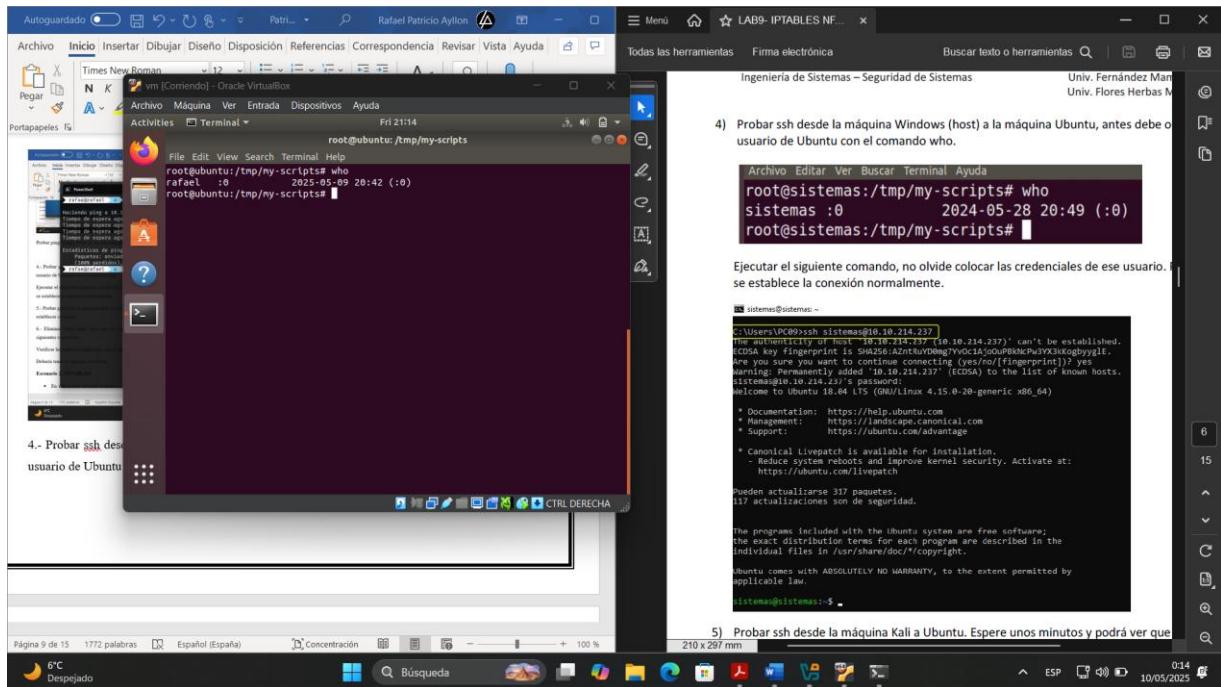
Probar ping (icmp) desde Kali a la máquina Ubuntu.



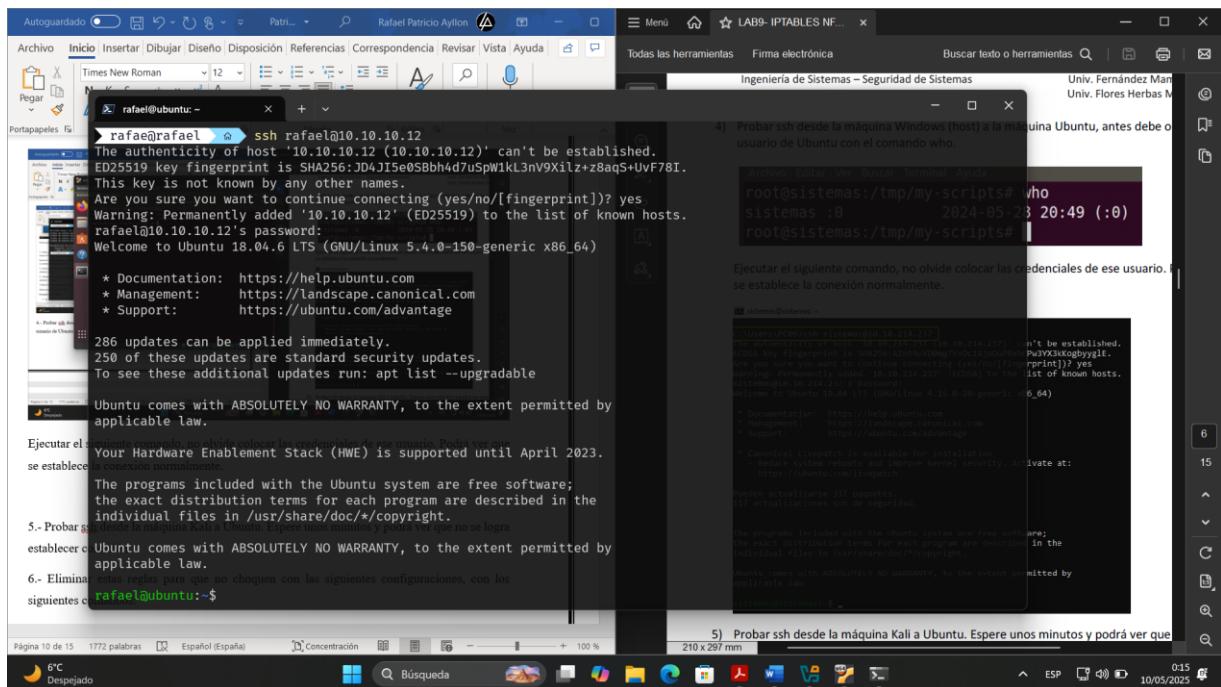
Probar ping (icmp) desde la misma máquina Windows (host) a la máquina Ubuntu.



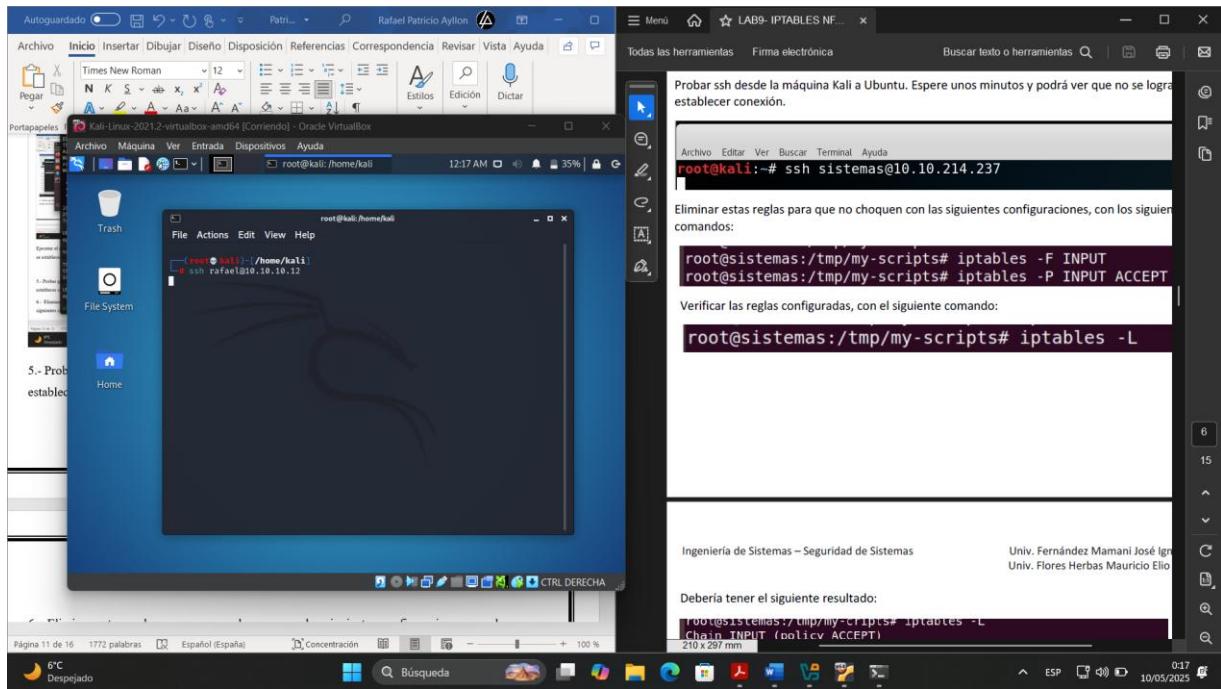
4.- Probar ssh desde la máquina Windows (host) a la máquina Ubuntu, antes debe obtener el usuario de Ubuntu con el comando who.



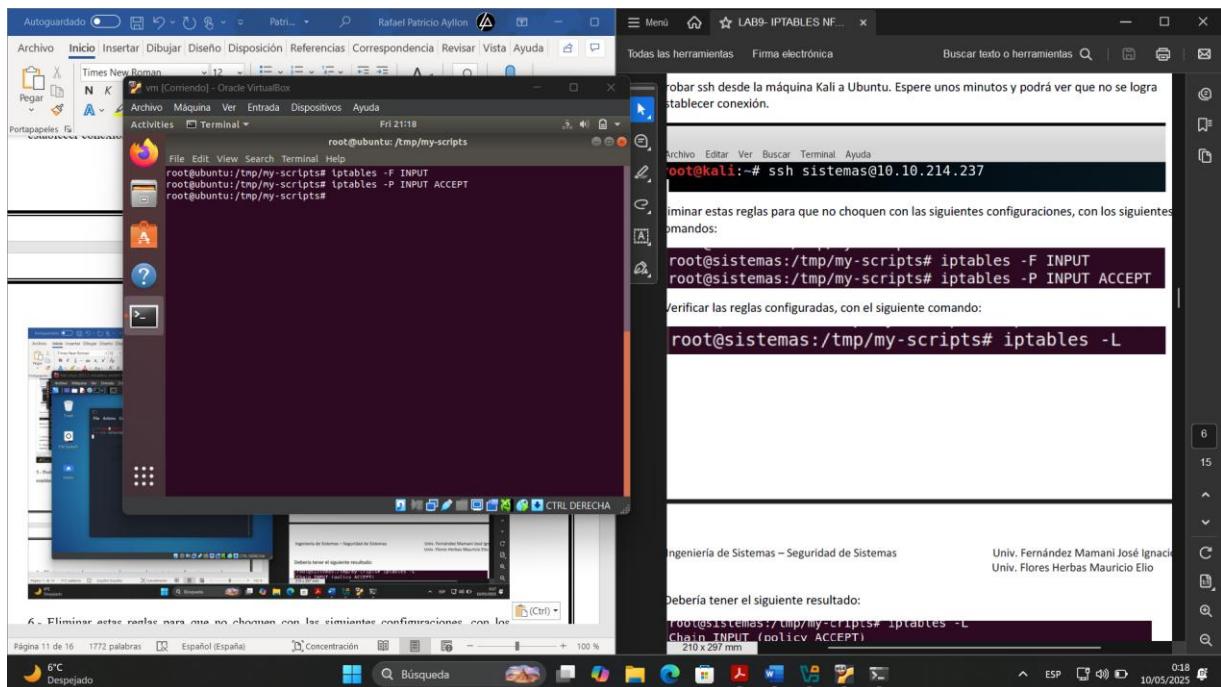
Ejecutar el siguiente comando, no olvide colocar las credenciales de ese usuario. Podrá ver que se establece la conexión normalmente.



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

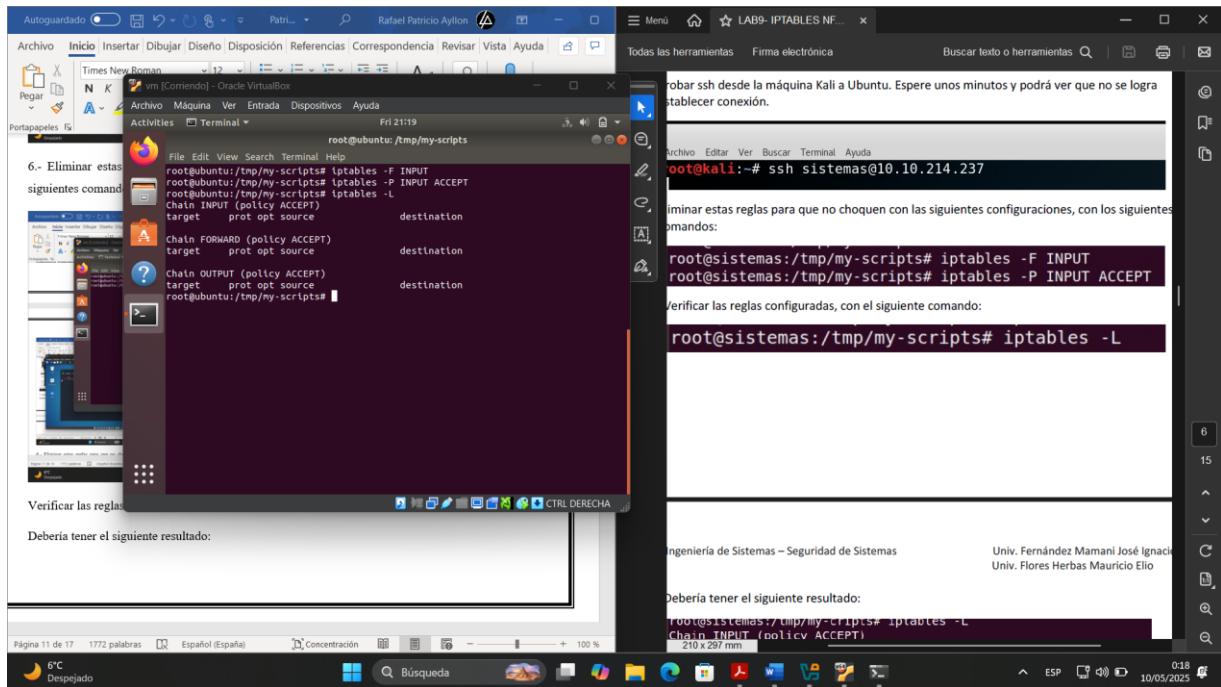


6.- Eliminar estas reglas para que no choquen con las siguientes configuraciones, con los siguientes comandos:



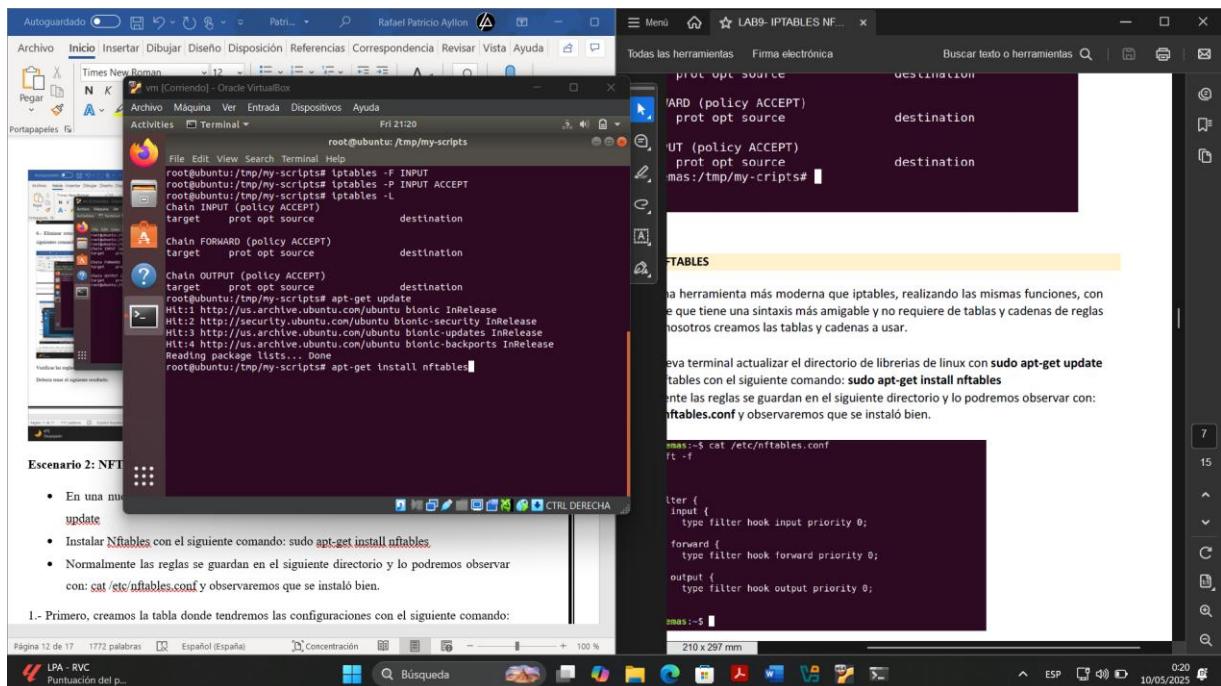
Verificar las reglas configuradas, con el siguiente comando:

