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

– CNO V. Seguridad Informática

Nombre: Alan Gilberto Sanchez Zavala 177263

Fecha: 9/2/26 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 / Accion

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Bloquear tráfico
NAT	Traducción de direcciones	Poder utilizar una IP pública
MANGLE	Modificación avanzada de paquetes	Poder modificar la calidad del servicio
RAW	Excepciones al seguimiento con.	Revisar que esta haciendo el paquete
SECURITY	Aplicar etiquetas de seguridad SELinux	Para validar si esta autorizado un proceso

3. *Anatomía de un comando iptables:*

iptables -A CADENA -p tcp -m Match module --dports 80,443 -j Accion

4. *Este comando permite:*

Trafico del puerto HTTP y HTTPS

5. *Variables y opciones communes*

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)

-l -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 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 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 conntrack --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*

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT