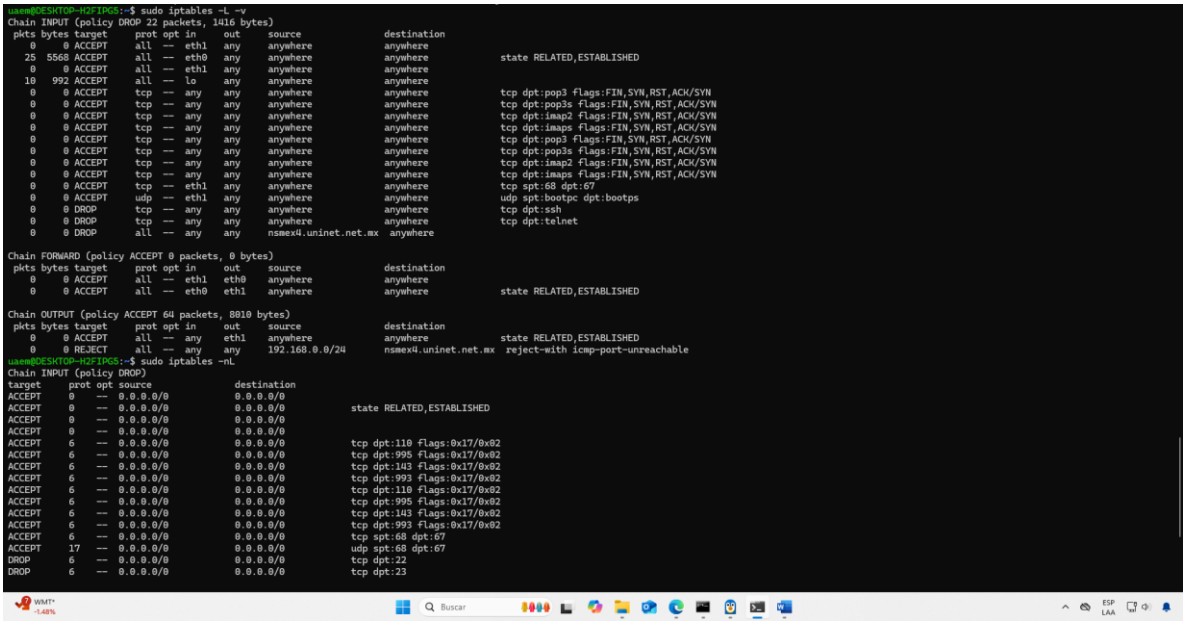
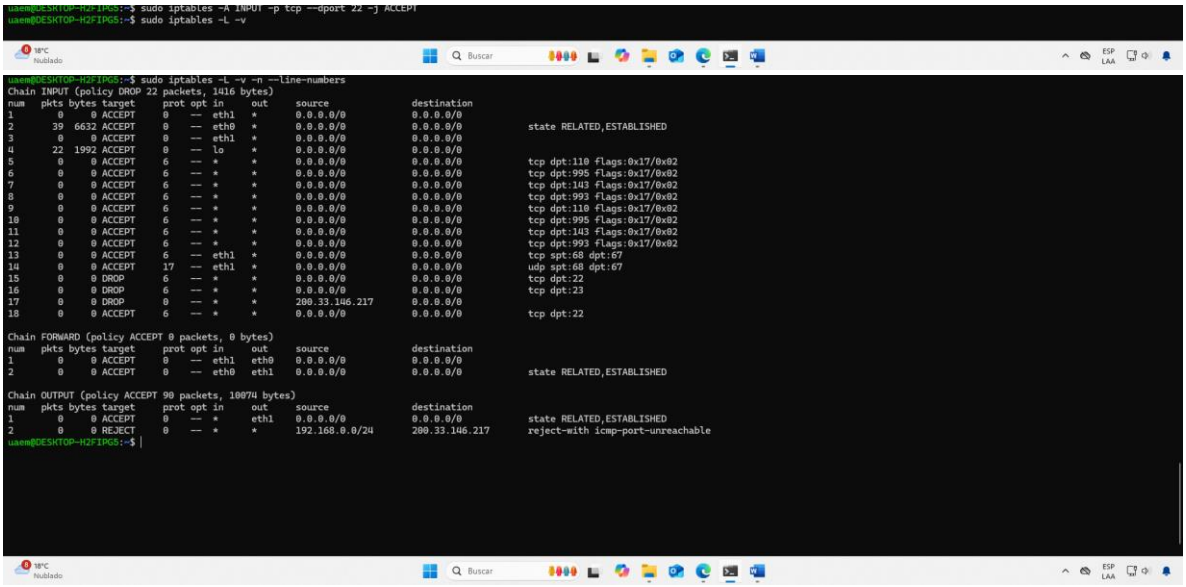
Alumno: Ariadna Abigail Alanis Estrada Sistemas operativos

