



Práctica UD2.- Suricata

SURICATA
PEDRO MANUEL GARCÍA ÁLVAREZ

Índice

1.- INTRODUCCIÓN	3
2.- SURICATA EN MODO IDS.....	3
2.1. ESQUEMA DEL ESCENARIO DE ATAQUE.....	4
2.2. GENERACIÓN DE USUARIOS Y CLAVES	4
3.- MÁQUINA OBJETIVO	6
3.1.- INSTALACIÓN DE UBUNTU EN VIRTUALBOX.....	6
3.2.- INSTALACIÓN DE LA MÁQUINA VIRTUAL KALI.....	16
3.3.- INSTALACIÓN DE SURICATA	19
3.4.- CONFIGURACIÓN DEL SURICATA.....	23
3.5.- VERIFICACIÓN SI ESTA SURICATA CONFIGURADA CORRECTAMENTE	26
3.6.- INSTALACIÓN SSH EN UBUNTU PARA HACER CONEXIONES SSH.....	27
3.7.- MECANISMOS DE DEFENSA	30
4.- PASOS PREVIOS AL ATAQUE	31
4.1.- MÁQUINA OBJETIVO CONFIGURACIÓN DE LA REGLA	31
4.2.- MÁQUINA ATACANTE CONFIGURACIÓN DE LOS ARCHIVOS	32
5.- LANZAMIENTO DEL ATAQUE	33
6.- SURICATA EN MODO IPS (OPCIONAL).....	34
7.- ARCHIVOS A ENTREGAR	37
7.1.- ARCHIVO SURICATA.RULES_IDS	37
7.2.- ARCHIVO SURICATA.RULES_IPS.....	38
7.3.- ARCHIVO FAST.LOG	38
7.4.- ARCHIVO SURICATA.YAML	39
8.- ANEXOS	40
8.1.- CYBER-SEGURIDAD 🐧 INSTALAR SURICATA Y KALI LINUX OK Y CONFIGURAR LAS REGLAS Y ALERTAS	40
8.2.- 🛡️ IPS IDS LINUX 🐧 INSTALAR SURICATA Y CONFIGURAR LAS REGLAS Y ALERTAS 🌐	40
8.3.- ¿CÓMO OBTENER LA CONTRASEÑA DE SERVICIO COMO SSH Y FTP - HYDRA?	41
8.4.- CRUNCH - CREACIÓN DE DICCIONARIOS PARA FUERZA BRUTA	41

1.- Introducción

La presente práctica tiene como objetivo principal la aplicación de herramientas y técnicas de detección y respuesta a incidentes de seguridad en un entorno controlado. En particular, se centra en la utilización de Suricata, una herramienta de detección de intrusiones de código abierto, para identificar y responder a ataques de fuerza bruta contra un servicio SSH.

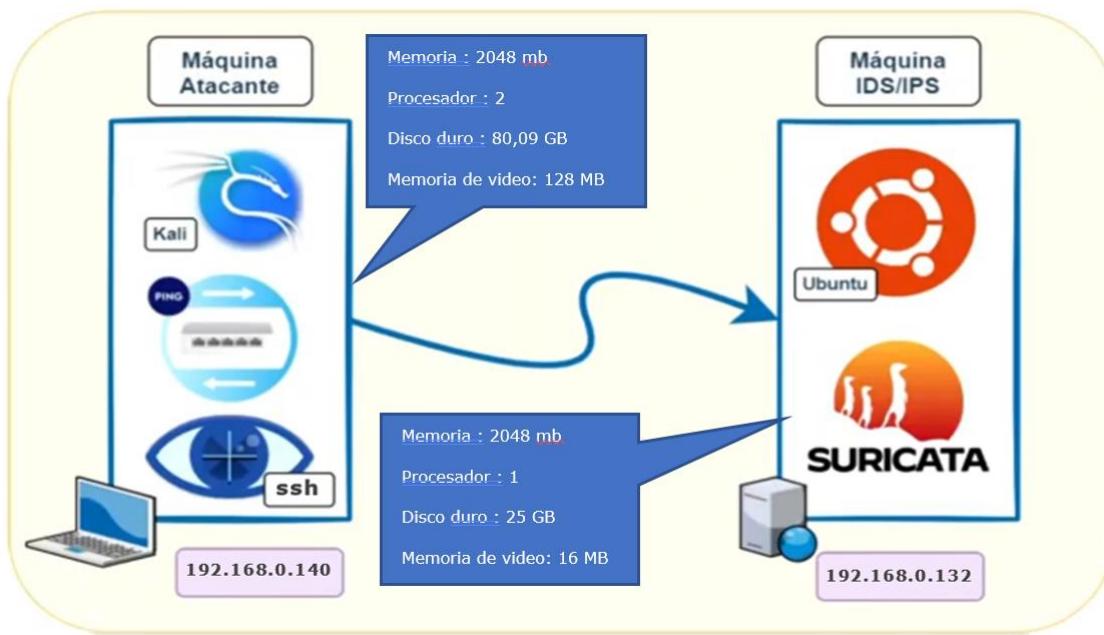
La gestión de incidentes de seguridad es un aspecto fundamental en la ciberseguridad moderna, ya que permite a las organizaciones detectar, responder y recuperarse de eventos que puedan comprometer la integridad, confidencialidad o disponibilidad de sus sistemas y datos. En este contexto, la detección de ataques de fuerza bruta contra servicios como SSH es crucial, ya que estos ataques son comunes y pueden conducir a la compromisión de cuentas y sistemas si no se detectan y mitigan de manera oportuna.

La práctica aborda específicamente la configuración de Suricata en modo IDS (Sistema de Detección de Intrusiones) para detectar y registrar los intentos de conexión SSH sospechosos, así como la implementación opcional de Suricata en modo IPS (Sistema de Prevención de Intrusiones) para bloquear activamente este tipo de tráfico malicioso. Mediante el uso de herramientas como Hydra y Crunch, se simularán ataques de fuerza bruta desde una máquina atacante hacia una máquina objetivo, lo que permitirá poner a prueba la efectividad de las medidas de seguridad implementadas.

En resumen, esta práctica proporciona una oportunidad para familiarizarse con herramientas y técnicas de detección y respuesta a incidentes de seguridad, así como para comprender la importancia de una respuesta proactiva y eficiente ante posibles amenazas cibernéticas.

2.- Suricata en Modo IDS

2.1. Esquema del Escenario de Ataque



Representación gráfica del escenario de ataque y descripción de las máquinas involucradas.

2.2. Generación de Usuarios y Claves

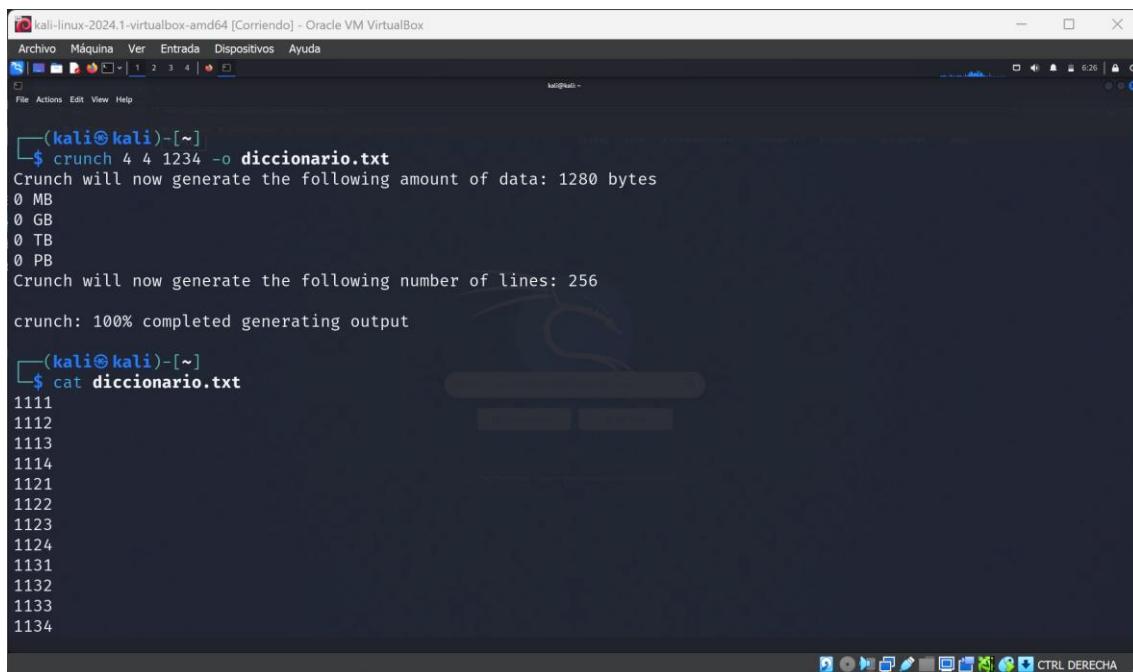
Crunch es una herramienta de línea de comandos utilizada principalmente en sistemas Unix y Linux para generar listas de palabras o contraseñas basadas en patrones definidos por el usuario. Esta herramienta es ampliamente utilizada por profesionales de la seguridad informática y administradores de sistemas para fines diversos, como pruebas de penetración, auditorías de seguridad y pruebas de fuerza bruta.

Con Crunch, los usuarios pueden especificar la longitud mínima y máxima de las palabras o contraseñas a generar, así como los caracteres permitidos y los patrones de caracteres que se utilizarán. Por ejemplo, puedes generar contraseñas que contengan solo letras minúsculas, letras mayúsculas, números y caracteres especiales, o cualquier combinación de estos.

Crunch es muy flexible y potente, permitiendo a los usuarios personalizar completamente la generación de palabras o contraseñas según sus necesidades específicas. Además, puede generar grandes

volúmenes de palabras o contraseñas en poco tiempo, lo que lo hace útil para pruebas de seguridad a gran escala.

En resumen, Crunch es una herramienta útil para generar listas de palabras o contraseñas personalizadas basadas en patrones definidos por el usuario, y es comúnmente utilizada en el campo de la seguridad informática.



The screenshot shows a terminal window titled '(kali㉿kali)-[~]'. The user has run the command '\$ crunch 4 4 1234 -o diccionario.txt'. The output indicates that Crunch will generate 1280 bytes of data and 256 lines. After the command completes, the user runs '\$ cat diccionario.txt' to view the generated dictionary, which contains lines such as 1111, 1112, 1113, 1114, 1121, 1122, 1123, 1124, 1131, 1132, 1133, and 1134.

En esta pantalla, se procede a crear el diccionario con el programa Crunch con los parámetros siguientes:

crunch 4 4 1234 -o diccionario.txt

crunch: Es el nombre del programa o comando que estás ejecutando. En este caso, se trata del programa "crunch" que se utiliza para generar contraseñas o listas de palabras basadas en ciertos criterios.

4: Este primer número indica la longitud mínima de las contraseñas o palabras generadas. En este caso, estás indicando que las contraseñas tendrán una longitud mínima de 4 caracteres.

4: El segundo número representa la longitud máxima de las contraseñas o palabras generadas. Aquí, estás

estableciendo que las contraseñas tendrán una longitud máxima de 4 caracteres.

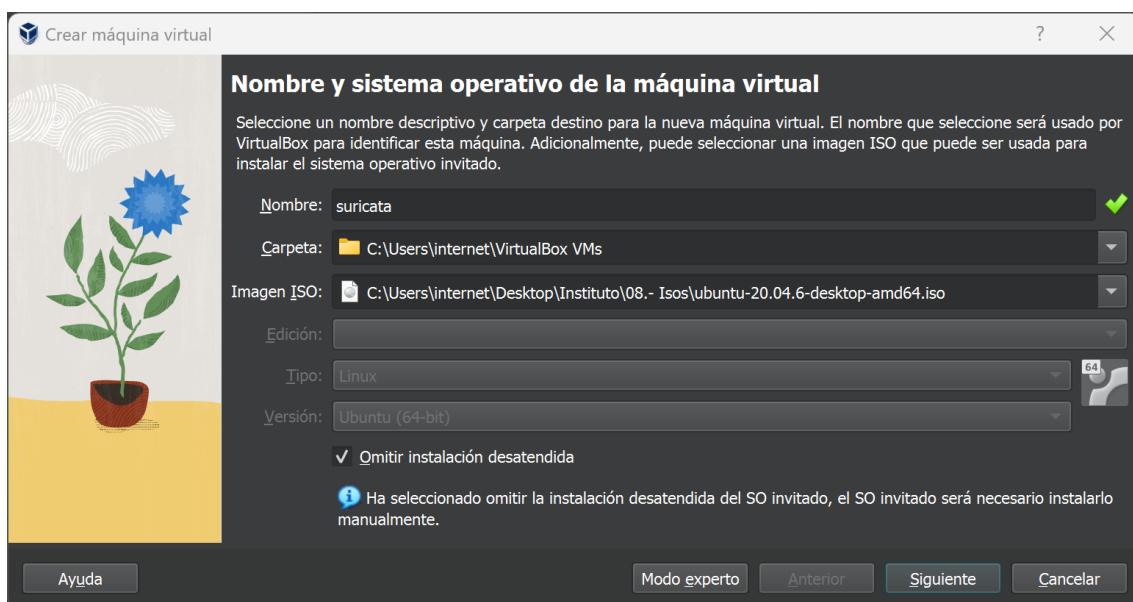
1234: Este es el patrón o conjunto de caracteres que se utilizará para generar las contraseñas o palabras. En este caso, estás diciendo que solo se utilizarán los números del 1 al 4 para generar las contraseñas.

-o diccionario.txt: Aquí estás indicando que las contraseñas o palabras generadas se guardarán en un archivo llamado "diccionario.txt". La opción -o se utiliza para especificar el nombre del archivo de salida.

En resumen, este comando ejecutará el programa "crunch" para generar contraseñas o palabras que tengan una longitud entre 4 y 4 caracteres, utilizando solo los números del 1 al 4 como caracteres posibles. Luego, guardará estas contraseñas o palabras en un archivo llamado "diccionario.txt".

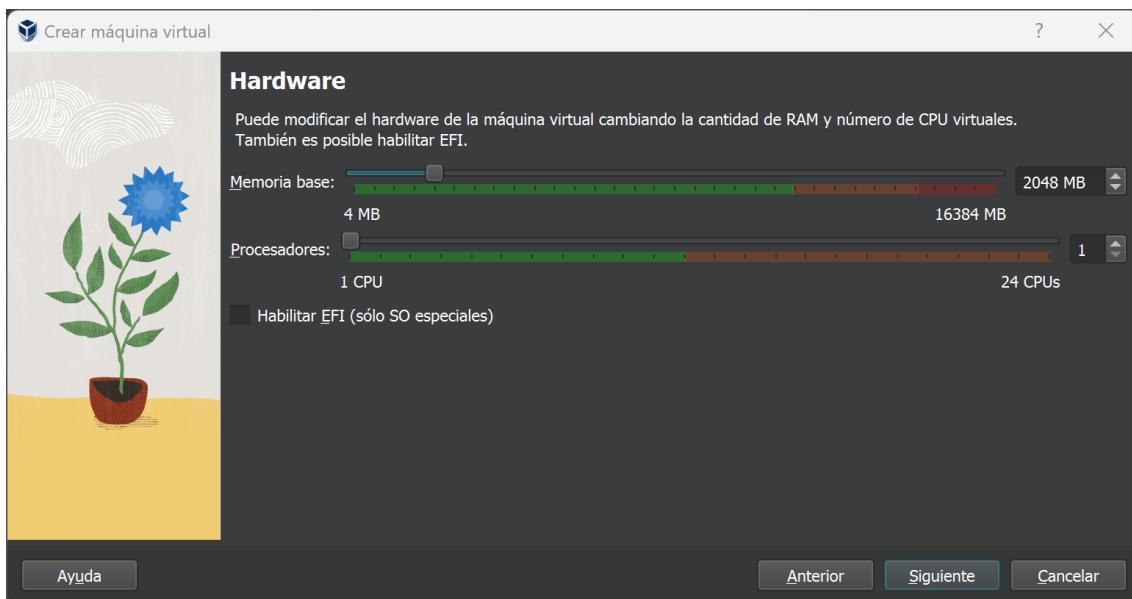
3.- Máquina Objetivo

3.1.- Instalación de ubuntu en virtualbox.

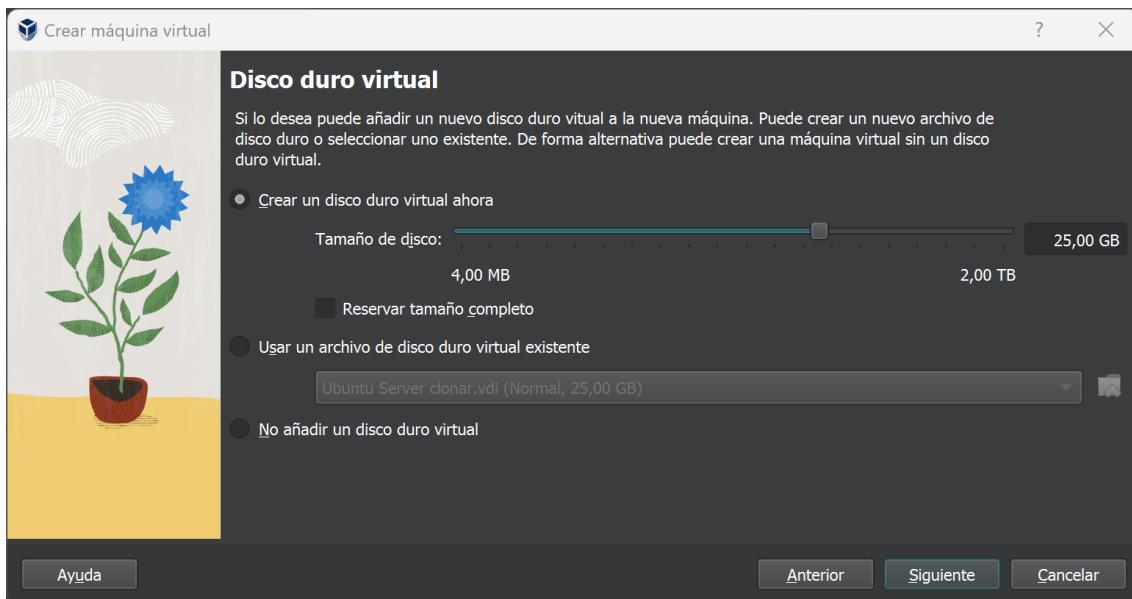


En esta pantalla, estamos llevando a cabo la instalación de la máquina virtual. Establecemos el nombre de la máquina como "suricata" y elegimos la ubicación de la carpeta en "c:/users/internet/virtualbox vms". Para la imagen de instalación, seleccionamos "ubuntu-20.04.6-desktop-amd64.iso" y optamos por

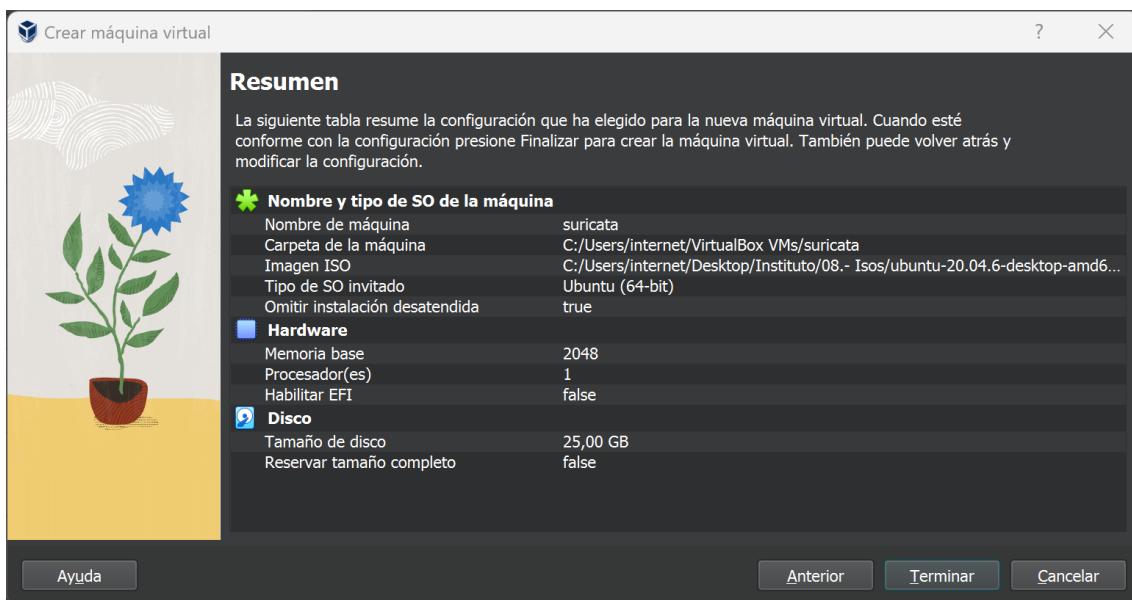
omitir la instalación desatendida. Finalmente, procedemos a hacer clic en el botón "Siguiente".