Debería tener el siguiente resultado:

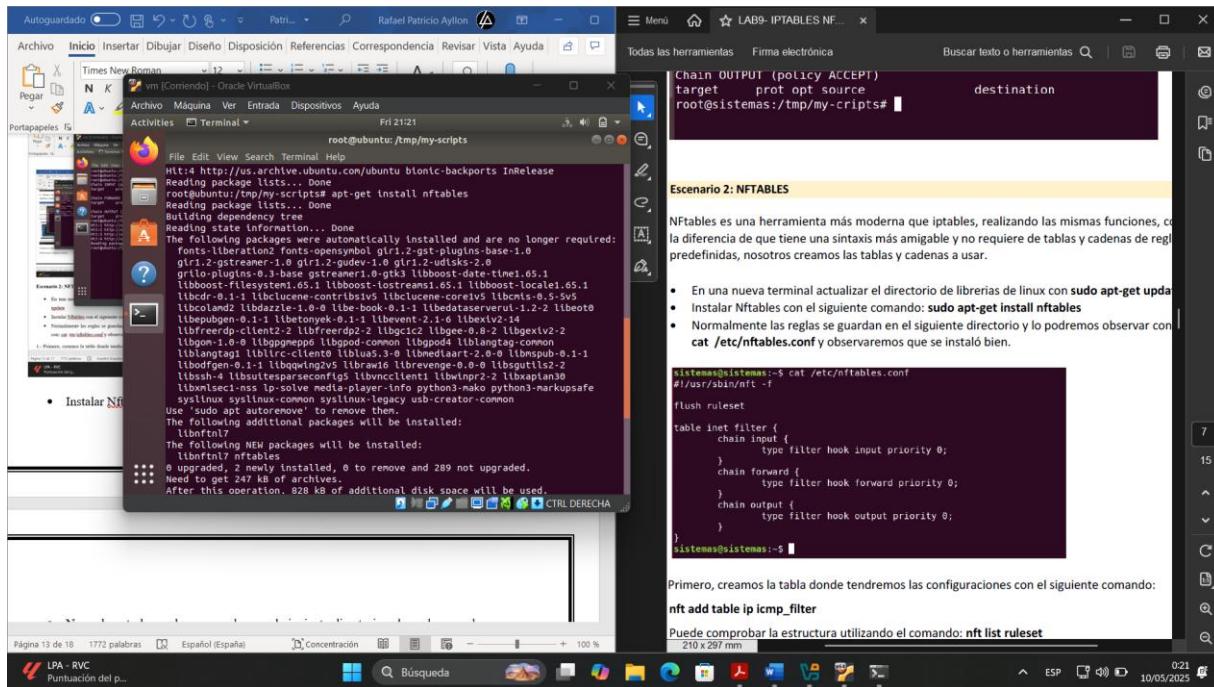


## Escenario 2: NFTABLES

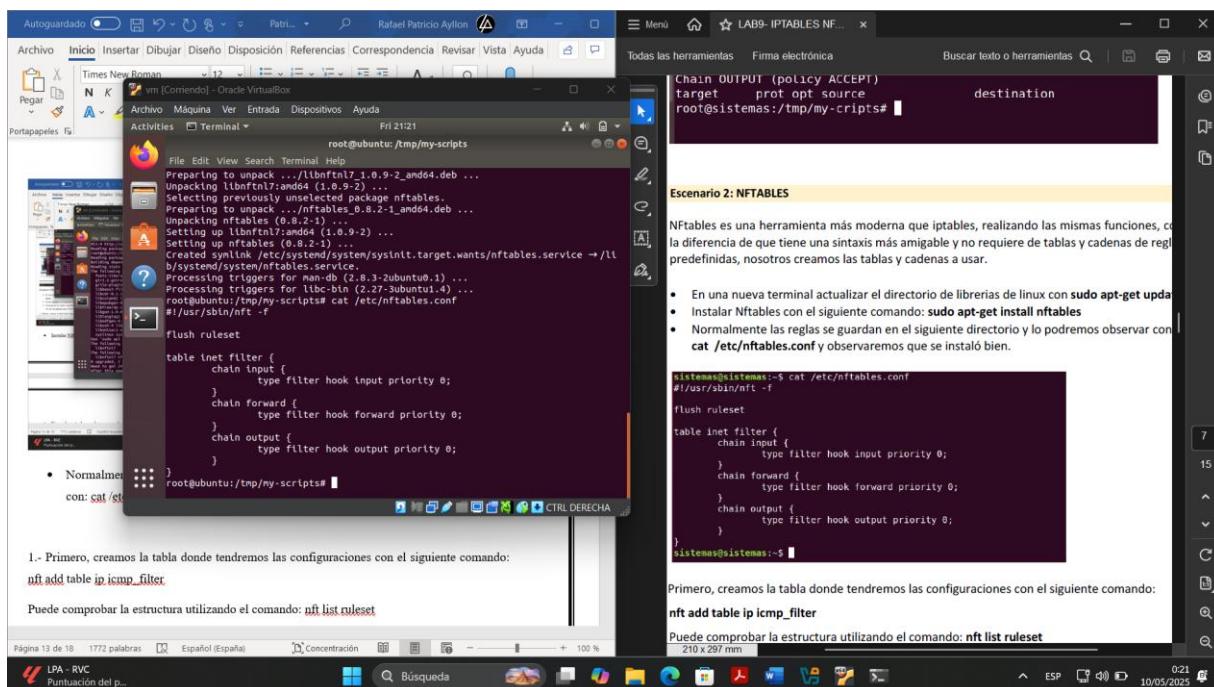
- En una nueva terminal actualizar el directorio de librerías de linux con sudo apt-get update



- Instalar Nftables con el siguiente comando: sudo apt-get install nftables

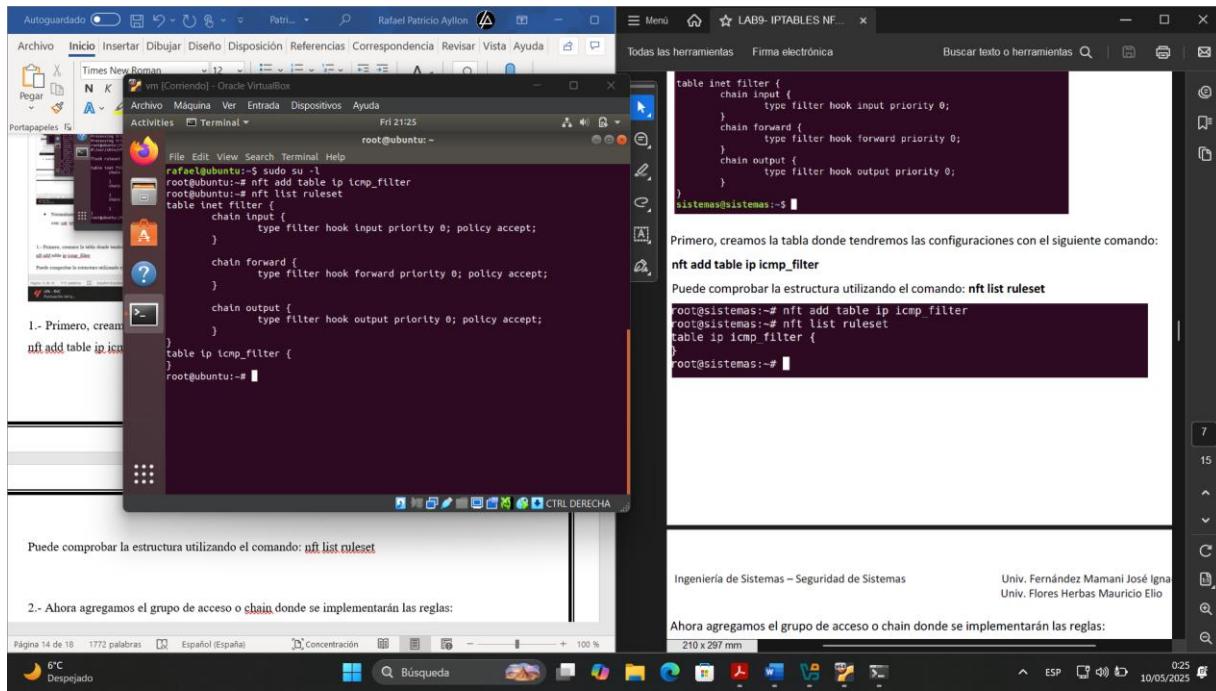


- Normalmente las reglas se guardan en el siguiente directorio y lo podremos observar con: cat /etc/nftables.conf y observaremos que se instaló bien.



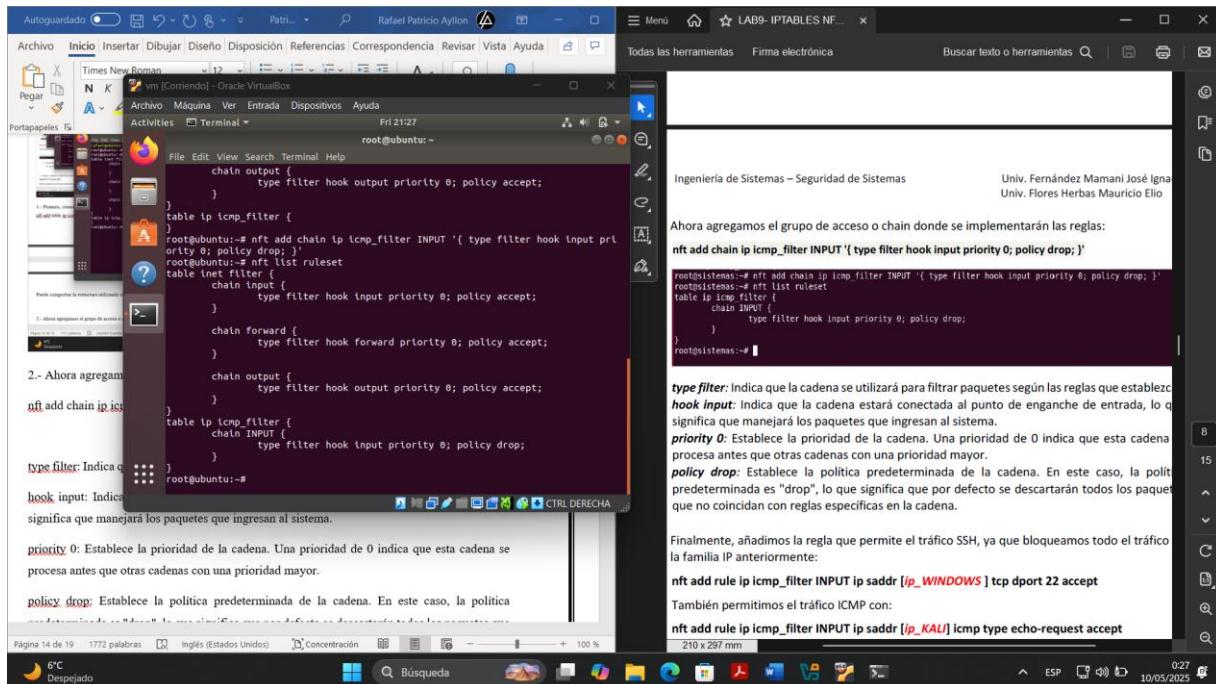
1.- Primero, creamos la tabla donde tendremos las configuraciones con el siguiente comando:  
**nft add table ip icmp\_filter**

Puede comprobar la estructura utilizando el comando: nft list ruleset



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; }'



type filter: 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.

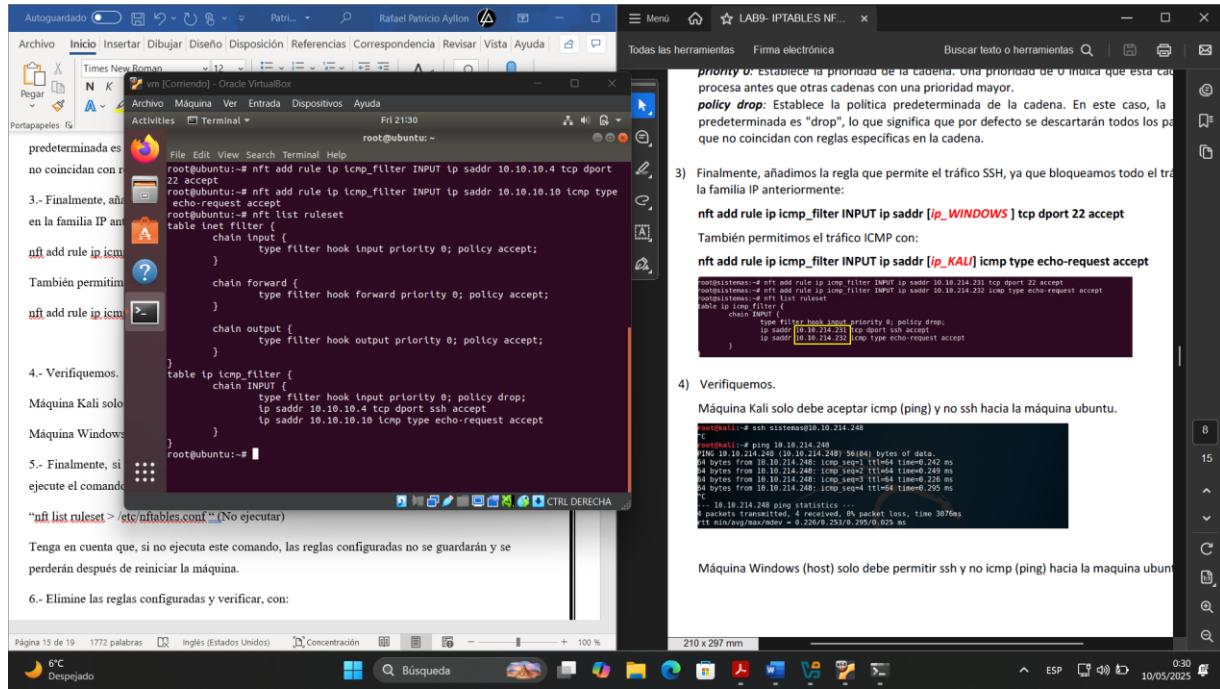
**policy drop:** Establece la política predeterminada de la cadena. En este caso, la política predeterminada es "drop", lo que significa que por defecto se descartarán todos los paquetes que no coincidan con reglas específicas en la cadena.

