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.

1. **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.

1. **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

1. **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 tenia 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?

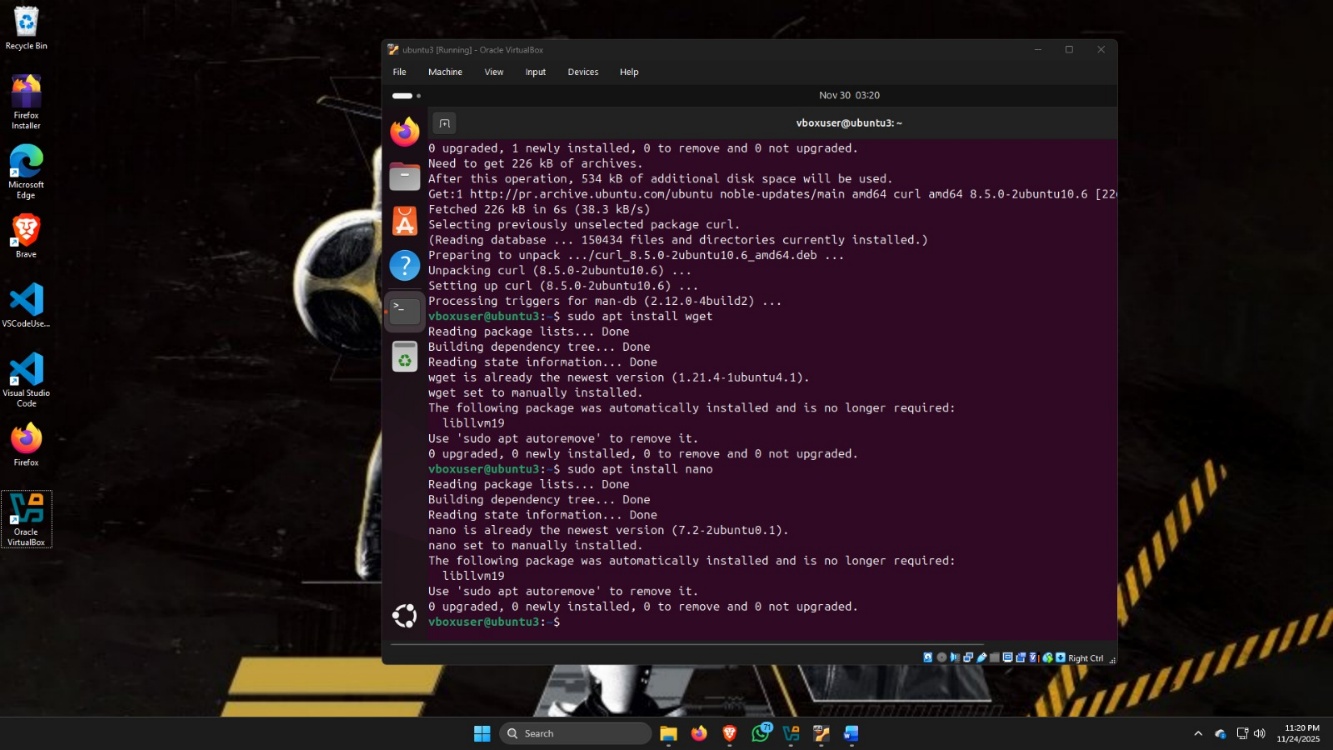
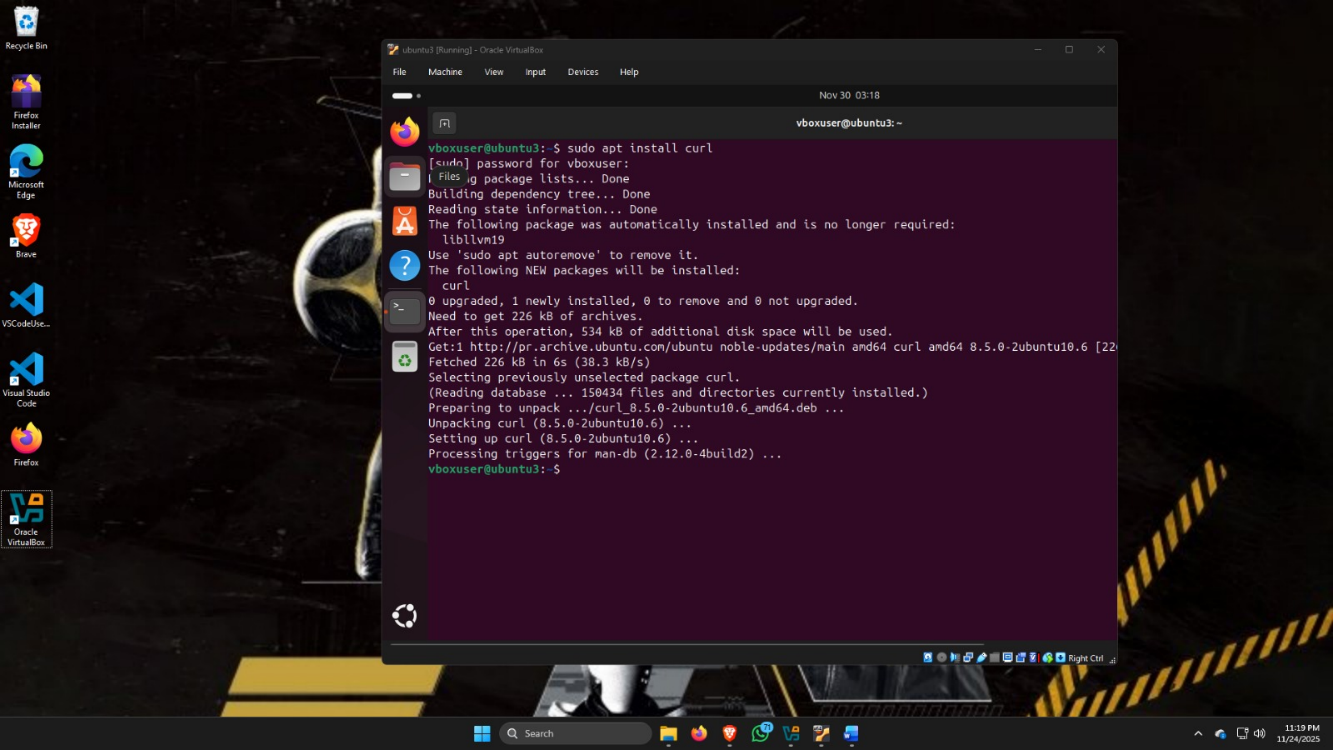
Si hubiéramos tenido mas conocimiento y tiempo implementaríamos una herramienta de IPS. Este permitiría no tan solo detectar cualquier tipo de tráfico está ocurriendo en el momento, pero también tomaría las medidas necesarias para bloquear este si estuviese lidiando con tráfico malicioso.

