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

– CNO V. Seguridad Informática

Nombre: Coronado Noriega Jesús Olaf

Fecha: 03/02/2026 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 accion.

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Filtrado de Paquetes	Bloqueo un puerto
NAT	traduccion de direcciones	Redireccion de Puertos
MANGLE	Alteracion de campos	Cambiar TTL o TOS
RAW	Configurar exepciones	Eximir del siguimiento
SECURITY	Marcar Paquetes SELinux	Etiquetas de seguridad

3. *Anatomía de un comando iptables:*

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

4. *Este comando permite:* Permite la entrada de trafico a traves del protocolo TCP hacia los puertos 80 y 443

5. *Variables y opciones communes*

a) Limitar intentos por minuto: --limit 5/minute

b) Filtrar por IP de origen: -s o -source

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

Añade una regla a la cadena de entrada INPUT para la red eth0 Permite protocolos tcp dirigidos a los puertos 22 (SSH), 80 y 443. Cuando el estado sea nuevo o ya establecido y la accion final es Aceptar (ACCEPT) de los paquetes

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 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*

IPtables -A INPUT -i eth0 -P tcP -m multiPort --dPorts 22,80,443 -m state NEW,ESTABLISHED -J ACCEPT