3.- Finalmente, añadimos la regla que permite el tráfico SSH, ya que bloqueamos todo el tráfico en la familia IP anteriormente:

```
nft add rule ip icmp_filter INPUT ip saddr 10.10.10.4 tcp dport 22 accept
```

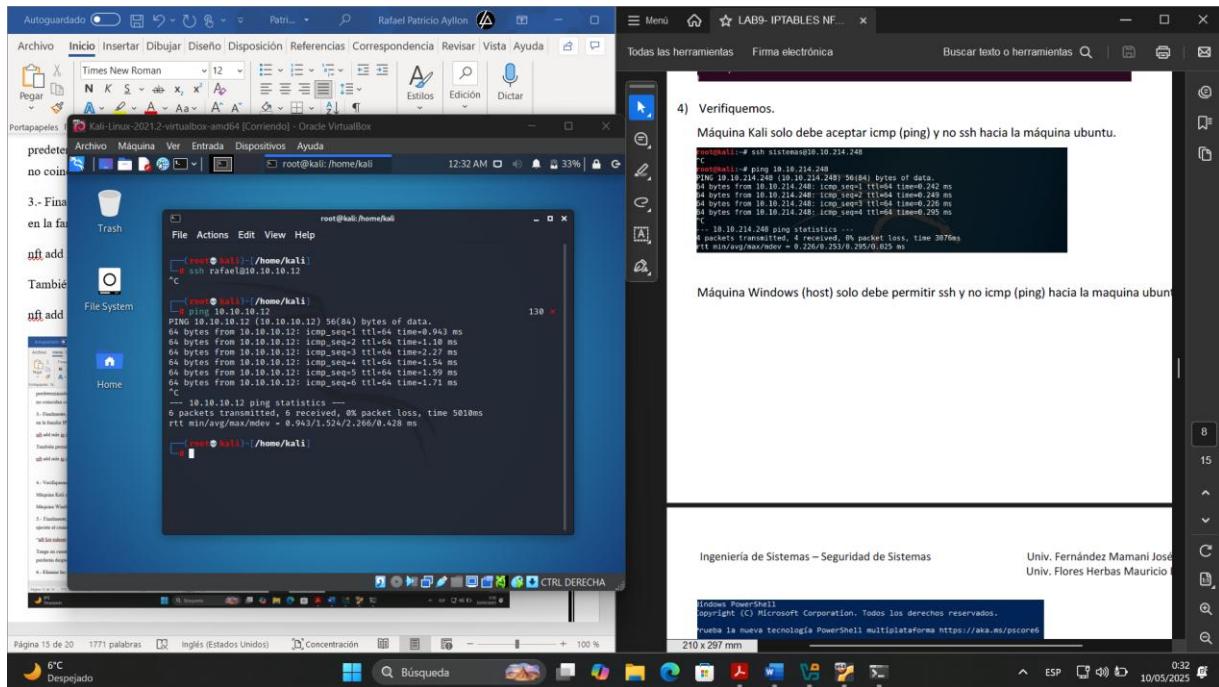
También permitimos el tráfico ICMP con:

```
nft add rule ip icmp_filter INPUT ip saddr 10.10.10.10 icmp type echo-request accept
```

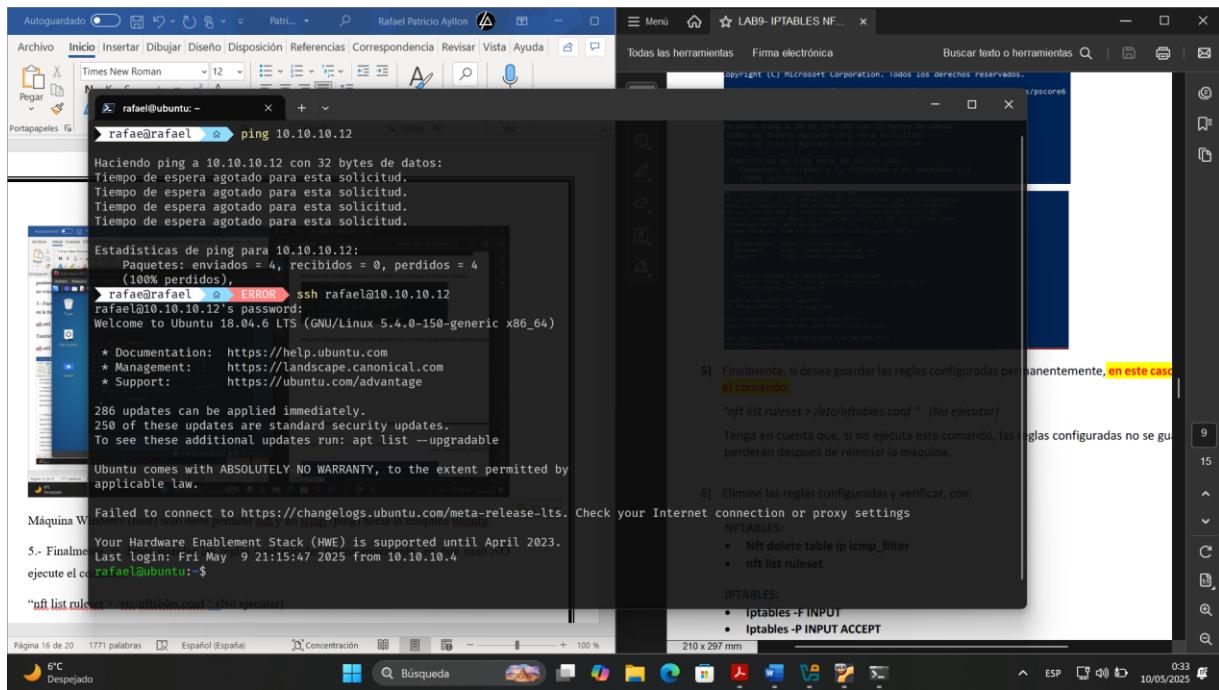


4.- Verifiquemos.

Máquina Kali solo debe aceptar icmp (ping) y no ssh hacia la máquina ubuntu.



Máquina Windows (host) solo debe permitir ssh y no icmp (ping) hacia la maquina ubuntu.



5.- Finalmente, si desea guardar las reglas configuradas permanentemente, en este caso NO ejecute el comando.

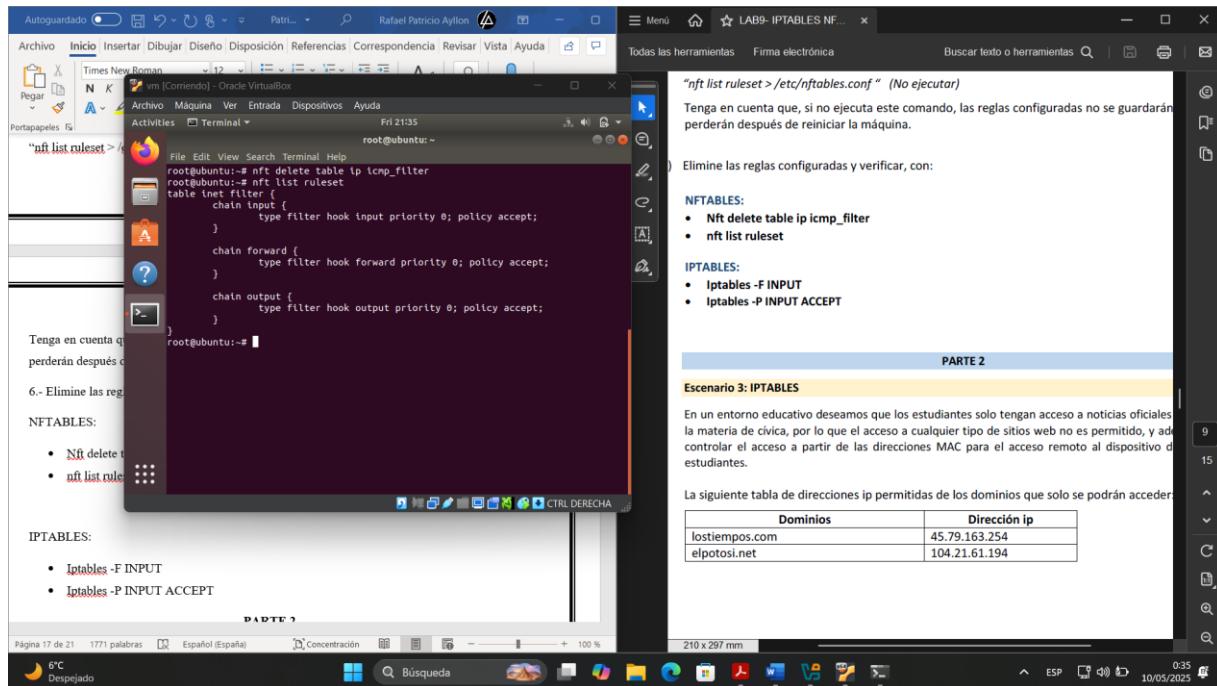
“nft list ruleset > /etc/nftables.conf “ (No ejecutar)

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

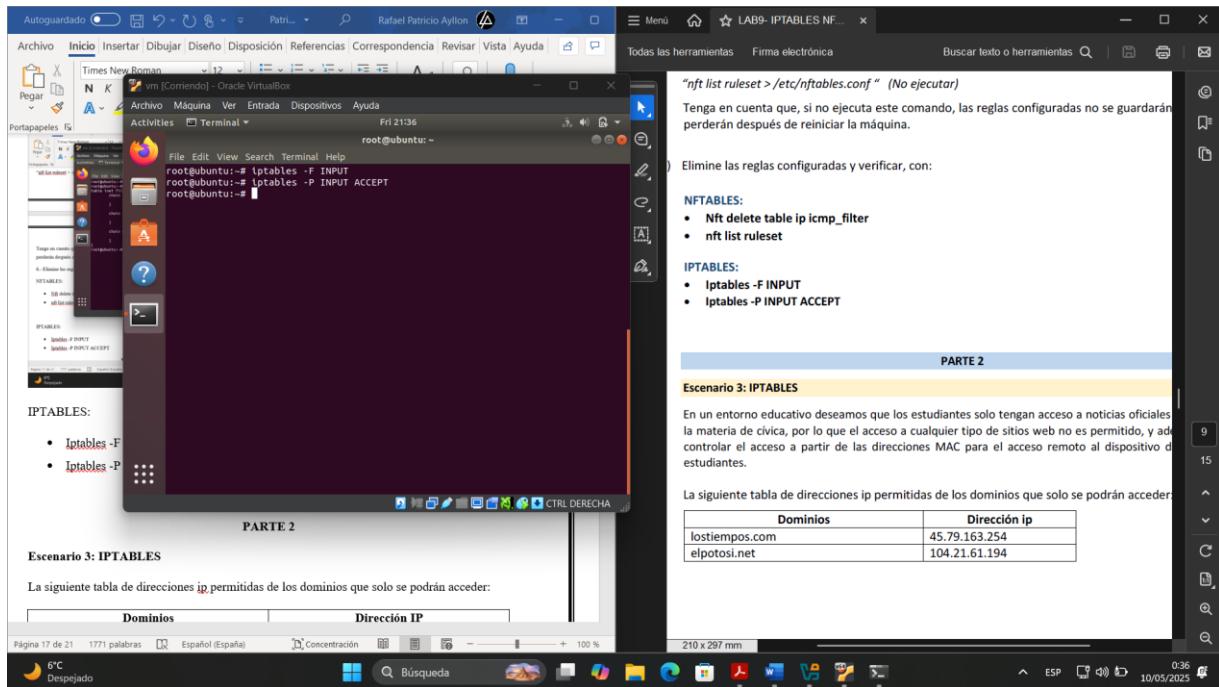
#### PART 2

##### Escenario 3: IPTABLES

En un entorno educativo deseamos que los estudiantes solo tengan acceso a noticias oficiales de 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 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



## PARTE 2

### Escenario 3: IPTABLES

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

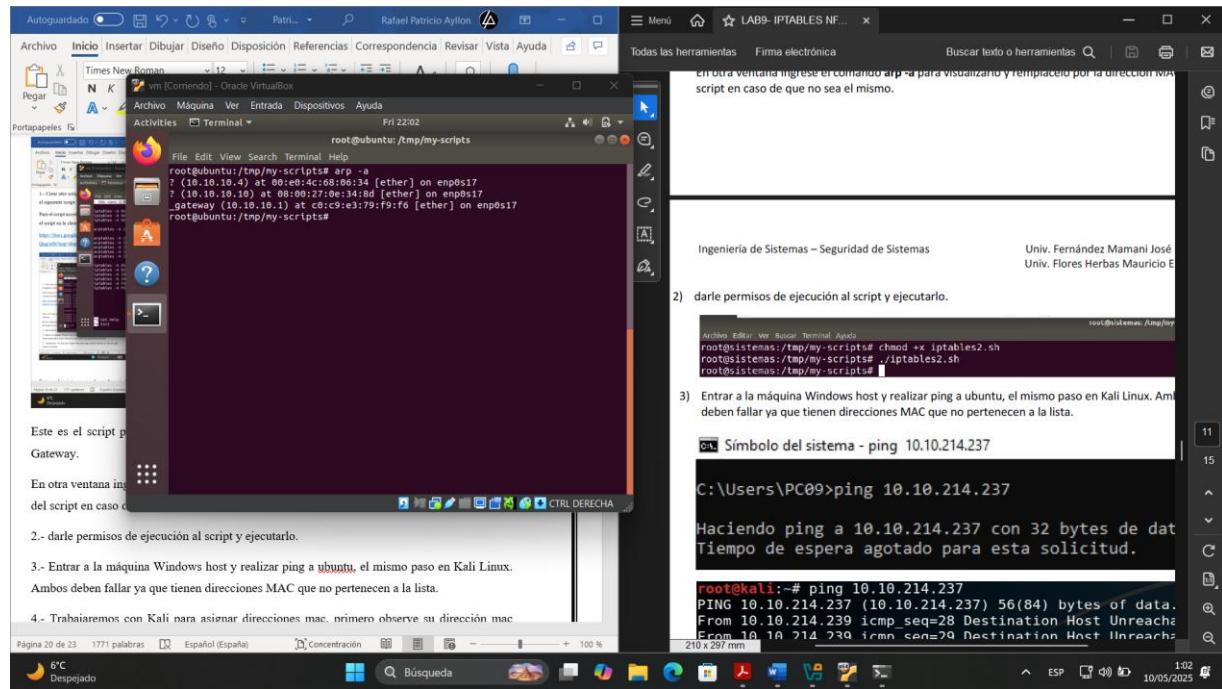
Tabla de direcciones mac permitida:

Dispositivo	MAC
Kali	12:34:56:78:90:00
Kali	99:88:77:66:55:44
Kali	40:50:60:70:80:90

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

Para el script acceda al siguiente enlace, también se le proporcionara un documento que contiene el script en la clase, cópielo dentro del script iptables2.sh

<https://docs.google.com/document/d/15jktnVjZONXZCAFLWzJWcmGW1ue6QB8ntnK69NaQng/edit?usp=sharing>



Este es el script para que le resulta más fácil configurarlo, si no tiene la dirección mac del Gateway.

```
#!/bin/bash
iptables -F INPUT
iptables -F OUTPUT
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
arptables -P INPUT DROP
arptables -A INPUT -d 45.79.163.254 -j ACCEPT
arptables -A INPUT -d 104.61.61.123 -j ACCEPT
arptables -A INPUT -d 104.67.213.89 -j ACCEPT
arptables -A INPUT -d 104.22.75.193 -j ACCEPT
arptables -A INPUT -d 104.22.74.193 -j ACCEPT
arptables -A INPUT -d 172.67.28.27 -j ACCEPT
arptables -A INPUT -d 37.59.238.221 -j ACCEPT
arptables -A INPUT -d 8.8.8.8 -j ACCEPT
arptables -A INPUT --source-mac c0:c9:e3:79:f9:f6 -j ACCEPT
arptables -A INPUT --source-mac 02:34:56:78:90:00 -j ACCEPT
arptables -A INPUT --source-mac 99:88:77:66:55:44 -j ACCEPT
arptables -A INPUT --source-mac 40:50:66:70:80:90 -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
Save modified buffer? (Answering "No" will DISCARD changes.)
  Y Yes
  N No
  C Cancel
```

2.- darle permisos de ejecución al script y ejecutarlo.

```
root@sistemas:/tmp/my-scripts chmod +x iptables2.sh
root@sistemas:/tmp/my-scripts ./iptables2.sh
root@sistemas:/tmp/my-scripts$
```

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

C:\ 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 dat

Tiempo de espera agotado para esta solicitud.

```
root@kali:~# ping 10.10.214.237
PING 10.10.214.237 (10.10.214.237) 56(84) bytes of data.
From 10.10.214.239 icmp_seq=28 Destination Host Unreache
```

1.- Crear otro script para el script acceso el script en la clase.

```
https://docs.google.com/document/d/1Qng/edit?usp=sharing
```

```
#!/bin/bash
iptables -F INPUT
iptables -F OUTPUT
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
arptables -P INPUT DROP
arptables -A INPUT -d 172.67.28.27 -j ACCEPT
arptables -A INPUT -d 37.59.238.221 -j ACCEPT
arptables -A INPUT -d 8.8.8.8 -j ACCEPT
arptables -A INPUT --source-mac c0:c9:e3:79:f9:f6 -j ACCEPT
arptables -A INPUT --source-mac 02:34:56:78:90:00 -j ACCEPT
arptables -A INPUT --source-mac 99:88:77:66:55:44 -j ACCEPT
arptables -A INPUT --source-mac 40:50:66:70:80:90 -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
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
```

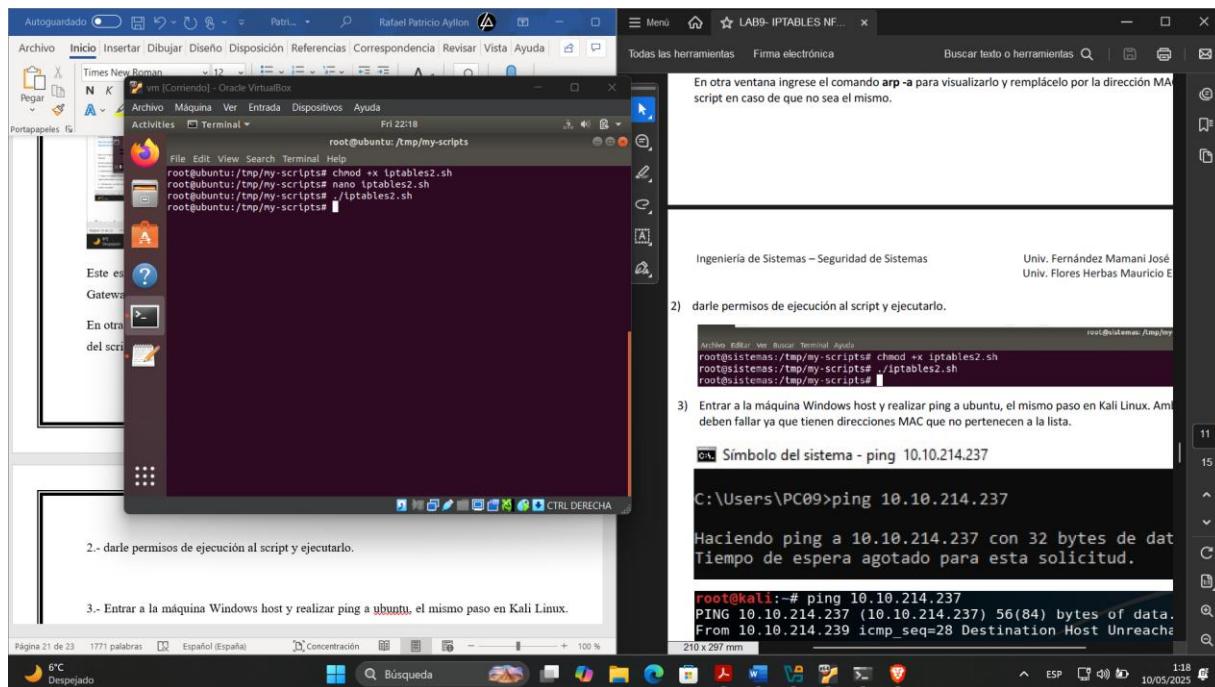
Este es el script para que resulta más fácil configurarlo, si no tiene la dirección mac del Gateway.

