REPORTE FORENSE DE CIBERSEGURIDAD

LOG-03: INTERPRETACION DE REGLAS IPTABLES

INFORMACION DEL AGENTE

ESTUDIANTE: Moreno Solis Gisela Geraldine

DOCENTE: Mtro. Servando Lopez Contreras

FECHA: 2026-02-20

1. IDENTIFICADOR: NETFILTER & IPTABLES

Iptables es la herramienta de espacio de usuario utilizada para configurar las tablas de filtrado de paquetes del kernel de Linux (Netfilter). Es la primera linea de defensa en servidores Linux.

CONCEPTOS FUNDAMENTALES (TABLAS)

TABLA	PROPOSITO	EJEMPLO
FILTER	Filtrado de paquetes.	Permitir / Bloquear trafico.
NAT	Traduccion de direcciones.	Uso de diferentes dispositivos.
MANGLE	Modificacion avanzada.	Cambio de cabeceras.
RAW	Excepciones al seguimiento.	Acceso sin inspeccion.
SECURITY	Aplica paquetes de seguridad.	Seguridad avanzada.

2. ANATOMIA TECNICA DE UN COMANDO

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

-A INPUT: Añadir regla | -p tcp: Protocolo | --dports 80,443: Puertos Destino | -j ACCEPT: Permitir

3. ANALISIS DE POLITICAS (EJERCICIOS)

Acceso Seguro via SSH

Req: Permitir conexion SSH desde 192.168.1.50.
Cmd: iptables -A INPUT -p tcp -s 192.168.1.50 --dport 22 -j ACCEPT

Hardening Web

Req: Abrir puertos 80 y 443 para trafico publico.
Cmd: iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT

Control de Estados

Req: Permitir trafico ESTABLISHED/RELATED.
Cmd: iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Politica Drop

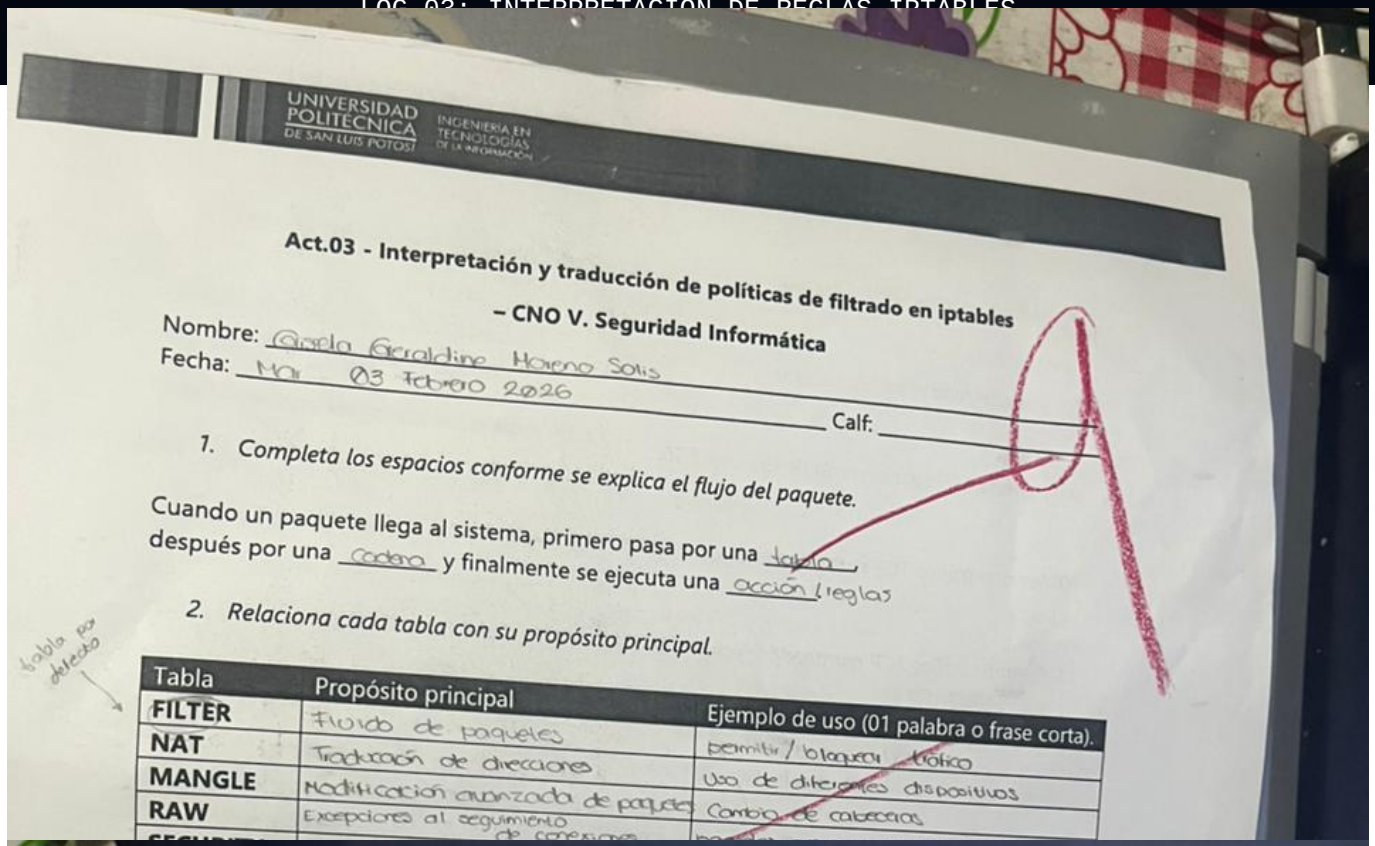
Req: Postura Deny by Default.
Cmd: iptables -P INPUT DROP

4. CONCLUSION

El estandar X.800 y el RFC 4949 se complementan para definir la arquitectura de seguridad.

