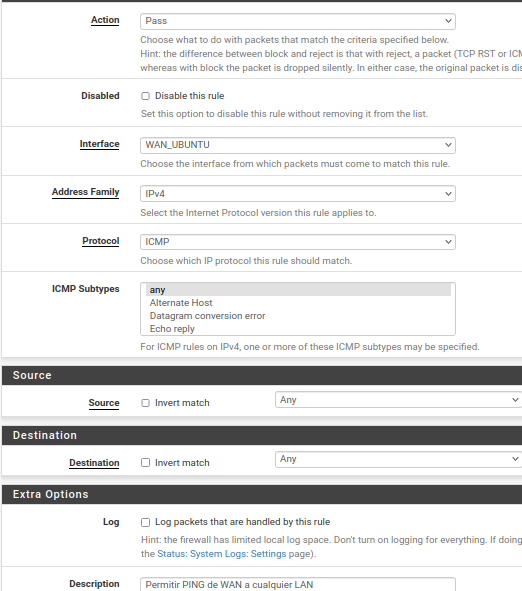
**TEAM CHALLENGE 5 – SPRING 5**

Después de muchas horas intentando, realizar el challenge, los resultados han sido infructuosos en casi todo, habiendo probado tanto desde la web pfsense con snort, cambiándolo por suricata, y hasta con reglas de firewall. Finalmente opte por probar instalar snort directamente en la WAN y después de muchas horas tampoco ha mejorado el resultado:

1. **PING:**

1.- Configura una regla para que permita realizar un ping desde WANa LANSRV.

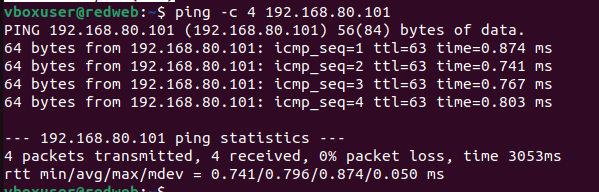
* Regla Firewall PfSense:



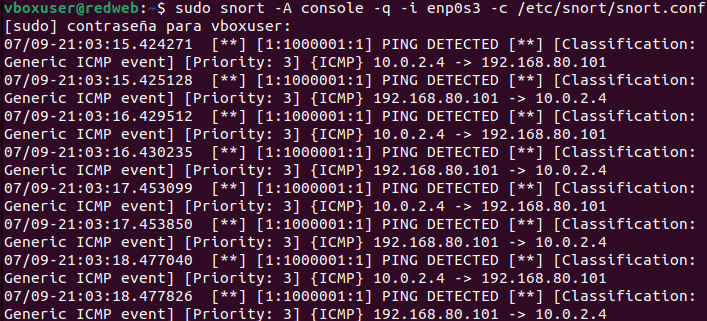
* Reglas Snort:

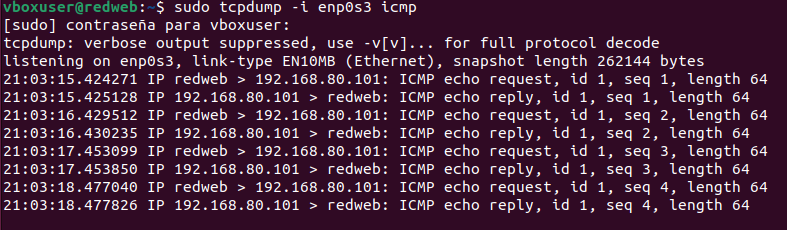


* Envío de PING:



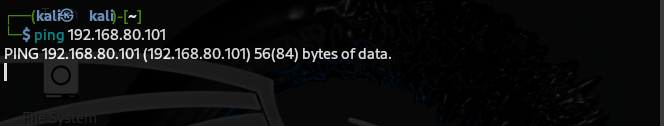
* Datos aportados por la consola snort:





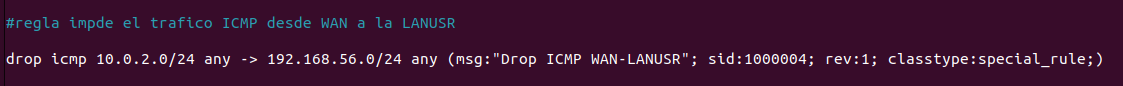
2.- Configura una regla que permita realizar un ping desde LANUSR a LANSRV.

