Memoria Ciberseguridad

Evaluación BlueTeam

Nombre del Auditor: Kacper Mariusz Koper Mielczarek

Fecha: 20/02/2025

Índice

PfSense

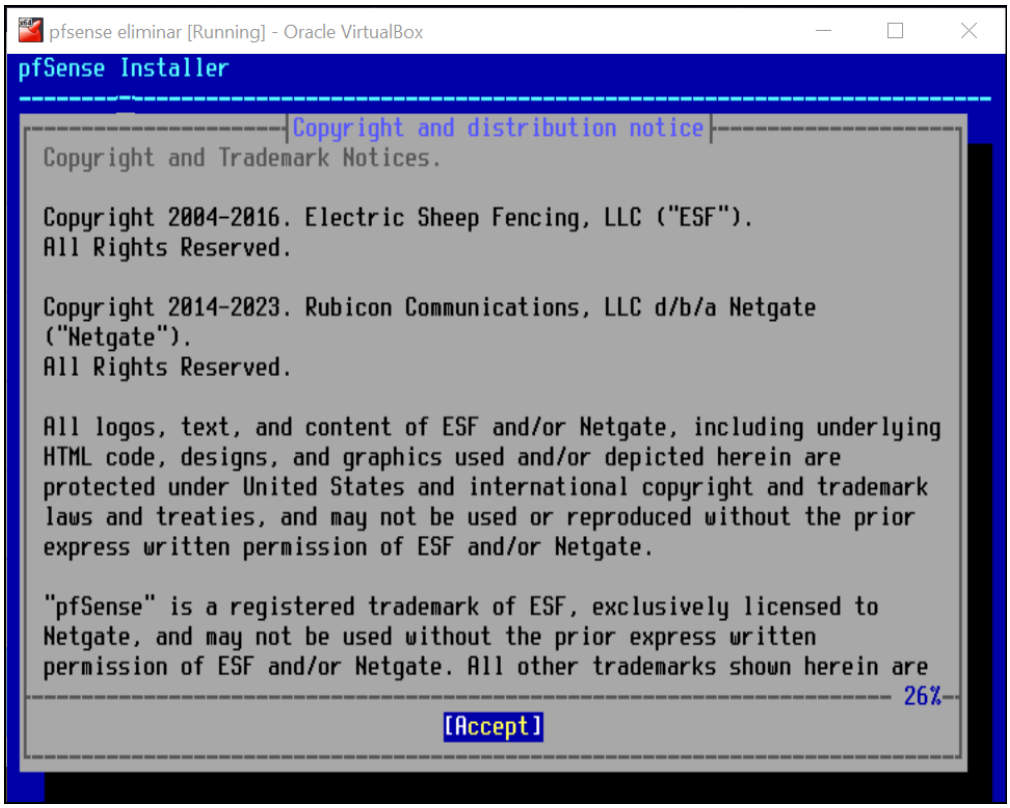
- SO: free BSD
- Memoria: 1024MB
- CPUs: 2
- Almacenamiento: 16GB

Instalación PFsense

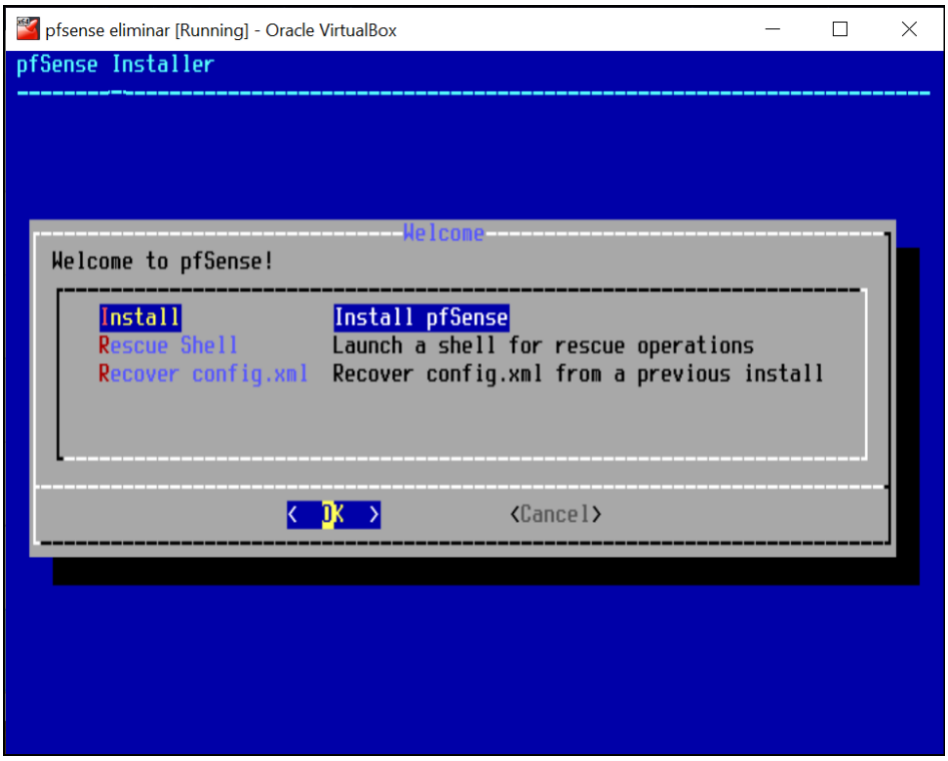
En esta primera etapa de la práctica, se realizó la instalación y configuración inicial de **Pfsense**, un sistema UTM (Unified Threat Management) utilizado para gestionar y controlar el tráfico de red de los equipos conectados. Inicialmente, se procedió con la instalación del sistema y la configuración básica, asignando las interfaces correspondientes para las redes internas (**LAN**) y externas (**WAN**). Este proceso permitió establecer los parámetros iniciales para obtener conexión en red.

Finalmente, se verificó el correcto funcionamiento de la máquina, comprobando que las interfaces asignadas operan según lo esperado. Se obtuvo con éxito el dato de las direcciones asignadas a la **WAN** y la **LAN**, confirmando que el sistema está preparado para proceder a gestionar las diferentes reglas del Pfsense.

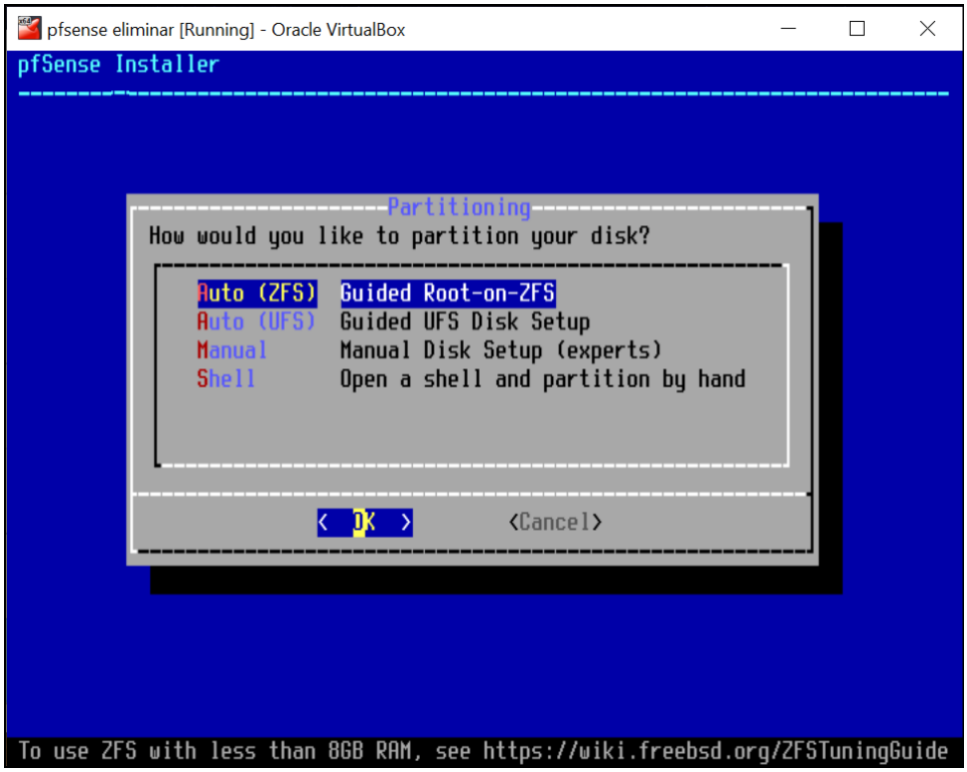
1. Accept copyright.



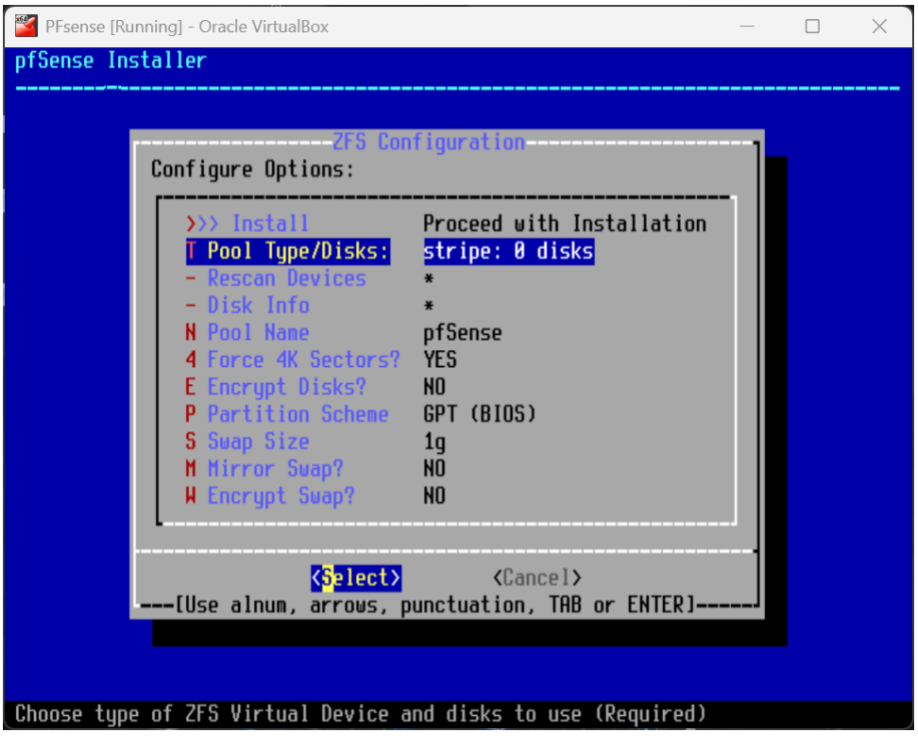
2. Install.



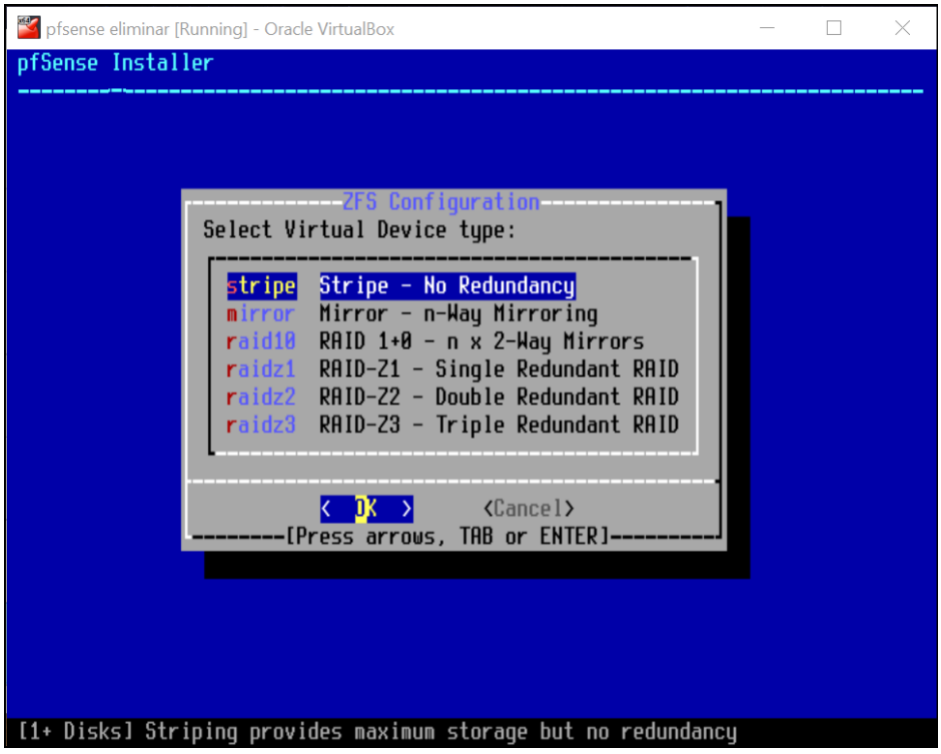
3. Guided Root-on-ZFS.



