



TAREA 06

IDS/IPS SNORT

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

La Detección Multipunto de Incidentes

En la Unidad 6 hemos estudiado cómo instalar y configurar el IDS Snort, situándolo en la misma máquina en la que estará el SIEM que procesará su información una vez filtrada y almacenada.

Sin embargo, aunque esta configuración es habitual en los laboratorios, no es la corriente en las instalaciones reales. En cualquier entorno productivo suele haber una sonda Snort en cada una de las máquinas perimetrales, comprometidas, vulnerables, etc., cuya información de logging se ha de redirigir hacia una única máquina en la que estará instalado el SIEM (Unidad 7).

En esta tarea abordaremos el registro de logs en los diferentes agentes IDS en tiempo real utilizando la aplicación SNORT.

Para el desarrollo de la práctica nos centraremos en la red DMZ, en concreto sobre el SNORT situado en dicha zona y una de las máquinas, la cual, tiene instalado los servicios SSH, HTTP y MySQL. Esta última máquina se proporciona en esta tarea (WebServer).

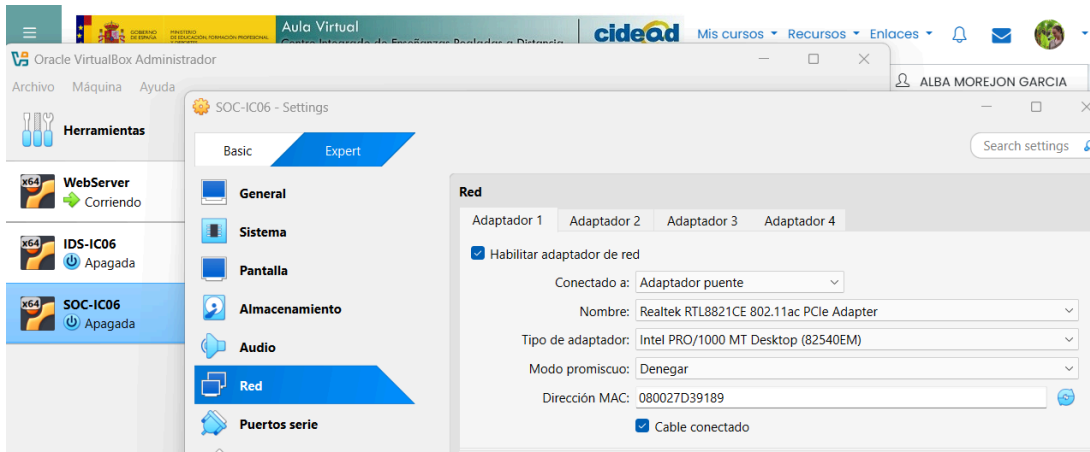
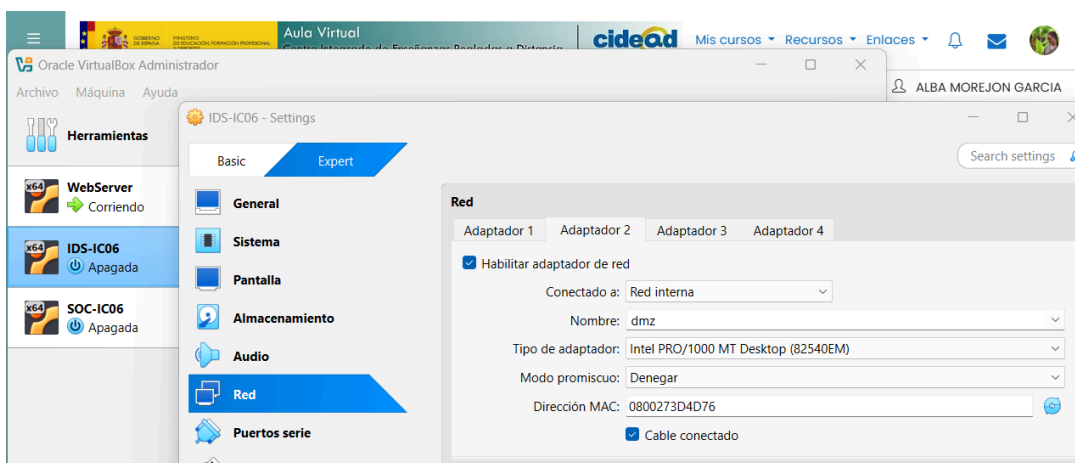
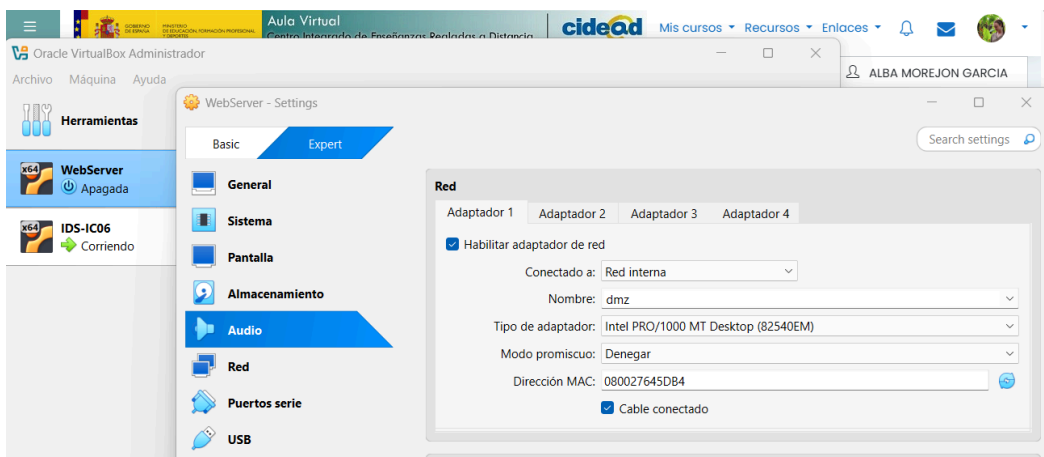
Apartado 1: Configurar las máquinas virtuales para que tengan comunicación completa.

