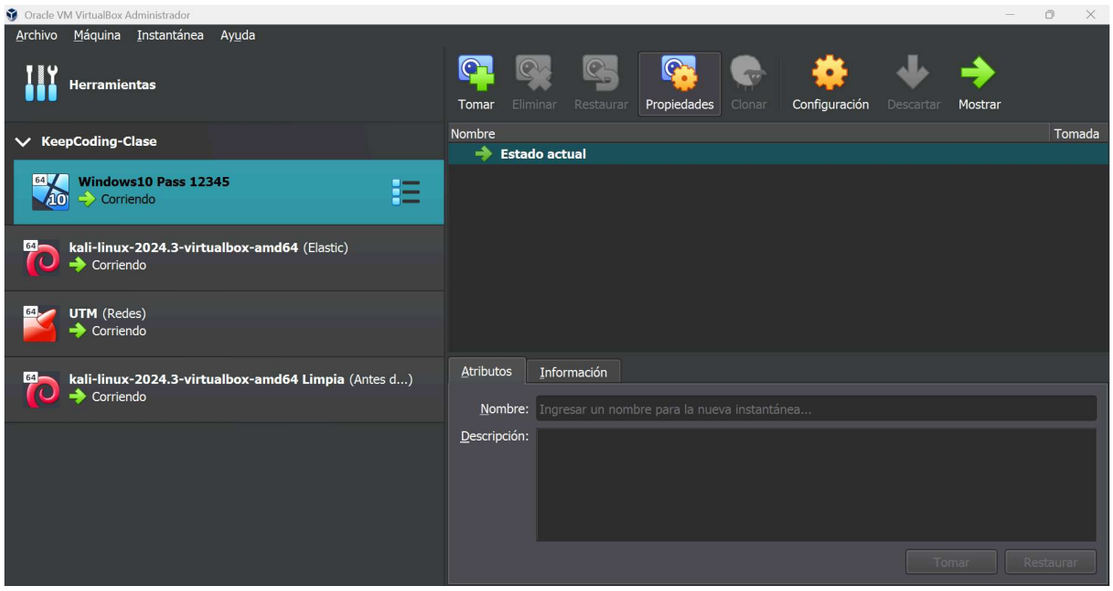
MEMORIA PRÁCTICA
BLUE TEAM 2025

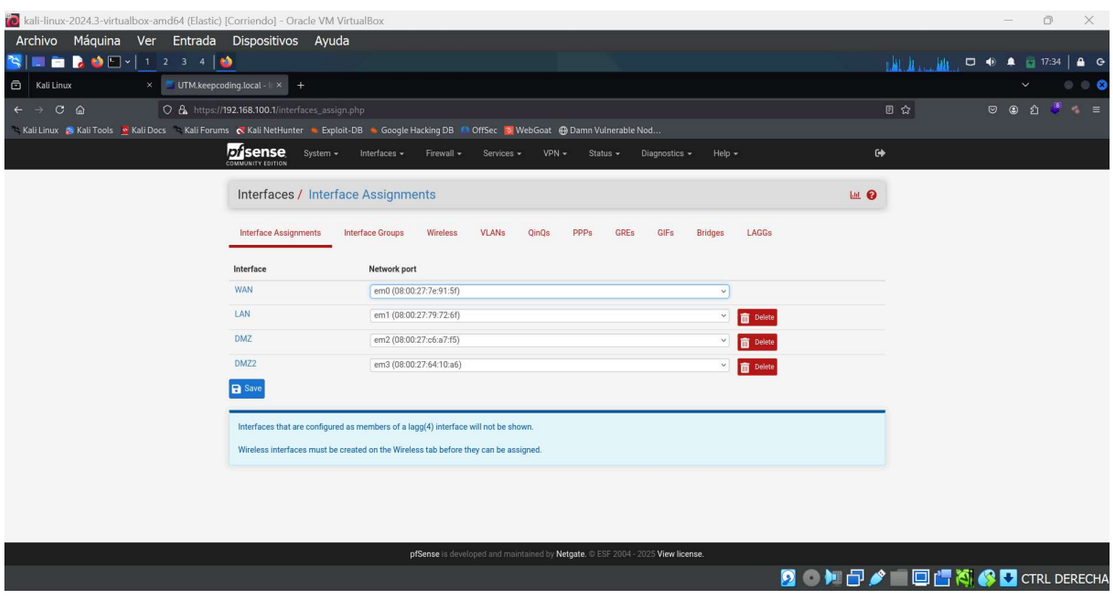
Rafael Figueroa
Versión 1.0

Se ha procedido a instalar las siguientes máquinas virtuales, para cumplir con los requisitos de estructura de red solicitada



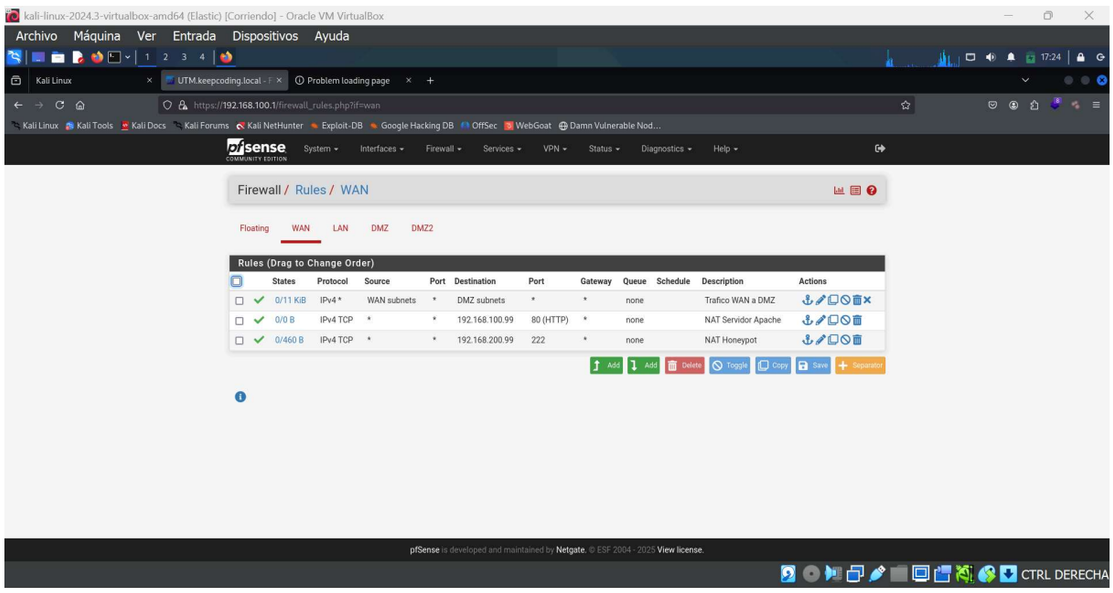
Arrancamos la máquina virtual UTM y una máquina Kali en la red LAN generada por el mismo UTM para proceder a configurar los parámetros de Pfsense desde el navegador web, ya que está es la red que se tiene que usar en la primera configuración

Añadimos las otras 2 redes, DMZ y DMZ2 a las que más adelante se conectarán las 2 máquinas Kali

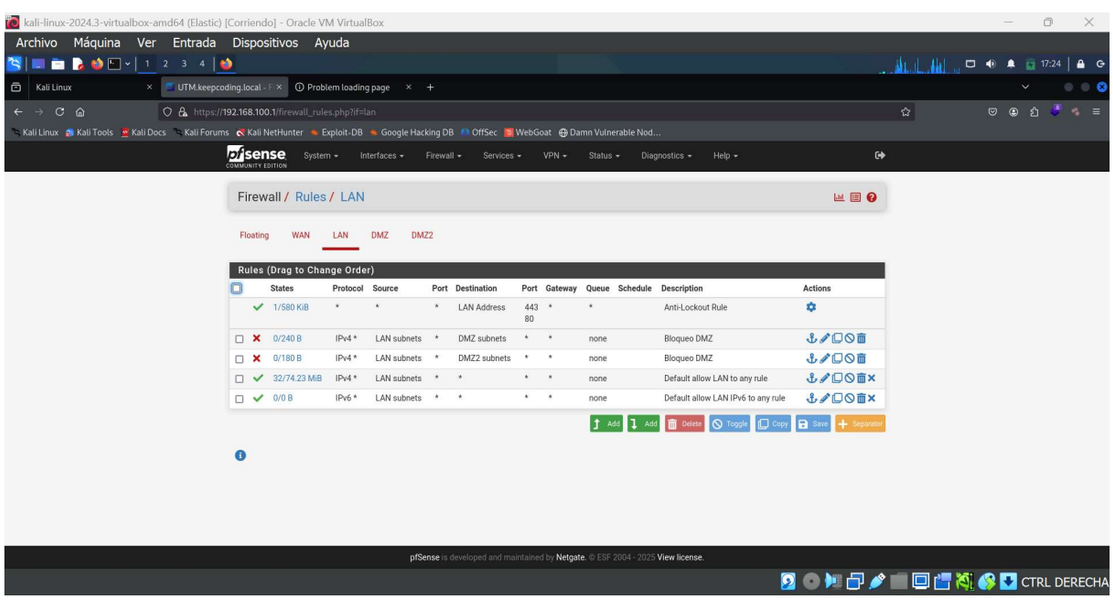


En las siguientes capturas se observa la configuración de las reglas del firewall, con ellas se ha configurado la red según los requisitos solicitados, se detalla cada paso y su función.

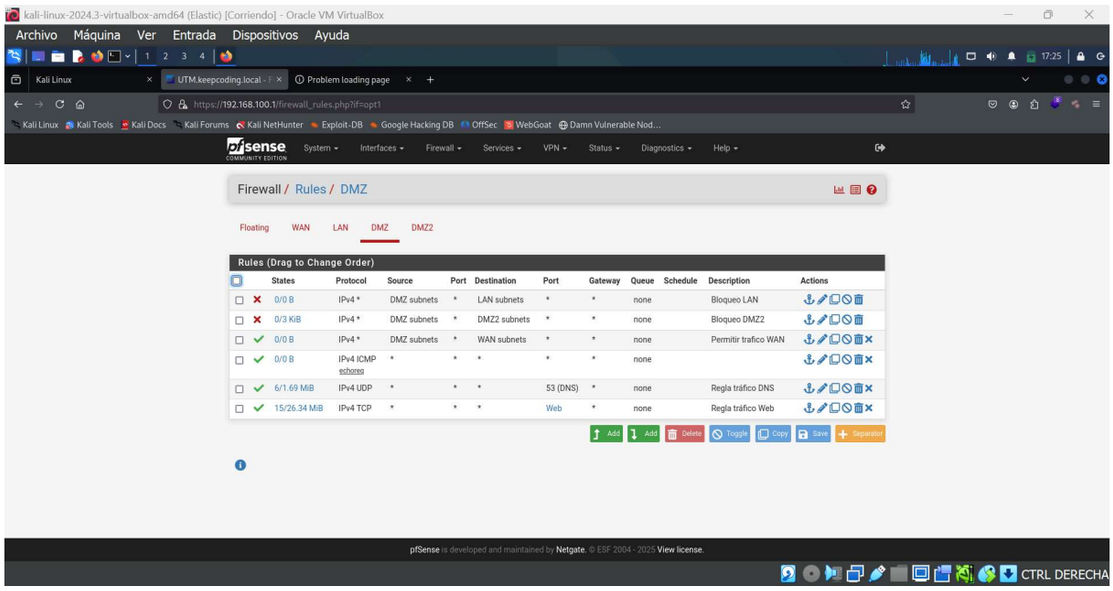
1- Red WAN con conexión a DMZ, para poder conectar por SSH con ella, habilitándose también el puerto 222 para dicha conexión



