**ANEXO IV**

**Práctica 4: Implementación de snort para IDS.**

**Reactivos**

* **¿Qué comando se utiliza para verificar que la configuración de Snort es válida antes de ejecutarlo?**

A) sudo snort -V

**B) sudo snort -c /etc/snort/snort.conf -T**

C) sudo snort -R /etc/snort/rules/local.rules

D) sudo snort --debug

* **¿Qué archivo debes editar para definir la red que Snort monitorizará?**

A) /etc/snort/snort.lua

B) /etc/snort/rules/local.rules

**C) /etc/snort/snort.conf**

D) /etc/network/interfaces

* ¿Cuál es el propósito de la regla personalizada alert icmp any any -> $HOME\_NET any (msg:"ICMP Detected"; sid:1000001; rev:1;)?

A) Bloquear todo el tráfico ICMP hacia $HOME\_NET.

**B) Generar una alerta cuando se detecte tráfico ICMP hacia $HOME\_NET.**

C) Permitir únicamente tráfico ICMP desde $HOME\_NET.

D) Evitar que $HOME\_NET genere tráfico ICMP.

* **¿Qué directorio almacena los logs generados por Snort de manera predeterminada?**

A) /var/snort/logs

B) /var/log/security/

C) /etc/snort/logs/

**D) /var/log/snort/**