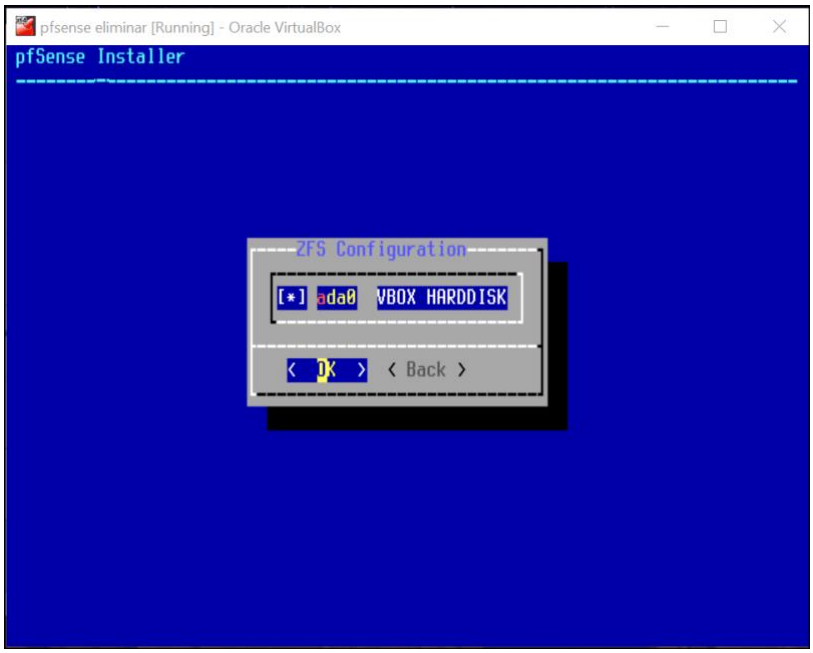
4. Pool Type/Disk.



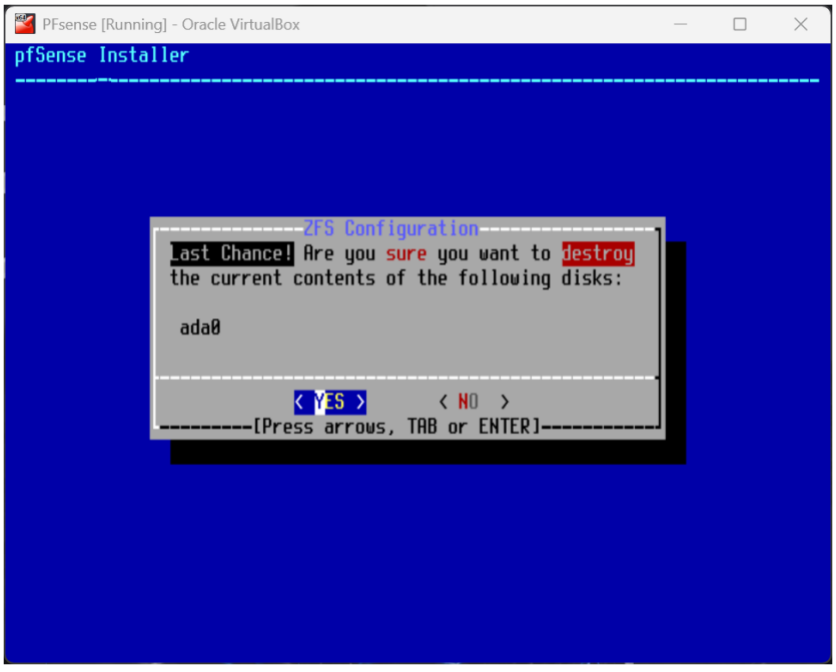
5. Stripe Stripe – No Redundancy.



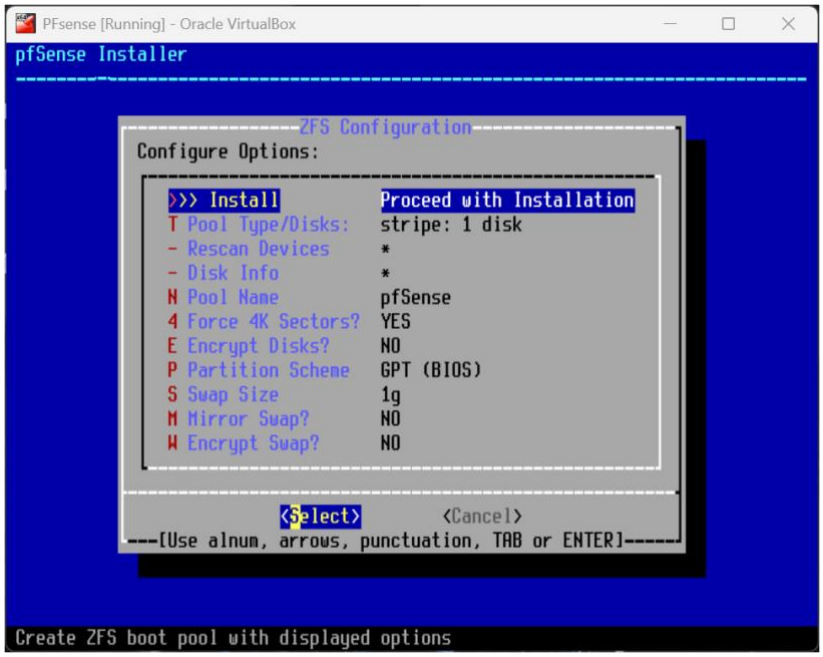
6. ada0 VBOX HARDDISK.



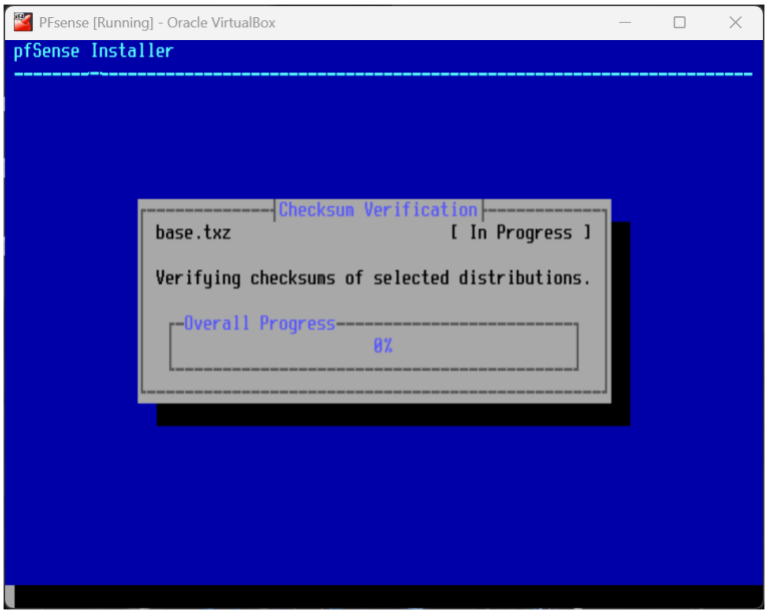
7. Destroy.



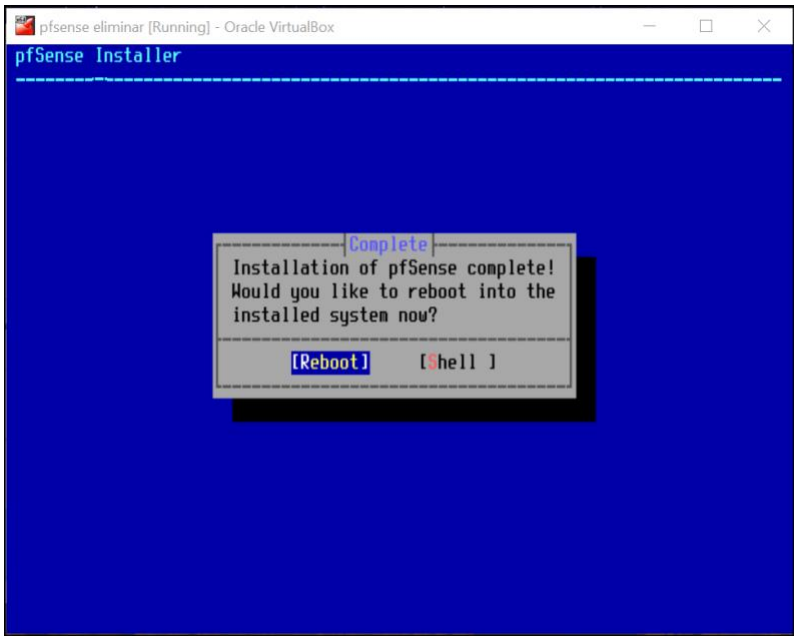
8. Proceed with installation.



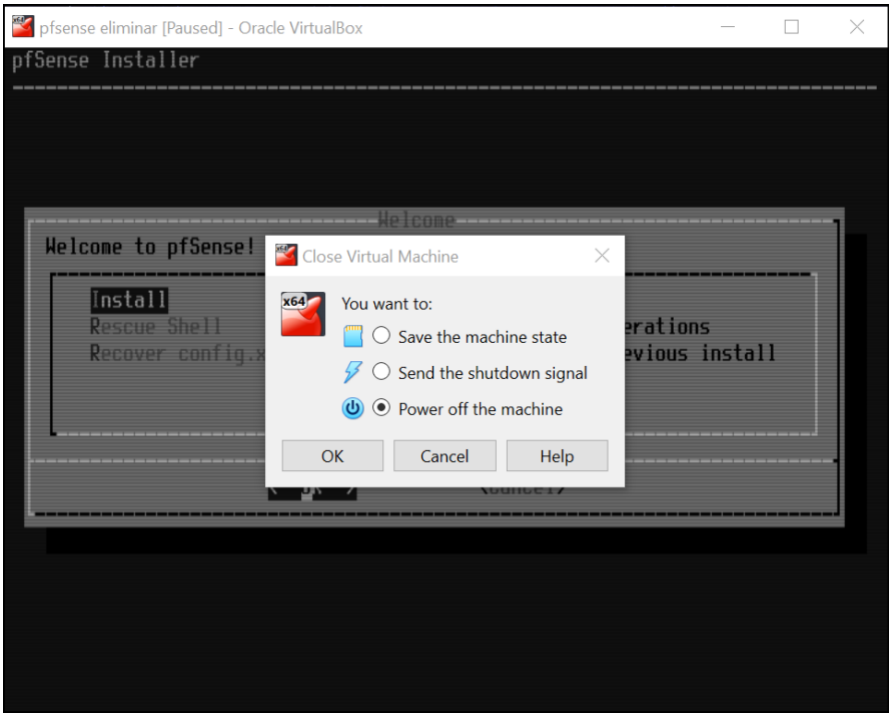
9. Comienza la instalación.



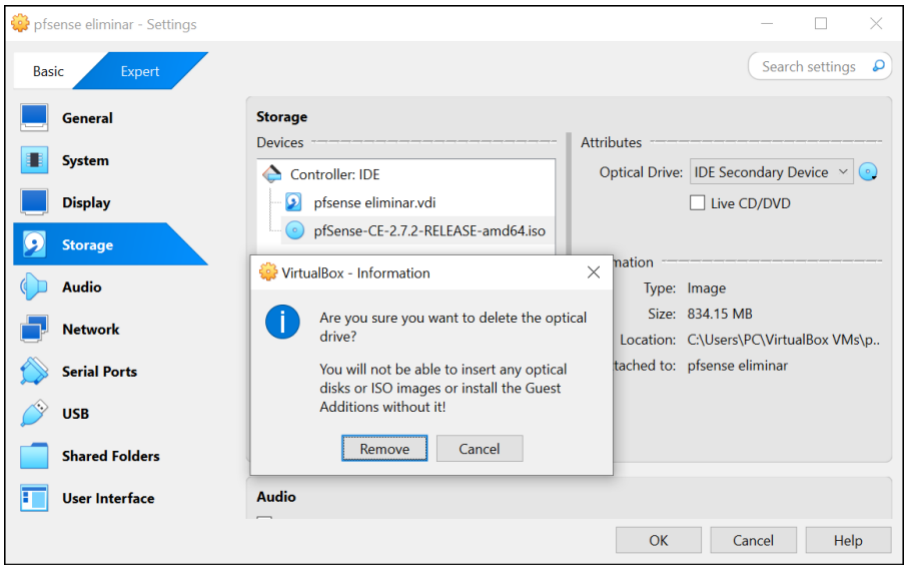
10. Reboot.



