

# Laboratorio 9 Seguridad de sistemas

**Nombre:** Uño Astoraique Maria Fernanda

**CI:** 10468920

## LABORATORIO – IPTABLE / NFTABLES

**PROPÓSITO:** IPtables y NFtables que nos permiten configurar reglas de firewall.

**COMPETENCIA:** La seguridad es un punto muy importante a tener en cuenta en cualquier organización, de ahí que sea fundamental hacer uso de aquellos mecanismos que tengamos a nuestro alcance para poner el mayor número de barreras posibles a los atacantes. Es por ello que el desarrollo de conocimientos básicos de la configuración de grupos de reglas firewall a nivel del kernel de Linux con las herramientas IPtables y NFtables es lo que se verá en este laboratorio.

**DESCRIPCIÓN:** Implementar 2 escenarios, desde los cuales el primero se enfoca en dar a conocer los comandos, sintaxis y funcionamiento básico de Iptables y Nftables, el segundo escenario se enfoca en simular un escenario de entorno educativo con la restricción de páginas web y restricción de acceso a partir de direcciones MAC.

### Recursos:

Máquina Virtual Ubuntu 18 y Kali Linux.

Todos en el mismo segmento de red.

### DESARROLLO

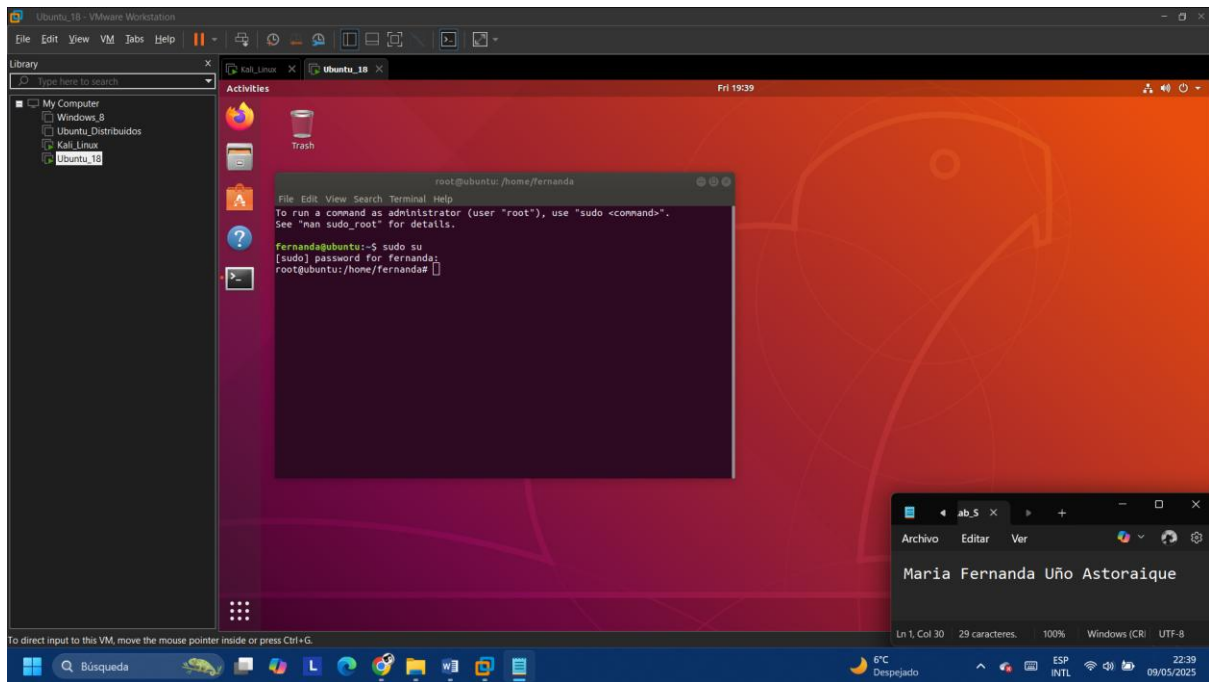
#### PASO 1:

Acceda a la máquina virtual Ubuntu y Kali entre a la terminal y colóquese modo super usuario.