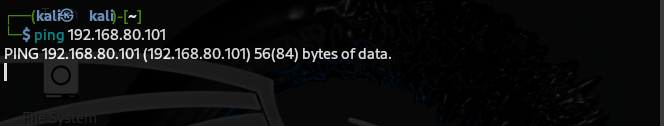


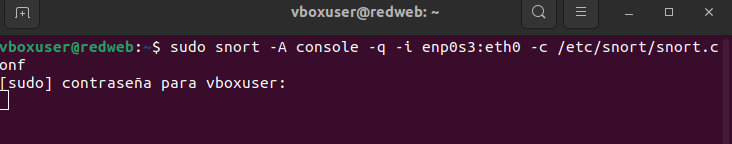


Se queda como si fuera bloqueada, pero no hay mensaje alguno en la consola snort. siendo infructuosa.

3.- Configura una regla que impida realizar un ping desde LANUSR a WAN.



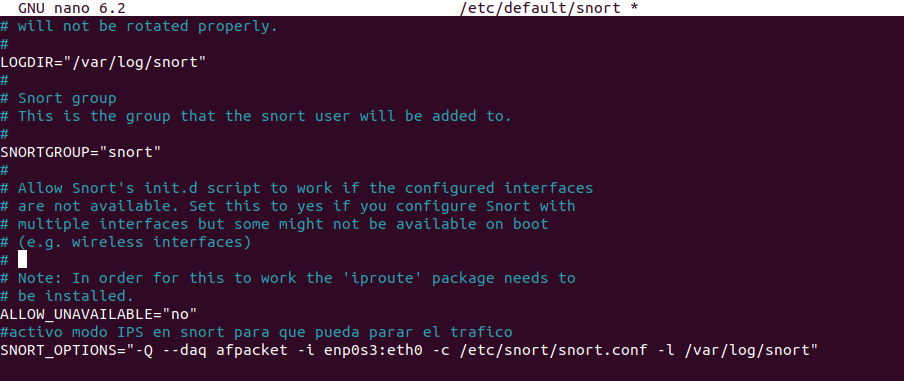




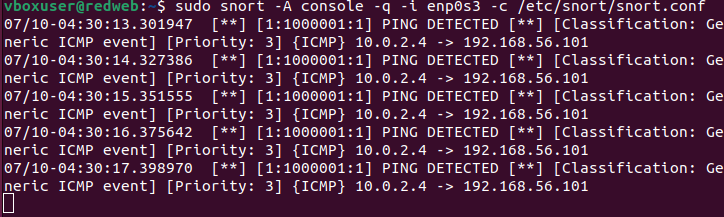
Se queda esperando como si estuviera bloqueada, pero no aporta ninguna señal en la consola snort, así que infructuosa.

4.- Configura una regla que impida realizar un ping desde WAN hasta LANUSR.

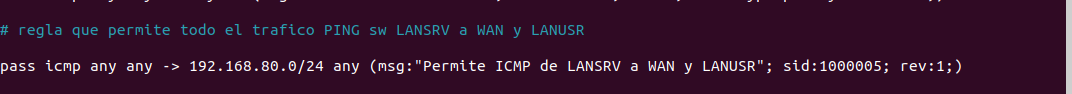
* Regla Snort, con la que activo el IPS de snort, usando \_Q, seguido del modulo afpacket para capturar el trafico en las redes establecidas teniendo en cuenta la configuración de snort y enviado los logs a una dirección concreta.



