Ivana Sánchez Pérez

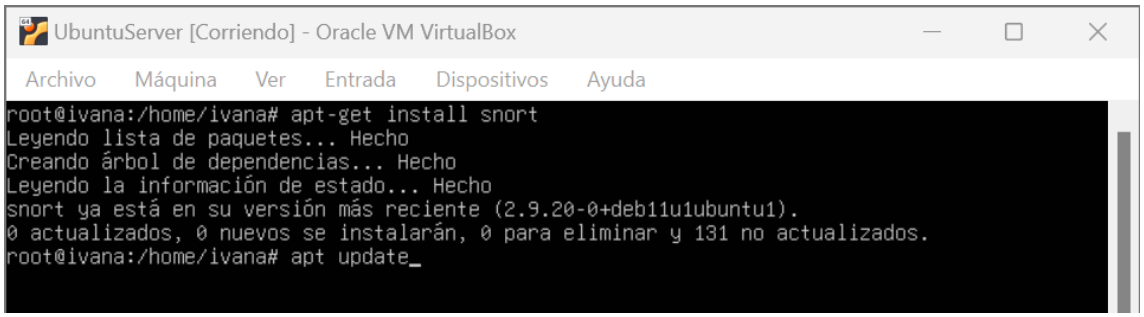
2º ASIR

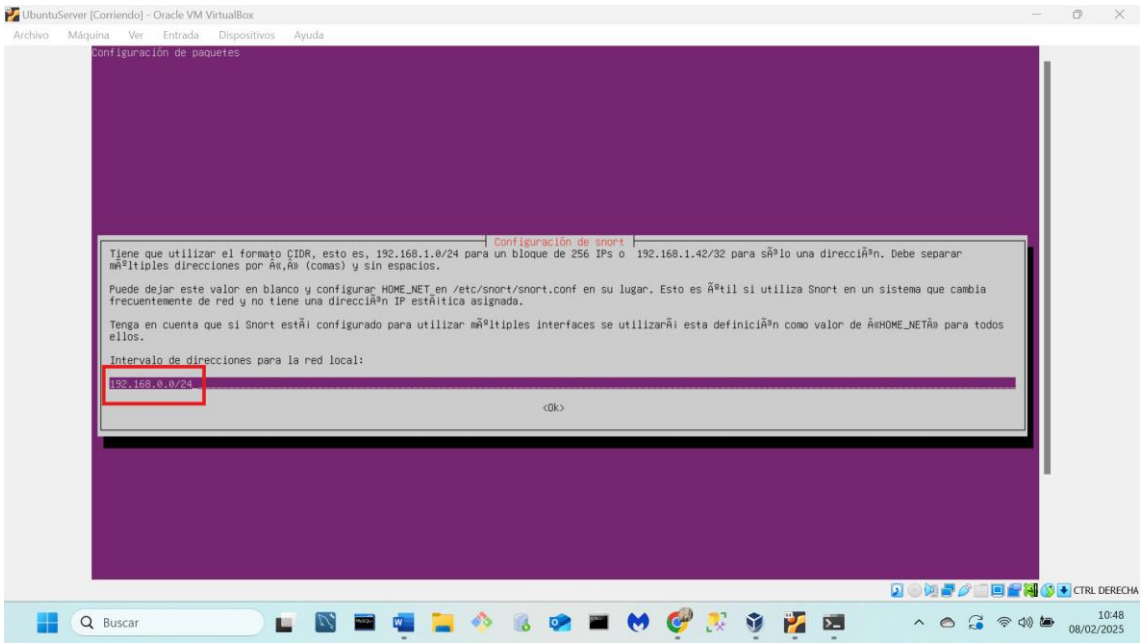
Introducción

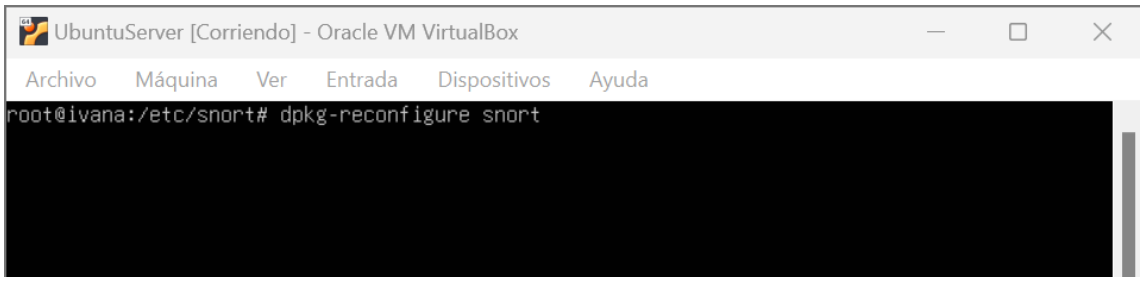
SNORT es una herramienta esencial para cualquier administrador de red que busque proteger sus sistemas contra intrusiones y ataques maliciosos. Su flexibilidad, potencia y la capacidad de personalización lo convierten en una opción popular tanto para entornos pequeños como para grandes infraestructuras de red. Sin embargo, su efectividad depende en gran medida de la correcta configuración y mantenimiento de las reglas, así como de la actualización constante para adaptarse a las nuevas amenazas.

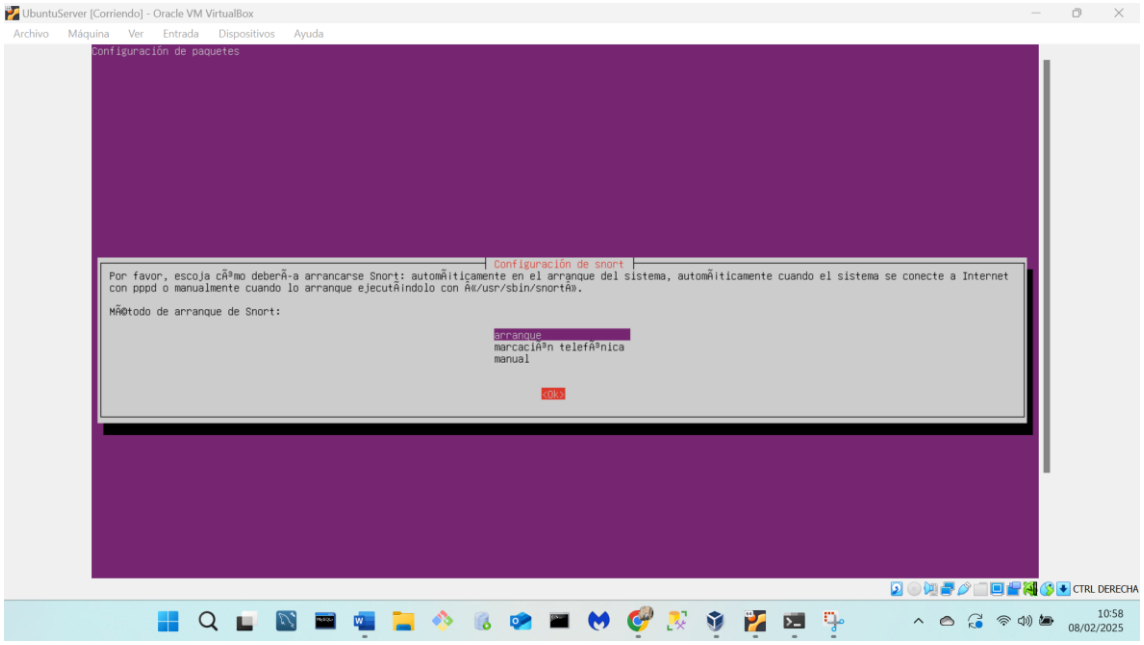
Instalación

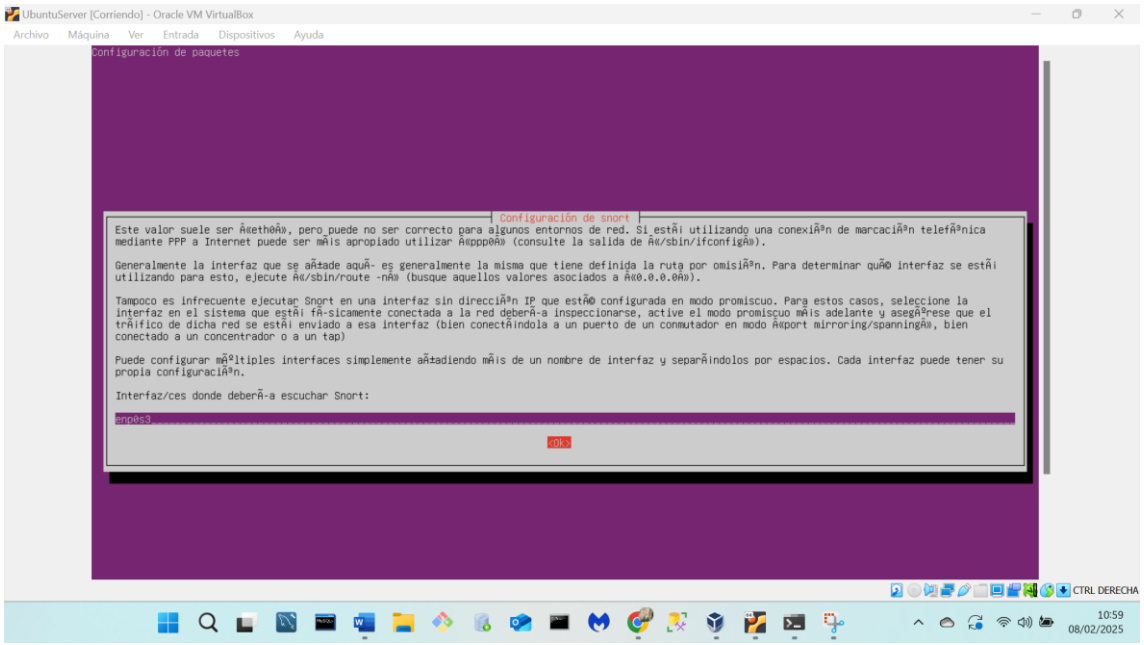
Procedemos a instalar y configurar SNORT en Ubuntu. Probé en Debian y en Docker, y me daban problemas.