1-Muestre las reglas IPTABLES en su equipo

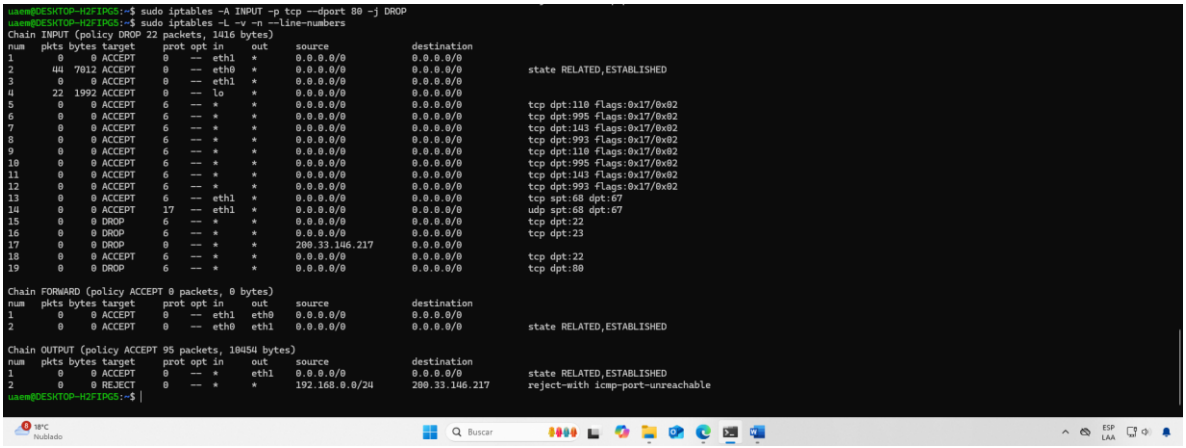


2-Cree dos reglas diferentes en IPTABLES, de las cuales

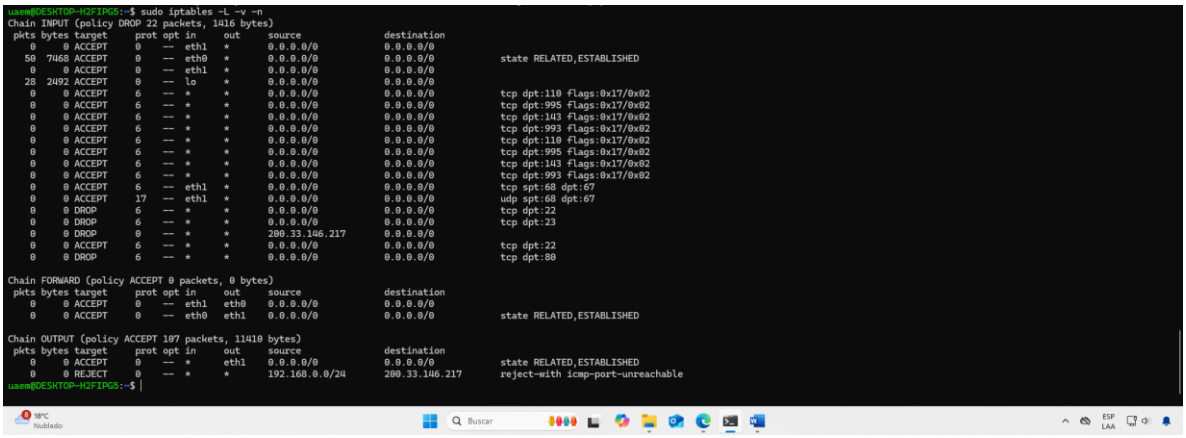
La primera permite las conexiones entrantes al puerto 22 esta permite el acceso remoto SSH al equipo.



La segunda bloquea todo el tráfico entrante al puerto 80, esta evita que el equipo reciba solicitudes HTTP.

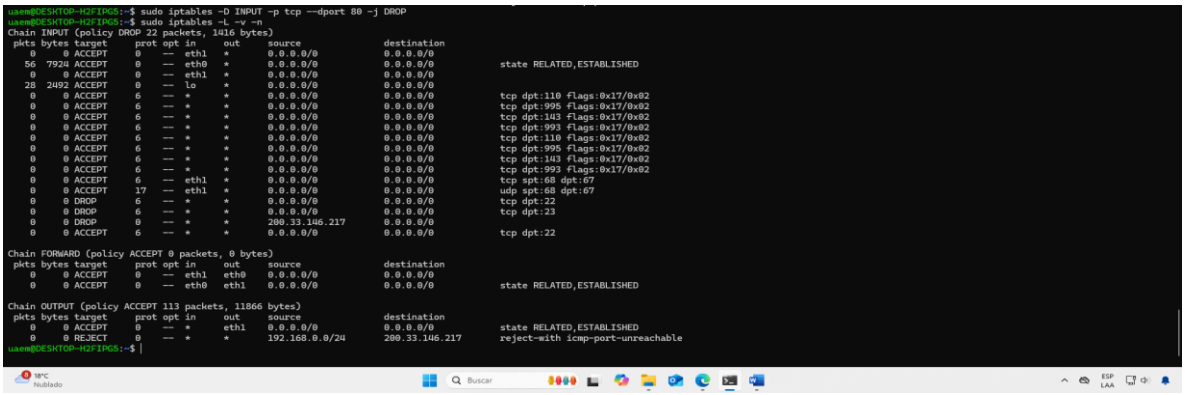


3-Muestre nuevamente las reglas en IPTABLES donde identifique las nuevas reglas creadas



4- Elimine una de las reglas creadas

5- Muestre las reglas en IPTABLES



6-Describa que acciones realiza ACCEPT, DROP Y RETURN, en IPTABLES

El ACCEPT nos permite el paso del paquete, cuando una regla tiene el ACCEPT, el paquete es aceptado y se detiene el procesamiento de reglas en esa cadena.
El DROP nos permite descartar el paquete sin enviar ninguna respuesta al emisor, el paquete simplemente se elimina, como si nunca hubiera existido.
El RETURN nos permite detener el procesamiento en la cadena actual y devuelve el control a la cadena que la llamó. Cuando se usa en una cadena personalizada RETURN hace que iptables salga de esa cadena y continúe evaluando reglas en la cadena anterior.