Deberás efectuar las siguientes tareas:

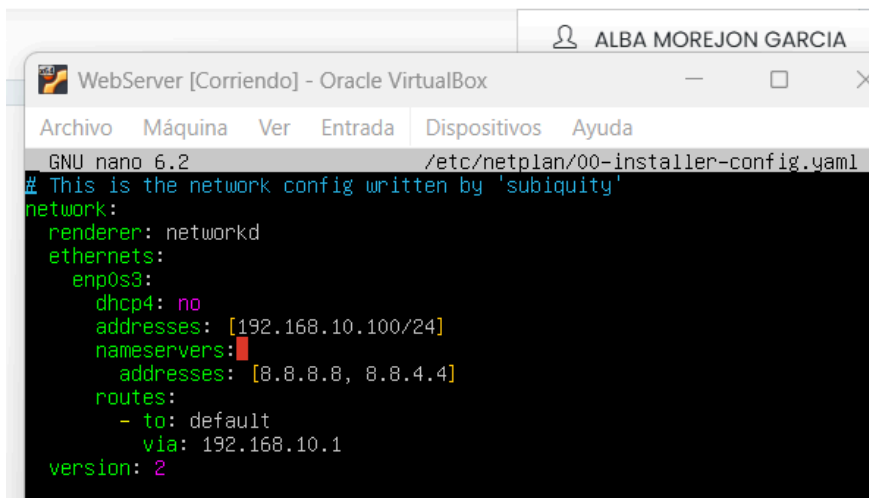
- Crear la máquina IDS (Snort) con dos interfaces de red y configurarla para que permita la comunicación completa entre ambas interfaces. Una tomará el rol de adaptador puente con la red externa y la otra interfaz sería la puerta de enlace predeterminada de la red DMZ. Se debe mostrar el fichero de configuración de las interfaces de red. Se recomienda el uso de Ubuntu SERVER o DEBIAN.
- Configurar la máquina IDS para que las máquinas de la red interna DMZ (WebServer) se puedan comunicar correctamente con el exterior. Se debe conseguir acceso a internet y a la red externa.
- Crear una máquina virtual que se denomine SOC, la cual esté conectada a la red externa (adaptador puente). Esta máquina debe tener comunicación con el WebServer. La máquina SOC debe tener interfaz gráfica, por lo que se recomienda la instalación de Ubuntu Desktop.

| NOMBRE | SISTEMA OPERATIVO | ADAPTADOR | IP |
|----------------|------------------------|--|-------------------------|
| IDS-IC06 | Ubuntu Server 24.04.2 | Adaptador puente 08:00:27:F7:6F:F7 enp0s3 | dhcp 192.168.0.36/24 |
| | | Red interna (dmz) 08:00:27:7E:1C:F2 enp0s8 | 192.168.10.1/24 |
| SOC-IC06 | Ubuntu Desktop 24.04.1 | Adaptador puente 08:00:27:4B:B1:F1 enp0s3 | dhcp 192.168.0.41/24 |
| WebServer-IC06 | Ubuntu 64bits | Red interna (dmz) 08:00:27:64:5D:B4 enp0s3 | 192.168.10.100/24 |

Importamos el archivo .ova facilitado en el enunciado de esta misma práctica y comprobamos su configuración.



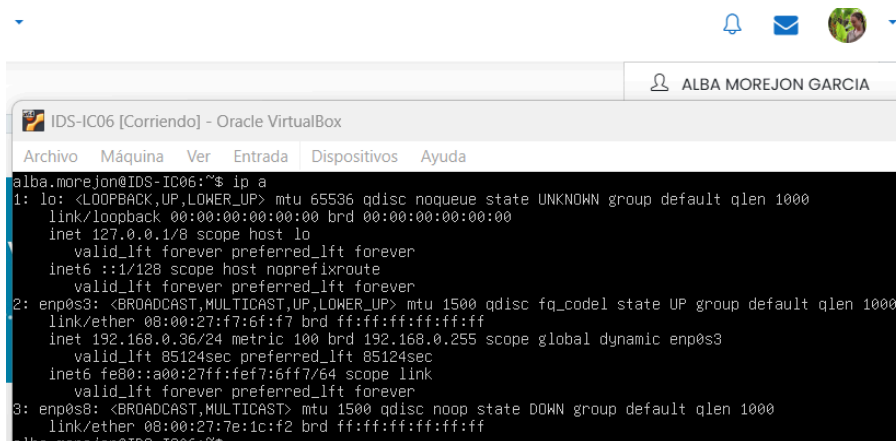
Configuración red WebServer



The screenshot shows a terminal window titled "WebServer [Corriendo] - Oracle VirtualBox". The user is editing the file `/etc/netplan/00-installer-config.yaml` using GNU nano 6.2. The configuration is for a network interface `enp0s3` with the following settings:

```
# This is the network config written by 'subiquity'
network:
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.100/24]
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
      routes:
        - to: default
          via: 192.168.10.1
      version: 2
```

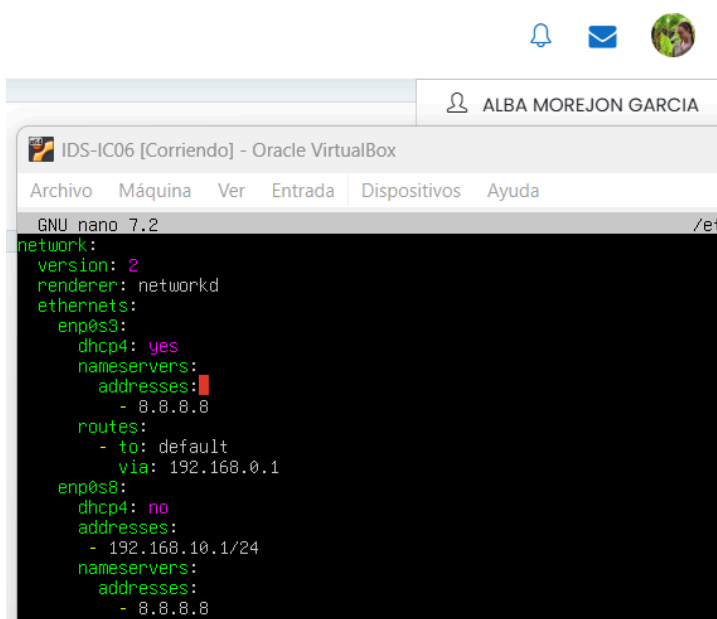
Maquina IDS:



