Universidad Autónoma del Estado de México

UAEM Zumpango

Ingeniería en Computación

Unidad de Aprendizaje:

Sistemas Operativos

Actividad:

IPTABLES

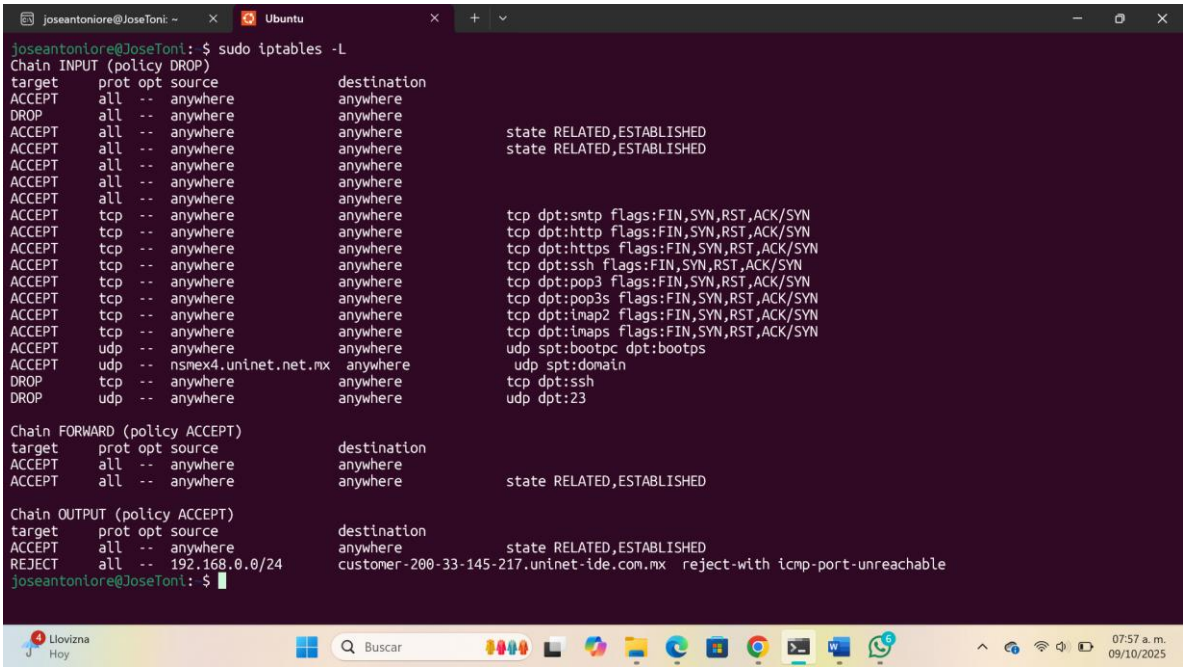
Alumno:

Rodríguez Estudillo Jose Antonio

Fecha:

09 Octubre de 2025

1. Muestres las reglas IPTABLES.



2. Cree dos reglas diferentes en IPTABLES.
   2.1. Describa que hace cada una de estas reglas.

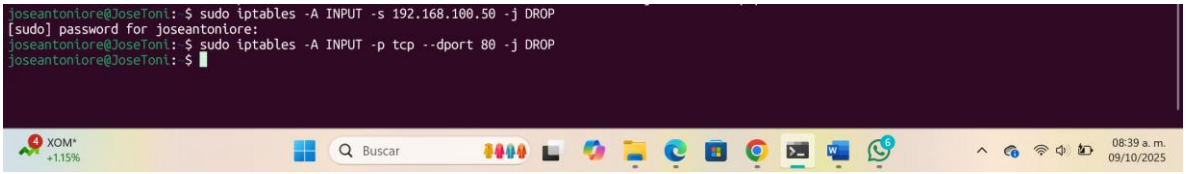
Regla 1: sudo iptables -A INPUT -s 192.168.100.50 -j DROP (Esta regla va a descartar silenciosamente todos los paquetes que vengan de la dirección IP 192.168.100.50).

-A INPUT: Añade (Append) la regla a la cadena INPUT. La cadena INPUT controla todo el tráfico que entra a tu máquina.
-s 192.168.100.50: Especifica el origen (source) del tráfico. En este caso, la IP que queremos bloquear.
-j DROP: Es la acción (jump) a realizar. DROP significa "descartar" el paquete. El remitente nunca recibe una respuesta, simplemente el paquete se pierde.