#### Ubuntu

Usuario: root

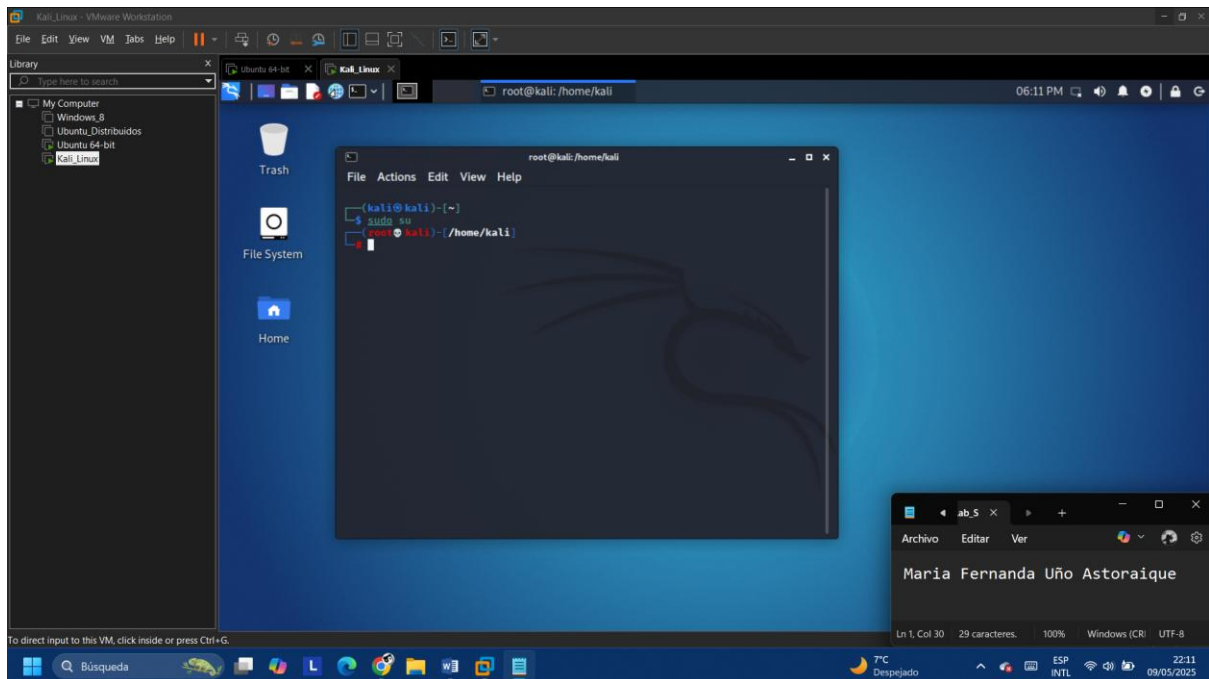
Password: sistemas



## Kali Linux

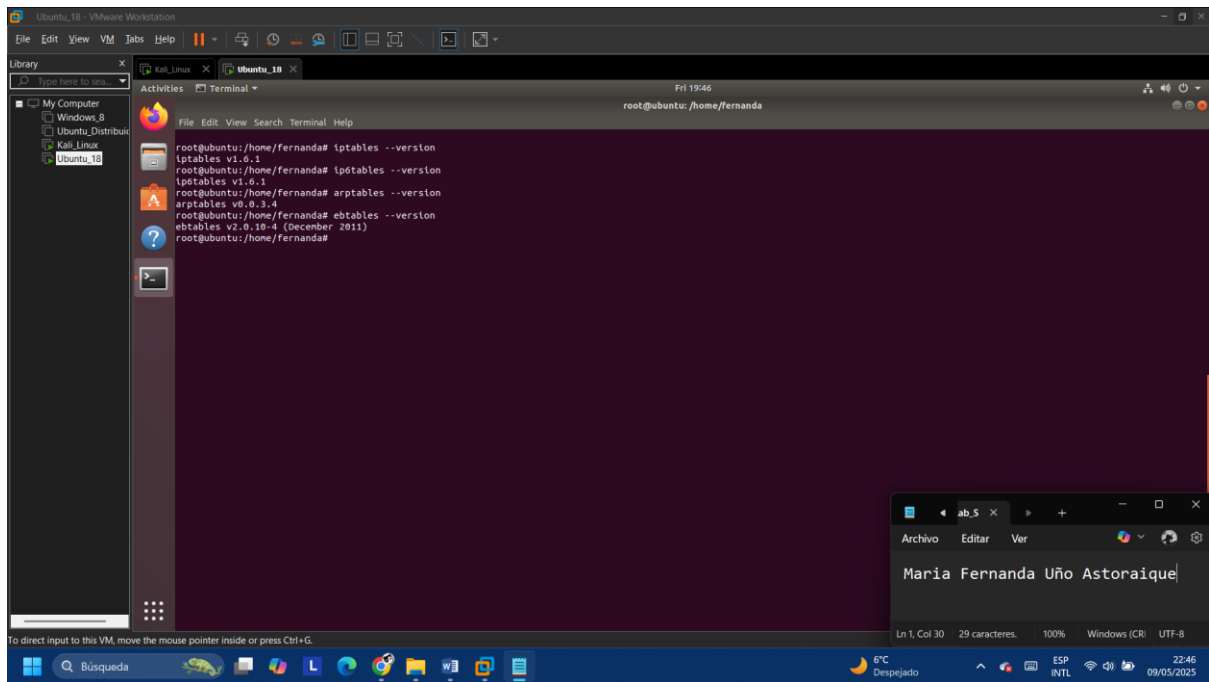
Usuario: root

Password: sistemas



**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.

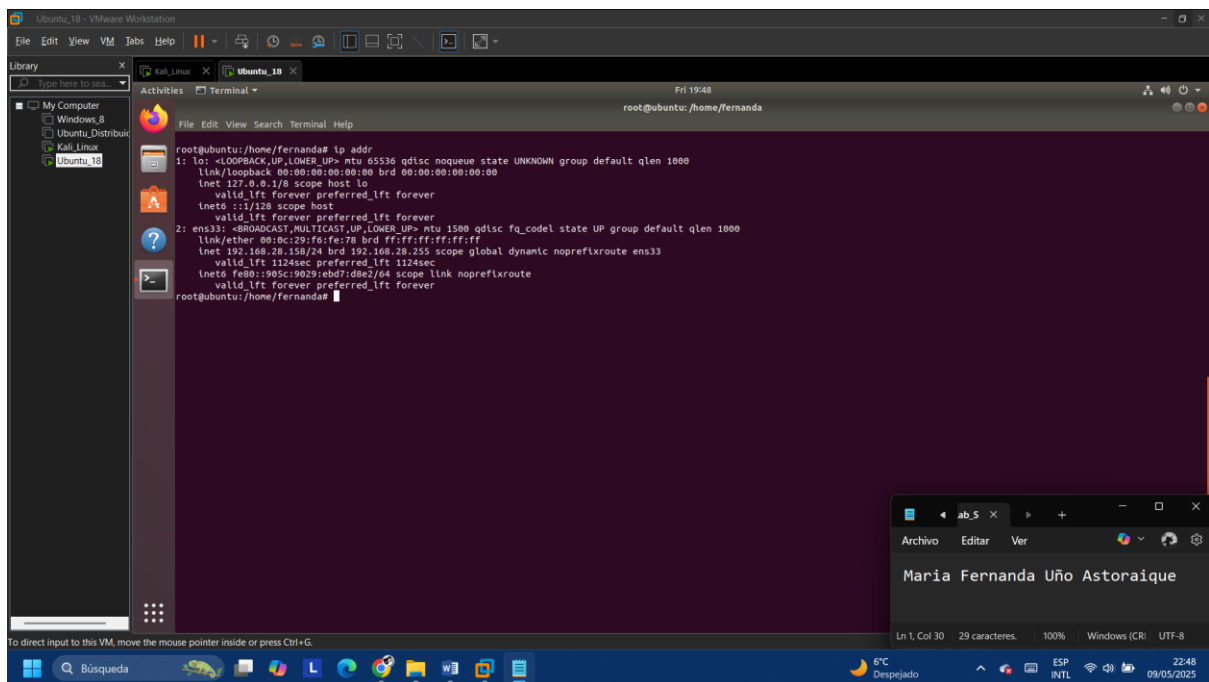
Estructura básica de una maquina regla :

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.