The screenshot shows a terminal window titled "IDS-IC06 [Corriendo] - Oracle VirtualBox". The user has run the command `ifconfig`, and the output shows the configuration for three network interfaces:




```
alba.morejon@IDS-IC06:~$ ifconfig
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f7:6f:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.36/24 metric 100 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 85124sec preferred_lft 85124sec
    inet6 fe80::a00:27ff:fef7:6ff7/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:7e:1c:f2 brd ff:ff:ff:ff:ff:ff
```

modificamos el fichero `/etc/netplan/50-cloud-init.yaml` y lo aplicamos con `sudo netplan apply`



The screenshot shows a terminal window titled "IDS-IC06 [Corriendo] - Oracle VirtualBox". The user is editing the file `/etc/netplan/50-cloud-init.yaml` using GNU nano 7.2. The configuration is for two network interfaces, `enp0s3` and `enp0s8`, with the following settings:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
      nameservers:
        addresses:
          - 8.8.8.8
      routes:
        - to: default
          via: 192.168.0.1
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.10.1/24
      nameservers:
        addresses:
          - 8.8.8.8
```



ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox




Archivo Máquina Ver Entrada Dispositivos Ayuda

```
alba.morejon@IDS-IC06:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.36 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe7:6ff7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:f7:6f:f7 txqueuelen 1000 (Ethernet)
    RX packets 2801 bytes 1675837 (1.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 406 bytes 30390 (30.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::a00:27ff:fe7e:1cf2 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:7e:1c:f2 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1336 (1.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 107 bytes 9098 (9.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 107 bytes 9098 (9.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hay conectividad entre las máquinas IDS y WebService



