Universidad Interamericana de Puerto Rico Recinto de Arecibo

COMP 2700 Cybersecurity Sección #92249

Prof. Eli S. Quintana

Instalación y Configuración de un Sistema de Detección de Intrusos (IDS) con Suricata

Fecha de entrega: 5 de diciembre de 2025

Miembros del equipo:

Benyahir Y. Martínez

Jacob J. Desuza

Emanuel V. Rodríguez

John A. Valentín

Desarrollo Teórico:

1. Definición de IDS

- ¿Qué es un Sistema de Detección de Intrusos (IDS)?

  Un IDS es una herramienta de seguridad que se encarga de monitorear el tráfico y los dispositivos de la red con el propósito de conseguir actividades maliciosas o infracciones en la política de la seguridad. El IDS ayuda en acelerar y automatizar la detección de vulnerabilidades en una red mediante alertas a los administradores de la red.

- Diferencia entre IDS y IPS.

  Un IPS es un componente activo de la red que examina cada paquete que pasa y toma las medidas correctivas en función de su configuración y política. Al contrario, un IDS es un componente pasivo que generalmente no se implementa en línea, y en cambio, monitorea el flujo del tráfico con una tecnología de SPAN o TAP para emitir notificaciones.

- Ejemplo de uso real en entornos empresariales.

  Un ejemplo del uso de los IDS en entornos empresariales seria la utilización de este en un centro de datos. Los centros de datos emplean el IDS para vigilar la actividad en segmentos específicos como los servidores web, bases de datos y sistemas de autenticación.

2. Comparación entre Snort y Suricata

- Ventajas y desventajas de cada uno.

  + Ventajas de Snort: multiplataforma, gratuito, manual y comunidad de apoyo, reglas actualizadas y personalizables, bajos requisitos necesarios y disponibilidad de interfaz web.

  - Desventajas de Snort: Dificultad de aprendizaje, no tiene GUI disponible, configuración especial para falsos positivos, saturación de información debido a tener reglas de base de dato muy amplias, no está enfocado a entornos grandes, no está diseñado para infraestructuras modernas.

+ Ventajas de Suricata: Multiplataforma, gratuito, contiene manual de usuario y desarrollo, reglas actualizadas y personalizables, mayor precisión que otros IDS y escalabilidad.

- Desventajas de Suricata: Mayor uso de recursos (CPU y RAM), obtención de mayor numero de falsos positivos posibilidad de positivos grises.

- Entornos recomendados para su implementación.

  Snort y Suricata se pueden implementar en varios entornos como: redes corporativas y empresariales, instituciones educativas, laboratorios de ciberseguridad y entornos domésticos.

3. Análisis de Logs y Detección de Ataques

- ¿Cómo se registran los eventos?

  Los eventos se registran a través de los logs de seguridad, donde se guarda una variedad de información como: fecha y hora del evento, usuario que realizo la acción, dirección IP o ubicación, tipo de evento, resultado de la acción y descripción.

- ¿Qué tipo de ataques puede detectar cada sistema?

  Se pueden detectar diferentes ataques a través de los logs como, por ejemplo: ataques de fuerza bruta, movimientos laterales, exfiltración de datos, malware y configuraciones cambiadas.

- Ejemplo de alertas o logs típicos.

```
Nov 17 04:19:52 cylon3 systemd: Stopping The Apache HTTP
Server...
Nov 17 04:19:53 cylon3 systemd: Stopped The Apache HTTP
Server.
Nov 17 04:19:54 cylon3 systemd: Starting The Apache HTTP
Server...
Nov 17 04:19:54 cylon3 httpd: AH00558: httpd: Could not
reliably determine the server's fully qualified domain
```

```
name, using fe80::4637:e6ff:fedd:fa27. Set the 'ServerName'
directive globally to suppress this message
```

4. Preguntas de análisis

- ¿Por qué seleccionaron Snort o Suricata para su proyecto?

  Se selecciono la herramienta de Suricata para realizar el proyecto ya que luego de realizar una comparación entre las dos herramientas, Suricata fue la mejor opción ya que Snort en algunos aspectos se está quedando atrás debido a los suportes que no provee y la falta de apoyo a estructuras modernas.

- ¿Qué configuraciones básicas realizaron y por qué son importantes?

  Hubo 3 cambios notables que realizaron en las configuraciones fueron la dirección de la HOME_NET y las interfaces para af-packet y pfring. El cambio de la dirección IP que tenía la HOME_NET tenía que realizarse ya que definía la red confiable para las reglas de suricata lo que permitía diferenciar el tráfico interno legítimo del externo malicioso. Para la

- ¿Qué aprendieron del proceso de instalación y análisis?

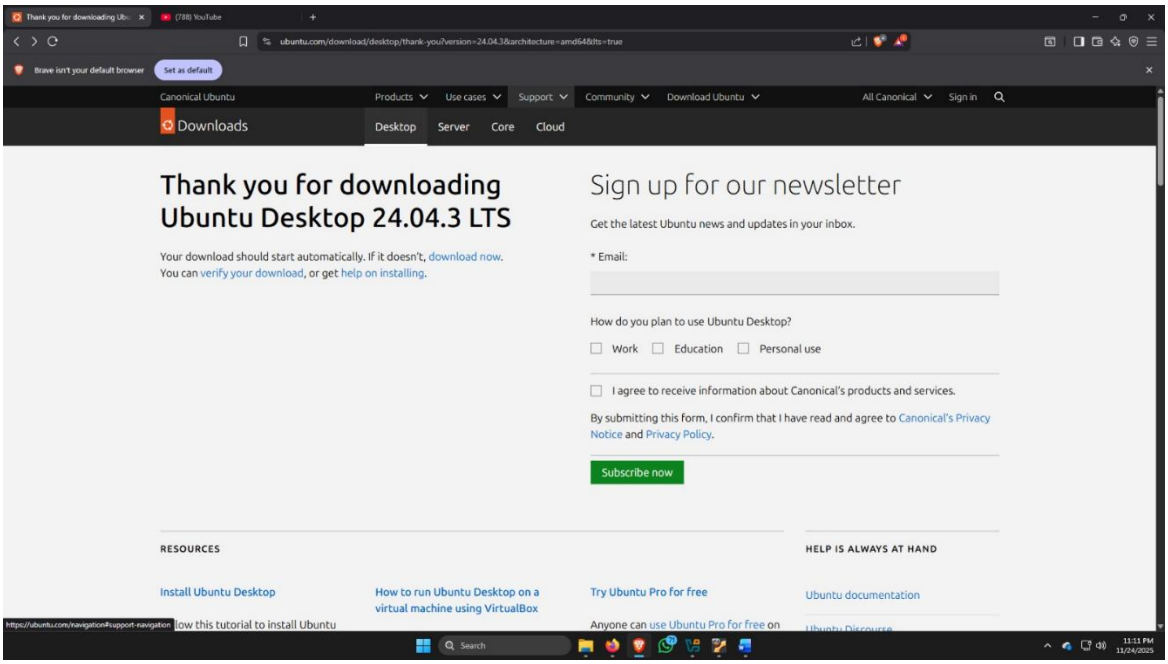
  Durante el proceso de este proyecto logramos comprender y reforzarnos en varios aspectos del análisis de datos. Tuvimos la oportunidad de reforzar nuestras habilidades creando máquinas virtuales con sus respectivas imágenes. Como grupo escogimos Suricata como herramienta para analizar el tráfico de red, pudimos observar cómo se registran actividades por más mínimas que sean.

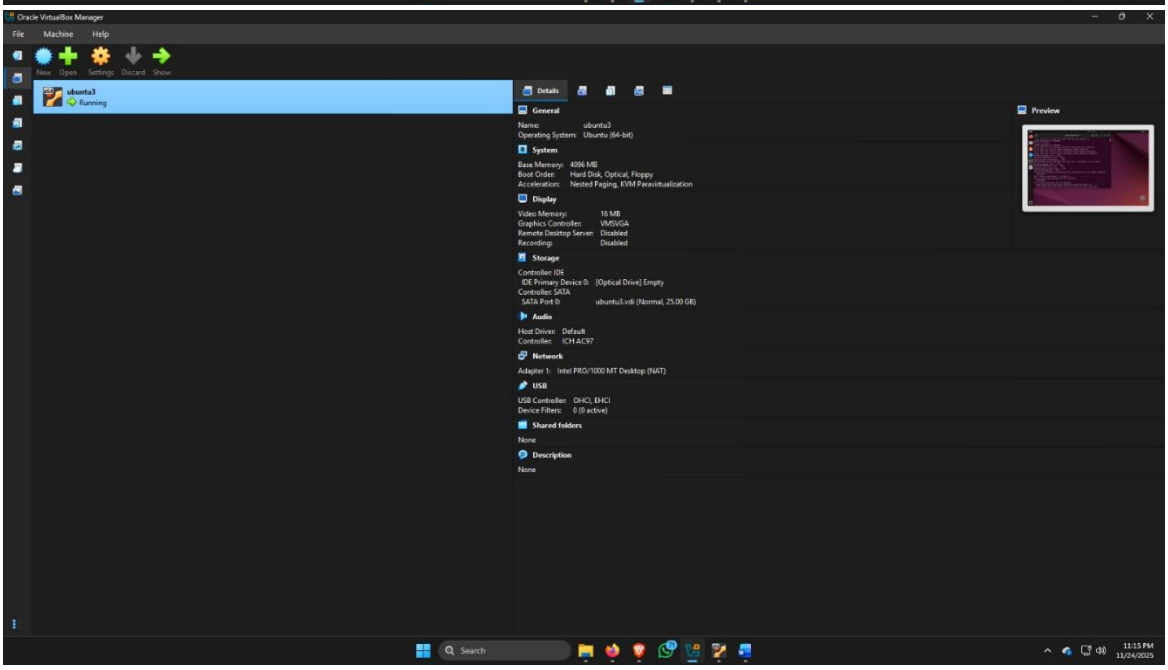
- ¿Qué mejoras implementarían si tuvieran más tiempo o recursos?