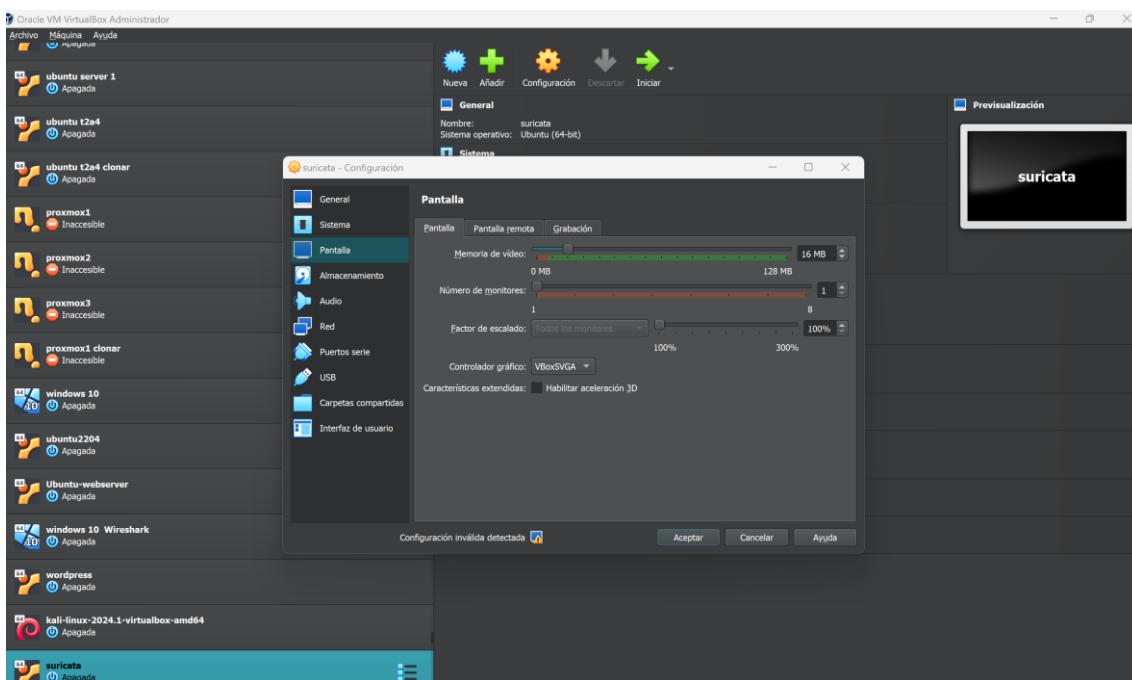
En este paso, estamos configurando la máquina virtual. Establecemos la memoria base en 2048 MB y asignamos 1 CPU como procesador. Luego, hacemos clic en el botón "Siguiente" para continuar con la configuración.



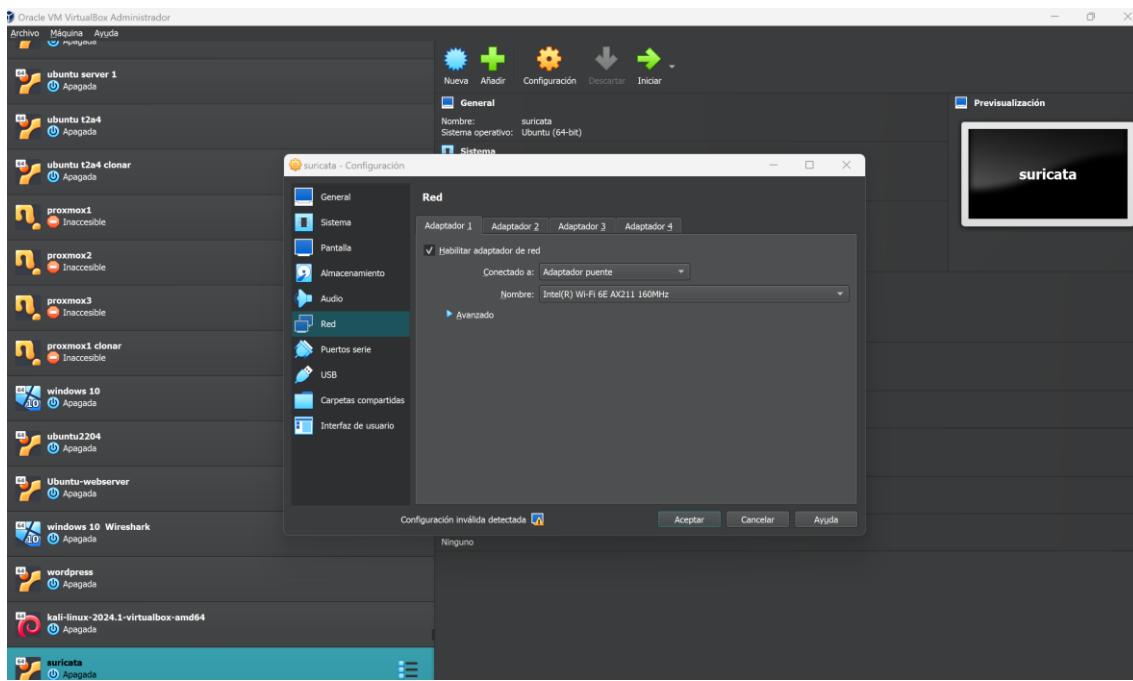
En esta etapa, configuramos el tamaño del disco virtual, optando por 25 GB. Posteriormente, hacemos clic en el botón "Siguiente" para avanzar en el proceso.



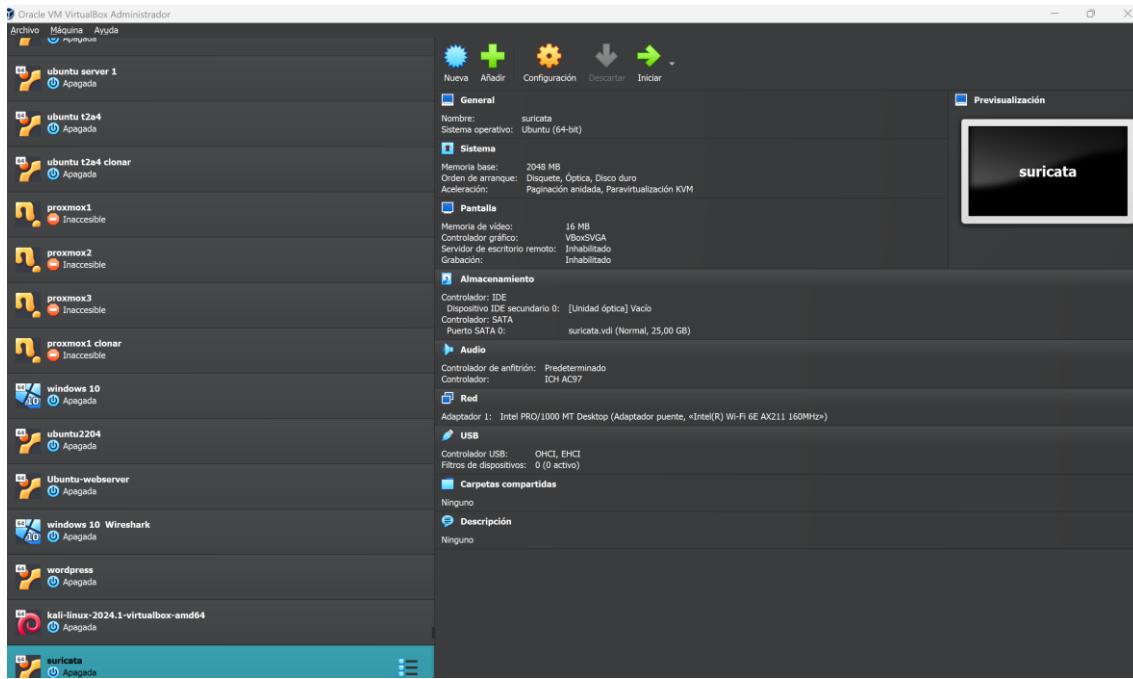
En este punto, se muestra un resumen de la configuración de la máquina virtual que estamos creando. Aquí podemos revisar los ajustes que hemos seleccionado previamente antes de finalizar la creación de la máquina virtual.



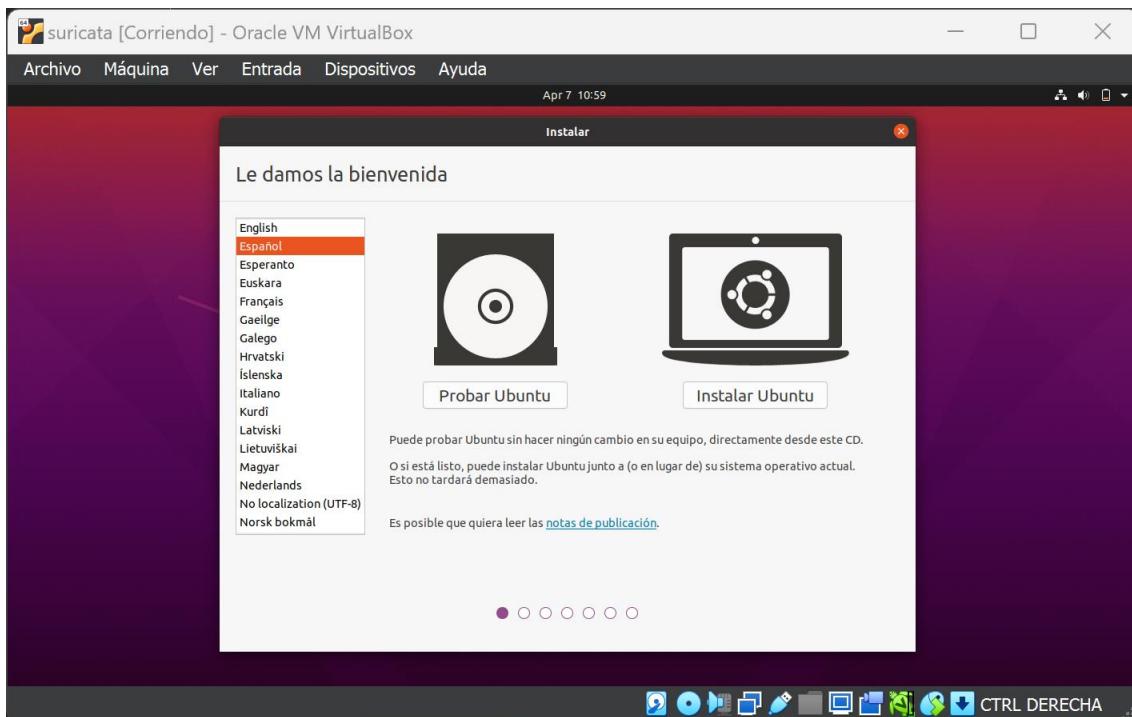
En esta etapa, configuramos la pantalla para evitar que la instalación se vea cortada. Para lograrlo, accedemos a la configuración de la imagen de la máquina virtual, seleccionamos la opción de pantalla y dentro de ella, establecemos el controlador gráfico en "VBoxSVGA". Posteriormente, confirmamos la configuración presionando el botón "Aceptar".



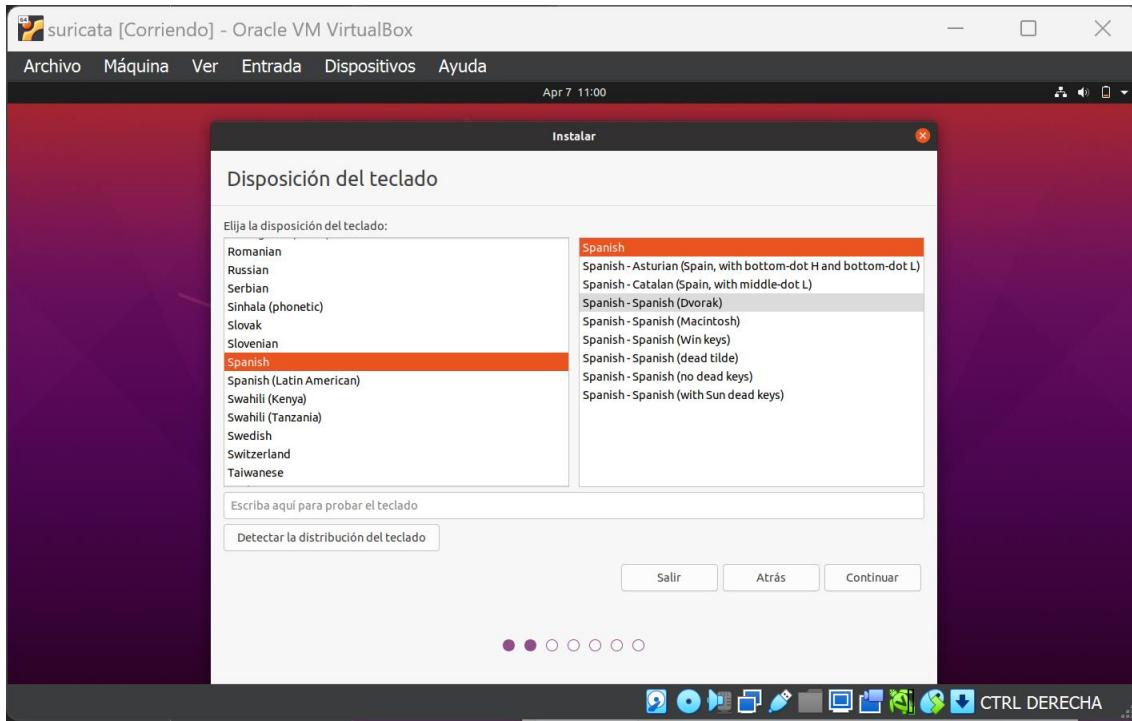
En este punto, realizamos la configuración de la máquina virtual accediendo a la opción de red. Seleccionamos la configuración "Conectado a: Adaptador puente" para establecer la conexión adecuada. Finalmente, confirmamos esta configuración al pulsar el botón "Aceptar".



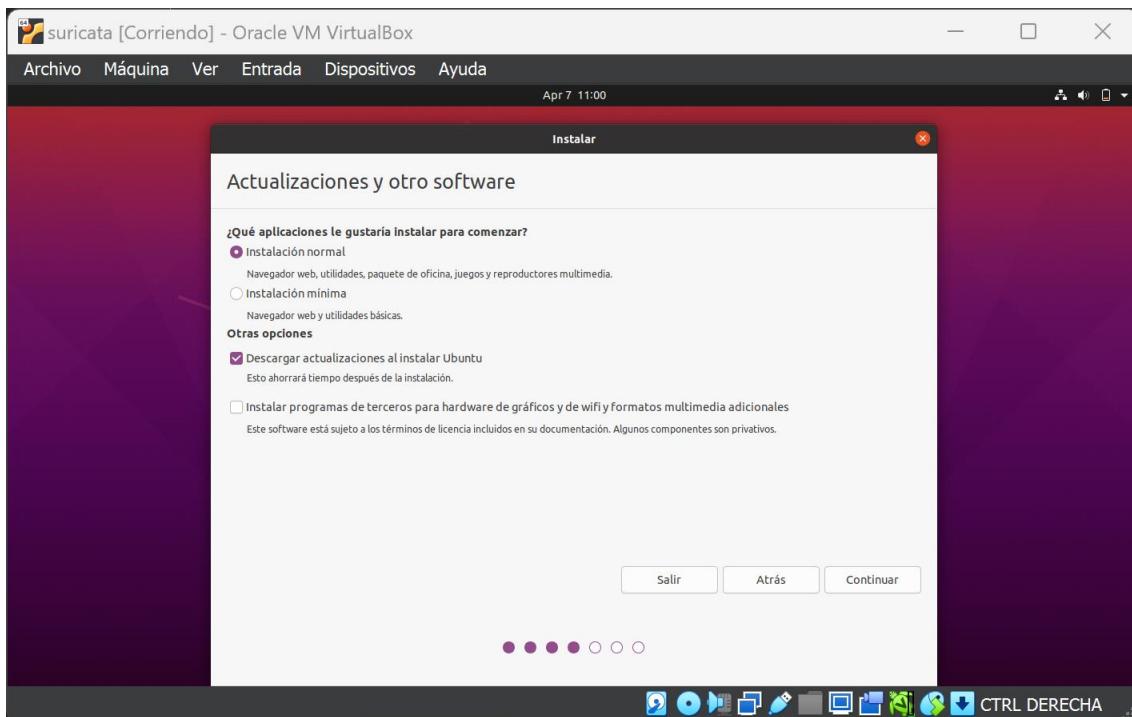
En esta etapa, procedemos a iniciar la máquina virtual para comenzar su instalación. Para hacerlo, simplemente hacemos doble clic sobre la máquina virtual para ejecutarla.



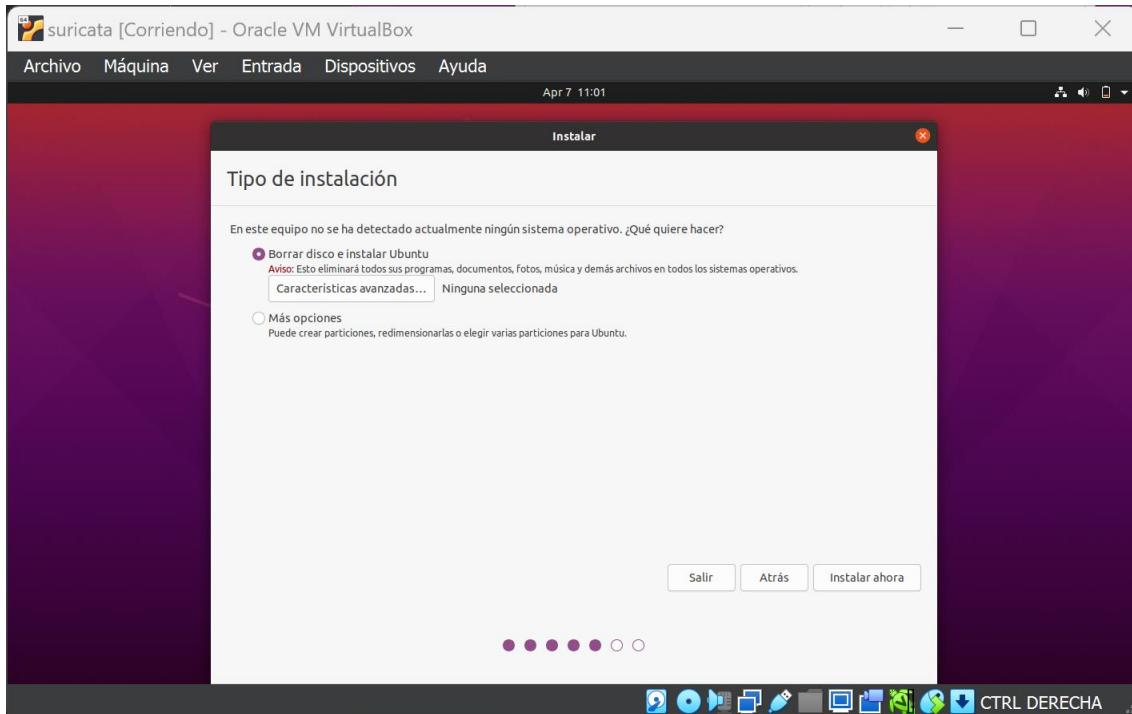
En esta fase, iniciamos el proceso de instalación de Ubuntu. Seleccionamos el idioma español y luego hacemos clic en el botón "Instalar Ubuntu" para comenzar la instalación del sistema operativo.



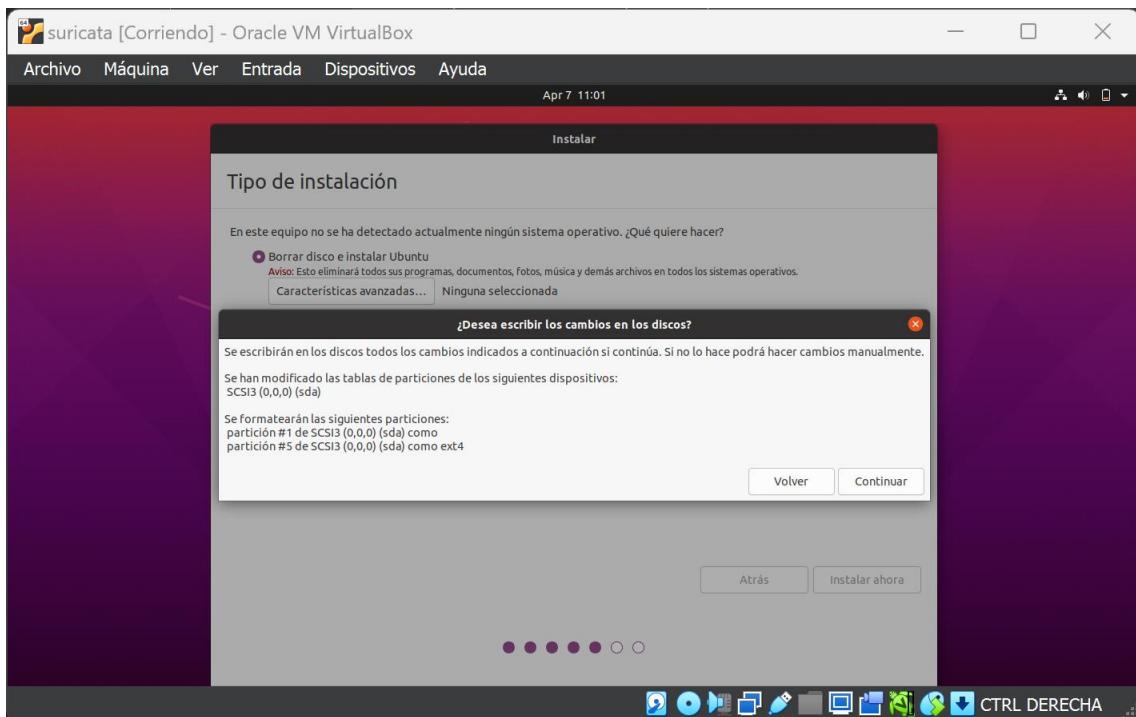
En este paso, seleccionamos el idioma del teclado, optando por "Spanish" y luego especificamos la variante como "Spanish". Posteriormente, pulsamos el botón "Continuar" para avanzar en el proceso de instalación.



