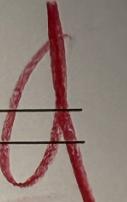


Act.03 - Interpretación y traducción de políticas de filtrado en iptables

- CNO V. Seguridad Informática

Nombre: Jorge Alejandro Cabeza Maza - 181591
 Fecha: 03/08/26

Calf: 

- Completa los espacios conforme se explica el flujo del paquete.

Cuando un paquete llega al sistema, primero pasa por una ~~table~~ y finalmente se ejecuta una ~~cadena~~ ~~anterior~~ ~~siguiente~~

- Relaciona cada tabla con su propósito principal.

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	filtrado de paquetes	Administrar que paquetes enviar
NAT	traducción de direcciones	Envío de paquetes en la red
MANGLE	modificación avanzada	Poner cabeceras
RAW	excepciones al seguimiento	paso libre de paquetes
SECURITY	aplicar etiquetas de seguridad	dar acceso al servicio

- Anatomía de un comando iptables:

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

- Este comando permite:

En el puerto 80,443, tabla INPUT se agregó la regla que acepta los paquetes mediante TCP

5. Variables y opciones comunes

a) Limitar intentos por minuto

--limit 5/minuto

b) Filtrar por IP de origen

-s / --source 192.168.1.0/24

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

-L -n

d) Ver reglas con contadores (paquetes y bytes)

L-V

- ¿Qué hace esta regla?

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

Permite el tráfico TCP entrante por la interfaz eth0, en el puerto 22,80 y 443, solo si es una conexión nueva o ya establecida

7. Permitir tráfico HTTP entrante

Iptables -A INPUT -P tcp --dport 80 -m state New -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 -m state NEW, ESTABLISHED

Iptables -A INPUT -P tcp -m multiport --dports 80, 443 -j ACCEPT

Iptables -A INPUT -P tcp -m state --state RELATED,ESTABLISHED -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 -m multiport --dports 22,80,443 -m state --state NEW -j LOG --log-prefix