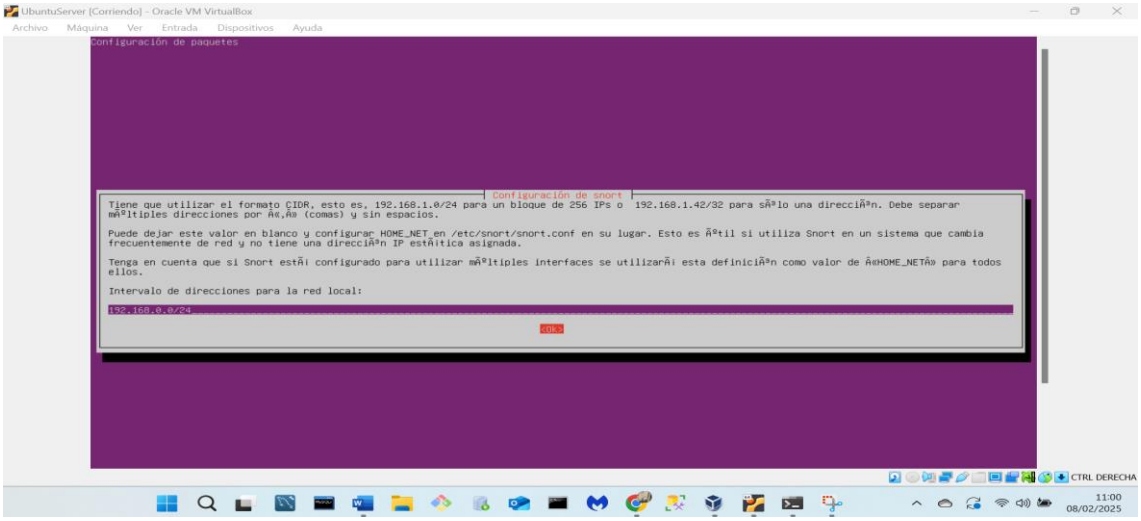


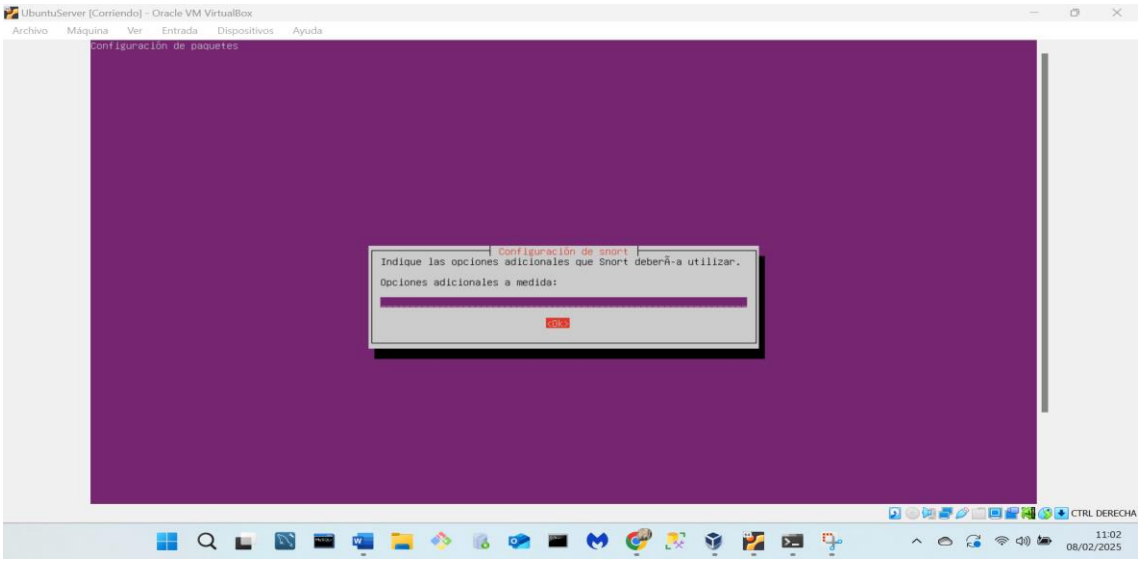


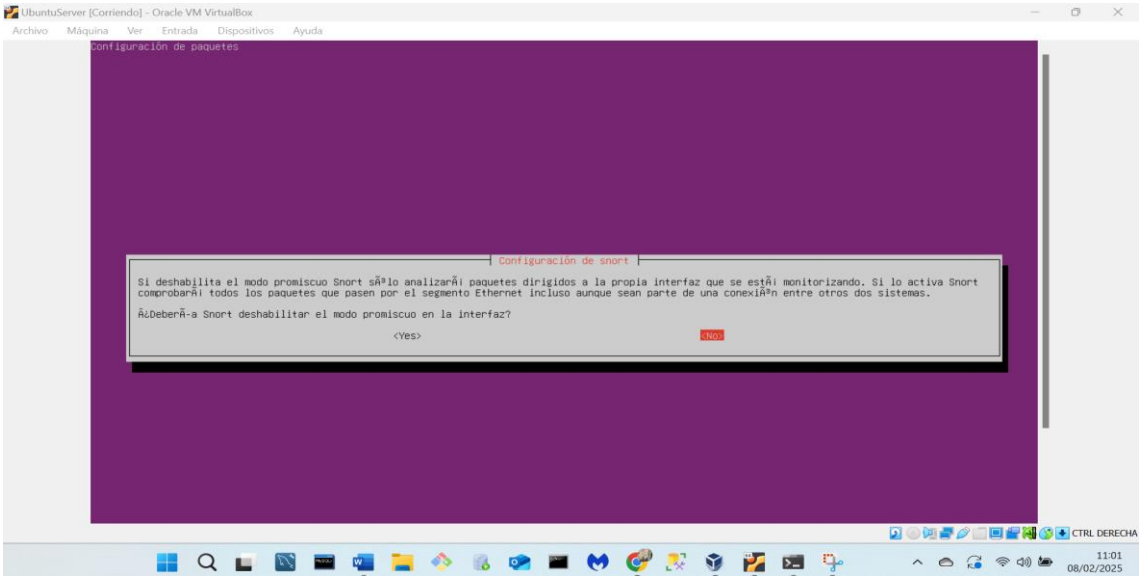

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@ivana:/etc/snort# dpkg-reconfigure snort

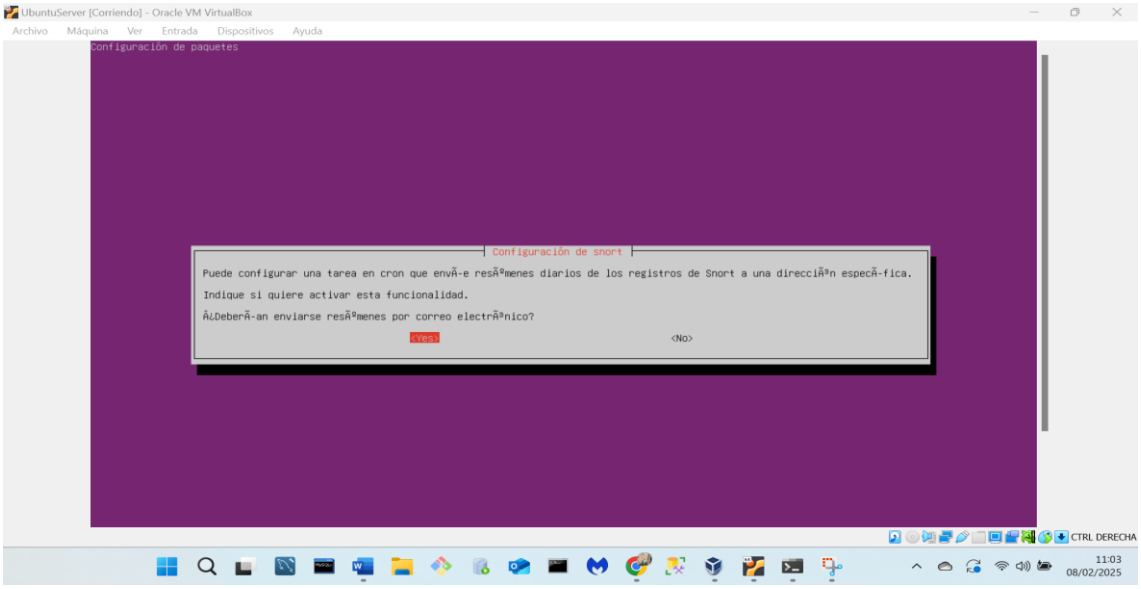

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Por favor, escoja cÃ³mo deberÃ-a arrancarse Snort: automÃ¡ticamente en el arranque del sistema, automÃ¡ticamente cuando el sistema se conecte a Internet con pppd o manualmente cuando lo arranque ejecutÃ¡ndolo con Â«/usr/sbin/snortÂ».
MÃ©todo de arranque de Snort:
arranque
marcaciÃ³n telefÃ³nica
manual
<Ok>
CTRL DERECHA
10:58
08/02/2025