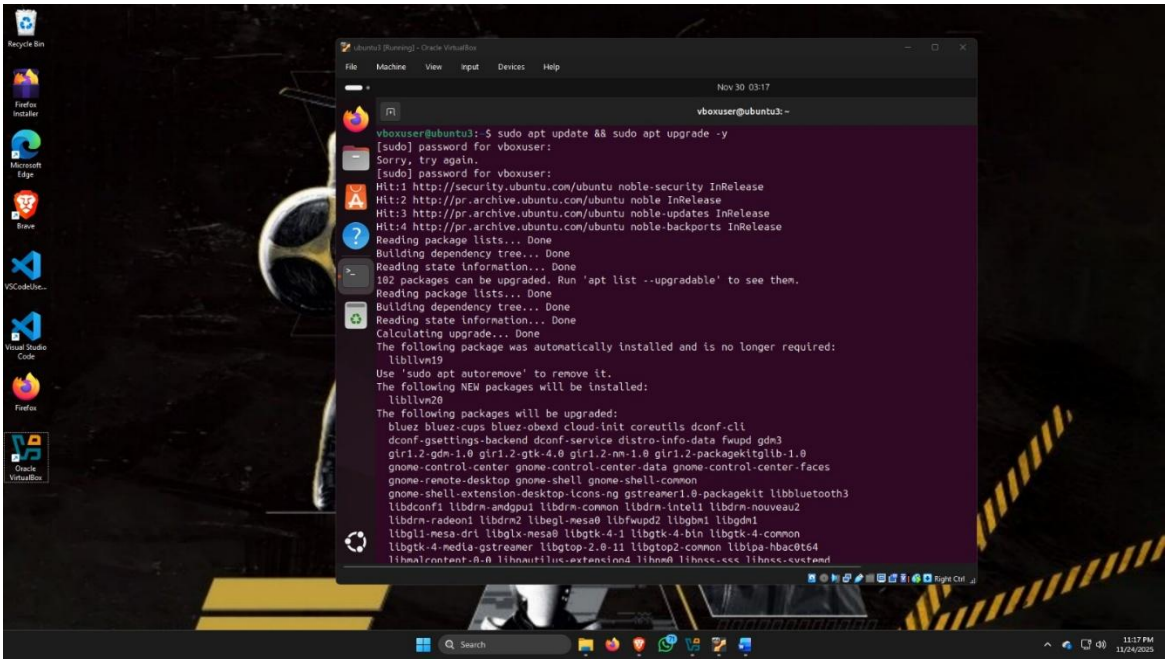
  Si tuviéramos tenido más conocimiento y tiempo implementaríamos una herramienta de IPS. Este permitiría no tan solo detectar cualquier tipo de tráfico está ocurriendo en el momento, pero también tomaría las medidas necesarias para bloquear este si estuviese lidiando con tráfico malicioso.

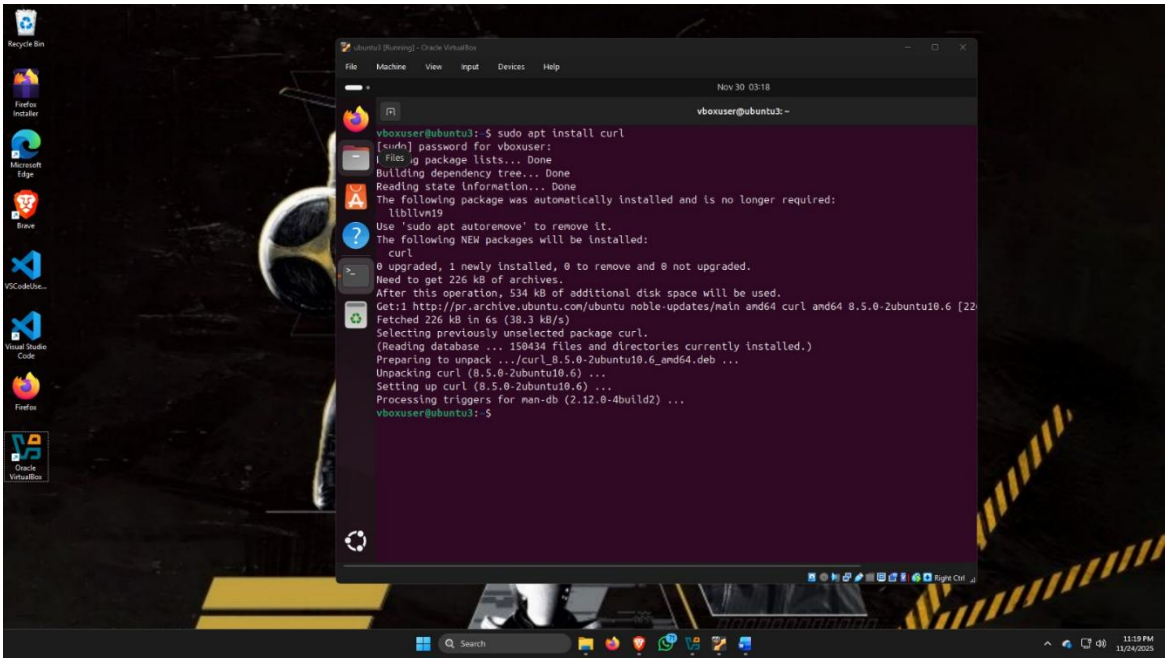
Desarrollo Practico:

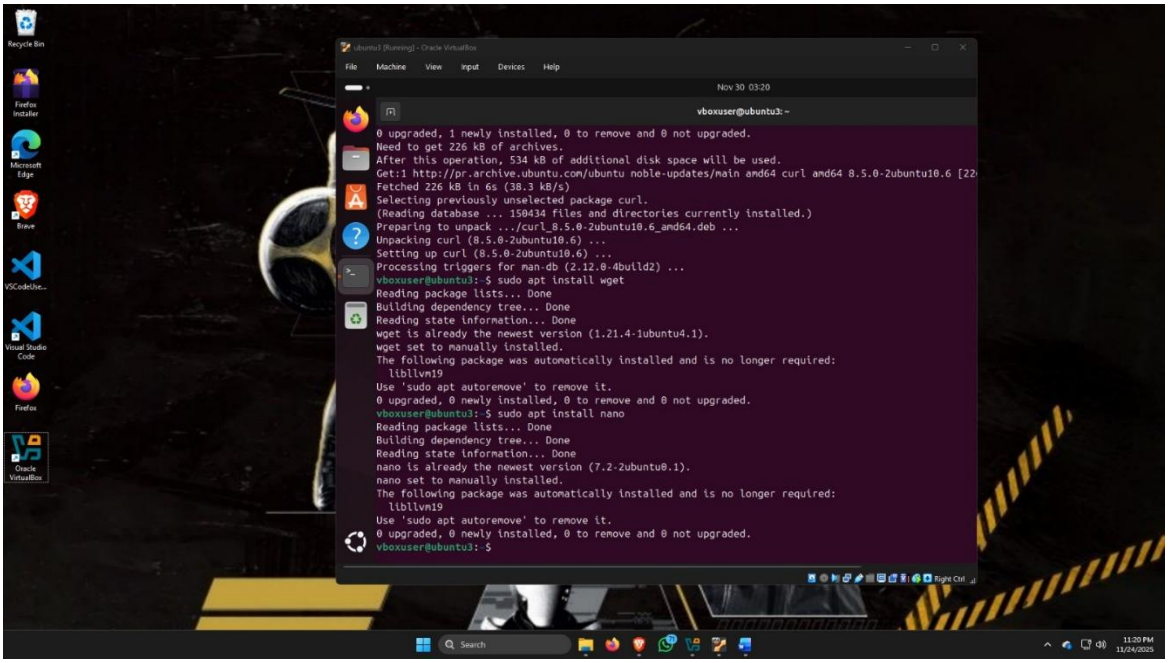
1. Preparación del entorno:



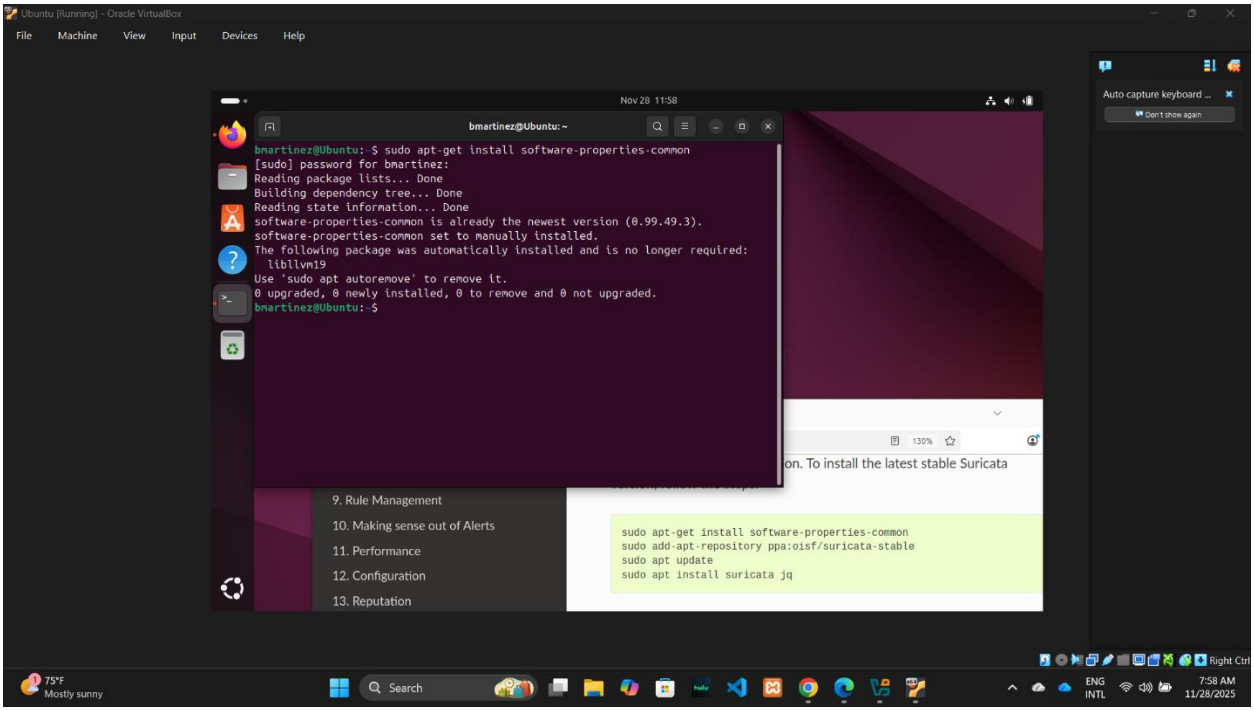


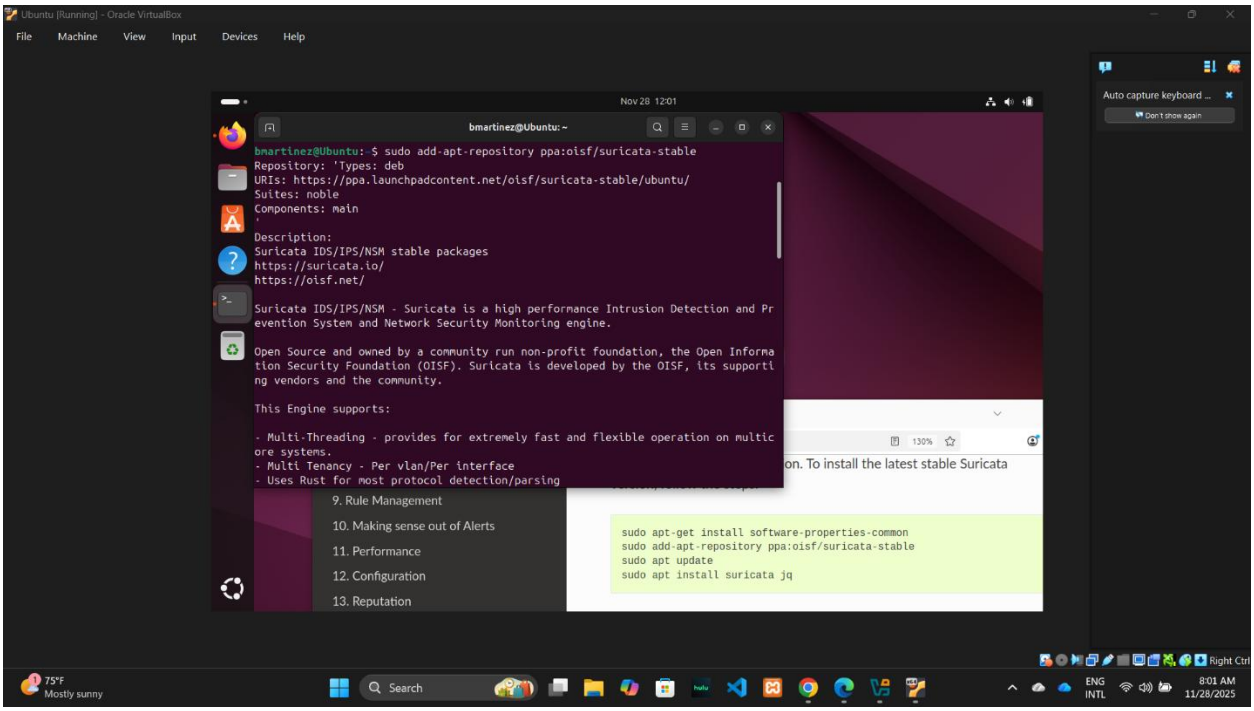

ubuntu3 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 30 03:17
vboxuser@ubuntu3: ~
vboxuser@ubuntu3:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for vboxuser:
Sorry, try again.
[sudo] password for vboxuser:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://pr.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://pr.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://pr.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
102 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
libllvm19
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
libllvm20
The following packages will be upgraded:
bluez bluez-cups bluez-obexd cloud-init coreutils dconf-cli
dconf-gsettings-backend dconf-service distro-info-data fwupd gdm3
gir1.2-gdm-1.0 gir1.2-gtk-4.0 gir1.2-nm-1.0 gir1.2-packagekitglib-1.0
gnome-control-center gnome-control-center-data gnome-control-center-faces
gnome-remote-desktop gnome-shell gnome-shell-common
gnome-shell-extension-desktop-icons-ng gstreamer1.0-packagekit libbluetooth3
libdconf1 libdrm-amdgpu1 libdrm-common libdrm-intel1 libdrm-nouveau2
libdrm-radeon1 libdrm2 libegl-mesa0 libfwupd2 libgbm1 libgdm1
libgl1-mesa-dri libglx-mesa0 libgtk-4-1 libgtk-4-bin libgtk-4-common
libgtk-4-media-gstreamer libgtop-2.0-11 libgtop2-common libipa-hbac0t64
Right Ctrl
Search
11:17 PM
11/24/2025

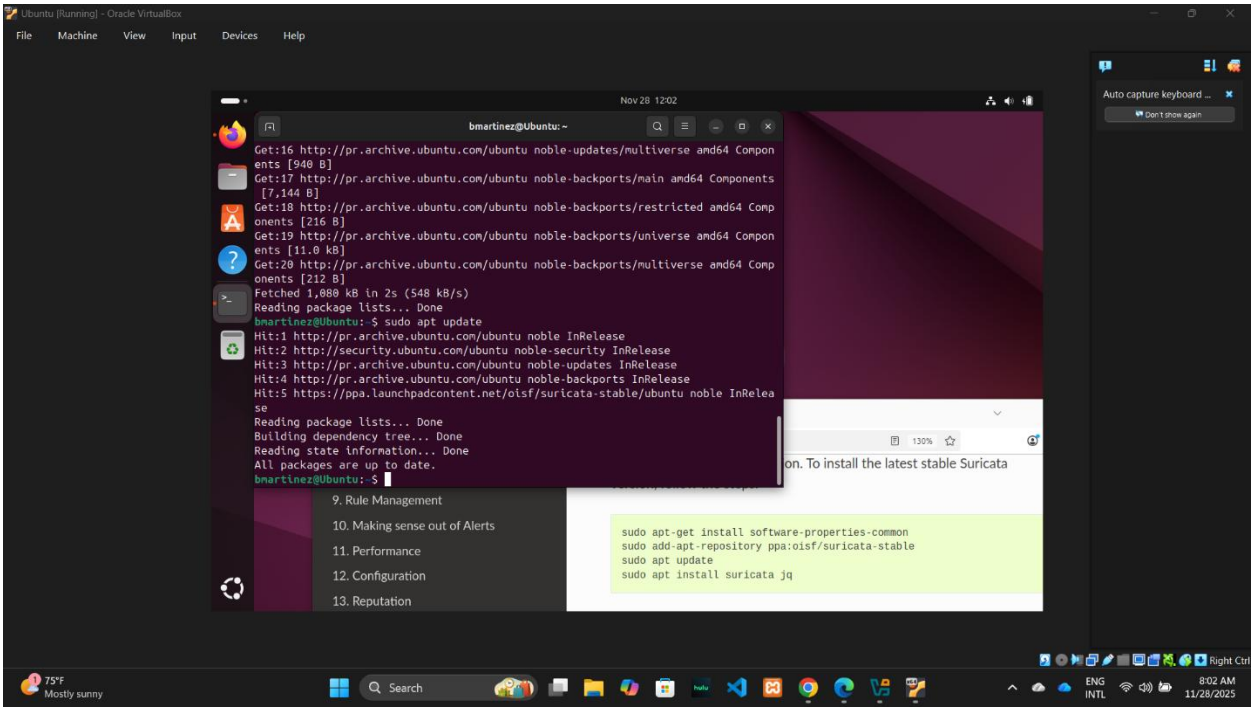

ubuntu3 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 30 03:18
vboxuser@ubuntu3: ~
vboxuser@ubuntu3:~$ sudo apt install curl
[sudo] password for vboxuser:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
libllvm19
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
curl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 226 kB of archives.
After this operation, 534 kB of additional disk space will be used.
Get:1 http://pr.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.5.0-2ubuntu10.6 [22
Fetched 226 kB in 6s (38.3 kB/s)
Selecting previously unselected package curl.
(Reading database ... 150434 files and directories currently installed.)
Preparing to unpack .../curl_8.5.0-2ubuntu10.6_amd64.deb ...
Unpacking curl (8.5.0-2ubuntu10.6) ...
Setting up curl (8.5.0-2ubuntu10.6) ...
Processing triggers for man-db (2.12.0-4build2) ...
vboxuser@ubuntu3:~$
Right Ctrl
Search
11:19 PM
11/24/2025