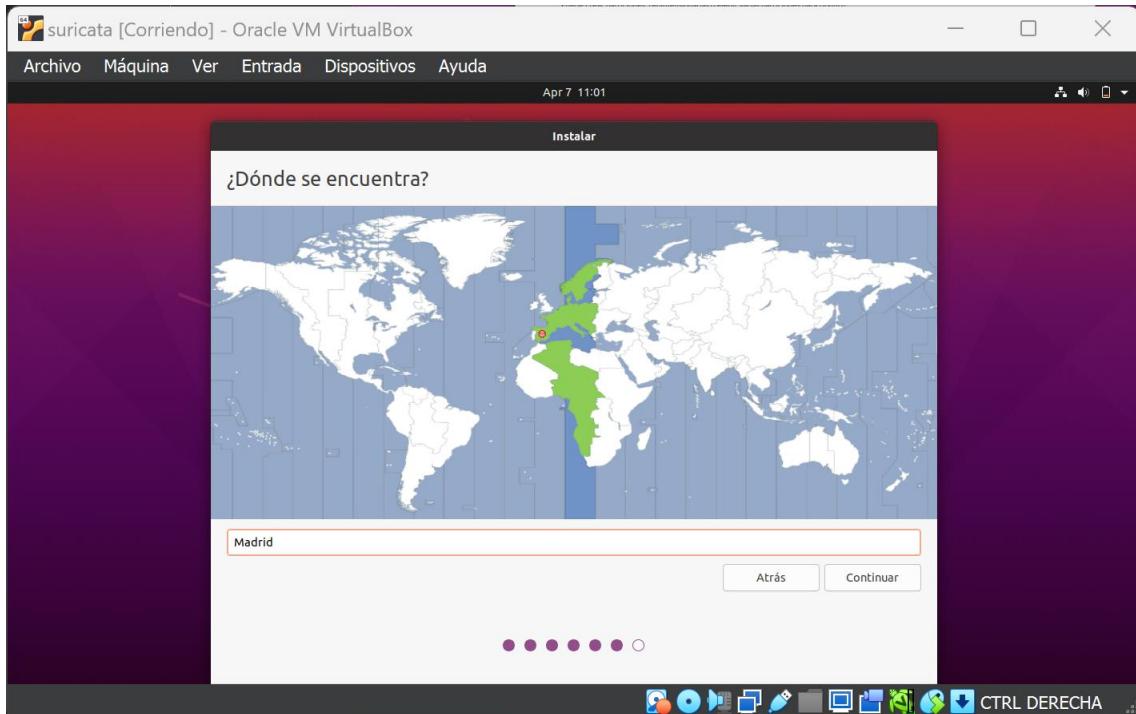
En este punto, configuramos la instalación de manera normal y optamos por descargar las actualizaciones durante la instalación de Ubuntu. Luego, hacemos clic en el botón "Continuar" para proseguir con el proceso de instalación.



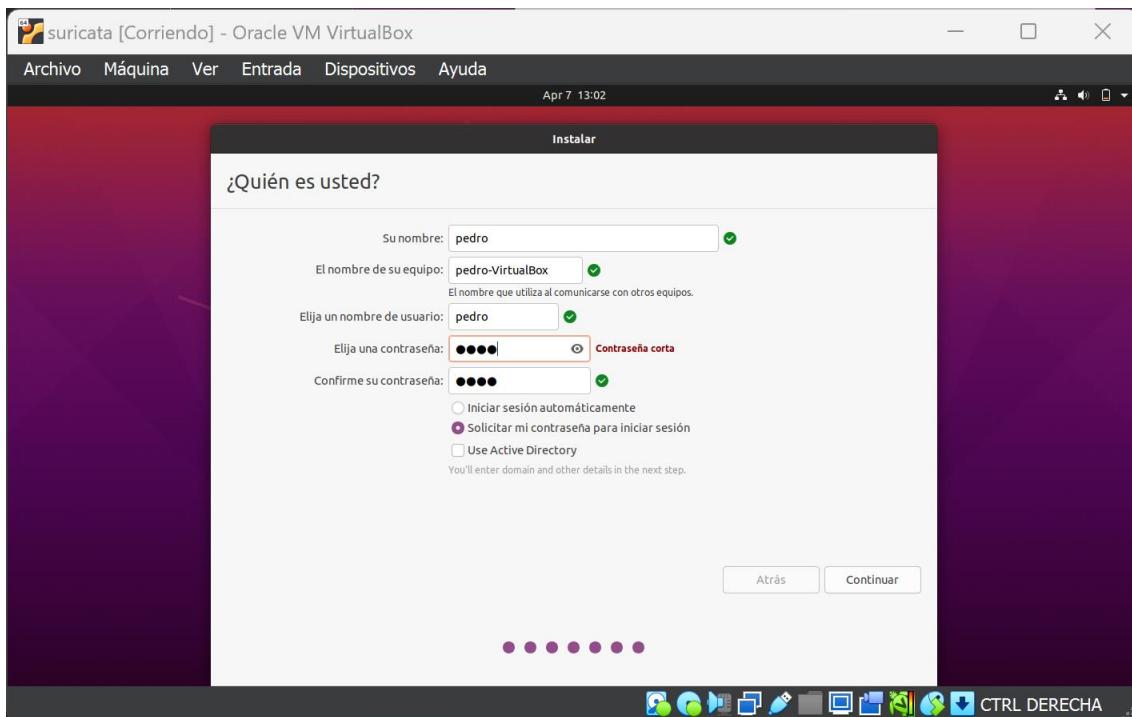
En esta etapa, seleccionamos el tipo de instalación "Borrar disco e instalar Ubuntu" para proceder con la instalación del sistema operativo en el disco. Luego, hacemos clic en el botón "Instalar ahora" para iniciar el proceso de instalación.



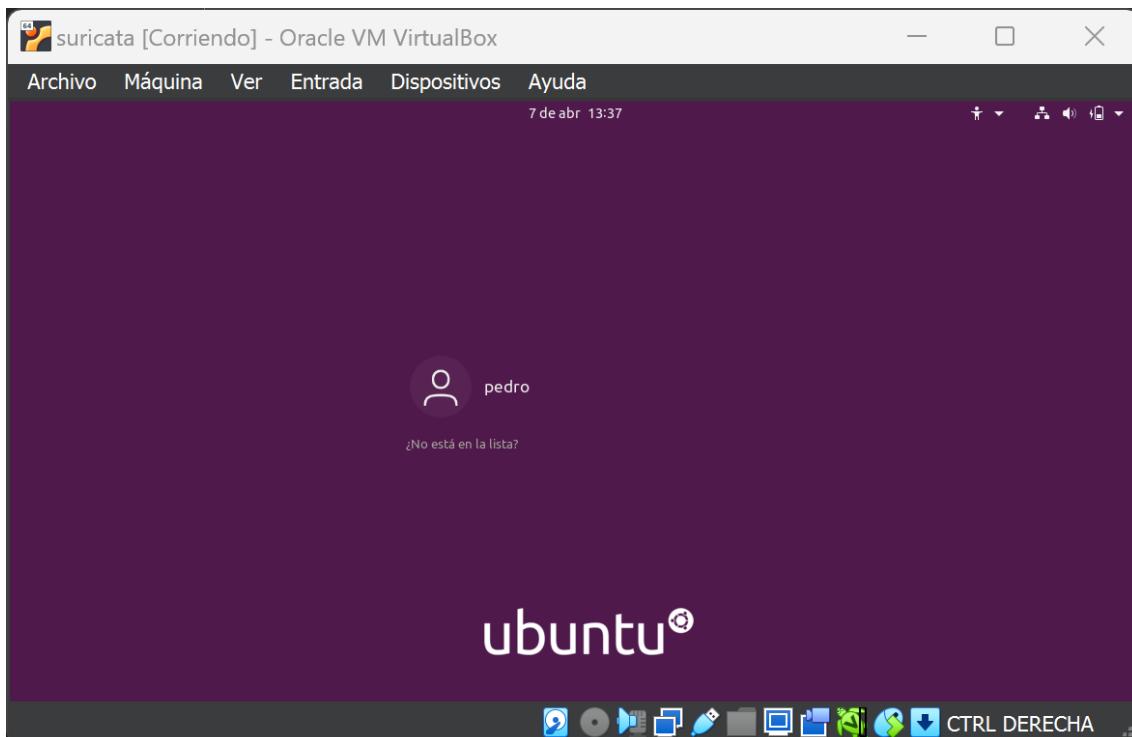
En esta pantalla, se muestra un aviso para confirmar si deseamos sobrescribir el disco duro. Si estamos seguros de que queremos proceder y no hay datos importantes en el disco, pulsamos el botón "Continuar" para confirmar y continuar con la instalación.



En este paso, configuraremos la ubicación seleccionando "Madrid" como la ubicación deseada. Después de seleccionarla, pulsamos el botón "Continuar" para avanzar en el proceso de instalación.

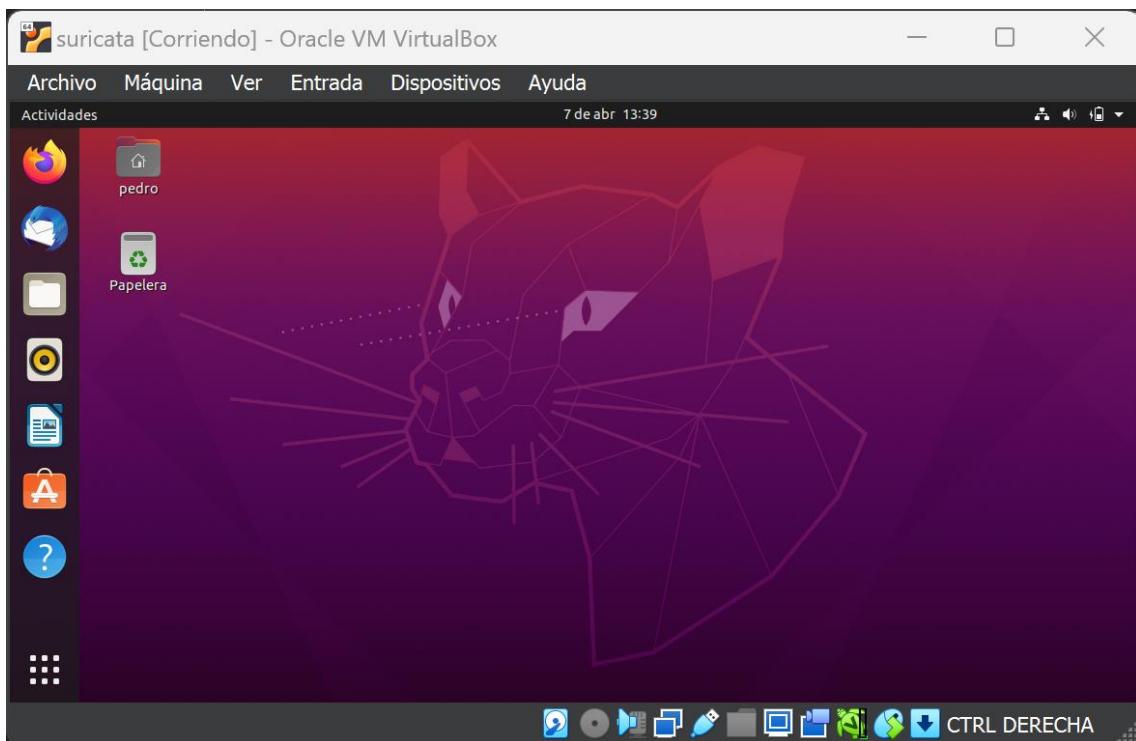


En este punto, llevamos a cabo la configuración de detalles importantes como el nombre, el nombre del equipo, el nombre de usuario y la contraseña. Optamos por la opción de "Solicitar mi contraseña para iniciar sesión". Una vez completada esta configuración, pulsamos el botón "Continuar" para proseguir con el proceso de instalación.

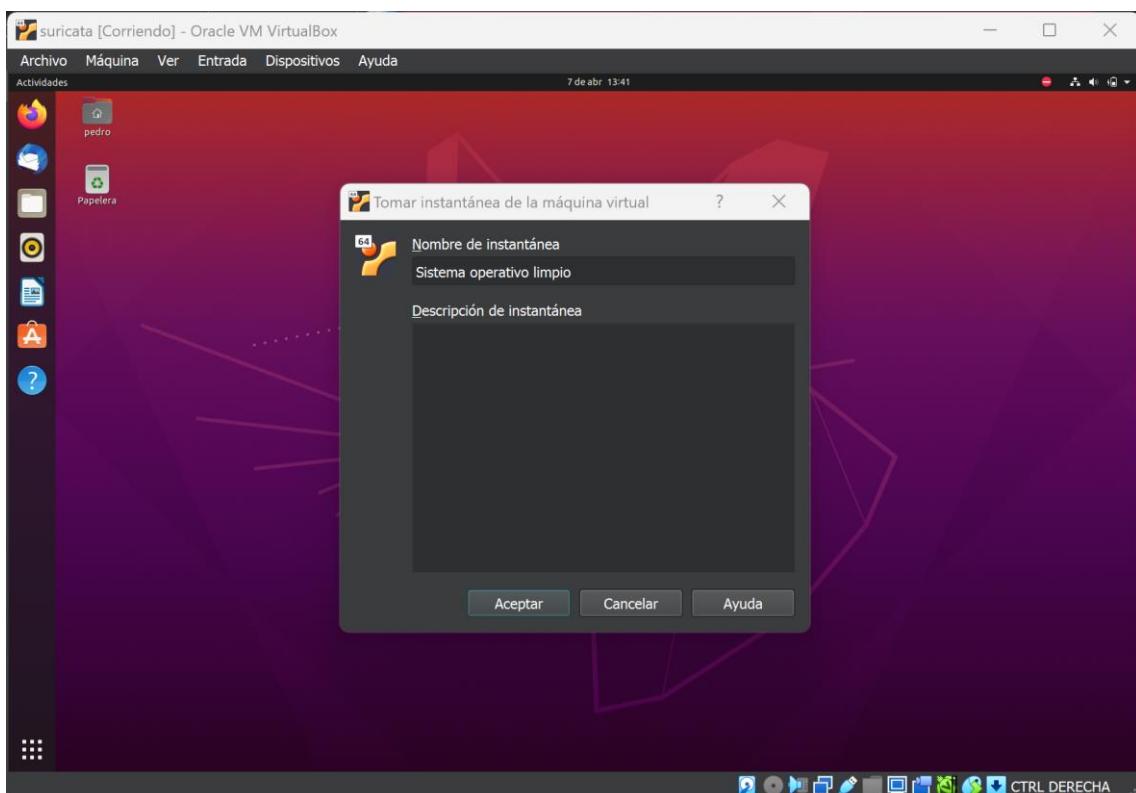


En esta pantalla, observamos el reinicio del sistema operativo recién instalado. Luego, procedemos a hacer clic en el nombre de

usuario y escribimos la contraseña correspondiente para iniciar sesión en la sesión del sistema operativo.



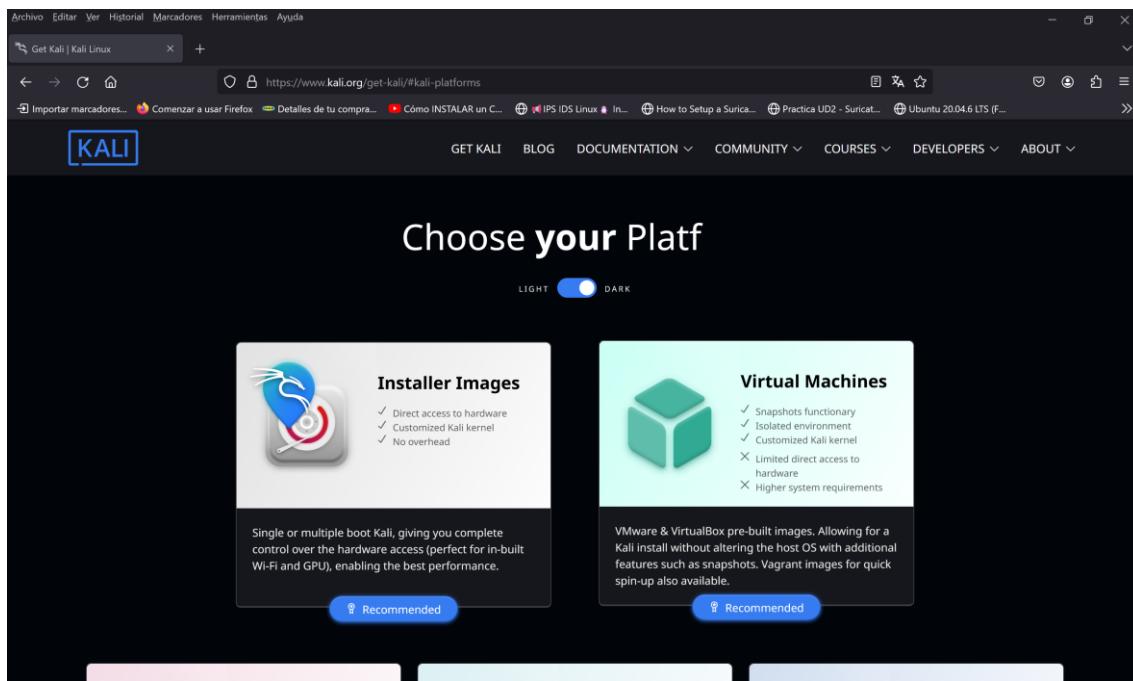
En esta pantalla, visualizamos el sistema operativo que ha sido instalado correctamente y está listo para ser utilizado.



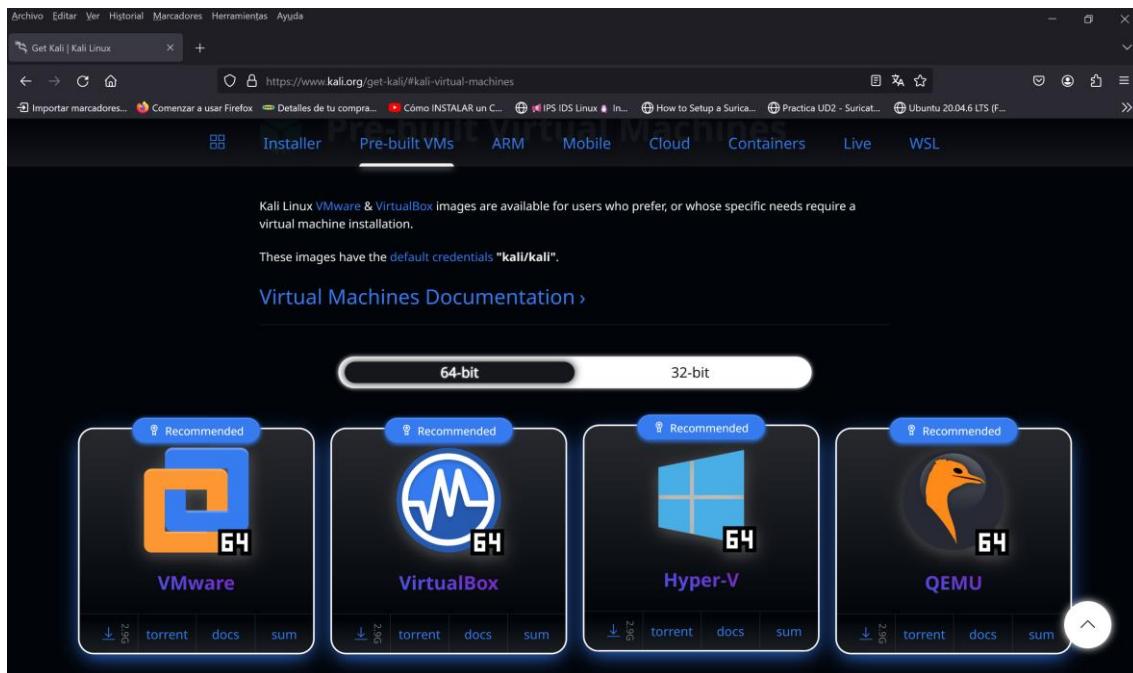
En esta etapa, accedemos al menú de VirtualBox a la opción Máquina y seleccionamos la opción "Tomar instantánea" para crear una

instantánea que nos permitirá regresar a este punto en caso de algún error. Le damos un nombre, como por ejemplo "Sistema Operativo Limpio", y luego pulsamos el botón "Aceptar" para confirmar la creación de la instantánea.