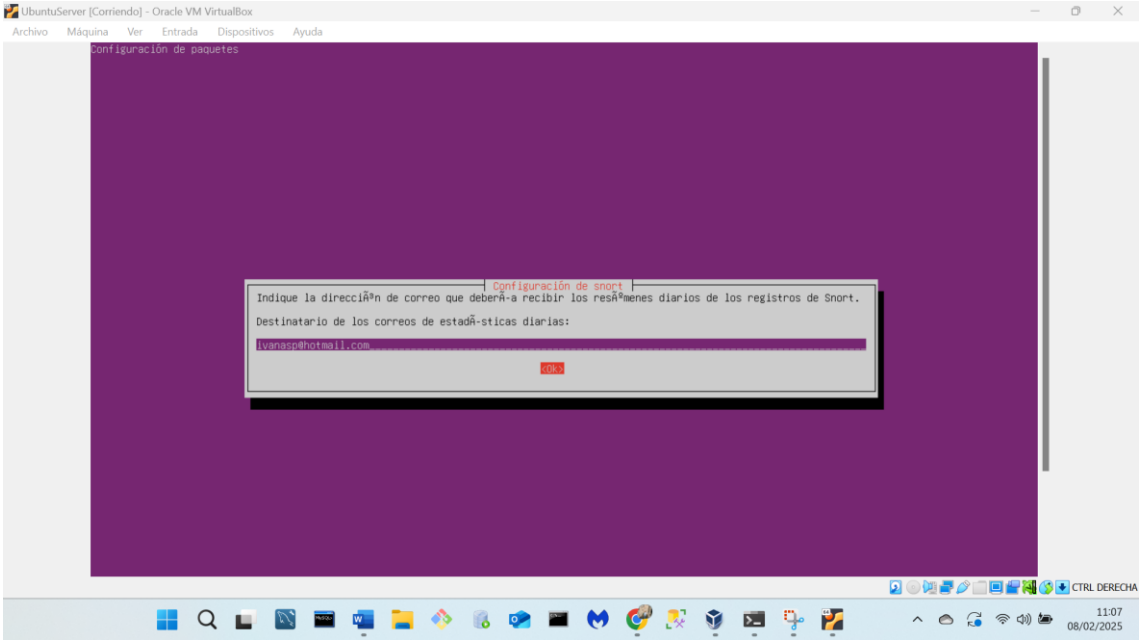

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Este valor suele ser Â«ethÃ0Â», pero puede no ser correcto para algunos entornos de red. Si estÃ¡ utilizando una conexiÃ³n de marcaciÃ³n telefÃ³nica mediante PPP a Internet puede ser mÃ¡s apropiado utilizar Â«pppÃ0Â» (consulte la salida de Â«/sbin/ifconfigÂ»).
Generalmente la interfaz que se aÃ±ade aquÃ- es generalmente la misma que tiene definida la ruta por omisiÃ³n. Para determinar quÃ© interfaz se estÃ¡ utilizando para esto, ejecute Â«/sbin/route -nÂ» (busque aquellos valores asociados a Â«0.0.0.0Â»).
Tampoco es infrecuente ejecutar Snort en una interfaz sin direcciÃ³n IP que estÃ© configurada en modo promiscuo. Para estos casos, seleccione la interfaz en el sistema que estÃ¡ fÃ-sicamente conectada a la red deberÃ-a inspeccionarse, active el modo promiscuo mÃ¡s adelante y asegÃºrese que el trÃ¡fico de dicha red se estÃ¡ enviado a esa interfaz (bien conectÃ¡ndola a un puerto de un conmutador en modo Â«port mirroring/spanningÂ», bien conectado a un concentrador o a un tap)
Puede configurar mÃºltiples interfaces simplemente aÃ±adiendo mÃ¡s de un nombre de interfaz y separÃ¡ndolos por espacios. Cada interfaz puede tener su propia configuraciÃ³n.
Interfaz/ces donde deberÃ-a escuchar Snort:
enp0s3
<Ok>
CTRL DERECHA
10:59
08/02/2025

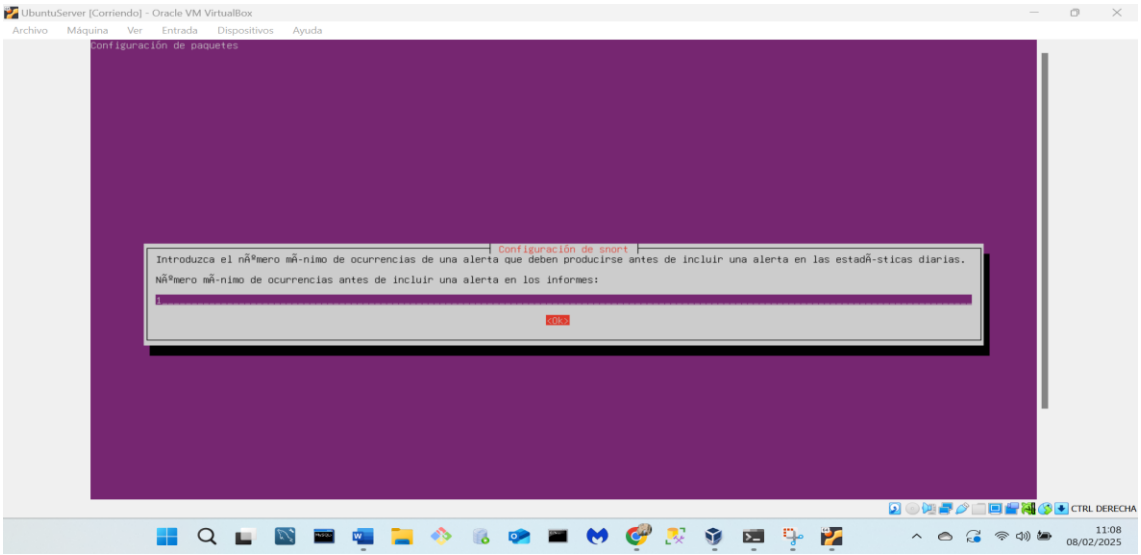

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Tiene que utilizar el formato CIDR, esto es, 192.168.1.0/24 para un bloque de 256 IPs o 192.168.1.42/32 para sÃ³lo una direcciÃ³n. Debe separar mÃºltiples direcciones por Â«,Â» (comas) y sin espacios.
Puede dejar este valor en blanco y configurar HOME_NET en /etc/snort/snort.conf en su lugar. Esto es Ãºtil si utiliza Snort en un sistema que cambia frecuentemente de red y no tiene una direcciÃ³n IP estÃ¡tica asignada.
Tenga en cuenta que si Snort estÃ¡ configurado para utilizar mÃºltiples interfaces se utilizarÃ¡ esta definiciÃ³n como valor de Â«HOME_NETÂ» para todos ellos.
Intervalo de direcciones para la red local:
192.168.0.0/24
<Ok>
CTRL DERECHA
11:00
08/02/2025


UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Indique las opciones adicionales que Snort deberÃ-a utilizar.
Opciones adicionales a medida:
<Ok>
CTRL DERECHA
11:02
08/02/2025