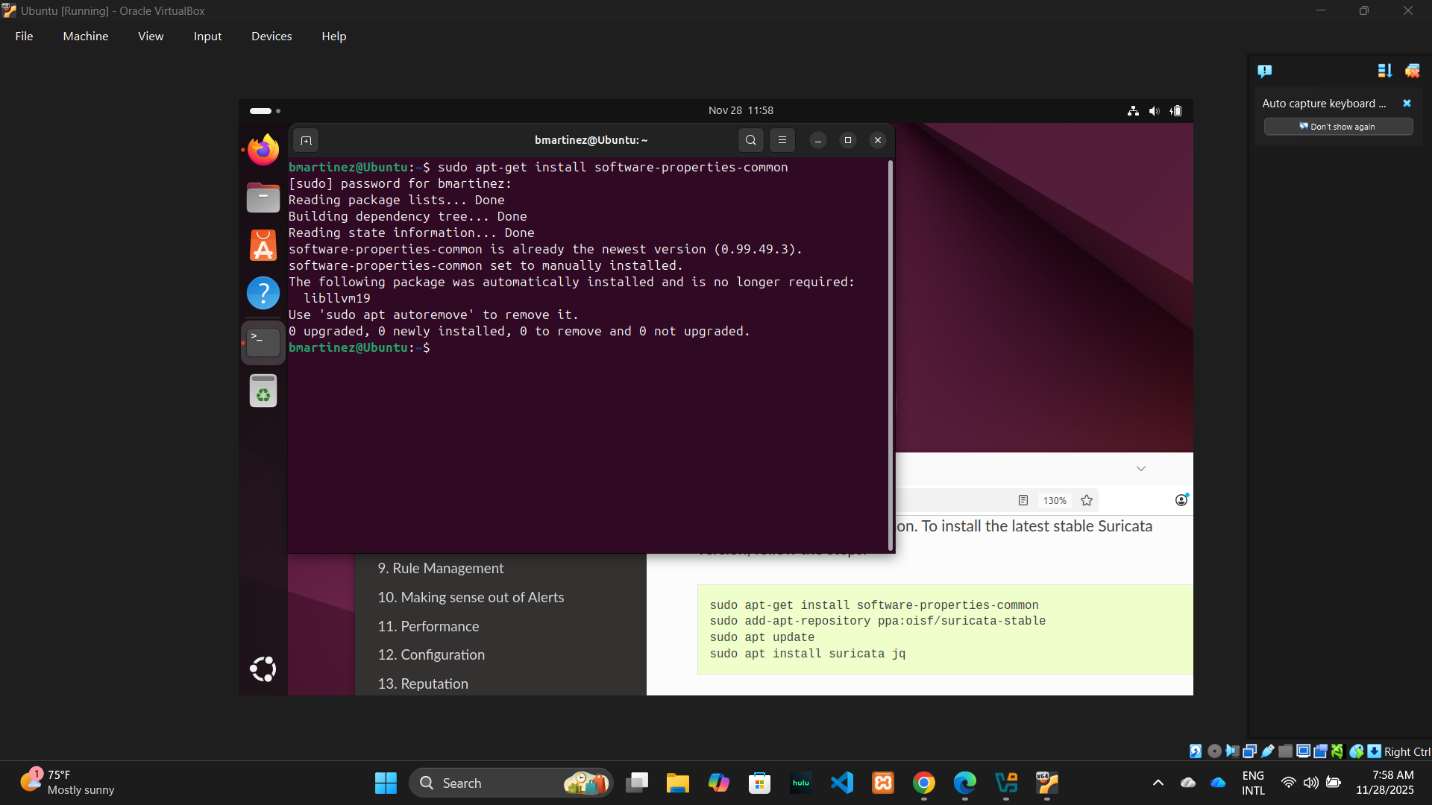
**Desarrollo Practico:**

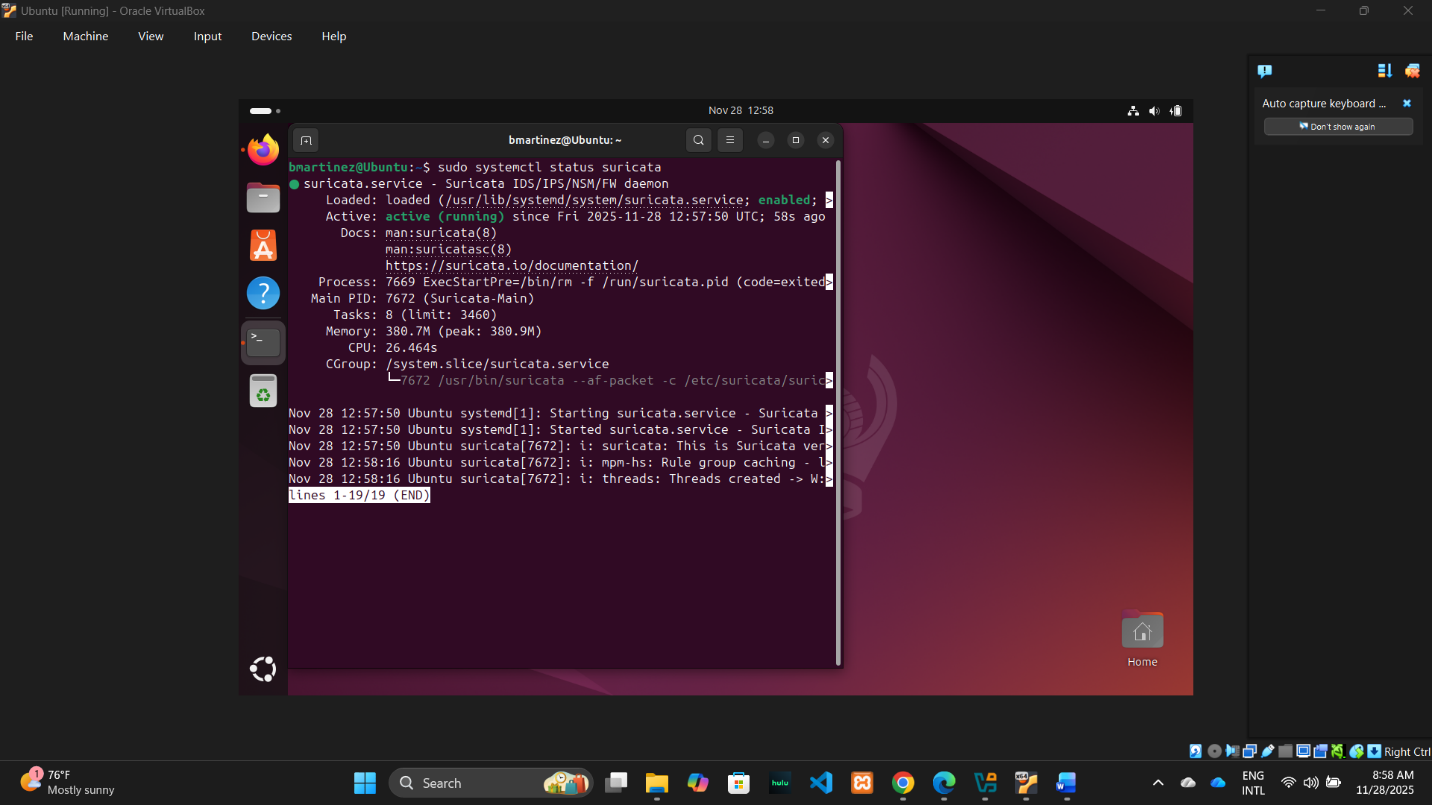