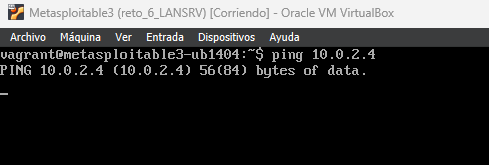
No consigo que me impida el tráfico, solo detecta las alertas de trafico:

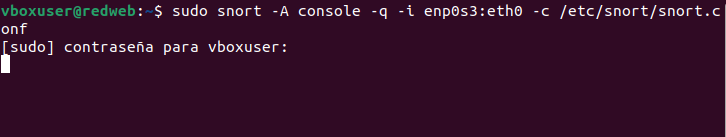


5.-Configura una regla que permita realizar un ping desde LANSRV a WAN y a LANUSR.



Se queda procesando sin aportar información, como si bloqueara la conexión, pero no ha aparece ningún mensaje en la consola de snort.

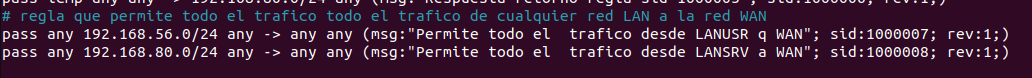




**B - TRAFICO DE RED**

1.- Crea una regla que permita todo el tráfico desde cualquier

dispositivo en la red LAN hacia cualquier destino en la red WAN.

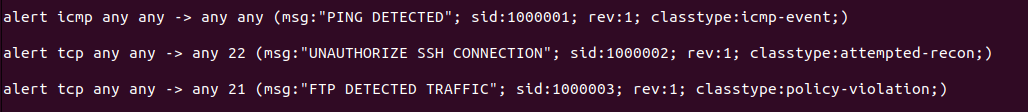


No consigo que las redes LAN conecten entre sí y con la WAN. Desde la WAN, consigo conexiones ICMP con los demás dispositivos, pero tampoco me funciona el SSH y ftp con las LAN.

1. **SSH**

1.- Configura una regla que permita conectarse por SSH desde

cualquier IP de la red LANUSR a LANSRV.



Al igual que las anteriores, Infructuosa su aplicación

El resto de preguntas no me ha dado tiempo ha realizarlas ya que mi preocupación era solventar las primeras no llegando a lograrlo salvo algunas, por lo que en definitiva un desastre.

Configuración rules snort

# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $

# ----------------

# LOCAL RULES

# ----------------

# This file intentionally does not come with signatures. Put your local

# additions here.

alert icmp any any -> any any (msg:"PING DETECTED"; sid:1000001; rev:1; classtype:icmp-event;)

alert tcp any any -> any 22 (msg:"UNAUTHORIZE SSH CONNECTION"; sid:1000002; rev:1; classtype:attempted-recon;)

alert tcp any any -> any 21 (msg:"FTP DETECTED TRAFFIC"; sid:1000003; rev:1; classtype:policy-violation;)

:"Permite ICMP de LANSRV a WAN y LANUSR"; sid:1000005; rev:1;)

pass icmp any any -> 192.168.80.0/24 any (msg:" # regla que permite todo el trafico todo el trafico de cualquier red LAN a la red WAN

pass ip 192.168.56.0/24 any -> any any (msg:"Permite todo el trafico desde LANUSR q WAN"; sid:1000008; rev:1;)

pass ip 192.168.80.0/24 any -> any any (msg:"Permite todo el trafico desde LANSRV a WAN"; sid:1000009; rev:1;)

#regla impde el trafico ICMP desde WAN a la LANUSR

drop icmp 10.0.2.0/24 any -> 192.168.56.0/24 any (msg:"Drop ICMP WAN-LANUSR"; sid:1000004; rev:1; classtype:special>

# regla que permite hacer ping de LANSRV a WAN y A LAN USR

pass icmp 192.168.80.0/24 any -> any any (msg Respuesta retorno regla sid 1000005"; sid:1000006; rev:1;)