En otra ventana ingrese el comando arp -a para visualizarlo y remplácelo por la dirección MAC del script en caso de que no sea el mismo.

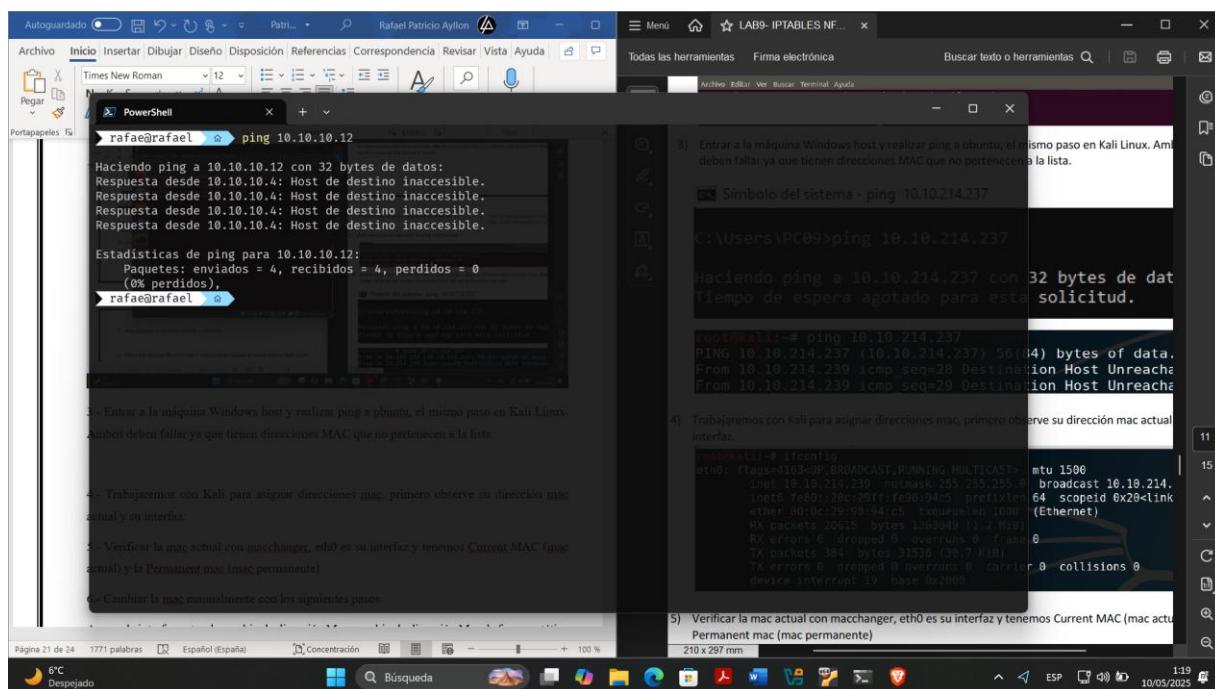
Este es el script para que le resulta más fácil configurarlo, si no tiene la dirección mac del Gateway.

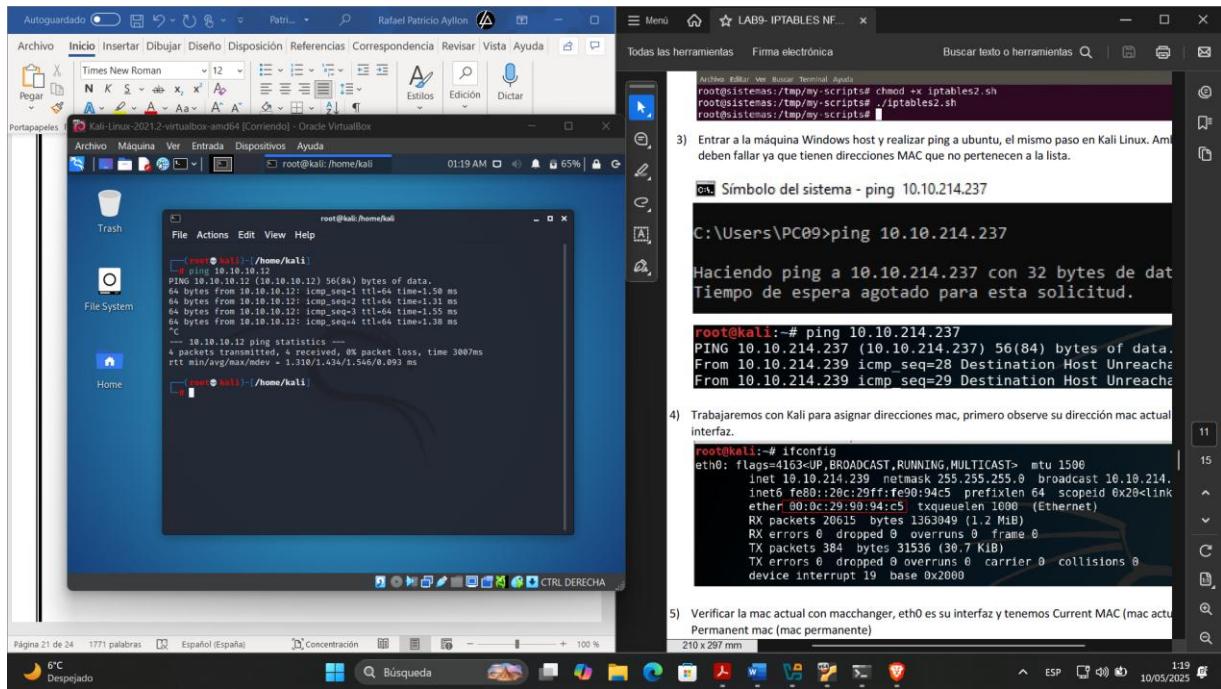
En otra ventana ingrese el comando arp -a para visualizarlo y remplácelo por la dirección MAC del script en caso de que no sea el mismo.

## 2.- darle permisos de ejecución al script y ejecutarlo.

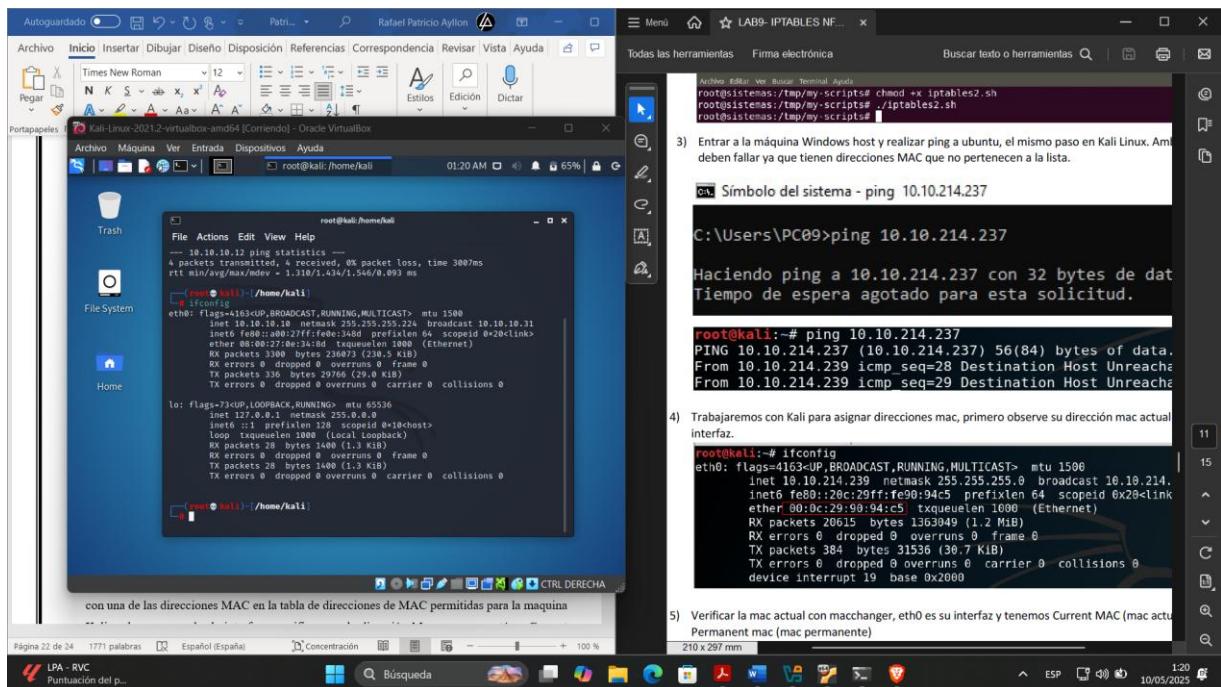


## 3.- Entrar a la máquina Windows host y realizar ping a ubuntu, el mismo paso en Kali Linux. Ambos deben fallar ya que tienen direcciones MAC que no pertenecen a la lista.

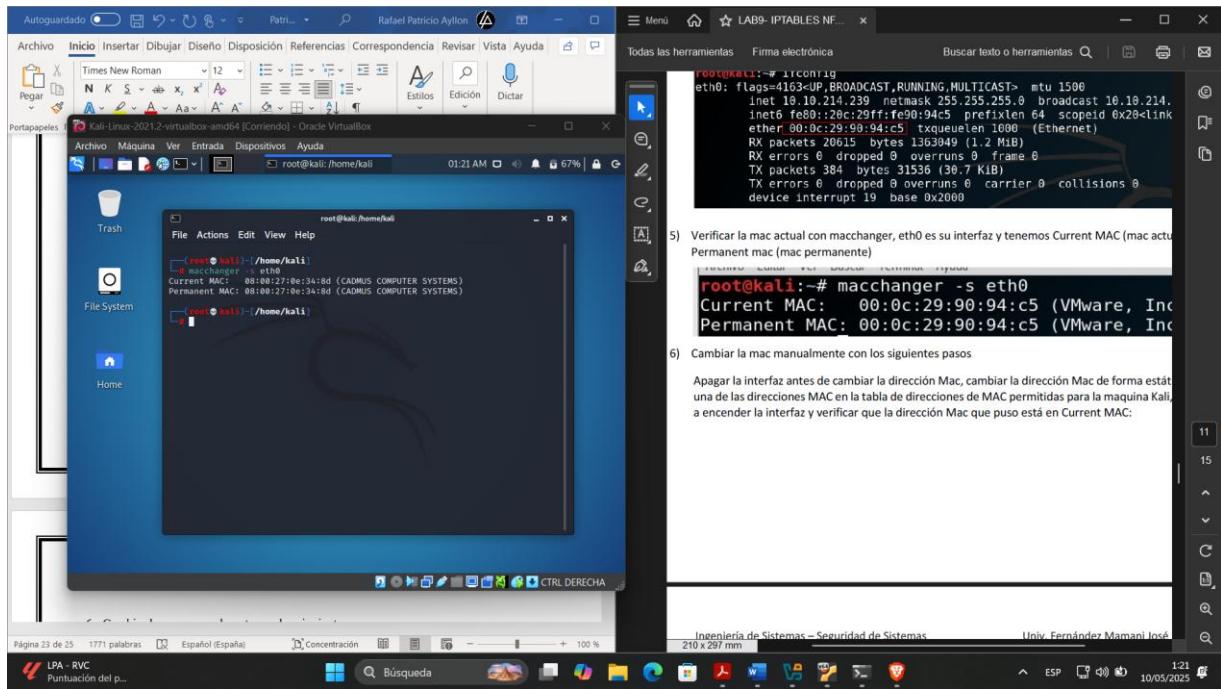




4.- Trabajaremos con Kali para asignar direcciones mac, primero observe su dirección mac actual y su interfaz.