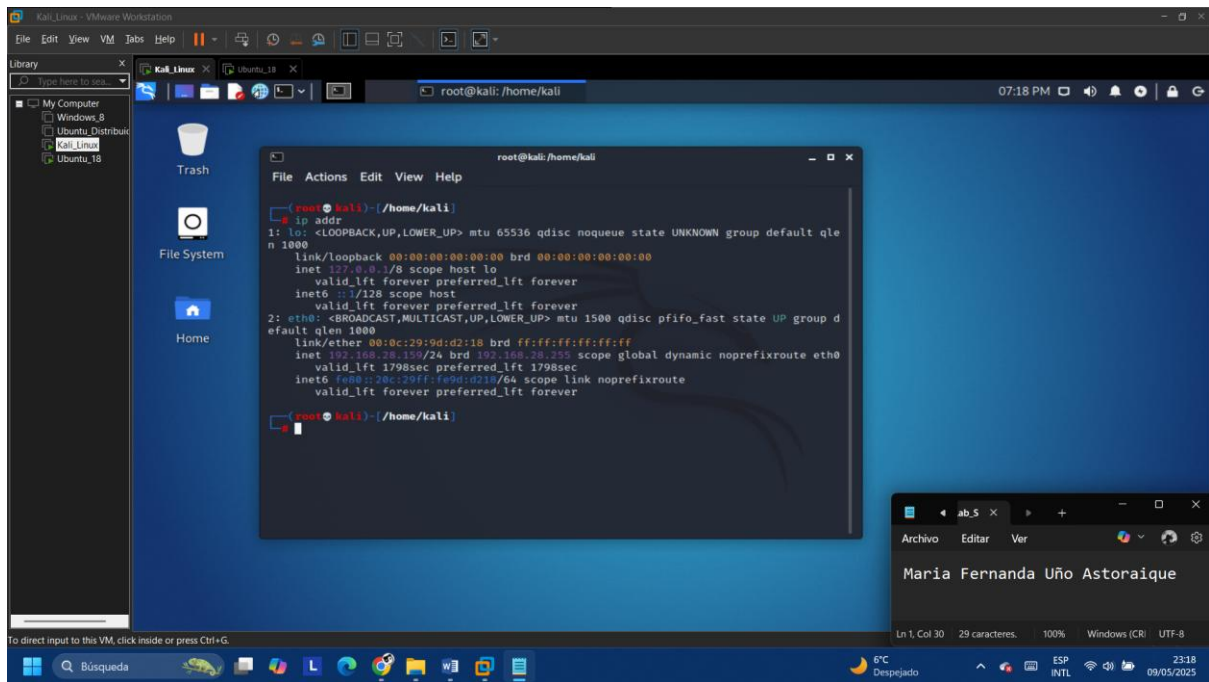
## Ubuntu



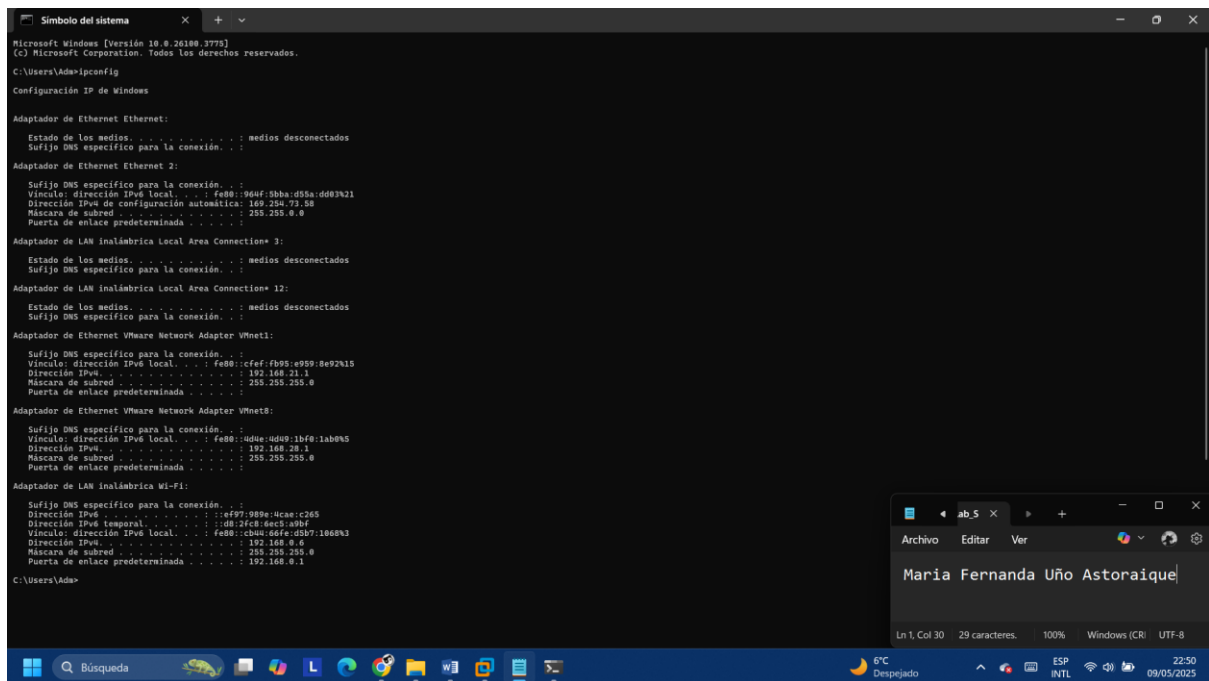
```

root@ubuntu:/home/fernanda# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 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 group default qlen 1000
    link/ether 00:0c:29:16:1f:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.28.158/24 brd 192.168.28.255 scope global dynamic noprefixroute ens33
