**ANEXO IV**

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

**Informe**

* **Documentar las configuraciones aplicadas.**

Las configuraciones realizadas se encuentran en la parte procedimiento de la práctica.

* **Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.**

Los resultados obtenidos de la práctica con la debida explicación se muestran en la parte de resultados de la práctica. Y también el impacto que tiene en la seguridad de los dispositivos.

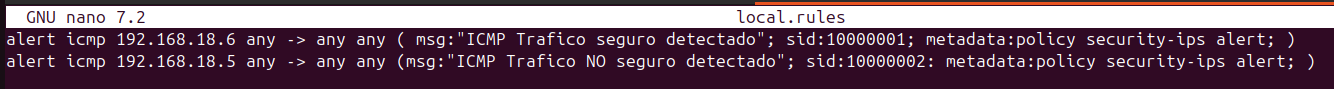
* **Crear reglas de tal forma que los resultados sean ¨Trafico seguro¨ y ¨Trafico inseguro¨ para dos dispositivos específicos.**

Para crear las reglas necesarias para obtener los resultados se requiere dos dispositivos, para el caso se utiliza un dispositivo móvil el cual actúa como terminal 1 (192.168.18.7) y la máquina física que actúa como terminal 2 (192.168.18.6) lo cuales generan tráfico que será monitoreado para obtener resultados.

De esta forma se debe configurar el archivo que contiene la reglas para diferenciar la tráfcico. De este modo se utiliza el comando sudo nano /usr/local/etc/rules/local.rules, y se añade lo siguiente:

alert icmp 192.168.18.6 any -> any any ( msg:"ICMP Trafico seguro detectado"; sid:10000001; metadata:policy security-ips alert; )

alert icmp 192.168.18.5 any -> any any ( msg:"Trafico NO seguro detectado"; sid:10000002; metadata:policy security-ips alert; )



**Figura 5.21.** Configuración de las reglas.

Se inicia el monitoreo con el comando snort -c /usr/local/etc/snort/snort.lua -i enp0s3 -A alert\_fast -s 65535 -k none De esta forma el terminal 1 se define como tráfico seguro y el terminal 2 se defino como tráfico inseguro y al realizar pingo desde ambos terminales hacia el servidor (192.168.18.51) se obtiene el siguiente resultado:

A screen shot of a computer screen

Description automatically generated

**Figura 5.22.** Escaneo del tráfico.

En consecuencia, la figura muestra la diferenciación de tráfico lo cual es de suma importancia para proteger el servidor puesto que se puede añadir todas las IPs o redes que no sean seguras para el usuario y así evitar intrusos que puedan robar información o personas que con la intención de atacar el equipo con algún tipo de virus.