

## 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:

### A- PING:

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

- Regla Firewall PfSense:

<b>Action</b>	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP) is sent back to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
<b>Interface</b>	WAN_UBUNTU
Choose the interface from which packets must come to match this rule.	
<b>Address Family</b>	IPv4
Select the Internet Protocol version this rule applies to.	
<b>Protocol</b>	ICMP
Choose which IP protocol this rule should match.	
<b>ICMP Subtypes</b>	<div>any</div> <div>Alternate Host</div> <div>Datagram conversion error</div> <div>Echo reply</div>
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.	
<b>Source</b>	
<b>Source</b>	<input type="checkbox"/> Invert match Any
<b>Destination</b>	
<b>Destination</b>	<input type="checkbox"/> Invert match Any
<b>Extra Options</b>	
<b>Log</b>	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing so, see the <a href="#">Status: System Logs: Settings</a> page).
<b>Description</b>	Permitir PING de WAN a cualquier LAN

- Reglas Snort:

```
GNU nano 6.2 /etc/snort/rules/local.rules
# $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;)
```

- Envío de PING:

```
vboxuser@redweb:~$ ping -c 4 192.168.80.101
PING 192.168.80.101 (192.168.80.101) 56(84) bytes of data.
64 bytes from 192.168.80.101: icmp_seq=1 ttl=63 time=0.874 ms
64 bytes from 192.168.80.101: icmp_seq=2 ttl=63 time=0.741 ms
64 bytes from 192.168.80.101: icmp_seq=3 ttl=63 time=0.767 ms
64 bytes from 192.168.80.101: icmp_seq=4 ttl=63 time=0.803 ms

--- 192.168.80.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.741/0.796/0.874/0.050 ms
vboxuser@redweb:~$
```

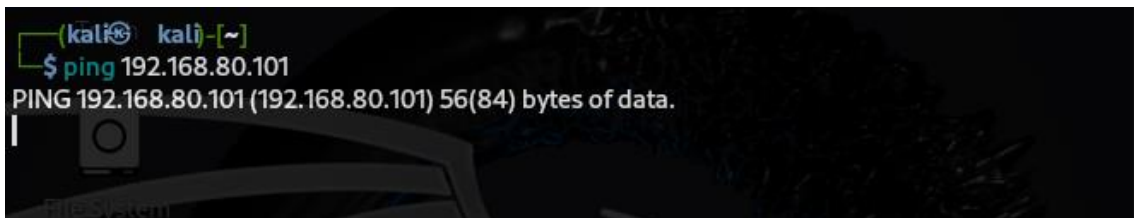
- Datos aportados por la consola snort:

```
vboxuser@redweb:~$ sudo snort -A console -q -i enp0s3 -c /etc/snort/snort.conf
[sudo] contraseña para vboxuser:
07/09-21:03:15.424271  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.80.101
07/09-21:03:15.425128  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 192.168.80.101 -> 10.0.2.4
07/09-21:03:16.429512  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.80.101
07/09-21:03:16.430235  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 192.168.80.101 -> 10.0.2.4
07/09-21:03:17.453099  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.80.101
07/09-21:03:17.453850  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 192.168.80.101 -> 10.0.2.4
07/09-21:03:18.477040  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.80.101
07/09-21:03:18.477826  ** [1:1000001:1] PING DETECTED ** [Classification:
Generic ICMP event] [Priority: 3] {ICMP} 192.168.80.101 -> 10.0.2.4
```

```
vboxuser@redweb:~$ sudo tcpdump -i enp0s3 icmp
[sudo] contraseña para vboxuser:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:03:15.424271 IP redweb > 192.168.80.101: ICMP echo request, id 1, seq 1, length 64
21:03:15.425128 IP 192.168.80.101 > redweb: ICMP echo reply, id 1, seq 1, length 64
21:03:16.429512 IP redweb > 192.168.80.101: ICMP echo request, id 1, seq 2, length 64
21:03:16.430235 IP 192.168.80.101 > redweb: ICMP echo reply, id 1, seq 2, length 64
21:03:17.453099 IP redweb > 192.168.80.101: ICMP echo request, id 1, seq 3, length 64
21:03:17.453850 IP 192.168.80.101 > redweb: ICMP echo reply, id 1, seq 3, length 64
21:03:18.477040 IP redweb > 192.168.80.101: ICMP echo request, id 1, seq 4, length 64
21:03:18.477826 IP 192.168.80.101 > redweb: ICMP echo reply, id 1, seq 4, length 64
```