        valid_lft 1124sec preferred_lft 1124sec
    inet6 fe80::985c:9029:161f:70e2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@ubuntu:/home/fernanda#
  
```

## Kali Linux



## Windows



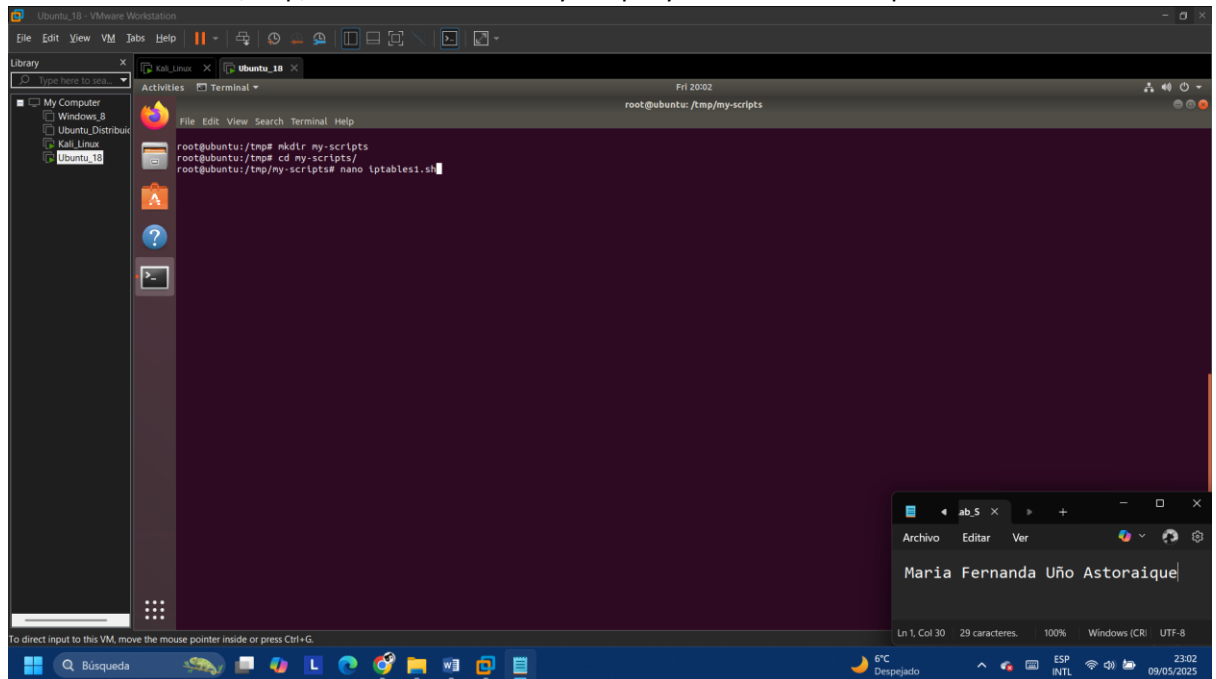
**Tabla:** Verifique que todas las máquinas se encuentren en el mismo segmento de red y tengan conectividad entre ellos. (ANOTE LAS IPs EN SU HOJA SEGÚN LA SIGUIENTE TABLA).