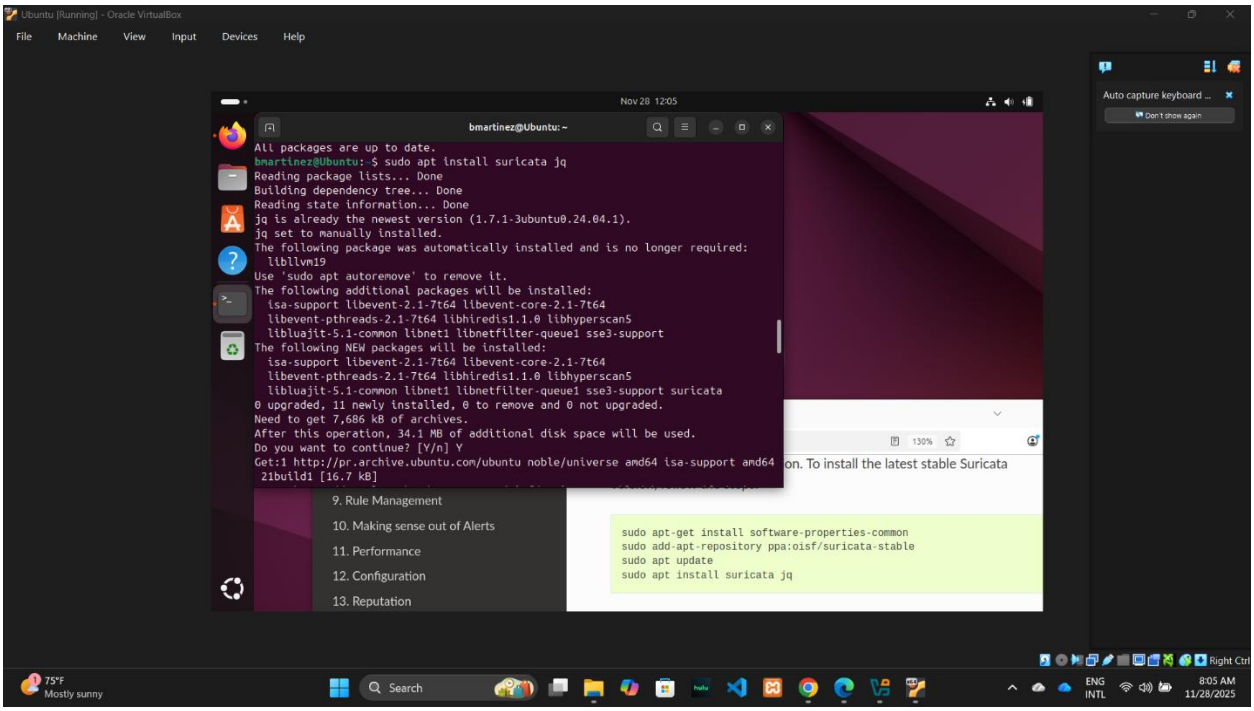


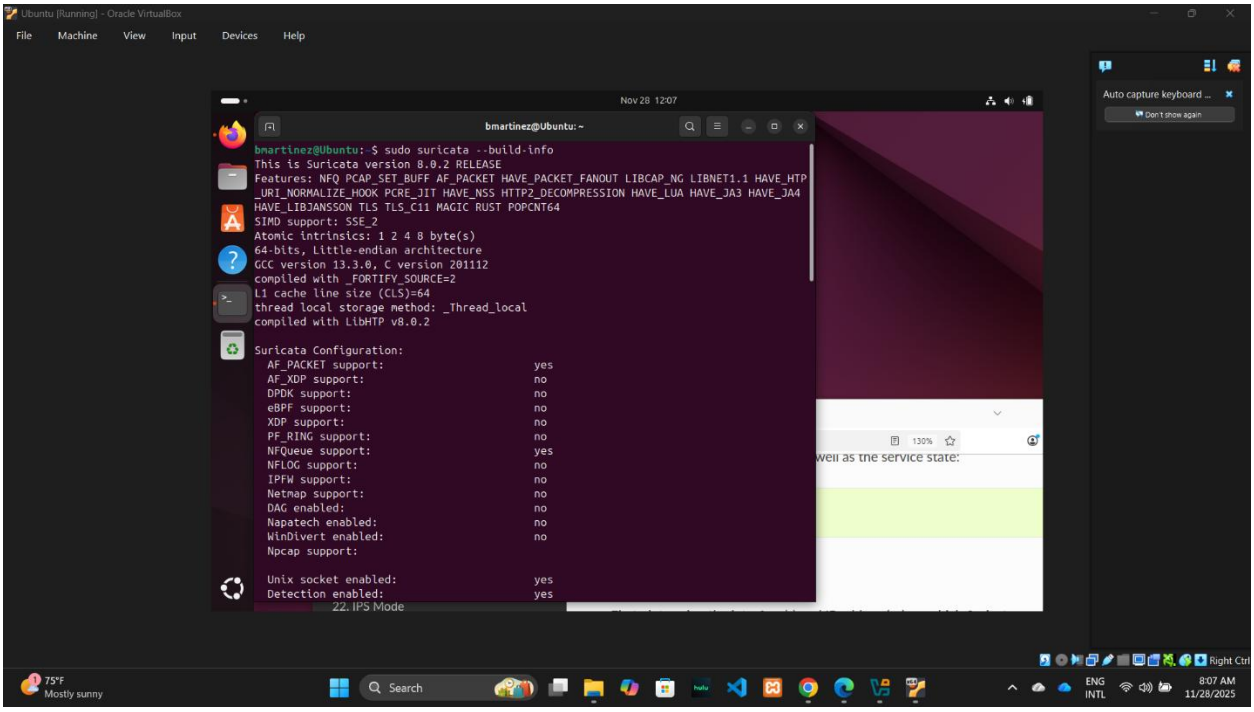
2. Instalación del IDS (Suricata):

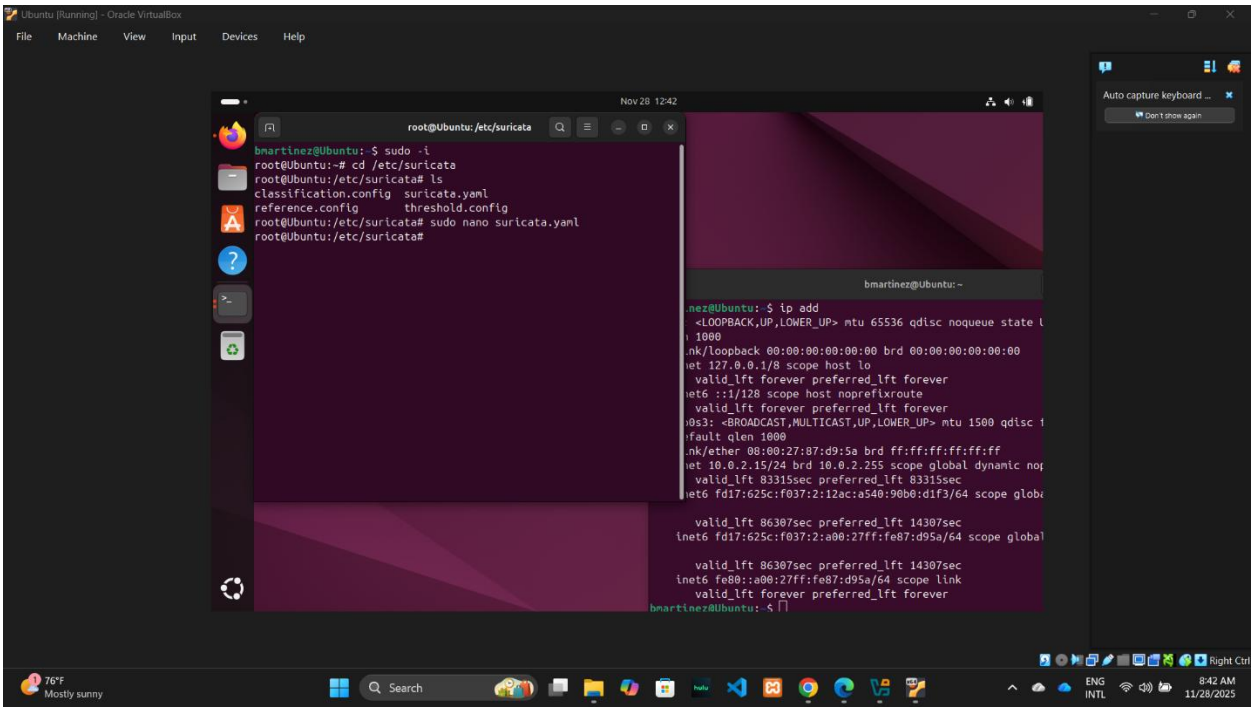


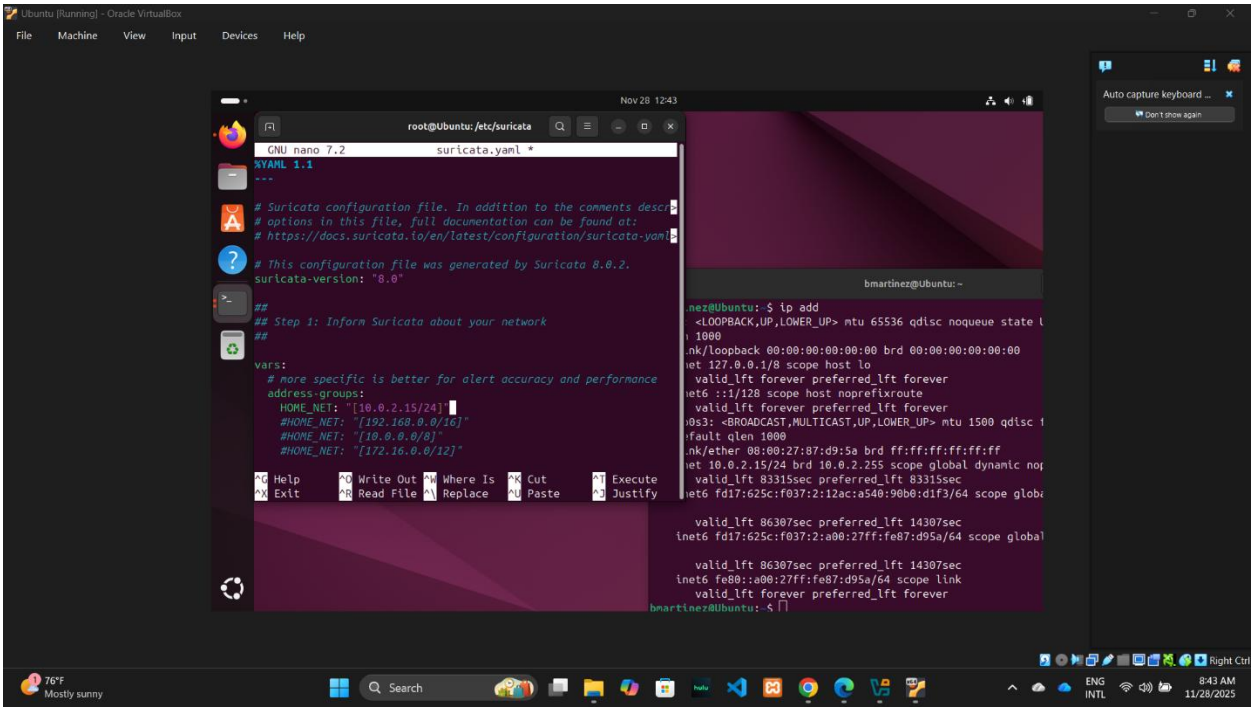

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:01
bmartinez@Ubuntu: ~
bmartinez@Ubuntu:~$ sudo add-apt-repository ppa:oisf/suricata-stable
Repository: 'Types: deb
URIs: https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/
Suites: noble
Components: main
'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/
Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.
Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community.
This Engine supports:
- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
9. Rule Management
10. Making sense out of Alerts
11. Performance
12. Configuration
13. Reputation
sudo apt-get install software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata jq
Auto capture keyboard ...
Don't show again
75°F
Mostly sunny
Search
ENG
INTL
8:01 AM
11/28/2025


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:02
bmartinez@Ubuntu: ~
Get:16 http://pr.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:17 http://pr.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,144 B]
Get:18 http://pr.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:19 http://pr.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.0 kB]
Get:20 http://pr.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 1,080 kB in 2s (548 kB/s)
Reading package lists... Done
bmartinez@Ubuntu:~$ sudo apt update
Hit:1 http://pr.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:3 http://pr.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://pr.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
bmartinez@Ubuntu:~$
9. Rule Management
10. Making sense out of Alerts
11. Performance
12. Configuration
13. Reputation
sudo apt-get install software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata jq
Auto capture keyboard ...
Don't show again
75°F
Mostly sunny
Search
ENG
INTL
8:02 AM
11/28/2025