11. Apagamos la máquina.

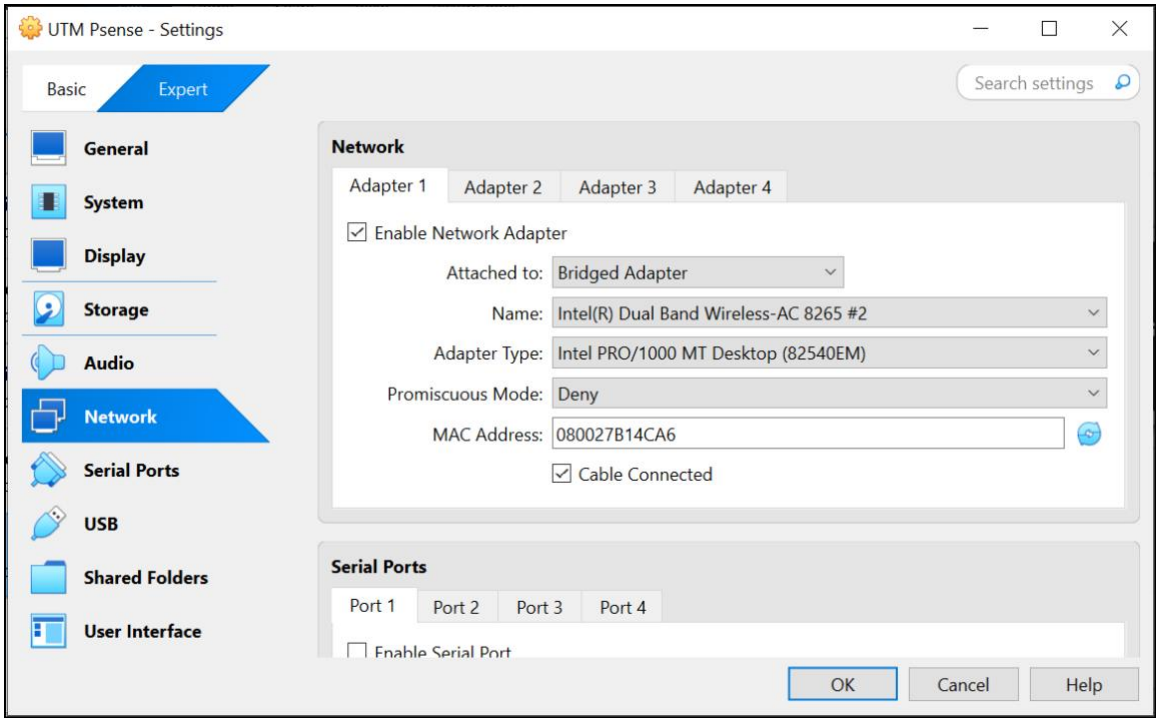


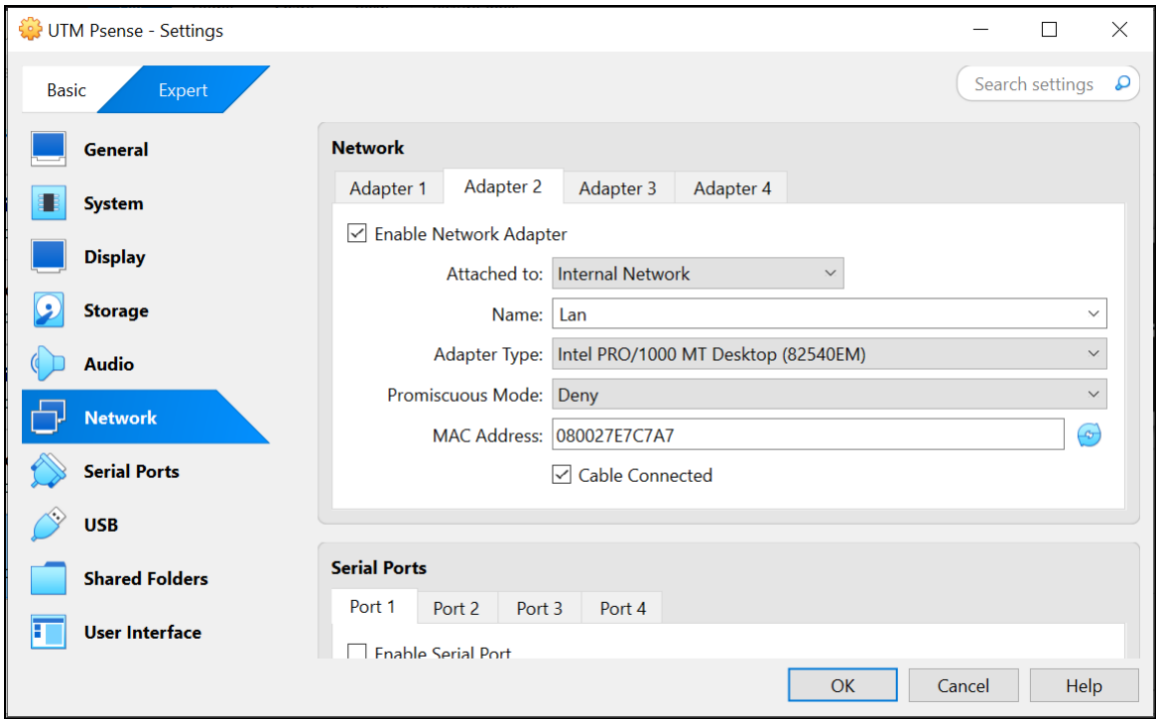
12. Eliminamos el disco de instalación.

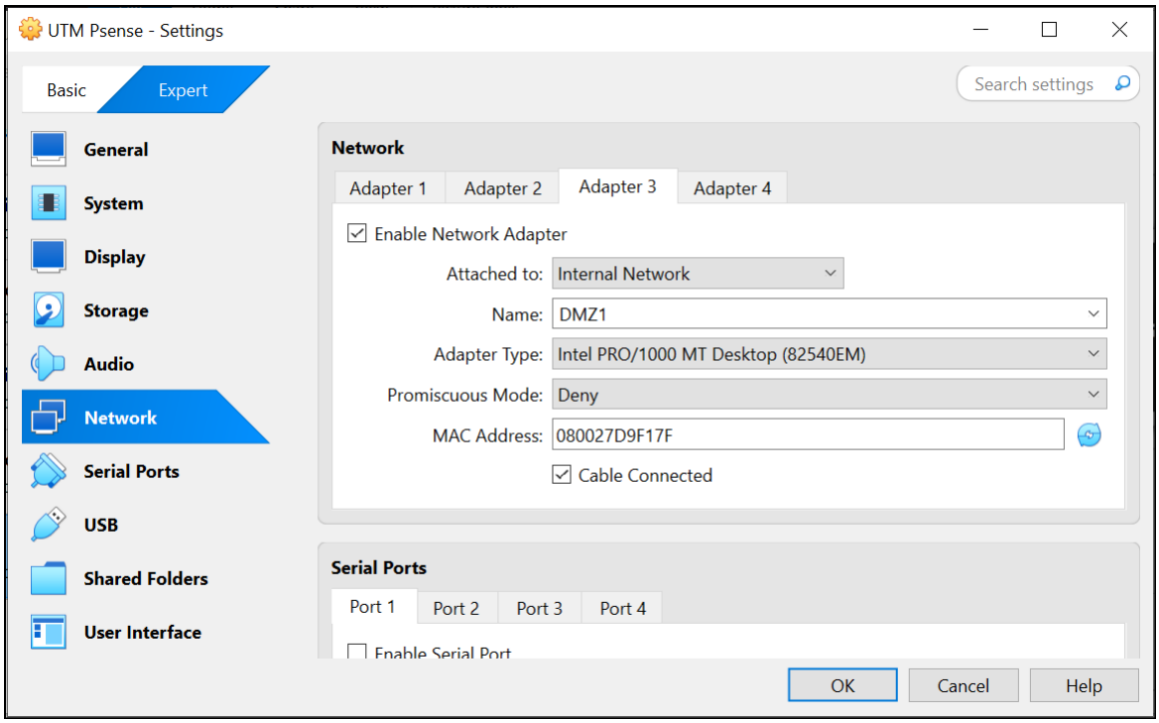


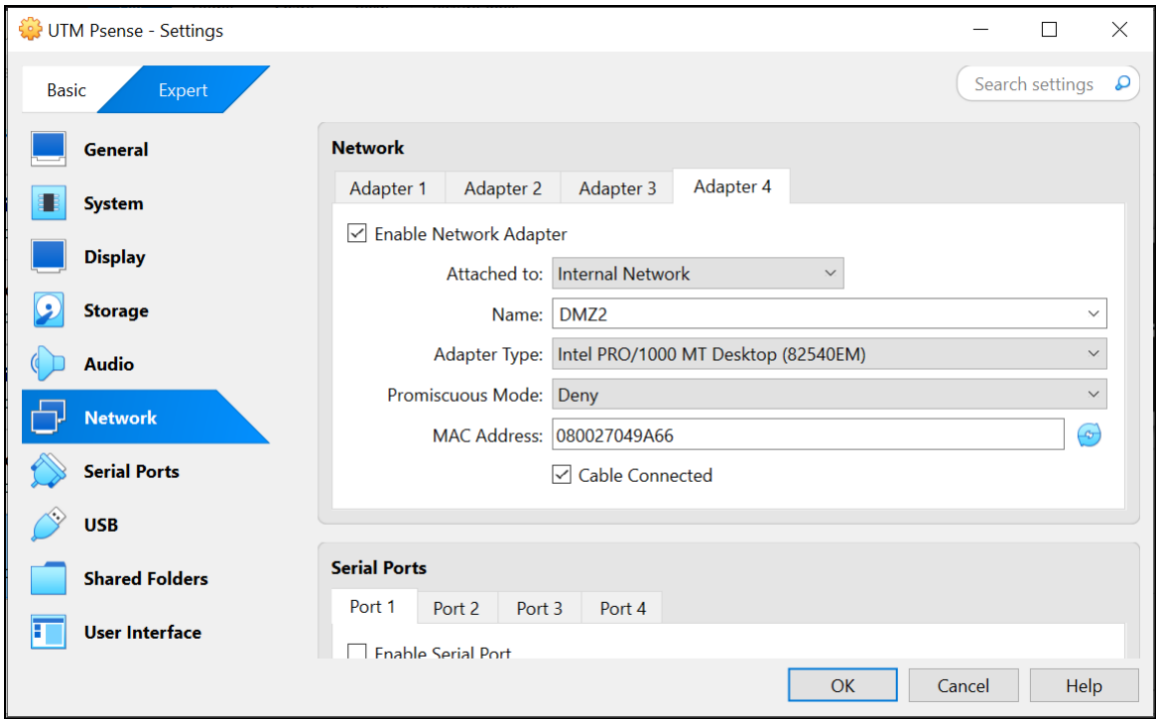
Creación de las redes en VirtualBox

13. Añadimos las redes al UTM.

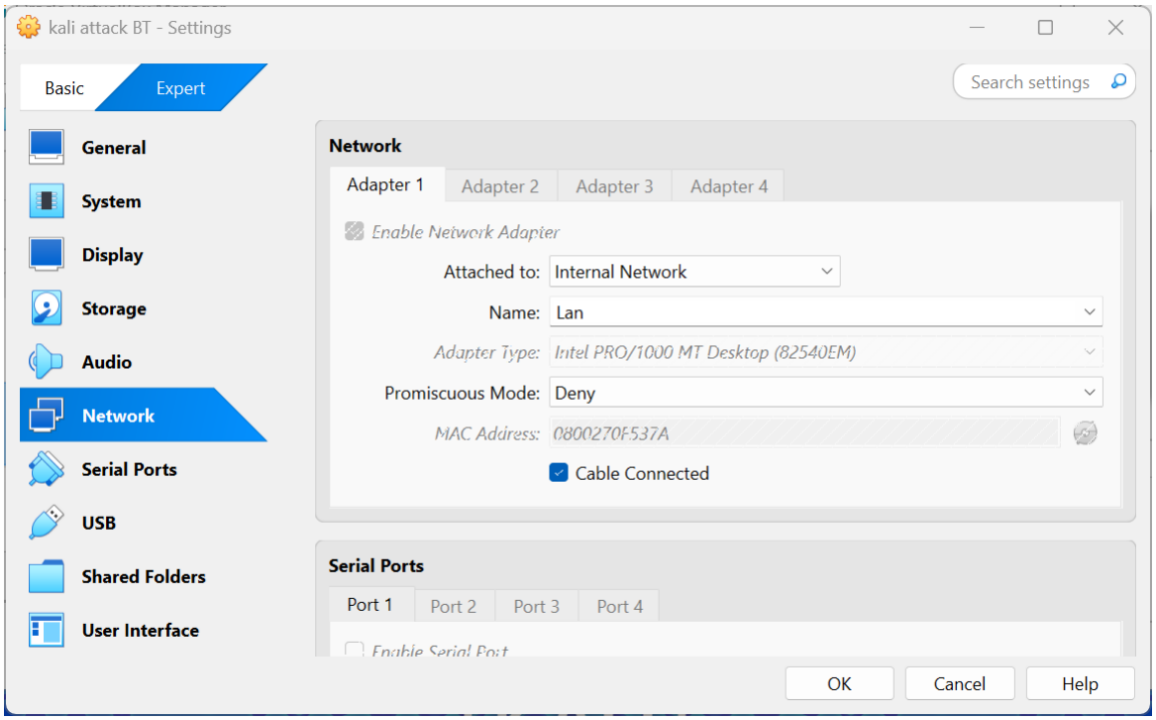



UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
Lan
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Deny
MAC Address:
080027E7C7A7
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help


UTM Psense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
DMZ1
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Deny
MAC Address:
080027D9F17F
Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help



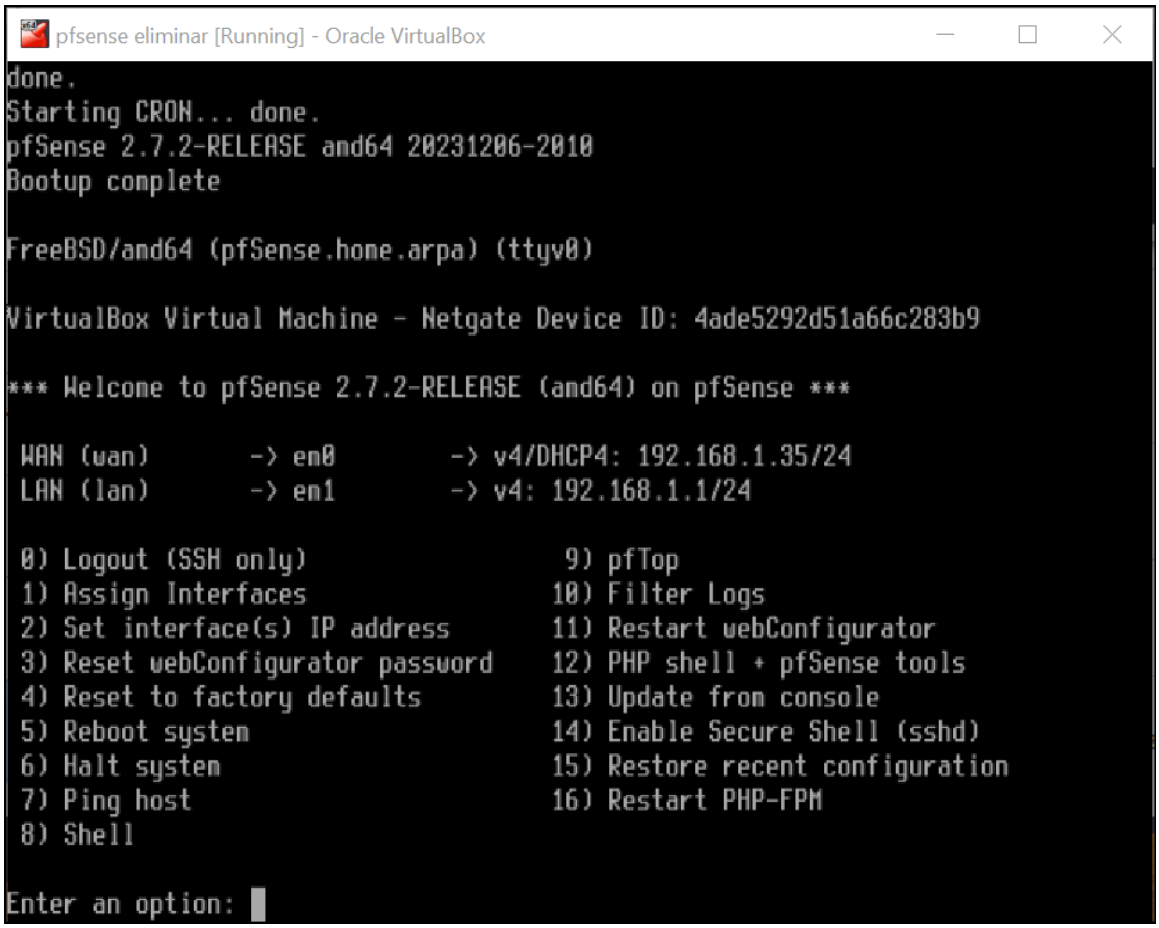
14. Añadimos la máquina Kali a la red interna.