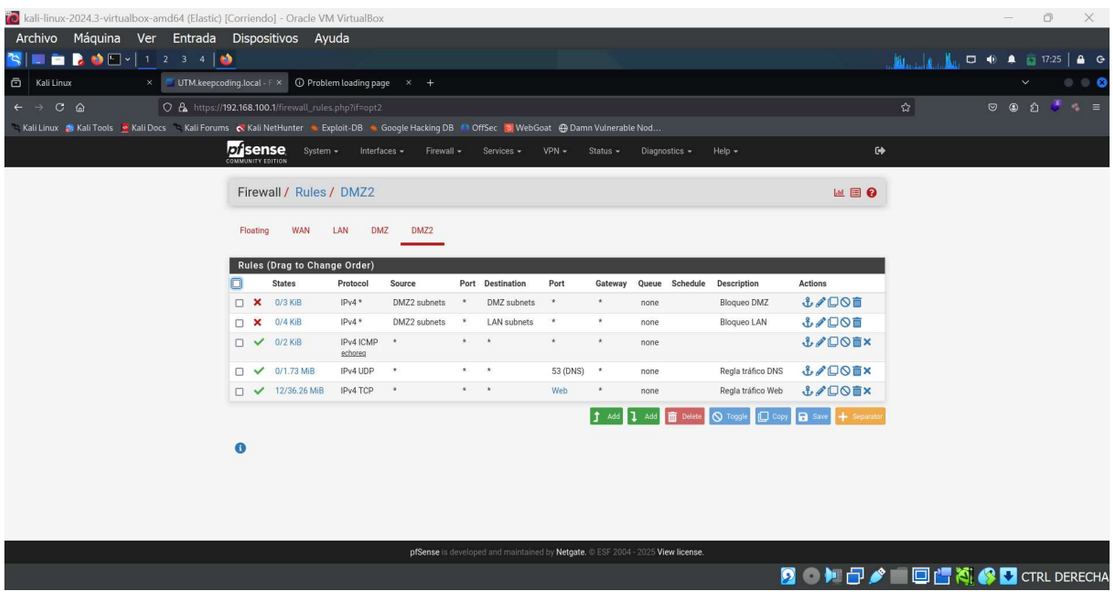
2- Red LAN con conexión a internet y aislada totalmente de DMZ y DMZ2



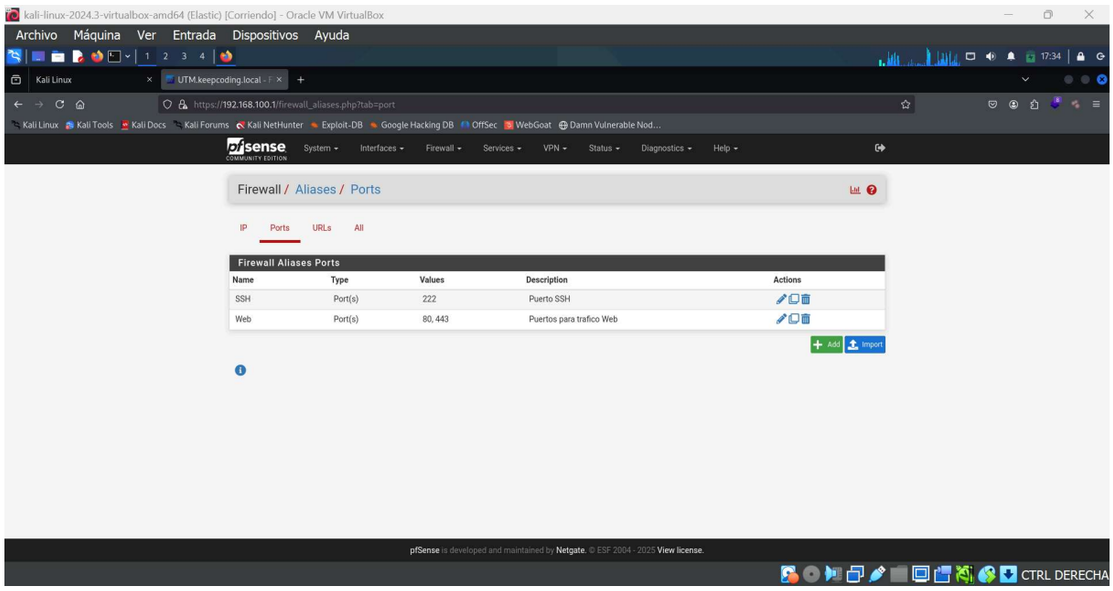
3- Red DMZ con conexión a internet, aislada de la red LAN y DMZ2 y con acceso a WAN para conexiones SSH.



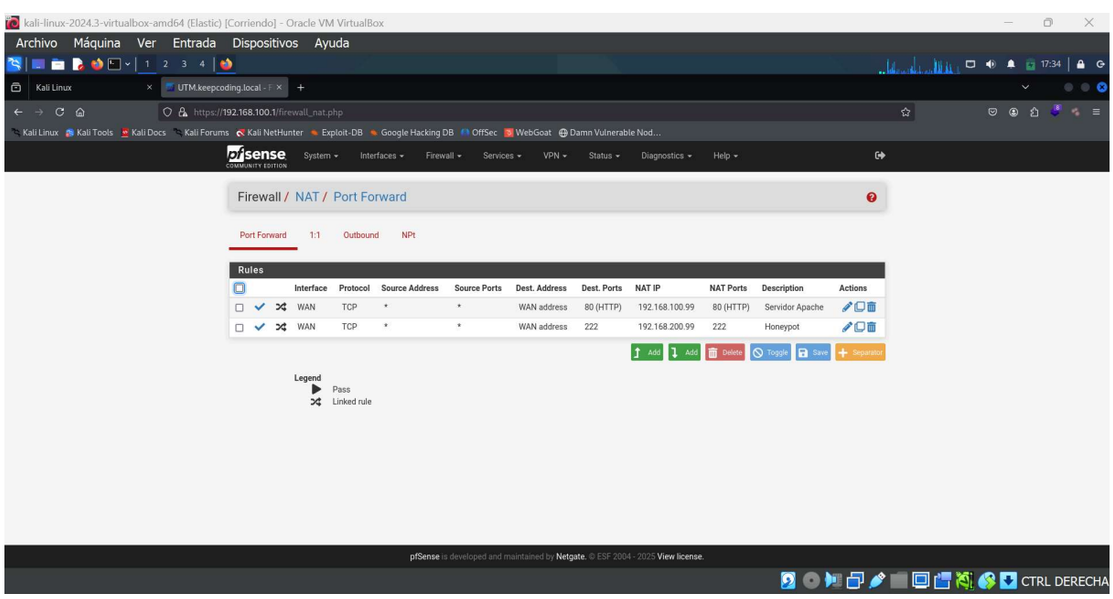
4- Red DMZ2 con conexión a internet, aislada de la red LAN y DMZ



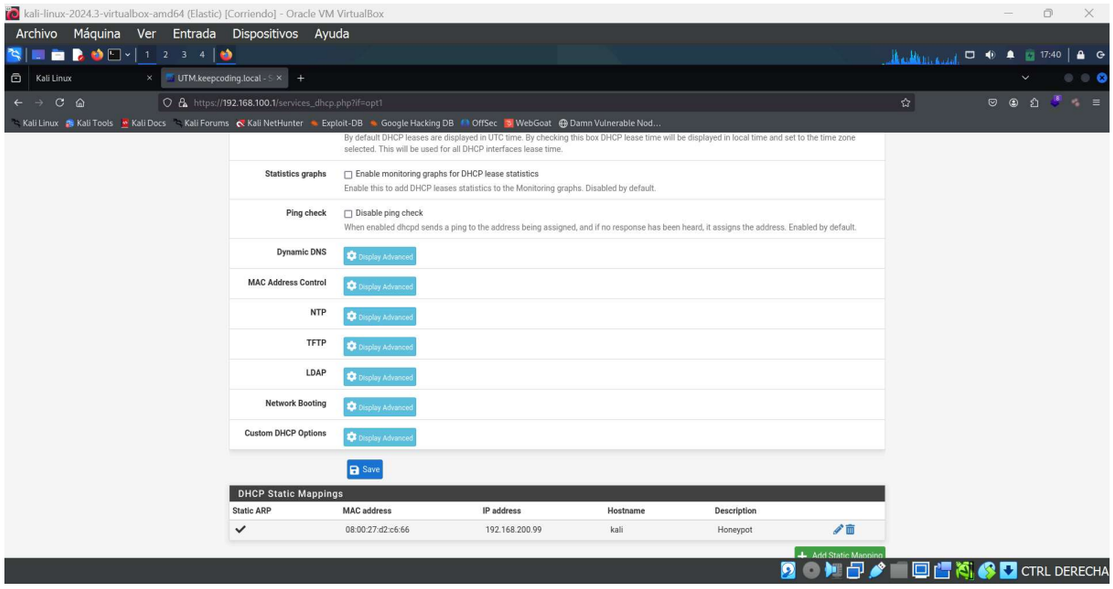
5- Se procede a abrir el tráfico de los puertos 80 y 443 para tráfico web y 222 para SSH

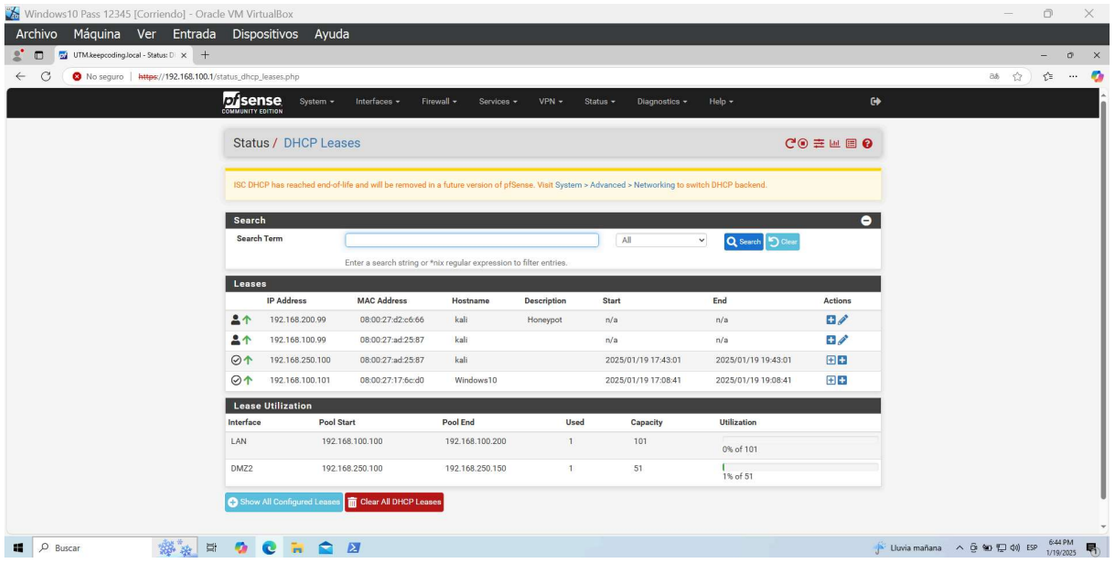


6- Se hace un portforwarding a las IP fija que se van a asignar a la red DMZ con el objetivo de que el honeypot que se instalará más sea accesible desde la red WAN