3.2.- Instalación de la máquina virtual Kali.

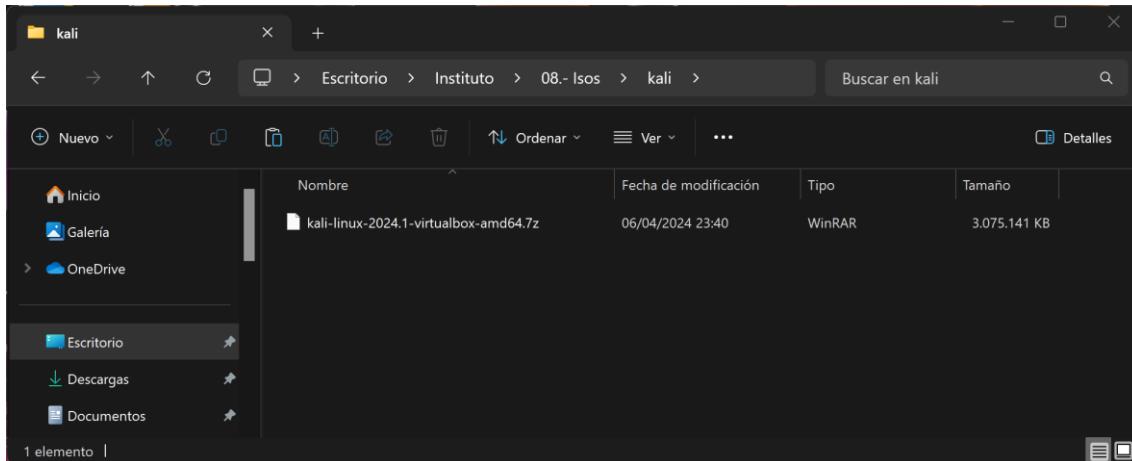


En esta pantalla, nos dirigimos al sitio web <https://www.kali.org/get-kali/#kali-platforms> para descargar la imagen de Kali Linux para VirtualBox.

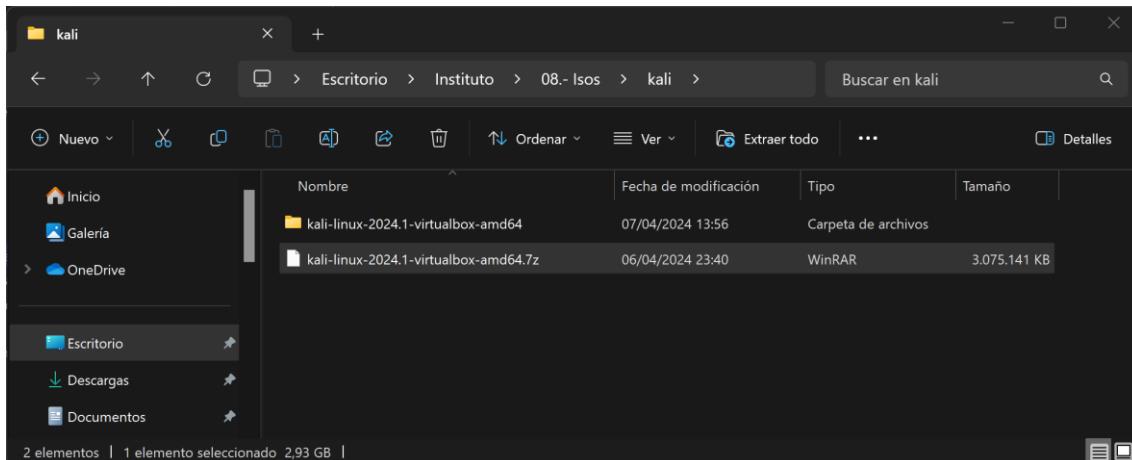


En esta etapa, realizamos la descarga de la imagen VirtualBox 64 desde la página web correspondiente. Simplemente hacemos doble

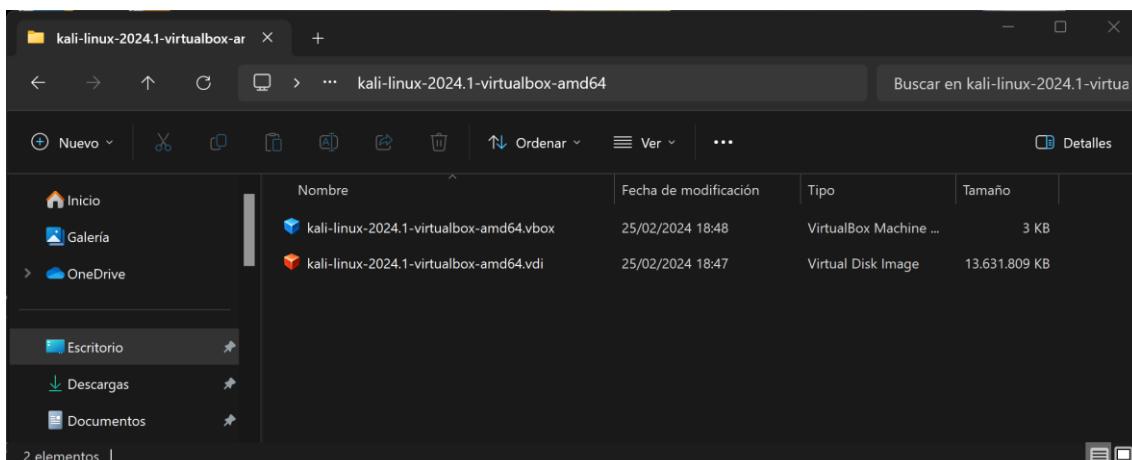
clic sobre la imagen de VirtualBox 64 para iniciar la descarga del archivo de imagen.



En esta pantalla, se ha completado la descarga del archivo de la máquina virtual de Kali.

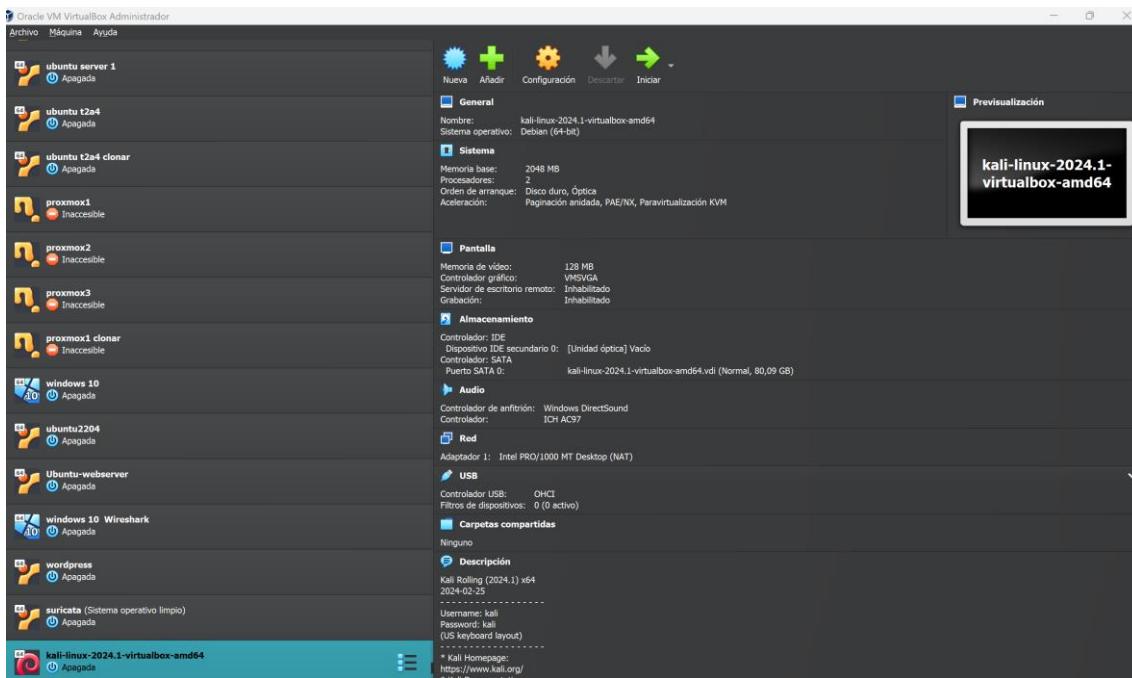


En este punto, procedemos a descomprimir el archivo de la máquina virtual en un directorio específico.

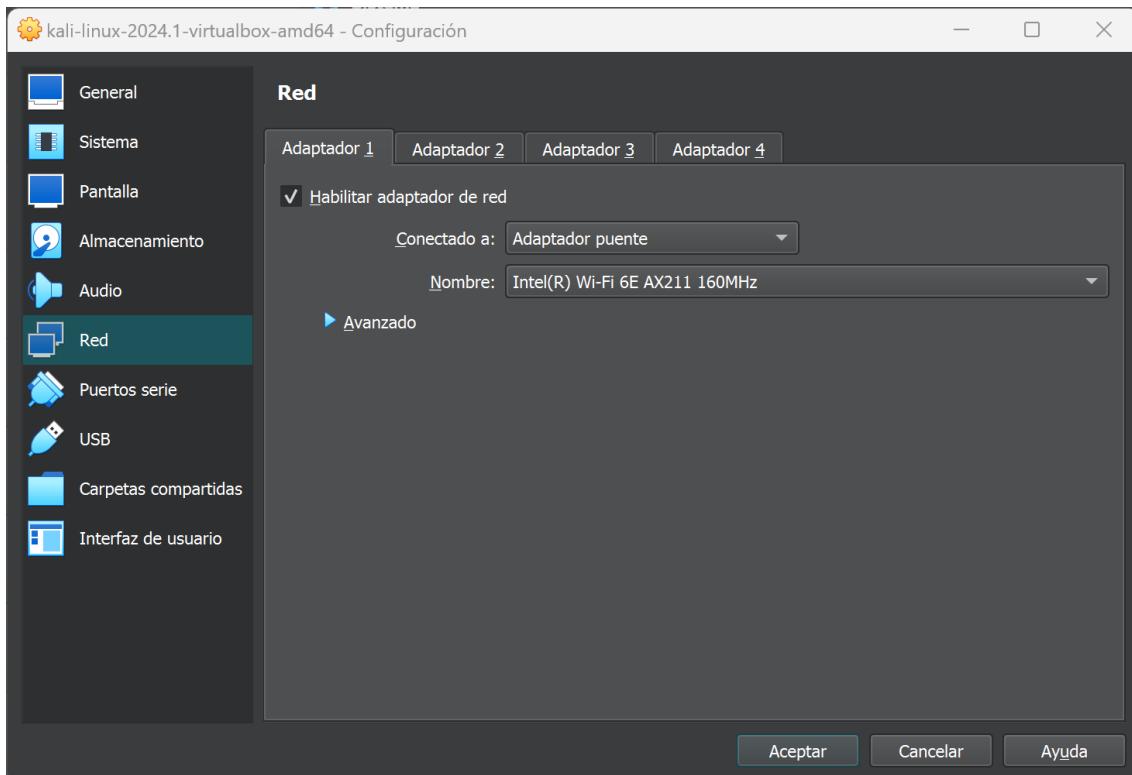


En esta etapa, llevamos a cabo la instalación de la máquina virtual en VirtualBox. Esto se realiza haciendo doble clic en el archivo

con la extensión .vbox, lo que iniciará el proceso de instalación de la máquina virtual en VirtualBox.



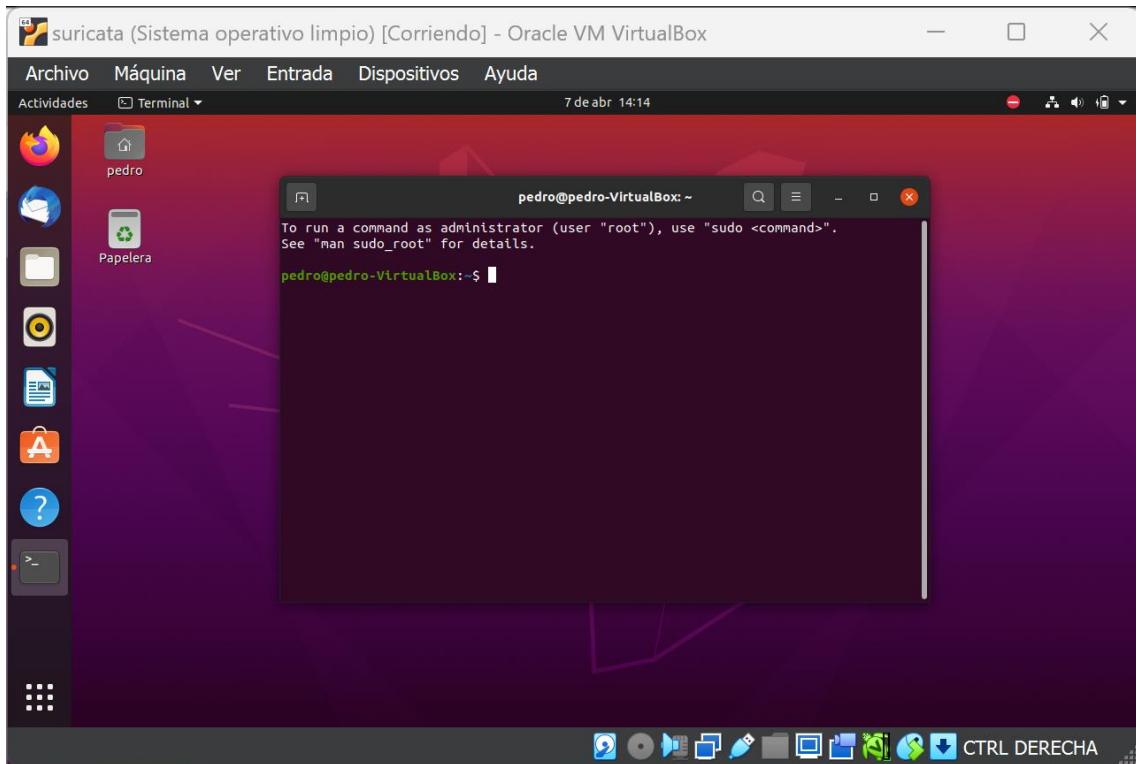
En esta pantalla, se observa que ya tenemos instaladas las dos imágenes: "suricata" y "Kali-linux-2024-1" en VirtualBox.



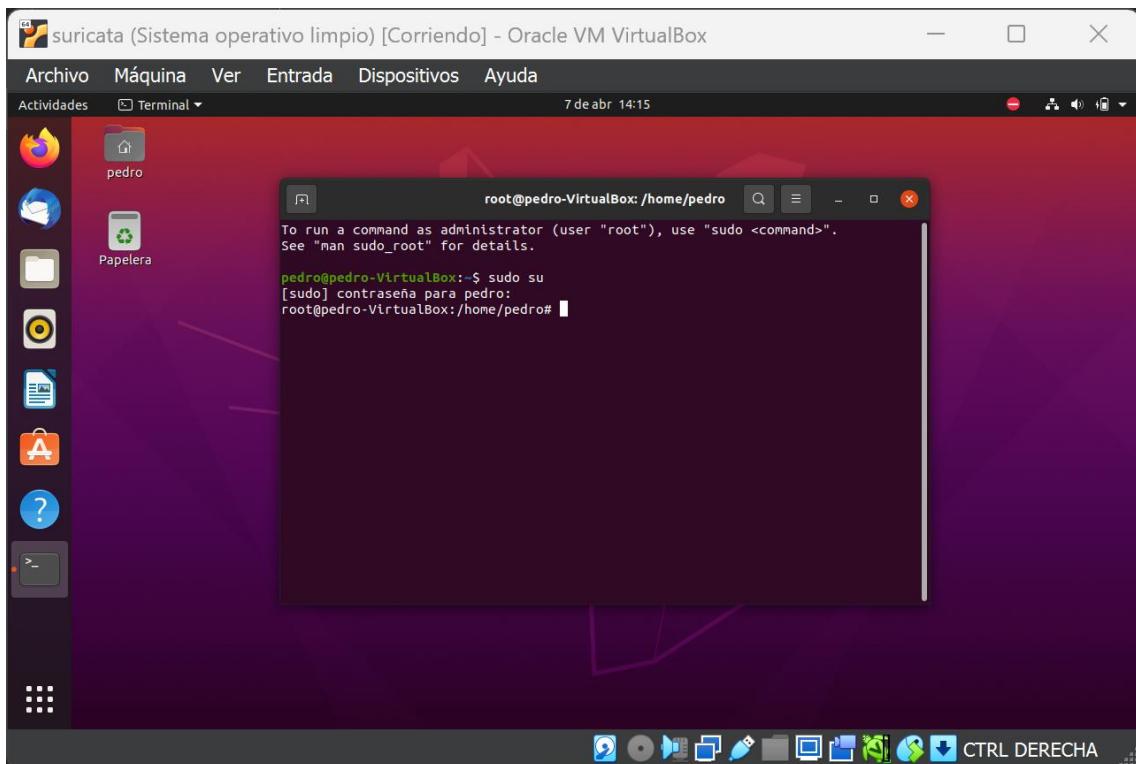
En este paso, accedemos a la configuración de la máquina virtual haciendo doble clic en ella. Luego, nos dirigimos a la opción de

configuración de red y seleccionamos "Adaptador puente". Finalmente, confirmamos la configuración pulsando el botón "Aceptar".

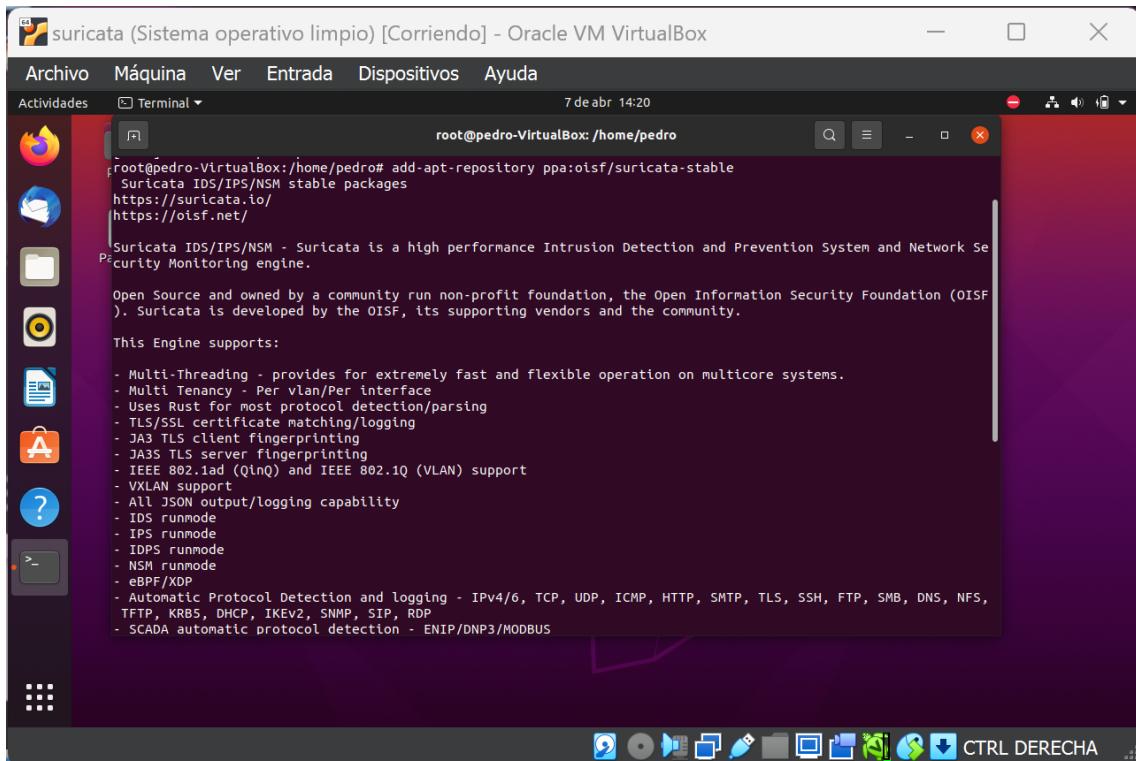
3.3.- instalación de Suricata



En esta pantalla, procedemos a abrir un terminal pulsando simultáneamente las teclas CTRL + ALT + T.