ALBA MOREJON GARCIA

WebServer-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
webuser@webserver:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=2.54 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=2.25 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=2.39 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.94 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=2.81 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=2.36 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=1.65 ms
^C
--- 192.168.10.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 1.653/2.277/2.812/0.354 ms
```

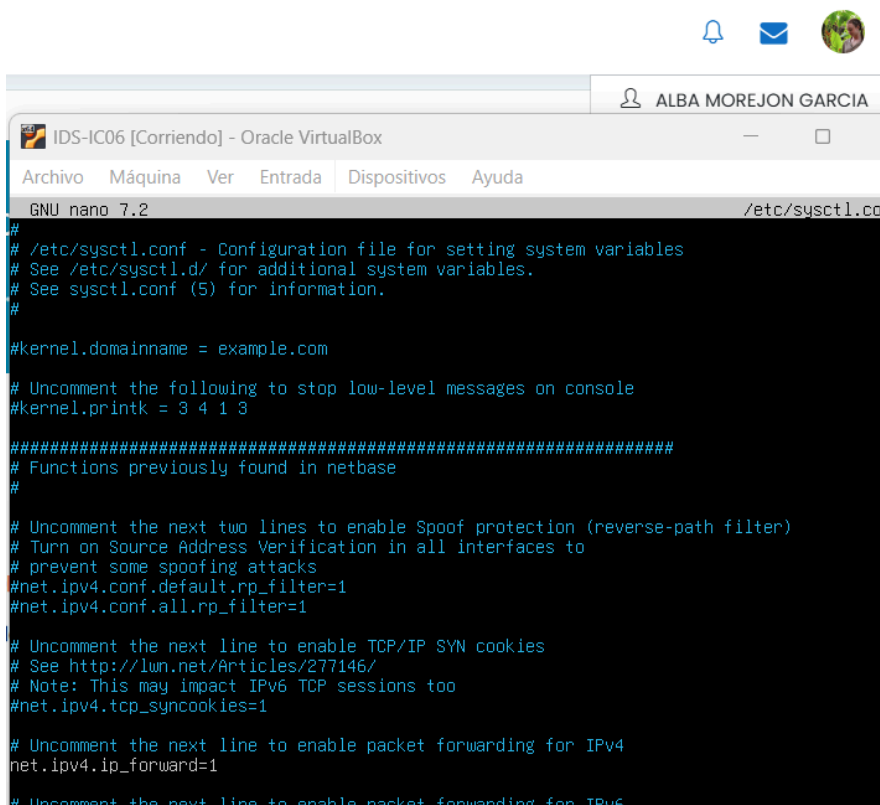
IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

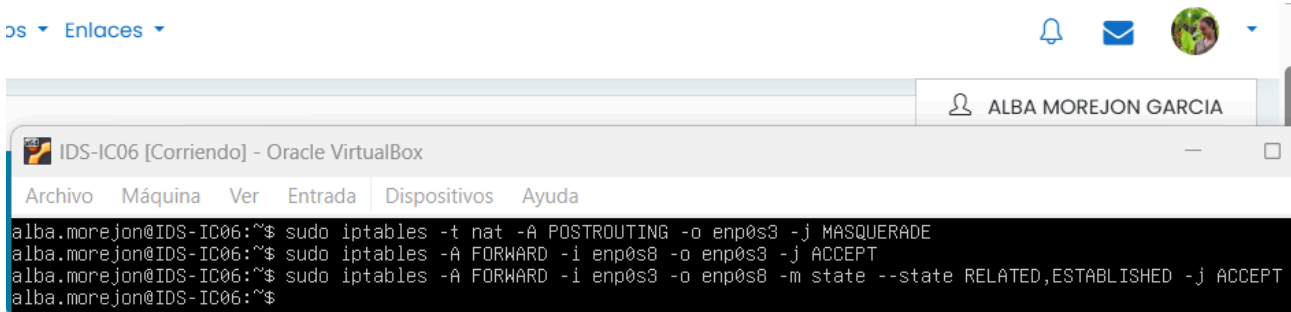
```
alba.morejon@IDS-IC06:~$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=64 time=1.35 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=64 time=1.24 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=64 time=1.57 ms
64 bytes from 192.168.10.100: icmp_seq=4 ttl=64 time=2.88 ms
64 bytes from 192.168.10.100: icmp_seq=5 ttl=64 time=2.12 ms
64 bytes from 192.168.10.100: icmp_seq=6 ttl=64 time=1.39 ms
^C
--- 192.168.10.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 1.241/1.924/2.882/0.639 ms
alba.morejon@IDS-IC06:~$
```

Vamos a hacer que ids enrute para que la máquina webserver tenga salida a internet.

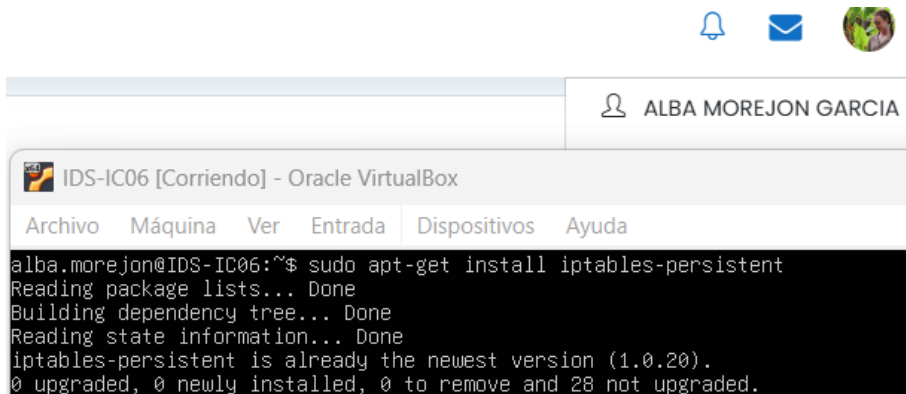
En el fichero /etc/sysctl.conf descomentamos la línea siguiente y aplicamos la configuración con el comando `sudo sysctl -p` (activar el enrutamiento ip)

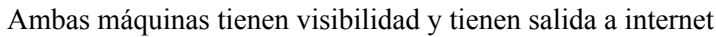
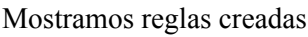


A continuación en caso de no estar instalado con el comando `sudo apt-get iptables` instalamos la herramienta, configuraremos el nat para permitir el tráfico.

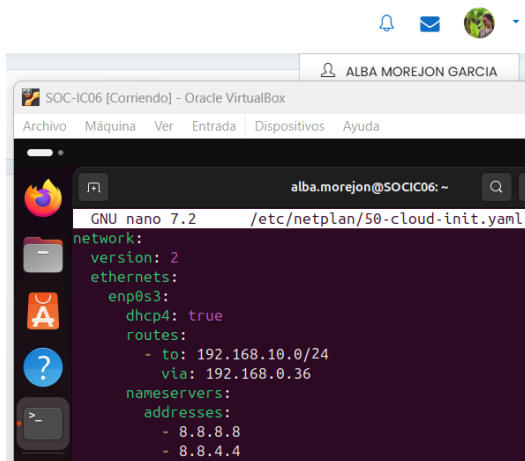


Instalamos la herramienta para hacer fijas las reglas tras cada reinicio

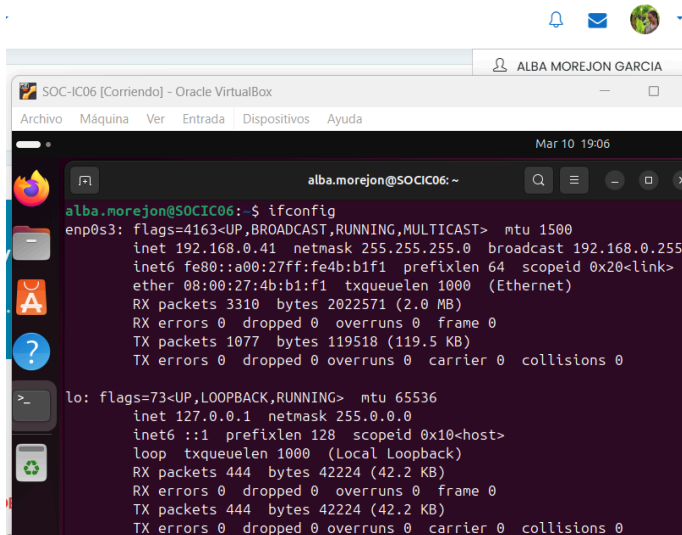




Máquina SOC

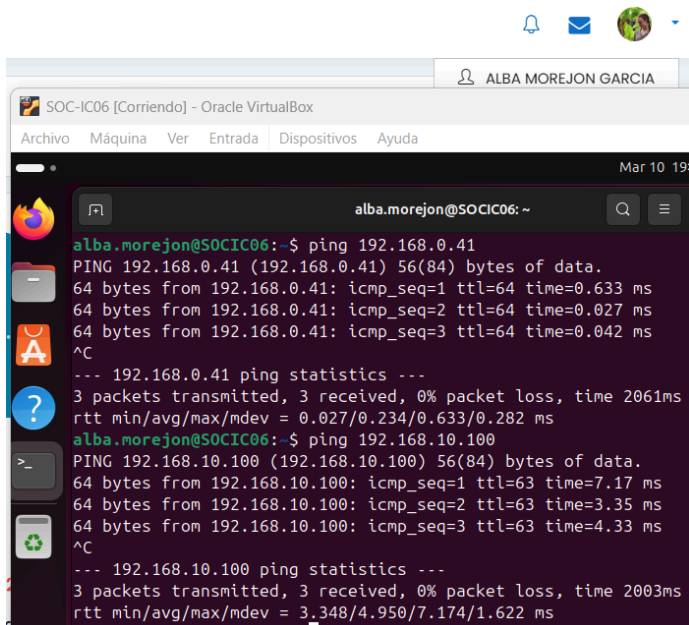