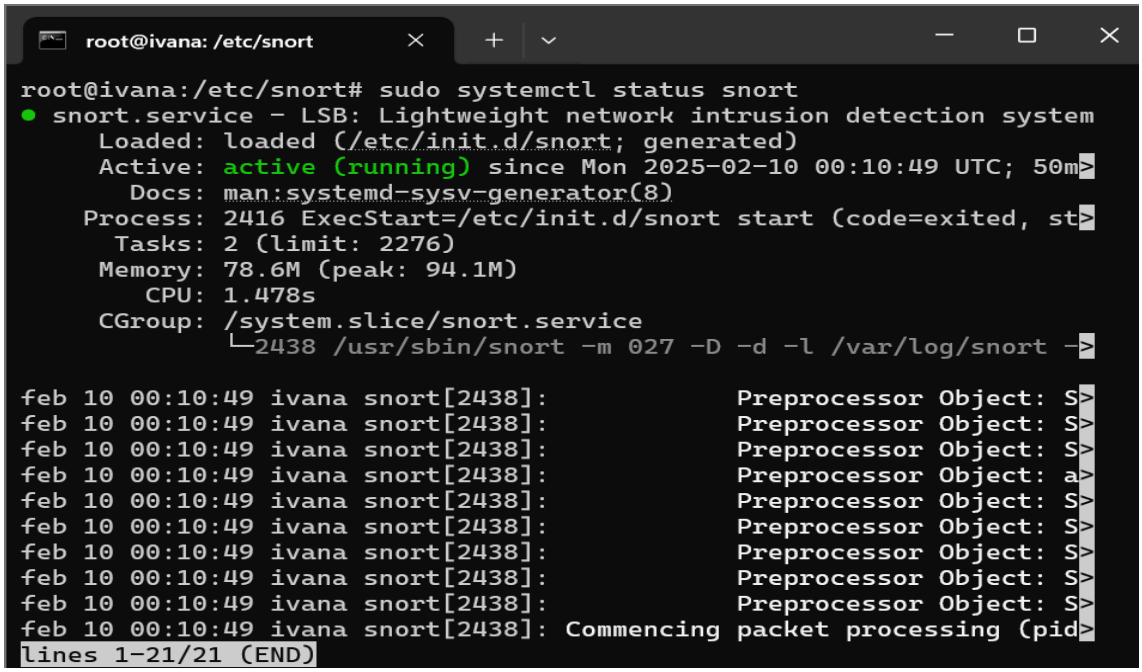

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Si deshabilita el modo promiscuo Snort sÃ³lo analizarÃ¡ paquetes dirigidos a la propia interfaz que se estÃ¡ monitorizando. Si lo activa Snort comprobarÃ¡ todos los paquetes que pasen por el segmento Ethernet incluso aunque sean parte de una conexiÃ³n entre otros dos sistemas.
Â¿DeberÃ-a Snort deshabilitar el modo promiscuo en la interfaz?
<Yes>
<No>
CTRL DERECHA
11:01
08/02/2025


UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Puede configurar una tarea en cron que envÃ-e resÃºmenes diarios de los registros de Snort a una direcciÃ³n especÃ-fica.
Indique si quiere activar esta funcionalidad.
Â¿DeberÃ-an enviarse resÃºmenes por correo electrÃ³nico?
<Yes>
<No>
CTRL DERECHA
11:03
08/02/2025

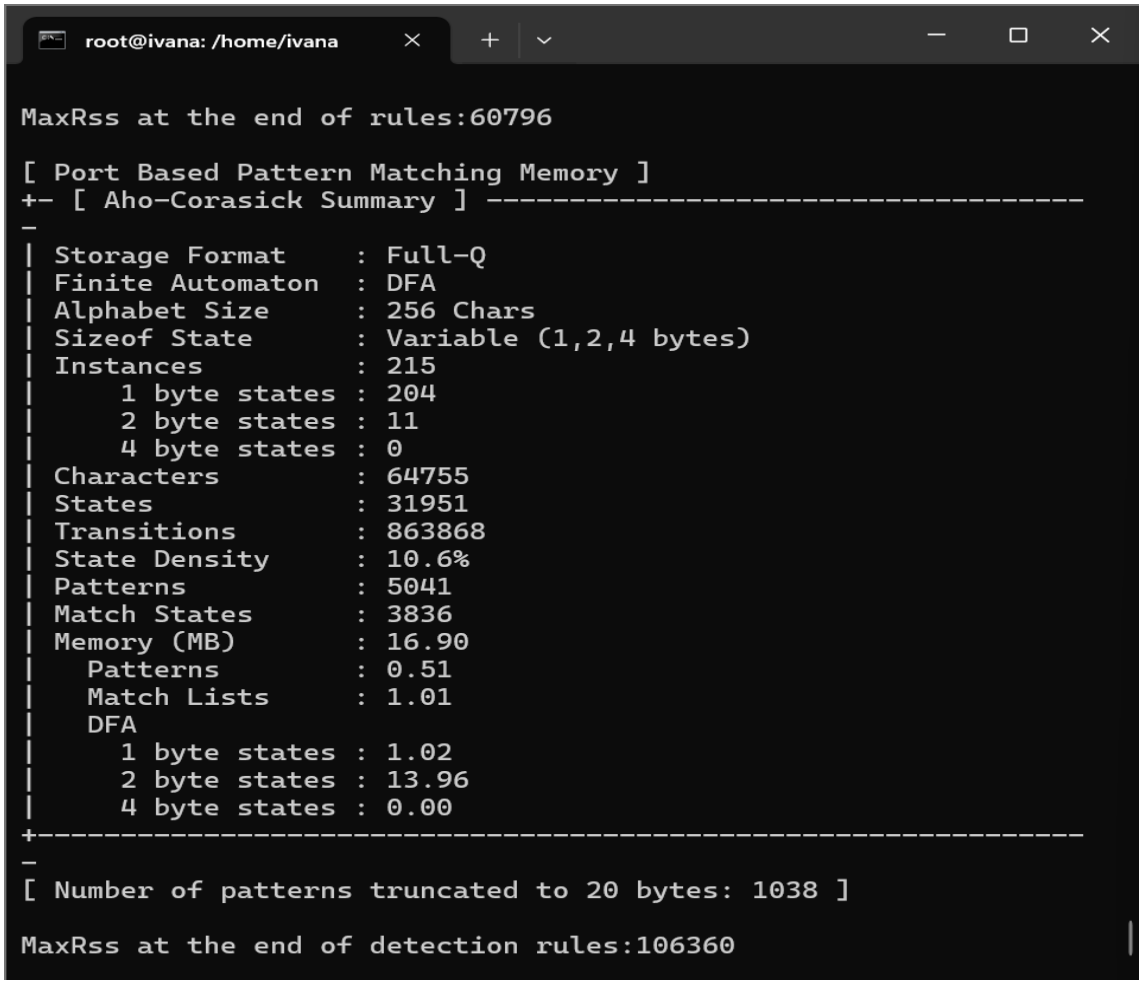

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Indique la direcciÃ³n de correo que deberÃ-a recibir los resÃºmenes diarios de los registros de Snort.
Destinatario de los correos de estadÃ-sticas diarias:
ivanasp@hotmail.com
<Ok>
CTRL DERECHA
11:07
08/02/2025