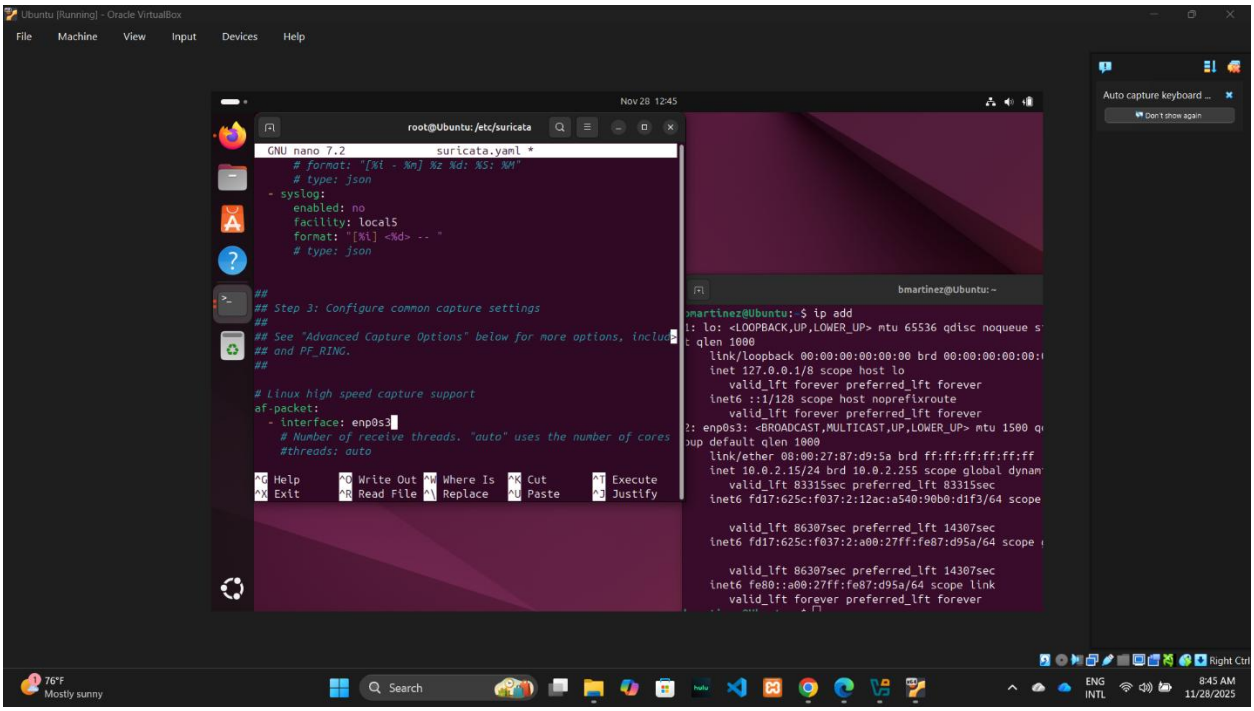

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:05
bmartinez@Ubuntu: ~
All packages are up to date.
bmartinez@Ubuntu:~$ sudo apt install suricata jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
jq is already the newest version (1.7.1-3ubuntu0.24.04.1).
jq set to manually installed.
The following package was automatically installed and is no longer required:
libllvm19
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
isa-support libevent-2.1-7t64 libevent-core-2.1-7t64
libevent-pthreads-2.1-7t64 libhiredis1.1.0 libhyperscan5
libluajit-5.1-common libnet1 libnetfilter-queue1 sse3-support
The following NEW packages will be installed:
isa-support libevent-2.1-7t64 libevent-core-2.1-7t64
libevent-pthreads-2.1-7t64 libhiredis1.1.0 libhyperscan5
libluajit-5.1-common libnet1 libnetfilter-queue1 sse3-support suricata
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 7,686 kB of archives.
After this operation, 34.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://pr.archive.ubuntu.com/ubuntu noble/universe amd64 isa-support amd64
21build1 [16.7 kB]
9. Rule Management
10. Making sense out of Alerts
11. Performance
12. Configuration
13. Reputation
sudo apt-get install software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata jq
Auto capture keyboard ...
Don't show again
75°F
Mostly sunny
Search
ENG
INTL
8:05 AM
11/28/2025

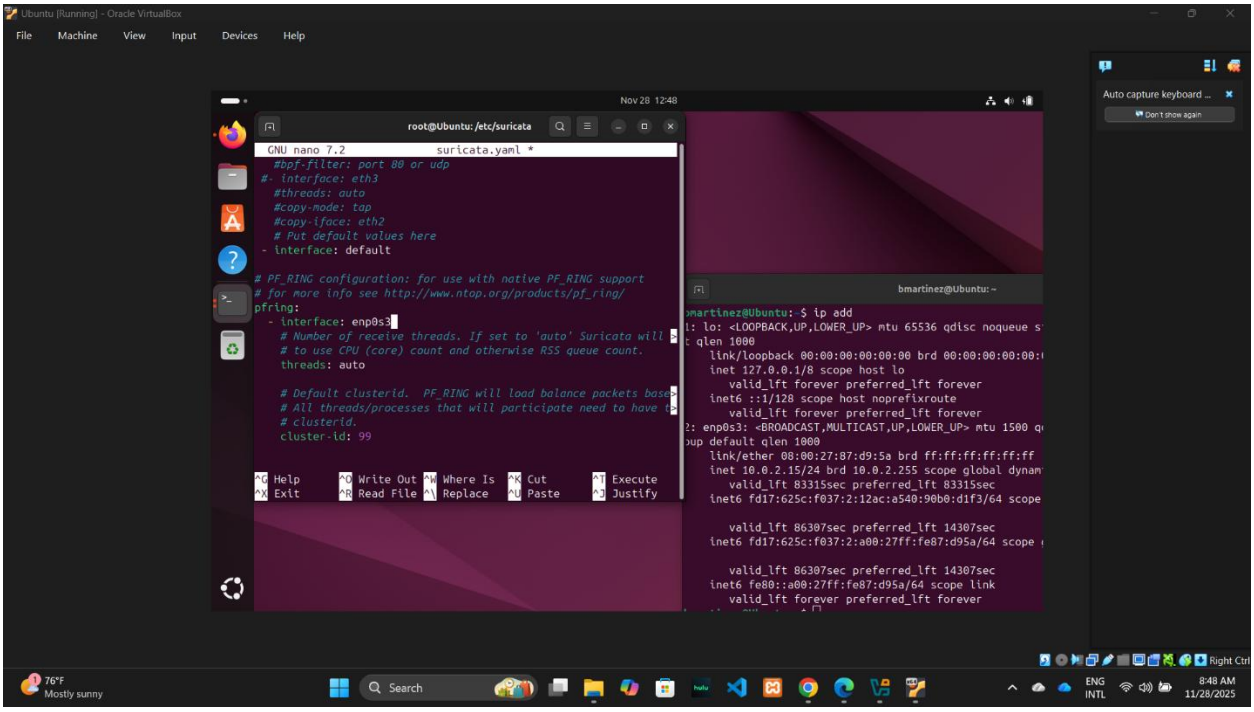

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:07
bmartinez@Ubuntu: ~
bmartinez@Ubuntu:~$ sudo suricata --build-info
This is Suricata version 8.0.2 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP
_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HTTP2_DECOMPRESSION HAVE_LUA HAVE_JA3 HAVE_JA4
HAVE_LIBJANSSON TLS TLS_C11 MAGIC RUST POPCNT64
SIMD support: SSE_2
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 13.3.0, C version 201112
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: _Thread_local
compiled with LibHTP v8.0.2
Suricata Configuration:
AF_PACKET support: yes
AF_XDP support: no
DPDK support: no
eBPF support: no
XDP support: no
PF_RING support: no
NFQueue support: yes
NFLOG support: no
IPFW support: no
Netmap support: no
DAG enabled: no
Napatech enabled: no
WinDivert enabled: no
Npcap support:
Unix socket enabled: yes
Detection enabled: yes
22. IPS Mode
Auto capture keyboard ...
Don't show again
75°F
Mostly sunny
Search
ENG
INTL
8:07 AM
11/28/2025

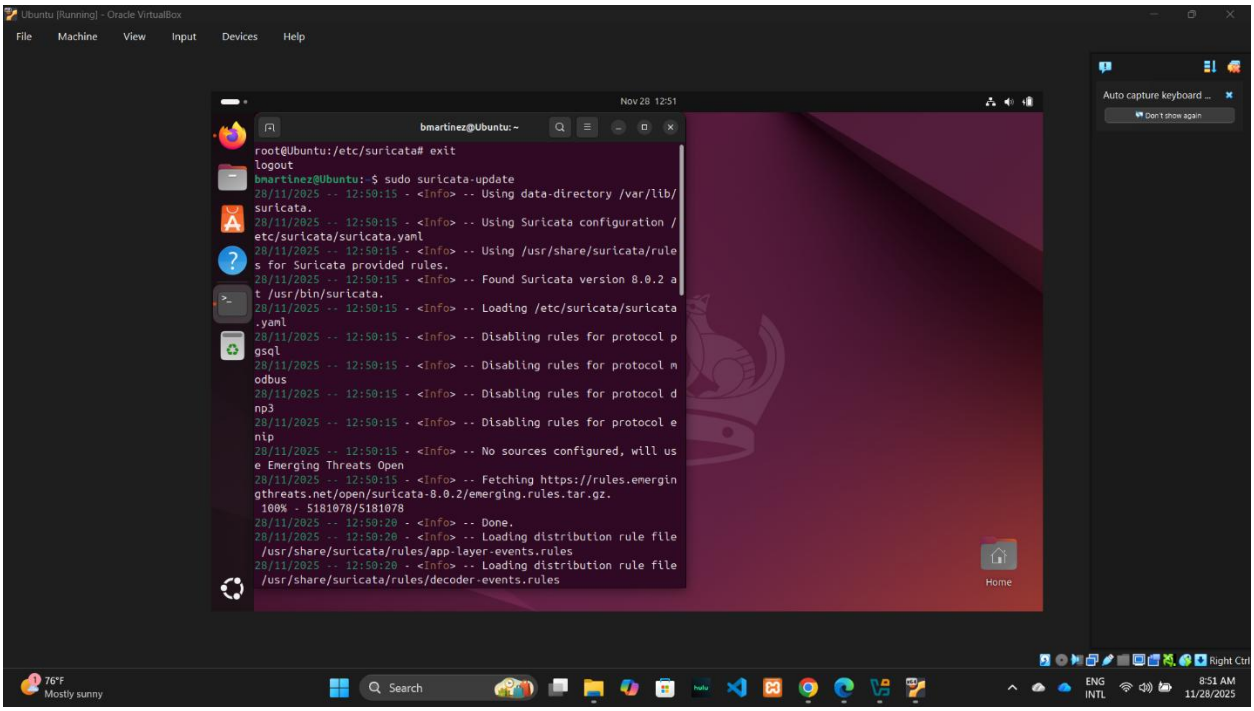

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:42
root@Ubuntu: /etc/suricata
bmartinez@Ubuntu: ~$ sudo -i
root@Ubuntu:~# cd /etc/suricata
root@Ubuntu:/etc/suricata# ls
classification.config suricata.yaml
reference.config threshold.config
root@Ubuntu:/etc/suricata# sudo nano suricata.yaml
root@Ubuntu:/etc/suricata#
bmartinez@Ubuntu: ~
Auto capture keyboard ...
Don't show again
Right Ctrl
76°F Mostly sunny
Search
ENG INTL
8:42 AM 11/28/2025