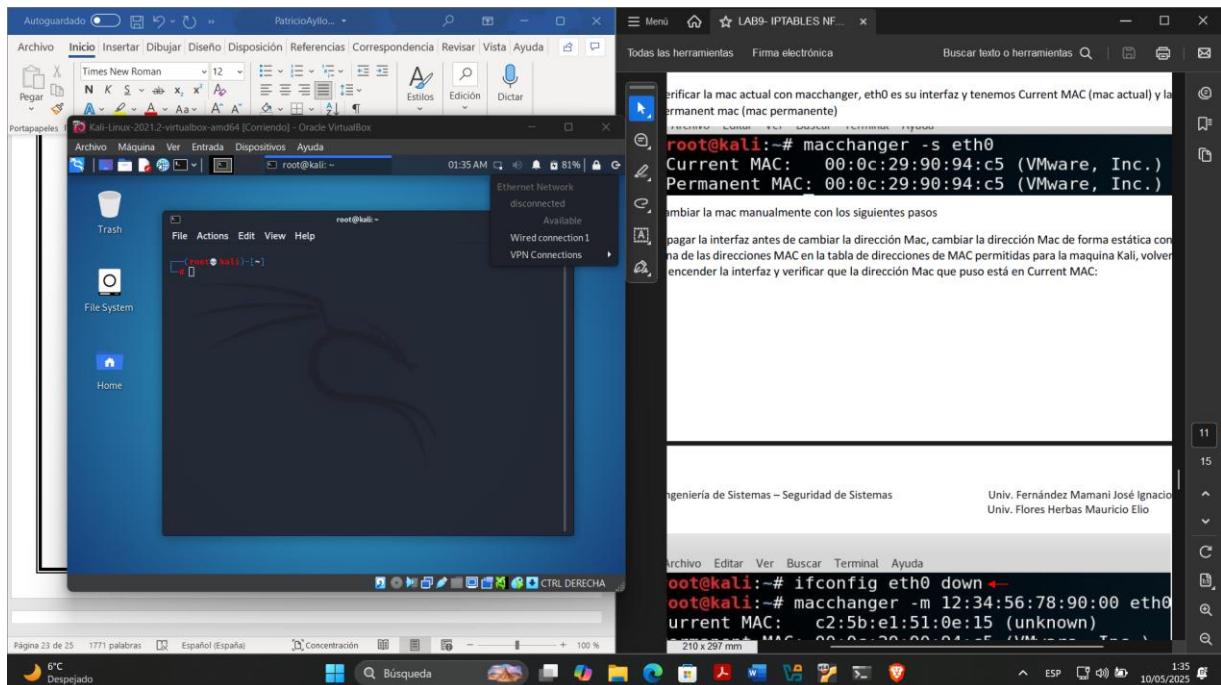


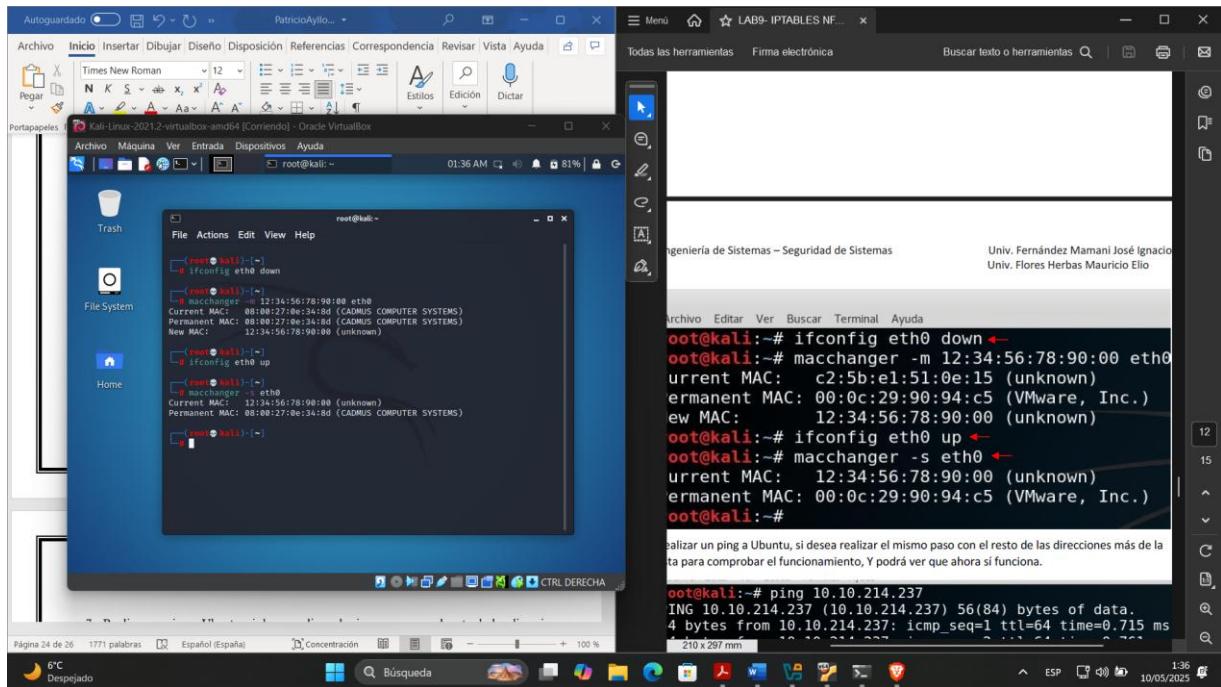
5.- Verificar la mac actual con macchanger, eth0 es su interfaz y tenemos Current MAC (mac actual) y la Permanent mac (mac permanente)



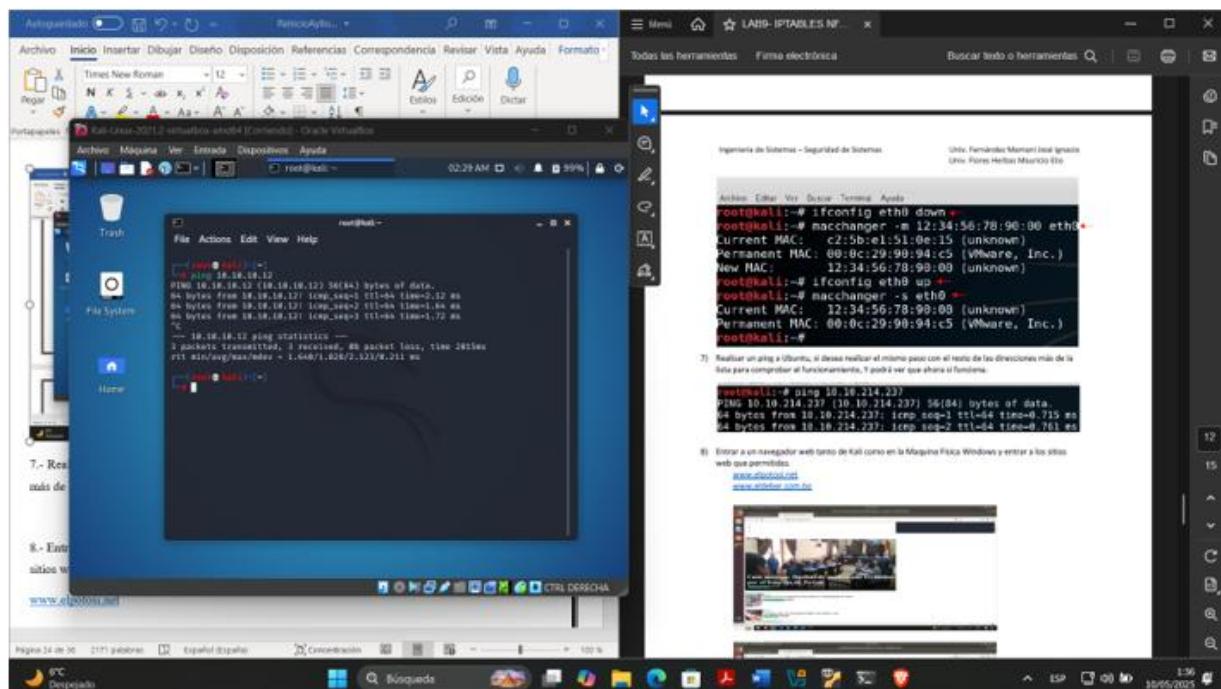
## 6.- Cambiar la mac manualmente con los siguientes pasos

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 maquina Kali, volver a encender la interfaz y verificar que la dirección Mac que puso está en Current MAC:





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



8.- Entrar a un navegador web tanto de Kali como en la Maquina Física Windows y entrar a los sitios web que permitidas.

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

Potosí, sábado 10 de mayo del 2025

**elPotosí**

Inicio Local Nacional Mundo Cultura Deporte Opinión Revista Ecos

Nacional

## YPFB garantiza abastecimiento de combustible y pide no hacer filas

Desde enero hasta abril de esta gestión, informó que se despacharon más de 400 millones de litros de diésel y de gasolina en todo el país

09/05/2025 17:59 | Erbol

LO MÁS LEÍDO

SEMANA

Local 07 May 2025 Accidentes en minas de Potosí dejan a dos jóvenes fallecidos

Local 05 May 2025 Menor desaparecido aparece muerto junto a "ofrenda satánica"

Nacional 08 May 2025 Moreno está en Palmasola y

LPA - RVC Puntuación del p... Búsqueda 10/05/2025

Autoguardado PatricioAylio... LAB9- IPTABLES NF... 10/05/2025

Archivo Inicio Insertar Dibujar Diseño Disposición Referencias Correspondencia Revisar Vista Ayuda

Portapapeles Kali-Linux-2021.2-virtualbox-amd64 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Diario El Potosí: Noticias de Potosí, Bolivia y el Mundo - Mozilla Firefox

8) Entrar a un navegador web tanto de Kali como en la Maquina Física Windows y entrar a los web que permitidas.

www.elpotosi.net  
www.eldeber.com.bo

root@kali:~# ping 10.10.214.237

PING 10.10.214.237 (10.10.214.237) 56(84) bytes of data

64 bytes from 10.10.214.237: icmp\_seq=1 ttl=64 time=0.7

64 bytes from 10.10.214.237: icmp\_seq=2 ttl=64 time=0.7

Ministerio de Educación mantiene vacaciones escolares para julio, pero no descarta ajustes por el frío

09 May 2025, 16:09 DIGITAL

Waiting for www.gstatic.com...

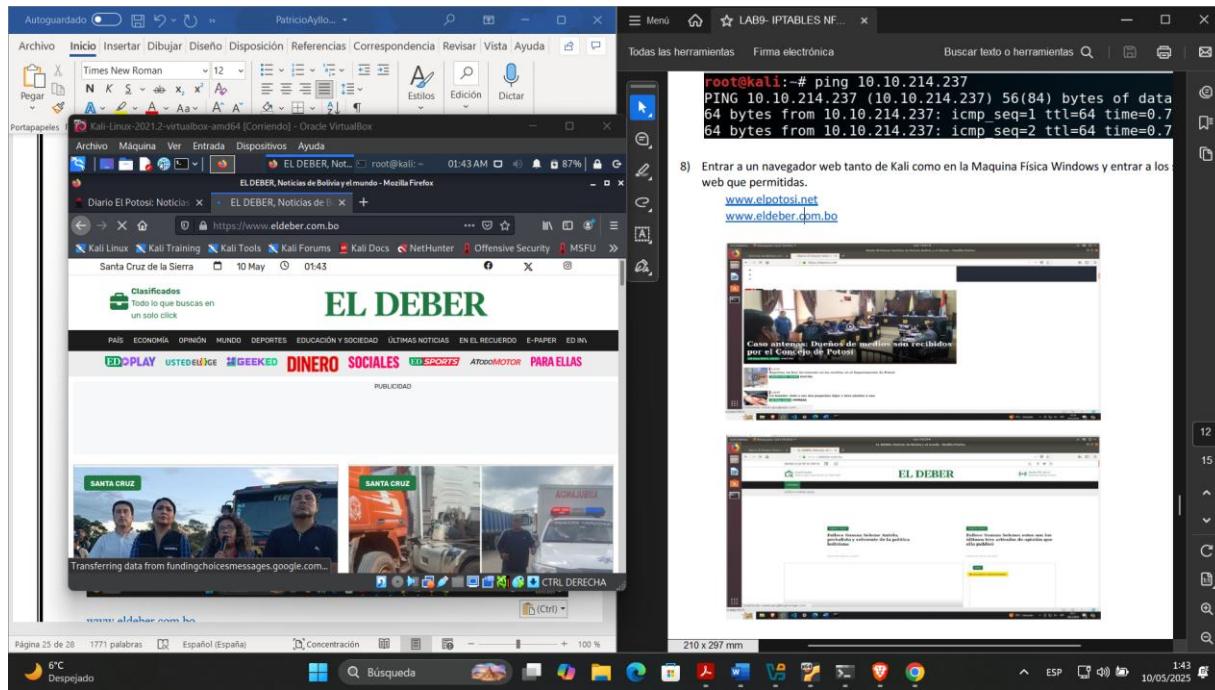
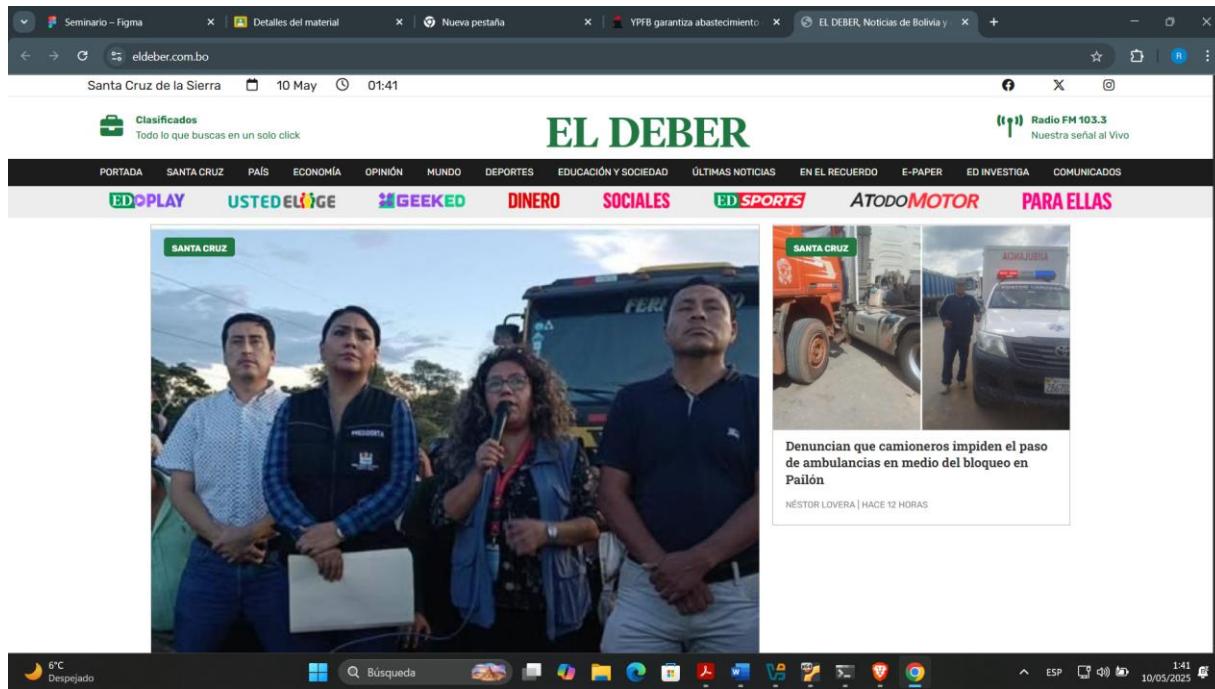
6°C Despejado

Página 24 de 27 1771 palabras Español (España)

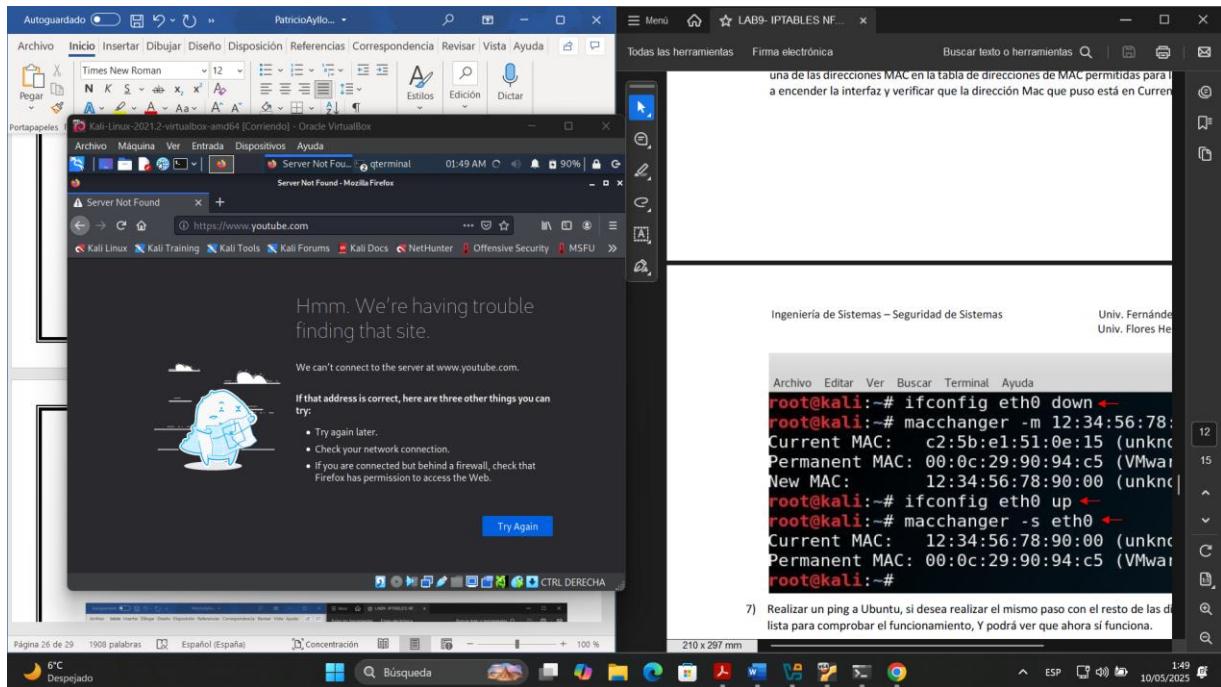
Concentración 210 x 297 mm

Búsqueda 10/05/2025

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



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



R.- Porque en la configuración realizada con iptables o nftables, se establecieron reglas que solo permiten el acceso a ciertas direcciones IP correspondientes a sitios web educativos oficiales (elpotosi.net, eldeber.com.bo, freeditorial.com, etc.).

