UNIVERSIDAD POLITECNICA 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: Jose Armando Pglomo Ceda

Fecha: 03/02/2024 Calf: _____

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 regla o acción

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	filtrado de paquetes	permitir o bloquear tráfico
NAT	traducción de direcciones	Hace NAT o port forwarding
MANGLE	Modificación avanzada de P	Cambiar cabeceras
RAW	excepciones al segu. de conex	Paquetes que no deben ser inspeccionados
SECURITY	aplican etiquetas de seguridad SELi	Contextos de seguridad adicionales

3. *Anatomía de un comando iptables:*

iptables -A Input -p tcp -m multiport --dports 80,443 -j Accept

4. *Este comando permite:* Activa un modulo de coincidencia adicional (en este caso, multiport) hace que permita usar múltiples puertos en una sola regla

5. *Variables y opciones communes*

a) Limitar intentos por minuto

— limit :--limit 5/minute

b) Filtrar por IP de origen

-S 0--Source ejemplo = -S 192.168.1.0/24

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

iptables -L -n

d) Ver reglas con contadores (paquetes y bytes)

iptables -L -V -n --line-numbers

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 ante TCP entrante por la interfaz eth0 a los puertos 22, 80, y 443, siempre que sea parte de una conexión nueva o establecida

7. *Permitir tráfico HTTP entrante*

iptables -A Input -p tcp -- dport -j accept

8. *Permitir todo el tráfico saliente*

iptables -P output accept

9. *Permitir SSH solo desde la IP 192.168.1.50*

Iptables -A Input -p tcp -s 192.168.1.50

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

Iptables -A Input -p tcp -m multiport -- dports 80,443 -m state -- state ESTABLISHED,RELATED -j ACCEPT

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

1: Iptables -A Input -i eth0 -p tcp -m multiport -- dports 22,80, 443 -j LOG -- log-prefix "Intento - entrada:"

2: Iptables -A INPUT -i eth0 -p tcp -m multiport -- dports 22,80, 443 -m state -- state NEW, ESTABLISHED -j ACCEPT