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

– CNO V. Seguridad Informática

Nombre: Mauricio Josafat Solinos Carrillo 177406

Fecha: 03 de Febrero de 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 regla o acción

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Permitir o bloquear paquetes	Filtrar el trafico en la red
NAT	Traducir direcciones IP	Distribuir el internet como proveedor de servicios
MANGLE	Modificacion de paquetes	cambiar encabezados de paquetes
RAW	Seguimiento de paquetes	saber si la información llega al destino
SECURITY	Aplicar seguridad	Añadir seguridad de paquetes permitidos

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

Filtrar todo lo que llegue de entrada por protocolo TCP de los puertos 80 y 443 y los ka a aceptar

5. *Variables y opciones commúnes*

a) Limitar intentos por minuto

--limit 5/minute

b) Filtrar por IP de origen

-s 192.168.25.0/24

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

-list -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 trafico TCP entrante por la interfaz eth0 a los puertos ssh,http,https, siempre que sea parte de una conexion nueva o establecida

7. *Permitir tráfico HTTP entrante*

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

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 --dport 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 --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 multiport --dports 22,80,443 -j LOG --log-prefix "Intento Acceso"

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

Ejemplos clase:

* iptables -A INPUT -p tcp -m multiport --dports 56,90 -j ACCEPT
* iptables -A OUTPUT -p tcp -s 192.168.1.30 --dport 22 -j REJECT