Configuración PfSense

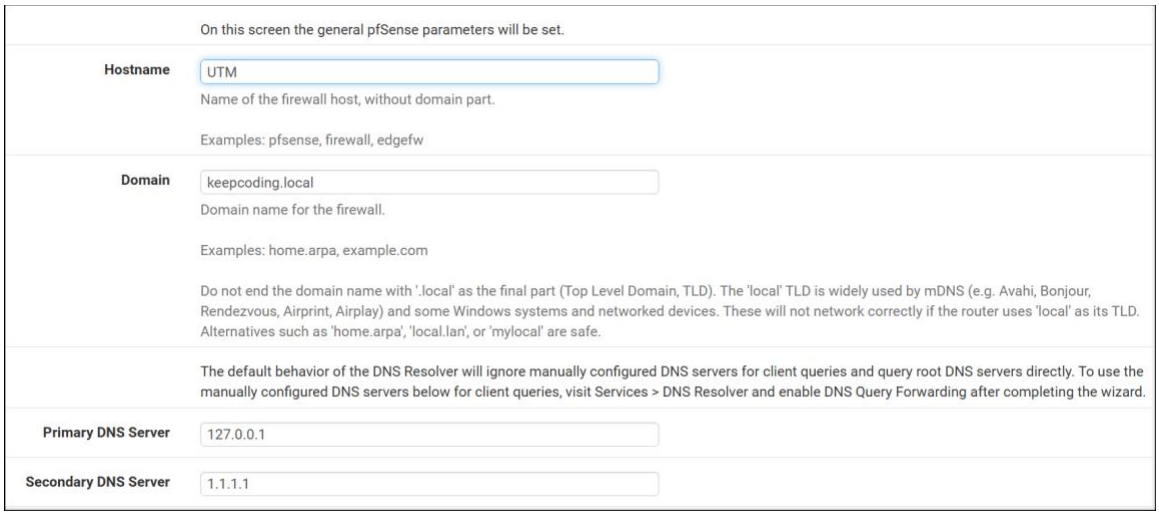
Pasos iniciales

15. Iniciamos PfSense.

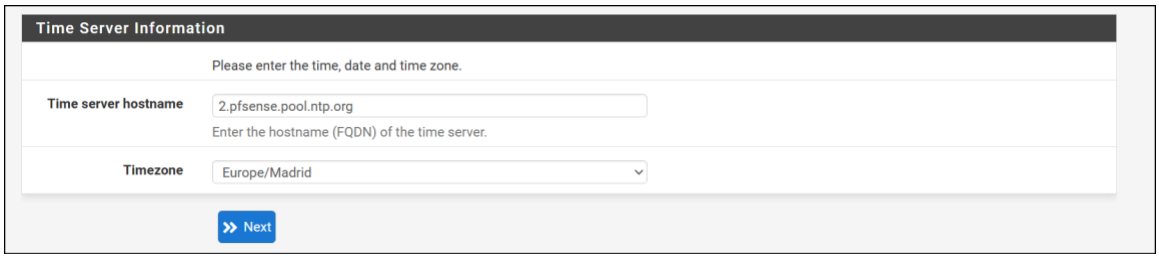


16. Entramos en la máquina UTM.
    En esta etapa de la práctica, se inició la máquina virtual con Kali Linux y se estableció conexión con Pfsense a través del navegador. Durante este proceso, se llevó a cabo la configuración inicial del sistema.
    a. 192.168.1.1
    b. User: Admin
    c. Pass: pfsense

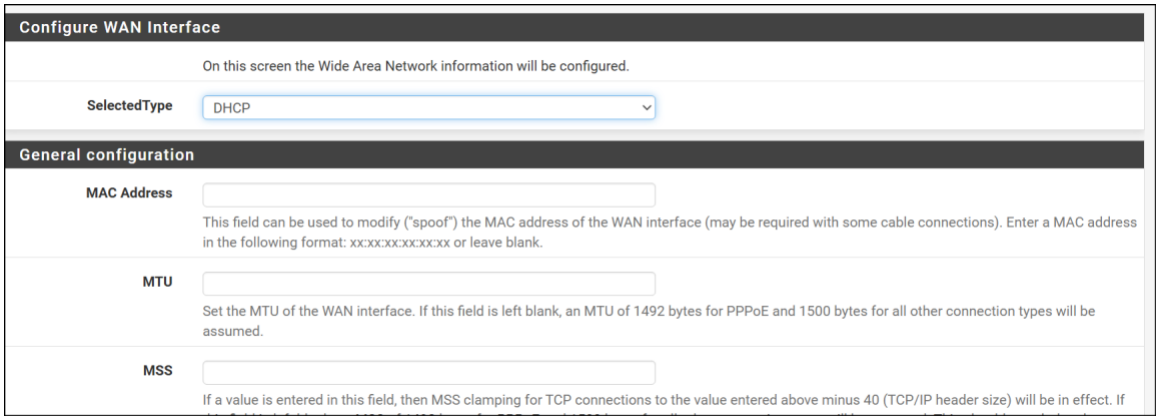
17. En el System>setup wizzard rellenamos la configuración:
    a. Hostname: UTM
    b. Domain: keepcoding.local
    c. Prymary DNS server 127.0.0.1
    d. Secondary DNS server 1.1.1.1
    e. NEXT

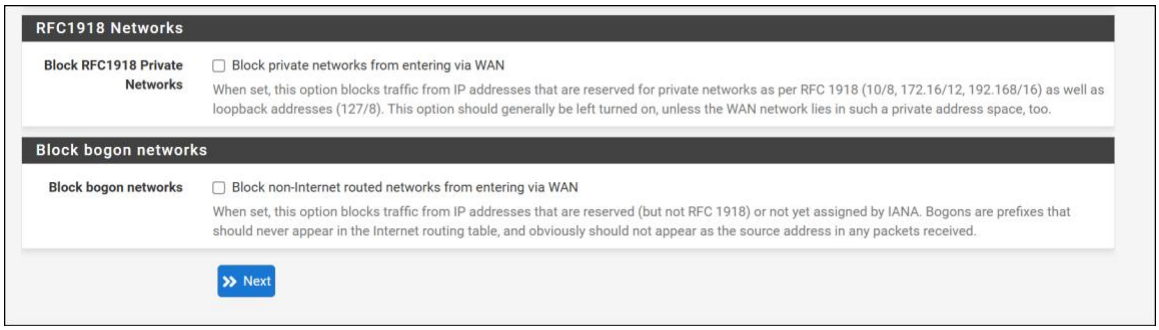


18. Time server information.
    a. Time server hostname: 2.pfsense.pool.ntp.org
    b. Timezone: Europe/Madrid
    c. NEXT

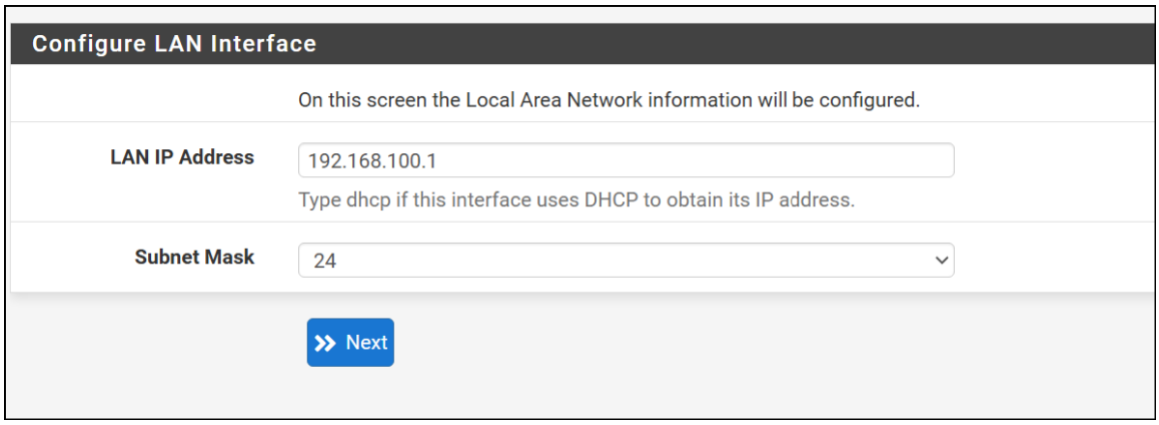


19. Dejamos todo en modo DHCP ya que va a ser el PfSense el que actúa como servidor DHCP y permitimos el uso de IPs privadas (RFC1918 y Bogons).

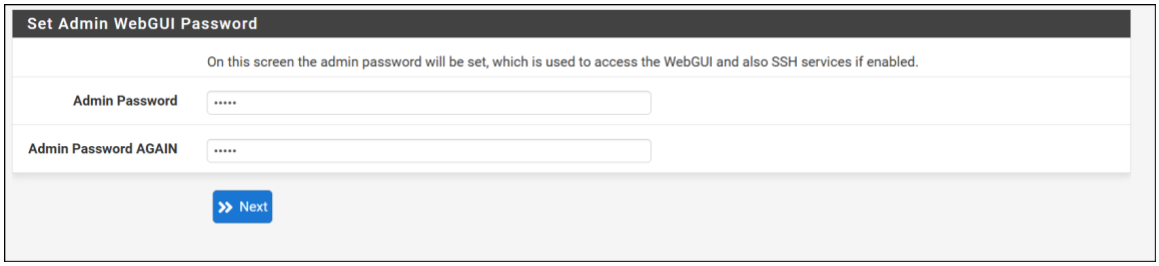




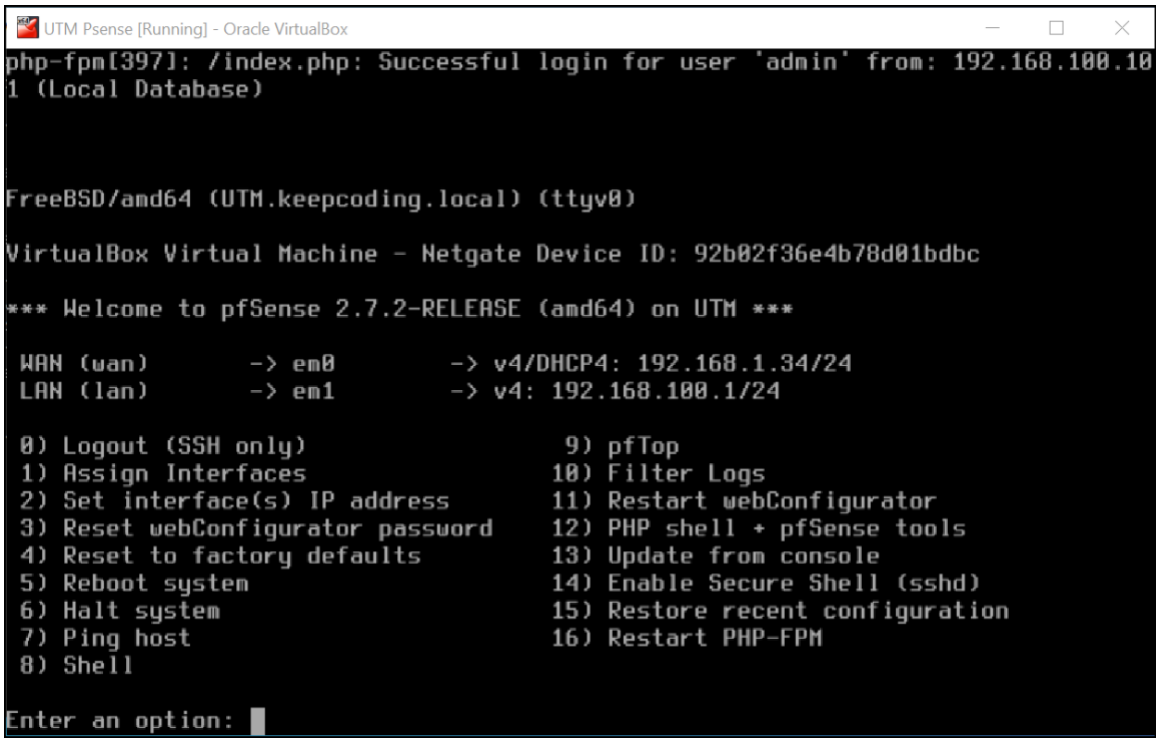
20. Cambiamos la IP de la LAN a 192.168.100.1
    a. LAN IP address: 192.168.100.1
    b. Subnet Mask: 24
    c. NEXT



