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

– CNO V. Seguridad Informática

Nombre: Aenar Cuevas Luis Eduardo 179880

Fecha: 3/2/2026 Calf: _____

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.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de paquetes	Bloquear una conexion
NAT	Traduccion de direcciones	Acceso al servicio por medio de puertos
MANGLE	Modificacion avanzada de flags	Medir calidad de servicio
RAW	Excepciones al seguimiento de conx.	Verificar los paquetes de inicio
SECURITY	Aplicar etiquetas de seguridad	Analizar el servicio HTTP

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:*

Tabla filter: Recibir Paquetes directos al host y aceptarlos a los puertos de destino 80 y

5. *Variables y opciones communes*

a) Limitar intentos por minuto

--limit 5/minute

b) Filtrar por IP de origen

-s 192.168.1.0/24

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

-list -n

d) Ver reglas con contadores (paquetes y bytes)

-list -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

Creamos una regla para la tabla filter, la cual se añade al final, con el paquete destinado host recibido interfaz eth0, por el protocolo tcp en los puertos 22, 80, y 443, el estado de conexion como nueva y establecida y aceptará todos los paquetes por puertos el puerto 22 es de SSH, 80 de HTTP, y 443 de HTTPS

7. *Permitir tráfico HTTP entrante*

iptable -A INPUT --dport 80 -j ACCEPT

8. *Permitir todo el tráfico saliente*

iptable -A OUTPUT -j ACCEPT

9. *Permitir SSH solo desde la IP 192.168.1.50*

iptable -A INPUT -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*

iptable -A INPUT -p tcp -m multiports --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*

iptable -A INPUT -i eth0 -p tcp -m multiports --dports 22,80,443 -m conntrack --state NEW, ESTABLISHED -j LOG --log-prefix "INTENTO" -- ACCEPT