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

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

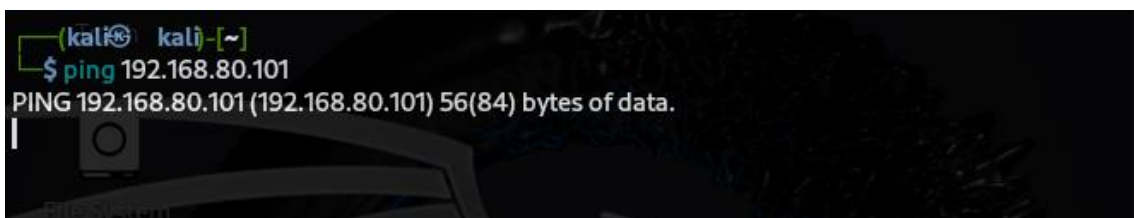


```
(kali) kali-[~]  
$ ping 192.168.80.101  
PING 192.168.80.101 (192.168.80.101) 56(84) bytes of data.  
|
```

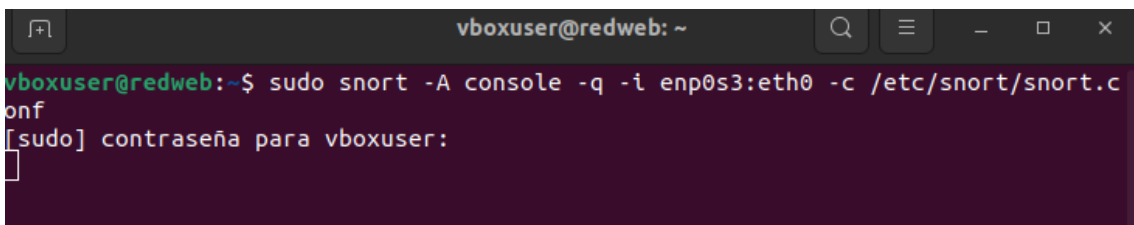
Se queda como si fuera bloqueada, pero no hay mensaje alguno en la consola snort. siendo infructuosa.

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

```
#regla impide 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_rule;)
```



```
(kali) kali-[~]  
$ ping 192.168.80.101  
PING 192.168.80.101 (192.168.80.101) 56(84) bytes of data.  
|
```



```
vboxuser@redweb: ~  
vboxuser@redweb:~$ sudo snort -A console -q -i enp0s3:eth0 -c /etc/snort/snort.conf  
[sudo] contraseña para vboxuser:  
|
```

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.

```
GNU nano 6.2 /etc/default/snort *
# will not be rotated properly.
#
LOGDIR="/var/log/snort"
#
# Snort group
# This is the group that the snort user will be added to.
#
SNORTGROUP="snort"
#
# Allow Snort's init.d script to work if the configured interfaces
# are not available. Set this to yes if you configure Snort with
# multiple interfaces but some might not be available on boot
# (e.g. wireless interfaces)
#
# Note: In order for this to work the 'iproute' package needs to
# be installed.
ALLOW_UNAVAILABLE="no"
#activo modo IPS en snort para que pueda parar el trafico
SNORT_OPTIONS="-Q --daq afpacket -i enp0s3:eth0 -c /etc/snort/snort.conf -l /var/log/snort"
```

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

```
vboxuser@redweb:~$ sudo snort -A console -q -i enp0s3 -c /etc/snort/snort.conf
07/10-04:30:13.301947  [**] [1:1000001:1] PING DETECTED [**] [Classification: Ge
neric ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.56.101
07/10-04:30:14.327386  [**] [1:1000001:1] PING DETECTED [**] [Classification: Ge
neric ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.56.101
07/10-04:30:15.351555  [**] [1:1000001:1] PING DETECTED [**] [Classification: Ge
neric ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.56.101
07/10-04:30:16.375642  [**] [1:1000001:1] PING DETECTED [**] [Classification: Ge
neric ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.56.101
07/10-04:30:17.398970  [**] [1:1000001:1] PING DETECTED [**] [Classification: Ge
neric ICMP event] [Priority: 3] {ICMP} 10.0.2.4 -> 192.168.56.101
```

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

```
# regla que permite todo el trafico PING sw LANSRV a WAN y LANUSR
pass icmp any any -> 192.168.80.0/24 any (msg:"Permite ICMP de LANSRV a WAN y LANUSR"; sid:1000005; rev:1;)
```

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

```
Metasploitable3 (reto_6_LANSRV) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
vagrant@metasploitable3-ub1404:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
-

vboxuser@redweb:~$ sudo snort -A console -q -i enp0s3:eth0 -c /etc/snort/snort.conf
[sudo] contraseña para vboxuser:

```

## 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.

```
pass icmp any any -> 192.168.0.0/24 any (msg: respuesta retorno regla sid:1000007; rev:1;)
# regla que permite todo el trafico todo el trafico de cualquier red LAN a la red WAN
pass any 192.168.56.0/24 any -> any any (msg:"Permite todo el trafico desde LANUSR q WAN"; sid:1000007; rev:1;)
pass any 192.168.80.0/24 any -> any any (msg:"Permite todo el trafico desde LANSRV a WAN"; sid:1000008; rev:1;)
```

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.

## B- SSH

1.- Configura una regla que permita conectarse por SSH desde cualquier IP de la red LANUSR a LANSRV.

```
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;)
```

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;)