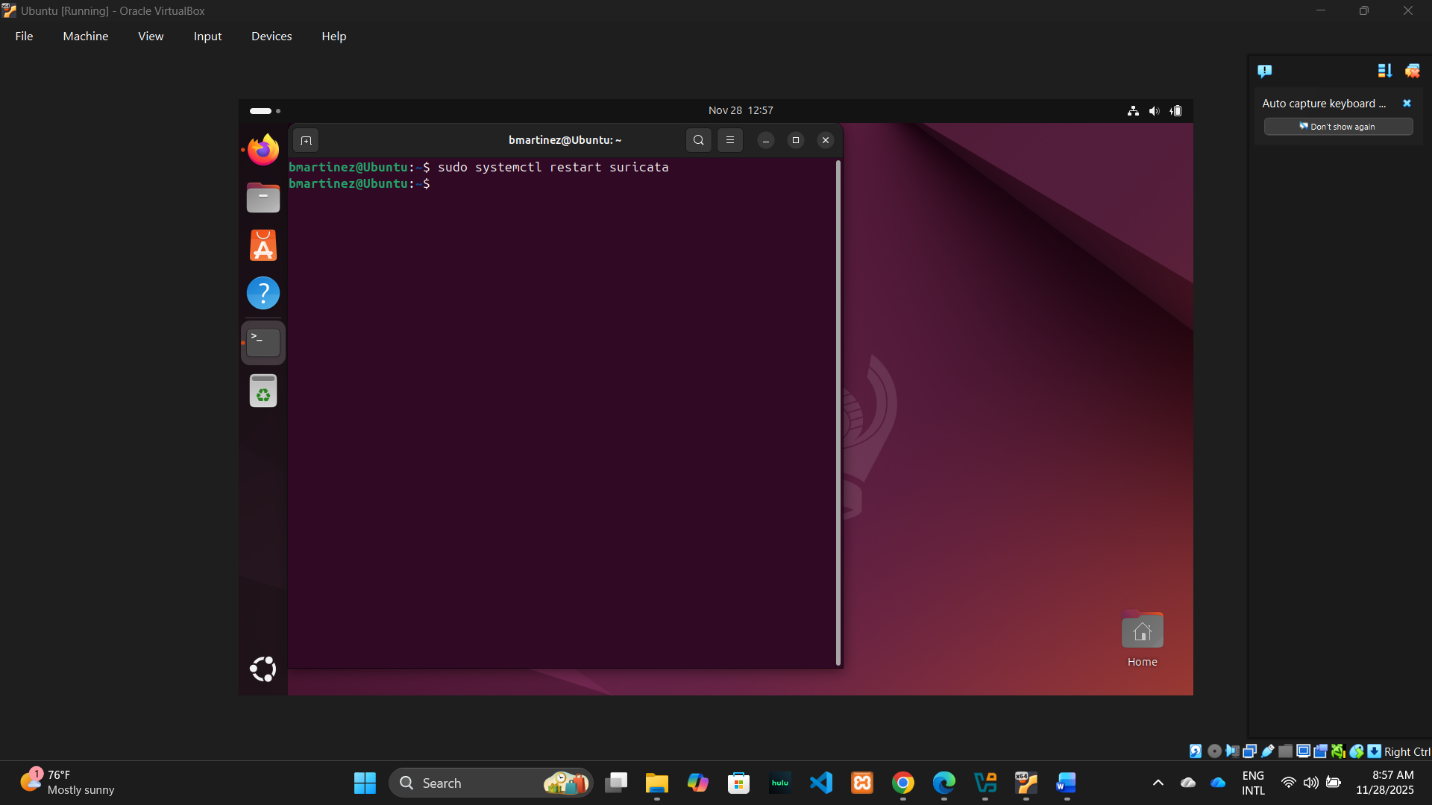
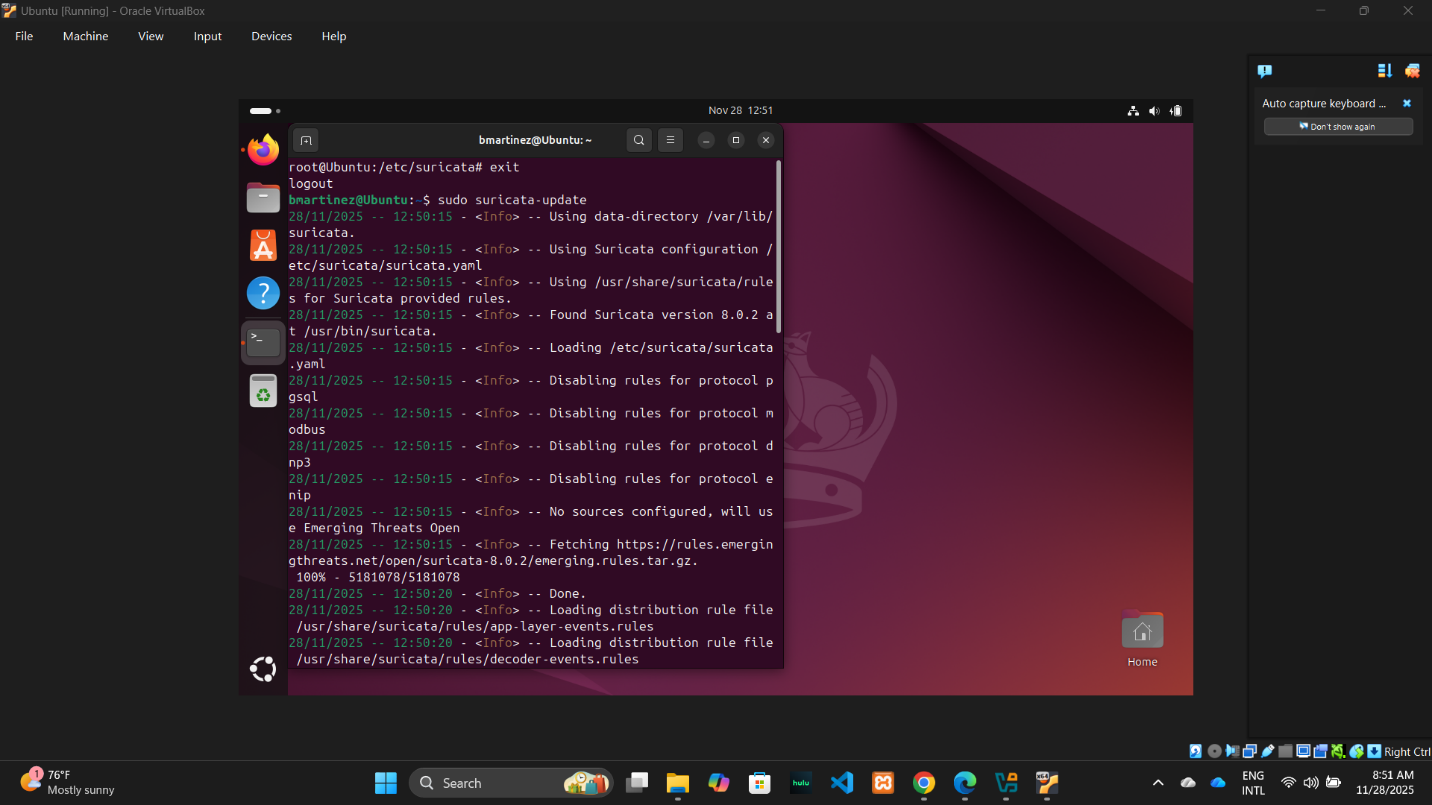