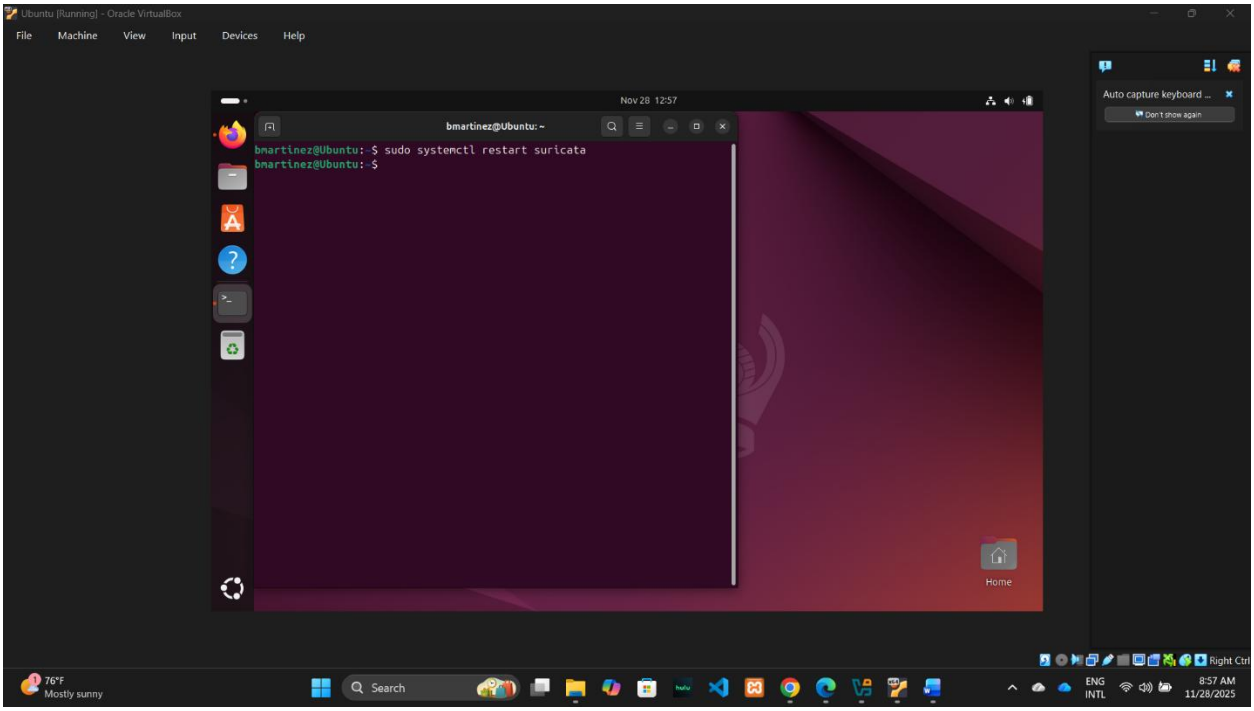

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:43
root@Ubuntu: /etc/suricata
GNU nano 7.2 suricata.yaml *
%YAML 1.1

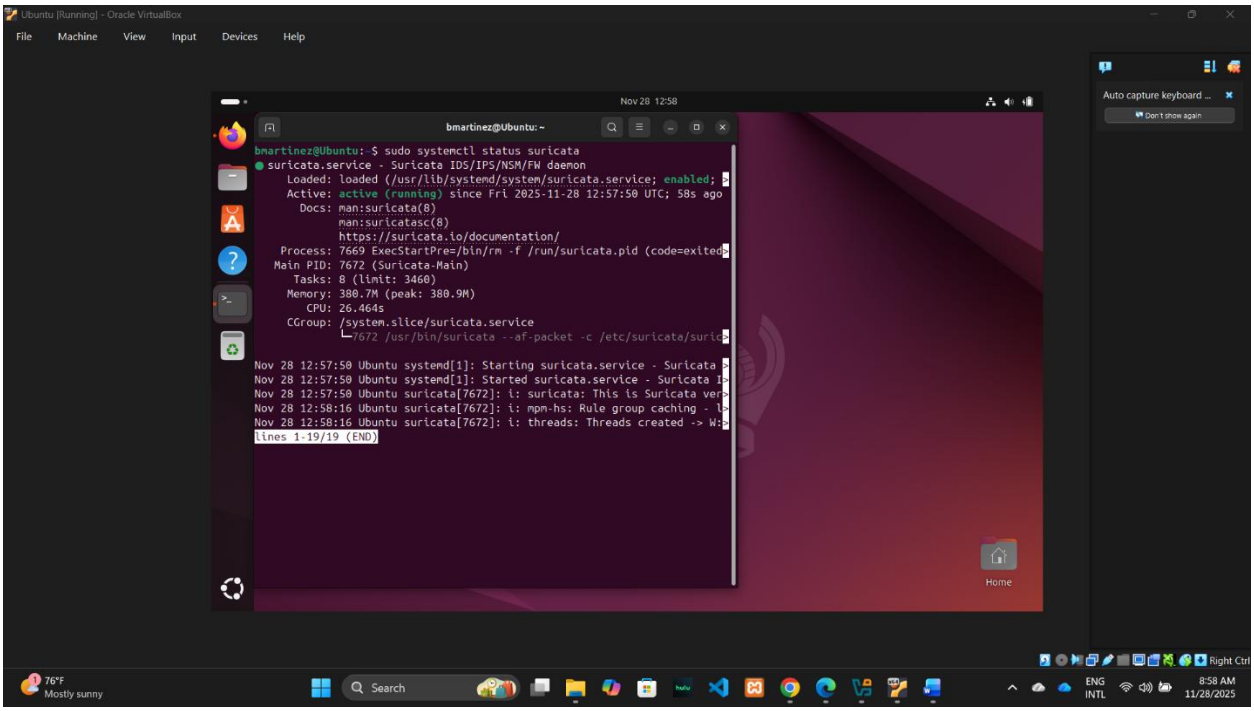
Suricata configuration file. In addition to the comments descr
options in this file, full documentation can be found at:
https://docs.suricata.to/en/latest/configuration/suricata-yaml
This configuration file was generated by Suricata 8.0.2.
suricata-version: "8.0"
##
Step 1: Inform Suricata about your network
##
vars:
more specific is better for alert accuracy and performance
address-groups:
HOME_NET: "[10.0.2.15/24]"
#HOME_NET: "[192.168.0.0/16]"
#HOME_NET: "[10.0.0.0/8]"
#HOME_NET: "[172.16.0.0/12]"
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
bmartinez@Ubuntu: ~
Auto capture keyboard ...
Don't show again
Right Ctrl
76°F Mostly sunny
Search
ENG INTL
8:43 AM 11/28/2025


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:45
root@Ubuntu: /etc/suricata
GNU nano 7.2 suricata.yaml *
format: "[%i - %m] %z %d: %S: %M"
type: json
- syslog:
enabled: no
facility: local5
format: "[%i] <%d> -- "
type: json
##
Step 3: Configure common capture settings
##
See "Advanced Capture Options" below for more options, includ
and PF_RING.
##
Linux high speed capture support
af-packet:
- interface: enp0s3
Number of receive threads. "auto" uses the number of cores
#threads: auto
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
bmartinez@Ubuntu: ~
bmartinez@Ubuntu:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue s
t qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:0
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 q
up default qlen 1000
link/ether 08:00:27:87:d9:5a brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynam
valid_lft 83315sec preferred_lft 83315sec
inet6 fd17:625c:f037:2:12ac:a540:90b0:d1f3/64 scope
valid_lft 86307sec preferred_lft 14307sec
inet6 fd17:625c:f037:2:a00:27ff:fe87:d95a/64 scope
valid_lft 86307sec preferred_lft 14307sec
inet6 fe80::a00:27ff:fe87:d95a/64 scope link
valid_lft forever preferred_lft forever
Auto capture keyboard ...
Don't show again
Right Ctrl
76°F
Mostly sunny
Search
ENG
INTL
8:45 AM
11/28/2025

