4-2-2026

Mecanismos de defensa en red

CNO V – Seguridad Informática

Elisa Alejandra Arellano Wratny
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

1. Establecer una política restrictiva.
   Iptables -P INPUT DROP && iptables -P OUTPUT DROP && iptables -P FORWARD DROP

2. Permitir el tráfico de conexiones ya establecidas.
   Iptables -A INPUT -m state –state ESTABLISHED, RELATED -j ACCEPT

3. Aceptar tráfico DNS (TCP) saliente de la red local.
   Iptables -A OUTPUT -p tcp –dport 53 -j ACCEPT

4. Aceptar correo entrante proveniente de Internet en el servidor de correo.
   Iptables -A INPUT -p tcp -d 192.1.2.10 -dport 25 -j ACCEPT

5. Permitir correo saliente a Internet desde el servidor de correo.
   Iptables -A OUTPUT -s tcp -d 192.1.2.10 -dport 25 -j ACCEPT

6. Aceptar conexiones HTTP desde Internet a nuestro servidor web.
   Iptables -A INPUT -p tcp -d 192.1.2.11 -dport 80 -j ACCEPT

7. Permitir tráfico HTTP desde la red local a Internet.
   Iptables -A INPUT -s tcp -d 192.1.2.0/24 -dport 80 -j ACCEPT