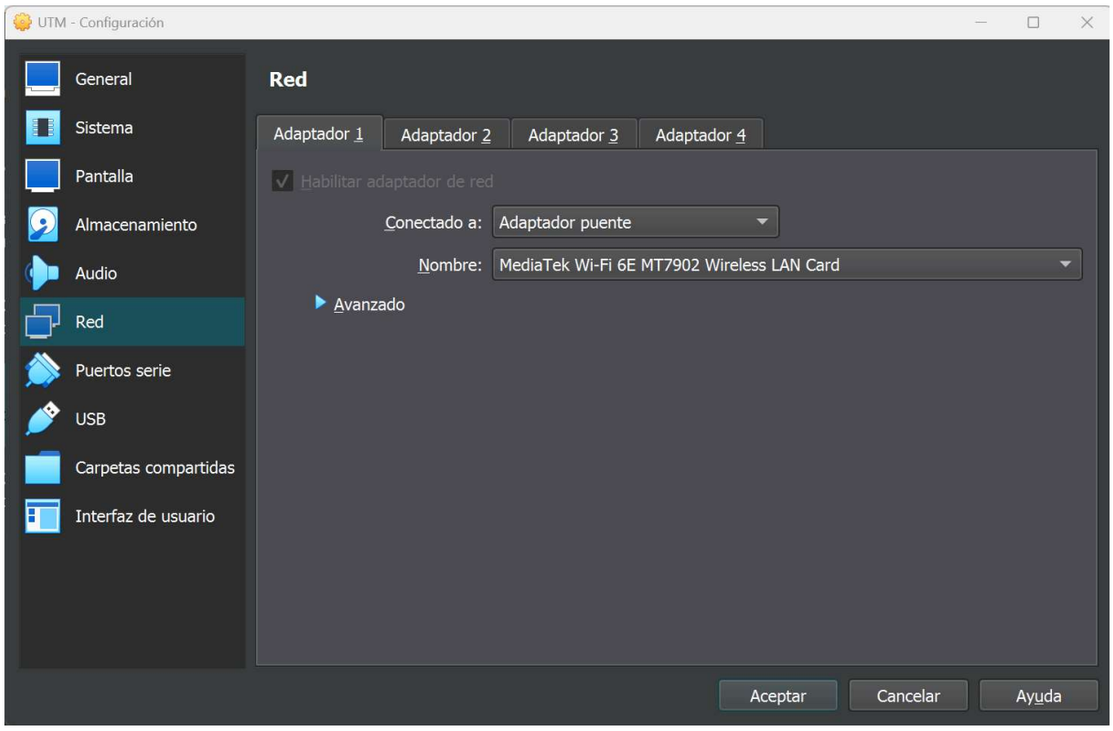


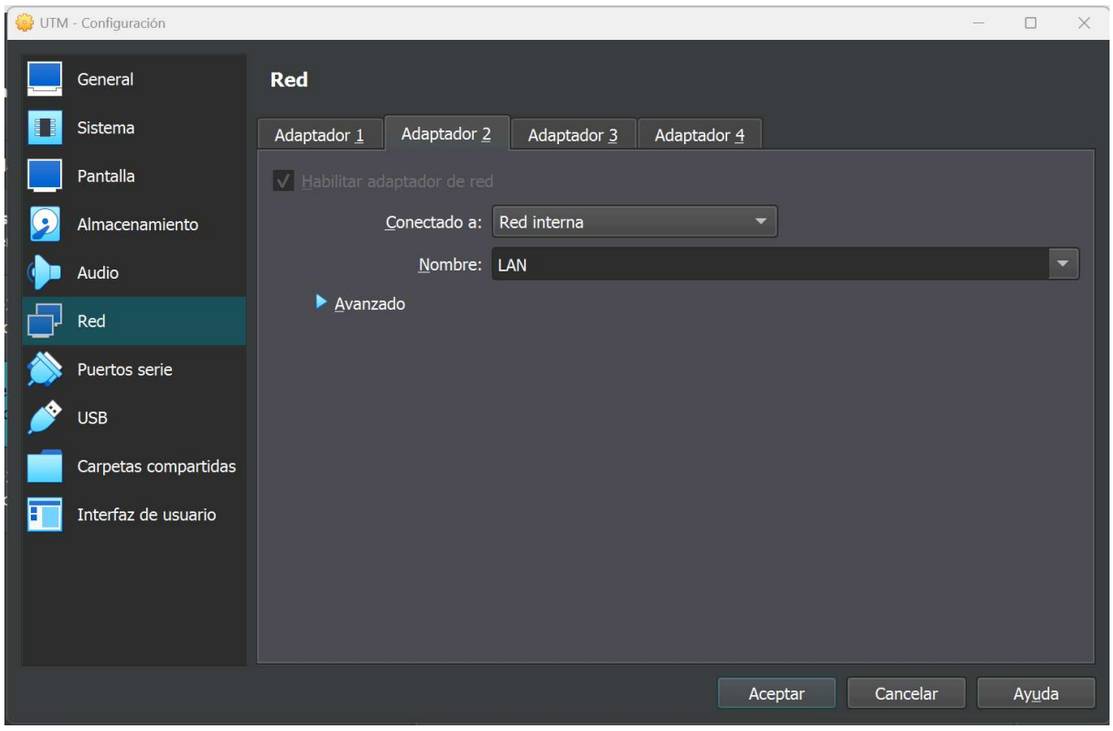
7- En las siguientes imágenes se puede ver como se ha asignado una IP fija dentro del rango de IPs correspondiente a la red DMZ, así como el pool de IPs de las redes.

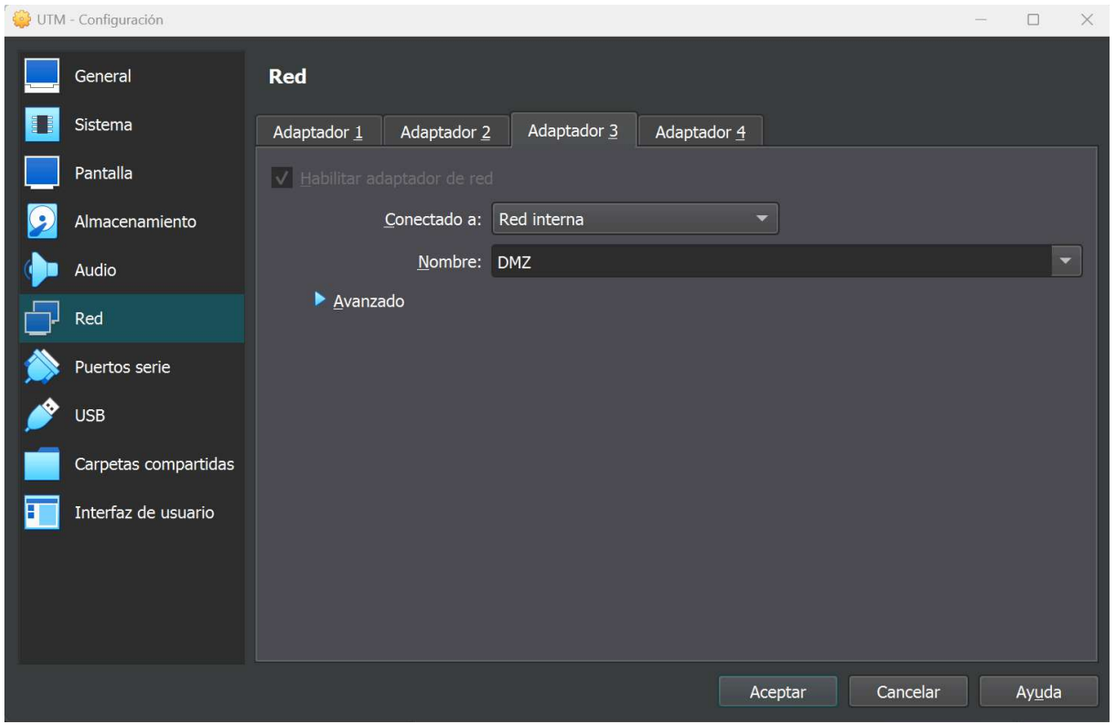


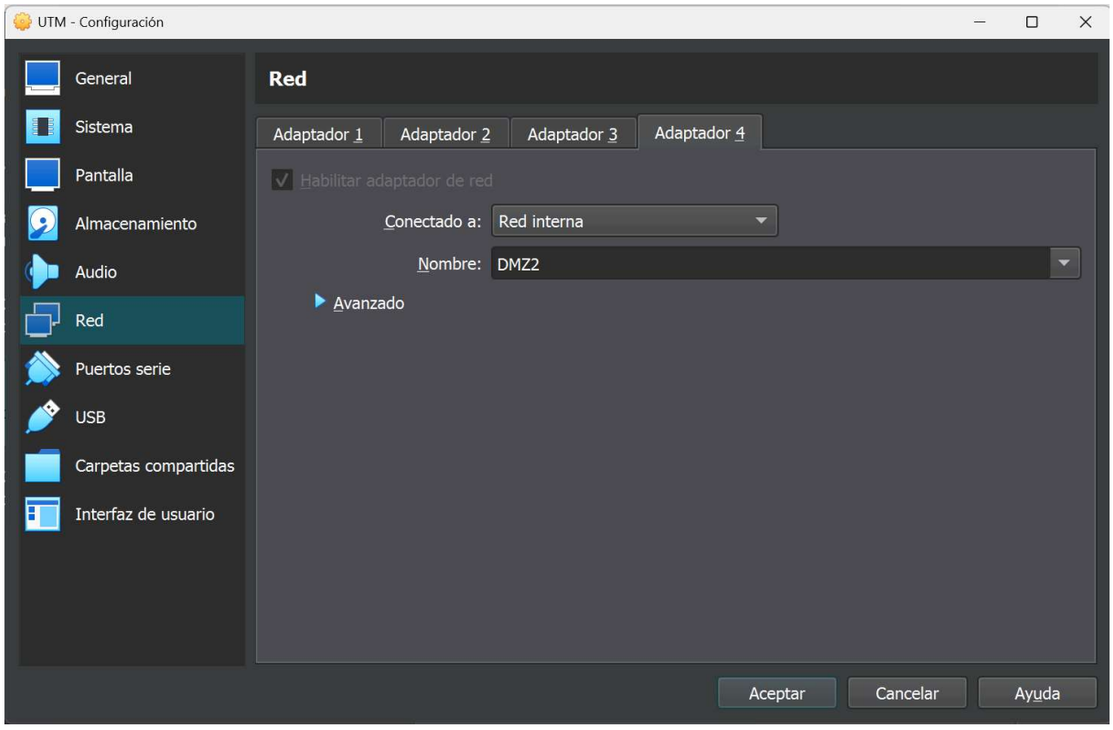


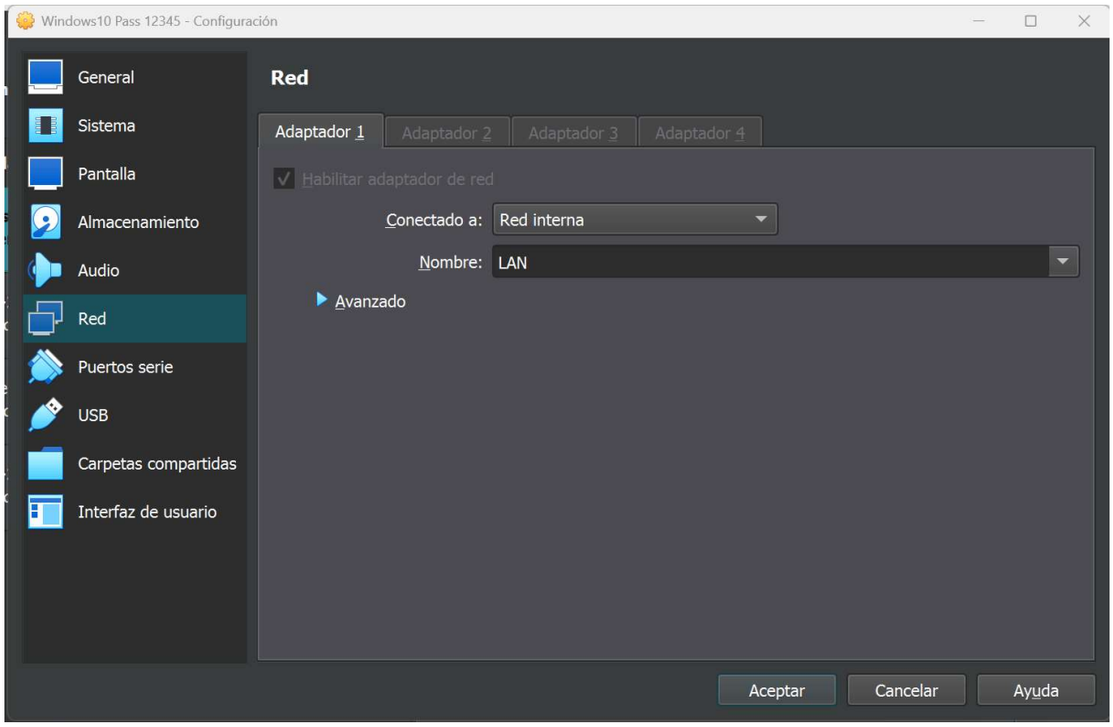
Una vez realizados estos ajustes se puede proceder a asignar a cada máquina su red correspondiente del UTM, en las siguientes imágenes se muestra la configuración del mismo con los distintos adaptadores y como ha cada máquina se le asocia el que le corresponde:

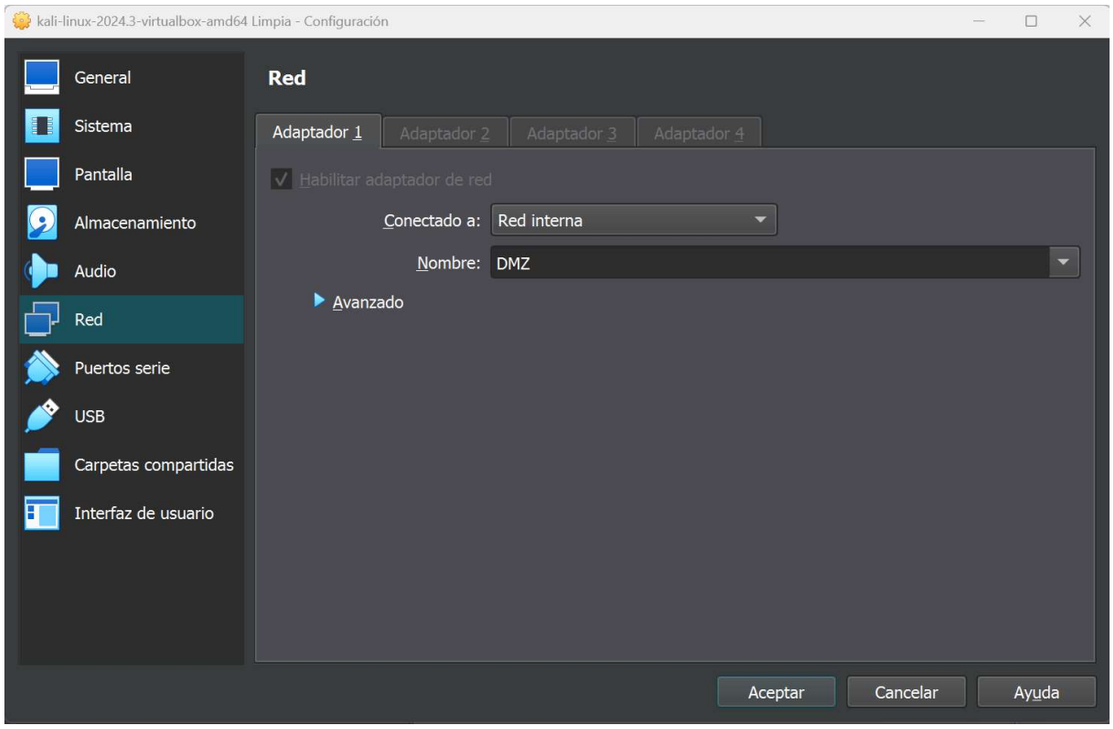


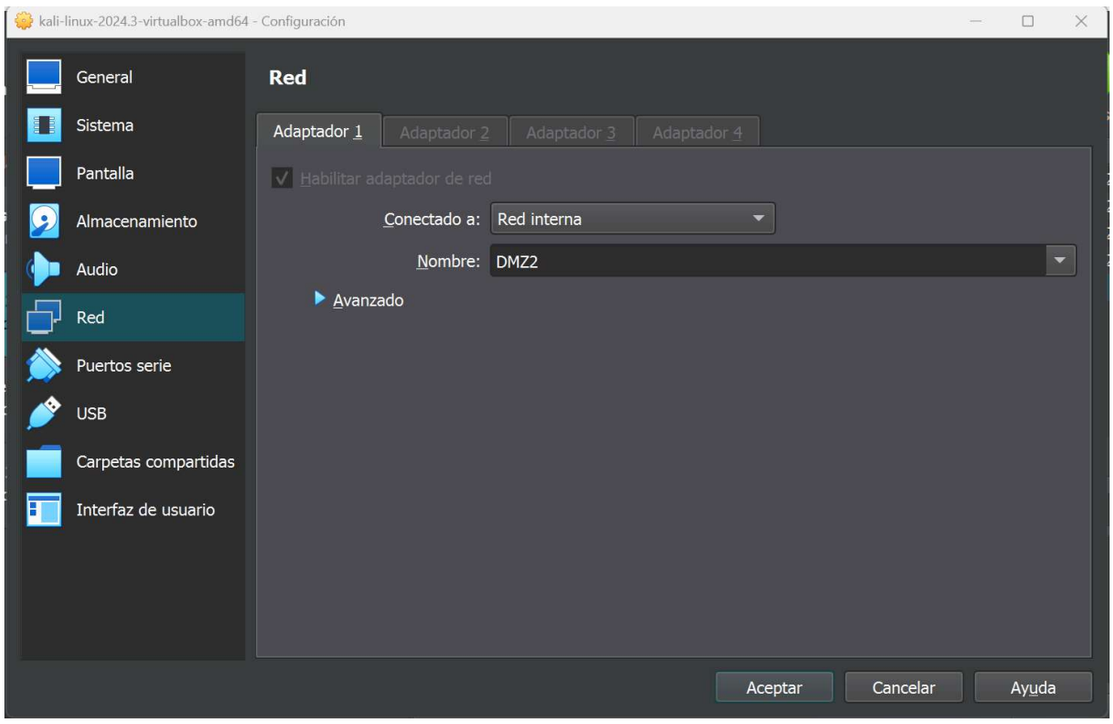



UTM - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
DMZ
Avanzado
Aceptar
Cancelar
Ayuda

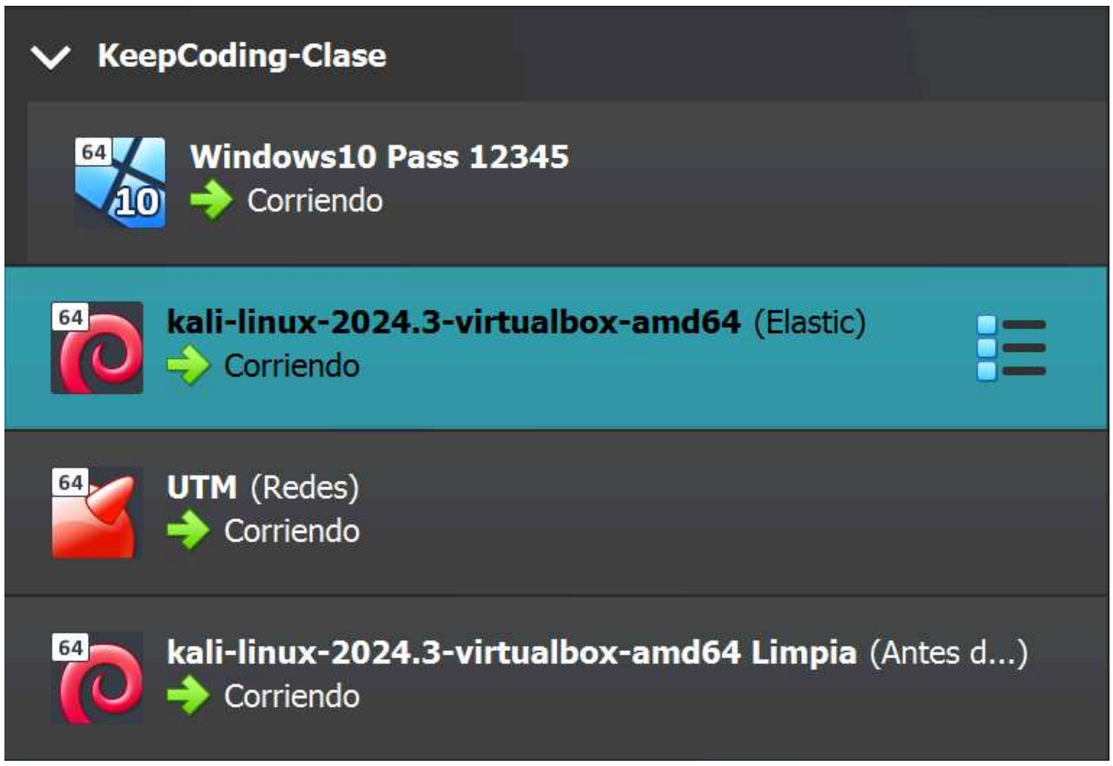

UTM - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
DMZ2
Avanzado
Aceptar
Cancelar
Ayuda


Windows10 Pass 12345 - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
LAN
Avanzado
Aceptar
Cancelar
Ayuda

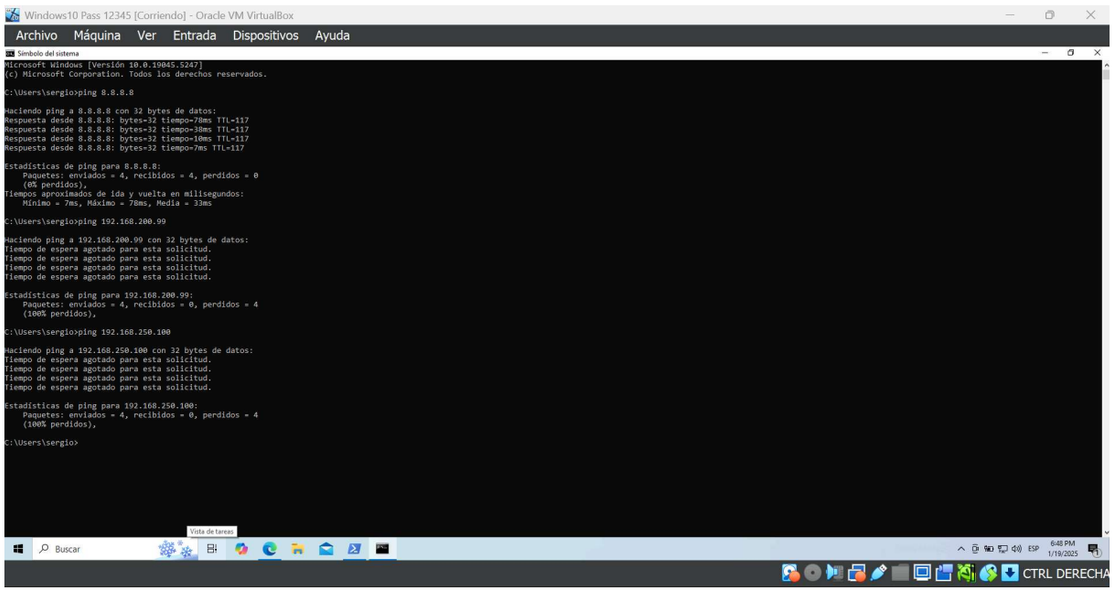

kali-linux-2024.3-virtualbox-amd64 Limpia - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
DMZ
Avanzado
Aceptar
Cancelar
Ayuda