```
alba.morejon@SOCIC06: ~  
GNU nano 7.2 /etc/netplan/50-cloud-init.yaml  
network:  
  version: 2  
  ethernet:  
    enp0s3:  
      dhcp4: true  
      routes:  
        - to: 192.168.10.0/24  
          via: 192.168.0.36  
      nameservers:  
        addresses:  
          - 8.8.8.8  
          - 8.8.4.4
```



```
alba.morejon@SOCIC06: ~  
alba.morejon@SOCIC06:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.41 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::a00:27ff:fe4b:b1f1 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:4b:b1:f1 txqueuelen 1000 (Ethernet)  
    RX packets 3310 bytes 2022571 (2.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1077 bytes 119518 (119.5 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 444 bytes 42224 (42.2 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 444 bytes 42224 (42.2 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

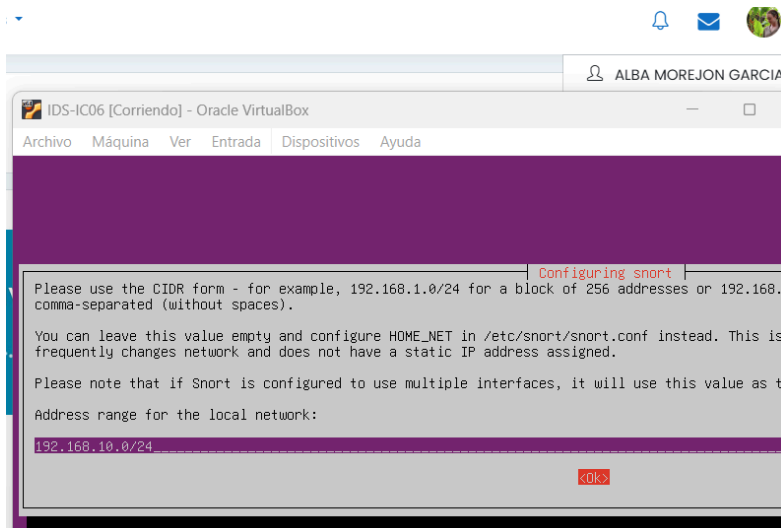
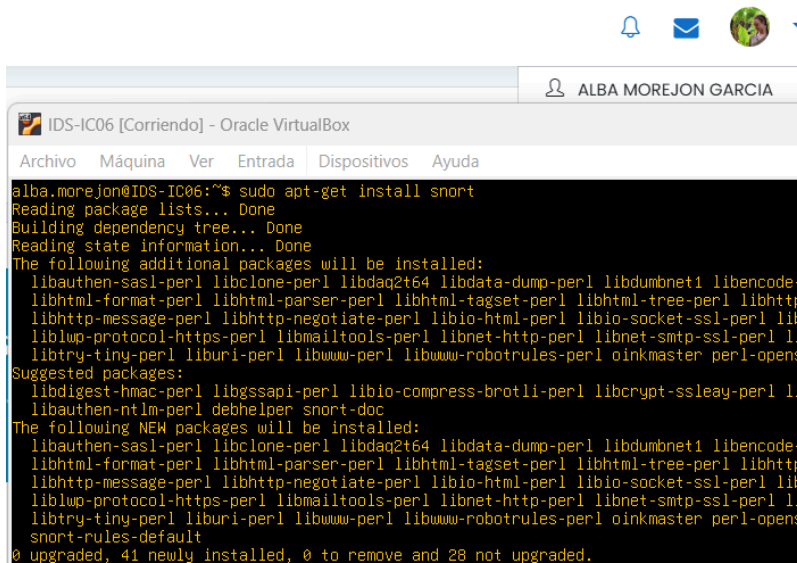
Comprobamos que tenga conexión con las otras máquinas



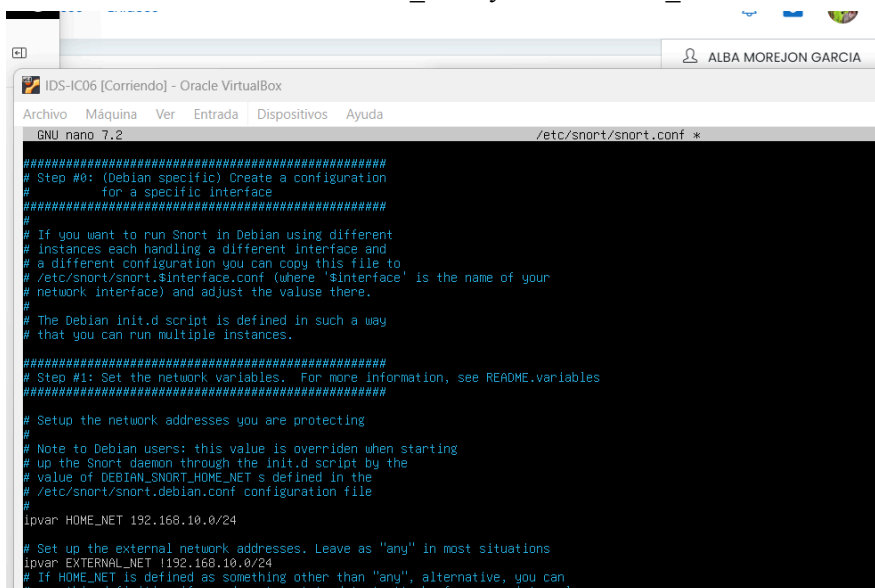
```
alba.morejon@SOCIC06: ~  
alba.morejon@SOCIC06:~$ ping 192.168.0.41  
PING 192.168.0.41 (192.168.0.41) 56(84) bytes of data.  
64 bytes from 192.168.0.41: icmp_seq=1 ttl=64 time=0.633 ms  
64 bytes from 192.168.0.41: icmp_seq=2 ttl=64 time=0.027 ms  
64 bytes from 192.168.0.41: icmp_seq=3 ttl=64 time=0.042 ms  
^C  
--- 192.168.0.41 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2061ms  
rtt min/avg/max/mdev = 0.027/0.234/0.633/0.282 ms  
alba.morejon@SOCIC06:~$ ping 192.168.10.100  
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.  
64 bytes from 192.168.10.100: icmp_seq=1 ttl=63 time=7.17 ms  
64 bytes from 192.168.10.100: icmp_seq=2 ttl=63 time=3.35 ms  
64 bytes from 192.168.10.100: icmp_seq=3 ttl=63 time=4.33 ms  
^C  
--- 192.168.10.100 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 3.348/4.950/7.174/1.622 ms
```