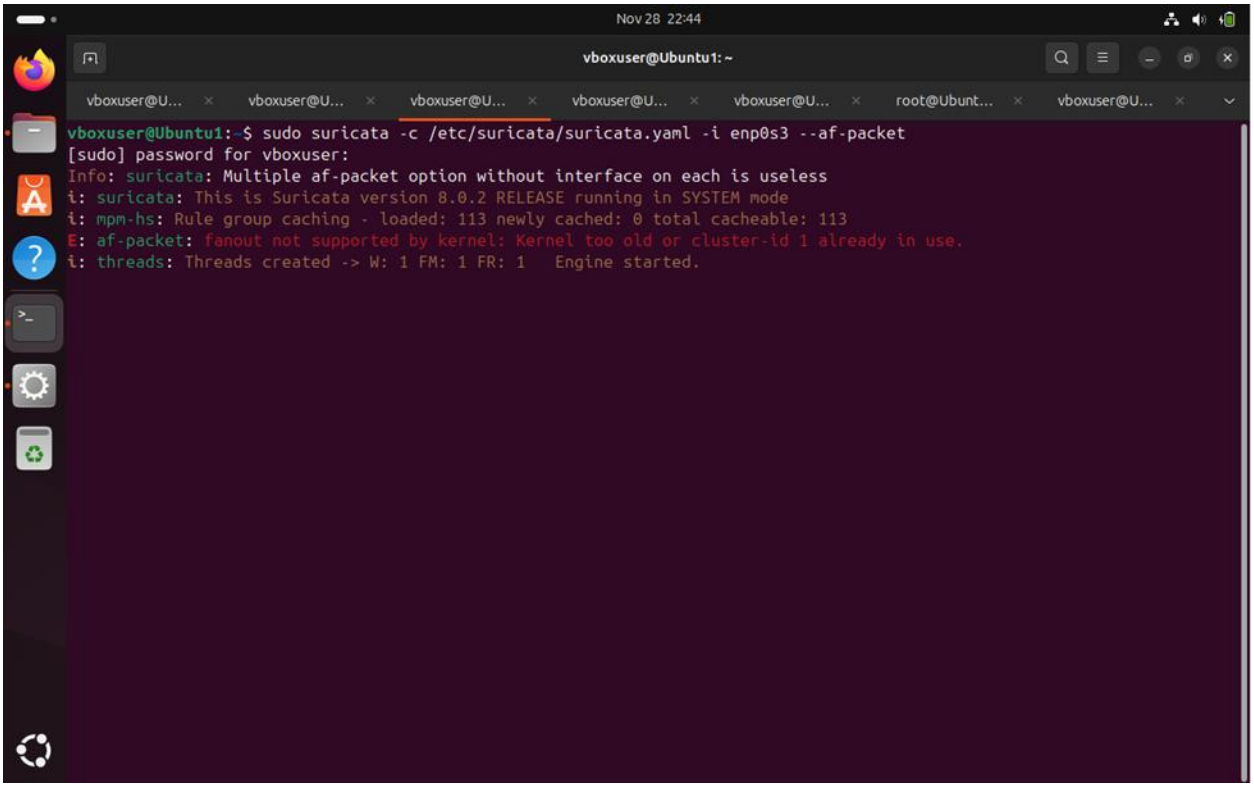

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:48
root@Ubuntu: /etc/suricata
GNU nano 7.2 suricata.yaml *
#bpf-filter: port 80 or udp
#- interface: eth3
#threads: auto
#copy-mode: tap
#copy-iface: eth2
Put default values here
- interface: default
PF_RING configuration: for use with native PF_RING support
for more info see http://www.ntop.org/products/pf_ring/
pfring:
- interface: enp0s3
Number of receive threads. If set to 'auto' Suricata will
to use CPU (core) count and otherwise RSS queue count.
threads: auto
Default clusterid. PF_RING will load balance packets base
All threads/processes that will participate need to have t
clusterid.
cluster-id: 99
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
bmartinez@Ubuntu: ~
bmartinez@Ubuntu:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue s
t qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:0
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 q
up default qlen 1000
link/ether 08:00:27:87:d9:5a brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynam
valid_lft 83315sec preferred_lft 83315sec
inet6 fd17:625c:f037:2:12ac:a540:90b0:d1f3/64 scope
valid_lft 86307sec preferred_lft 14307sec
inet6 fd17:625c:f037:2:a00:27ff:fe87:d95a/64 scope
valid_lft 86307sec preferred_lft 14307sec
inet6 fe80::a00:27ff:fe87:d95a/64 scope link
valid_lft forever preferred_lft forever
Auto capture keyboard ...
Don't show again
Right Ctrl
76°F
Mostly sunny
Search
ENG
INTL
8:48 AM
11/28/2025

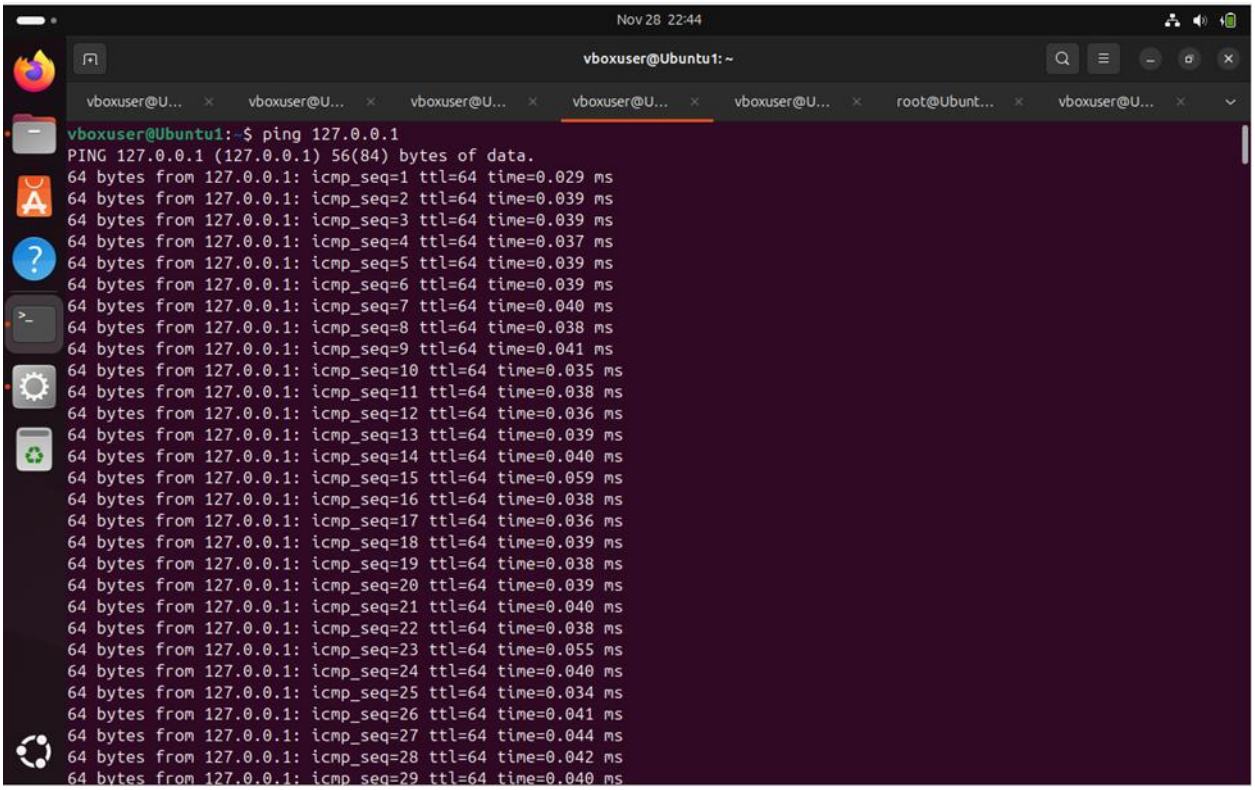

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:51
bmartinez@Ubuntu: ~
root@Ubuntu:/etc/suricata# exit
logout
bmartinez@Ubuntu:~$ sudo suricata-update
28/11/2025 -- 12:50:15 - <Info> -- Using data-directory /var/lib/suricata.
28/11/2025 -- 12:50:15 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
28/11/2025 -- 12:50:15 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
28/11/2025 -- 12:50:15 - <Info> -- Found Suricata version 8.0.2 at /usr/bin/suricata.
28/11/2025 -- 12:50:15 - <Info> -- Loading /etc/suricata/suricata.yaml
28/11/2025 -- 12:50:15 - <Info> -- Disabling rules for protocol pgsql
28/11/2025 -- 12:50:15 - <Info> -- Disabling rules for protocol modbus
28/11/2025 -- 12:50:15 - <Info> -- Disabling rules for protocol dnp3
28/11/2025 -- 12:50:15 - <Info> -- Disabling rules for protocol enip
28/11/2025 -- 12:50:15 - <Info> -- No sources configured, will use Emerging Threats Open
28/11/2025 -- 12:50:15 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-8.0.2/emerging.rules.tar.gz.
100% - 5181078/5181078
28/11/2025 -- 12:50:20 - <Info> -- Done.
28/11/2025 -- 12:50:20 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-events.rules
28/11/2025 -- 12:50:20 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules
Home
Auto capture keyboard ...
Don't show again
Right Ctrl
76°F Mostly sunny
Search
ENG INTL
8:51 AM 11/28/2025

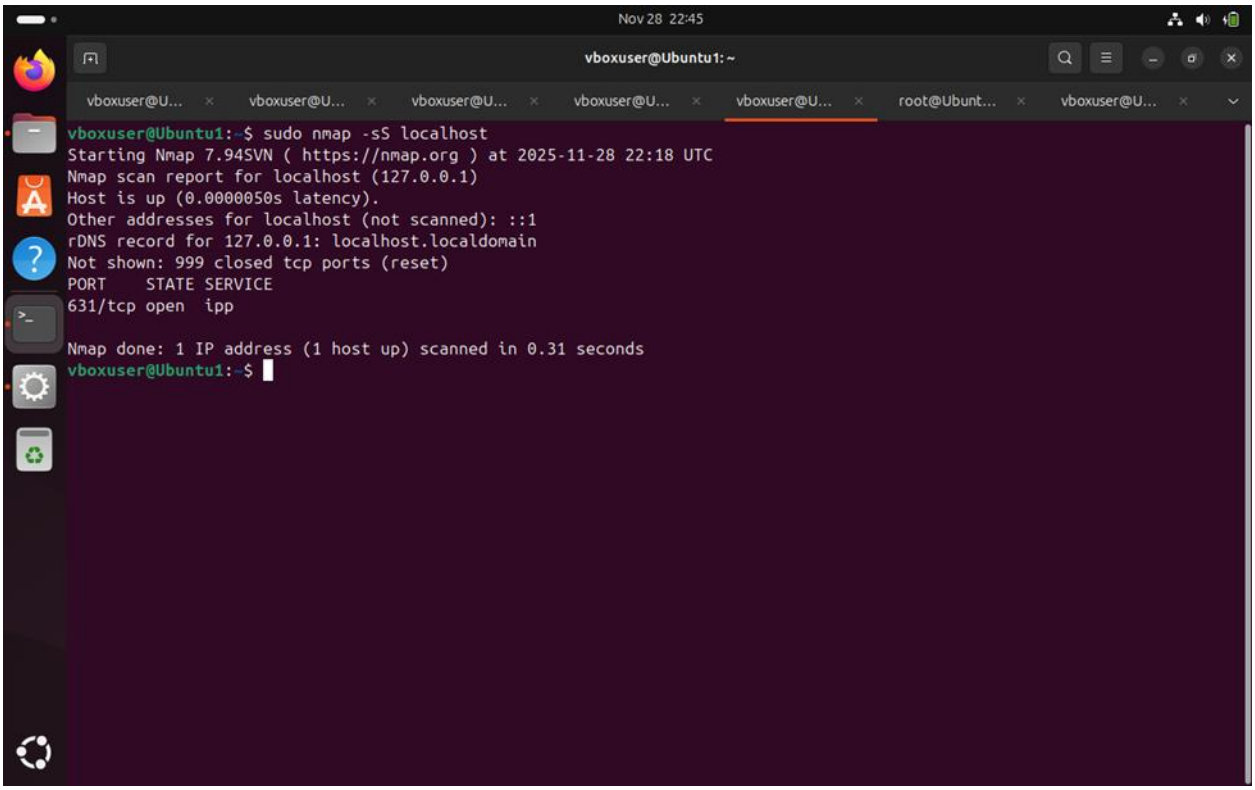

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Nov 28 12:57
bmartinez@Ubuntu: ~
bmartinez@Ubuntu:~$ sudo systemctl restart suricata
bmartinez@Ubuntu:~$
Home
Auto capture keyboard ...
Don't show again
Right Ctrl
76°F Mostly sunny
Search
ENG INTL
8:57 AM 11/28/2025