Máquina Virtual o Dispositivo	Dirección IP
Ubuntu	192.168.28.158
Kali Linux	192.168.28.159
Windows (Máquina física)	169.254.73.58

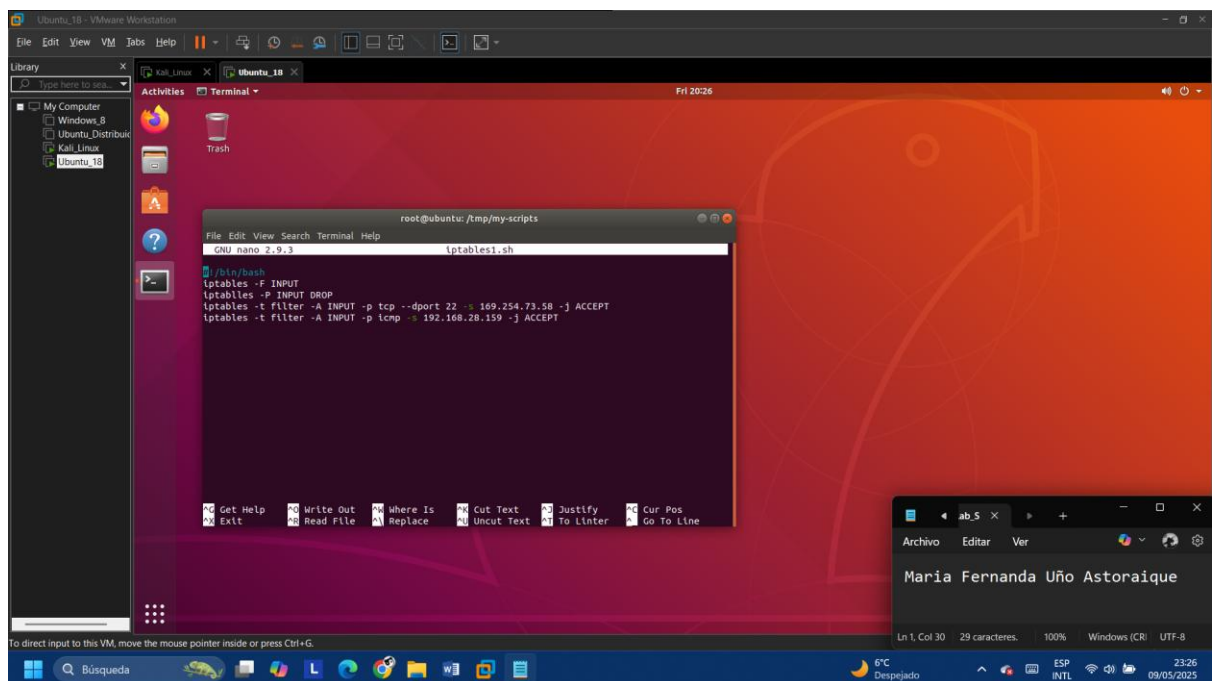
## Escenario 1: IPTABLES

Supongamos que la máquina host debe conectarse a la máquina Ubuntu por medio del protocolo ssh, y además la máquina kali debe tener únicamente conexión ICMP (ping) con la máquina Ubuntu, y todo el resto de tráfico que provenga de cualquier otro dispositivo debe ser descartado.

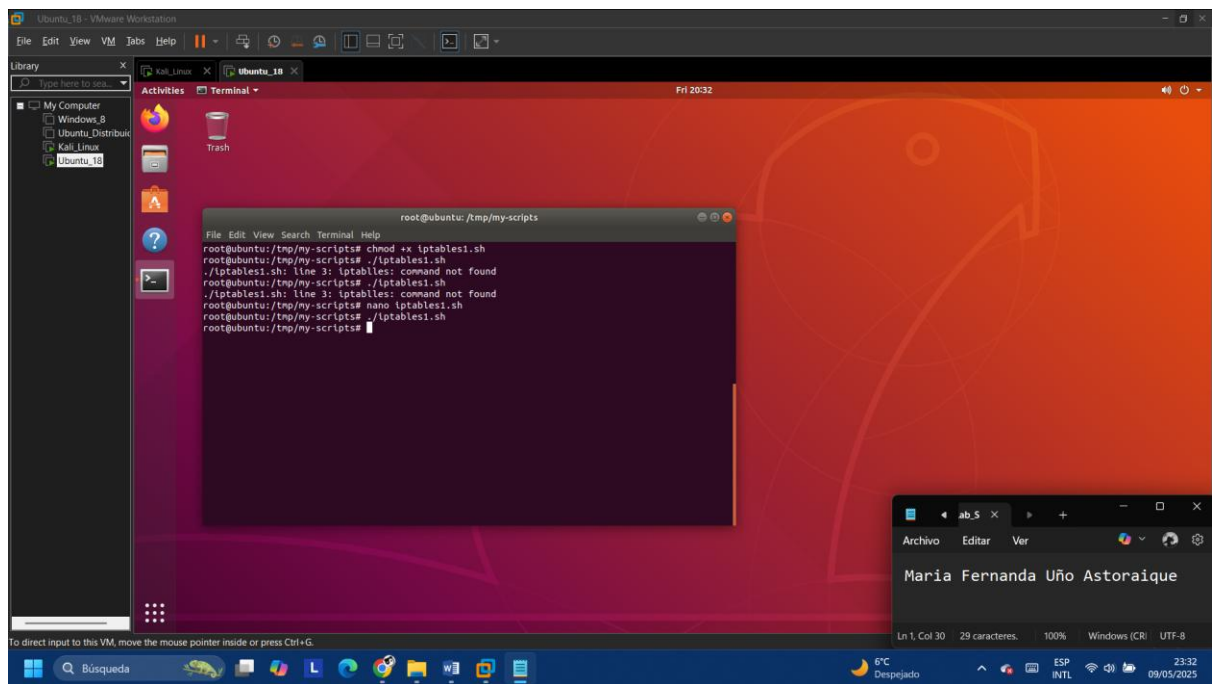
- 1) Acceder al sistema ubuntu con sus credenciales correspondientes, entrar a la terminal, entrar al directorio /tmp, crear el directorio my-scripts y crear un archivo iptables1.sh



- 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.