Apartado 2: Configuración del IDS para registrar el tráfico de red. (SNORT)

- **Instalar y configurar SNORT en el IDS para poder escuchar y guardar todo el tráfico de la red DMZ.**



Establecemos las variables HOME NET y EXTERNAL NET



- **Configurar las reglas de detección de Snort, cada una de ellas debe recoger un mensaje indicando el tipo de conexión que se establece y un identificador único. Las alertas a generar son:**
 - **Ping (Request) desde la red interna (DMZ) hacia el exterior. Se debe registrar únicamente el Request de la interna y no la respuesta de la externa.**

Recursos ▾ Enlaces ▾

ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 7.2 /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.

#ping request de la DMZ al exterior
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Solicitud ping desde DMZ al exterior"; sid:1000001; rev:1; icmp_type:8;)
```

- **Ping (Request) desde el exterior hacia la DMZ. Se debe registrar únicamente el Request de la externa y no la respuesta de la DMZ.**

Recursos ▾ Enlaces ▾

ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 7.2 /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.

#ping desde DMZ al exterior
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Solicitud ping desde DMZ al exterior"; sid:1000001; rev:1; icmp_type:8;)

#ping desde el exterior a DMZ
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Solicitud ping desde el exterior a la DMZ"; sid:1000002; rev:1; icmp_type:8;)
```

- **Intentos de las conexiones SSH hacia WebServer. Solamente registra el primer paquete de sincronización de este intento de conexión.**

Recursos ▾ Enlaces ▾

ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 7.2 /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.

#ping desde DMZ al exterior
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Solicitud ping desde DMZ al exterior"; sid:1000001; rev:1; icmp_type:8;)

#ping desde el exterior a DMZ
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Solicitud ping desde el exterior a la DMZ"; sid:1000002; rev:1; icmp_type:8;)

#Conexiones SSH al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Intento conexion SSH al WebServer"; sid:1000003; rev:1; flags:S;)
```

- **Intentos de las conexiones HTTP hacia WebServer. Solamente registra el primer paquete de sincronización de este intento de conexión.**

Recursos Enlaces

ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 7.2 /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.

#ping desde DMZ al exterior
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Solicitud ping desde DMZ al exterior"; sid:1000001; rev:1; icmp_type:8;)

#ping desde el exterior a DMZ
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Solicitud ping desde el exterior a la DMZ"; sid:1000002; rev:1; icmp_type:8;)

#Conexiones SSH al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Intento conexion SSH al WebServer"; sid:1000003; rev:1; flags:S;)

#Conexiones HTTP al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Intento de conexion HTTP al WebServer"; sid:1000004; rev:1; flags:S;)
```

- **Intentos de las conexiones a phpMyAdmin hacia WebServer. La ruta hacia la base de datos es <http://ip-de-WebServer/phpmyadmin>.**

stancia cidead Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 7.2 /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.

#ping desde DMZ al exterior
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Solicitud ping desde DMZ al exterior"; sid:1000001; rev:1; icmp_type:8;)

#ping desde el exterior a DMZ
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Solicitud ping desde el exterior a la DMZ"; sid:1000002; rev:1; icmp_type:8;)

#Conexiones SSH al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Intento conexion SSH al WebServer"; sid:1000003; rev:1; flags:S;)

#Conexiones HTTP al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Intento de conexion HTTP al WebServer"; sid:1000004; rev:1; flags:S;)

#Conexiones phpMyAdmin hacia el WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Intento de conexion phpMyAdmin al WebServer"; sid:1000005; rev:1; flags:S;content: "/phpmyadmin"; http_uri:)
```

Tuvimos que cambiar el icmp_type de las dos primeras líneas por itype

stancia cidead Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

IDS-IC06 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 7.2 /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.

#ping desde DMZ al exterior
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"Solicitud ping desde DMZ al exterior"; sid:1000001; rev:1; itype:8;)

#ping desde el exterior a DMZ
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Solicitud ping desde el exterior a la DMZ"; sid:1000002; rev:1; itype:8;)

#Conexiones SSH al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Intento conexion SSH al WebServer"; sid:1000003; rev:1; flags:S;)

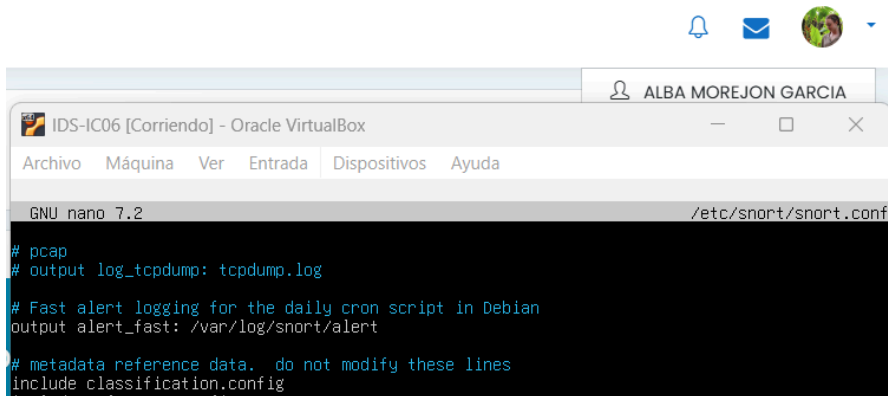
#Conexiones HTTP al WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Intento de conexion HTTP al WebServer"; sid:1000004; rev:1; flags:S;)

#Conexiones phpMyAdmin hacia el WebServer
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Intento de conexion phpMyAdmin al WebServer"; sid:1000005; rev:1; flags:S;content: "/phpmyadmin"; http_uri:)
```