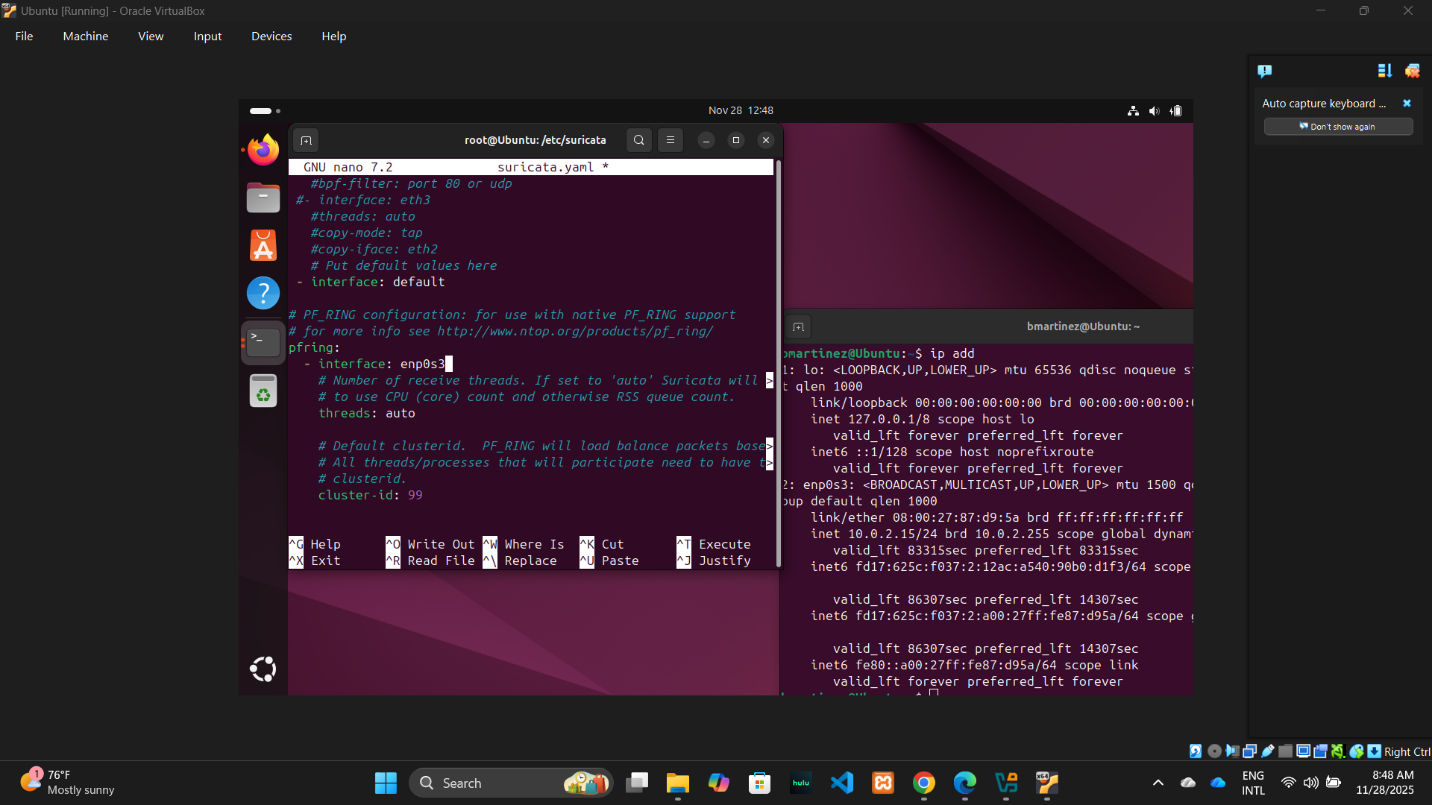
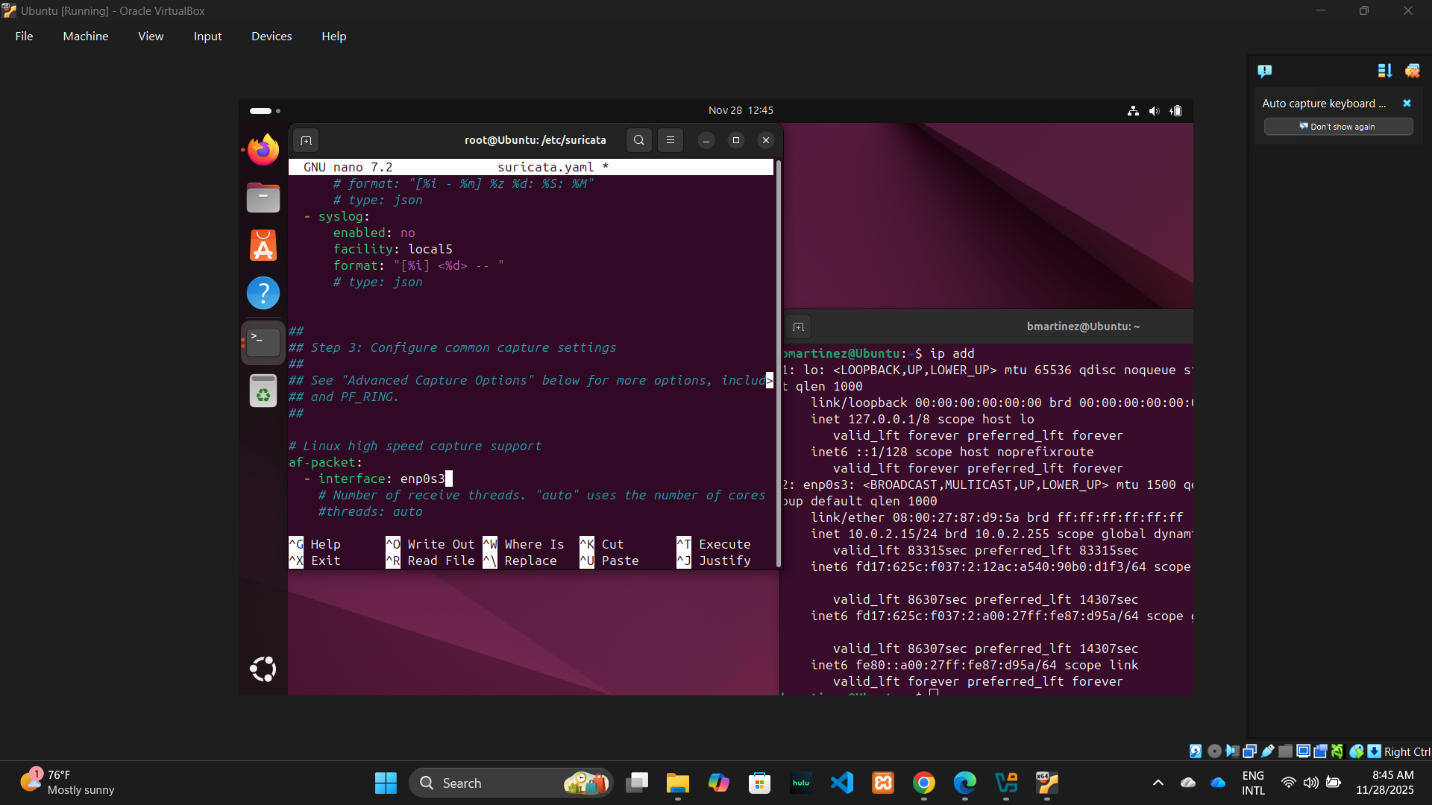
