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

– CNO V. Seguridad Informática

Nombre: Mayeli Sánchez Ramírez / 173030

Fecha: 03/02/2026 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 accion / regla.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	filtrado de paquetes; Nos permite o bloquea el tráfico	Bloquear conexiones
NAT	Traducción de direcciones IP	Port forwarding: los paquetes se enrutan con el puerto de servicio
MANGLE	Modificación avanzada de paquetes	cambiar cabeceras. TCP
RAW	Excepciones al seguimiento de conexiones.	Selecaon de paquetes
SECURITY	Analiza propósito o servicio	se aplica contexto de seguridad

Manejo de Paquetes Para auditorias o calidad de servicio

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*
Definir la tabla, cadena, el protocolo, multiport es para más de un puerto, Estado del puerto, en este caso ACCEPT.

80 = http
443 = https
22 = ssh

5. *Variables y opciones communes*

a) Limitar intentos por minuto
-- limit 5/minute

b) Filtrar por IP de origen
-- source o -s
-s 192.168.25.0/24

c) Ver solo números, sin DNS (ni resolución de puertos)
-list -n ó -l -n
↳ listar → numeros.

d) Ver reglas con contadores (paquetes y bytes)
-v contadores
-n numeros

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 tráfico TCP entrante por la interfaz eth0 a los puertos 22, 80, 443, siempre que sea parte de una conexion nueva o establecida.

7. *Permitir tráfico HTTP entrante*

iPtables -A INPUT -p tcp --dports 80 -j ACCEPT
(Filter, cadena, Rule)

8. *Permitir todo el tráfico saliente*

iPtables -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 --d ports 22 -j ACCEPT

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

iPtables -A INPUT -p tcp -m multiport --d ports 80,443 -m state --state ENTABLISHED, RELATED -j ACCEPT

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

iPtables -A INPUT -p tcp -i eth0 -m multiport --d ports 80,22,443 - m state NEW ENTABLISHED -j ACCEPT

9. iPtables -A OUTPUT -p tcp -s 192.168.1.50 - - d ports 22 -j REJECT

10. iptables -A INPUT -i eth0 -p tcp -m multiport - - d ports 80,443 -m state - - state ESTABLISHED, RELATED -j ACCEPT

11. iptables -A ~~INPUT~~ INPUT -i eth0 -p tcp -m multiport -- dports 22,80,443 -m conntrack -- ct state NEW, ESTABLISHED -j LOG -- log- prefix "Conexion nueva:" -j ACCEPT