Las reglas de salida (OUTPUT) en ambos casos bloquean todo el tráfico HTTP/HTTPS (puertos 80 y 443) que no esté dirigido a esas IPs. Como www.youtube.com no está en la lista blanca de IPs permitidas, el acceso es denegado.

**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.**

**PowerShell**

```

rafael@rafael ~ ping 10.10.10.12
Haciendo ping a 10.10.10.12 con 32 bytes de datos:
Respuesta desde 10.10.10.4: Host de destino inaccesible.

Estadísticas de ping para 10.10.10.12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    rafael@rafael ~ ssh rafael@10.10.10.12.com no está en la lista blanca de hosts.
    ssh: connect to host 10.10.10.12 port 22: Connection timed out
    rafael@rafael ~ 255

```

Regresa al escenario anterior en el último escenario ya sea con Iptables, intente acceder a la máquina Ubuntu mediante ssh desde su host Windows. ¿Puede acceder?, capture de pantalla y explique el porqué del comportamiento.

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**

Página 26 de 28 1842 palabras Búsqueda 100 % 210 x 297 mm 6°C Despejado 1:47 ESP 10/05/2025

**LAB9- IPTABLES NF...**

Todos las herramientas Firma electrónica Buscar texto o herramientas

Ingeniería de Sistemas – Seguridad de Sistemas Univ. Fernando Univ. Flores He

**Pregunta 1.** Ahora pruebe acceder a la página de youtube, ¿puede acceder? porqué.

**Pregunta 2.** Nos ubicamos en el último escenario ya sea con Iptables, máquina Ubuntu mediante ssh desde su host Windows, ¿puede acceder?, explique el porqué del comportamiento.

9) Eliminar todas las reglas con:

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

En el último escenario se aplicaron reglas para filtrar el tráfico en base a direcciones MAC, donde solo se permiten MACs específicas (de Kali Linux) para acceder a Ubuntu.

La dirección MAC de la máquina física Windows no está en la lista permitida, por lo tanto, cualquier intento de conexión SSH desde esta máquina será bloqueado por iptables, aunque esté en el mismo segmento de red.

#### 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

```

root@ubuntu:/tmp/my-scripts# iptables -F FORWARD
root@ubuntu:/tmp/my-scripts# iptables -P INPUT ACCEPT
root@ubuntu:/tmp/my-scripts# iptables -P OUTPUT ACCEPT
root@ubuntu:/tmp/my-scripts# iptables -P FORWARD ACCEPT
root@ubuntu:/tmp/my-scripts# iptables -N chain
root@ubuntu:/tmp/my-scripts# iptables -A FORWARD -j chain
root@ubuntu:/tmp/my-scripts# iptables -A chain -m name --name my-chain -j FORWARD
root@ubuntu:/tmp/my-scripts# iptables -A my-chain -m name --name my-script -j ACCEPT
root@ubuntu:/tmp/my-scripts# iptables -P FORWARD ACCEPT
root@ubuntu:/tmp/my-scripts#

```

Pregunta 1. Ahora pruebe acceder a la página de youtube, ¿puede acceder porqué.

Pregunta 2. Nos ubicamos en el último escenario ya sea con Iptables, máquina Ubuntu mediante ssh desde su host Windows, ¿puede acceder?, explique el porqué del comportamiento.

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 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.

Verificar: iptables -L

```

root@ubuntu:/tmp/my-scripts# nft add table inet filterWeb
root@ubuntu:/tmp/my-scripts# nft add chain inet filterWeb OUTPUT '{type filter hook output priority 0;}' 

```

Pregunta 1. Ahora pruebe acceder a la página de youtube, ¿puede acceder porqué.

Pregunta 2. Nos ubicamos en el último escenario ya sea con Iptables, máquina Ubuntu mediante ssh desde su host Windows, ¿puede acceder?, explique el porqué del comportamiento.

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 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.

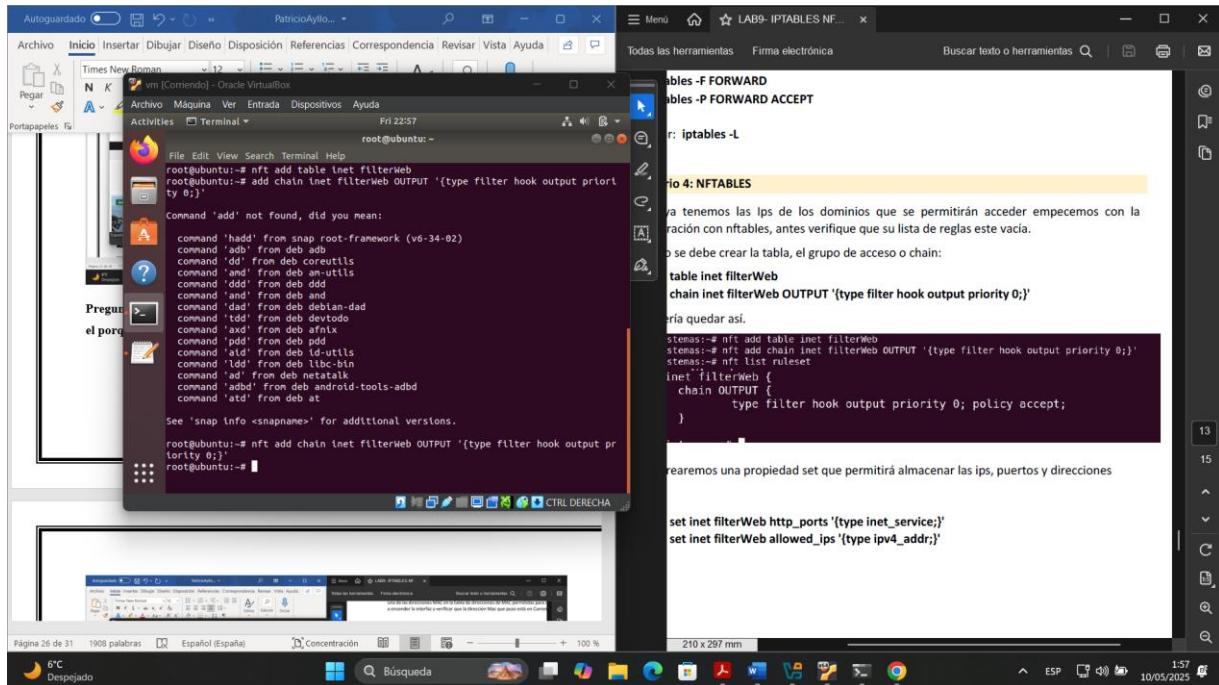
## Escenario 4: NFTABLES

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.



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:

```

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

nft add set inet filterWeb allowed_ips '{type ipv4_addr;}'  

nft add rule inet filter filterWeb http_ports type filter hook input priority 0; policy accept;  

nft add rule inet filter filterWeb allowed_ips type filter hook output priority 0; policy accept;

```

2) Luego crearemos una propiedad set que permitirá almacenar las ips, puertos y dirección MAC

```

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

nft add set inet filterWeb allowed_ips '{type ipv4_addr;}'  


```

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

Le debería quedar de la siguiente forma:

```

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

nft add set inet filterWeb allowed_ips '{type ipv4_addr;}'  

table inet filterWeb {  

    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;  

    }  

}

```

3.- Nos faltaría añadir los elementos:

`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,`

`104.22.74.193, 172.67.20.27, 37.59.238.221 }`

Debería quedar de la siguiente forma:

```

nft add element inet filterWeb allowed_ip { 45.79.163.254,
104.21.61.194,172.67.213.89,104.22.75.193,
104.22.74.193,172.67.20.27,37.59.238.221 }

Debería quedar de la siguiente forma:

root@sistemas:~# nft add element inet filterWeb http_ports { 80,443 }
root@sistemas:~# nft add element inet filterWeb allowed_ip { 45.79.163.254,104.
21.61.194,172.67.213.89,104.22.75.193,104.22.74.193,172.67.20.27,37.59.238.221 }

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_ip accept
nft add rule inet filterWeb OUTPUT tcp dport @http_ports drop

```

```

nft add element inet filterWeb allowed_ip { 45.79.163.254,
104.21.61.194,172.67.213.89,104.22.75.193,
104.22.74.193,172.67.20.27,37.59.238.221 }

Debería quedar de la siguiente forma:

root@sistemas:~# nft add element inet filterWeb http_ports { 80,443 }
root@sistemas:~# nft add element inet filterWeb allowed_ip { 45.79.163.254,104.
21.61.194,172.67.213.89,104.22.75.193,104.22.74.193,172.67.20.27,37.59.238.221 }

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_ip accept
nft add rule inet filterWeb OUTPUT tcp dport @http_ports drop

```

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_ip accept`

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

Por el momento les debería quedar de la siguiente forma:

The screenshot shows a Linux desktop environment with a terminal window open in the foreground. The terminal window displays the following command and its output:

```
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
Error: Set 'http_ports' does not exist
add rule inet filterWeb OUTPUT tcp dport @http_ports drop
           ^^^^^^^^^^
root@ubuntu:~# nft add rule inet filterWeb OUTPUT tcp dport @http_port drop
root@ubuntu:~# 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 inet filterweb {
    set http_port {
        type inet_service
        elements = { http, https }
    }

    set allowed_ips {
        type ipv4_addr
        elements = { 37.59.238.221, 45.79.163.254,
                     104.21.61.194, 104.22.74.195,
                     104.22.74.207, 172.67.213.89 }
    }
}

chain INPUT {
    type filter hook input priority 0; policy accept;
    in header allowed_ip accept
    tcp dport @http_ports drop
}
```

To the right of the terminal, a browser window is open, displaying the following configuration code:

```
nft add rule inet filterWeb OUTPUT ip daddr @allowed_ips accept
nft add rule inet filterWeb OUTPUT tcp dport @http_ports drop
```

Below the terminal window, the desktop environment shows various icons for applications like file manager, terminal, and system settings.

The screenshot shows a Linux desktop environment with several windows open:

- A terminal window titled "root@ubuntu:~" containing the following iptables configuration:

```
root@ubuntu:~# nft add rule inet filterWeb OUTPUT ip daddr @allowed_ips accept
nft add rule inet filterWeb OUTPUT tcp dport @http_ports drop

chain forward {
    type filter hook forward priority 0; policy accept;
}

chain output {
    type filter hook output priority 0; policy accept;
}
table inet filterWeb {
    set http_port {
        type inet_service
        elements = { http, https }
    }

    set allowed_ips {
        type ipv4_addr
        elements = { 37.59.238.221, 45.79.163.254,
                    104.21.61.194, 104.22.74.193,
                    104.22.75.193, 172.63.28.27,
                    172.67.213.89 }
    }

    chain OUTPUT {
        type filter hook output priority 0; policy accept;
        ip daddr @allowed_ips accept
        tcp dport @http_port drop
    }
}
root@ubuntu:~#
```

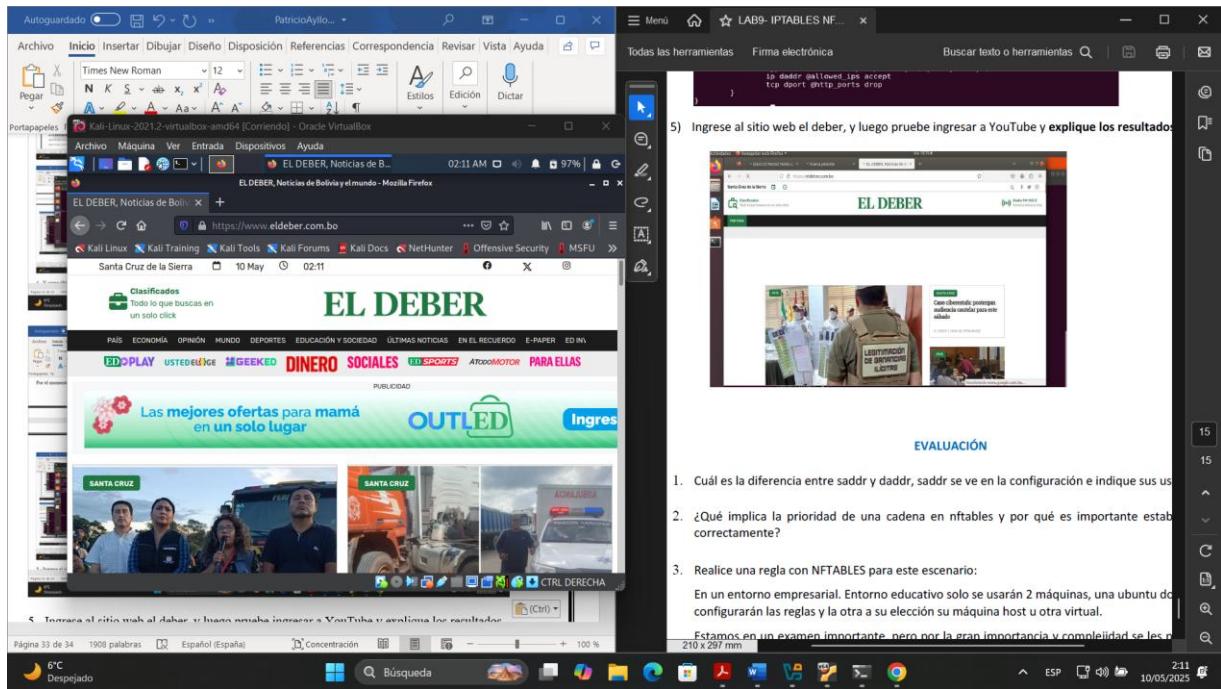
- A browser window titled "vm ([Corriendo]) - Oracle VirtualBox" showing a security page from "Seguridad de Sistemas" with the message: "Por el momento les debería quedar de la siguiente forma:" followed by the same iptables configuration.
- A status bar at the bottom with the message: "5) Ingrese al sitio web el deber, y luego pruebe ingresar a YouTube y explique los resultados".

5.- Ingrese al sitio web el deber, y luego pruebe ingresar a YouTube y explique los resultados.

Se configuró nftables para:

Permitir solo tráfico HTTP/HTTPS (puertos 80 y 443) hacia un conjunto específico de IPs permitidas (como eldeber.com.bo) y bloquear todo el resto del tráfico web saliente.

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

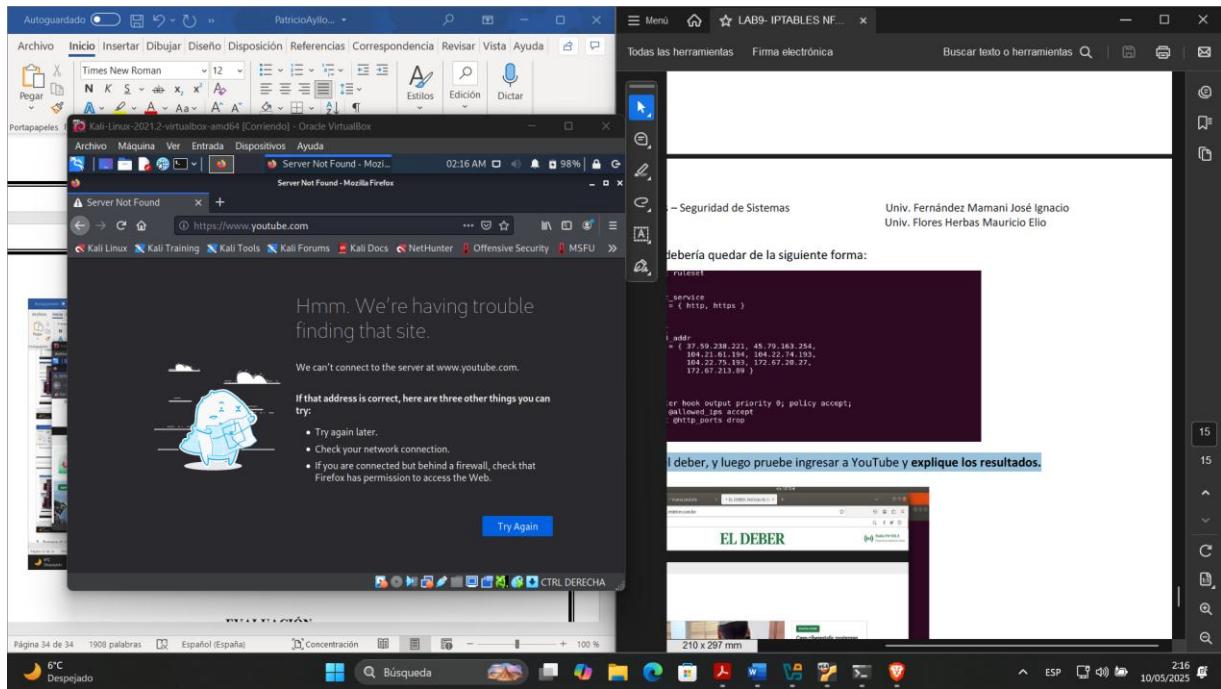


Funciona correctamente porque su IP está en el conjunto @allowed\_ips, por tanto la regla:

nft add rule inet filterWeb OUTPUT ip daddr @allowed\_ips accept

permite la conexión.