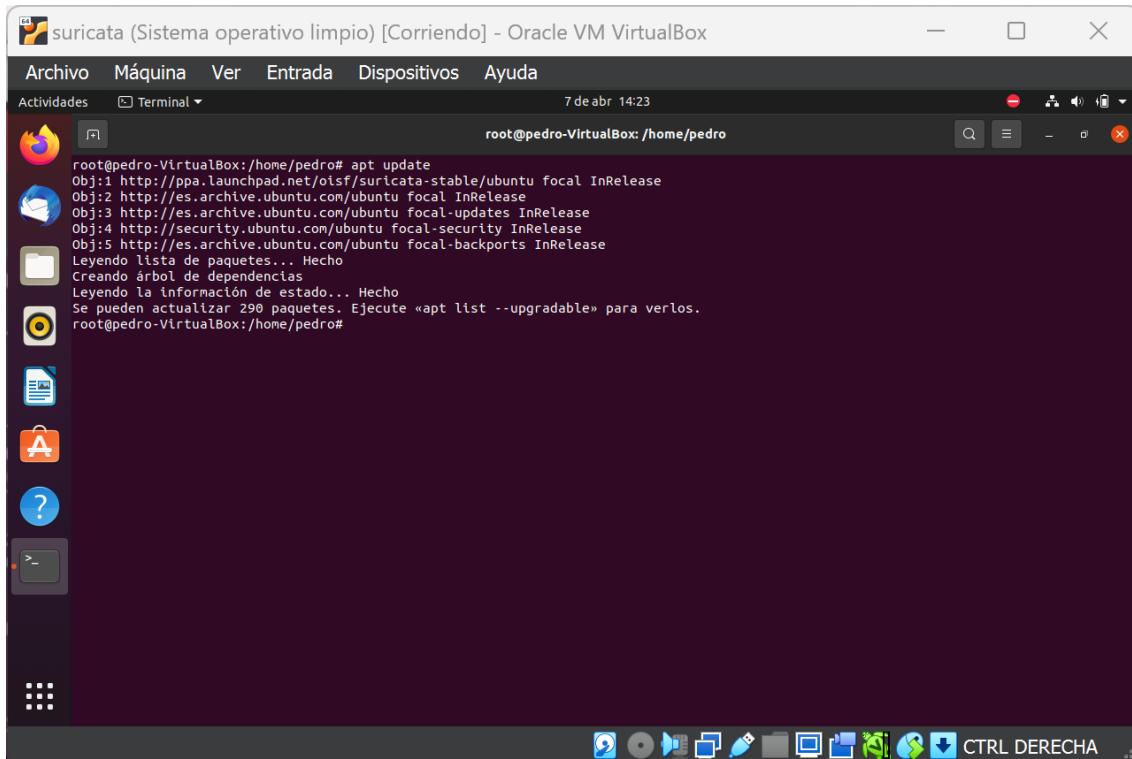


En este paso, adquirimos los derechos de administrador utilizando el comando "sudo su" y luego presionamos la tecla Intro para confirmar y ejecutar el comando.

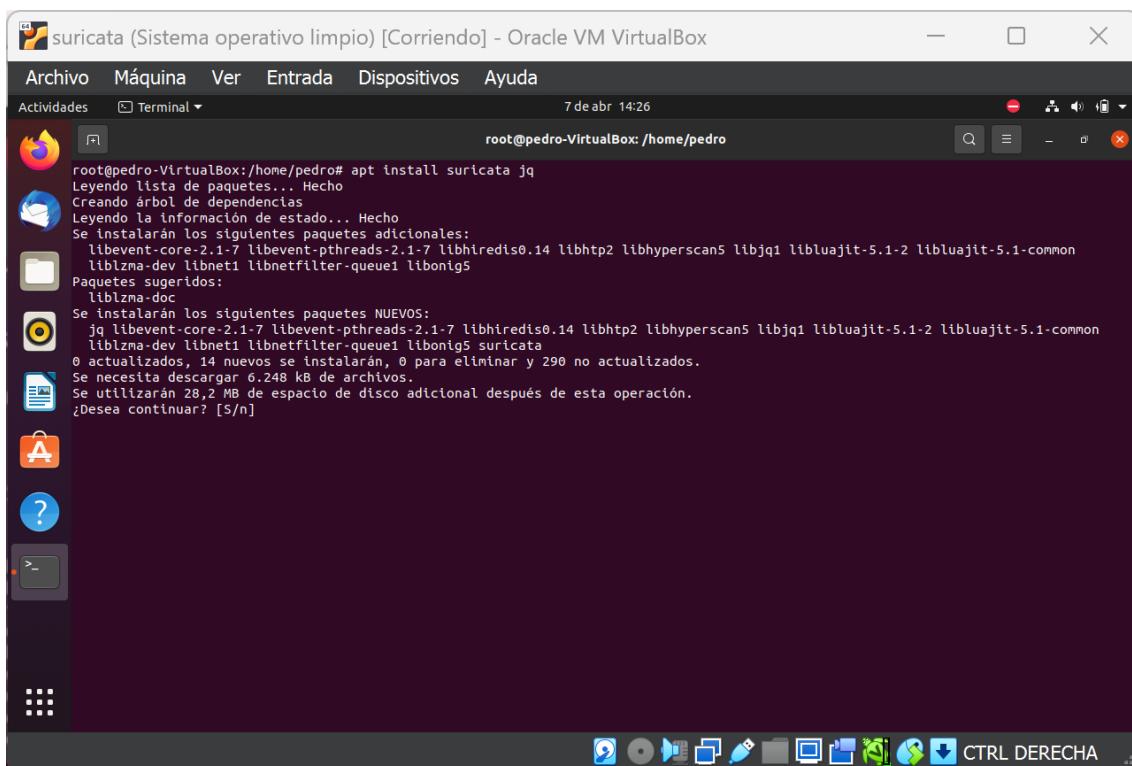


En este paso, procedemos a instalar el repositorio de la última versión estable del Suricata utilizando el comando "add-apt-repository

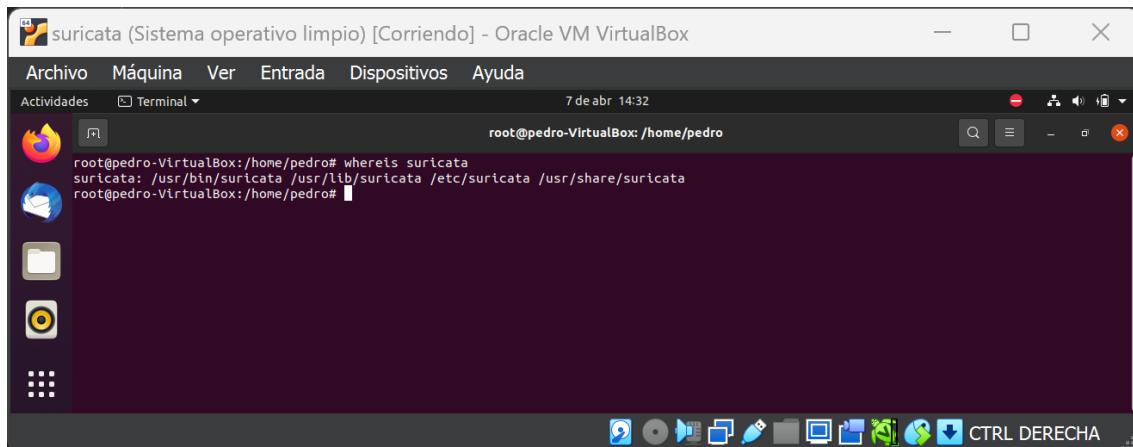
"ppa:oisf/suricata-stable" y luego pulsamos la tecla Intro para confirmar y ejecutar el comando.



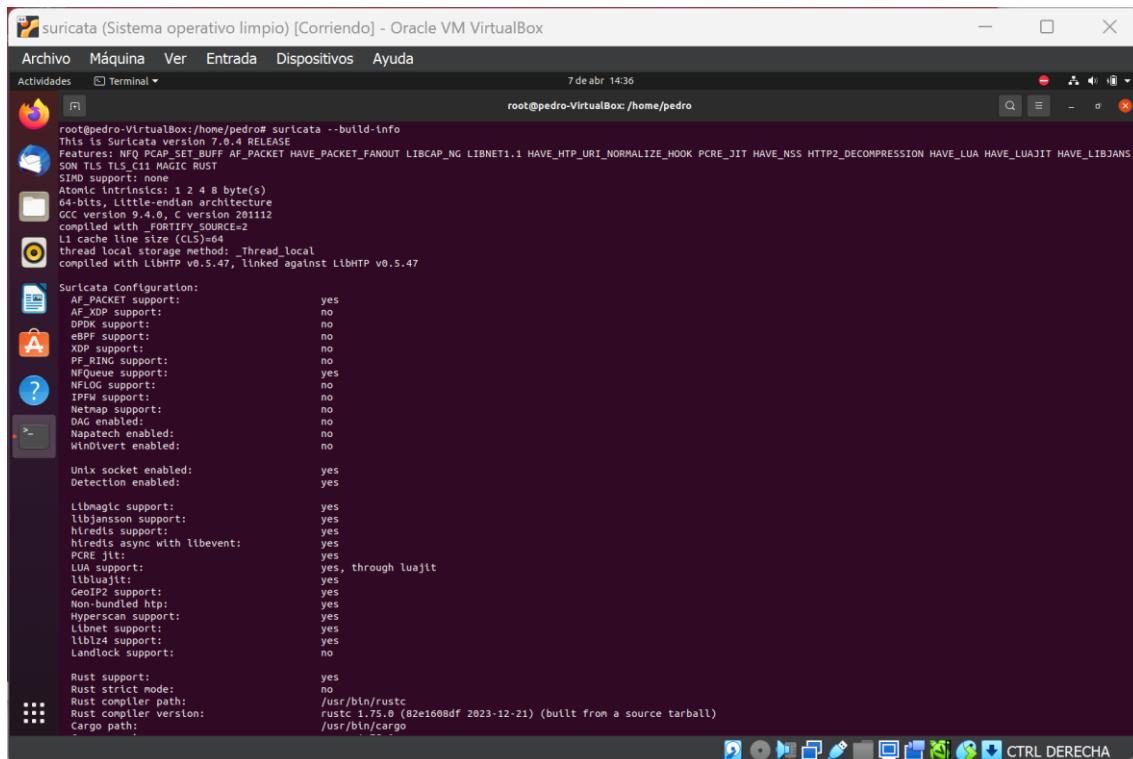
En esta pantalla, procedemos a actualizar todos los repositorios utilizando el comando "apt update", y luego pulsamos la tecla Intro para ejecutar el comando y llevar a cabo la actualización.



En esta pantalla, procedemos a instalar el programa Suricata y jq, que es un lector de registro, utilizando el comando "apt install suricata jq". Luego, pulsamos la tecla Intro para ejecutar el comando. Cuando nos pregunte si deseamos continuar con la instalación, pulsamos la tecla "s" para confirmar y continuar con el proceso de instalación.

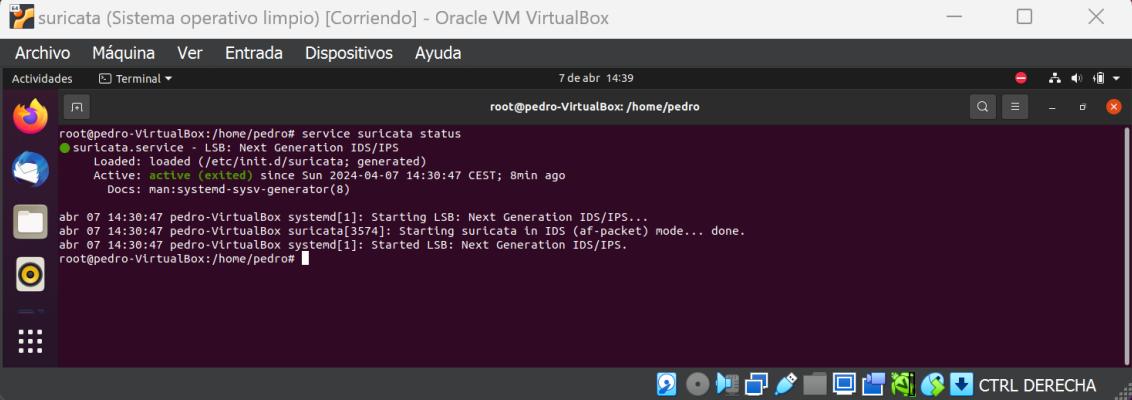


En esta pantalla, procedemos a ejecutar el comando "whereis suricata" para ver en qué directorio se ha instalado Suricata. Simplemente pulsamos la tecla Intro para ejecutar el comando y obtener la información deseada.



En esta pantalla, procedemos a ejecutar el comando "suricata --build-info" para ver la información de compilación y la versión del

programa Suricata. Simplemente pulsamos la tecla Intro para ejecutar el comando y obtener la información deseada.

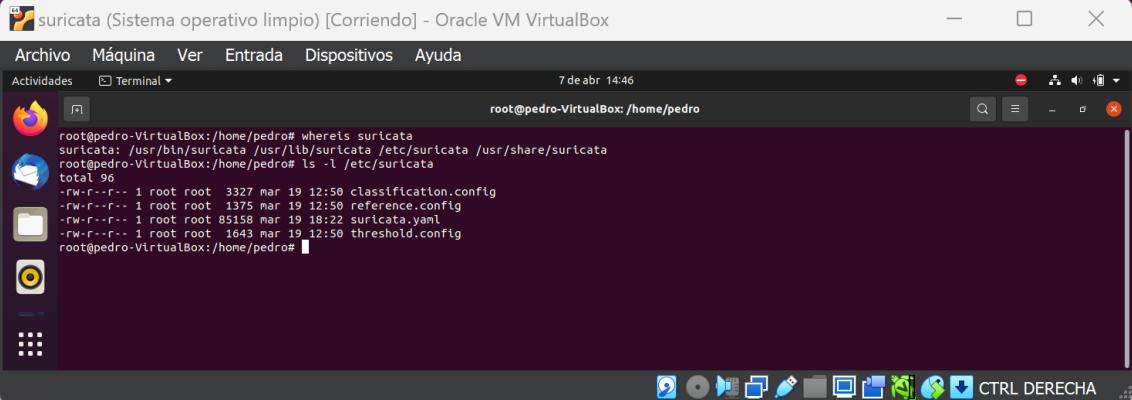


```
suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
root@pedro-VirtualBox:/home/pedro# service suricata status
● suricata.service - LSB: Next Generation IDS/IPS
  Loaded: loaded (/etc/init.d/suricata; generated)
  Loaded: loaded (/etc/init.d/suricata; generated)
  Active: active (exited) since Sun 2024-04-07 14:30:47 CEST; 8min ago
    Docs: man:systemd-sysv-generator(8)

abr 07 14:30:47 pedro-VirtualBox systemd[1]: Starting LSB: Next Generation IDS/IPS...
abr 07 14:30:47 pedro-VirtualBox suricata[3574]: Starting suricata in IDS (af-packet) mode... done.
abr 07 14:30:47 pedro-VirtualBox systemd[1]: Started LSB: Next Generation IDS/IPS.
root@pedro-VirtualBox:/home/pedro#
```

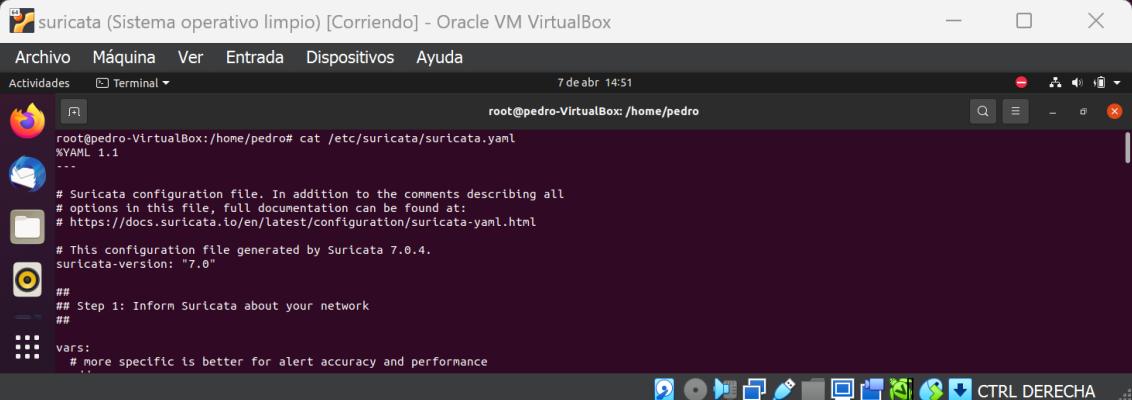
En esta pantalla, ejecutamos el comando "service suricata status" para verificar el estado del servicio Suricata. Simplemente pulsamos la tecla Intro para ejecutar el comando y obtener el estado actual del servicio.

3.4.- Configuración del Suricata



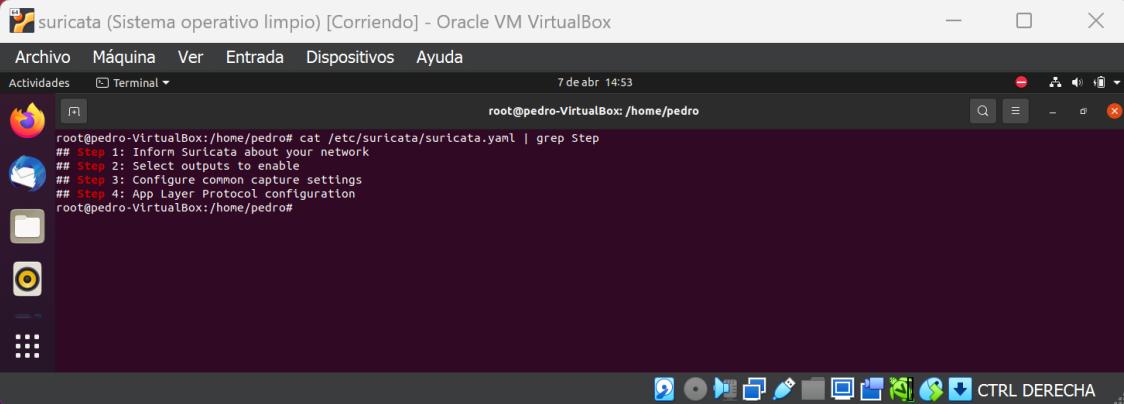
```
suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
root@pedro-VirtualBox:/home/pedro# whereis suricata
suricata: /usr/bin/suricata /usr/lib/suricata /etc/suricata /usr/share/suricata
root@pedro-VirtualBox:/home/pedro# ls -l /etc/suricata
total 96
-rw-r--r-- 1 root root 3327 mar 19 12:50 classification.config
-rw-r--r-- 1 root root 1375 mar 19 12:50 reference.config
-rw-r--r-- 1 root root 85158 mar 19 18:22 suricata.yaml
-rw-r--r-- 1 root root 1643 mar 19 12:50 threshold.config
root@pedro-VirtualBox:/home/pedro#
```

En esta pantalla, ejecutamos el comando "ls -l /etc/suricata" para listar los archivos de configuración de Suricata en el directorio "/etc/suricata". Simplemente pulsamos la tecla Intro para ejecutar el comando y ver la lista de archivos de configuración disponibles.



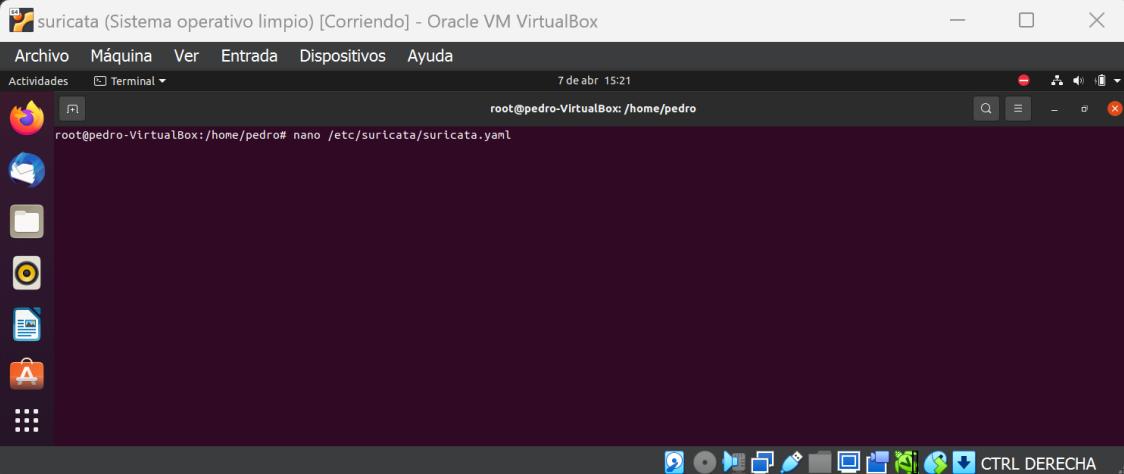
```
suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
root@pedro-VirtualBox:/home/pedro# cat /etc/suricata/suricata.yaml
YAML 1.1
...
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html
#
# This configuration file generated by Suricata 7.0.4.
suricata-version: "7.0"
##
## Step 1: Inform Suricata about your network
##
vars:
  # More specific is better for alert accuracy and performance
```

En esta pantalla, ejecutamos el comando "cat /etc/suricata/suricata.yaml" para mostrar el contenido del archivo de configuración de Suricata llamado "suricata.yaml". Simplemente pulsamos la tecla Intro para ejecutar el comando y visualizar el contenido del archivo.