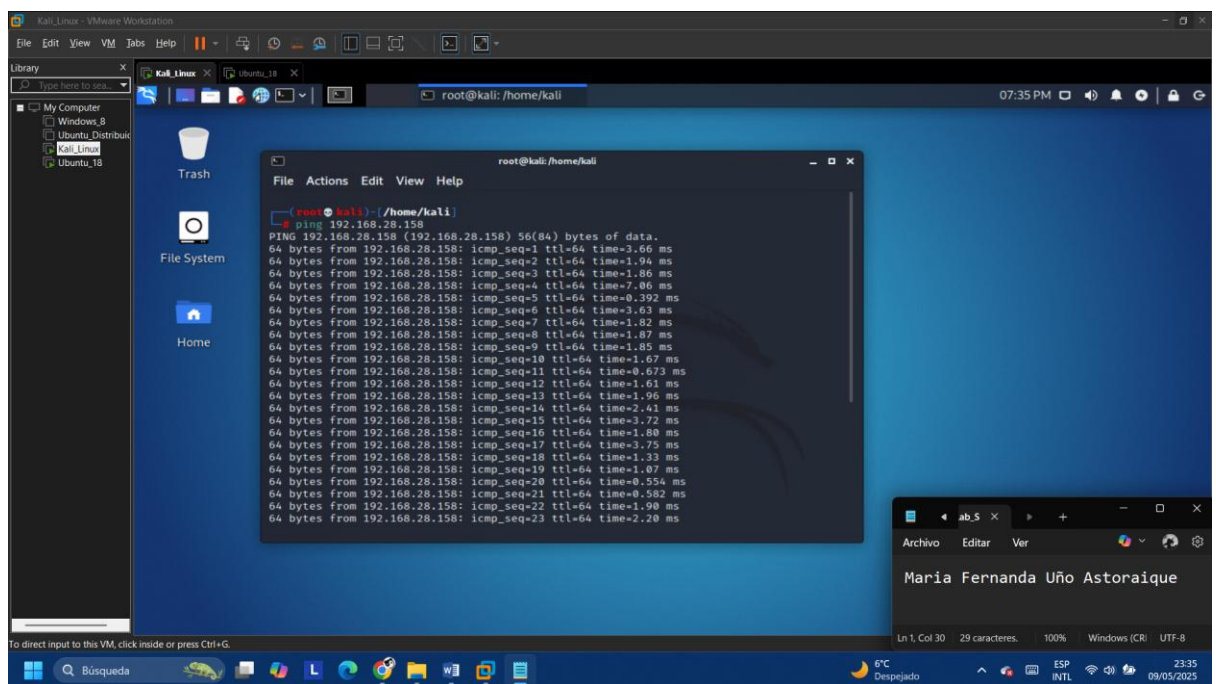


Guardar el archivo y darle permisos de ejecución y ejecutar el script.



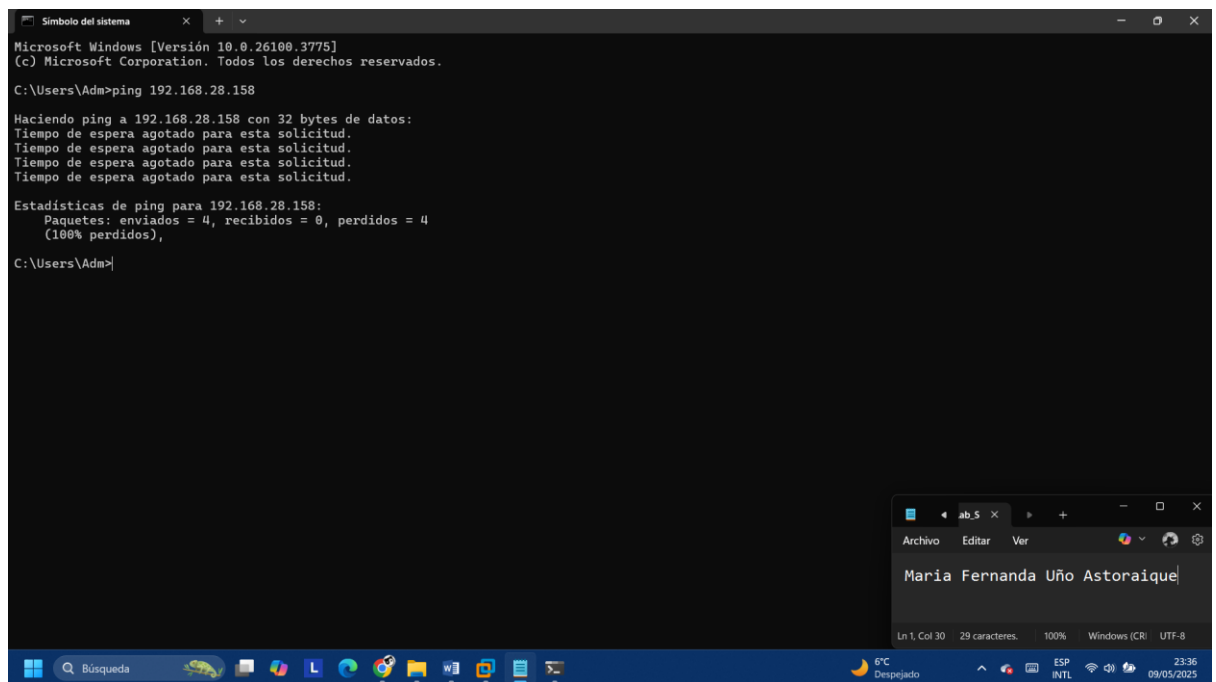
- 3) Entrar a la máquina kali y probar que existe tráfico icmp y ssh (colocar las credenciales del usuario) en el puerto 22 para el acceso a ubuntu.