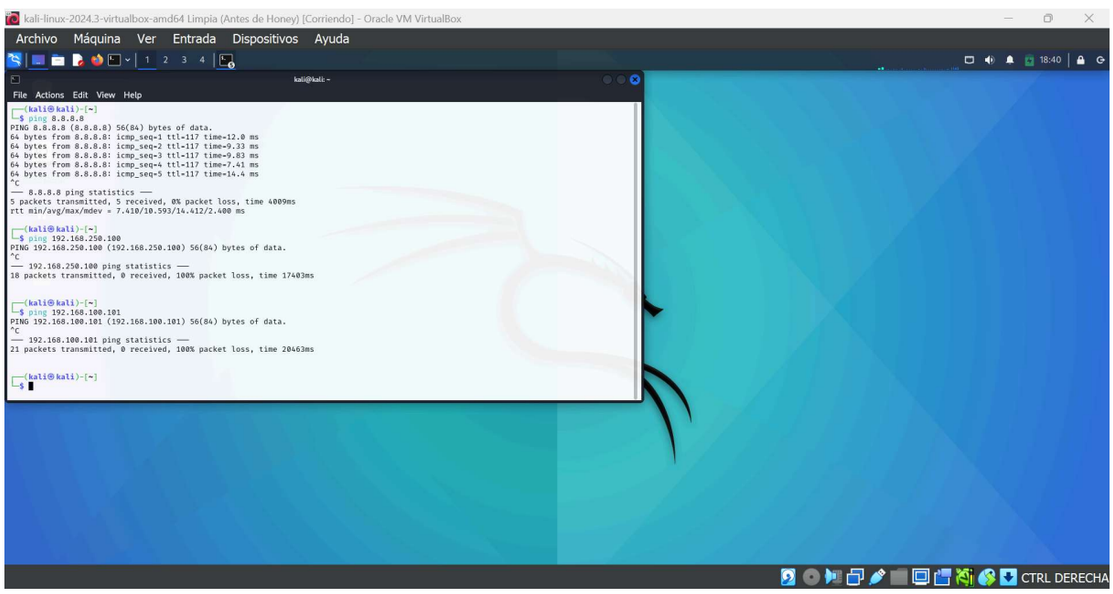


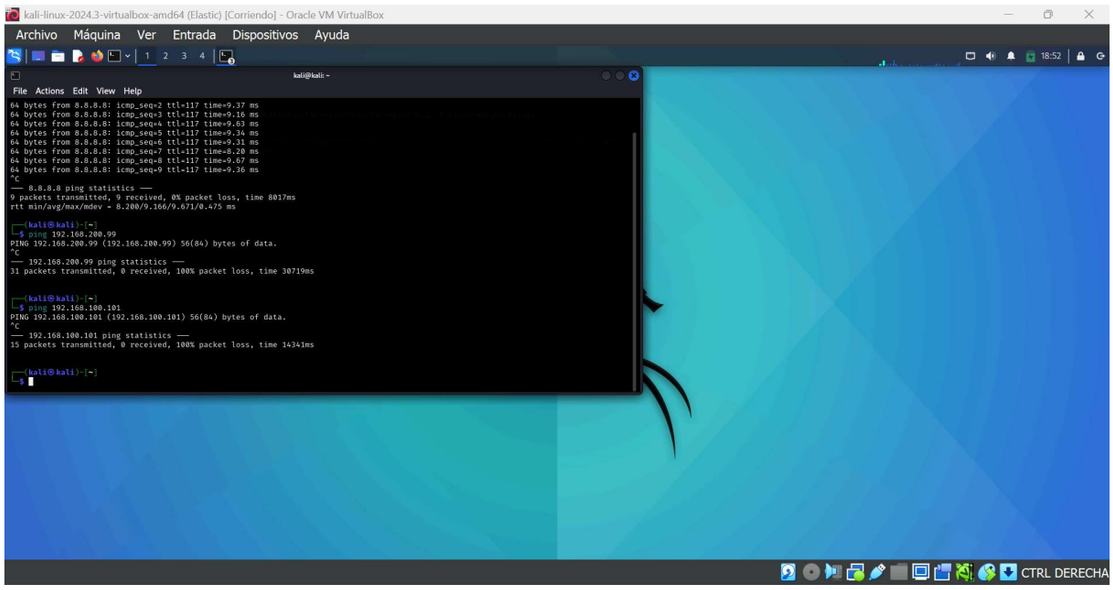
Una vez hecho esto se ha procedido a conectar todas las máquinas a la vez y testear si las reglas del firewall son las requeridas por la práctica:



Se procede a desde cada máquina a hacer un ping a la ip de google, para comprobar que hay conexión a internet, y un ping a las otras 2 IPs para comprobar que cada red está aislada de las otras 2:

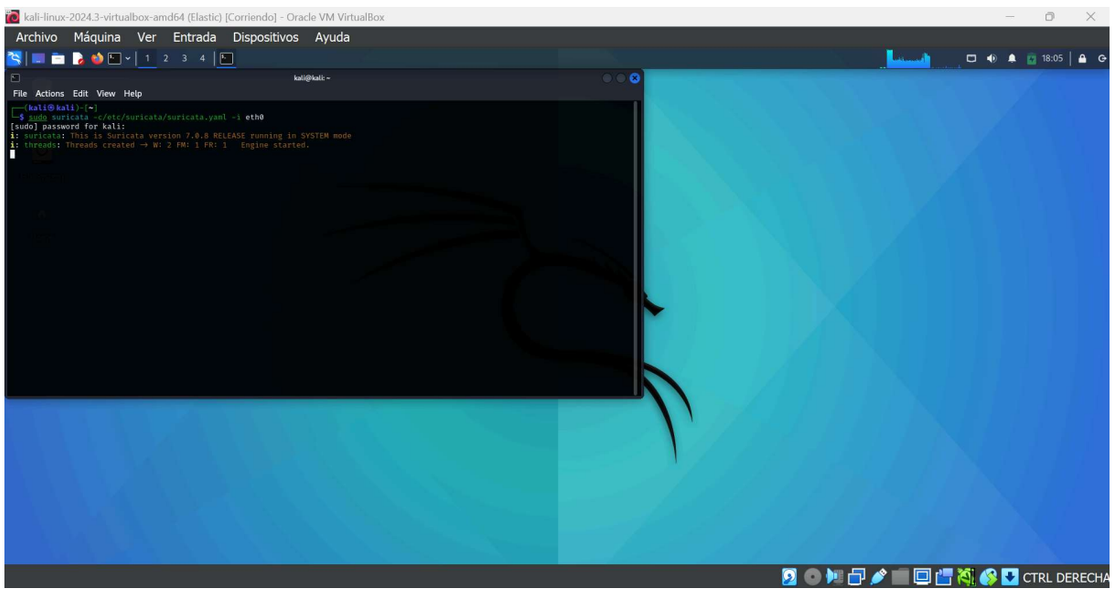




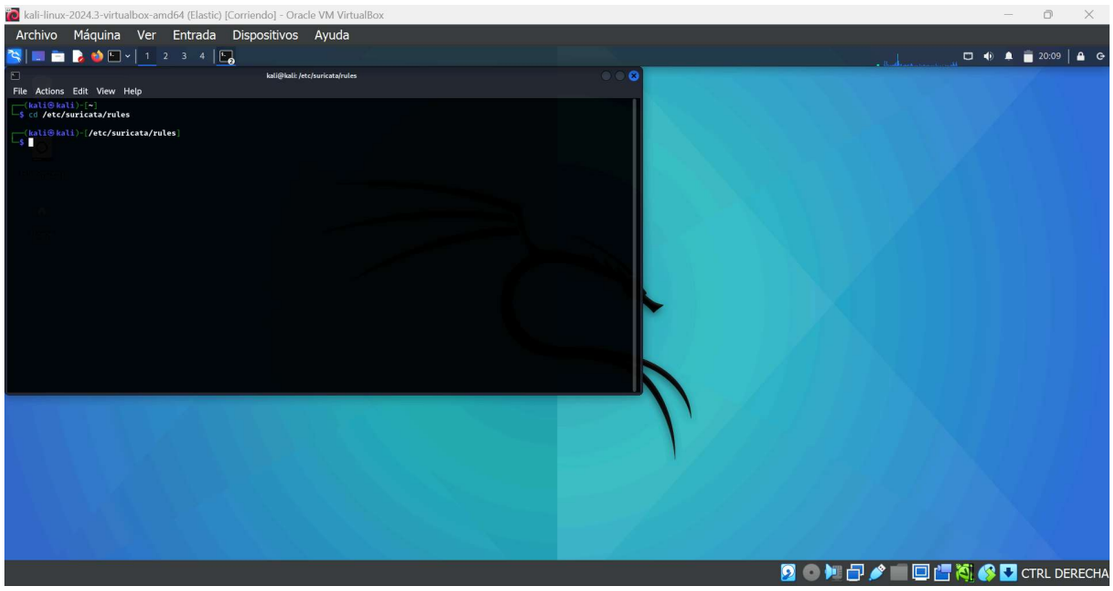


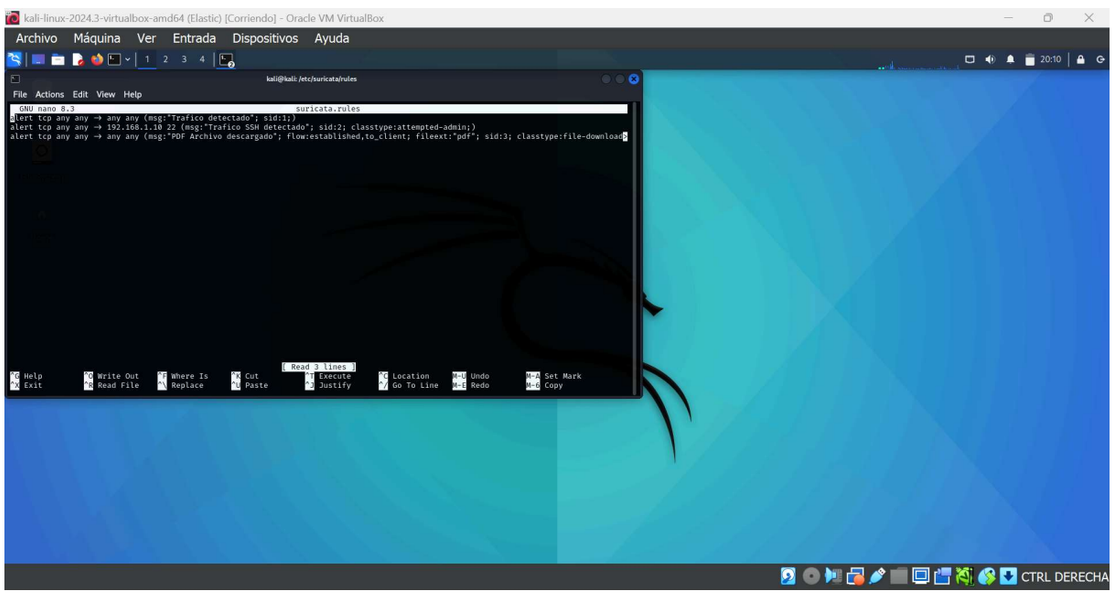
Una vez hechas las comprobaciones se procede a instalar Suricata en la máquina alojada en DMZ2 mediante los siguientes comandos:

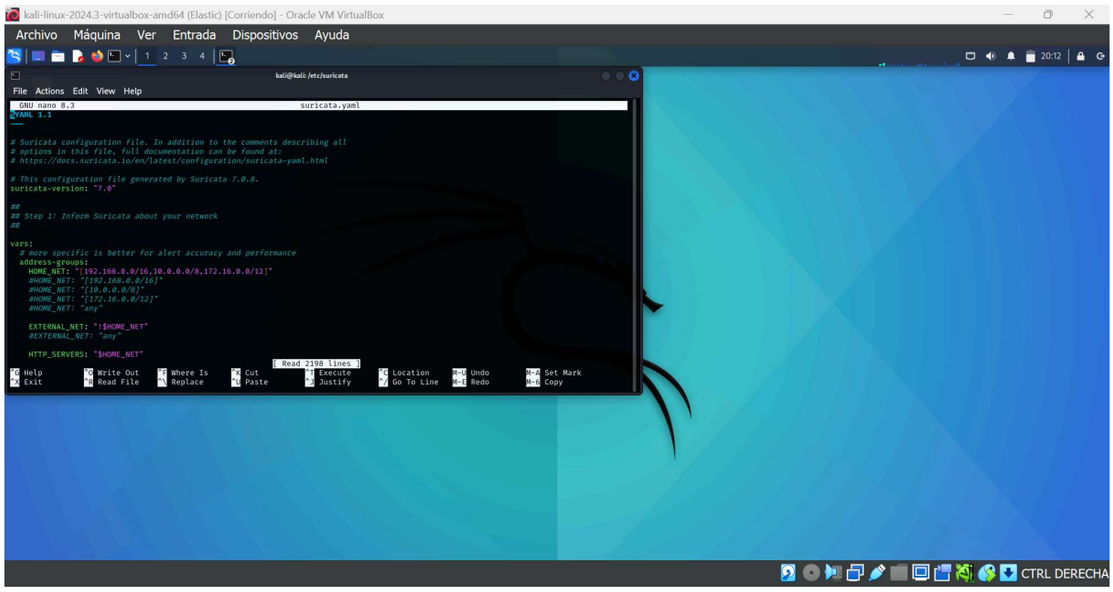
sudo apt update
sudo apt install suricata
sudo suricata -c /etc/suricata/suricata.yaml -i eth0