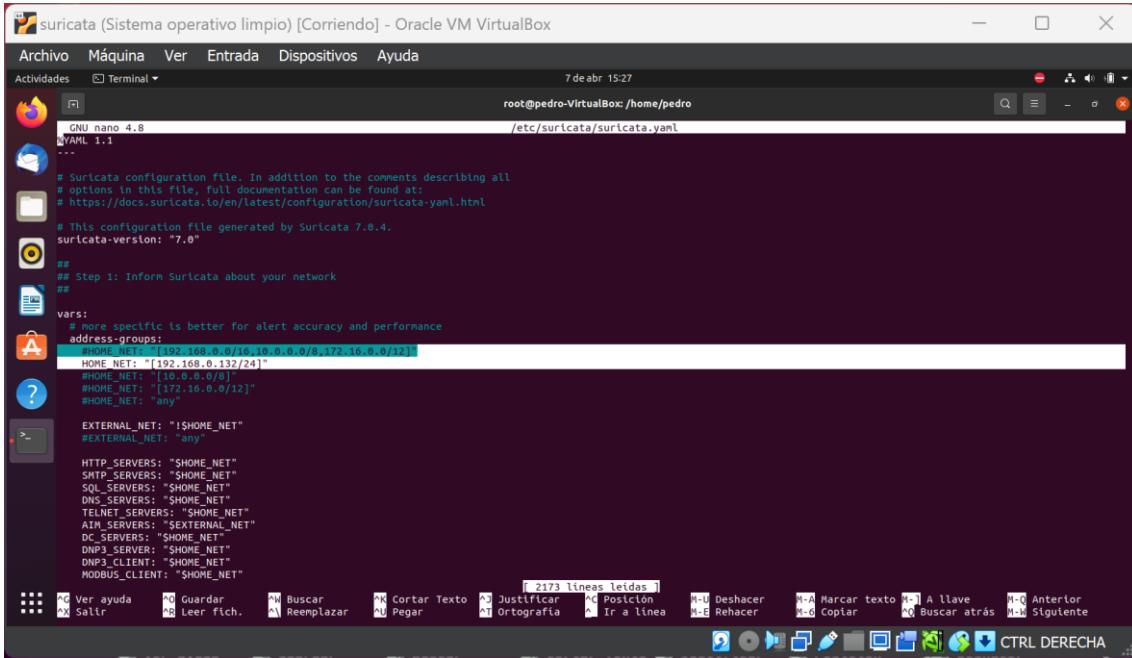
```
suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 7 de abr 14:53
root@pedro-VirtualBox:/home/pedro# cat /etc/suricata/suricata.yaml | grep Step
## Step 1: Inform Suricata about your network
## Step 2: Select outputs to enable
## Step 3: Configure common capture settings
## Step 4: App Layer Protocol configuration
root@pedro-VirtualBox:/home/pedro#
```

En esta pantalla, ejecutamos el comando "cat /etc/suricata/suricata.yaml | grep Step" y pulsamos la tecla Intro para filtrar y mostrar únicamente las líneas que contienen la palabra "Step" en el archivo de configuración de Suricata, "suricata.yaml". Esto nos permitirá ver los pasos específicos que están presentes en el archivo de configuración.



```
suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 7 de abr 15:21
root@pedro-VirtualBox:/home/pedro# nano /etc/suricata/suricata.yaml
```

En esta pantalla, ejecutamos el comando "nano /etc/suricata/suricata.yaml" para abrir el archivo de configuración de Suricata en el editor de texto nano, lo que nos permitirá editararlo. Luego, pulsamos la tecla Intro para ejecutar el comando y abrir el archivo en el editor nano.



```

suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 7 de abr 15:27
root@pedro-VirtualBox: /home/pedro
GNU nano 4.8
/etc/suricata/suricata.yaml

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.4.
suricata-version: "7.0"

## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: ["192.168.0.0/16", "10.0.0.0/8", "172.16.0.0/12"]
    HOME_NET: ["192.168.0.132/24"]
    HOME_NET: ["192.168.0.132/12"]
    HOME_NET: "any"

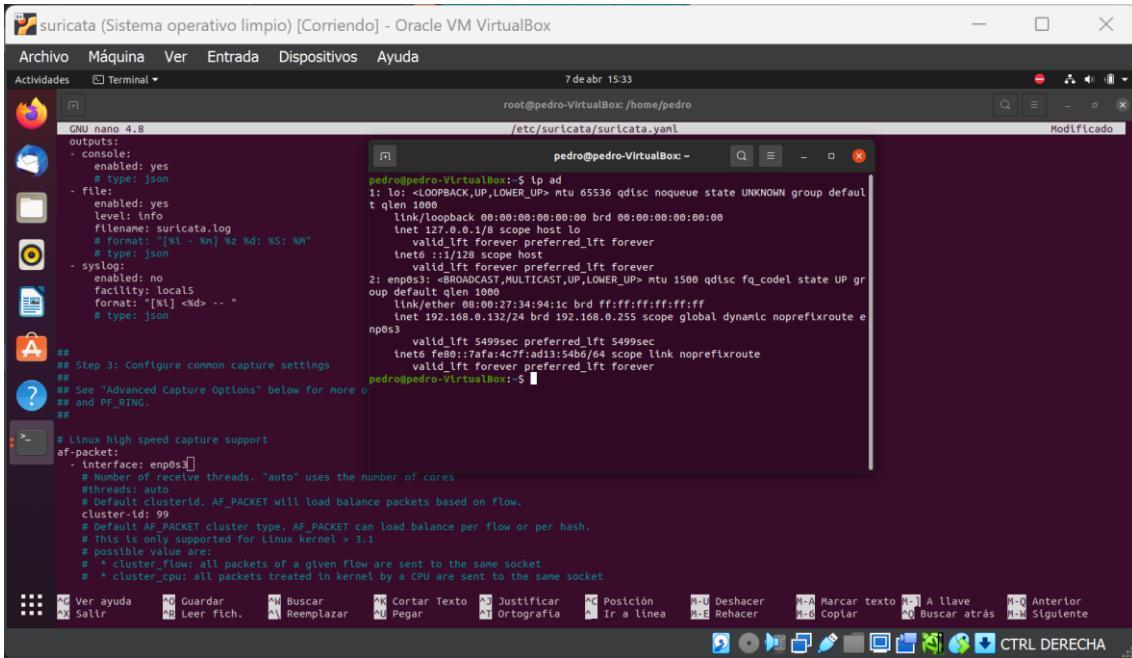
  EXTERNAL_NET: "$HOME_NET"
  #EXTERNAL_NET: "any"

  HTTP_SERVERS: "$HOME_NET"
  SMTP_SERVERS: "$HOME_NET"
  SQL_SERVERS: "$HOME_NET"
  DNS_SERVERS: "$HOME_NET"
  TELNET_SERVERS: "$HOME_NET"
  AIM_SERVERS: "$EXTERNAL_NET"
  DC_SERVERS: "$HOME_NET"
  DNP3_SERVER: "$HOME_NET"
  DNP3_CLIENT: "$HOME_NET"
  MODBUS_CLIENT: "$HOME_NET"

  ## Ver ayuda  Ver Guardar  Buscar  Cortar Texto  Justificar  Posición  Deshacer  Marcar texto  A llave  Ctrl Derecha
  ## Salir  Leer fich.  Reemplazar  Pegar  Ortografía  Ir a línea  Rehacer  Copiar  Buscar atrás  Siguiente
  ## 2173 líneas leídas
  ## CTRL DERECHA

```

En esta etapa, modificamos la primera línea seleccionada añadiendo un símbolo "#" al principio para comentar la línea. En la segunda línea, establecemos la dirección IP en "192.168.0.132/24", que es la dirección con la que trabajaremos con Suricata. Luego, guardamos los cambios y salimos del editor nano utilizando las teclas CTRL + O para guardar y CTRL + X para salir.



```

suricata (Sistema operativo limpio) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 7 de abr 15:33
root@pedro-VirtualBox: /home/pedro
GNU nano 4.8
outputs:
  console:
    enabled: yes
    type: json
  - file:
      enabled: yes
      level: info
      filename: suricata.log
    type: json
  - syslog:
      enabled: no
      facility: local5
      format: "[%{!%m} %d %H:%M %N]"
      type: json
  ## Step 3: Configure common capture settings
  ## See "Advanced Capture Options" below for more options
  ## and PF_RING.
  ##

  # Linux high speed capture support
  af-packet:
    interfaces: enp0s3
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    #Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    # * cluster_flow: all packets of a given flow are sent to the same socket
    # * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket

  ## Ver ayuda  Ver Guardar  Buscar  Cortar Texto  Justificar  Posición  Deshacer  Marcar texto  A llave  Ctrl Derecha
  ## Salir  Leer fich.  Reemplazar  Pegar  Ortografía  Ir a línea  Rehacer  Copiar  Buscar atrás  Siguiente
  ## Modificado
  ## 1 líneas modificadas
  ## CTRL DERECHA

```

En esta pantalla, ejecutamos el comando "ip ad" para identificar en qué interfaz está ubicada la tarjeta de red "enp0s3". Luego, modificamos la configuración de la interfaz en el archivo correspondiente. Una vez realizados los cambios, guardamos los cambios en el archivo pulsando las teclas CTRL+O y luego presionamos

la tecla Enter para confirmar. Después, salimos del editor pulsando las teclas CTRL+X.

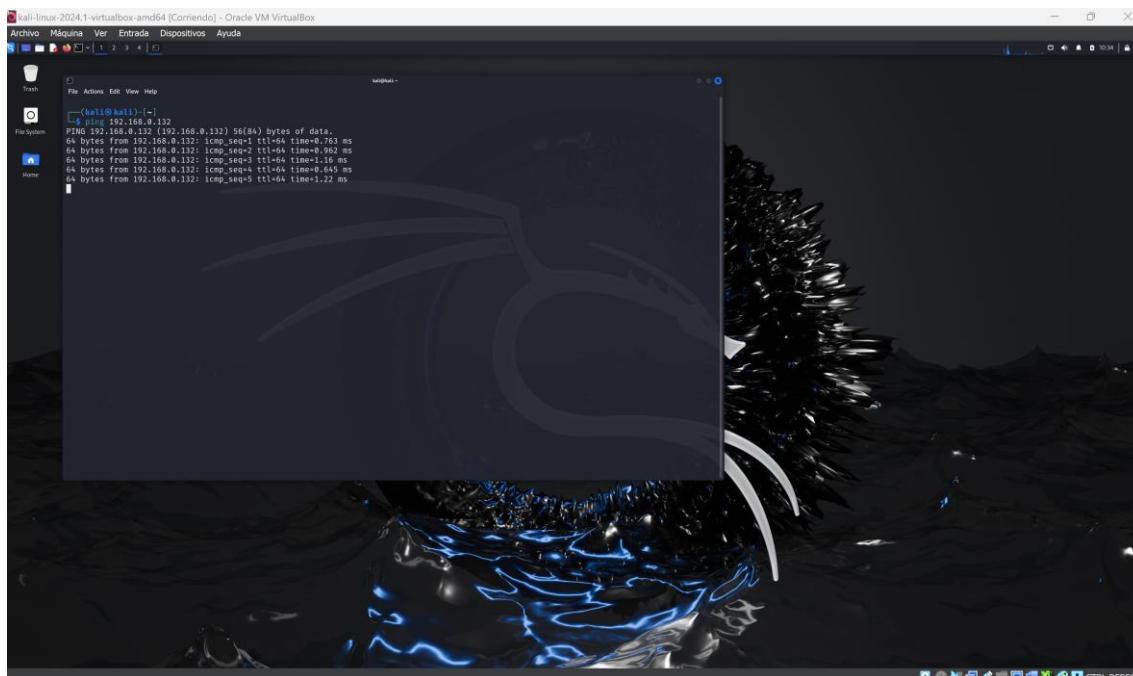
3.5.- Verificación si esta suricata configurada correctamente



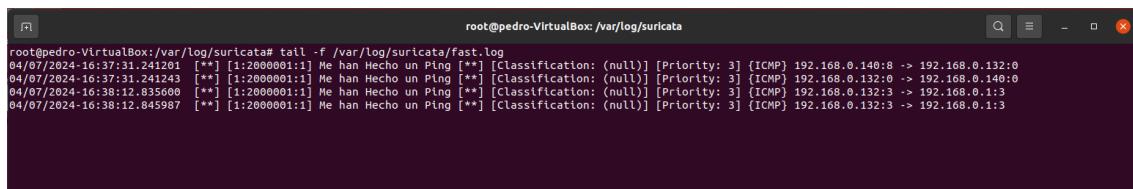
```
root@pedro-VirtualBox: /var/lib/suricata/rules
GNU nano 4.8                                         suricata.rules
alert icmp any any -> any any (msg: "Me han Hecho un Ping"; sid:2000001; rev:1;)
```

The terminal window shows the nano text editor with the command 'suricata.rules' open. The content of the file is a single line: 'alert icmp any any -> any any (msg: "Me han Hecho un Ping"; sid:2000001; rev:1;)'. Below the editor are standard nano key bindings.

En esta etapa, ejecutamos el comando nano /var/lib/suricata/rules en la terminal para abrir el archivo de reglas de Suricata. Luego, añadimos la regla específica para detectar pings ICMP: alert icmp any any -> any any (msg: "Me han hecho un ping"; sid: 2000001; rev: 1;). Después de agregar la regla, presionamos las teclas Ctrl + O para guardar los cambios y Ctrl + X para salir del editor nano, lo que guarda la nueva regla en el archivo de reglas de Suricata.



En esta pantalla, se procede a ejecutar en Kali un ping a la maquina objetivo para saber si funciona bien el suricata.



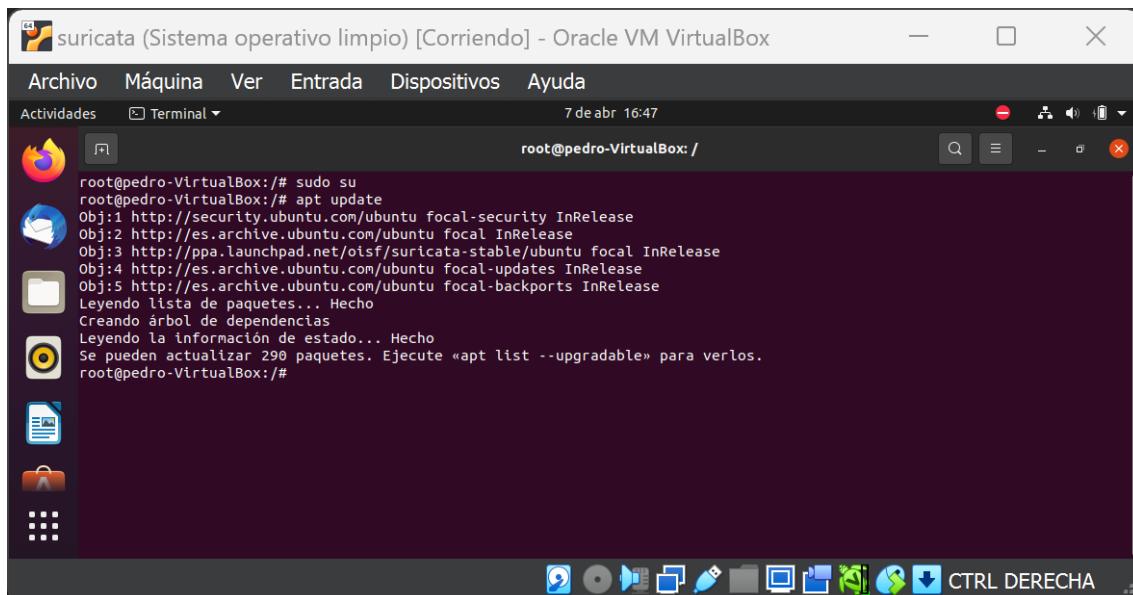
```
root@pedro-VirtualBox: /var/log/suricata# tail -f /var/log/suricata/fast.log
04/07/2024-16:37:31.241201 [**] [1:2000001:1] Me han Hecho un Ping [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.140:8 -> 192.168.0.132:0
04/07/2024-16:37:31.241243 [**] [1:2000001:1] Me han Hecho un Ping [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.132:0 -> 192.168.0.140:0
04/07/2024-16:38:12.835600 [**] [1:2000001:1] Me han Hecho un Ping [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.132:3 -> 192.168.0.1:3
04/07/2024-16:38:12.845987 [**] [1:2000001:1] Me han Hecho un Ping [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.132:3 -> 192.168.0.1:3
```

The terminal window shows the command 'tail -f /var/log/suricata/fast.log' running. It displays several log entries from the Suricata fast log, each corresponding to an ICMP echo request sent by the user to the target host (192.168.0.132) and its replies.

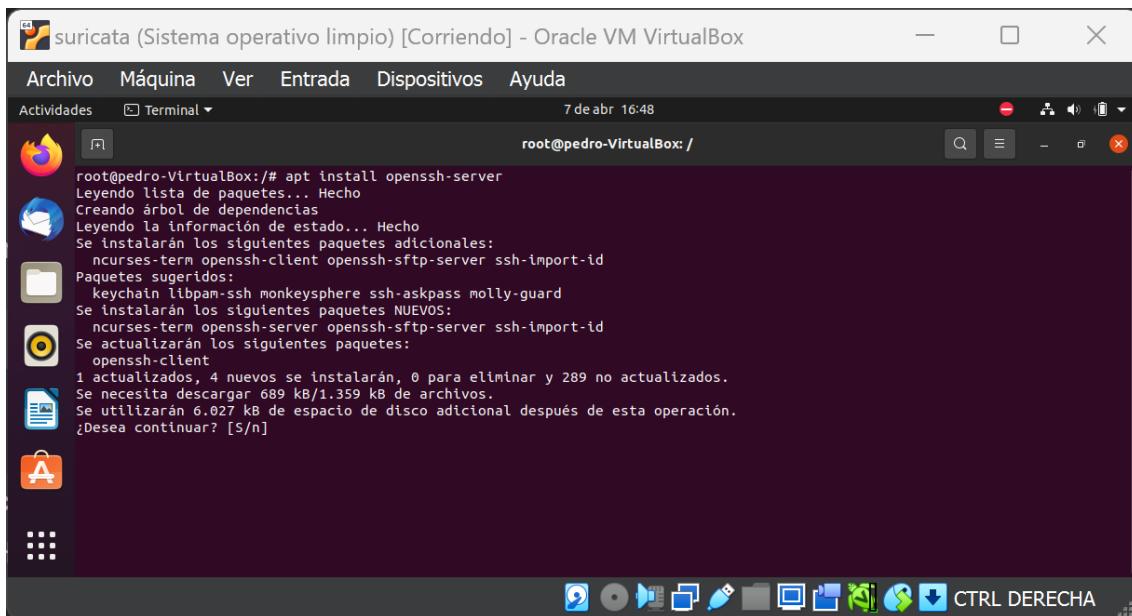
En esta pantalla, observamos los pings realizados a la máquina objetivo y detectados por Suricata utilizando el comando tail -f /var/log/suricata/fast.log, el cual nos permite visualizar en tiempo real los registros de los pings provenientes de la máquina atacante Kali en el archivo de registro de Suricata.

La configuración implicó la creación de reglas específicas en el archivo de configuración de Suricata para detectar pings ICMP, seguida de la monitorización en tiempo real de los registros de Suricata para visualizar los eventos de red capturados y verificar la detección adecuada de los pings. Se aseguró que los cambios realizados estuvieran correctamente implementados, confirmando que Suricata esté listo para detectar y prevenir intrusiones relacionadas con pings ICMP en el sistema.

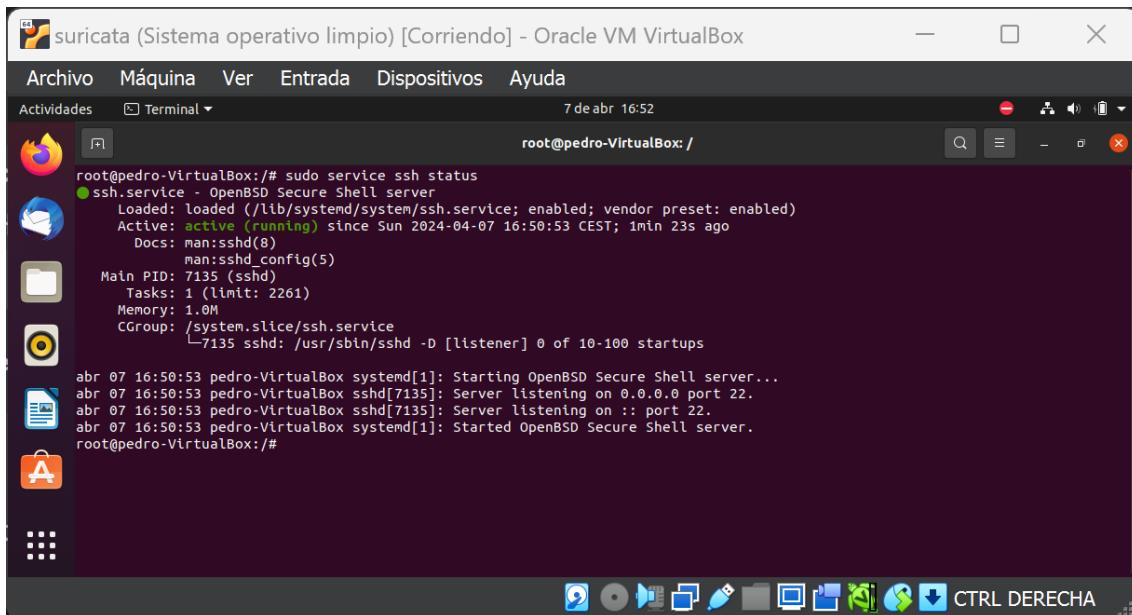
3.6.- Instalación ssh en ubuntu para hacer conexiones ssh.



