ACTIVIDAD 4

Mecanismos de defensa en red.

Alan Gilberto Sánchez Zavala

177263

Ciberseguridad

Actividad 4

1. Establecer una política restrictiva.

    Iptables -A INPUT -p tcp -m multiport - - dports 80,443 -j ACCEPT

2. Permitir el tráfico de conexiones ya establecidas.

    Iptables -A INPUT -p tcp -m state –state ESTABLESHED -j ACCEPT

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

    Iptables -A OUTPUT -p tcp -j ACCEPT

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

    Iptables -A INPUT -p tcp -d 192.1.2.10 -j ACCEPT

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

    Iptables -A OUTPUT -p tcp -s 192.1.2.10 -j ACCEPT

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

    Iptables -A INPUT -p tcp -s 192.1.2.11 - -dport 80 -j ACCEPT

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

    Iptables -A OUTPUT -p tcp - - dport 80 -j ACCCEPT