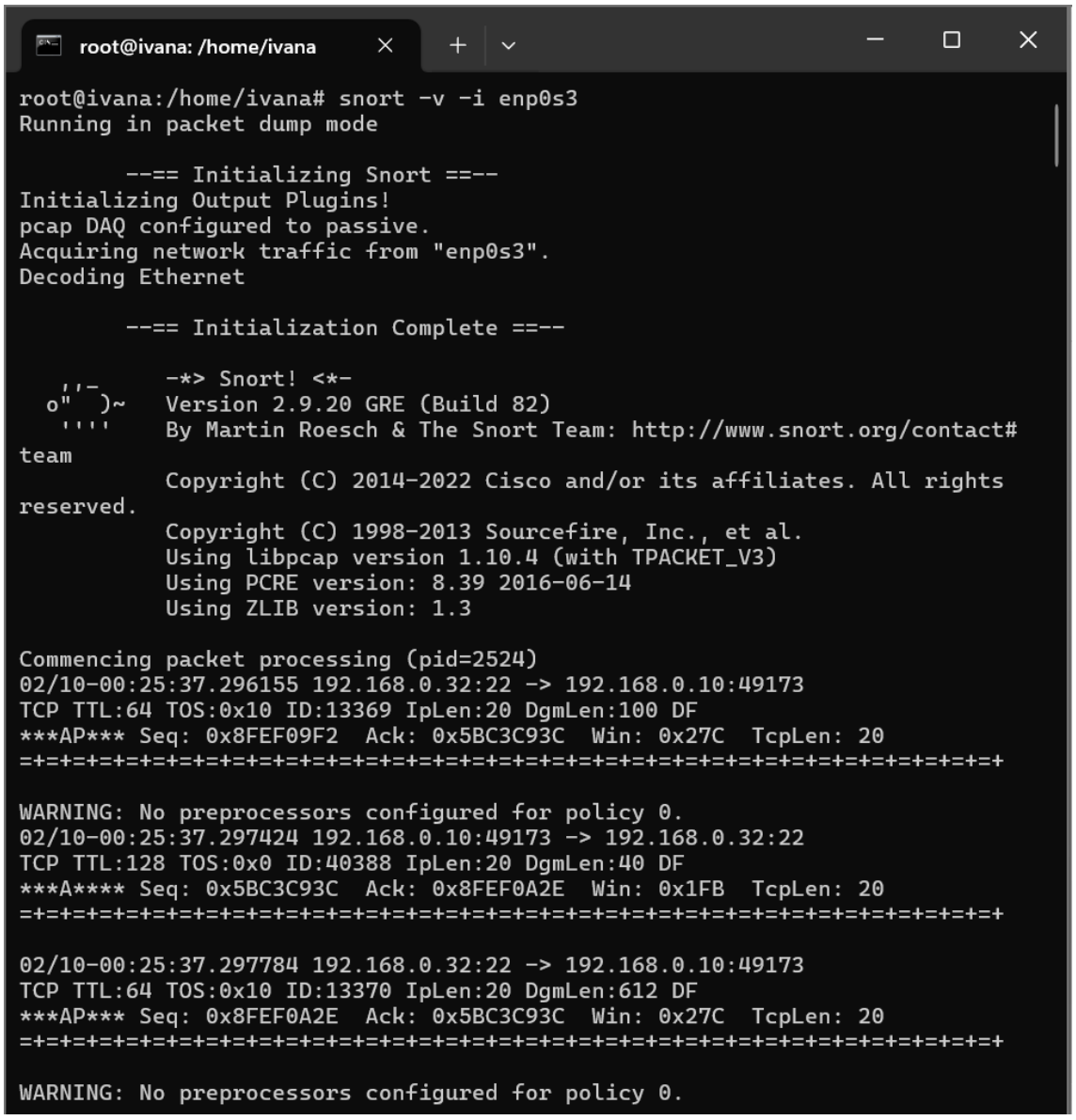

UbuntuServer [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Configuración de paquetes
Configuración de snort
Introduzca el nÃºmero mÃ-nimo de ocurrencias de una alerta que deben producirse antes de incluir una alerta en las estadÃ-sticas diarias.
NÃºmero mÃ-nimo de ocurrencias antes de incluir una alerta en los informes:
1
<Ok>
CTRL DERECHA
11:08
08/02/2025

Comprobamos que el servicio esté corriendo correctamente.

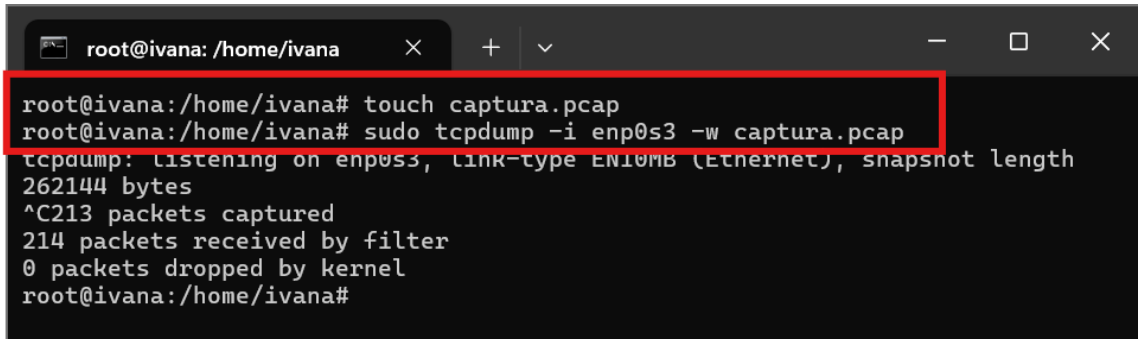


Pruebo la configuración con sudo snort -T -c /etc/snort/snort.conf

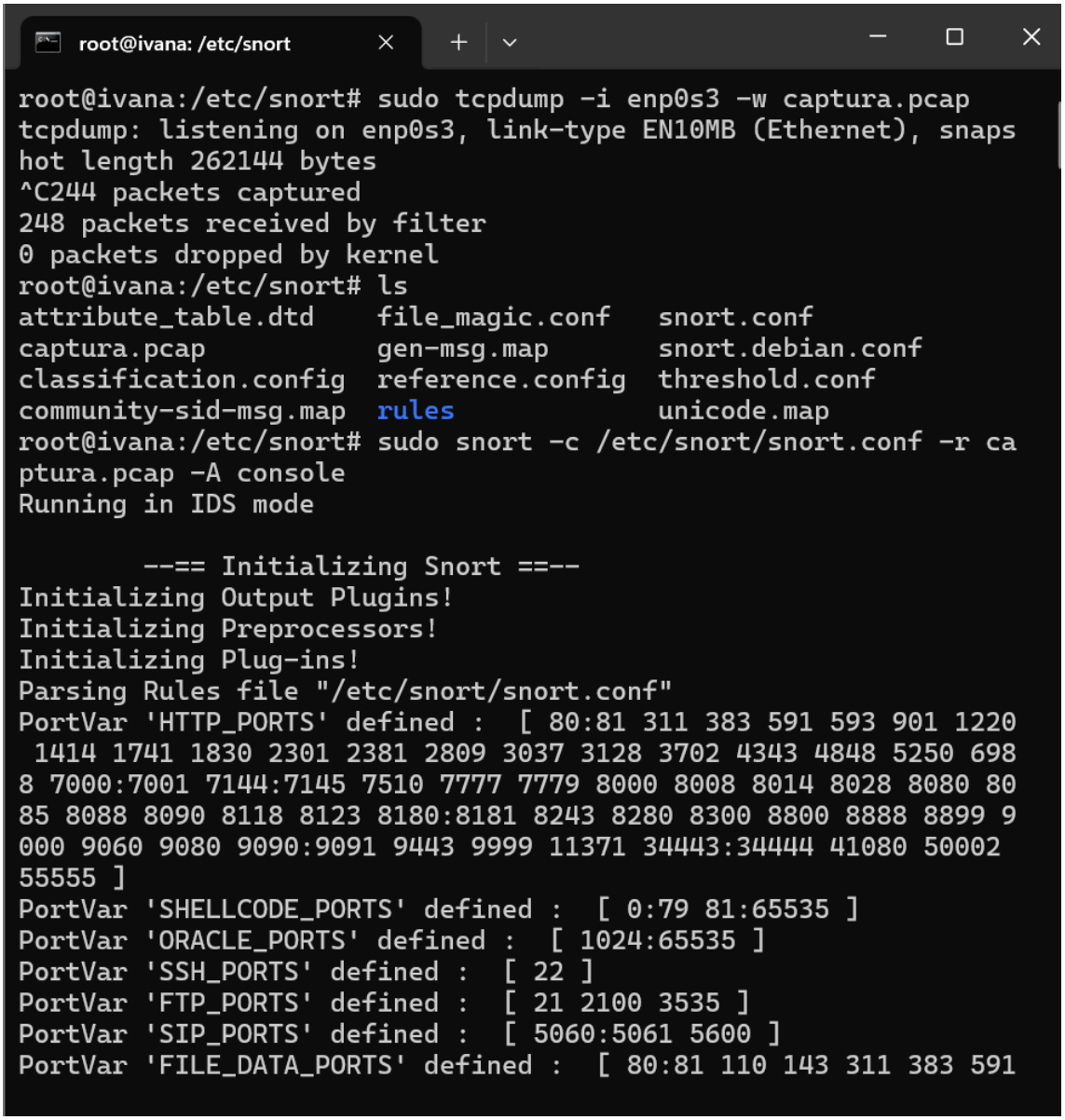




Creamos el archivo ***captura.pcap*** para capturar tráfico y guardarlo en un archivo ***.pcap.***