21. Admin password: 123456
    Admin password again: 123456



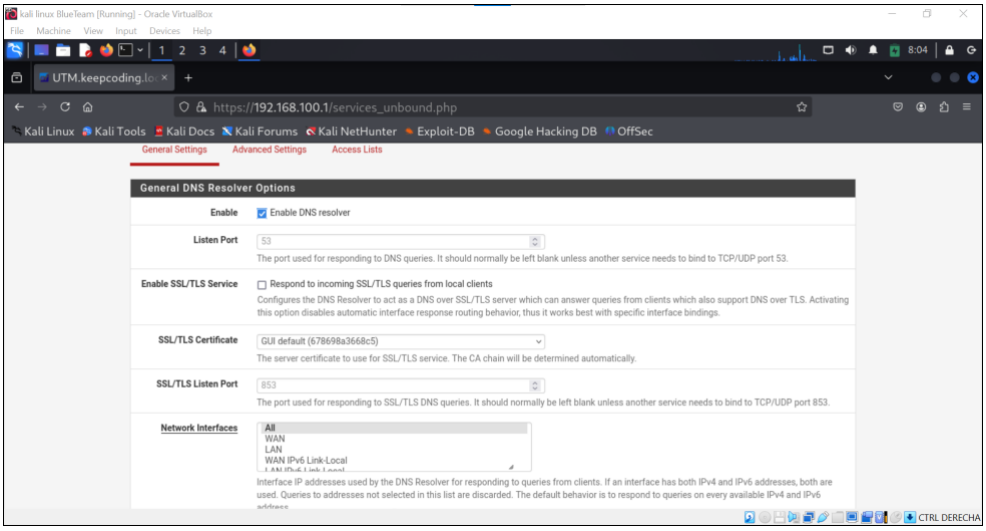
22. Resultado del PfSense tras pulsar enter

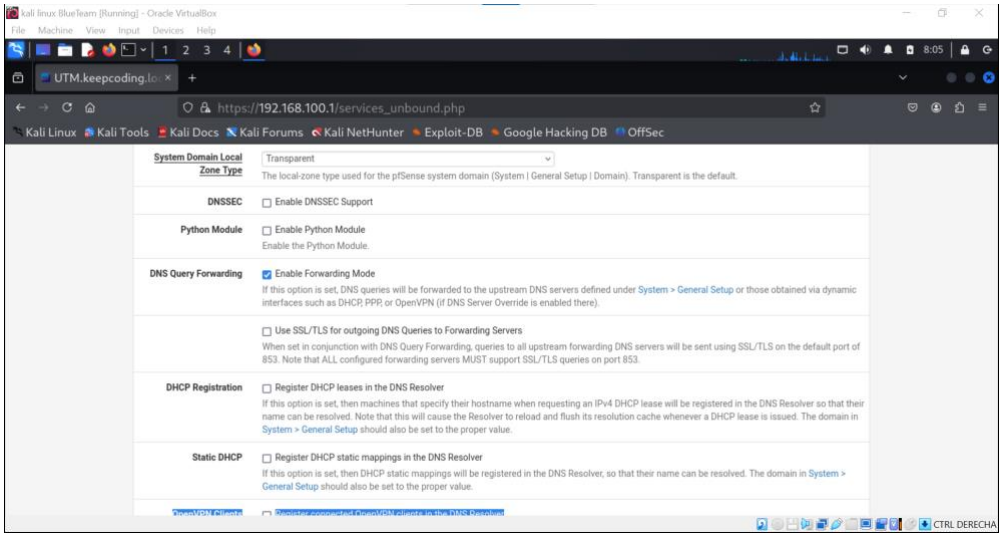


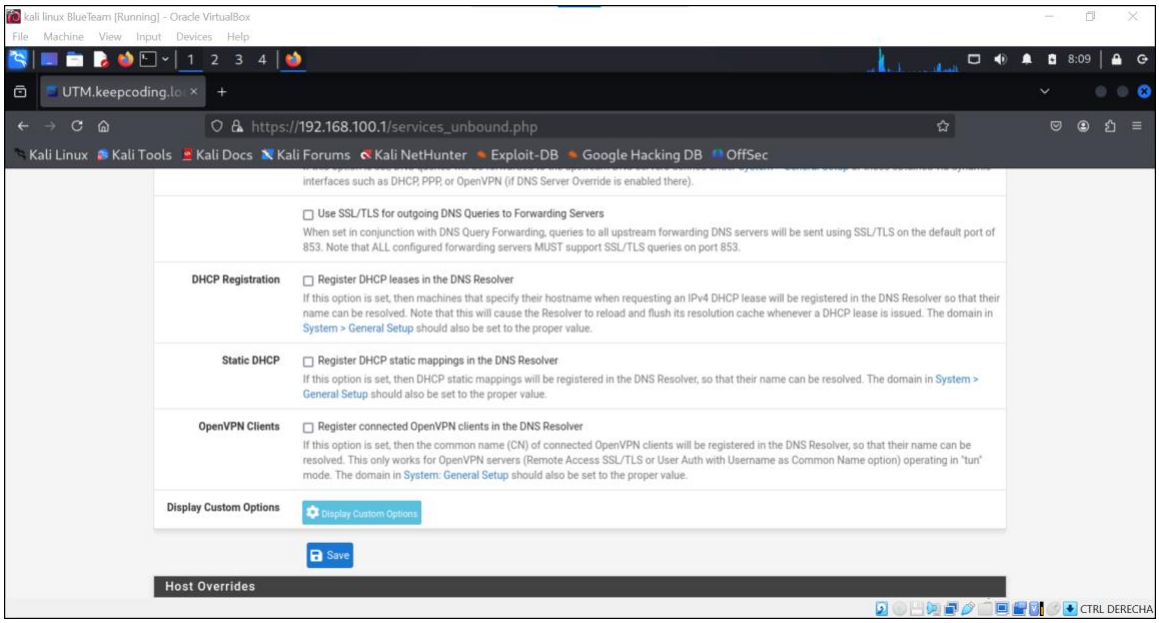
Vamos a configurar la resolución DNS

En este apartado, se procedió a asignar direcciones IP dinámicas a las redes LAN, DMZ y DMZ2, estableciendo rangos específicos de direcciones IP para cada una de ellas, con el objetivo de prevenir conflictos. Para ello, se habilitó el servicio DHCP en dichas redes, permitiendo la asignación automática de direcciones IP a los dispositivos conectados. Además, DHCP simplifica la administración de la red al proporcionar de manera centralizada otros parámetros esenciales, como la máscara de subred, la puerta de enlace predeterminada y los servidores DNS, asegurando así una configuración correcta y eficiente en todas las conexiones.

23. Services > DNS resolver.
    a. Comprobamos si está habilitado
    b. Quitamos el DNSSec
    c. Habilitamos el Forwarding mode

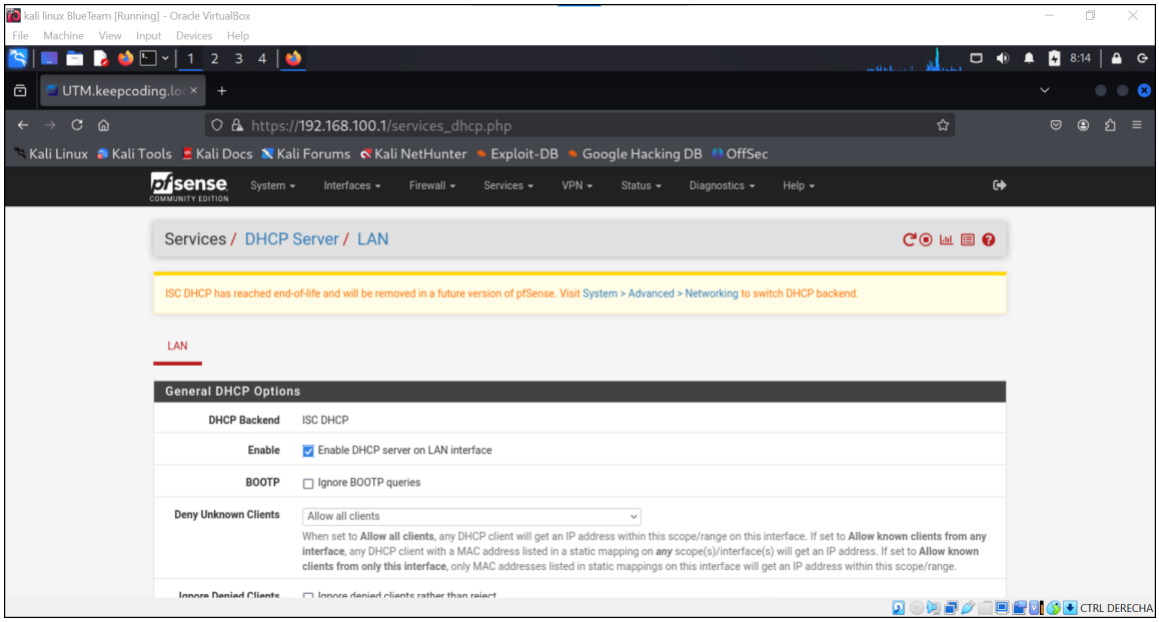


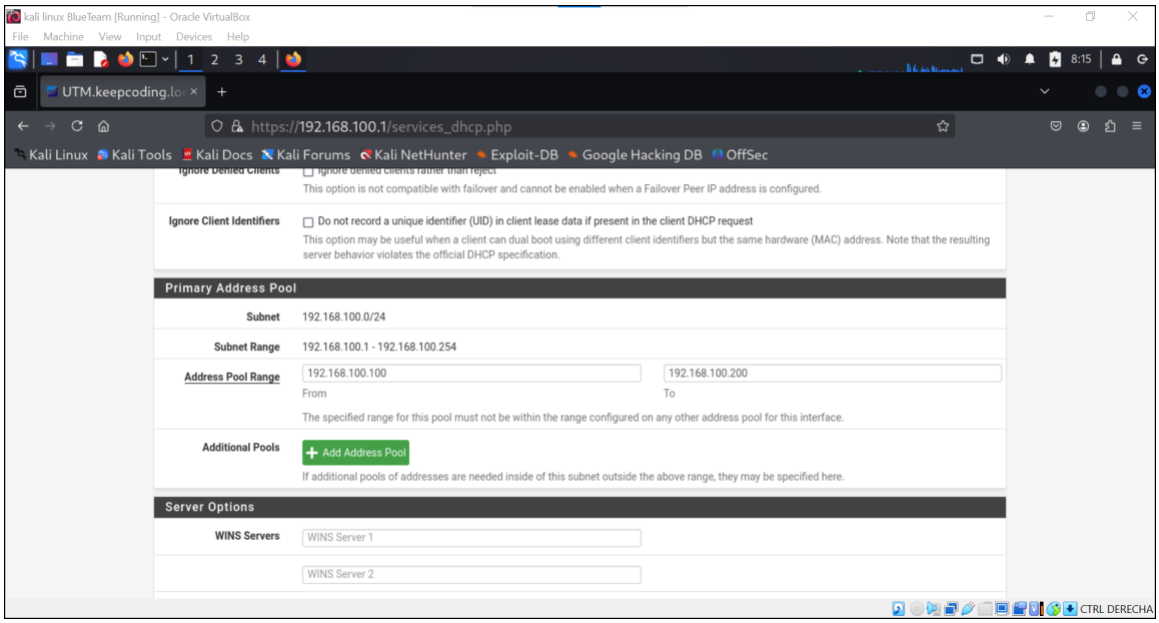




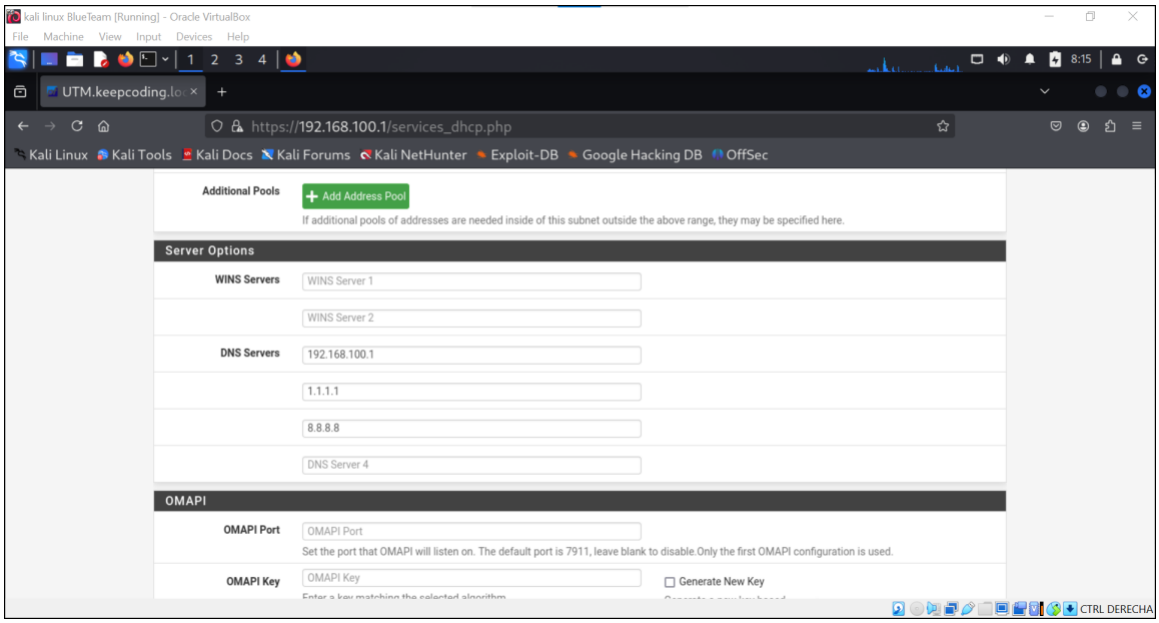
24. Configuración del DHCP server en la LAN.