REPORTE FORENSE DE CIBERSEGURIDAD

LOG 03: INTERPRETACION DE REGLAS IPTABLES



UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ — INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

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

– CNO V. Seguridad Informática

Nombre: Gisela Geraldine Moreno Solis

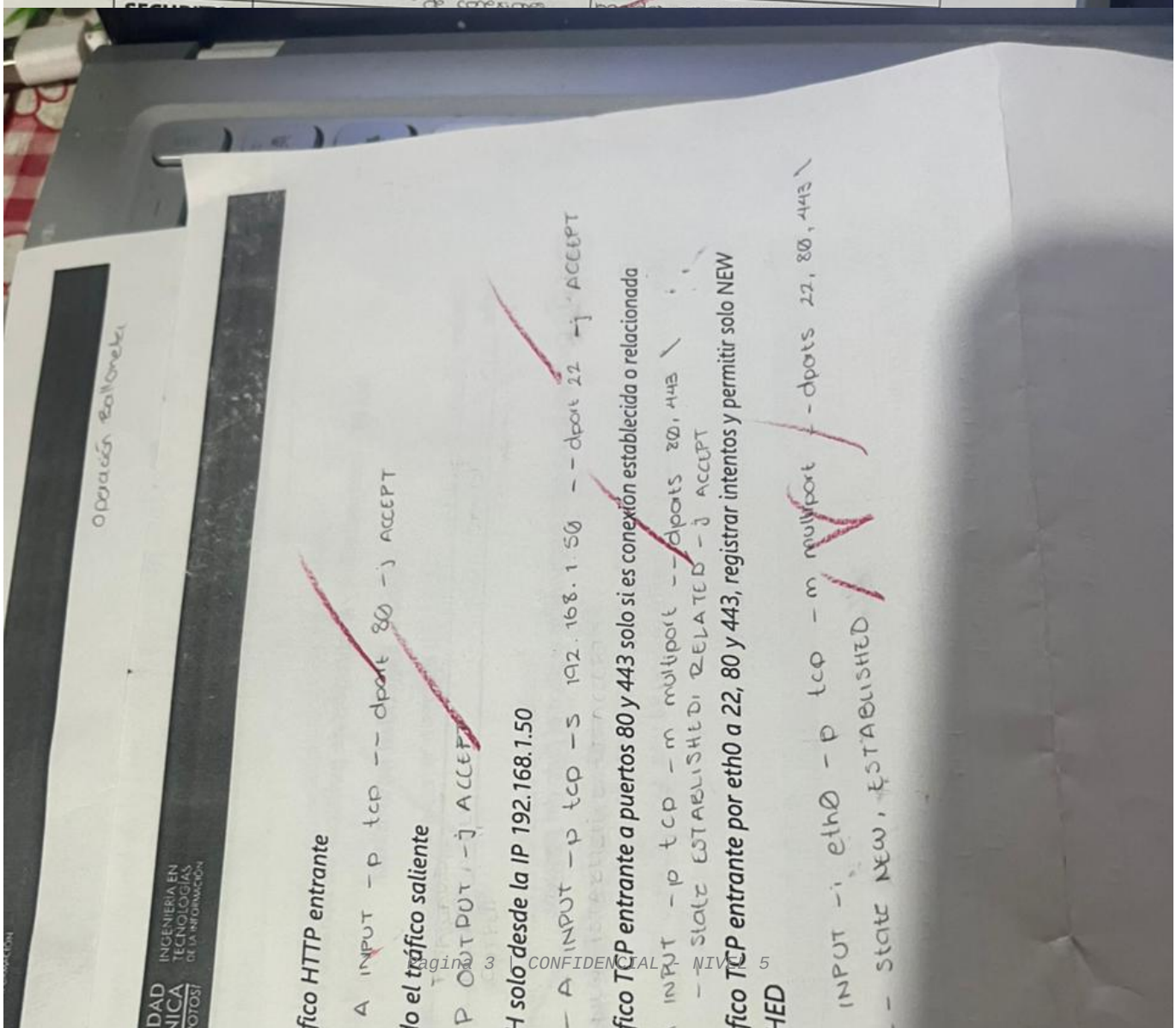
Fecha: Mar 03 febrero 2026 Calf:

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 acción (reglas)

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

Tabla	Propósito principal	Ejemplo de uso (01 palabra o frase corta).
FILTER	Flujo de paquetes	permitir / bloquear tráfico
NAT	Traducción de direcciones	Uso de diferentes dispositivos
MANGLE	Modificación avanzada de paquetes	Cambio de cabeceras
RAW	Excepciones al seguimiento	



UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ — INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Operación Bolloneta

...fico HTTP entrante

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

...lo el tráfico saliente

P OUTPUT -j ACCEPT

...H solo desde la IP 192.168.1.50

A INPUT -p tcp -s 192.168.1.50 --dport 22 -j ACCEPT

...fico TCP entrante a puertos 80 y 443 solo si es conexión establecida o relacionada

INPUT -p tcp -m multiport --dports 80,443 \
-m state ESTABLISHED,RELATED -j ACCEPT

...fico TCP entrante por eth0 a 22, 80 y 443, registrar intentos y permitir solo NEW

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