Añadimos una linea como adicional para evitar en trafico dhcp

```
#Ignorar trafico DHCP
pass udp any 68 -> any 67 (msg:"Ignorar trafico dhcp"; sid:1000006; rev:1;)
```

Configuramos la ruta del log

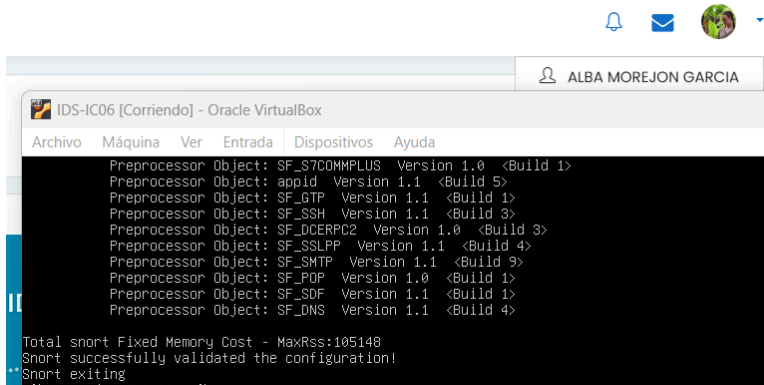


```
ALBA MOREJON GARCIA
IDS-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2 /etc/snort/snort.conf
# pcap
# output log_tcpdump: tcpdump.log
# Fast alert logging for the daily cron script in Debian
output alert_fast: /var/log/snort/alert
# metadata reference data. do not modify these lines
include classification.config
```

Apartado 3: Pruebas de las alertas generadas.

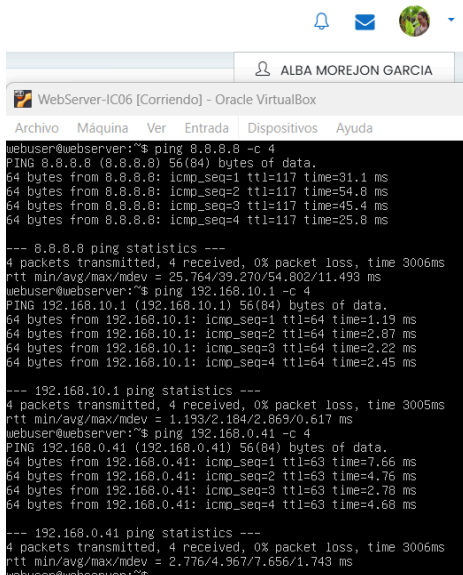
- Realizar las pruebas pertinentes donde se demuestren las diferentes alertas generadas en el apartado 2.
- Para cada una de estas alertas se debe recoger pantallazo con las acciones realizadas y un volcado final del archivo de log resultante tras todas las pruebas.

Al usar el comando para probar snort: `sudo snort -T -c /etc/snort/snort.conf`, se consigue un resultado favorable:



```
ALBA MOREJON GARCIA
IDS-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Total snort Fixed Memory Cost - MaxRss:105148
Snort successfully validated the configuration!
** Snort exiting
```

Tenian conectividad entre las máquinas



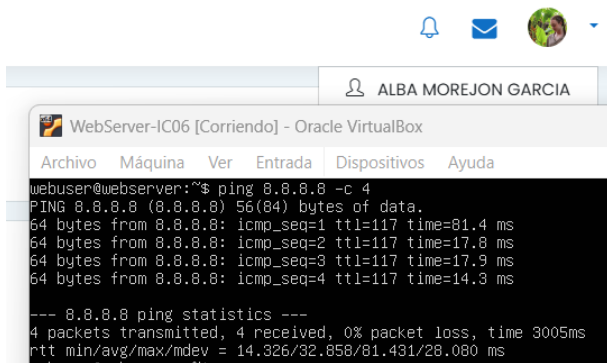
```
ALBA MOREJON GARCIA
WebServer-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
webuser@webserver:~$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=31.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=54.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=45.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=25.8 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 25.764/39.270/54.802/11.493 ms
webuser@webserver:~$ ping 192.168.10.1 -c 4
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=2.87 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=2.22 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=2.45 ms

--- 192.168.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.193/2.184/2.869/0.617 ms
webuser@webserver:~$ ping 192.168.0.41 -c 4
PING 192.168.0.41 (192.168.0.41) 56(84) bytes of data:
64 bytes from 192.168.0.41: icmp_seq=1 ttl=63 time=7.66 ms
64 bytes from 192.168.0.41: icmp_seq=2 ttl=63 time=4.76 ms
64 bytes from 192.168.0.41: icmp_seq=3 ttl=63 time=2.78 ms
64 bytes from 192.168.0.41: icmp_seq=4 ttl=63 time=4.68 ms

--- 192.168.0.41 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.776/4.967/7.656/1.743 ms
webuser@webserver:~$
```