En esta pantalla, procedemos a adquirir privilegios de root utilizando el comando sudo su en la terminal. Una vez adquiridos los privilegios de root, ejecutamos el comando apt update para actualizar la lista de paquetes disponibles en el sistema. Finalmente, pulsamos la tecla Intro para ejecutar el comando y llevar a cabo la actualización.



En esta pantalla, procedemos a instalar el servidor SSH (openssh-server) utilizando el comando `apt install openssh-server` en la terminal. Después de escribir el comando, pulsamos la tecla Intro para ejecutarlo y comenzar el proceso de instalación del servidor SSH en el sistema. Luego, si se nos solicita, podemos pulsar la tecla 's' para confirmar y continuar con la instalación, si es necesario.



En esta pantalla, procedemos a verificar si el servicio SSH está activo utilizando el comando `service ssh status` en la terminal. Después de escribir el comando, pulsamos la tecla Intro para ejecutarlo y obtener información sobre el estado actual del servicio SSH en el sistema.

The screenshot shows a terminal window titled "kali-linux-2024.1-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox". The terminal content is as follows:

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ ssh pedro@192.168.0.132 -p 22
The authenticity of host '192.168.0.132 (192.168.0.132)' can't be established
ED25519 key fingerprint is SHA256:thyKtrrvIwunjGl2M+eTgPdOZv/yGbtEUnSebiDj8k
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.132' (ED25519) to the list of known hosts.
pedro@192.168.0.132's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
 Receive updates to over 25,000 software packages with your
 Ubuntu Pro subscription. Free for personal use.

 https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

pedro@pedro-VirtualBox:~$
```

En esta pantalla, realizamos una conexión SSH desde la máquina atacante hacia la máquina objetivo Ubuntu utilizando el comando ssh pedro@192.168.0.132 -p 22 en la terminal. Después de ejecutar el comando, si es la primera vez que nos conectamos, es posible que se nos pregunte si deseamos continuar con la conexión. En este caso, escribimos "yes" y luego pulsamos la tecla Intro para confirmar. Después, se nos pedirá que introduzcamos la contraseña de la cuenta de usuario "pedro" en el servidor Ubuntu. Luego de introducir la contraseña, pulsamos la tecla Intro para completar la conexión SSH y verificar si todo funciona correctamente.

3.7.- Mecanismos de Defensa

En el contexto de la seguridad informática, los mecanismos de defensa son las herramientas, políticas y procedimientos diseñados para proteger los sistemas y datos contra amenazas y ataques ciberneticos. Estos mecanismos se implementan con el objetivo de prevenir, detectar, responder y recuperarse de posibles incidentes de seguridad.

Algunos de los mecanismos de defensa comunes incluyen:

- **Firewalls:** Los firewalls son dispositivos o programas diseñados para controlar y monitorear el tráfico de red entrante y saliente. Pueden configurarse para bloquear o permitir ciertos tipos de tráfico con base en reglas predefinidas.
- **Sistemas de Detección de Intrusos (IDS) y Sistemas de Prevención de Intrusos (IPS):** Los IDS monitorean el tráfico de red en busca de comportamientos sospechosos o maliciosos y generan alertas cuando se detecta una actividad anómala. Los IPS van un paso más allá al tomar medidas activas para prevenir o bloquear tales actividades.
- **Antivirus y Antimalware:** Estos programas se utilizan para detectar, prevenir y eliminar software malicioso, como virus, gusanos, troyanos y spyware, que pueden comprometer la seguridad de un sistema.
- **Autenticación y Control de Acceso:** Los mecanismos de autenticación, como contraseñas, tokens y biometría, se utilizan para verificar la identidad de los usuarios antes de permitirles acceder a recursos o sistemas protegidos. El control de acceso establece qué recursos pueden acceder los usuarios autorizados y en qué condiciones.
- **Cifrado de Datos:** El cifrado se utiliza para proteger la confidencialidad de los datos al convertirlos en un formato

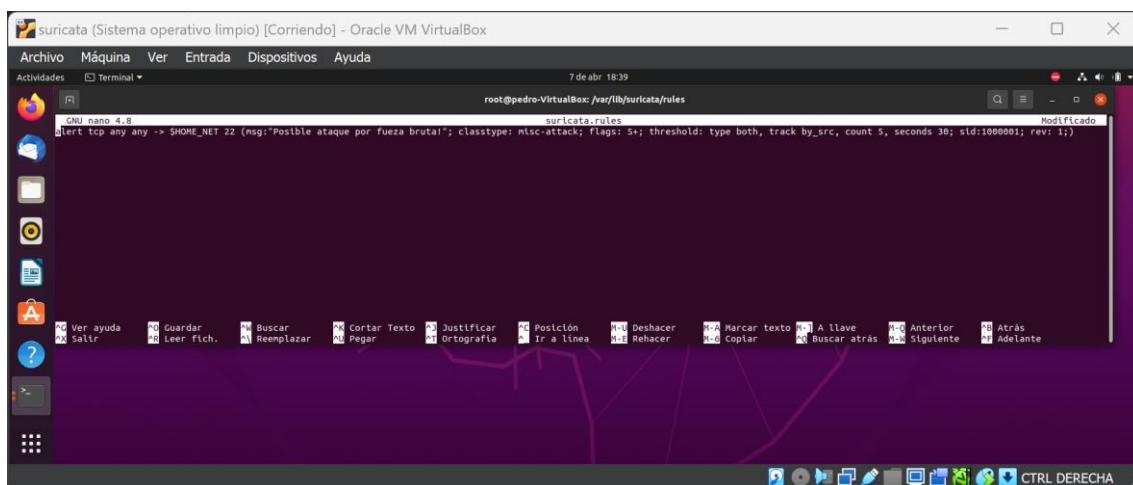
ilegible que solo puede ser descifrado por usuarios autorizados que posean la clave de cifrado adecuada.

- **Actualizaciones y Parches de Seguridad:** Mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad ayuda a proteger contra vulnerabilidades conocidas y a mitigar los riesgos de ataques.
- **Copias de Seguridad y Recuperación de Desastres:** Realizar copias de seguridad periódicas de datos importantes y tener planes de recuperación de desastres en su lugar ayuda a mitigar los efectos de ataques cibernéticos, errores humanos y desastres naturales al permitir la restauración rápida de datos y sistemas.

Estos son solo algunos ejemplos de los mecanismos de defensa utilizados en seguridad informática. Es importante implementar una combinación de estos mecanismos y adaptarlos a las necesidades y riesgos específicos de cada organización para garantizar una protección efectiva contra las amenazas cibernéticas.

4.- Pasos Previos al Ataque

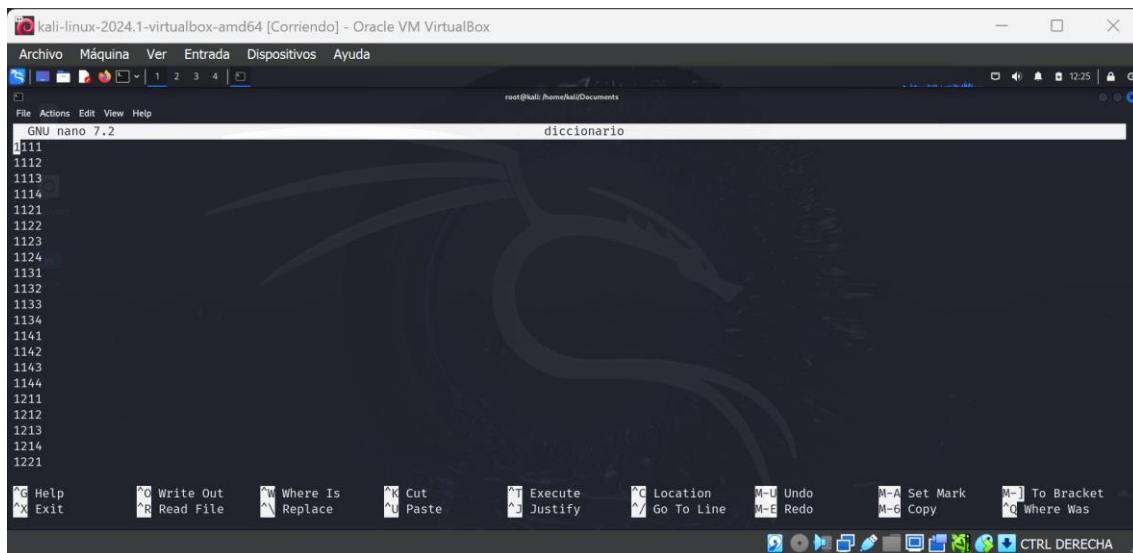
4.1.- Máquina Objetivo configuración de la regla



En esta pantalla, se procede a modificar el fichero suricata.rules con el comando nano /var/lib/suricata/rules/suricata.rules y escribimos la regla siguiente:

```
alert tcp any any -> $HOME_NET 22 (msg:"Possible SSH brute forcing!";
classtype: misc-attack; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid:1000001; rev: 1;)
```

4.2.- Máquina atacante configuración de los archivos

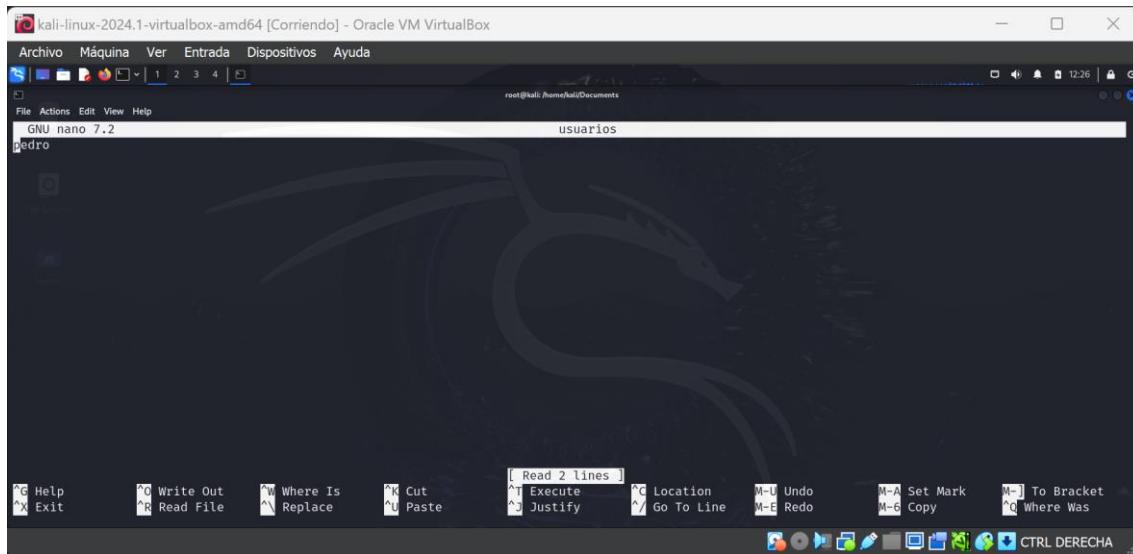


En esta pantalla, procedemos a examinar el archivo generado por Crunch, denominado "diccionario.txt", utilizando el editor Nano. Posteriormente, presionamos la tecla Enter para ejecutar el comando.



En esta pantalla, llevamos a cabo la creación del archivo "hosts" que contendrá las direcciones IP de los servidores que serán objetivo de nuestro ataque. Para ello, utilizamos el comando Nano escribiendo

"nano hosts". Luego, introducimos la dirección IP del servidor, que en este caso es 192.168.0.132. Finalmente, guardamos los cambios pulsando CTRL+O y salimos del editor con CTRL+X.



En esta pantalla, comenzamos la creación del archivo de usuarios utilizando el comando "nano usuarios". Luego, ingresamos el nombre de usuario "pedro" y presionamos la tecla CTRL+O para guardar el archivo. Finalmente, salimos del editor con CTRL+X.

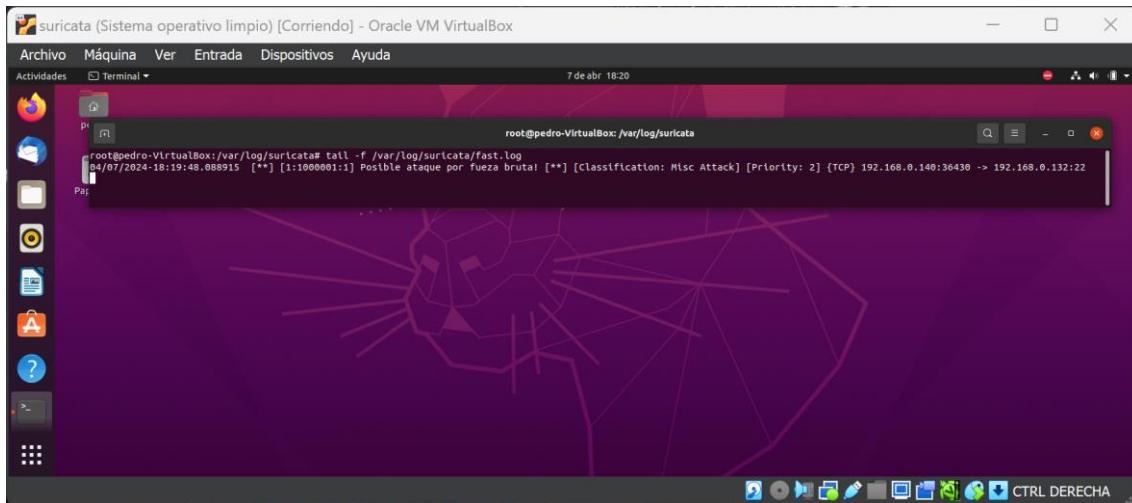
5.- Lanzamiento del Ataque

