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

– CNO V. Seguridad Informática

Nombre: David Beltrán Reyna - 183636

Fecha: a 3 de febrero de 2026 Calf: A

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	Filtrar paquetes	Bloquear conexiones peligrosas
NAT	Traducir las direcciones	NAT estático en servidores
MANGLE	Modificar paquetes (TTL, etc)	Marca y priorizar el DNS para juegos online
RAW	Son las excepciones a las conexiones	Usar notrack para liberar recursos
SECURITY	Etiquetas de seguridad, como SELinux	Denegar el paso de paquetes de acuerdo a las etiquetas

3. *Anatomía de un comando iptables:*

iptables -A INPUT (OUTPUT ...) -p tcp (protocolo) -m multiport (englobar) --dports 80,443 (filtro) -j ACCEPT (DROP, REJECT ...)

4. *Este comando permite:*

Definir tanto la tabla, cadena y la acción/regla para realizar acciones del iptable. En este caso filtra puertos para el protocolo http/https.

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit, ejemplo: --limit 5/minute

b) Filtrar por IP de origen

-s o --source, ejemplo: -s 192.168.25.0/24

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

-list -n, ejemplo: -list 443

d) Ver reglas con contadores (paquetes y bytes)

-L -v, ejemplo: -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

Se crea la regla para la tabla FILTER, se define el paquete que pasará por eth0, se define el tipo de protocolo (TCP), se especifican los puertos 22 (ssh), 80 (http), 443 (https), se define el estado de conexión de forma nueva y estable, finalmente se aceptan los paquetes en la interfaz.

7. *Permitir tráfico HTTP entrante*

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

usa http · puerto destino · permitir

8. *Permitir todo el tráfico saliente*

```
iptables -P OUTPUT ACCEPT   | iptables -A OUTPUT -j ACCEPT
```

política p.der. · exterior

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
```

filtrar la dirección IP de origen · puerto estándar del SSH

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
```

múltiples puertos en una regla · paquetes ya aceptados o asociados

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 -m state --state
NEW,ESTABLISHED -j LOG --log-prefix 2.
```

rastro de auditoría · "Texto:" · ... (se pone lo mismo pero cambia :) `-j ACCEPT`

- `-i eth0` : restringir a la interfaz de red física

7.1 `iptables -A INPUT -p tcp -m multiport --dports 56,80 -j ACCEPT`