    a. Modificamos el rango de direcciones de la LAN
        i. 192.168.100.100 to 192.168.100.200

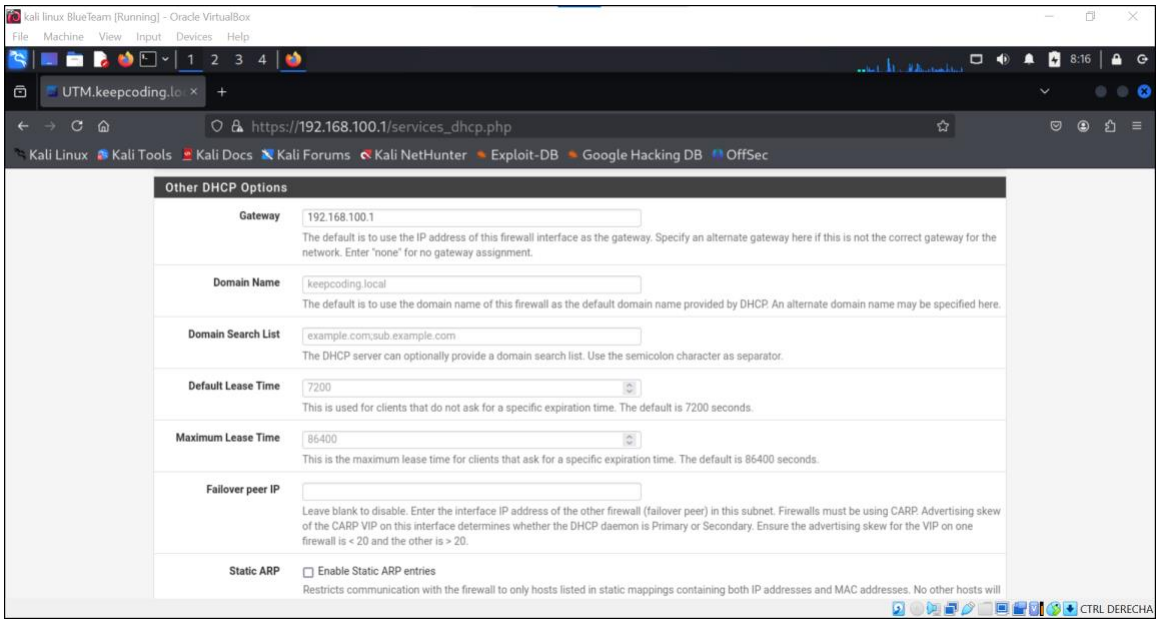


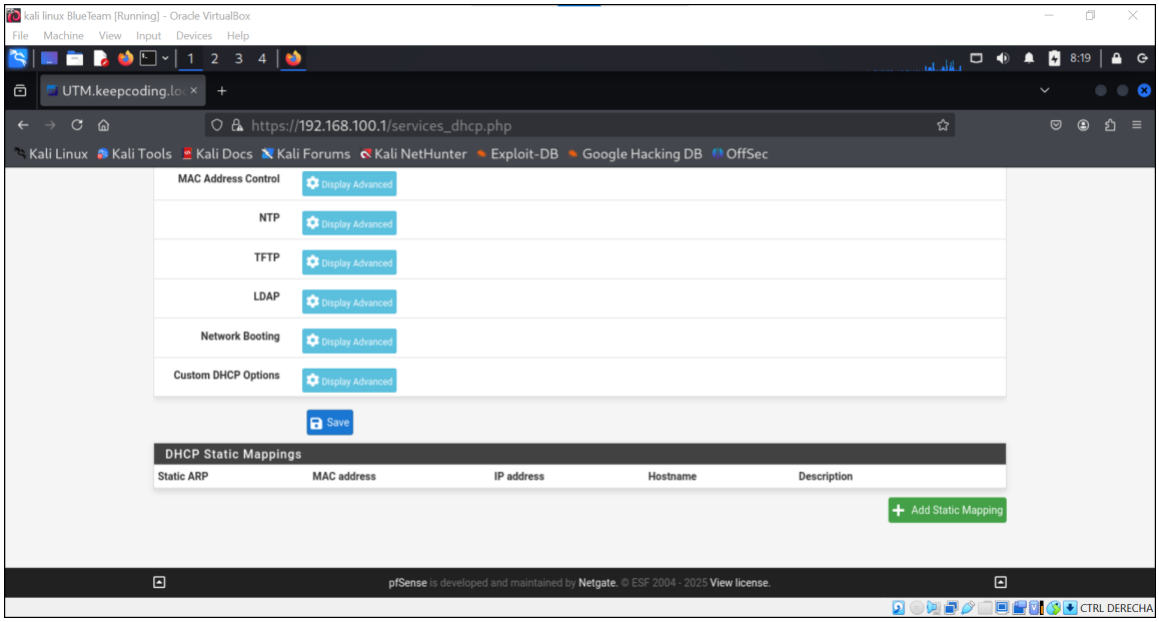


b. Modificamos los servidores DNS
   i. 192.168.100.1
   ii. 1.1.1.1
   iii. 8.8.8.8