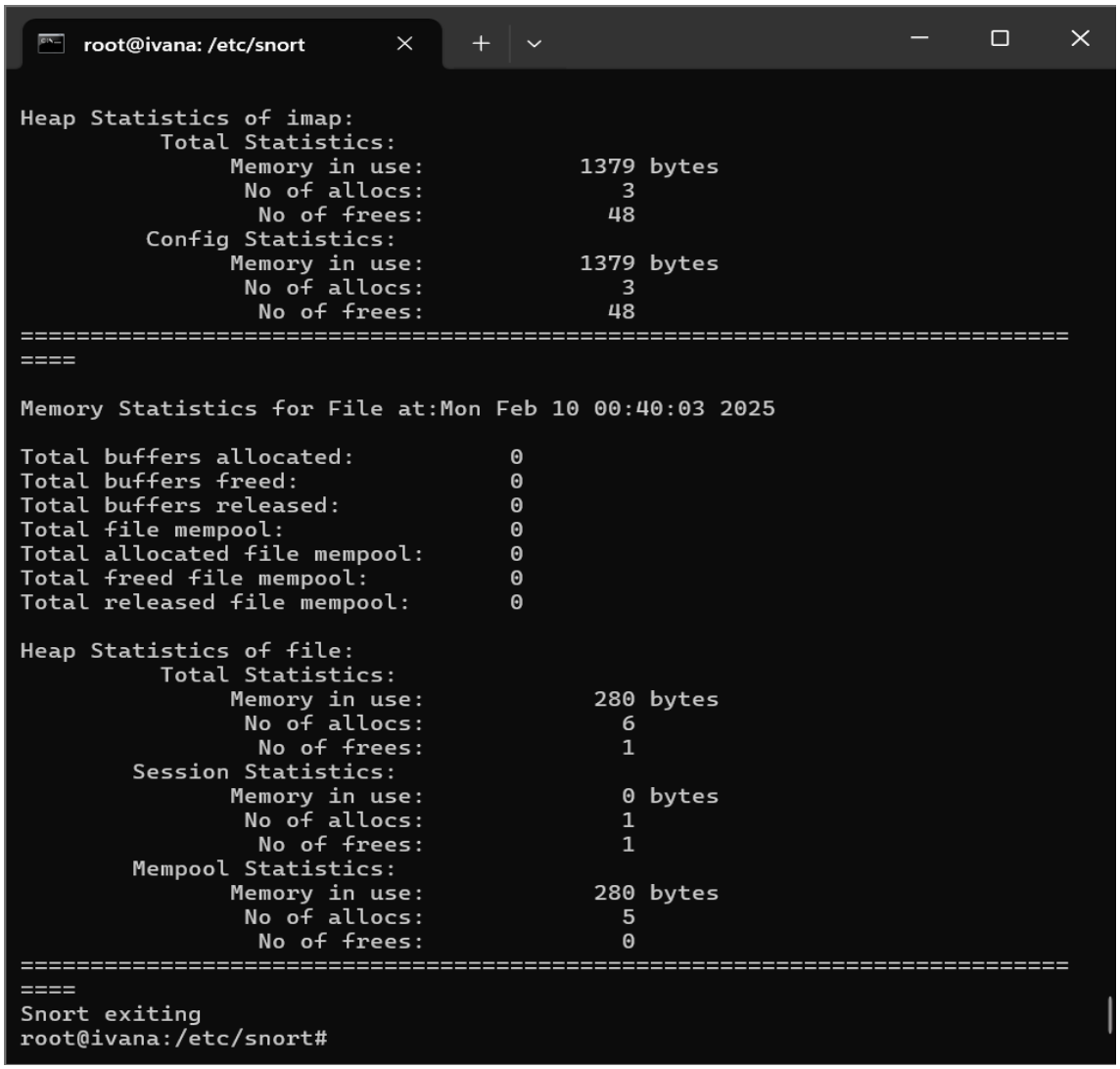


Y podemos hacer las consultas con el comando ***sudo snort -c /etc/snort/snort.conf -r captura.pcap -A console***

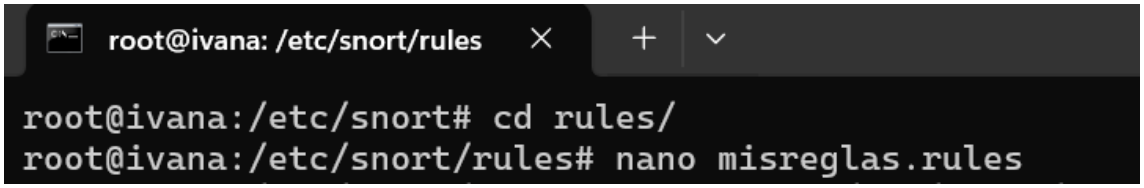


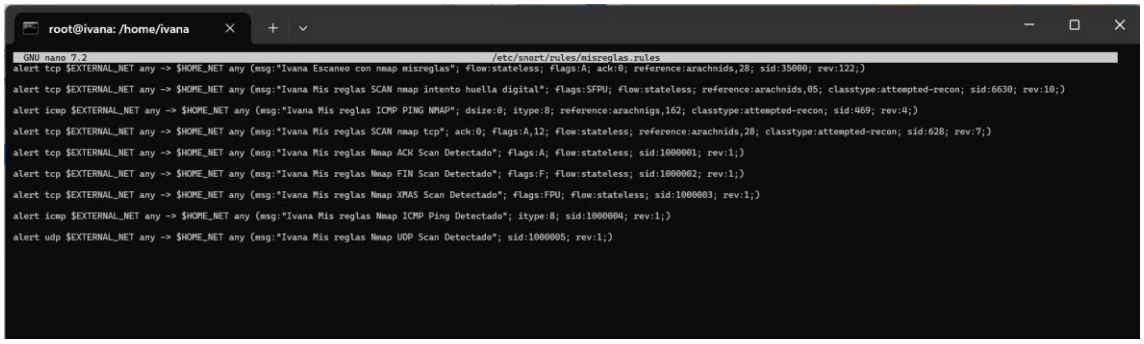
Vuelvo a realizar el escaneo general para confirmar el funcionamiento de snort

Con ***root@ivana:/etc/snort# sudo snort -c /etc/snort/snort.conf -r captura.pcap -A console***

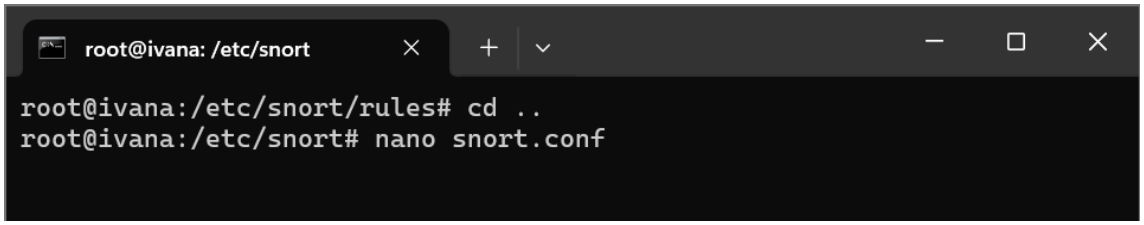


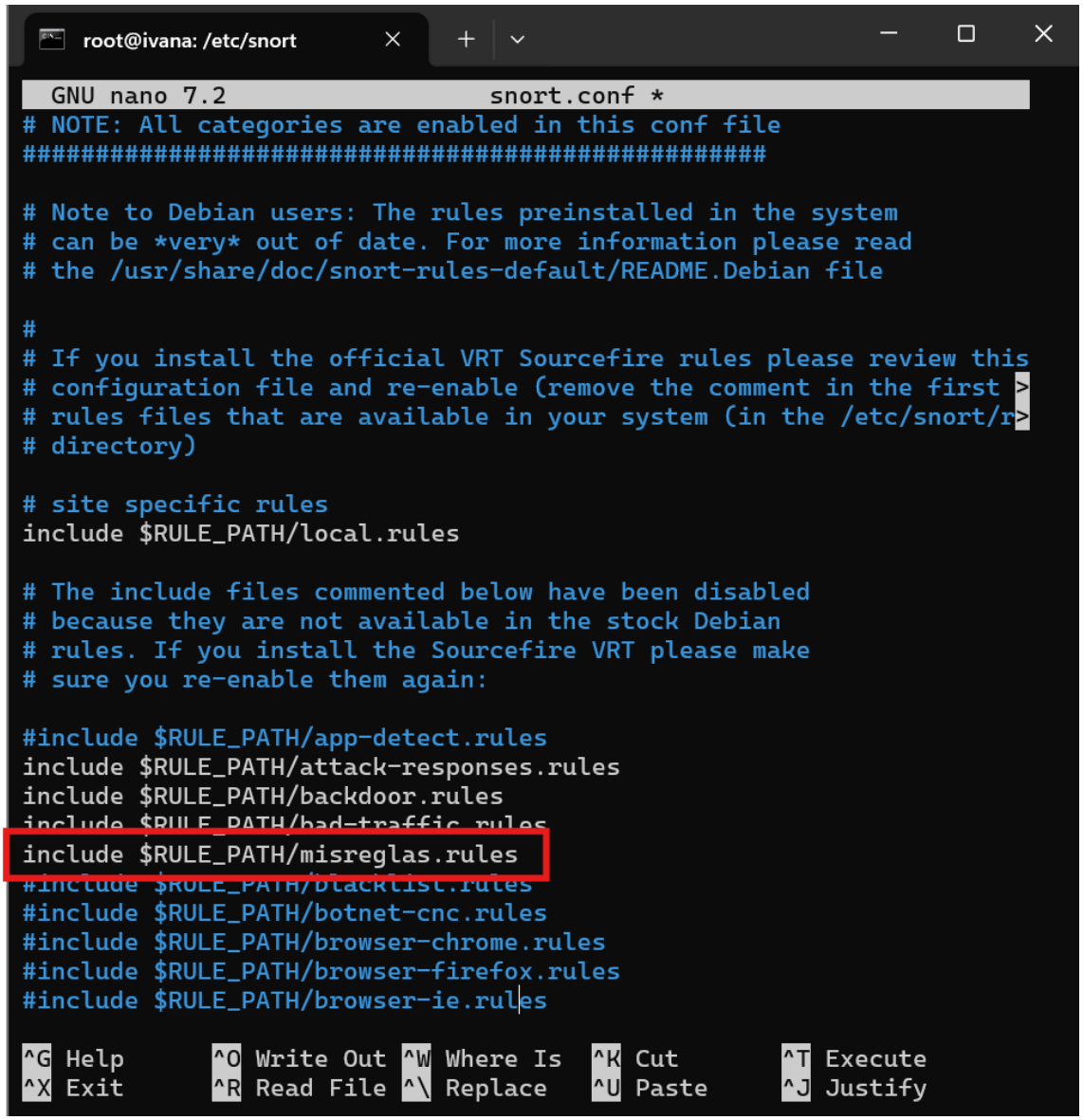
Nos colocamos en **/etc/snort/rules** y creamos el archivo **misreglas.rules**