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



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





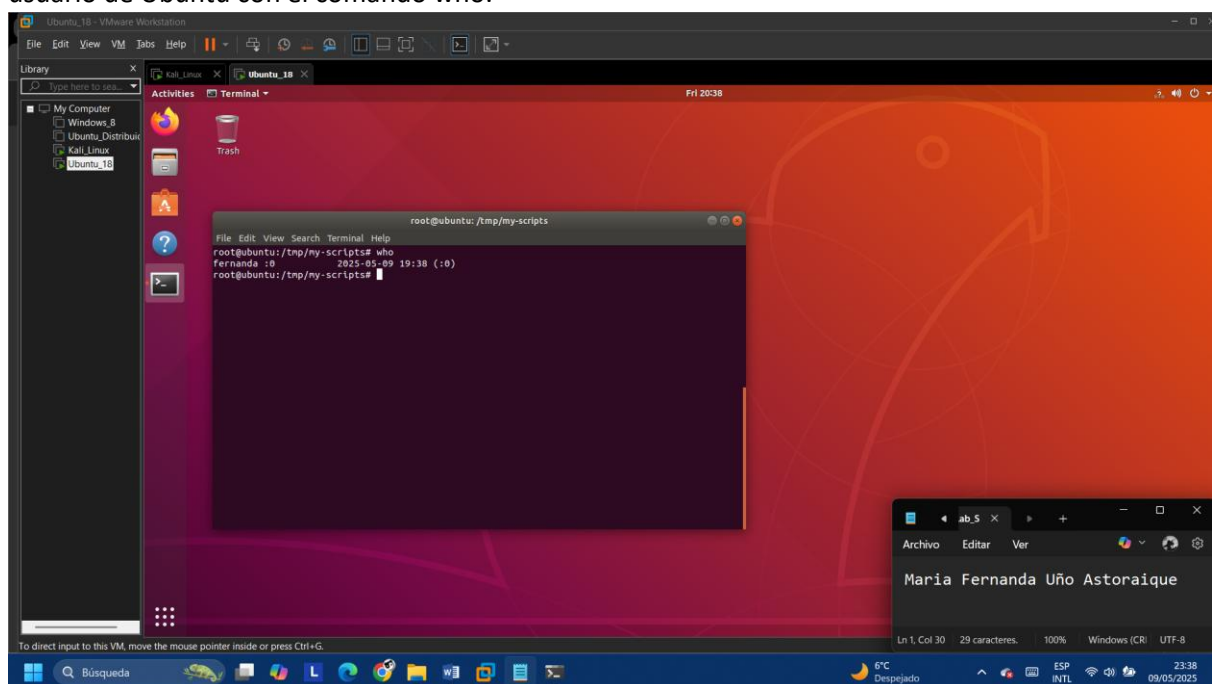
```
Símbolo del sistema
Microsoft Windows [Versión 10.0.26100.3775]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Adm>ping 192.168.28.158

Haciendo ping a 192.168.28.158 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.28.158:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos),
C:\Users\Adm>
```