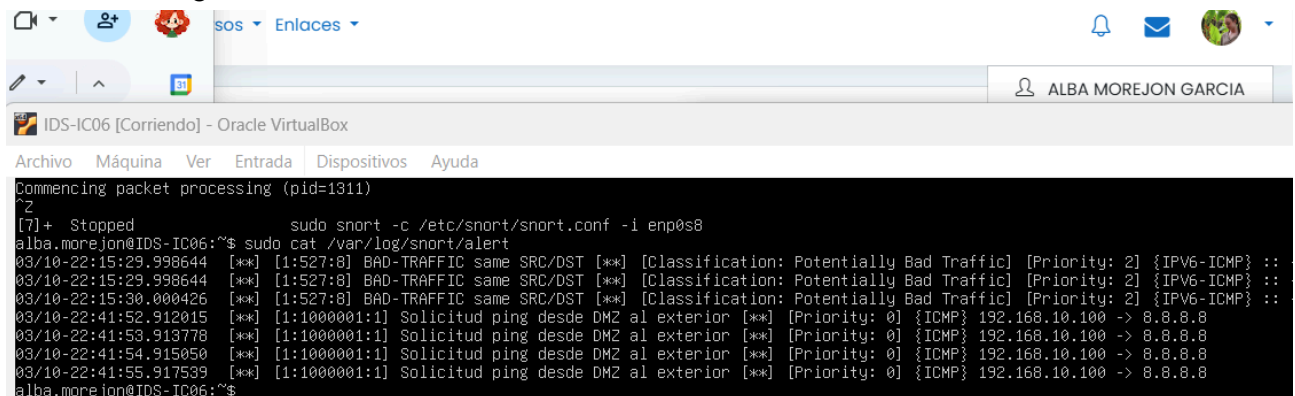
Primera prueba, trafico fuera de la red



```
ALBA MOREJON GARCIA
WebServer-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
webuser@webserver:~$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=81.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=17.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=17.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=14.3 ms

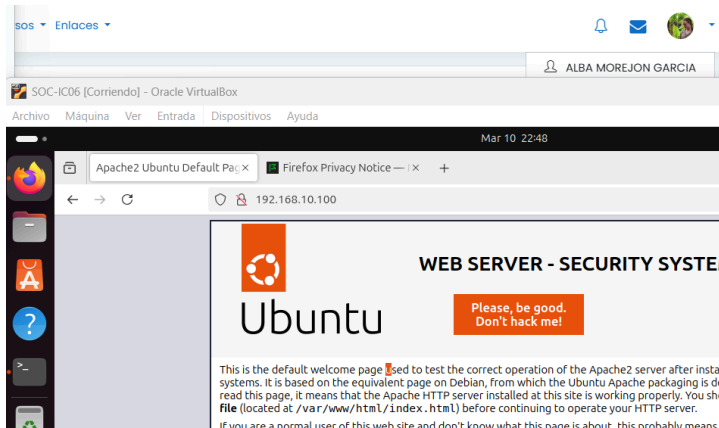
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 14.326/32.858/81.431/28.080 ms
```

Mostramos el log

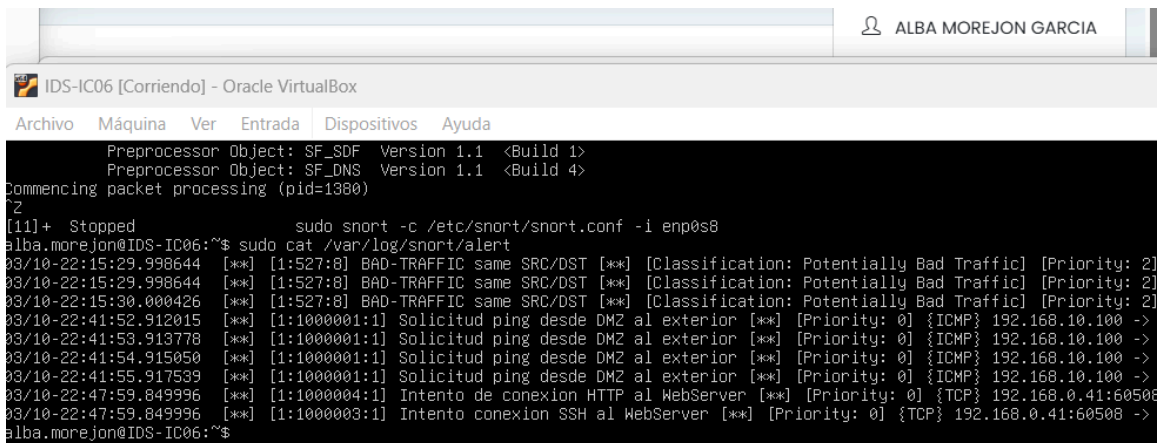


```
ALBA MOREJON GARCIA
IDS-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Commencing packet processing (pid=1311)
^Z
[7]+ Stopped sudo snort -c /etc/snort/snort.conf -i enp0s8
alba.morejon@IDS-IC06:~$ sudo cat /var/log/snort/alert
03/10-22:15:29.998644 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::
03/10-22:15:29.998644 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::
03/10-22:15:30.000426 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::
03/10-22:41:52.912015 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 -> 8.8.8.8
03/10-22:41:53.913778 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 -> 8.8.8.8
03/10-22:41:54.915050 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 -> 8.8.8.8
03/10-22:41:55.917539 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 -> 8.8.8.8
alba.morejon@IDS-IC06:~$
```

Conexión desde http a WebServer



Mostramos el log



```
ALBA MOREJON GARCIA
IDS-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Commencing packet processing (pid=1380)
^Z
[11]+ Stopped sudo snort -c /etc/snort/snort.conf -i enp0s8
alba.morejon@IDS-IC06:~$ sudo cat /var/log/snort/alert
03/10-22:15:29.998644 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2]
03/10-22:15:29.998644 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2]
03/10-22:15:30.000426 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2]
03/10-22:41:52.912015 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 ->
03/10-22:41:53.913778 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 ->
03/10-22:41:54.915050 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 ->
03/10-22:41:55.917539 [**] [1:1000001:1] Solicitud ping desde DM2 al exterior [**] [Priority: 0] {ICMP} 192.168.10.100 ->
03/10-22:47:59.849996 [**] [1:1000004:1] Intento de conexion HTTP al WebServer [**] [Priority: 0] {TCP} 192.168.0.41:60508 ->
03/10-22:47:59.849996 [**] [1:1000003:1] Intento conexion SSH al WebServer [**] [Priority: 0] {TCP} 192.168.0.41:60508 ->
alba.morejon@IDS-IC06:~$
```