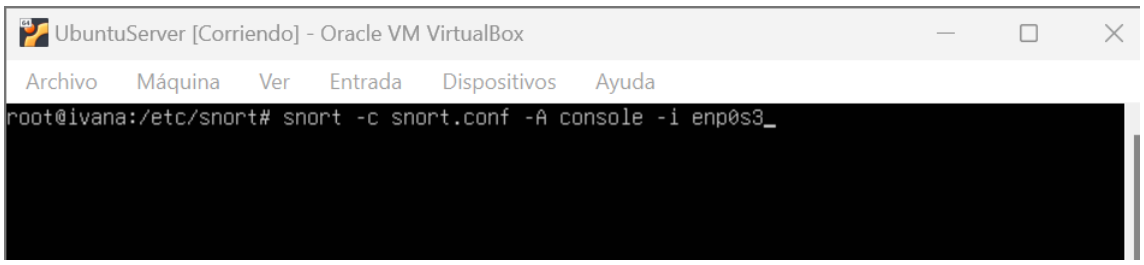


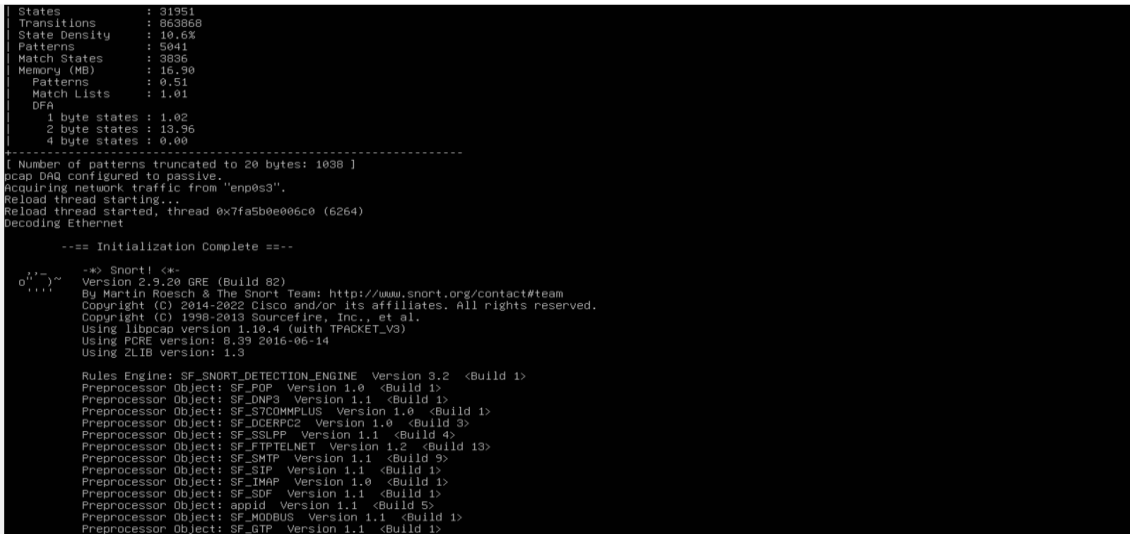


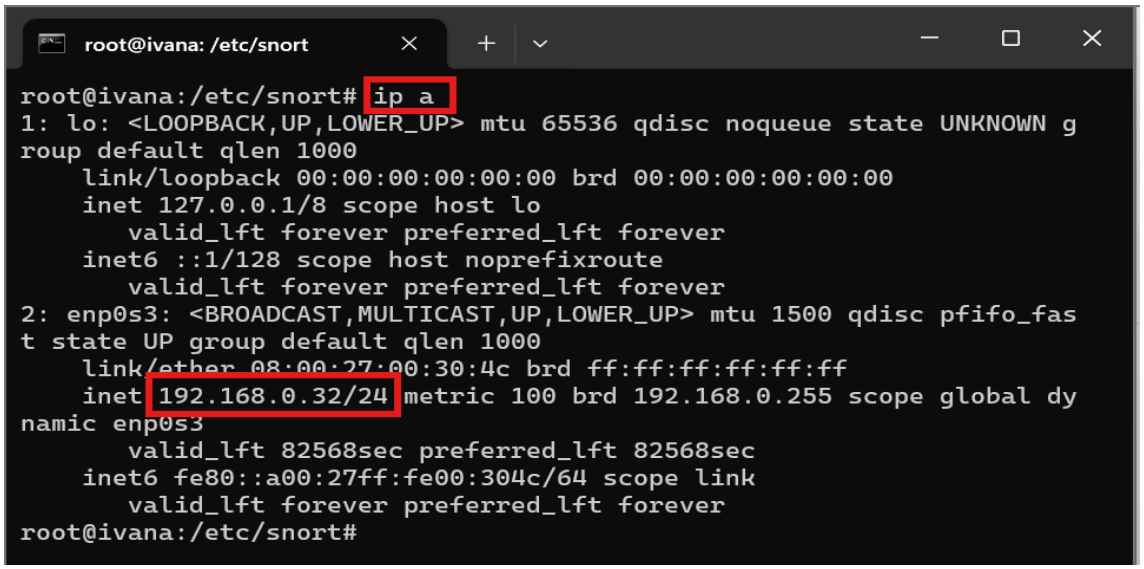
Y ahora nos vamos al archivo de configuración de snort para modificarlo añadiéndole la ruta del archivo **misreglas.rules**

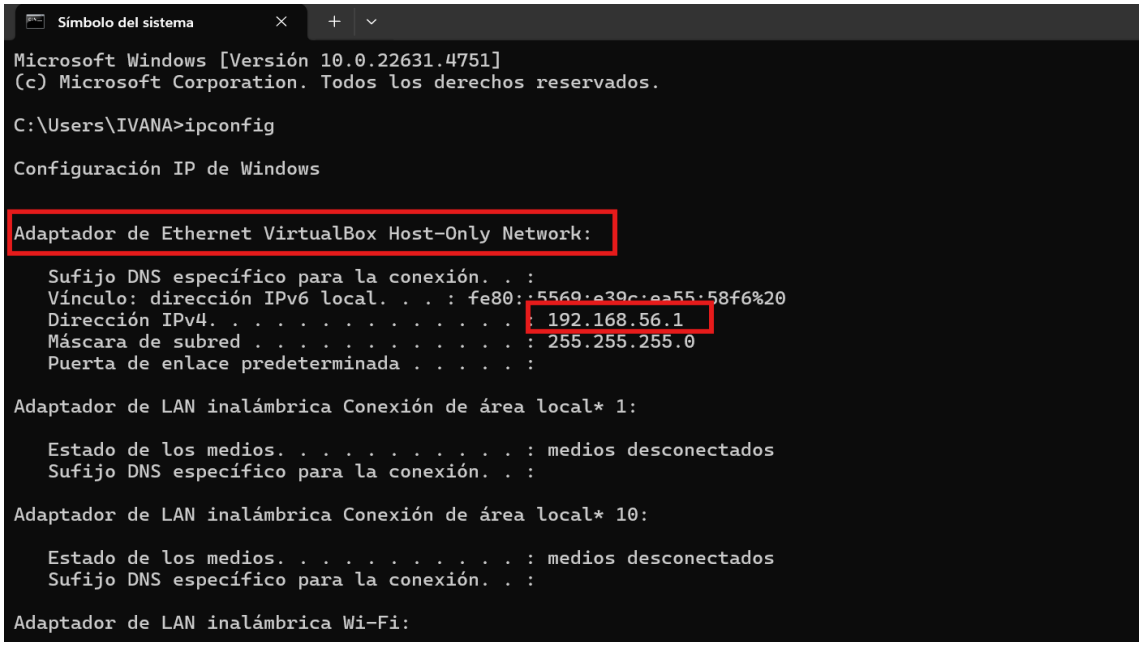






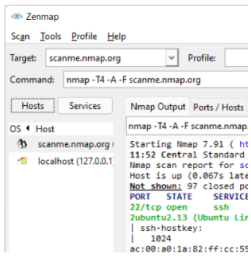

| States : 31951
| Transitions : 863868
| State Density : 10.6%
| Patterns : 5041
| Match States : 3836
| Memory (MB) : 16.90
| Patterns : 0.51
| Match Lists : 1.01
| DFA
| 1 byte states : 1.02
| 2 byte states : 13.96
| 4 byte states : 0.00
[Number of patterns truncated to 20 bytes: 1038]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7fa5b0e006c0 (6264)
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>


root@ivana: /etc/snort
root@ivana:/etc/snort# ip a
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 pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:00:30:4c brd ff:ff:ff:ff:ff:ff
inet 192.168.0.32/24 metric 100 brd 192.168.0.255 scope global dynamic enp0s3
valid_lft 82568sec preferred_lft 82568sec
inet6 fe80::a00:27ff:fe00:304c/64 scope link
valid_lft forever preferred_lft forever
root@ivana:/etc/snort#


Símbolo del sistema
Microsoft Windows [Versión 10.0.22631.4751]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\IVANA>ipconfig
Configuración IP de Windows
Adaptador de Ethernet VirtualBox Host-Only Network:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::5569:e39c:ea55:58f6%20
Dirección IPv4. . . . . : 192.168.56.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
Adaptador de LAN inalámbrica Conexión de área local* 1:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Conexión de área local* 10:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Wi-Fi:

Instalo **NMAP** en Windows

Archivos binarios de Microsoft Windows



Lea la sección de Windows de la Guía de instalación para conocer las limitaciones e instrucciones de instalación de la versión de Windows de Nmap. Se proporciona como un autoinstalador ejecutable que incluye las dependencias de Nmap y la interfaz gráfica de usuario de Zenmap. Ofrecemos soporte para Nmap en Windows 7 y versiones posteriores, así como en Windows Server 2008 R2 y versiones posteriores. También mantenemos una guía para los usuarios que deben ejecutar Nmap en versiones anteriores de Windows .