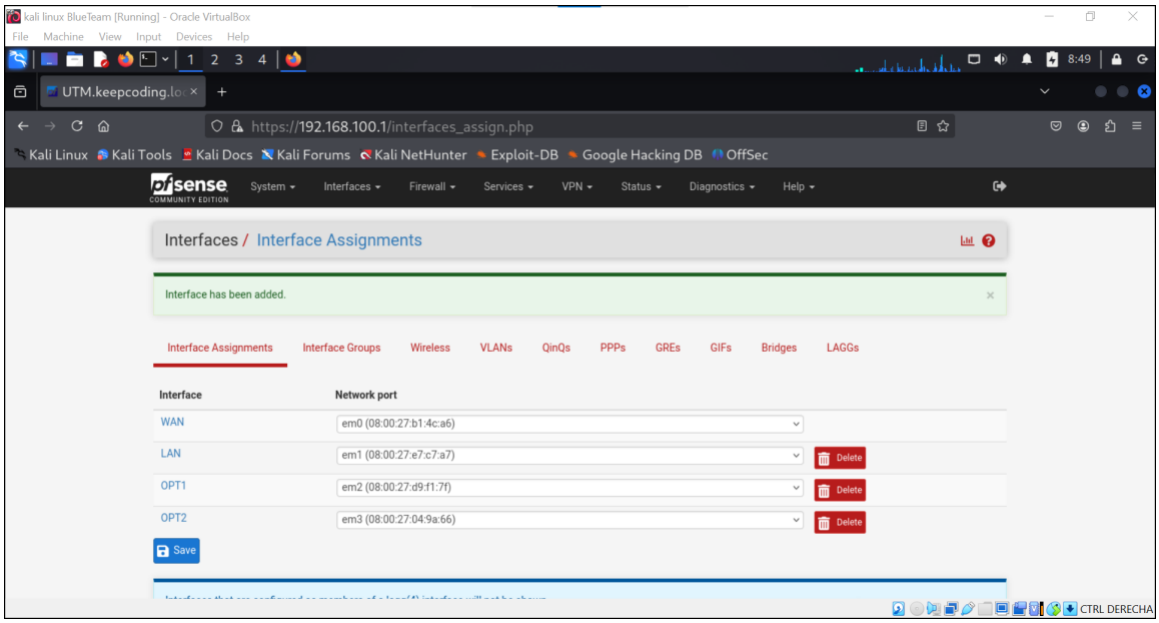


c. Modificamos la puerta de enlace/Gateway

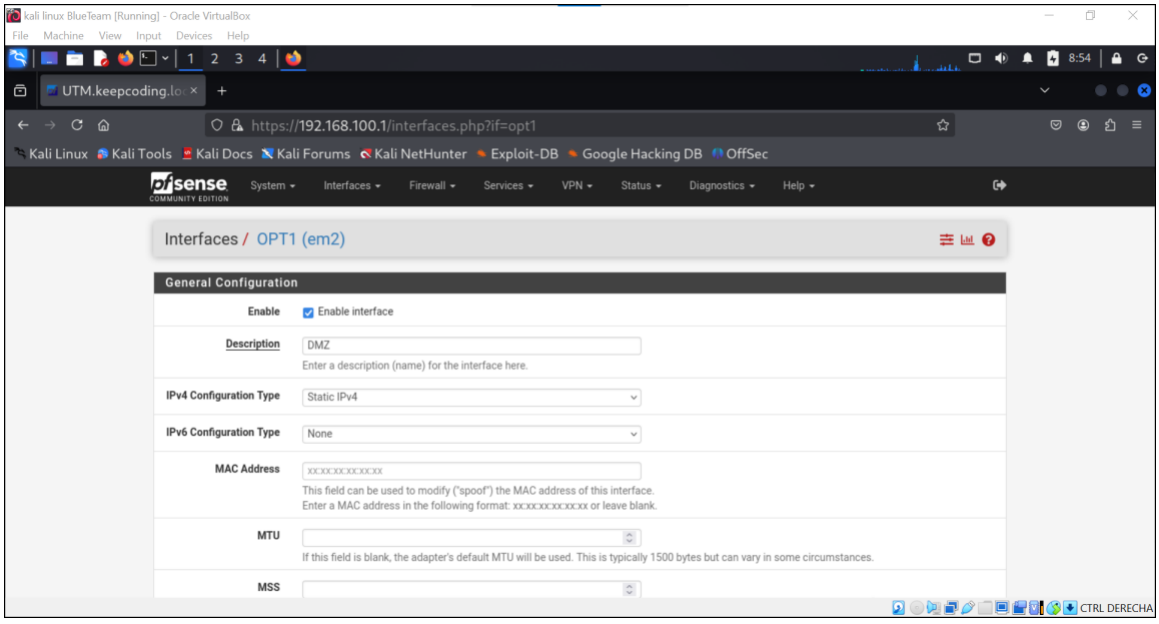


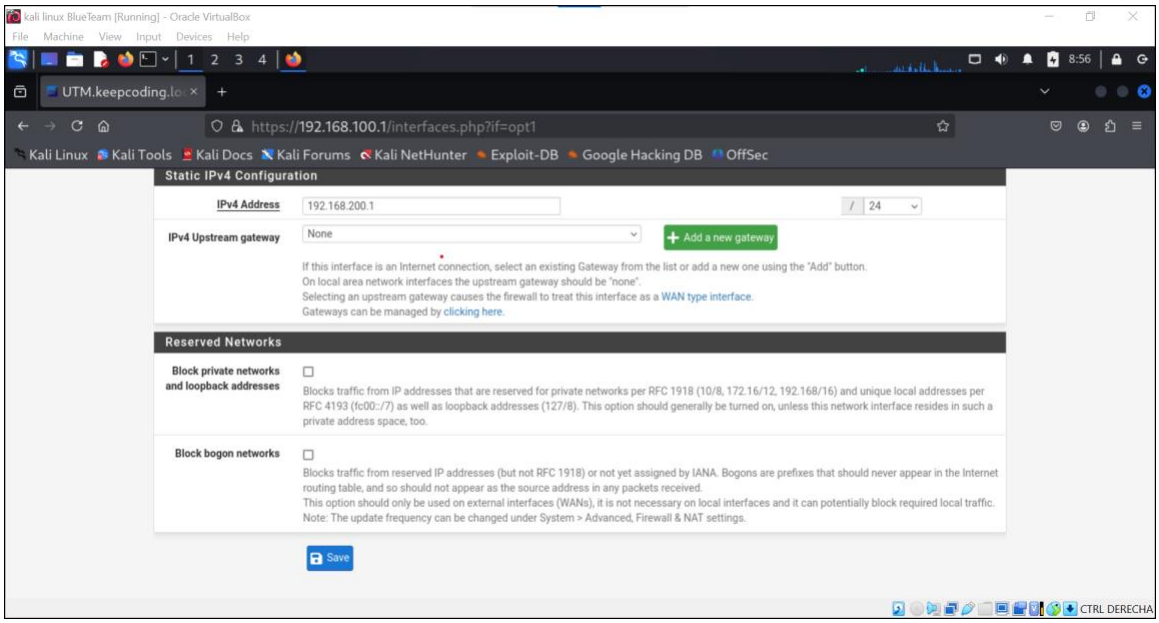


25. Declaramos el resto de las tarjetas de red que nos faltan (DMZs).

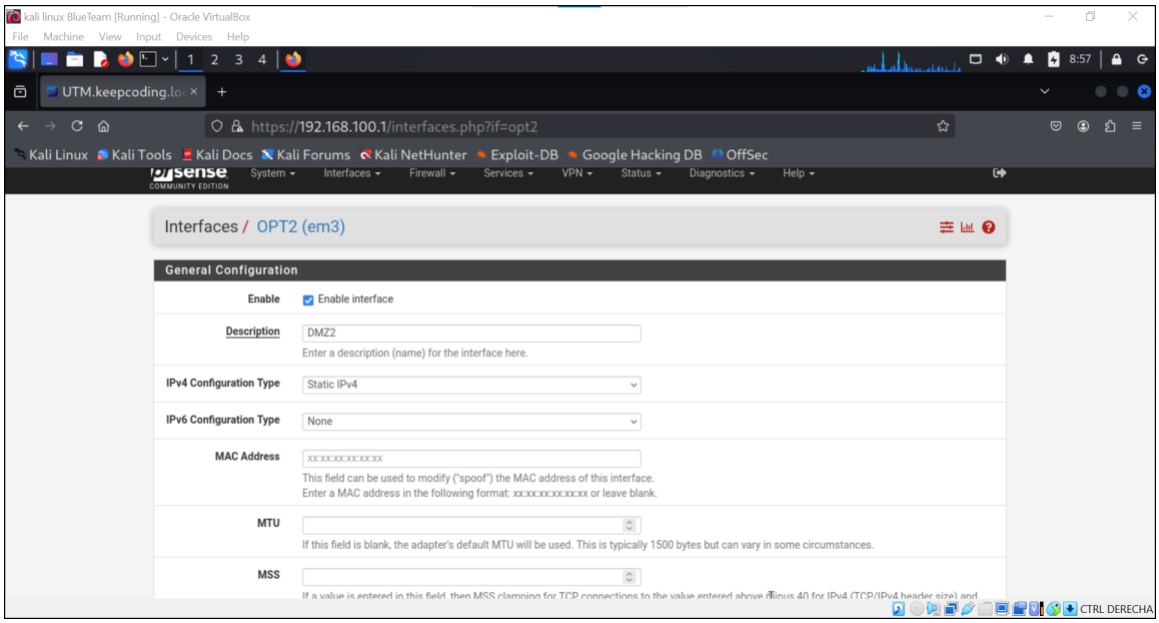


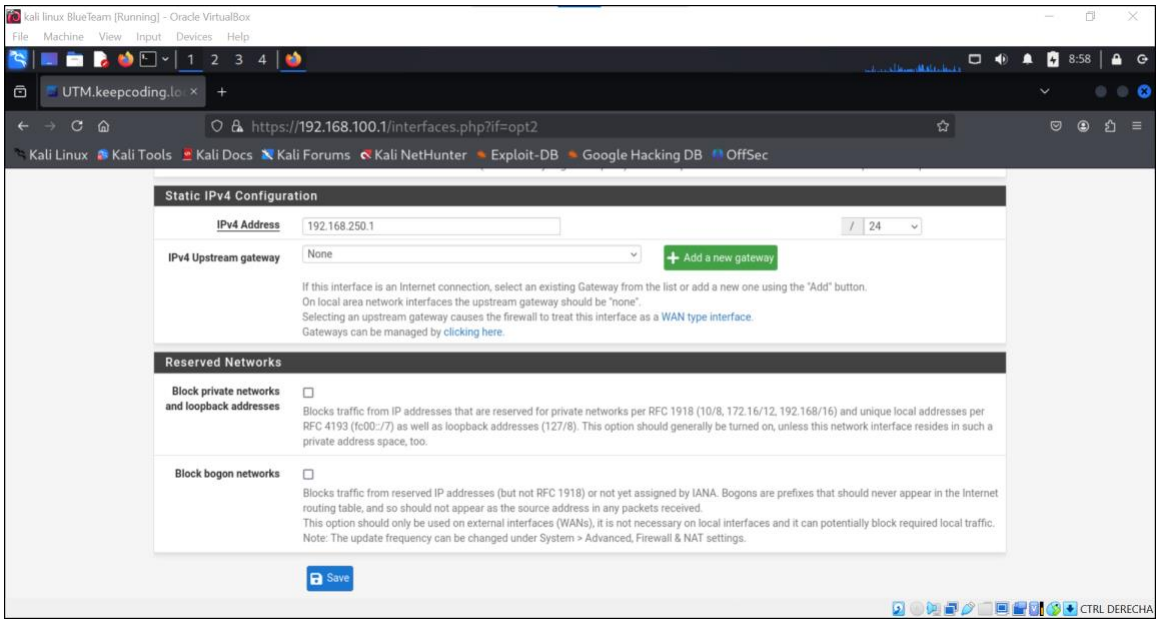
26. Configuramos las interfaces -> Interfaces > OPT1
    a. Descripción -> DMZ
    b. IPv4 Configuration type -> Static IPv4
    c. IPv4 Address -> 192.168.200.1/24



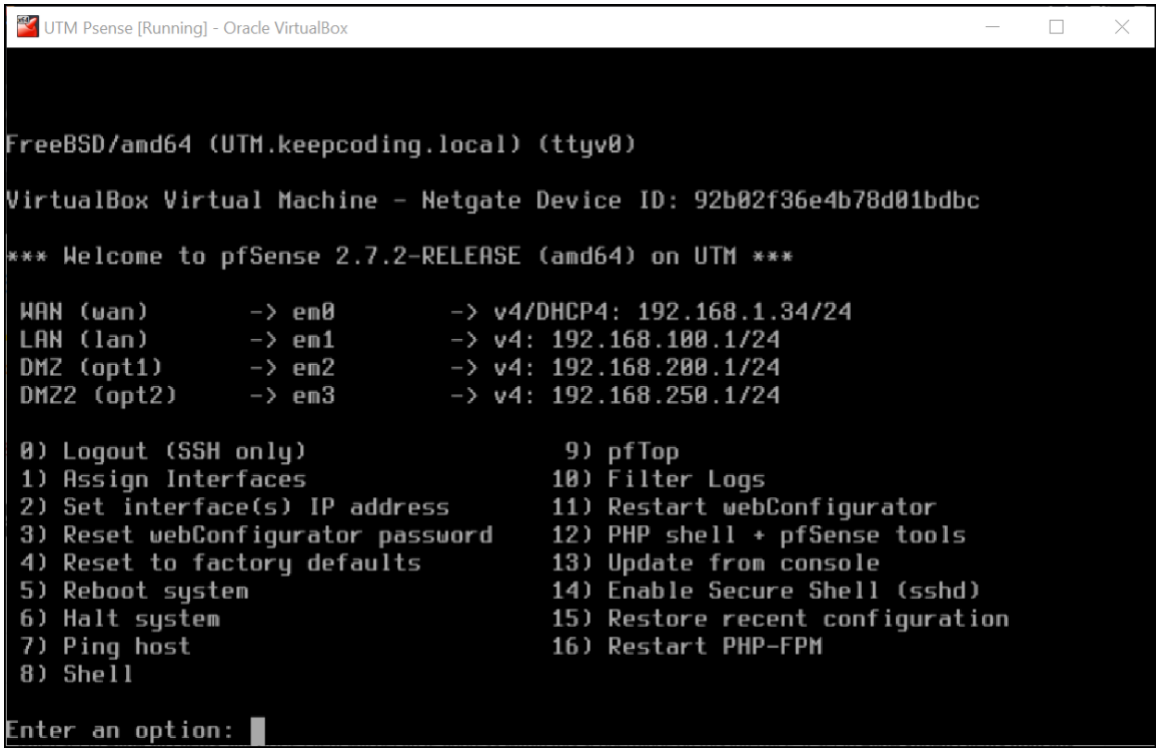


27. Interfaces > OPT2 (Igual que OPT1 pero cambiando la IP).
    a. Descripción -> DMZ2
    b. IPv4 Configuration type -> Static IPv4
    c. IPv4 Adress -> 192.168.250.1/24



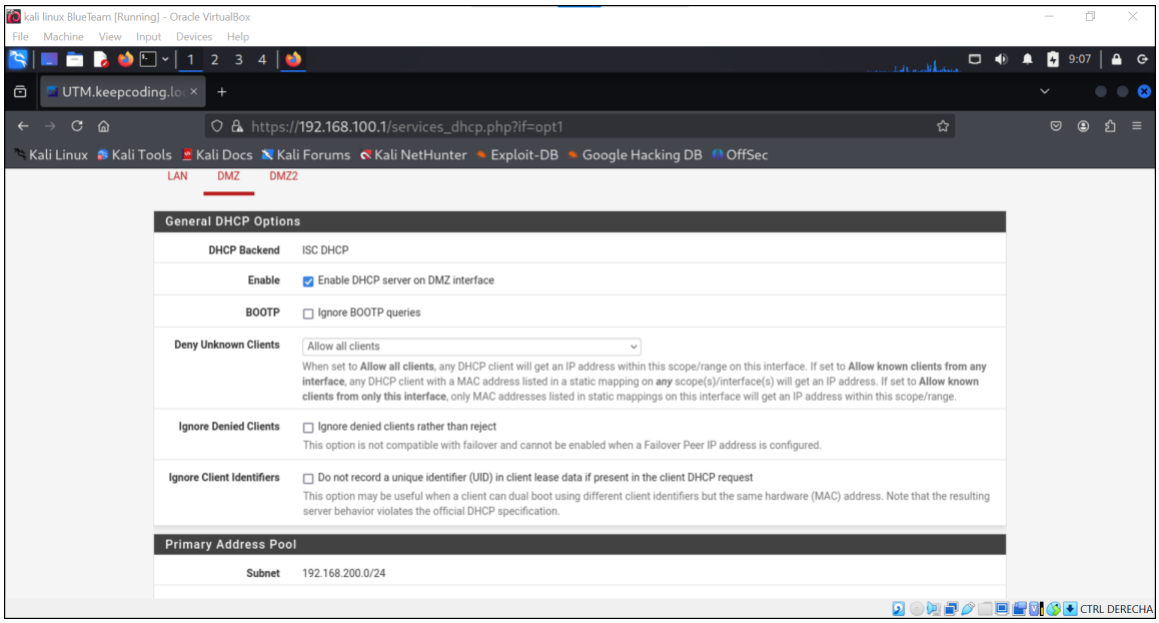


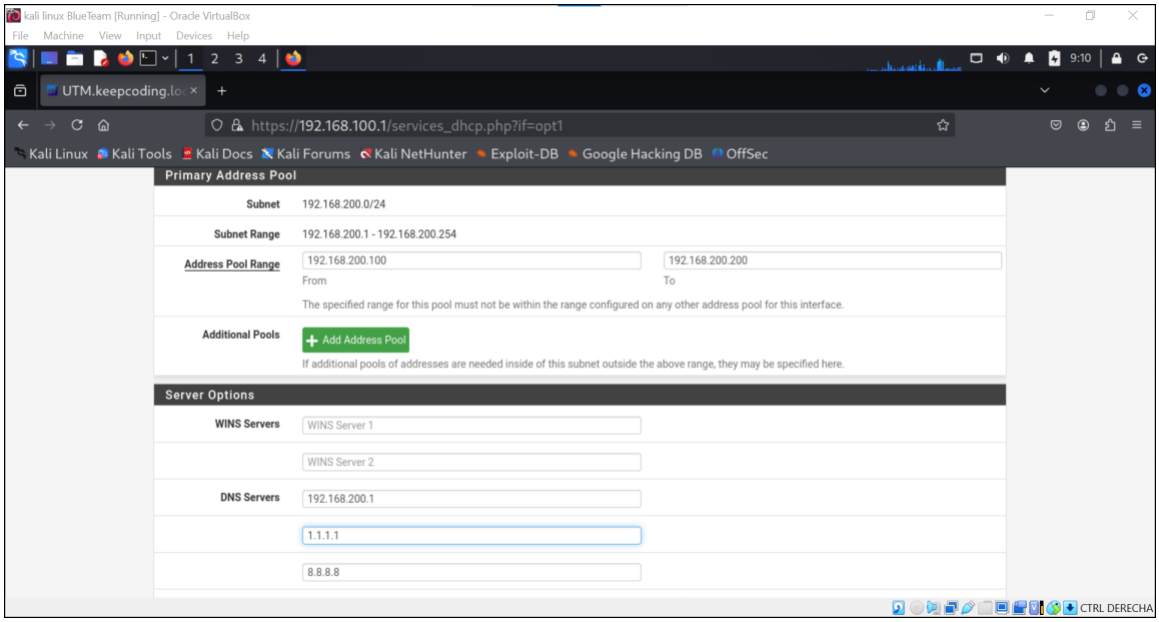
28. Ahora vamos a comprobar que en el PfSense aparecen las 4 interfaces.