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



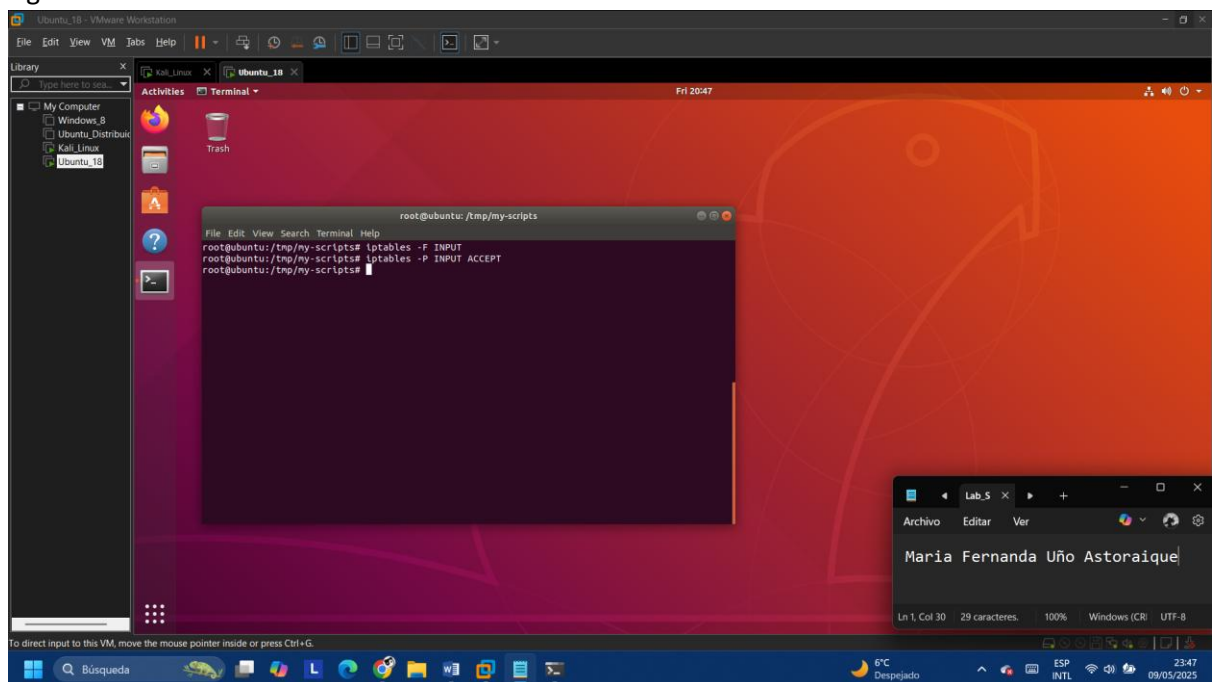
```
root@ubuntu: /tmp/my-scripts
root@ubuntu: /tmp/my-scripts# who
fernanda :0                2025-05-09 19:38 (:0)
root@ubuntu: /tmp/my-scripts#
```

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.

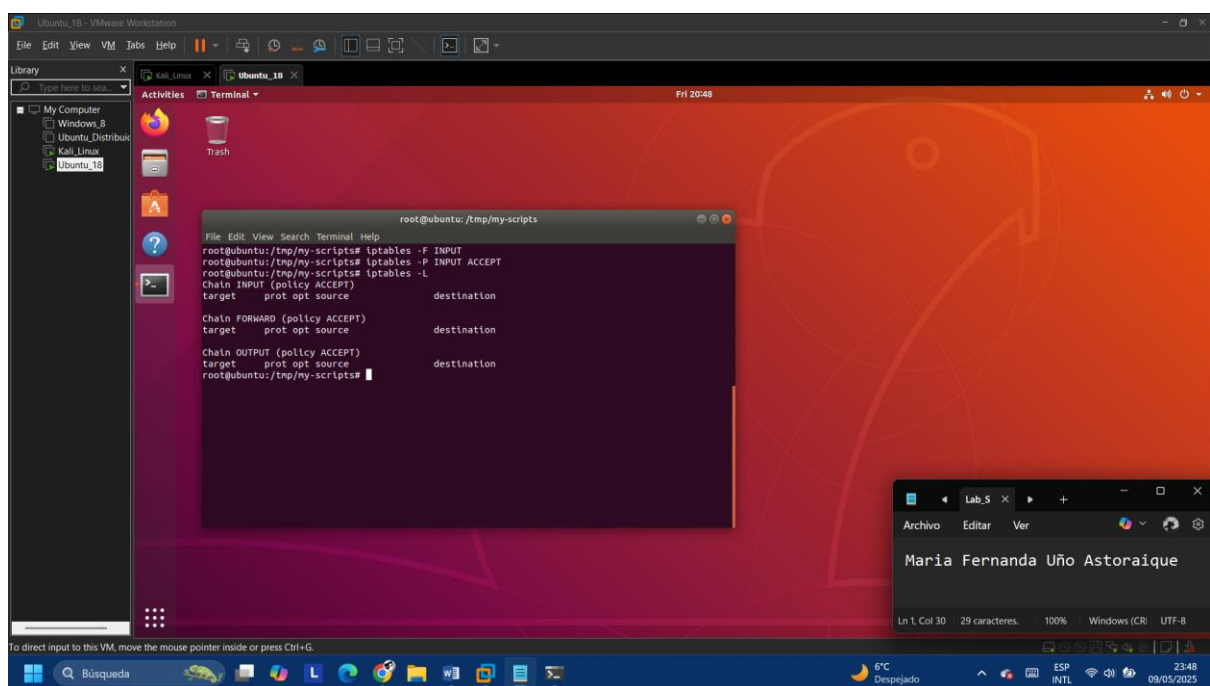


- 6) Eliminar estas reglas para que no choquen con las siguientes configuraciones, con los siguientes comandos:



Verificar las reglas configuradas, con el siguiente comando:

Debería tener el siguiente resultado:



## Escenario 2: NFTABLES

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 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 [ip_WINDOWS] tcp dport 22 accept`**

También permitimos el tráfico ICMP con:

**`nft add rule ip icmp_filter INPUT ip saddr [ip_KALI] 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 máquina 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

## 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 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
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. En otra ventana ingrese el comando **arp -a** para visualizarlo y replácelo 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)  
[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.

.....  
.....

**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.

- 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.

- 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:

```
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:

- 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.

#### **EVALUACIÓN**

- 1.Cuál es la diferencia entre saddr y daddr, saddr se ve en la configuración e indique sus usos.
2. ¿Qué implica la prioridad de una cadena en nftables y por qué es importante establecerla correctamente?
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