Al ingresar a [www.youtube.com](http://www.youtube.com):



El acceso es bloqueado, ya que la IP de YouTube no está en el conjunto permitido, y la siguiente regla impide el resto de tráfico web:

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

## EVALUACIÓN

### 1.- Cuál es la diferencia entre **saddr** y **daddr**, **saddr** se ve en la configuración e indique sus usos.

- **saddr** (source address): Dirección IP de origen del paquete. Se usa para filtrar o aplicar reglas según de dónde viene un paquete.

`ip saddr 192.168.1.0/24 accept` # Aceptar paquetes que vienen de la red 192.168.1.0/24

- **daddr** (destination address): Dirección IP de destino del paquete. Se usa para reglas que controlan a dónde va un paquete.

`ip daddr 8.8.8.8 drop` # Bloquear paquetes que se dirigen al servidor 8.8.8.8

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

La prioridad de una cadena (chain) en nftables determina el orden en el que las reglas dentro de las distintas cadenas se evalúan en relación a otras cadenas del mismo tipo (ej. input, output, forward).

Se expresa con un número entero: cuanto menor el número, mayor la prioridad.

priority -100 se evalúa antes que priority 0

priority 100 se evalúa más tarde

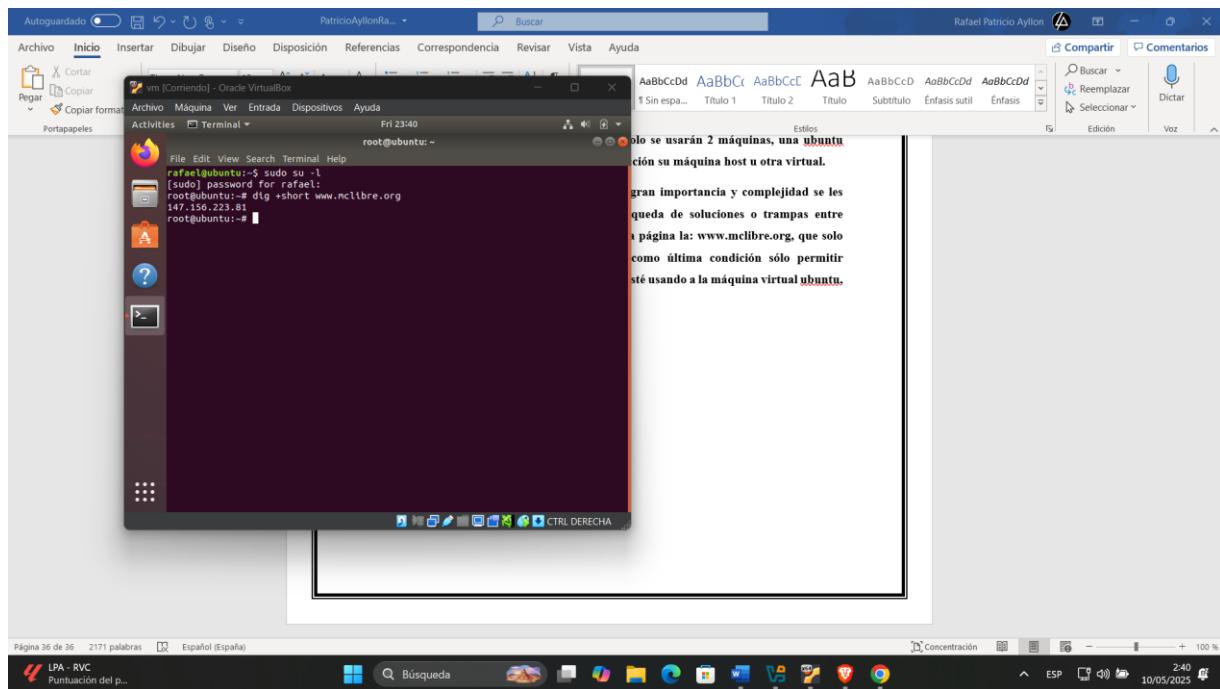
Es importante si hay múltiples reglas en diferentes tablas o hooks, establecer la prioridad evita que una regla menos relevante se aplique antes que otra crítica, como aceptar o denegar tráfico esencial).

### **3. Realice una regla con NFTABLES para este escenario:**

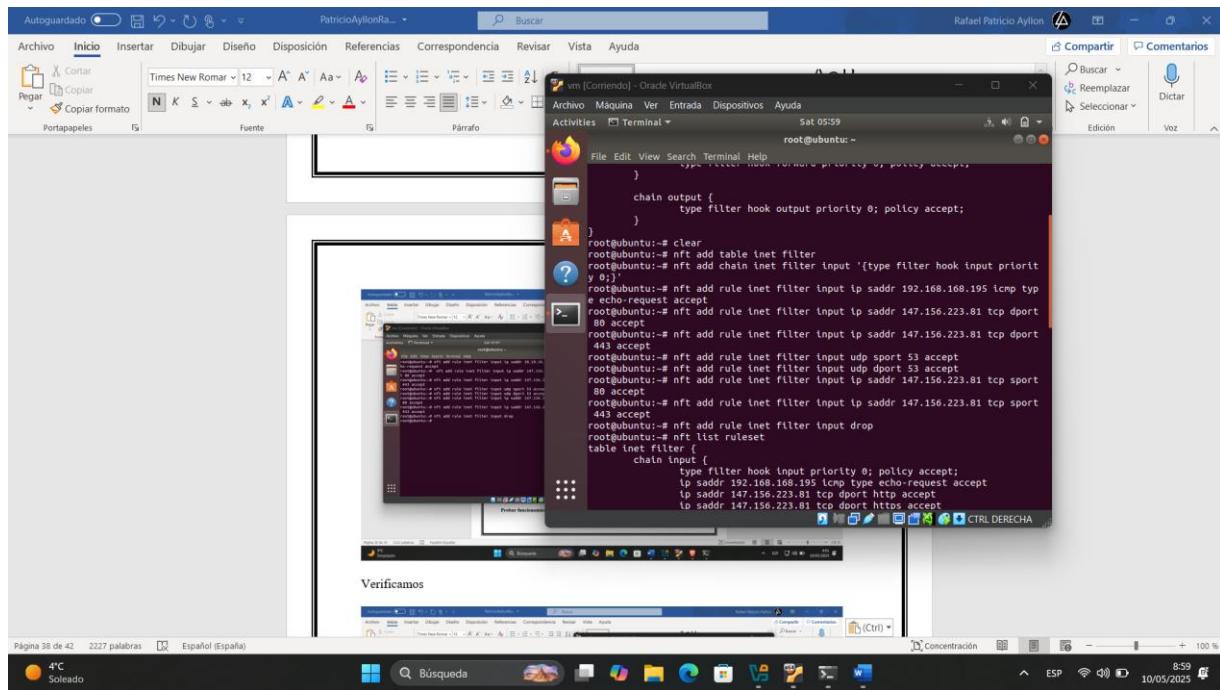
**En un entorno empresarial. Entorno educativo solo se usarán 2 máquinas, una ubuntu donde se configurarán las reglas y la otra a su elección su máquina host u otra virtual.**

**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 contienen 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**

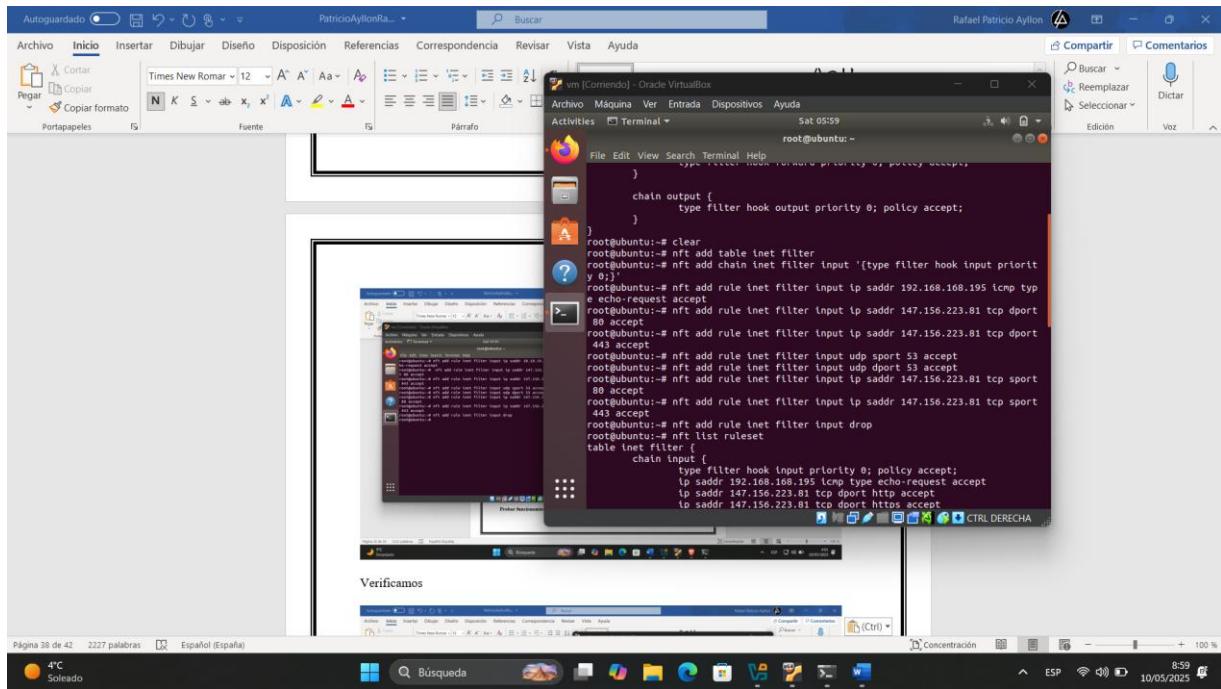
Hallamos la dirección IP de la pagina



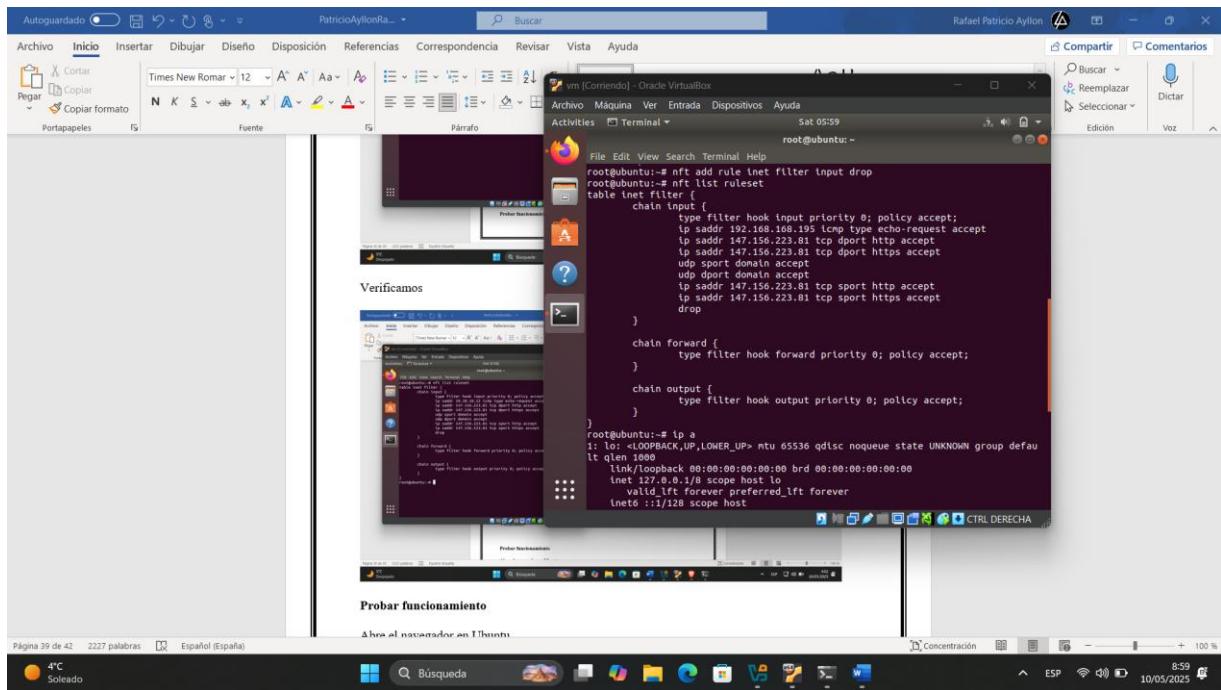
## Creamos la tabla



## Creamos las reglas



## Verificamos

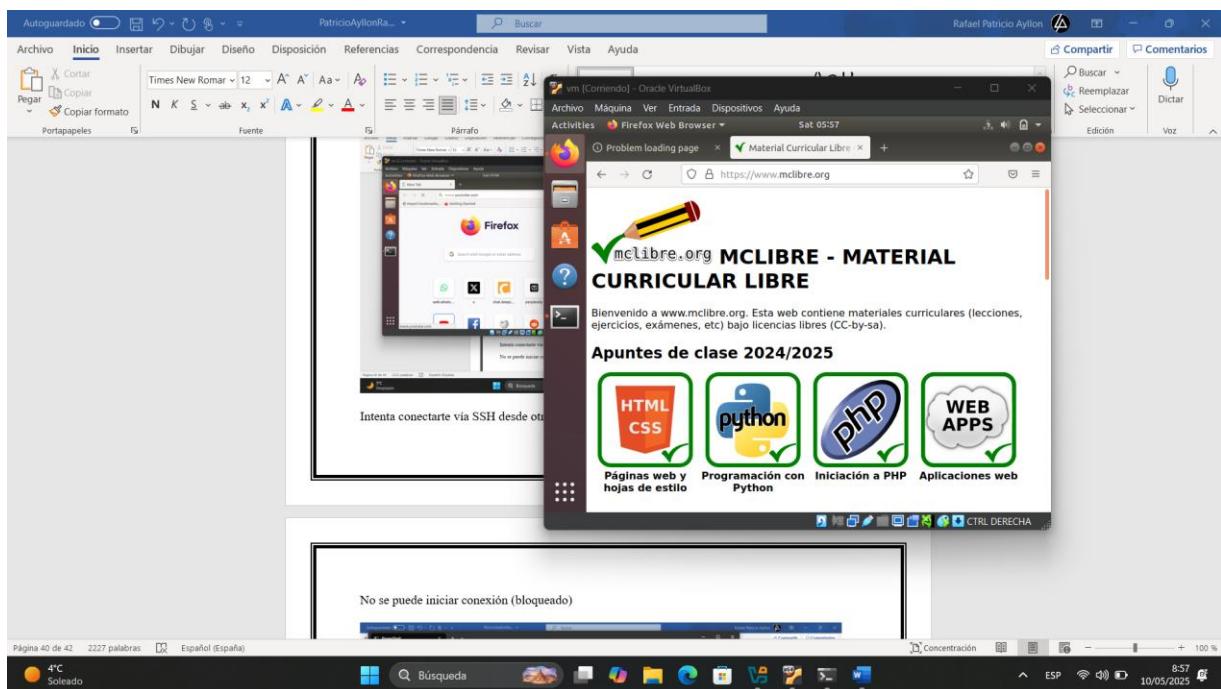
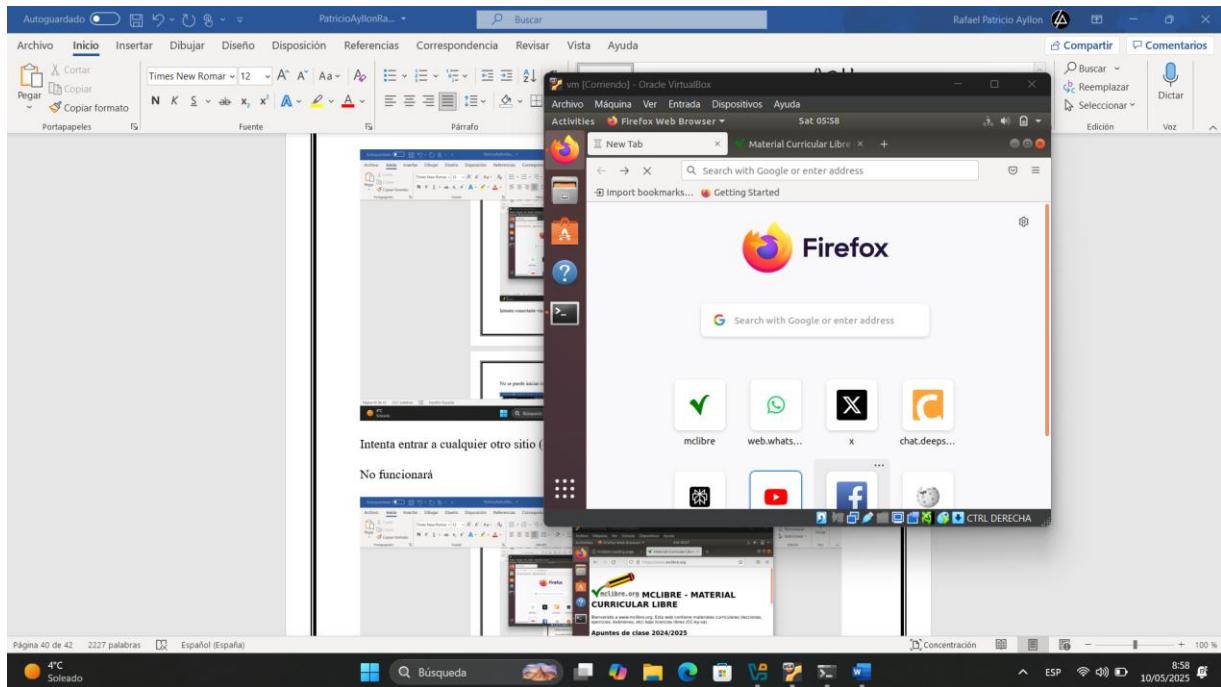


## Probar funcionamiento

Abre el navegador en Ubuntu.