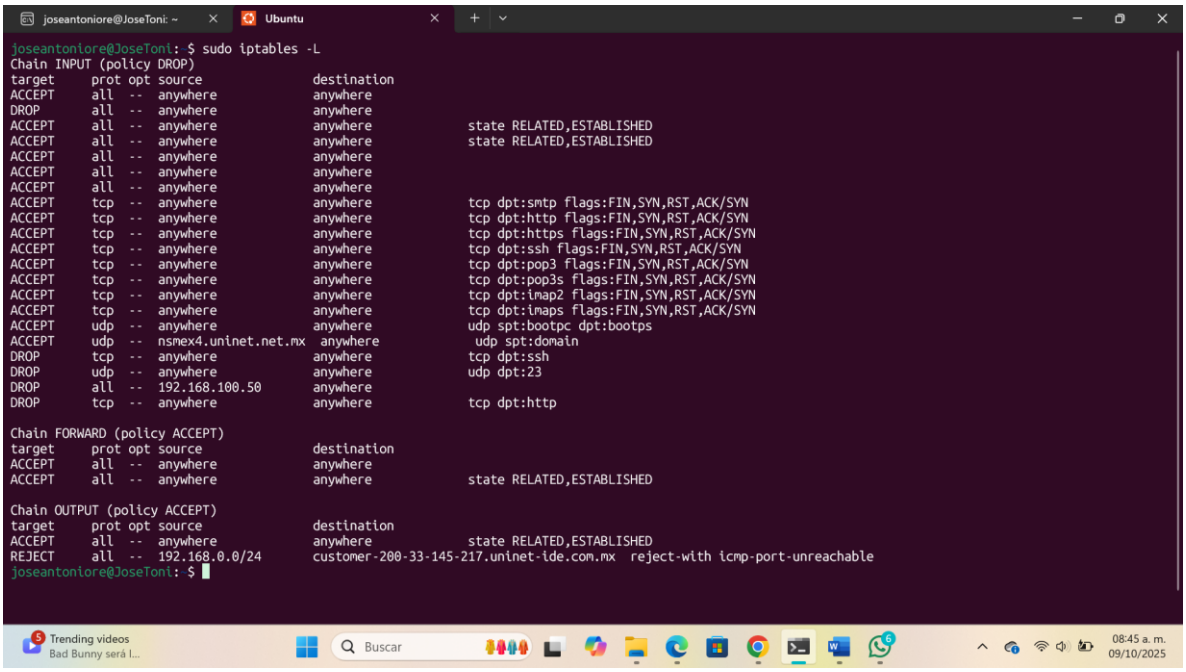
Regla 2: sudo iptables -A INPUT -p tcp --dport 80 -j DROP (Esta regla bloqueará todas las conexiones entrantes que intenten acceder al puerto 80, que es el puerto estándar para el tráfico web HTTP).

-A INPUT: De nuevo, añadimos la regla a la cadena de tráfico entrante.
-p tcp: Especifica el **protocolo** (protocol) que estamos filtrando, en este caso, TCP.
--dport 80: Especifica el **puerto de destino** (destination port) que es el 80 (HTTP).
-j DROP: La acción es descartar el paquete.

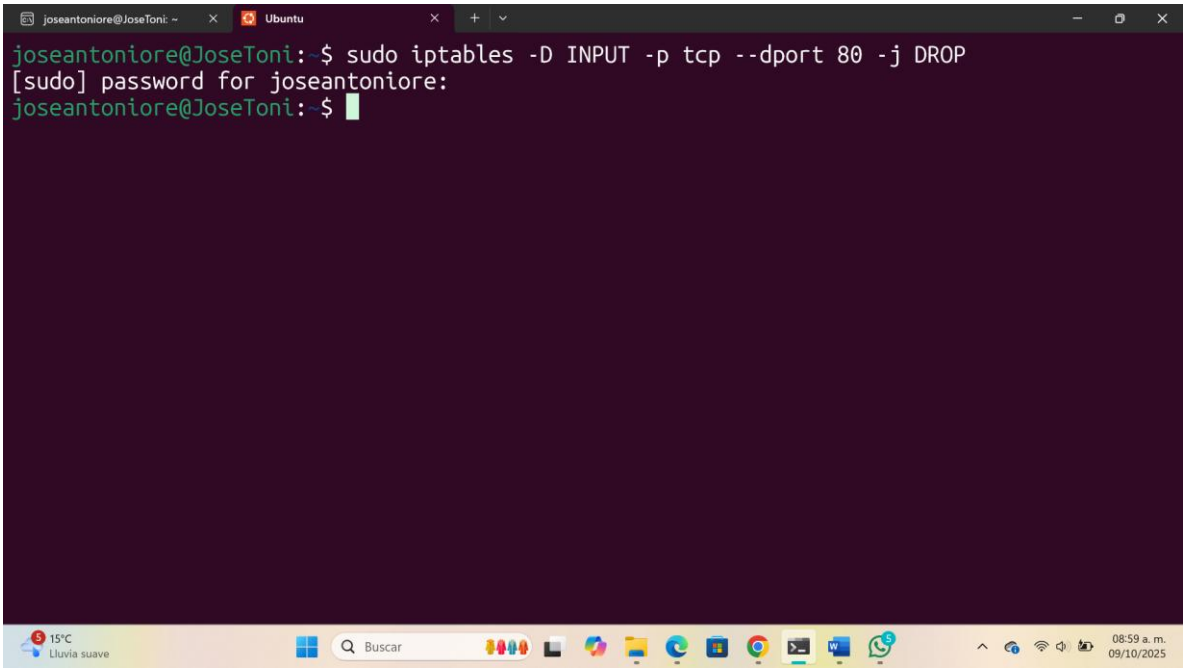
2.2. Acompañe con las captura de los comandos utilizados para crear las reglas.



