ACTIVIDAD 04-Mecanismos de defensa en red. Pablo de Jesús Salazar Hernández - 171580

Introducción

Con esta actividad veremos reglas de firewall que deberemos de aplicar para cumplir ciertas reglas que necesitamos por llevar cierta seguridad específica, es notable que muchas de ellas sean necesarias en la vida real para múltiples entradas o salidas de información

1. Establecer una política restrictiva.

   Iptable -p input drop

2. Permitir el tráfico de conexiones ya establecidas.

   Iptable -a INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT

3. Aceptar tráfico DNS (TCP) saliente de la red local.

   Iptable -a FOWARD -s 192.168.1.0/24 -p tcp –dport 53 -m state –state new -j accept

4. Aceptar correo entrante proveniente de Internet en el servidor de correo.

   Iptable -a foward -d 192.1.2.10 -p tcp –dport 25 -state –state new -j accept

5. Permitir correo saliente a Internet desde el servidor de correo.

   Iptable -a foward -s 192.1.2.10 -p tcp –dport 25 -state –state new -j accept

6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.

   Iptable -a foward -d 192.1.2.11 -p tcp –dport 80 -m state –state new -j accept

7. Permitir tráfico HTTP desde la red local a Internet.

   Iptable -a foward -s 192.1.2.0/24 -p tcp –dport 80 -m state –state new -j accept

Conclusión

Las reglas de firewall tienden a ser de importancia para poder manegar cierta entrada de datos al igual que la salida de los mismos y su origen o incluso su envío, es posible que sea más complejo de lo que parece pero suele ser de vital importancia para añadir esa capa de seguridad que se necesita en un servidor.