Interpretacion y traducción de politicas de filtrado en iptables

ACTIVIDAD 3

Francisco Javier Cruz Juarez
177622

Maestro: Servando López Contreras

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ — INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Act.03 - Interpretación y traducción de políticas de filtrado en iptables

– CNO V. Seguridad Informática

Nombre: Francisco Javier Cruz Juarez – 177622

Fecha: 03-02-2026 Calf: 9

1. *Completa los espacios conforme se explica el flujo del paquete.*

Cuando un paquete llega al sistema, primero pasa por una tabla, después por una Cadena y finalmente se ejecuta una acción / Regla.

2. *Relaciona cada tabla con su propósito principal.*

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de Paquetes	Permitir/bloquear el trafico
NAT	traduccion de direcciones	hacer NAT o Port forwarding
MANGLE	modificacion avanzada de Paquetes	Cambiar cabeceras
RAW	excepciones al seguimiento de conexiones	Paquete que no deben inspeccionarse
SECURITY	aplicar etiquetas de seguridad	Contexto de seguridad

3. *Anatomía de un comando iptables:*

iptables -A INPUT -p tcp -m multiport --dports 80,443 -j accept

4. *Este comando permite:* el trafico de entrada (INPUT) que utiliza el Protocolo TCP con direccion a los Puertos de destino (--dport) 80 (HTTP) y 443 (HTTPS)

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit 1/minute

b) Filtrar por IP de origen

-S ó' --source / -s 192.168.0.1/24

c) Ver solo números, sin DNS (ni resolución de puertos)

-L -n

d) Ver reglas con contadores (paquetes y bytes)

-L -V

6. *¿Que hace esta regla?*

**iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 **
-m state --state NEW,ESTABLISHED -j ACCEPT

Permite el trafico TCP de entrada por la interfaz eth0 hacia los Puertos 22, 80 (HTTP) y 443 (HTTPS), esto siempre que sea Parte de una conexion nueva o establecida.

7. *Permitir tráfico HTTP entrante*

IPtable -A INPUT -p tcp --dport 80 -j ACCEPT

8. *Permitir todo el tráfico saliente*

IPtable -A OUTPUT -j ACCEPT

9. *Permitir SSH solo desde la IP 192.168.1.50*

IPtables -A INPUT -p tcp -s 192.168.1.50 --dport 22 -j ACCEPT

10. *Permitir tráfico TCP entrante a puertos 80 y 443 solo si es conexión establecida o relacionada*

IPtable -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack -state ESTABLISHED RELATED → ACCEPT

11. *Permitir tráfico TCP entrante por eth0 a 22, 80 y 443, registrar intentos y permitir solo NEW y ESTABLISHED*

IPtable -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m conntract --ctstate NEW, ESTABLISHED -J ACCEPT