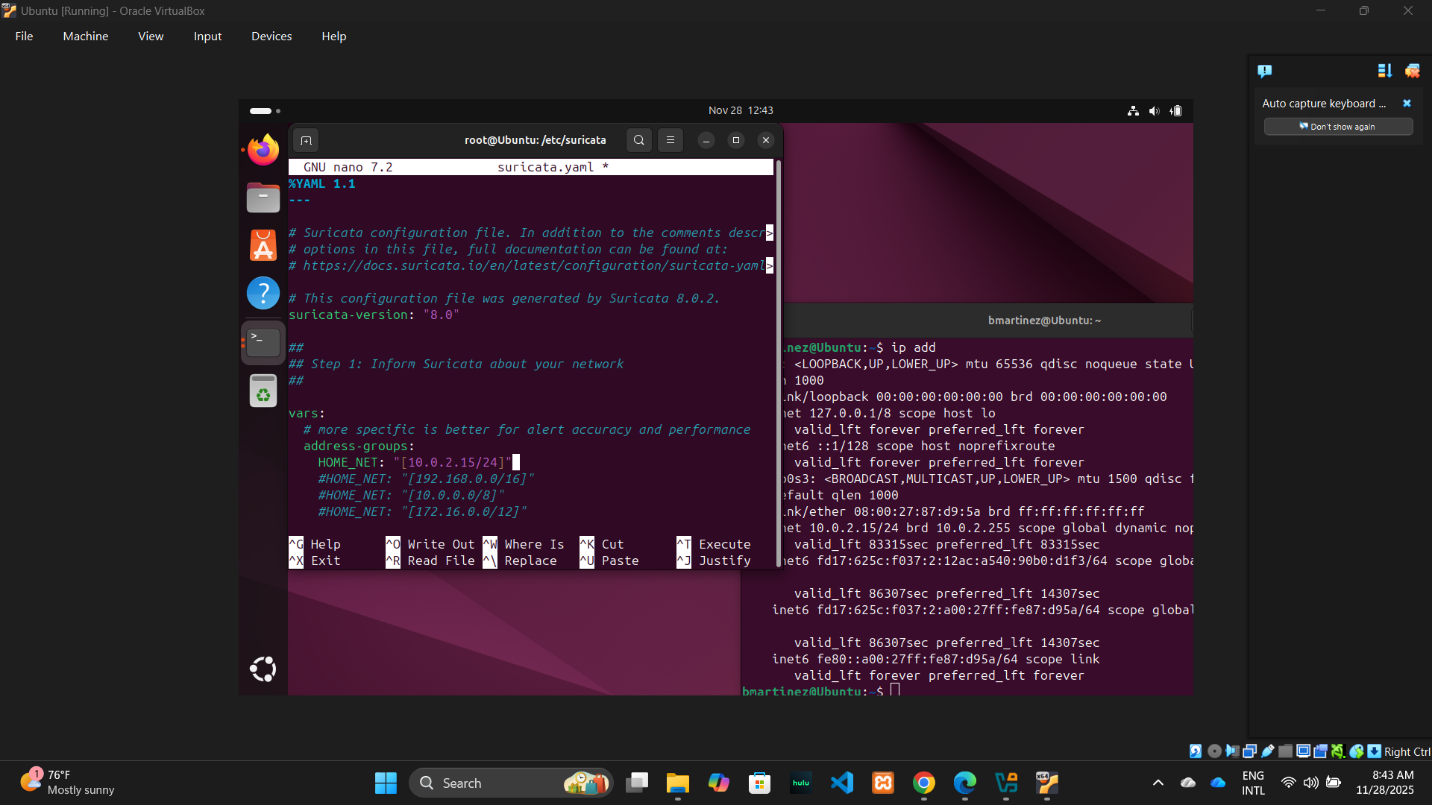
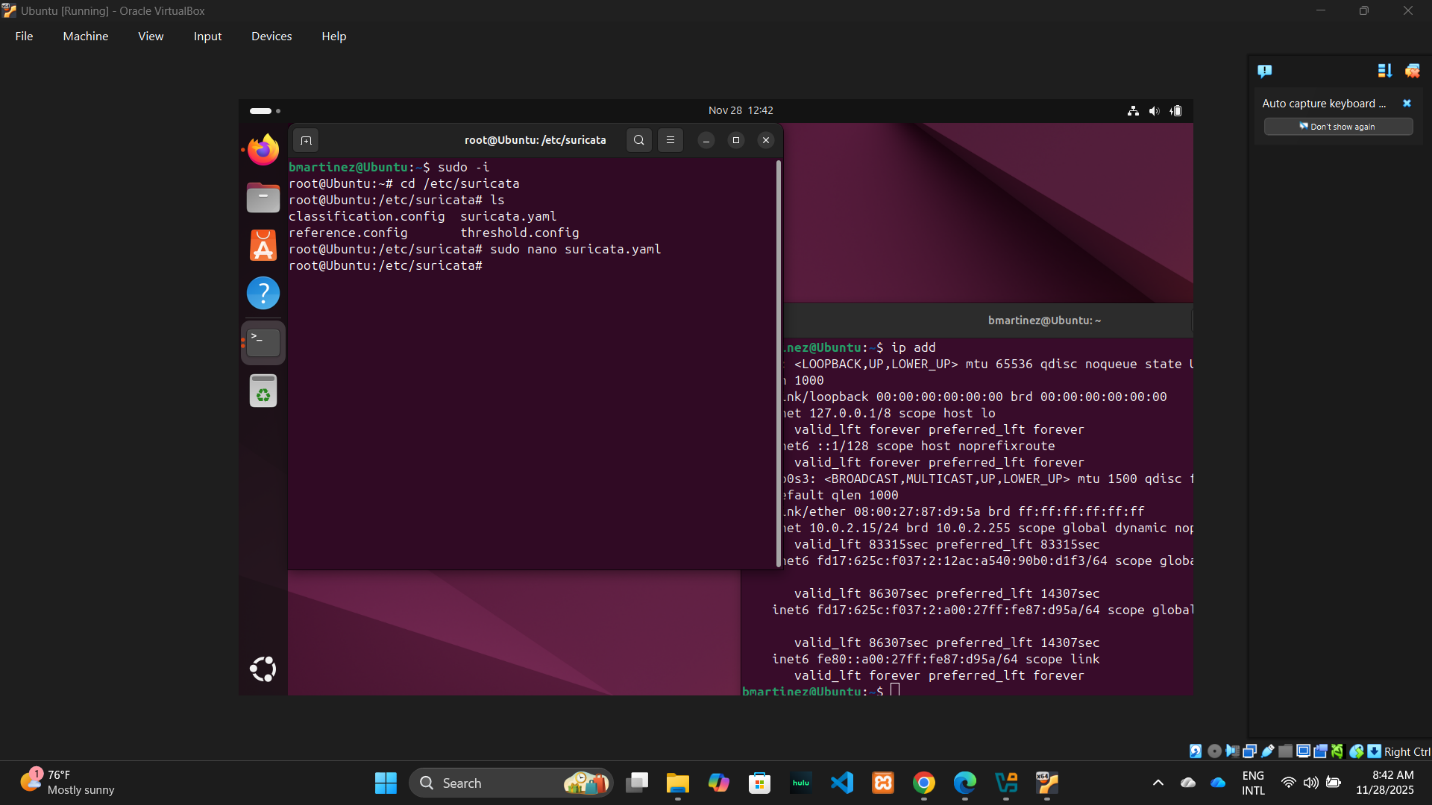
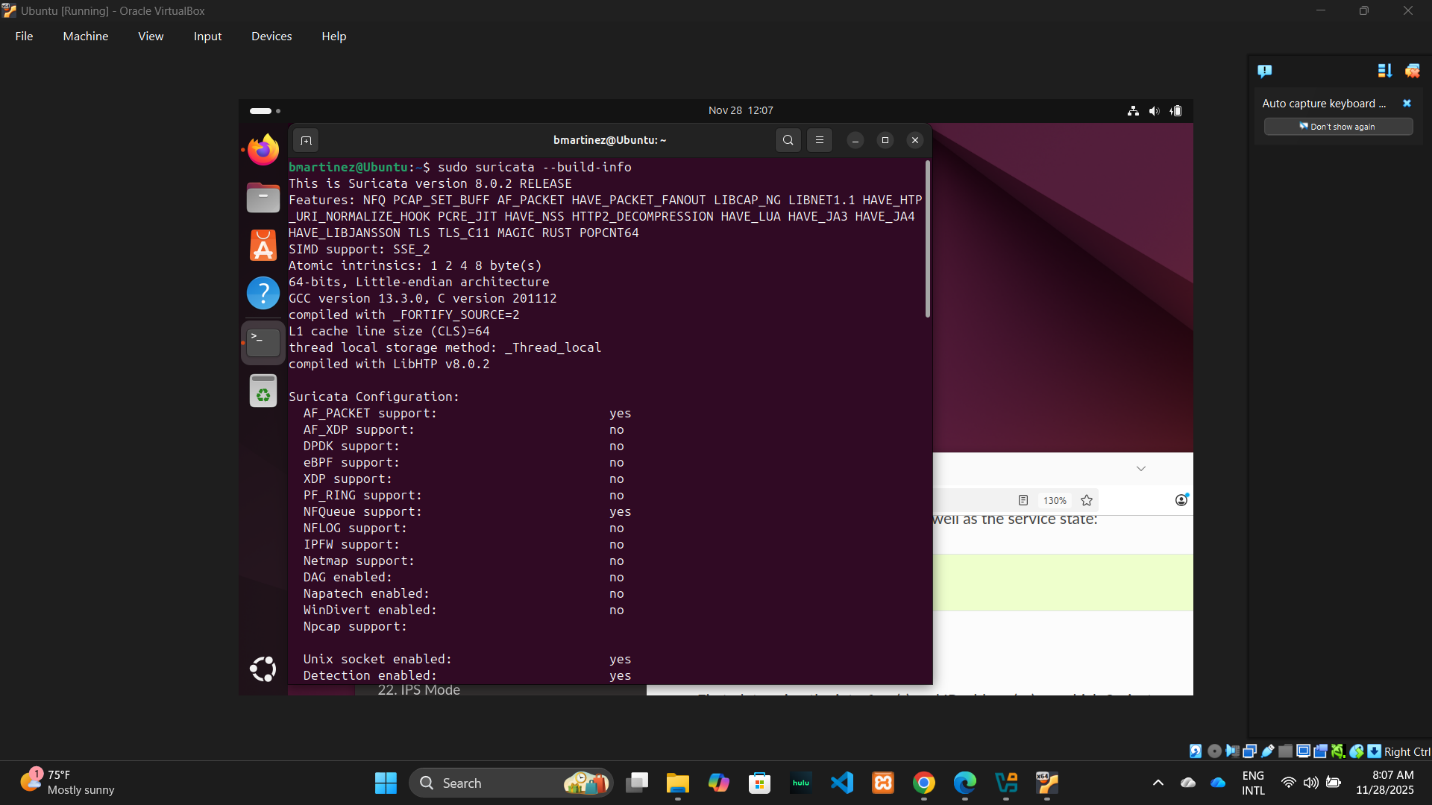