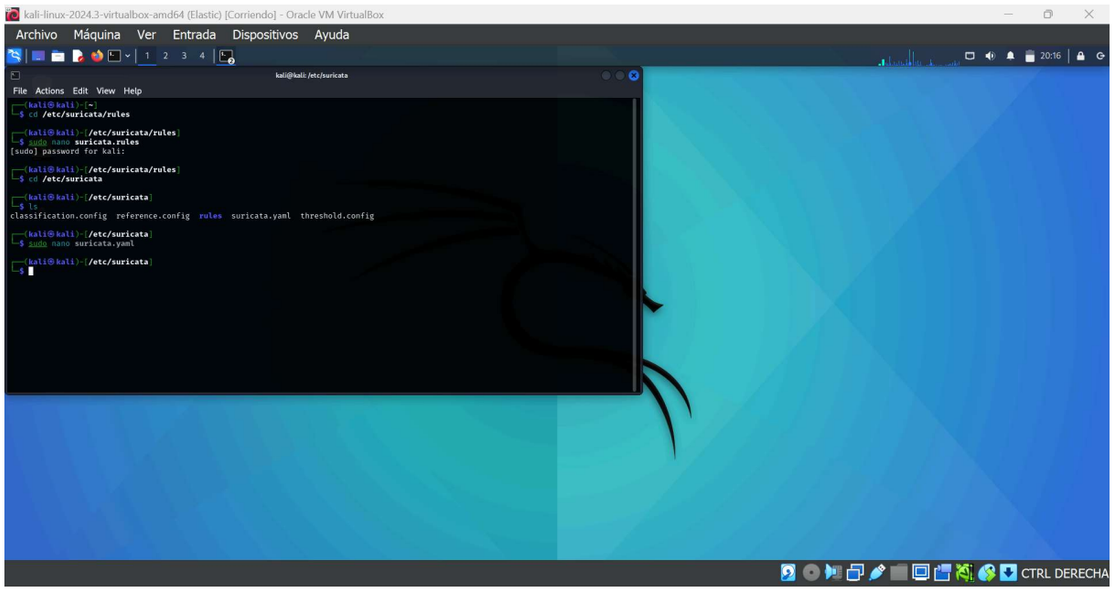


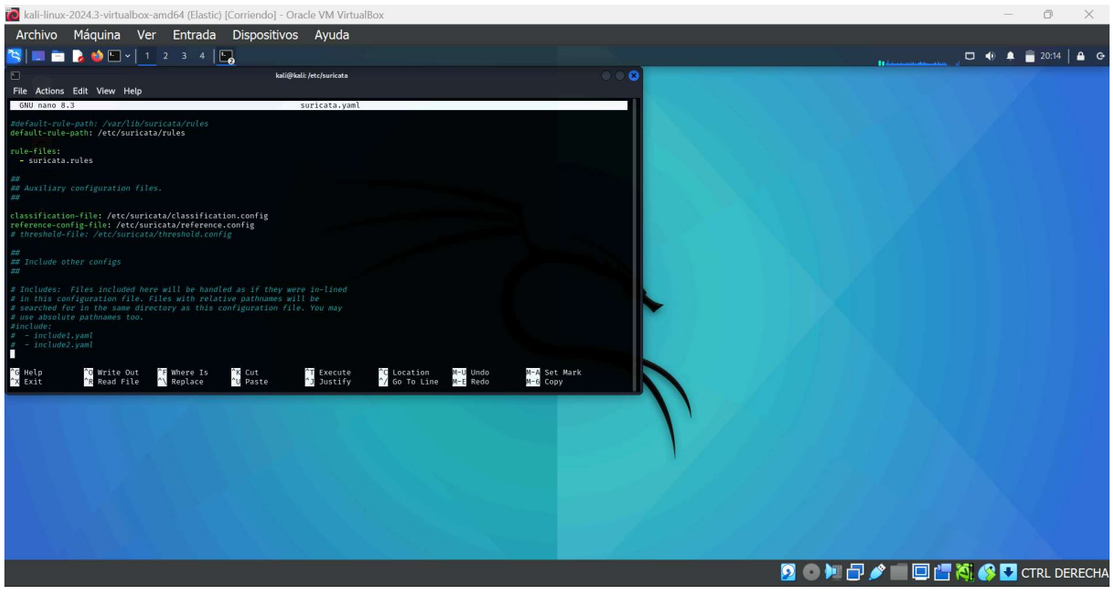
En las siguientes imágenes se puede ver como se procede a editar las reglas de suricata:






kali-linux-2024.3-virtualbox-amd64 (Elastic) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali@kali: /etc/suricata
File Actions Edit View Help
GNU nano 8.3 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 7.0.8.
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: "[192.168.0.0/16]"
#HOME_NET: "[10.0.0.0/8]"
#HOME_NET: "[172.16.0.0/12]"
#HOME_NET: "any"
EXTERNAL_NET: "!$HOME_NET"
#EXTERNAL_NET: "any"
HTTP_SERVERS: "$HOME_NET"
[Read 2198 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy
20:12
CTRL DERECHA

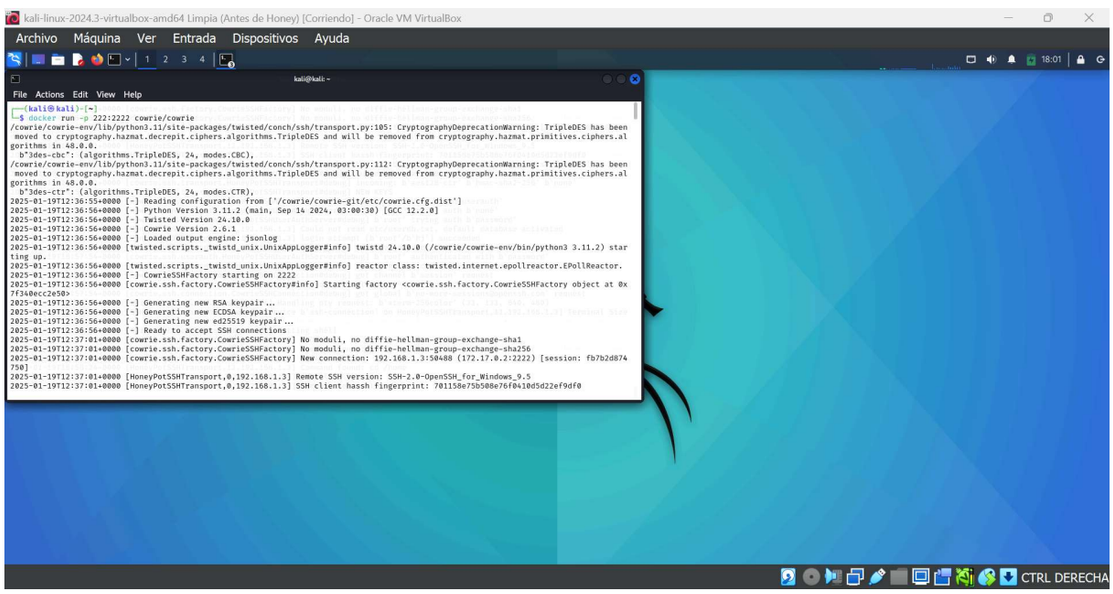

kali-linux-2024.3-virtualbox-amd64 (Elastic) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali@kali: /etc/suricata
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd /etc/suricata/rules
┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ sudo nano suricata.rules
[sudo] password for kali:
┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ cd /etc/suricata
┌──(kali㉿kali)-[/etc/suricata]
└─$ ls
classification.config reference.config rules suricata.yaml threshold.config
┌──(kali㉿kali)-[/etc/suricata]
└─$ sudo nano suricata.yaml
┌──(kali㉿kali)-[/etc/suricata]
└─$
20:16
CTRL DERECHA



Con esto quedaría configurado correctamente suricata.

Se procede ahora a instalar en la máquina Kali alojada en DMZ el honeypot Cowrie mediante los siguientes comandos

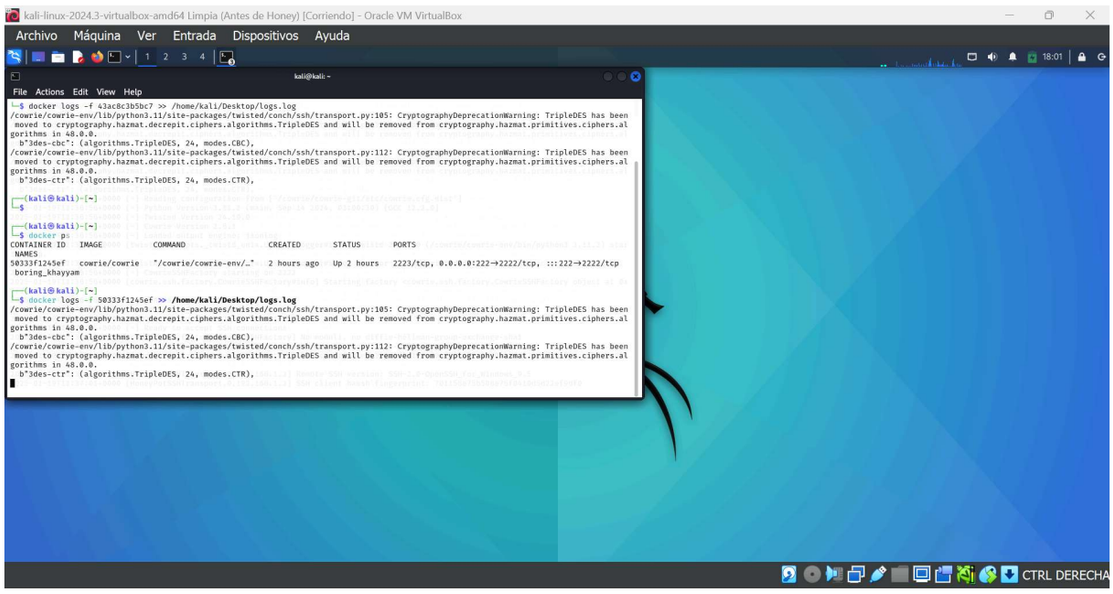
Docker run -p 222:2222 cowrie/cowrie



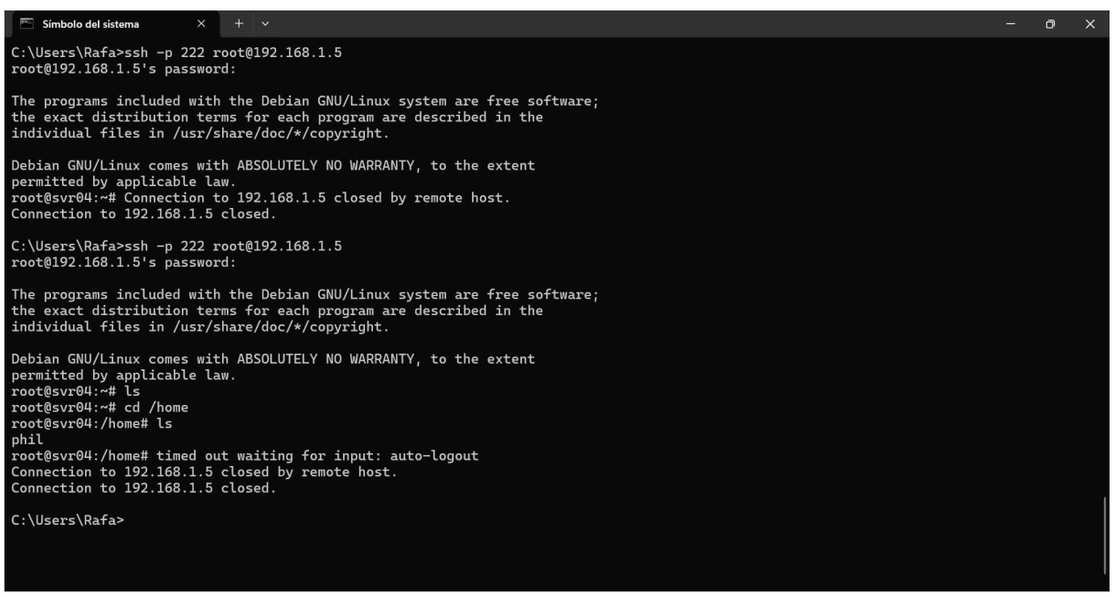
Como requisito de la práctica, es necesario extraer los logs que genera dicho honeypot a un archivo que se subirá más adelante a Elastic, para ello se ha usado el siguiente comando:

docker logs -f (id_contenedor_docker) >> /home/kali/desktop/logs.log

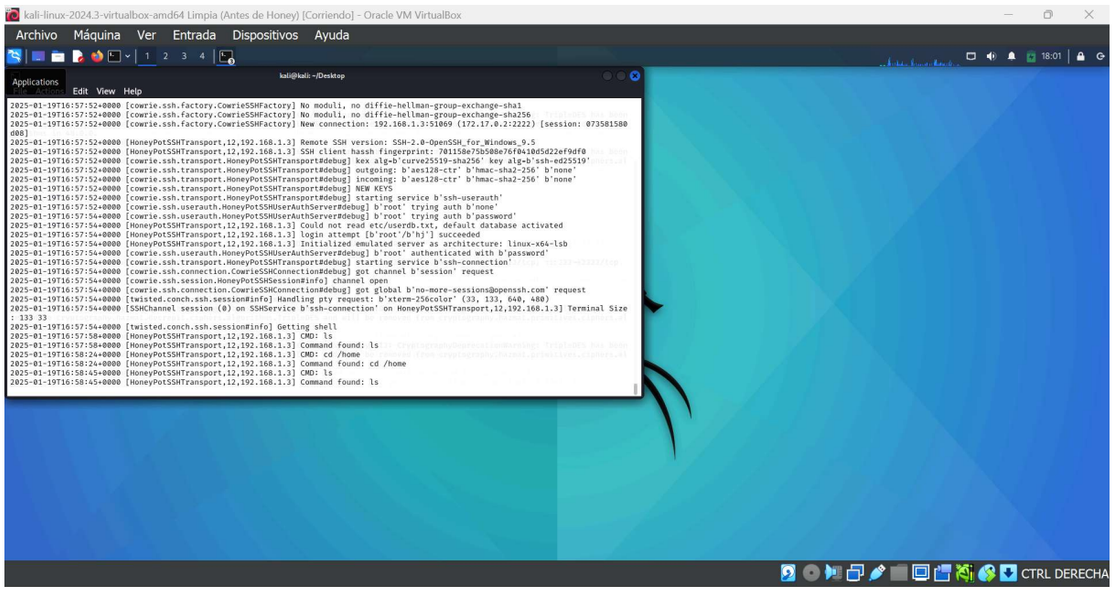
Con esto se consigue un archivo que se actualiza añadiendo nuevas líneas cada vez que se produce una conexión SSH desde WAN, registrándose los comandos introducidos.



