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

– CNO V. Seguridad Informática

Nombre: Diego López Castro

Fecha: 03 de febrero de 2026 Calf: 10

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/acción.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrar tráfico de paquetes	Bloquear el tráfico de paquetes
NAT	Traducción de direcciones	Compartir el internet
MANGLE	Modificación avanzada de paquetes	Cambiar las cabeceras
RAW	Excepción de seguimiento	Paquetes no inspeccionados
SECURITY	Aplicación de políticas de seguridad	Colocar seguridad adicional

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

El comando permite el tráfico tipo tcp a los puertos 80 y 440

5. *Variables y opciones communes*

a) Limitar intentos por minuto

iptables --limit 1/minute

b) Filtrar por IP de origen

iptables -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

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

Esta regla permite que el tráfico de tipo TCP que pasa por la interfaz "eth0" al puerto 22 y a los puertos de navegación web 80 y 443, mientras cumpla la condición de que esté establecida y sea nueva

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 --dport 22 -s 192.168.1.50 -j ACCEPT
```

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

```
ip tables -A INPUT -p tcp -m multiport --dports 80,443 -m
  state --state ESTABLISHED RELATED
```

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

```
iptables -A INPUT -i eth0 -p tcp -m multiport --dports
  22,80,443 -m state --state NEW -j LOG
  --log-prefix "intento"

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