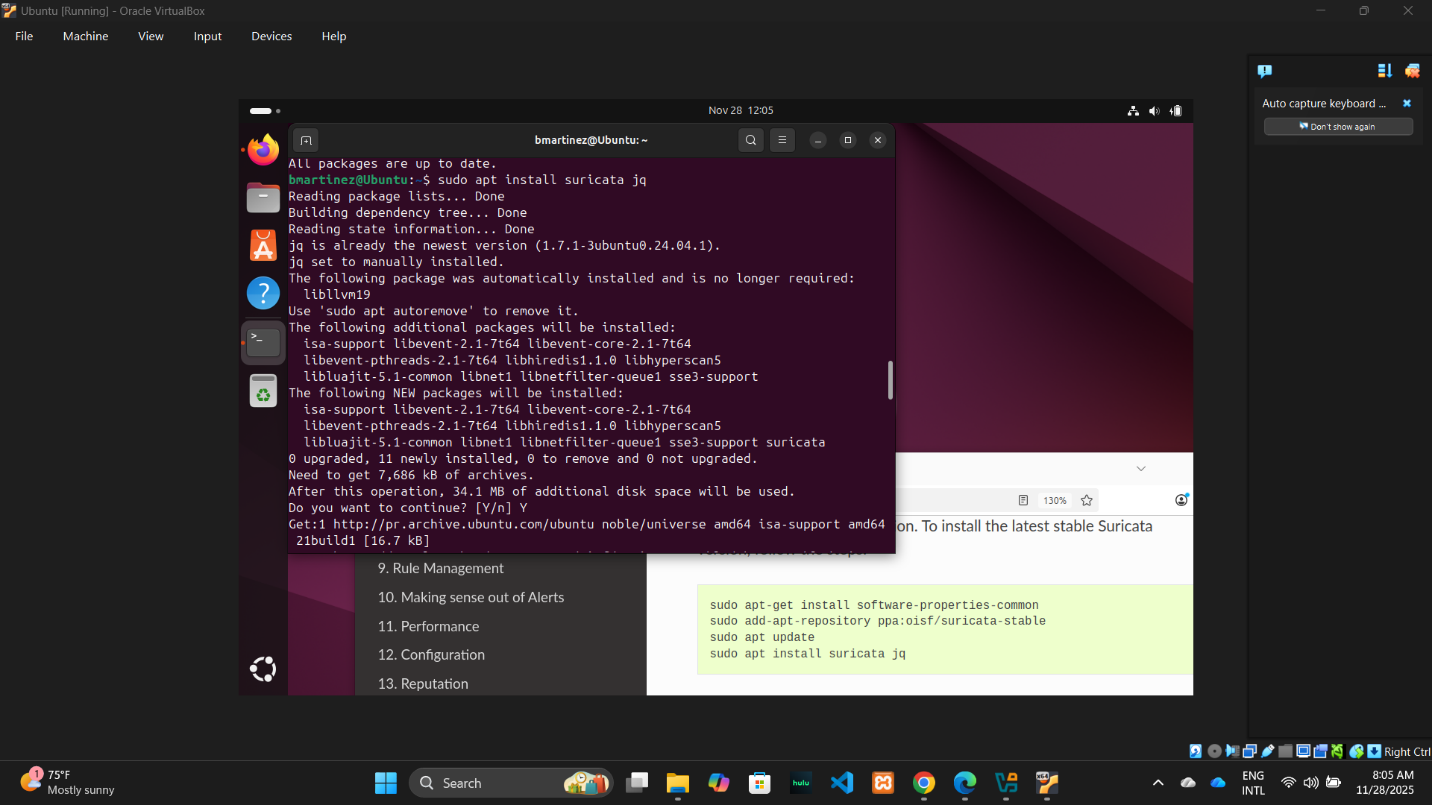
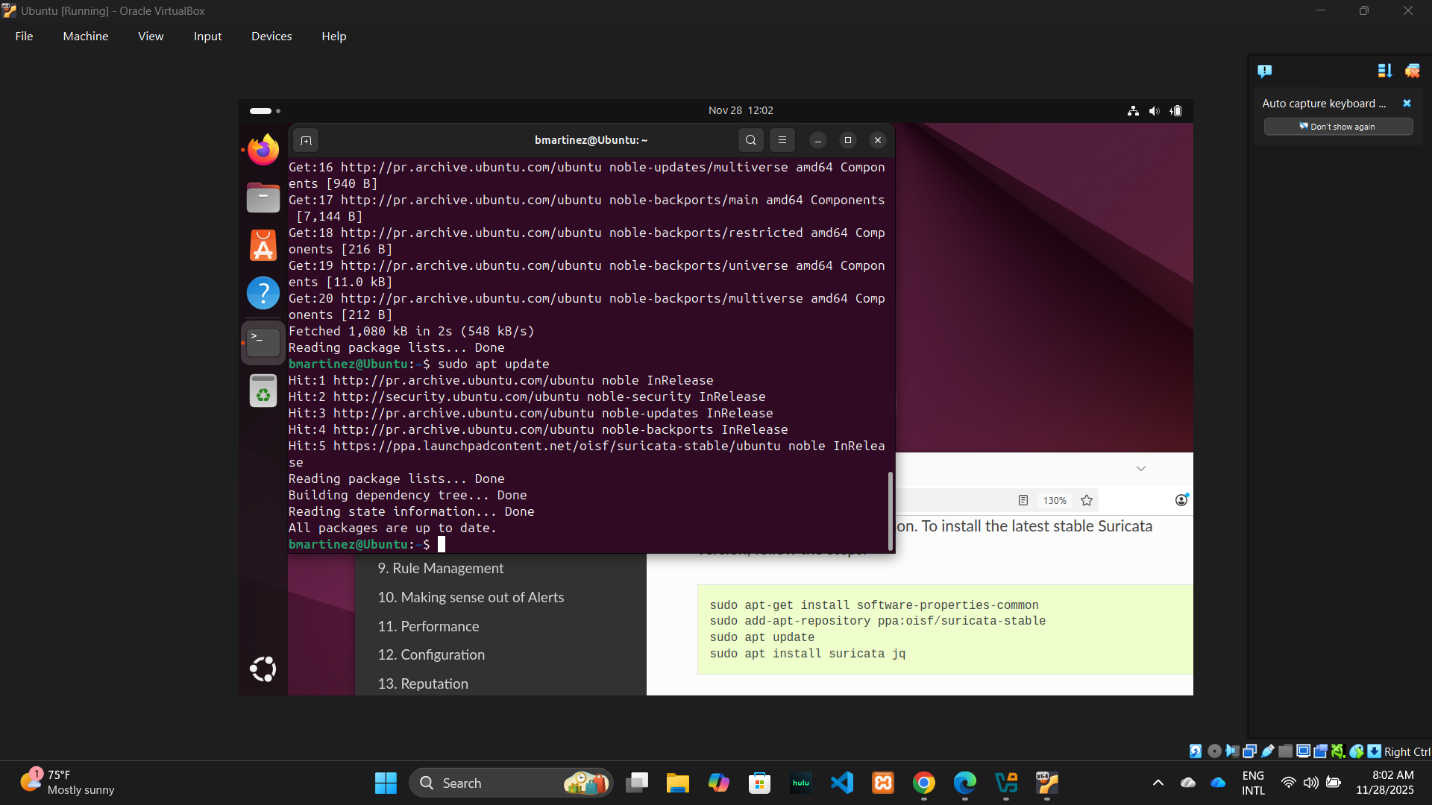