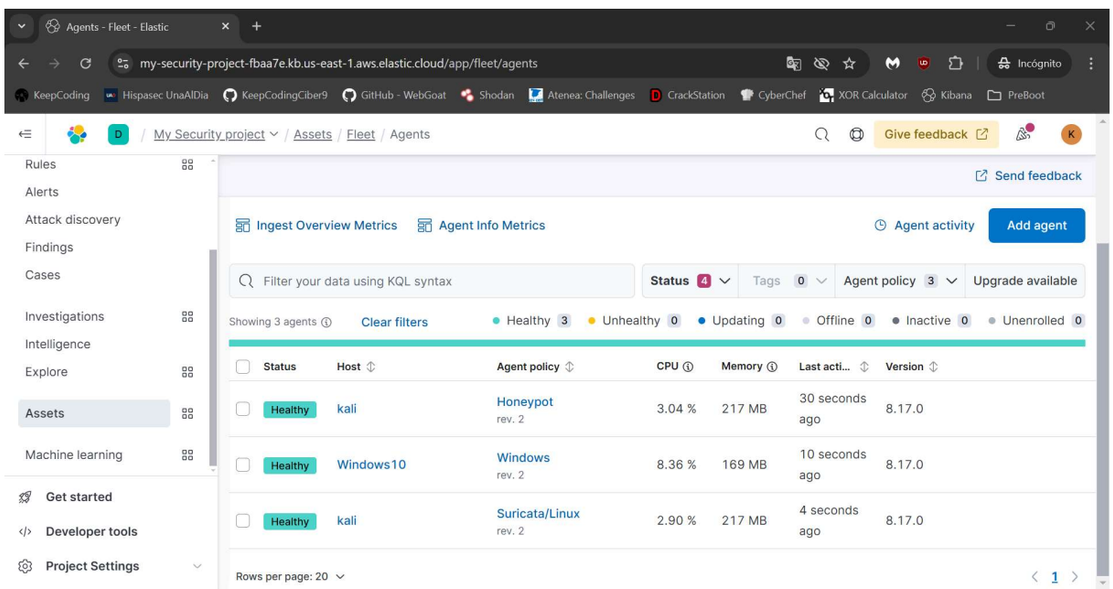
A continuación podemos ver como un SSH desde el equipo Host llega a la máquina alojada en la red DMZ a través de la red WAN



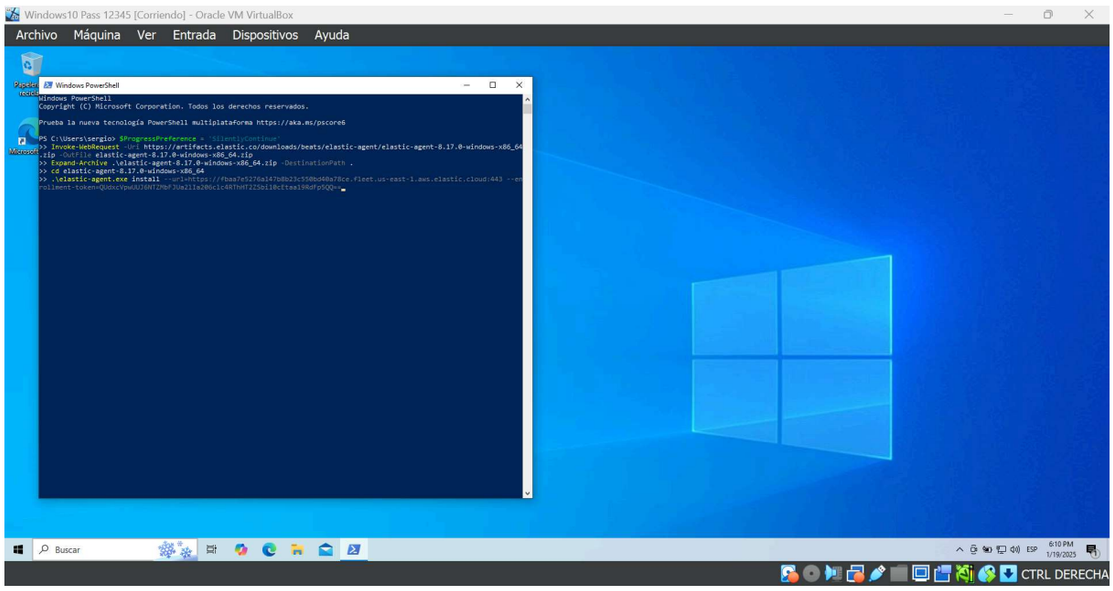
Como se puede apreciar con este comando CAT al archivo logs.log, los inputs de la conexión SSH se añaden a continuación de la última linea.

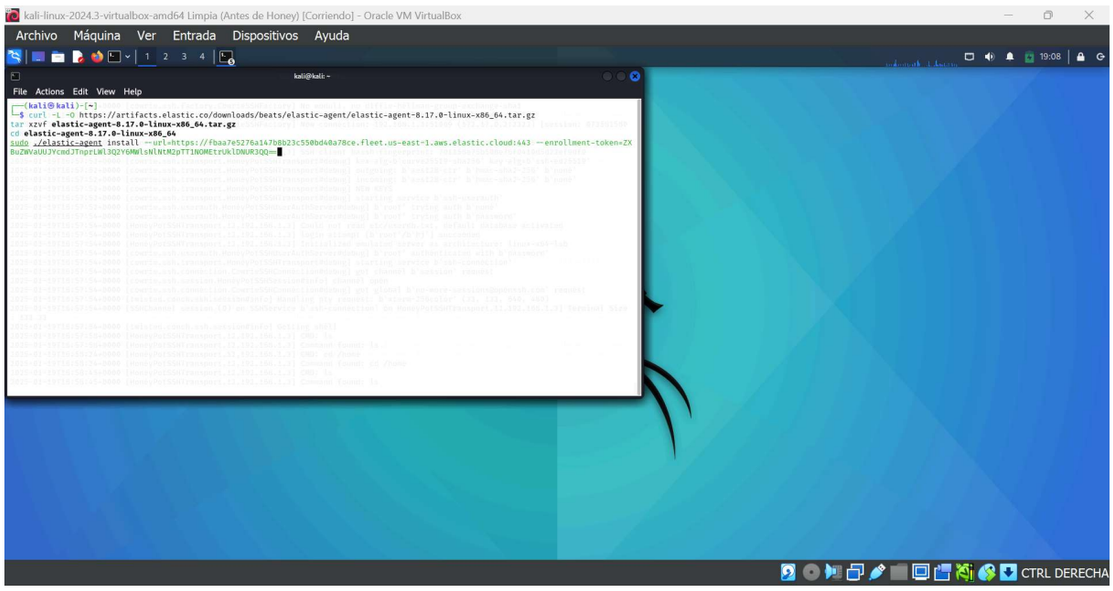


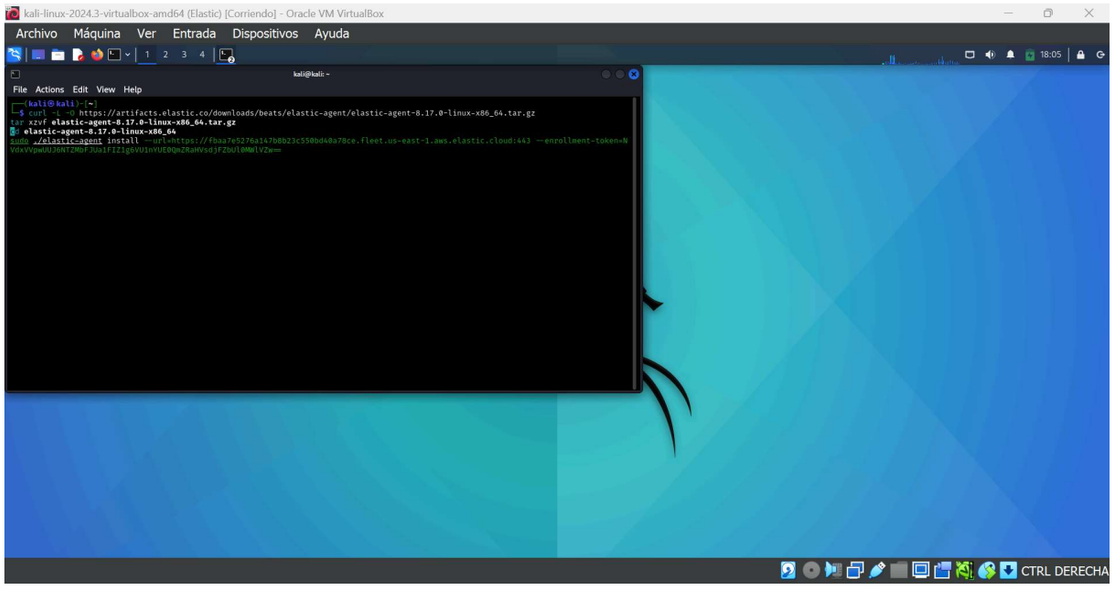
Una vez que hemos llegado a este punto se puede proceder a crear una cuenta en la web de elastic y configurar las máquinas, en está imagen se puede apreciar las 3 máquinas funcionando tras la instalación de los respectivos agentes en las terminales de cada una



A continuación se muestra la instalación de cada uno de ellos en su máquina correspondiente