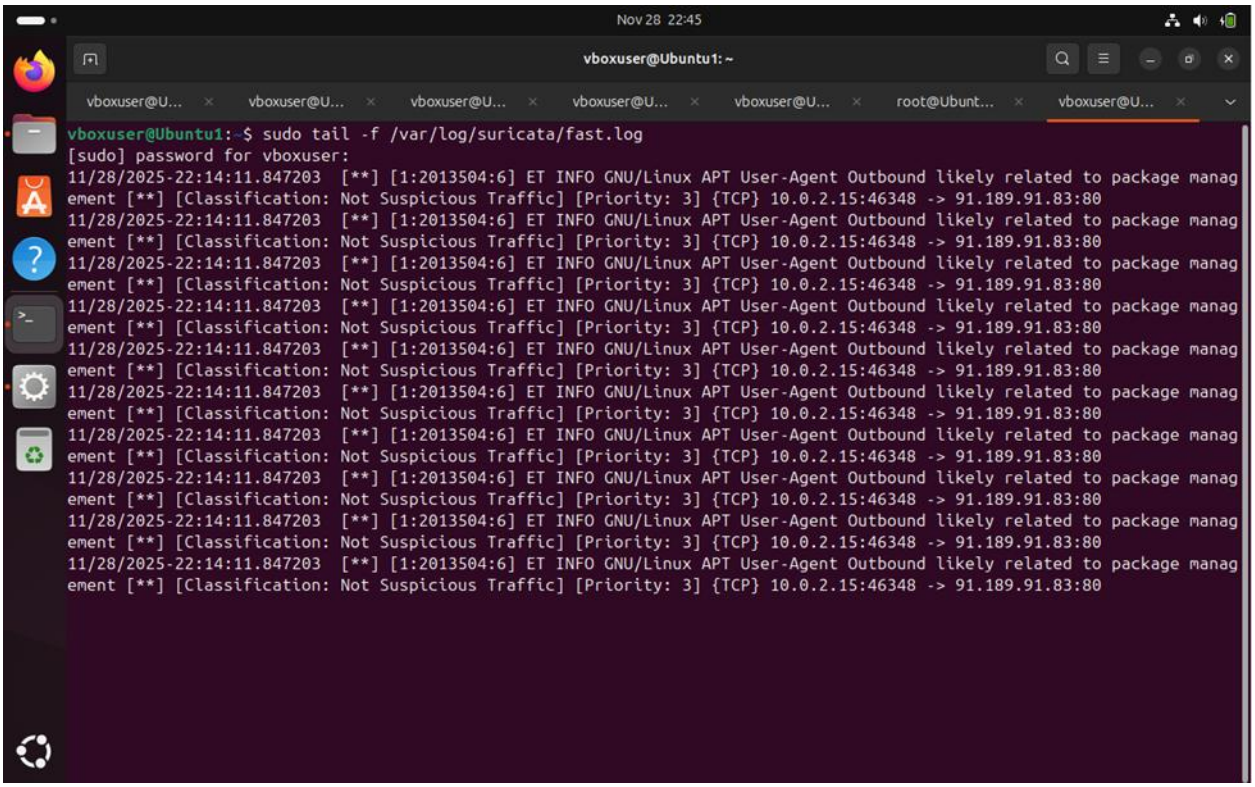


3. Prueba de detección:




Nov 28 22:44
vboxuser@Ubuntu1: ~
vboxuser@U...
vboxuser@U...
vboxuser@U...
vboxuser@U...
vboxuser@U...
root@Ubunt...
vboxuser@U...
vboxuser@Ubuntu1:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.036 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=15 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=16 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=17 ttl=64 time=0.036 ms
64 bytes from 127.0.0.1: icmp_seq=18 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=19 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=20 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=21 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=22 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=23 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=24 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=25 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=26 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=27 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=28 ttl=64 time=0.042 ms
64 bytes from 127.0.0.1: icmp_seq=29 ttl=64 time=0.040 ms


Nov 28 22:45
vboxuser@Ubuntu1: ~
vboxuser@U...
vboxuser@U...
vboxuser@U...
vboxuser@U...
vboxuser@U...
root@Ubunt...
vboxuser@U...
vboxuser@Ubuntu1:~$ sudo nmap -sS localhost
Starting Nmap 7.94SVN (https://nmap.org) at 2025-11-28 22:18 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
631/tcp open ipp
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
vboxuser@Ubuntu1:~$



```
vboxuser@Ubuntu1:~$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for vboxuser:
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
11/28/2025-22:14:11.847203  [**] [1:2013504:6] ET INFO GNU/Linux APT User-Agent Outbound likely related to package manag
ement [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2.15:46348 -> 91.189.91.83:80
```

4. Documentación de los resultados:

Fecha y Hora	Tipo de Evento Detectado	Clasificación	Acción del IDS
28/11/2025 – 22:14:11.847203	ET INFO GNU/Linux APT User-Agent Outbound likely related to package management	Not Suspicious Traffic (Priority 3)	Alerta
28/11/2025 – 22:14:11.847203	ET INFO GNU/Linux APT User-Agent Outbound likely related to package management	Not Suspicious Traffic (Priority 3)	Alerta
28/11/2025 – 22:14:11.847203	ET INFO GNU/Linux APT User-Agent Outbound likely related to package management	Not Suspicious Traffic (Priority 3)	Alerta

Conclusión:

Este proyecto nos enseñó cómo ver qué hasta los más mínimos movimientos pueden ser registradas y observadas por diferentes herramientas de análisis. Esto es un aspecto fundamental para la ciberseguridad debido a que es una excelente herramienta para comprender el campo más allá de los que estamos acostumbrados. Las dificultades que hubo al hacer el proyecto fueron la implementación del código y las configuraciones del programa, pero al final se pudo hacer. También, en entender si lo que está demostrando el programa es lo correcto, pero se pudo investigar y entender mejor. Hubo errores en todas partes, pero de los errores se aprende y cuando se logra hacer esas dificultades, te hace sentir muy bien. Para futura implementación nos gustaría incorporar un IPS que es algo que suricata puede acomodar. Este servicio no tan solo detecta la entrada el tráfico que pasa por el sistema como lo demuestra suricata, pero también toma las medidas necesarias para bloquear el tráfico si este demuestra patrones de malware. Los IDS tienen gran importancia para la protección de redes porque permite detectar actividades sospechosas y ataques en el momento en que ocurren, ofreciendo una alerta temprana antes de que se produzcan daños mayores. Además, da visibilidad completa del tráfico y del comportamiento dentro de la red, lo que ayuda a identificar intrusiones que podrían pasar desapercibidas por otros sistemas. Esto nos lleva a concluir que el IDS refuerza la seguridad informática y complementa otras defensas como los firewalls, contribuyendo a una infraestructura más segura y confiable.

Tabla de contribuciones:

Nombre del integrante	Tarea realizada	% de contribución
Benyahir Y. Martínez	Desarrollo teórico, Desarrollo practico, Conclusión	25%
Jacob J. Desuza	Desarrollo practico, Desarrollo teórico, Conclusión	25%
Emanuel V. Rodríguez	Desarrollo teórico, Desarrollo practico, Conclusión	25%
John A. Valentín	Desarrollo practico, Desarrollo teórico, Conclusión	25%

Referencias:

Networks Spanish. (n.d.). *IDS frente a IPS: diferencias entre IDS e IPS | Versa Networks*. Versa Networks | Spanish. https://versa-networks.com/es/sd-wan/ids-ips/

Jorge Yussel Nuñez Peña & José Antonio Morales Flores. (2023). *Breve análisis comparativo de Snort y Suricata.* REVISTA INCAING ISSN 2448 9131. https://share.google/rLyodhN3cuGbhykoD

De RL De CV, C. S. (2024, October 18). *Guía Rápida: ¿Cómo Saber Cuál es mi dirección IP?* CertSuperior. https://www.certsuperior.com/log-que-es-y-como-se-usan-para-sistemas-de-seguridad/

ANÁLISIS DE LOGS DE SEGURIDAD ¿COMO DETECTAR AMENAZAS A TIEMPO? | VenCERT - Sistema Nacional de Gestión de Incidentes Telemáticos. (n.d.). https://vencert.suscerte.gob.ve/an%C3%A1lisis-de-logs-de-seguridad-como-detectar-amenazas-a-tiempo/

Sancho Lerena. (2024, March 5). *Logs: qué son y por qué monitorizarlos*. Pandora Tech Blog. https://pandorafms.com/blog/es/logs/

HARTEK. (2018, 20 marzo). *Suricata IDS –Jugando con las reglas*. Follow The White Rabbit.

https://fwhibbit.es/suricata-ids-jugando-con-las-reglasA

Suricata - IDS/IPS - Instalación, configuración básica reglas. (2021, 7 marzo). *elhacker.net*.

https://blog.elhacker.net/2021/03/suricata-ids-ips-instalacion-configuracion-reglas-.html