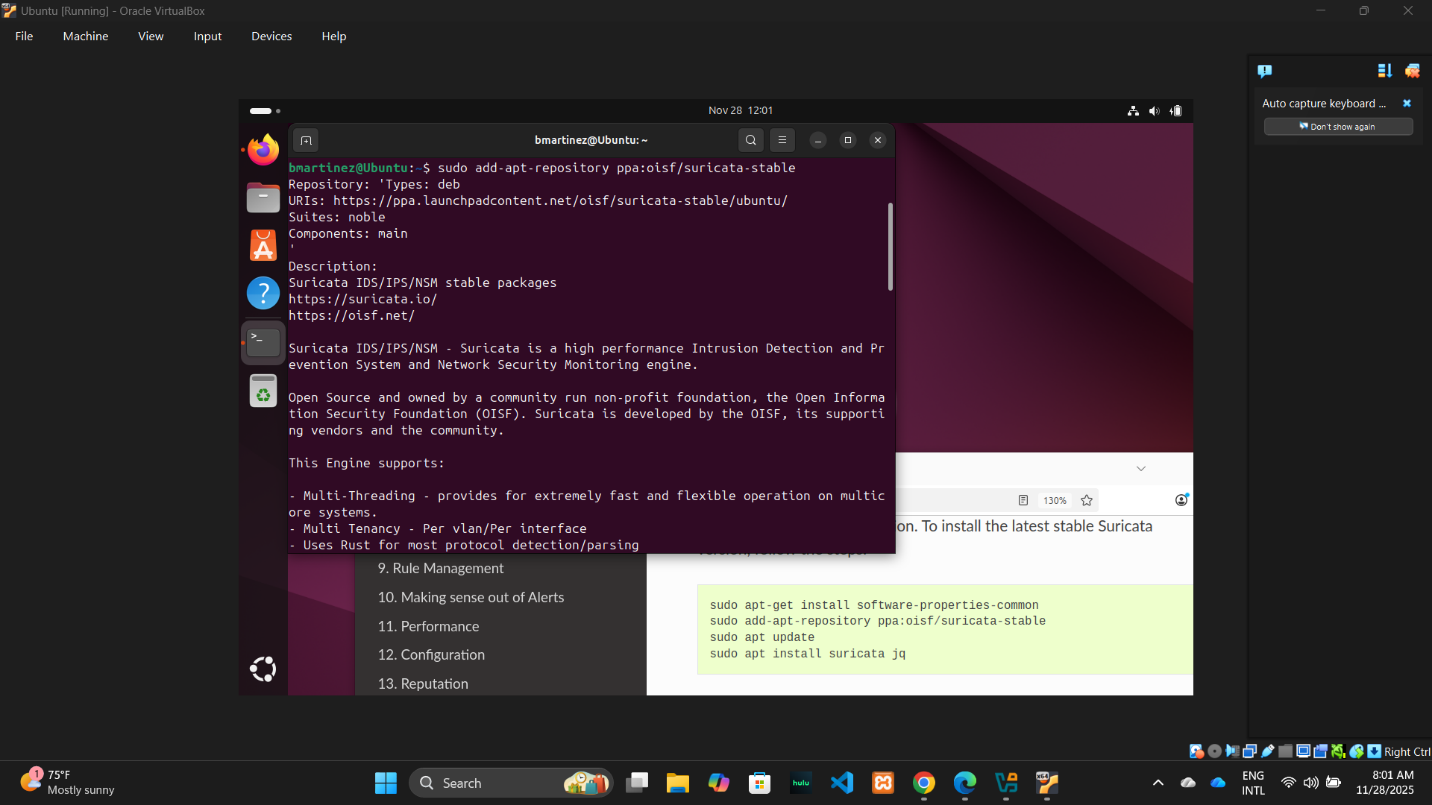
1. **Preparación del entorno:** A screenshot of a computer