```
(root㉿kali)-[~/home/kali/Documents]
# hydra -L usuarios -P diccionario.txt -M hosts ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-07 12:48:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 512 login tries (l:2/p:256), ~32 tries per task
[DATA] attacking ssh://192.168.0.132:22/
[22][ssh] host: 192.168.0.132 login: pedro password: 123
```

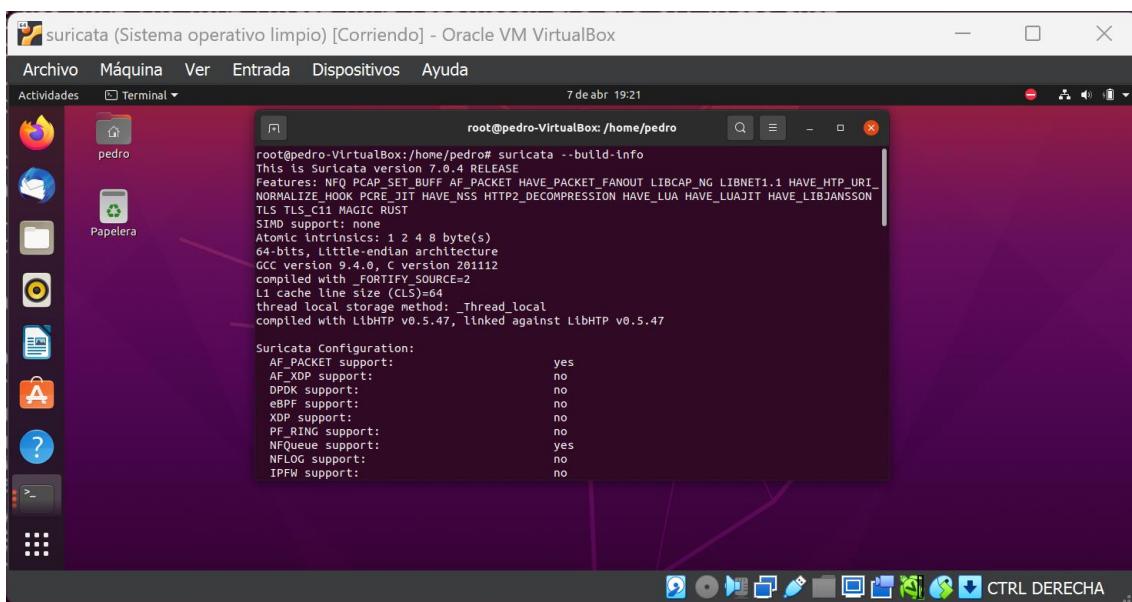
En esta pantalla, ejecutamos el ataque utilizando el comando Hydra, donde especificamos la lista de usuarios con el parámetro "-L usuarios" y la lista de contraseñas con "-P diccionario.txt". Además, identificamos la máquina objetivo con "-M hosts" y el servicio SSH.

Después de ejecutar el comando, se observa que se ha llevado a cabo un ataque de fuerza bruta contra la máquina con la dirección IP 192.168.0.132, logrando obtener el nombre de usuario "pedro" y la contraseña "1234"

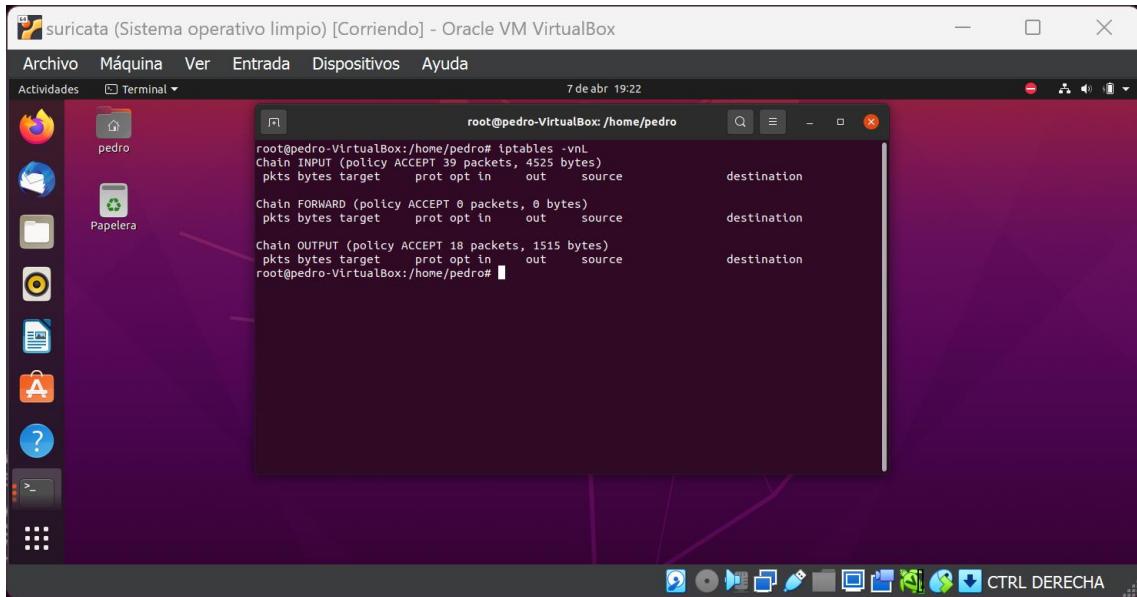


En esta pantalla, se destaca que Suricata ha detectado un posible ataque de fuerza bruta.

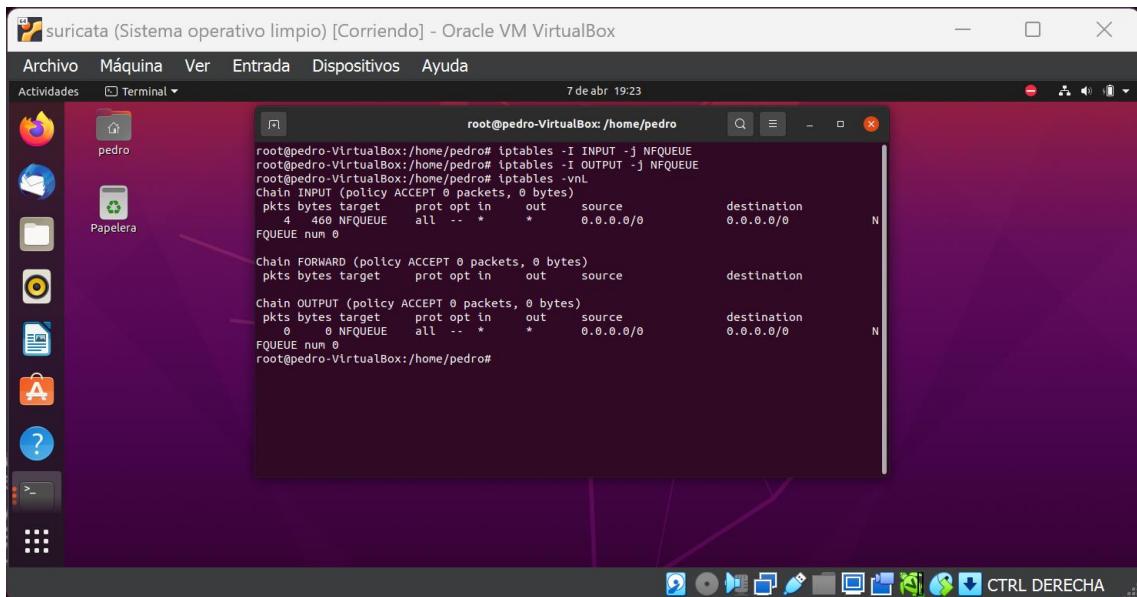
6.- Suricata en Modo IPS (Opcional)



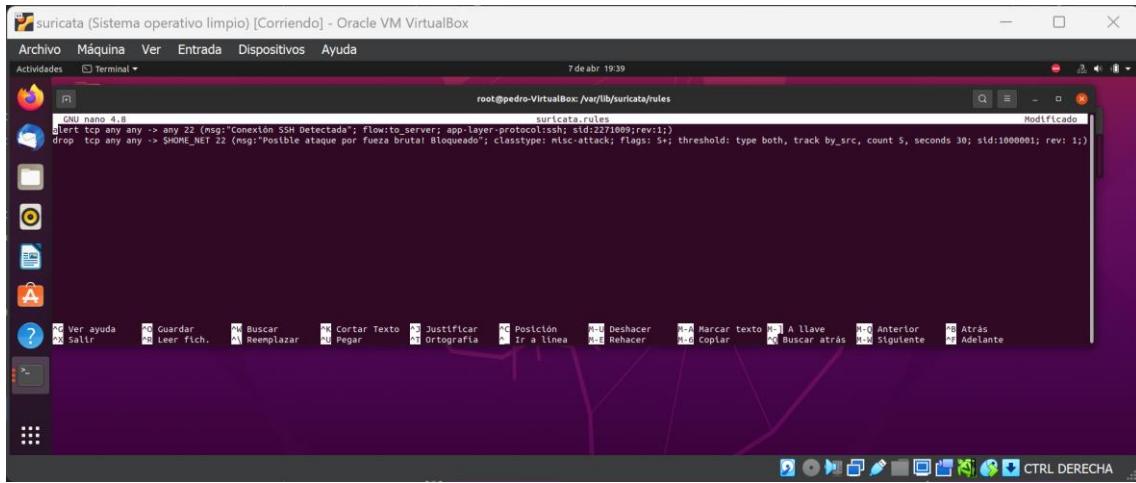
En esta pantalla, verificamos si NFQUEUE está activado en Suricata utilizando el comando suricata --build-info y presionando la tecla Enter. Observamos que la opción NFQUEUE está presente y su estado es "yes".



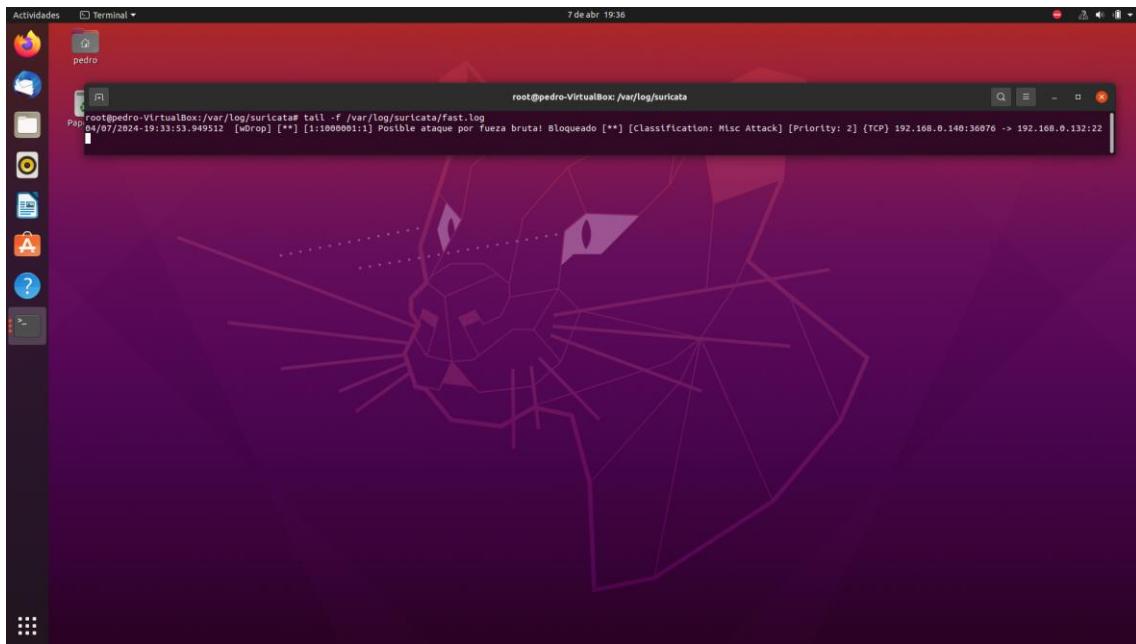
En esta pantalla, verificamos si hay alguna regla activa utilizando el comando `iptables -vnL` y presionando la tecla Enter para ejecutarlo.



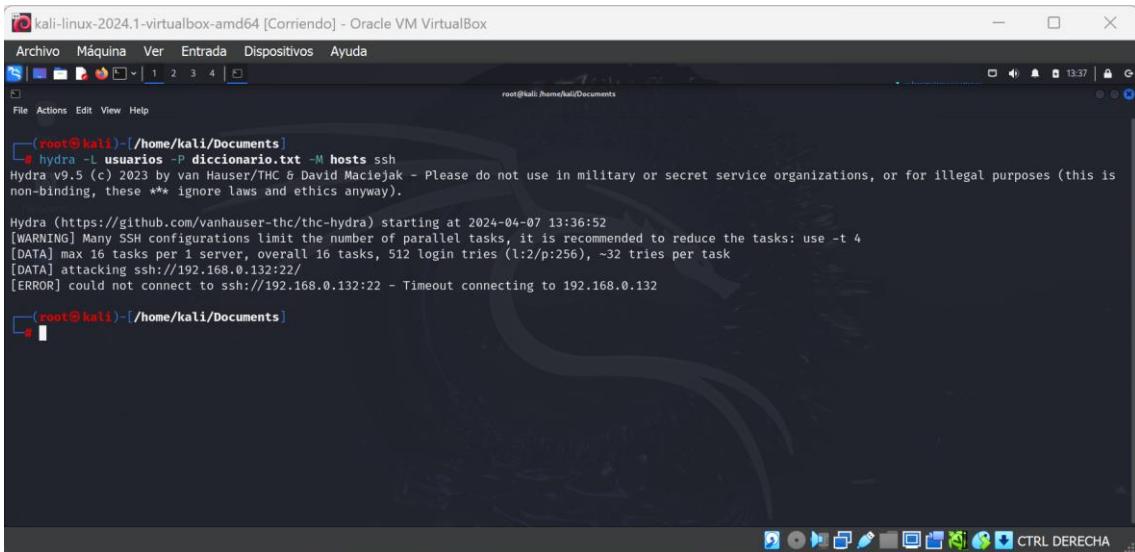
En esta pantalla, procedemos a activar las siguientes reglas de `iptables`: primero, ejecutamos "`iptables -I INPUT -j NFQUEUE`" y luego presionamos Enter. Seguidamente, activamos la regla de salida con "`iptables -I OUTPUT -j NFQUEUE`" y nuevamente presionamos Enter. Para verificar las reglas activadas, utilizamos "`iptables -vnL`" y pulsamos Enter para ejecutar el comando y observar las reglas actualizadas.



En esta pantalla, procedemos a modificar el archivo con el comando "nano /var/lib/suricata/rules/suricata.rules". Dentro del archivo, encontramos la opción "alert" y la cambiamos a "drop" para bloquear las alertas. Luego, guardamos los cambios y salimos del editor.



En esta pantalla, observamos que se ha bloqueado un posible ataque por fuerza bruta. El sistema ha respondido activamente al identificar la amenaza y ha bloqueado el intento de ataque.



```
(root@kali)-[~/home/kali/Documents]
└─# hydra -L usuarios -P diccionario.txt -M hosts ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-07 13:36:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 512 login tries (1:/p:256), -32 tries per task
[DATA] attacking ssh://192.168.0.132:22/
[ERROR] could not connect to ssh://192.168.0.132:22 - Timeout connecting to 192.168.0.132

(root@kali)-[~/home/kali/Documents]
```

En esta pantalla, notamos que el intento de llevar a cabo un ataque de fuerza bruta ha fracasado. El sistema ha sido exitoso en prevenir el ataque, lo que sugiere una configuración efectiva de las medidas de seguridad implementadas.

7.- Archivos a Entregar

7.1.- Archivo Suricata.rules_ids

El archivo "suricata.rules_ids" es un archivo de identificación de reglas de Suricata. En Suricata, las reglas se organizan en archivos, y "suricata.rules_ids" es uno de esos archivos. Contiene identificadores (IDs) que corresponden a las reglas definidas en otros archivos, como "suricata.rules".

Estos IDs se utilizan para hacer referencia a reglas específicas cuando se configura Suricata para ejecutar ciertas acciones, como bloquear paquetes maliciosos o generar alertas.

Es importante mantener el archivo "suricata.rules_ids" actualizado y sincronizado con los archivos de reglas correspondientes para asegurar que los IDs sean coherentes y no se produzcan conflictos al ejecutar las reglas.

El archivo "suricata.rules_ips" es un archivo de definiciones de reglas de Intrusion Prevention System (IPS) utilizado por Suricata. En

Suricata, las reglas IPS se utilizan para detectar y prevenir actividades maliciosas en una red.

Estas reglas pueden incluir patrones de tráfico específicos que indican actividades sospechosas, como intentos de intrusión, exploración de vulnerabilidades o tráfico malicioso conocido.

7.2.- Archivo suricata.rules_ips

El archivo "suricata.rules_ips" contiene las reglas que Suricata utiliza para tomar acciones preventivas cuando detecta una actividad maliciosa. Estas acciones pueden incluir bloquear el tráfico, registrar eventos o tomar otras medidas para proteger la red contra posibles ataques.

Es importante mantener este archivo actualizado con las últimas definiciones de reglas para garantizar una protección efectiva contra amenazas en la red.

7.3.- Archivo fast.log

El archivo "fast.log" es un archivo de registro generado por Suricata que contiene información sobre eventos rápidos. Estos eventos son generalmente aquellos que Suricata puede procesar rápidamente y que no requieren una inspección más profunda.

El contenido específico del archivo "fast.log" puede variar dependiendo de la configuración de Suricata y de los eventos que ocurran en la red. Sin embargo, típicamente incluirá información como la marca de tiempo del evento, la dirección IP de origen y destino, los puertos utilizados, el protocolo de red, y detalles sobre la acción tomada por Suricata en respuesta al evento (como permitir, bloquear, o registrar el evento).

El archivo "fast.log" es útil para obtener una visión general de la actividad de red detectada por Suricata de manera rápida y eficiente, sin necesidad de examinar eventos más detallados. Sin embargo, es importante tener en cuenta que este archivo puede no incluir todos los eventos y detalles, por lo que puede ser necesario consultar otros

archivos de registro para obtener una imagen completa de la actividad de red y de las acciones tomadas por Suricata.

7.4.- Archivo suricata.yaml

El archivo "suricata.yaml" es el archivo de configuración principal de Suricata. Contiene una gran cantidad de opciones y configuraciones que controlan el comportamiento y el rendimiento de Suricata, así como la forma en que detecta y responde a las amenazas en la red.

Algunas de las configuraciones que puedes encontrar en el archivo "suricata.yaml" incluyen:

Configuración de interfaces de red y modos de captura.

Configuración de reglas y archivos de reglas utilizados para la detección de amenazas.

Configuración de la salida de registro y los archivos de registro utilizados para almacenar información sobre eventos de red.

Configuración de los preprocesadores de tráfico que se aplican antes de la detección de reglas.

Configuración de la administración de recursos, como la memoria y la CPU utilizadas por Suricata.

Es importante editar este archivo con cuidado y comprender cómo cada configuración afecta el comportamiento de Suricata. Cambiar la configuración incorrectamente puede afectar la efectividad de la detección de amenazas o incluso causar problemas de rendimiento en el sistema. Se recomienda realizar copias de seguridad del archivo antes de realizar cambios significativos y consultar la documentación oficial de Suricata para obtener orientación sobre cómo configurar correctamente el sistema de acuerdo a tus necesidades específicas.

8.- Anexos.

8.1.- CYBER-SEGURIDAD 🐧 Instalar SURICATA y KALI Linux ✅ y configurar las REGLAS y Alertas

<https://www.youtube.com/watch?v=FUh4WT9cm24>

El vídeo "CYBER-SEGURIDAD 🐧 Instalar SURICATA y KALI Linux ✅ y configurar las REGLAS y Alertas" explica cómo instalar y configurar Suricata y Kali Linux en una máquina Ubuntu para realizar monitoreo de red y detección de intrusiones. Los pasos incluyen:

- Crear dos máquinas virtuales en VirtualBox, una con Kali Linux y otra con Suricata.
- Instalar VirtualBox desde su sitio web y crear una nueva máquina virtual.
- Descargar la imagen ISO de Ubuntu 20.04 y montarla en la máquina virtual.
- Configurar la máquina virtual con 2 GB de RAM y un procesador.
- Instalar Suricata en la máquina Ubuntu y configurar reglas y alertas para detectar intrusiones.
- Utilizar herramientas como Pin, nmap y el monitor de red de Kali Linux para probar la capacidad de detección y reacción de Suricata.

El objetivo del vídeo es mostrar cómo usar Suricata como sistema de detección e interrupción de intrusiones (IDS/IPS) y cómo utilizar Kali Linux como una herramienta de ataque para simular ataques contra la máquina Ubuntu monitoreada por Suricata.

8.2.- 🔊 IPS IDS Linux🐧 Instalar SURICATA y configurar las REGLAS y Alertas 🌐

<https://www.youtube.com/watch?v=vQNB7nenT2E>

En este vídeo, se explica cómo instalar y configurar Suricata, un sistema de detección e interrupción de intrusiones (IDS/IPS), en un sistema operativo Linux. Se abordan diferentes aspectos del software, como su funcionamiento, configuración de reglas y alertas, y se

muestra cómo integrarlo con Kali Linux. El vídeo está dividido en varias secciones y ofrece información práctica para usuarios interesados en mejorar la protección de sus sistemas contra posibles ataques o intrusiones. Los pasos incluyen la creación de dos máquinas virtuales en VirtualBox, una con Kali Linux y otra con Suricata, y la instalación y configuración de ambos sistemas. El objetivo del vídeo es mostrar cómo usar Suricata como sistema de detección e interrupción de intrusiones y cómo utilizar Kali Linux como una herramienta de ataque para simular ataques contra la máquina Ubuntu monitoreada por Suricata.

8.3.- ¿Cómo obtener la contraseña de servicio como SSH y FTP - Hydra?

<https://www.youtube.com/watch?v=dpnHSB5VoLo>

El vídeo "¿Cómo obtener la contraseña de servicio como SSH y FTP - Hydra?" en YouTube explica cómo usar la herramienta Hydra para obtener las contraseñas de servicios como SSH y FTP mediante el método de fuerza bruta. El vídeo comienza mostrando la interfaz de Hydra en Kali Linux y luego explica cómo leer su manual y explorar opciones como la opción "-h" para obtener ayuda rápida y la opción "man space hydra" para obtener una versión más completa del manual. Luego, se discuten alternativas a Hydra, como Medusa, Crack y Pataton. El vídeo también cubre la importancia de estar en un contexto apropiado para usar la herramienta, como en un entorno de pruebas o penetración autorizada. Finalmente, se muestra cómo usar Hydra para auditar servicios específicos, como SSH, FTP y HTTP, y cómo utilizar opciones como "-l" para especificar una lista de usuarios, "-p" para especificar una lista de contraseñas y "-m" para especificar un archivo de metadatos que contiene información sobre los objetivos de ataque.

8.4.- CRUNCH - Creación de diccionarios para fuerza bruta

<https://www.youtube.com/watch?v=9HXbfFRYus8>

Este vídeo en YouTube explica cómo usar la herramienta CRUNCH para crear diferentes tipos de diccionarios para la fuerza bruta. Las secciones principales del vídeo incluyen:

- Creación de diccionarios con números del 0 al 999: crunch 1 3 0123456789.
- Creación de diccionarios alfabéticos con palabras de 3 a 4 caracteres: crunch 3 4.
- Creación de diccionarios con palabras de 4 a 5 caracteres y formato específico: crunch 4 5 "formato".

Las opciones disponibles en CRUNCH incluyen:

- @: Minúsculas.
- ,: Mayúsculas.
- ^: Símbolos.
- %: Números.

Los usuarios pueden especificar el número mínimo y máximo de caracteres en las palabras del diccionario y utilizar opciones como -l para especificar una lista de usuarios y -p para especificar una lista de contraseñas. Además, se puede utilizar el parámetro -m para especificar un archivo de metadatos que contiene información sobre los objetivos de ataque. La herramienta CRUNCH es útil para la generación de diccionarios personalizados y la creación de combinaciones de palabras con diferentes caracteres.

Índice Alfabético

A

actualizaciones	11
Adaptador	9, 19
ajustes	8
ALT	19
atacante	3, 27, 29, 32
Ataque	4, 31, 33
ataques	3, 30, 31, 38, 40, 41
aviso	12

C

caracteres	4, 5, 6, 42
cibernéticas	3, 31
ciberseguridad	3
Claves	4
comandos	4
comunes	3, 30
conexión	3, 9, 29
confidencialidad	3, 30
configuración	3, 7, 8, 9, 13, 18, 23, 24, 25, 27, 31, 32, 37, 38, 39, 40
conjunto	6
CPU	7, 39
creación	8, 15, 27, 32, 33, 41, 42
criterios	5
Crunch	3, 4, 5, 32
CTRL	19, 25, 33
cuentas	3

D

descripción	4
detalles	13, 38
detección	3, 27, 39, 40
diccionario	5, 6, 32, 33, 42
directorio	17, 22, 23
disponibilidad	3

E

editor	24, 25, 26, 32, 33, 36
efectividad	3, 39
Enter	26, 32, 34, 35
entorno	3, 41
escala	5
Escenario	4
específica	26

específicas	4, 27, 37, 39
específicos	24, 31, 38, 41
Esquema	4
Establecemos	6, 7
eventos	3, 27, 38, 39
extensión	18

F

fines	4
-------------	---

G

Generación	4
gráfica	4
gráfico	8

H

herramientas	3, 30, 40
Hydra	3, 33, 41

I

ICMP	26, 27
IDS3	30, 40
imágenes	18
implementación	3
importancia	3, 41
importantes	12, 13, 31
información	22, 28, 38, 39, 41, 42
informática	4, 5, 30, 31
Instalación	6, 16, 27
integridad	3
intentos	3, 38
interfaz	25, 41
Intro	20, 21, 22, 23, 24, 27, 28, 29
intrusiones	3, 27, 40
IPS3	30, 34, 37, 40
iso 6	

K

Kali	16, 17, 18, 26, 27, 40, 41
------------	----------------------------

L

- lector 22
 Limpio 15
 Linux 4, 16, 40, 41
 listas 4, 5
-

M

- malicioso 3, 30, 38
 máquina 3, 6, 7, 8, 9, 16, 17, 18, 27, 29, 33, 34, 40, 41
 máquinas 4, 40, 41
 mayúsculas 4
 minúsculas 4
 monitorización 27
-

N

- necesidades 4, 31, 39
-

O

- Objetivo 6, 31
 oisf/suricata 21
 opción 6, 8, 9, 13, 14, 18, 34, 36, 41
 Operativo 15
 oportunidad 3
 Optamos 13
 organizaciones 3
-

P

- página 16
 pantalla . 5, 6, 8, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23,
 24, 25, 26, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37
 paquetes 27, 37
 patrones 4, 5, 38
 penetración 4, 41
 práctica 3, 41
 Prevención 3, 30
 promisión 3
 puedes 4, 39
-

R

- reglas 26, 27, 30, 35, 37, 38, 39, 40
 repositorio 20
 repositorios 21
 Representación 4
 respuesta 3, 38
-

S

- seguridad 3, 4, 5, 30, 31, 37, 39
 Seleccionamos 9, 10
 servicio 3, 23, 28, 33, 41
 servicios 3, 41
 sesión 13, 14
 símbolo 25
 Sistema 3, 15
 sospechosos 3, 30
 Spanish 10
 SSH 3, 28, 29, 32, 33, 41
 status 23, 28
 Suricata ... 3, 19, 20, 22, 23, 24, 25, 26, 27, 34, 37, 38,
 39, 40
-

T

- teclas 19, 25, 26
 técnicas 3
 tráfico 3, 30, 38, 39
-

U

- ubicación 6, 12
 Ubuntu 10, 11, 29, 40, 41
 Unix 4
 users/internet/virtualbox 6
 Usuarios 4
 utilización 3
-

V

- variante 10
 VBoxSVGA 8
 Verificación 26
 VirtualBox 14, 16, 17, 18, 40, 41
 volúmenes 5