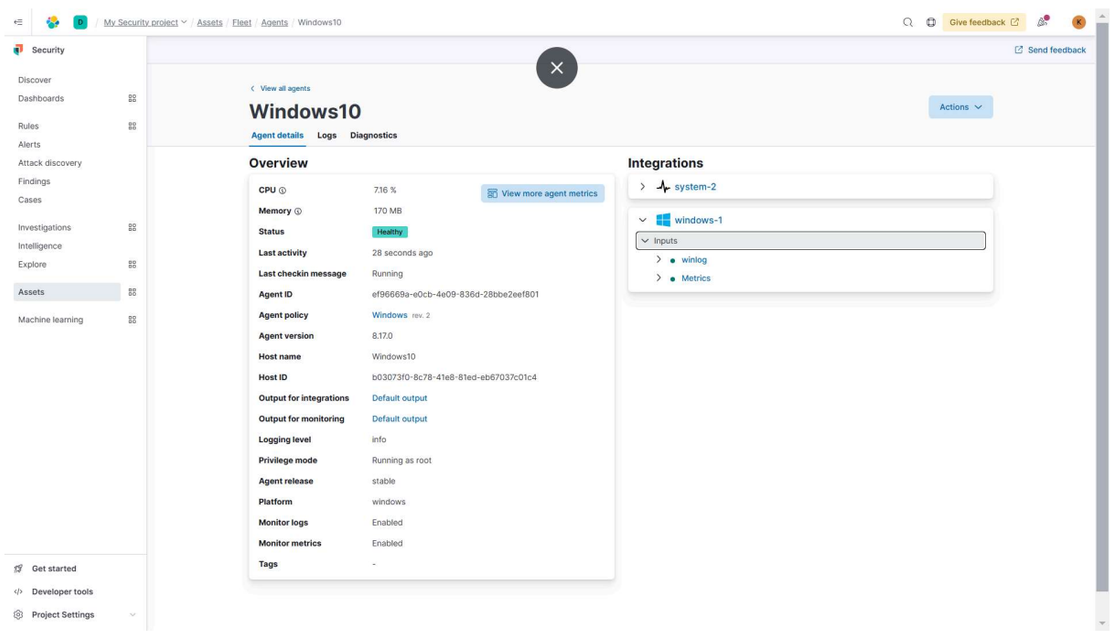




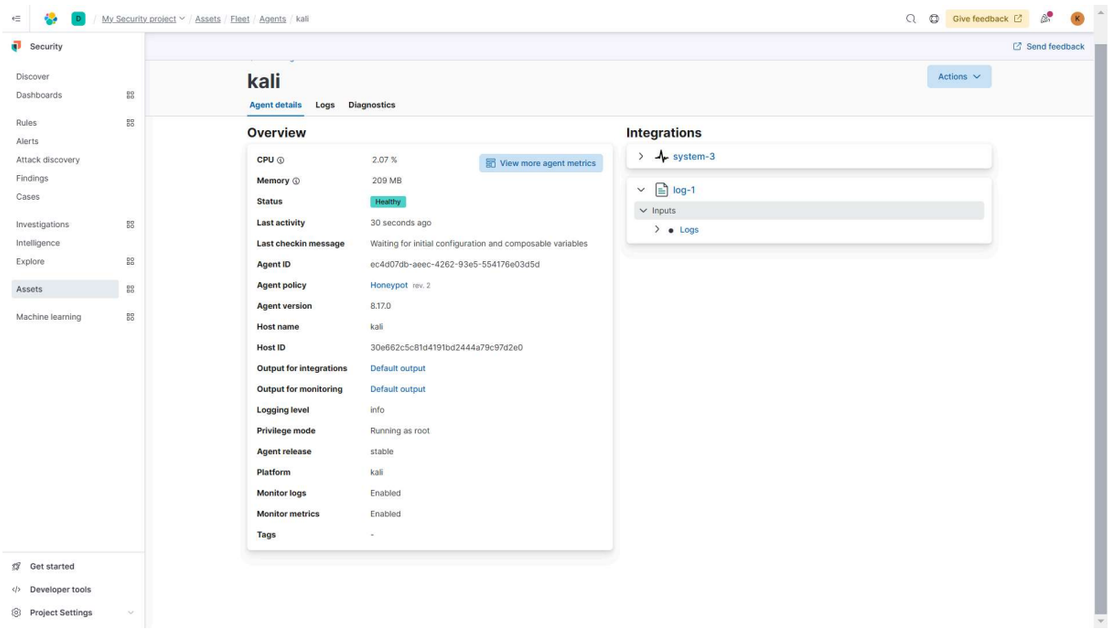


Una vez hechos estos pasos se pueden consultar los logs de cada uno, se ha procedido a filtrar por el campo Agent ID de cada uno

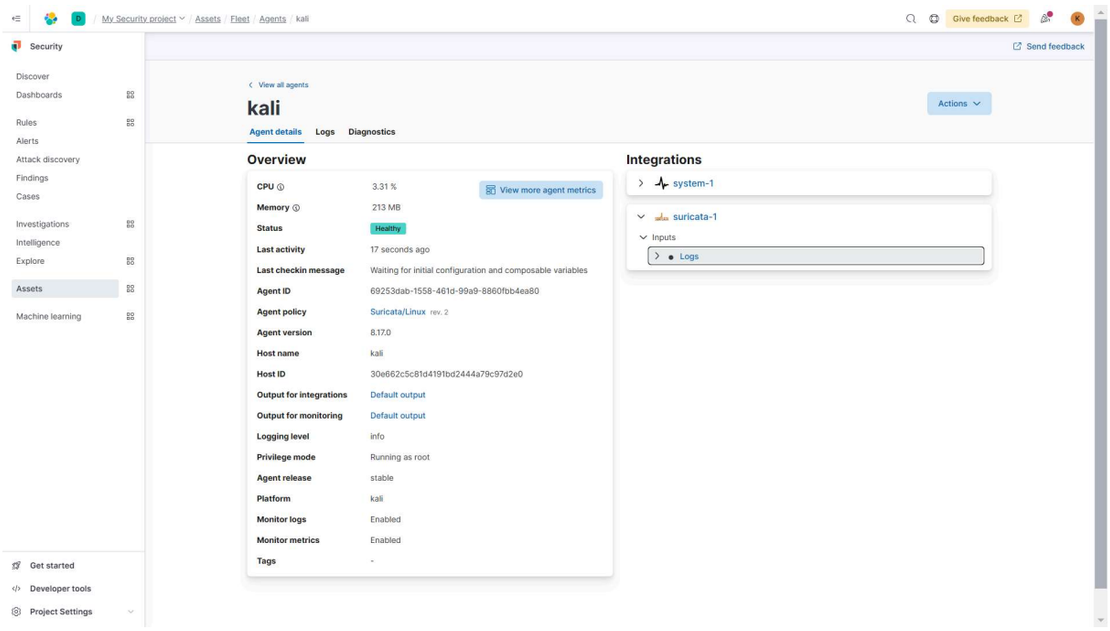
Máquina Windows



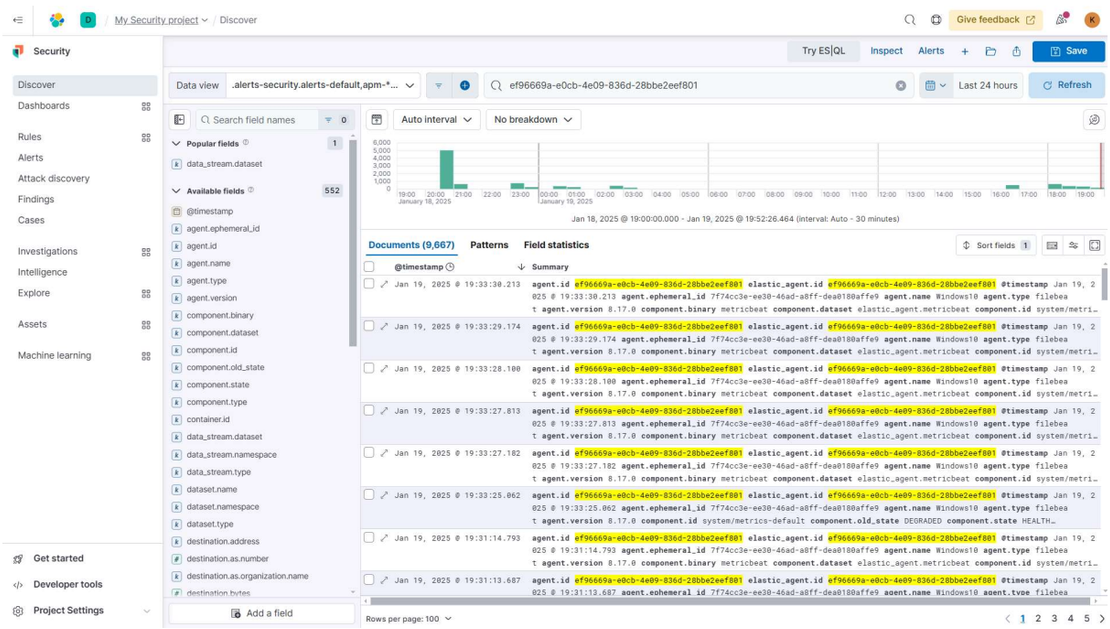
Máquina Kali con Honeypot



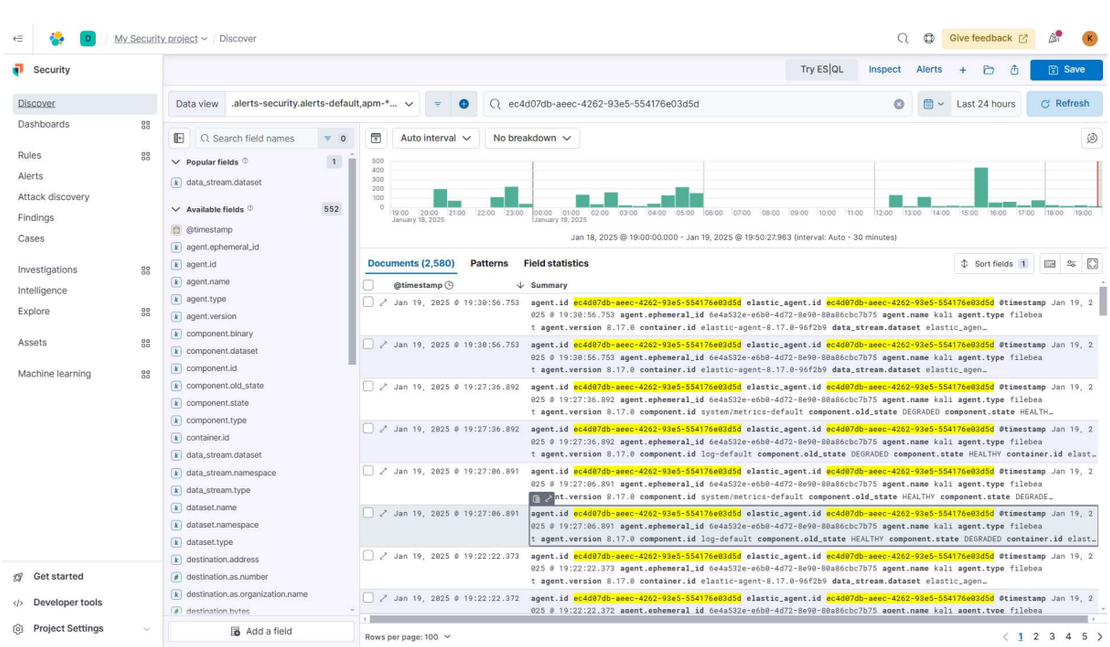
Máquina Kali con Suricata



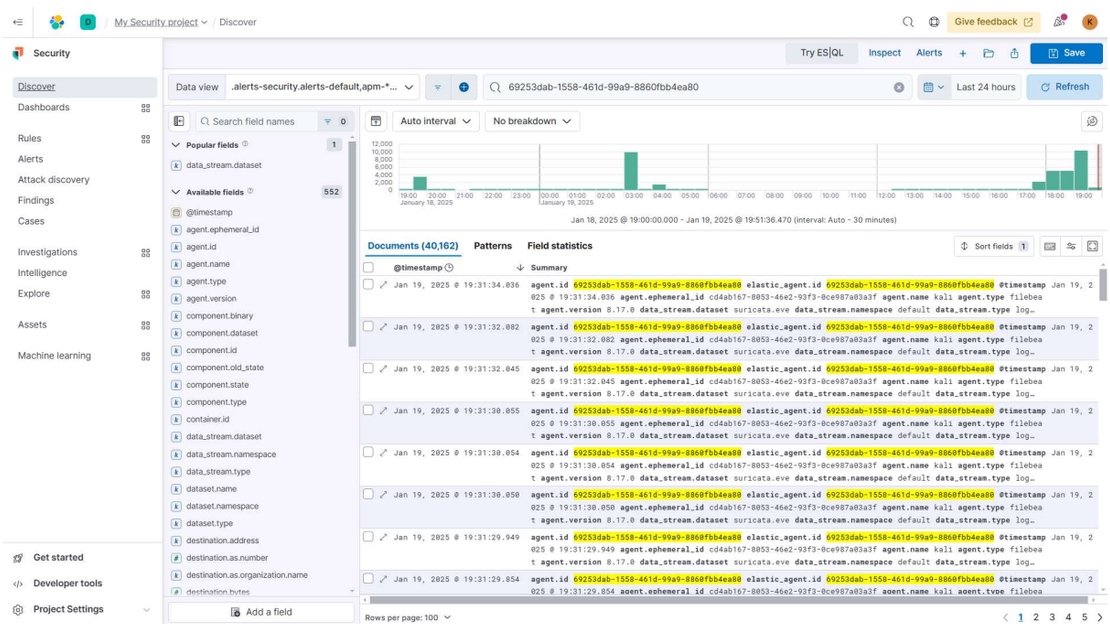
Logs generados por máquina la Windows en las últimas 24 horas:



Logs generados por máquina Kali con honeypot en las últimas 24 horas:



Logs generados por máquina Kali con Suricata en las últimas 24 horas:



Con esto se da por concluida la memoria, se adjuntará en github archivos .txt con copia de los datos de una entrada del log de cada máquina.