   AI-generated content may be incorrect.A screenshot of a computer

   AI-generated content may be incorrect.

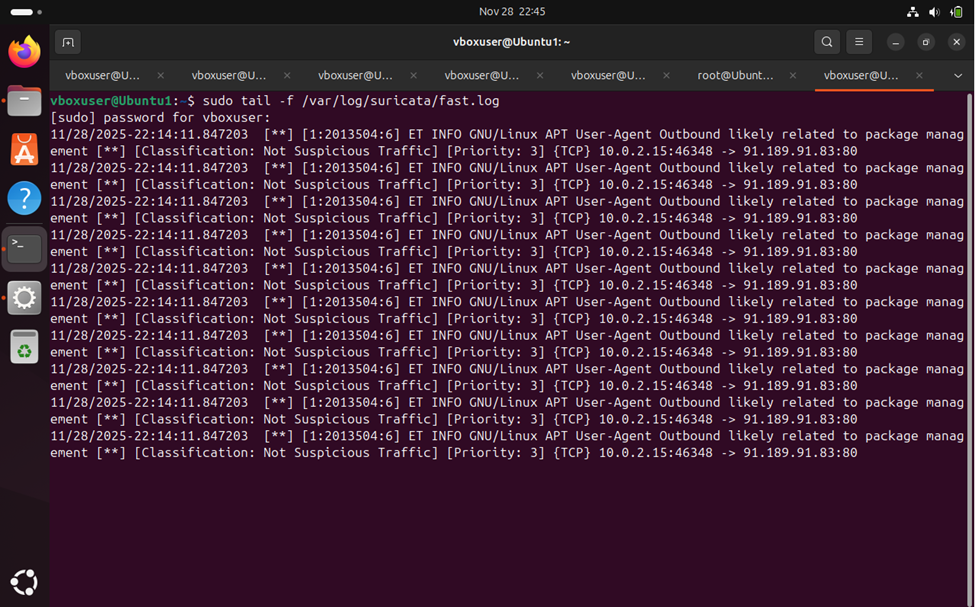
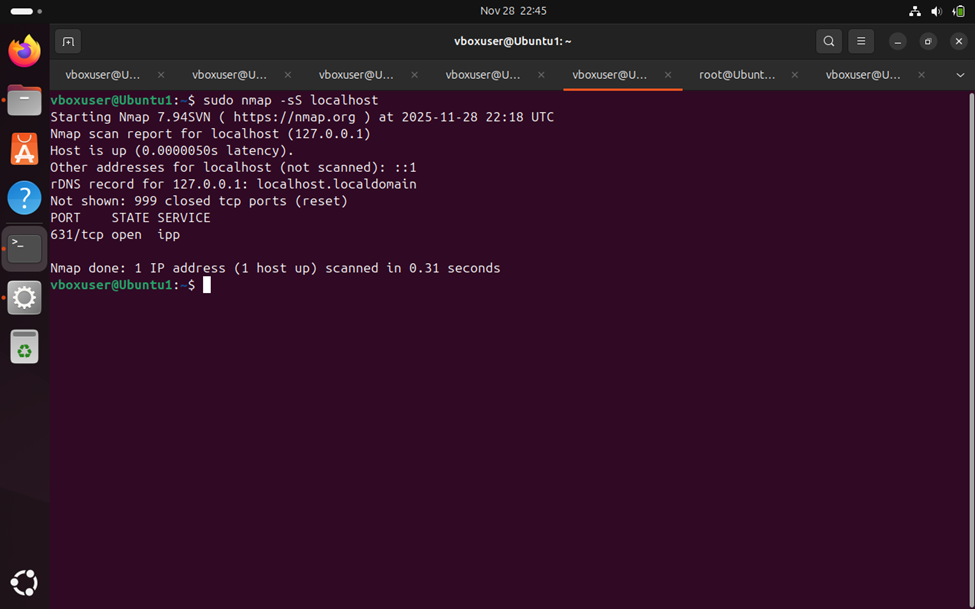
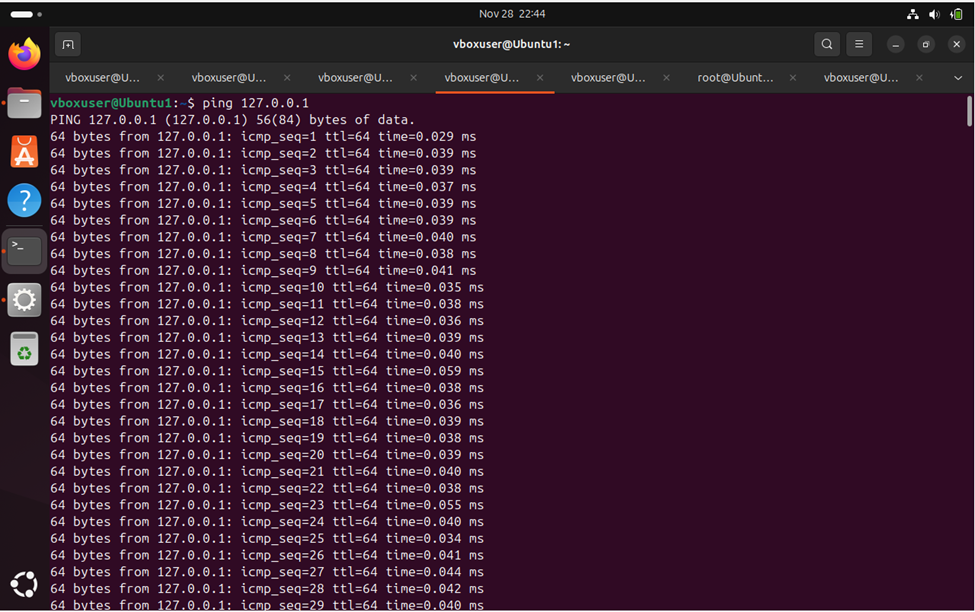


1. **Instalación del IDS (Suricata):** 



1. **Prueba de detección: A screenshot of a computer

   AI-generated content may be incorrect.**

****

1. **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 fina se pudo hacer. También, en entender si lo que esta 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 trafico 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.

**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