Nota: La versión de Npcap incluida en nuestros instaladores puede no ser siempre la última versión. Si tiene problemas o simplemente desea la última y mejor versión, descargue e instale la última versión de Npcap.

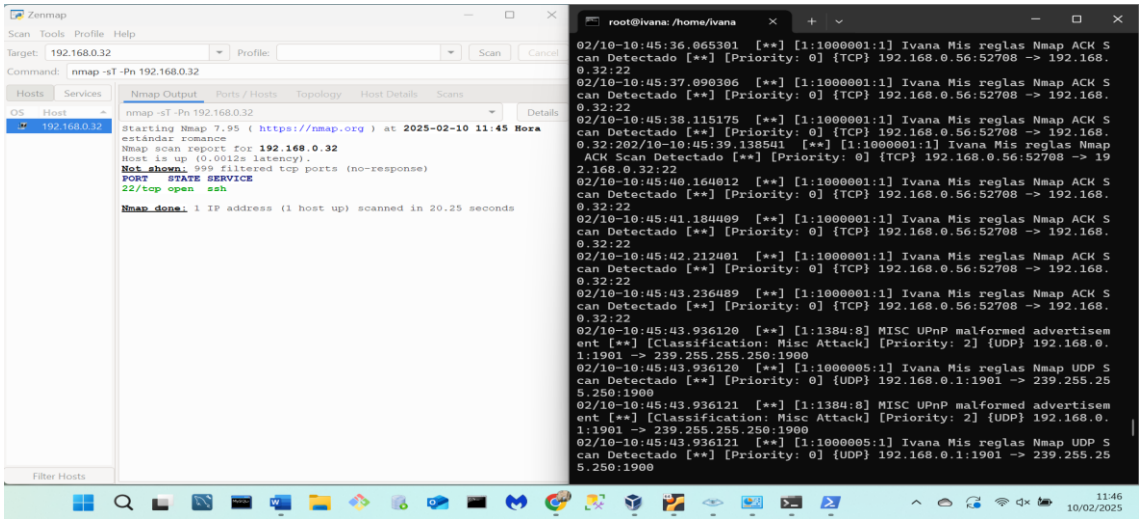
Última versión estable del instalador automático: nmap-7.95-setup.exe
Última versión estable del instalador automático: npcap-1.80.exe

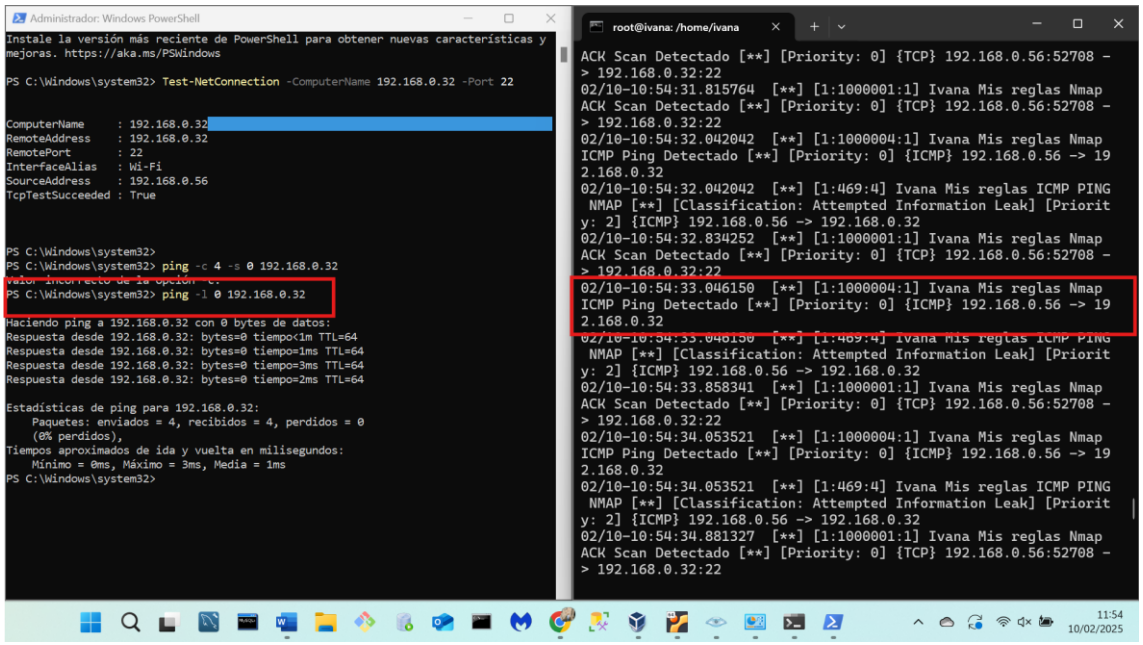
Hemos redactado instrucciones de uso posteriores a la instalación . Notifíquenos si tiene algún problema o sugerencias para el instalador.

Fuentes y binarios de RPM para Linux

Iniciamos snort con **snort -c /etc/snort/snort.conf -i enp0s3 -A console** o con

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3




Administrador: Windows PowerShell
Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows
PS C:\Windows\system32> Test-NetConnection -ComputerName 192.168.0.32 -Port 22
ComputerName : 192.168.0.32
RemoteAddress : 192.168.0.32
RemotePort : 22
InterfaceAlias : Wi-Fi
SourceAddress : 192.168.0.56
TcpTestSucceeded : True
PS C:\Windows\system32>
PS C:\Windows\system32> ping -c 4 -s 0 192.168.0.32
PS C:\Windows\system32> ping -l 0 192.168.0.32
Haciendo ping a 192.168.0.32 con 0 bytes de datos:
Respuesta desde 192.168.0.32: bytes=0 tiempo<1m TTL=64
Respuesta desde 192.168.0.32: bytes=0 tiempo=1ms TTL=64
Respuesta desde 192.168.0.32: bytes=0 tiempo=3ms TTL=64
Respuesta desde 192.168.0.32: bytes=0 tiempo=2ms TTL=64
Estadísticas de ping para 192.168.0.32:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 3ms, Media = 1ms
PS C:\Windows\system32>
root@ivana: /home/ivana
ACK Scan Detectado [**] [Priority: 0] {TCP} 192.168.0.56:52708 -> 192.168.0.32:22
02/10-10:54:31.815764 [**] [1:1000001:1] Ivana Mis reglas Nmap ACK Scan Detectado [**] [Priority: 0] {TCP} 192.168.0.56:52708 -> 192.168.0.32:22
02/10-10:54:32.042042 [**] [1:1000004:1] Ivana Mis reglas Nmap ICMP Ping Detectado [**] [Priority: 0] {ICMP} 192.168.0.56 -> 192.168.0.32
02/10-10:54:32.042042 [**] [1:469:4] Ivana Mis reglas ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.0.56 -> 192.168.0.32
02/10-10:54:32.834252 [**] [1:1000001:1] Ivana Mis reglas Nmap ACK Scan Detectado [**] [Priority: 0] {TCP} 192.168.0.56:52708 -> 192.168.0.32:22
02/10-10:54:33.046150 [**] [1:1000004:1] Ivana Mis reglas Nmap ICMP Ping Detectado [**] [Priority: 0] {ICMP} 192.168.0.56 -> 192.168.0.32
02/10-10:54:33.046150 [**] [1:469:4] Ivana Mis reglas ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.0.56 -> 192.168.0.32
02/10-10:54:33.858341 [**] [1:1000001:1] Ivana Mis reglas Nmap ACK Scan Detectado [**] [Priority: 0] {TCP} 192.168.0.56:52708 -> 192.168.0.32:22
02/10-10:54:34.053521 [**] [1:1000004:1] Ivana Mis reglas Nmap ICMP Ping Detectado [**] [Priority: 0] {ICMP} 192.168.0.56 -> 192.168.0.32
02/10-10:54:34.053521 [**] [1:469:4] Ivana Mis reglas ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.0.56 -> 192.168.0.32
02/10-10:54:34.881327 [**] [1:1000001:1] Ivana Mis reglas Nmap ACK Scan Detectado [**] [Priority: 0] {TCP} 192.168.0.56:52708 -> 192.168.0.32:22
11:54
10/02/2025