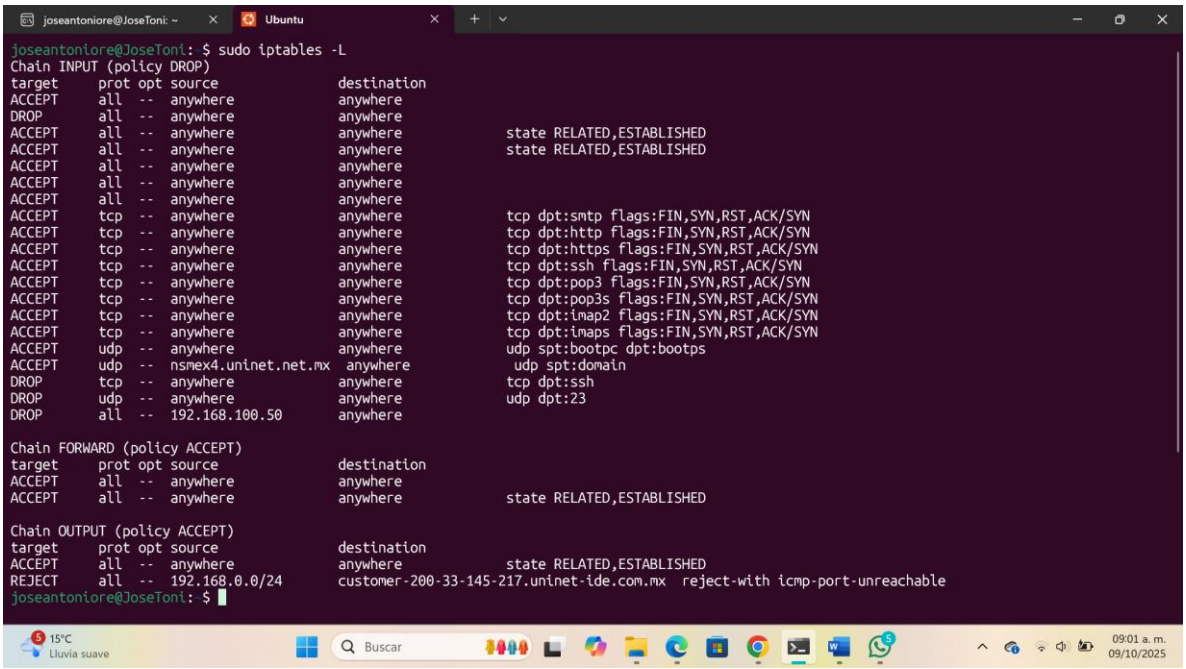
3. Muestre nuevamente las reglas de IPTABLES, donde identifique las nuevas reglas creadas anteriormente.



4. Elimine de las reglas creadas.



5. Muestre las reglas en IPTABLES



6. Describa que acciones hace ACCEPT, DROP Y RETURN, en IPTABLES

   ACCEPT (Aceptar): Esta acción le dice al firewall que deje pasar el paquete. Una vez que un paquete coincide con una regla que tiene la acción ACCEPT, el firewall deja de revisar más reglas en esa cadena y permite que el paquete continúe su camino hacia su destino (una aplicación, el sistema operativo, etc).

   DROP (Descartar): Esta acción le dice al firewall que descarte el paquete silenciosamente. El paquete simplemente se elimina, y no se envía ninguna notificación o mensaje de error al remitente. Desde el punto de vista del remitente, es como si el paquete se hubiera perdido en la red; su conexión simplemente esperará hasta que se agote el tiempo de espera (timeout). Es útil para hacer que tu sistema sea "invisible" a escaneos de red.

   RETURN (Regresar): Esta acción es un poco más avanzada. Significa "dejar de procesar las reglas en esta cadena y volver a la cadena anterior". Se usa principalmente cuando tienes cadenas personalizadas. Imagina que desde la cadena INPUT "saltas" a una cadena personalizada llamada REGLAS_WEB. Si un paquete dentro de REGLAS_WEB coincide con una regla RETURN, dejará de ser evaluado en REGLAS_WEB y volverá a la cadena INPUT justo en el punto donde se fue, para seguir siendo evaluado por las reglas restantes de INPUT. Si se usa en una cadena principal como INPUT, simplemente aplica la política por defecto de la cadena (por ejemplo, ACCEPT).