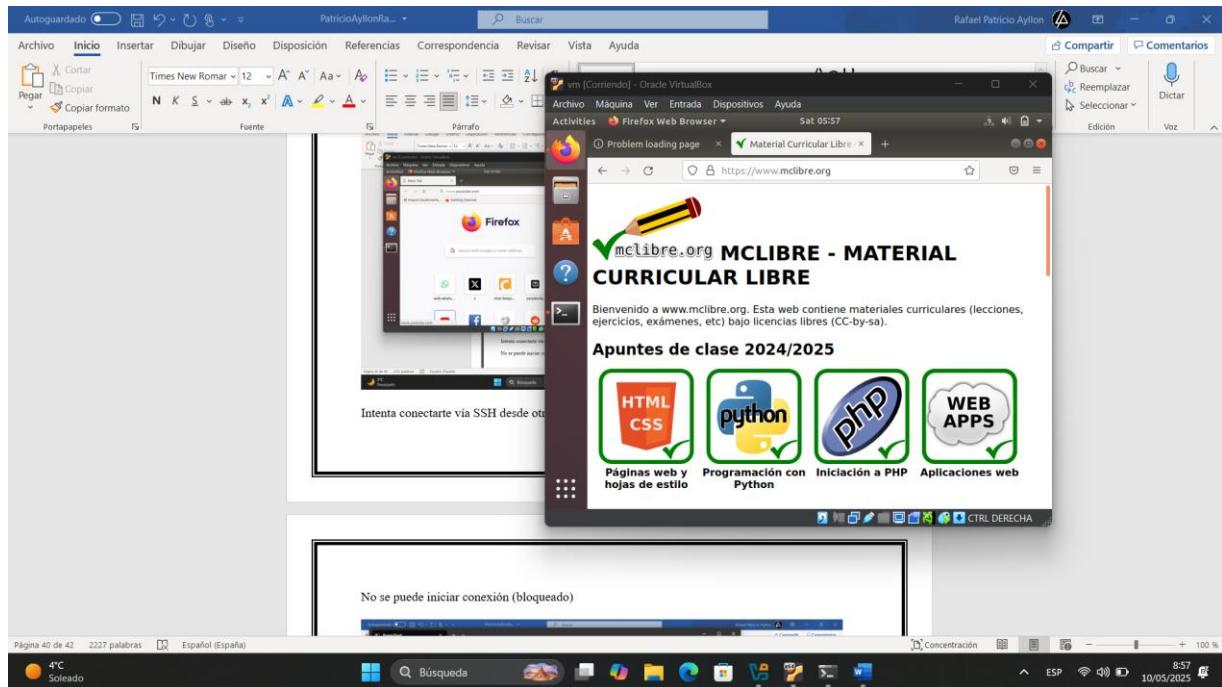
Accede a: <http://www.mclibre.org>

## Debe funcionar



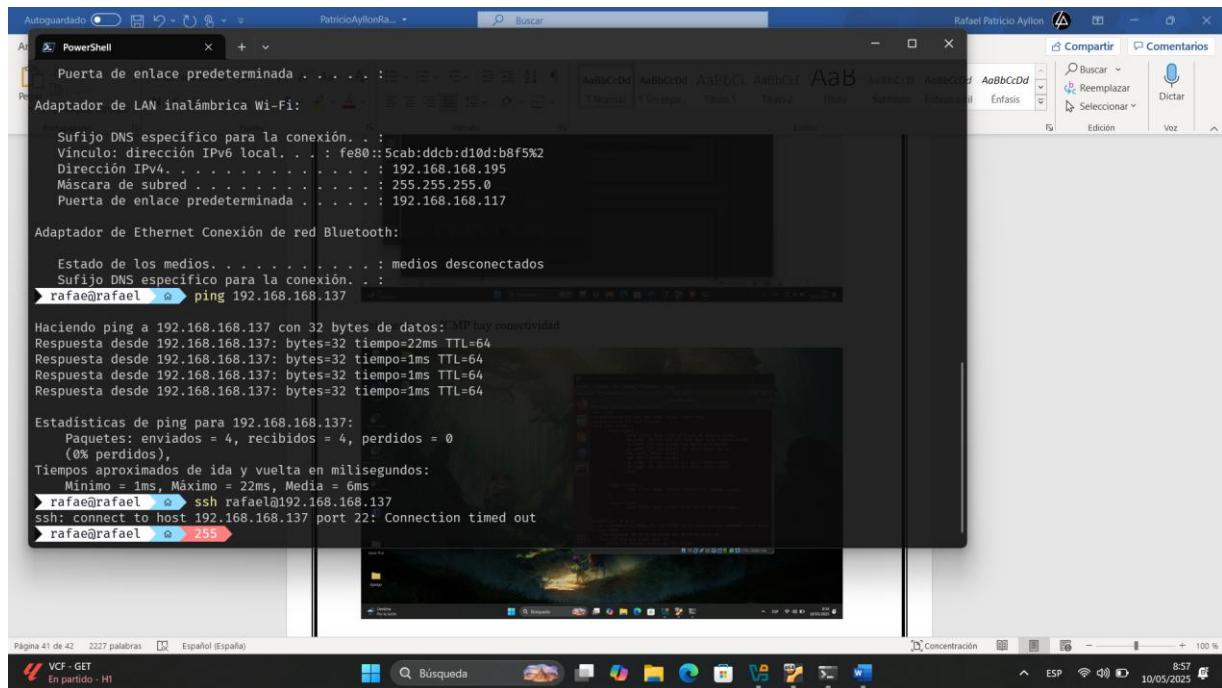
Intenta entrar a cualquier otro sitio (como YouTube)

No funcionará

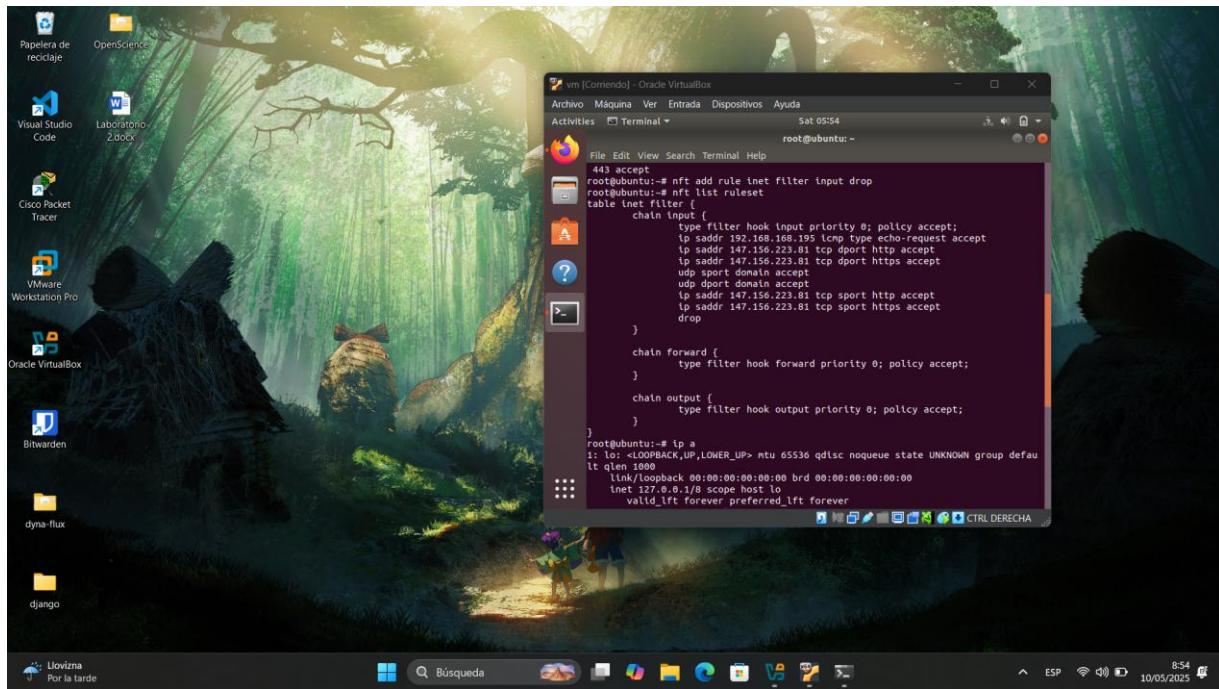


Intenta conectarte vía SSH desde otra máquina a Ubuntu

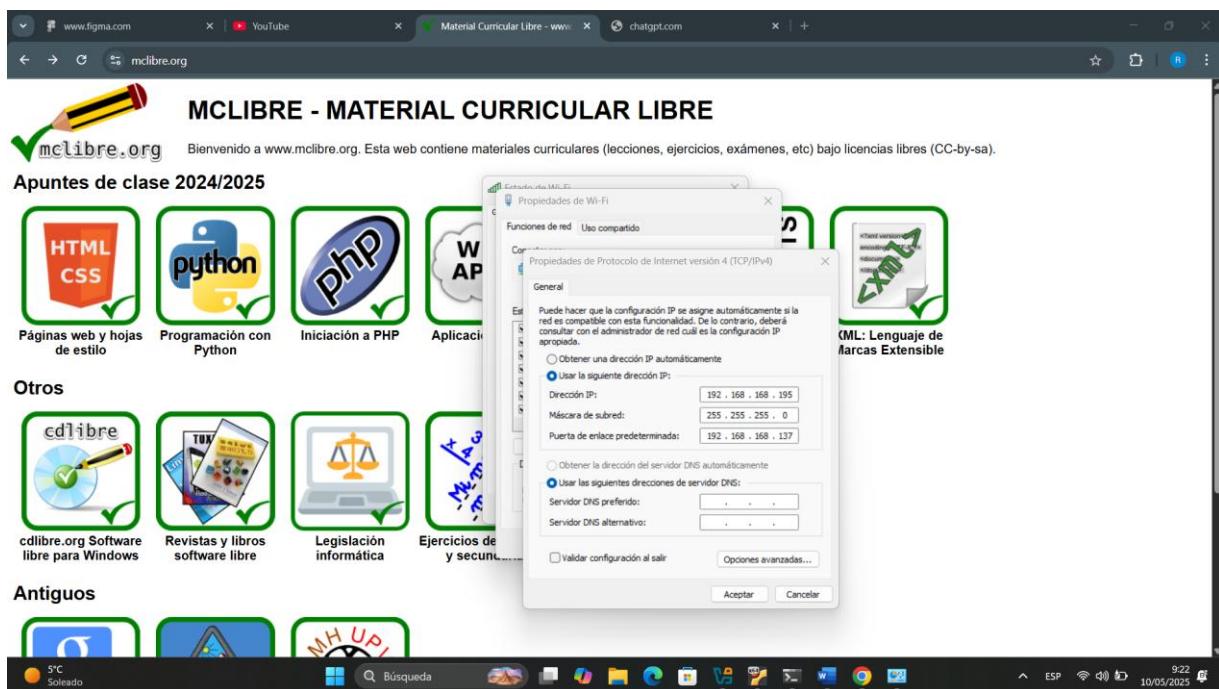
No se puede iniciar conexión (bloqueado)

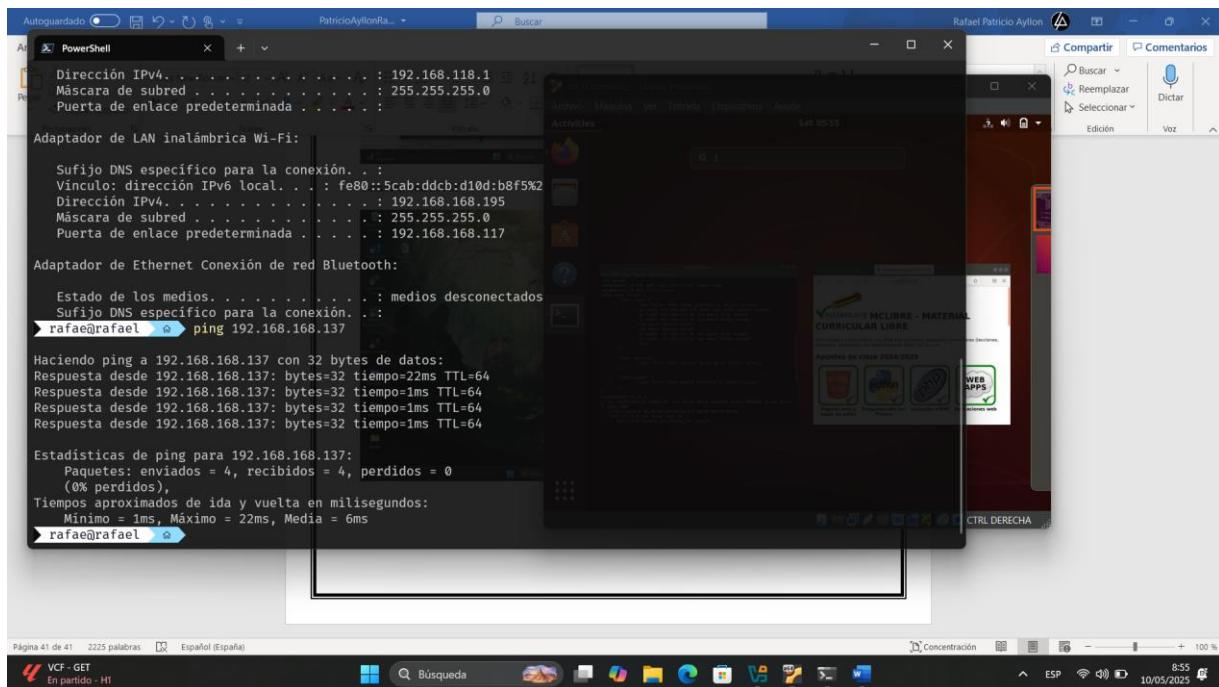


Solamente con ICMP hay conectividad



Cambiamos la ip de Windows y cambiamos como Gateway la IP de Ubuntu





Entramos a la pagina [www.mclibre.org](http://www.mclibre.org) en la maquina Windows



Entramos a [www.youtube.com](https://www.youtube.com)