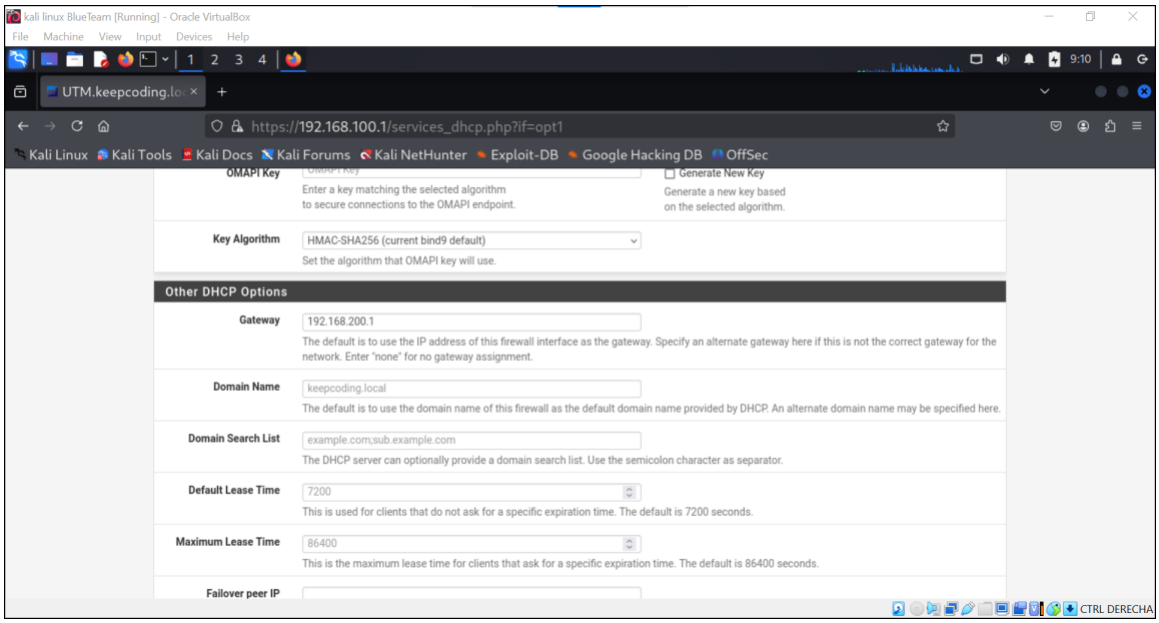


Configuración DHCP -> DMZ y DMZ2

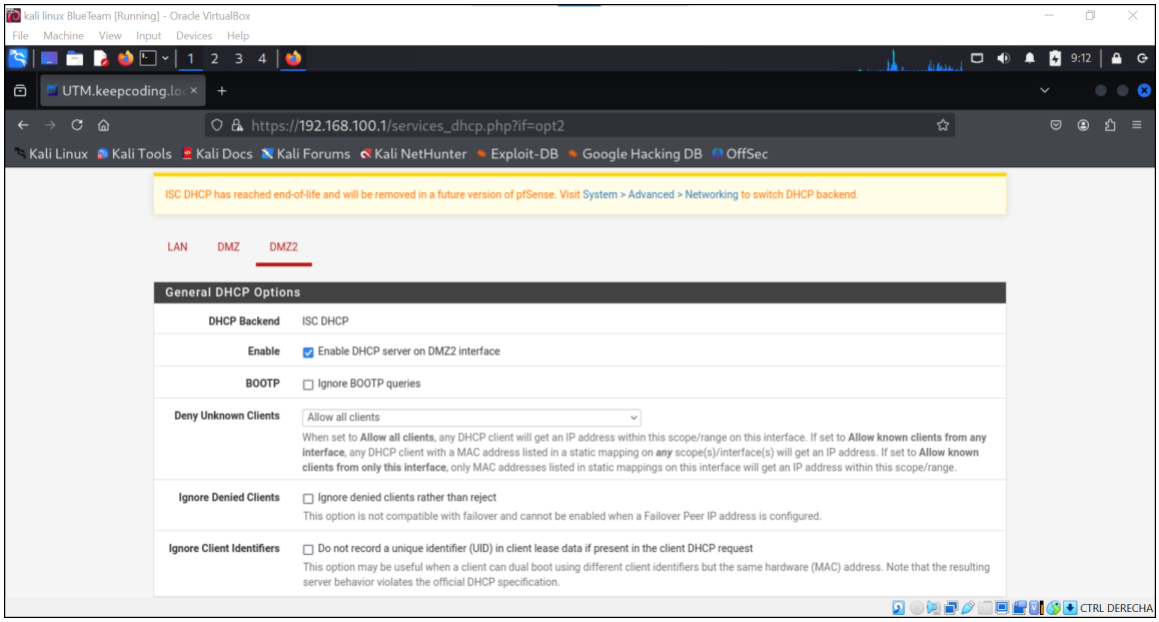
29. Vamos a la configuración del DHCP y habilitamos el DHCP server en esas interfaces.
    a. Enable DHCP server on DMZ interface
    b. Range 192.168.200.100 to 192.168.200.150
    c. DNS servers:
        i. 192.168.200.1
        ii. 1.1.1.1
        iii. 8.8.8.8
    d. Gateway 192.168.200.1

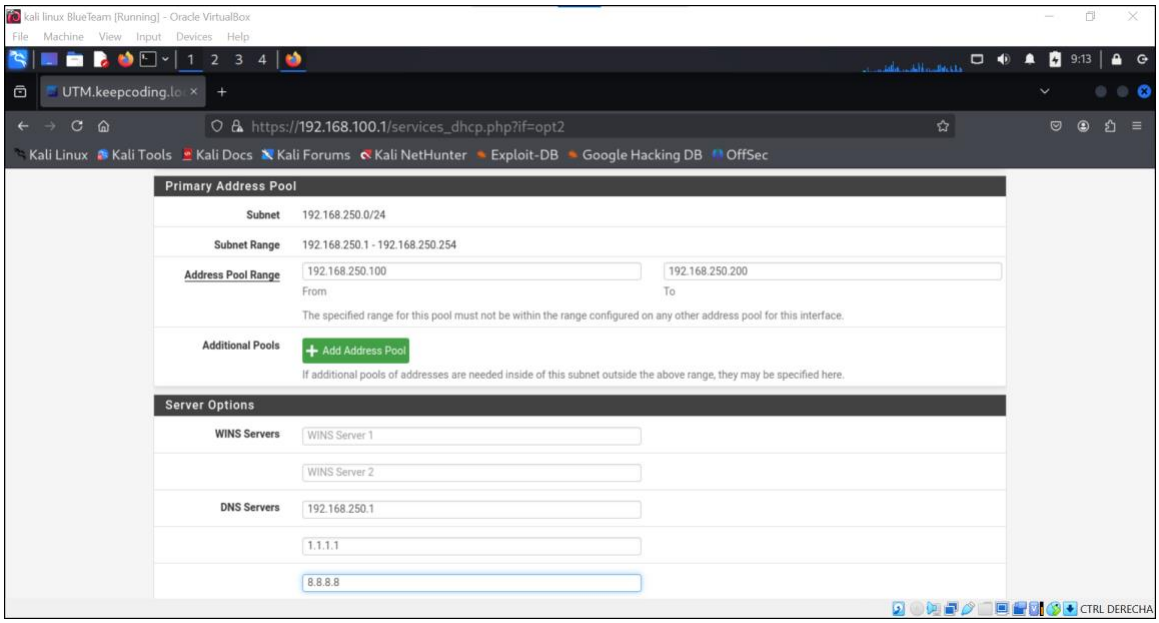


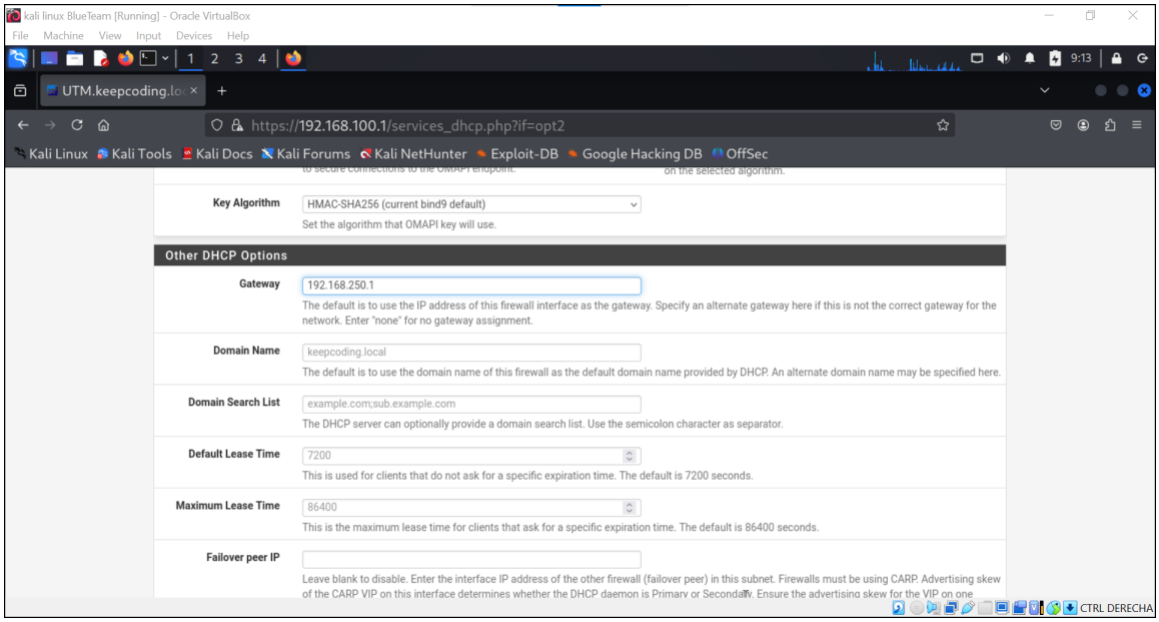




30. Interfaz DMZ_2.
    a. Enable DHCP server on DMZ_2 interface
    b. Range 192.168.250.100 to 192.168.250.150
    c. DNS servers:
        i. 192.168.250.1
        ii. 1.1.1.1
        iii. 8.8.8.8
    d. Gateway 192.168.250.1





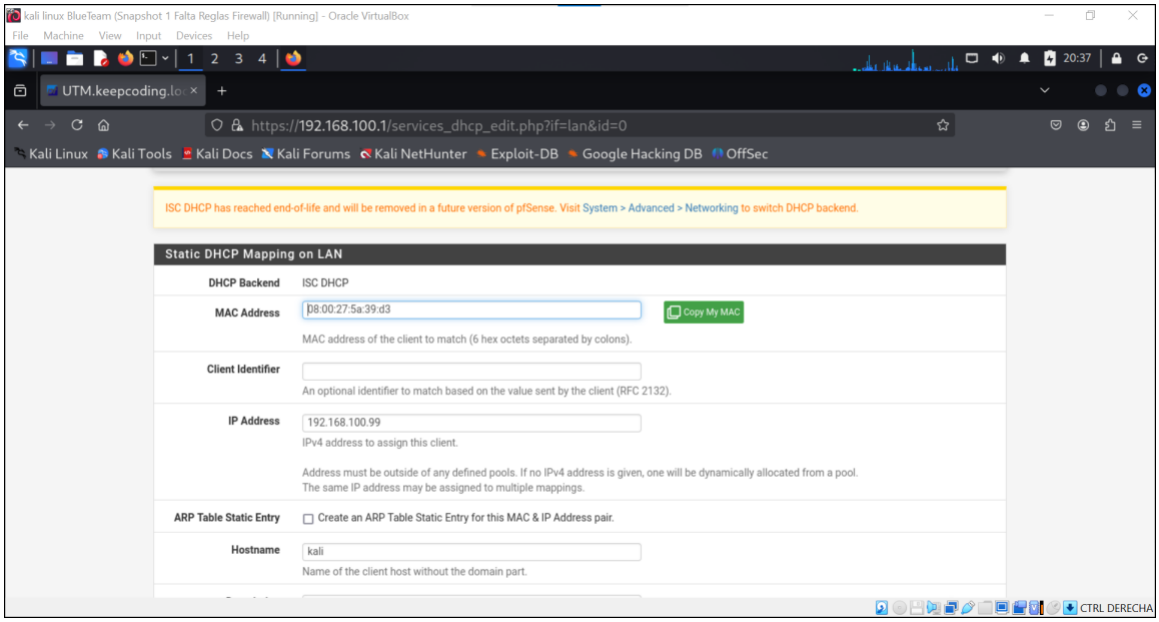


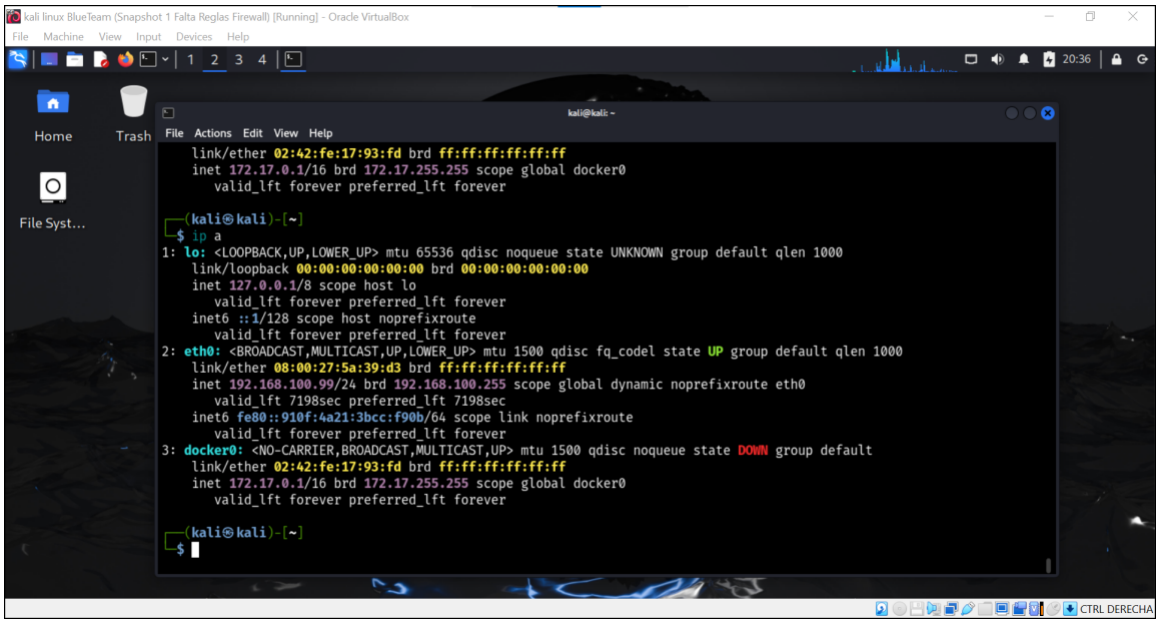
31. Comprobamos que funciona todo lo que hemos hecho.
    a. Cambiamos la Kali de red y nos asigna una IP del rango correcto por DHCP

Establecer IP estática

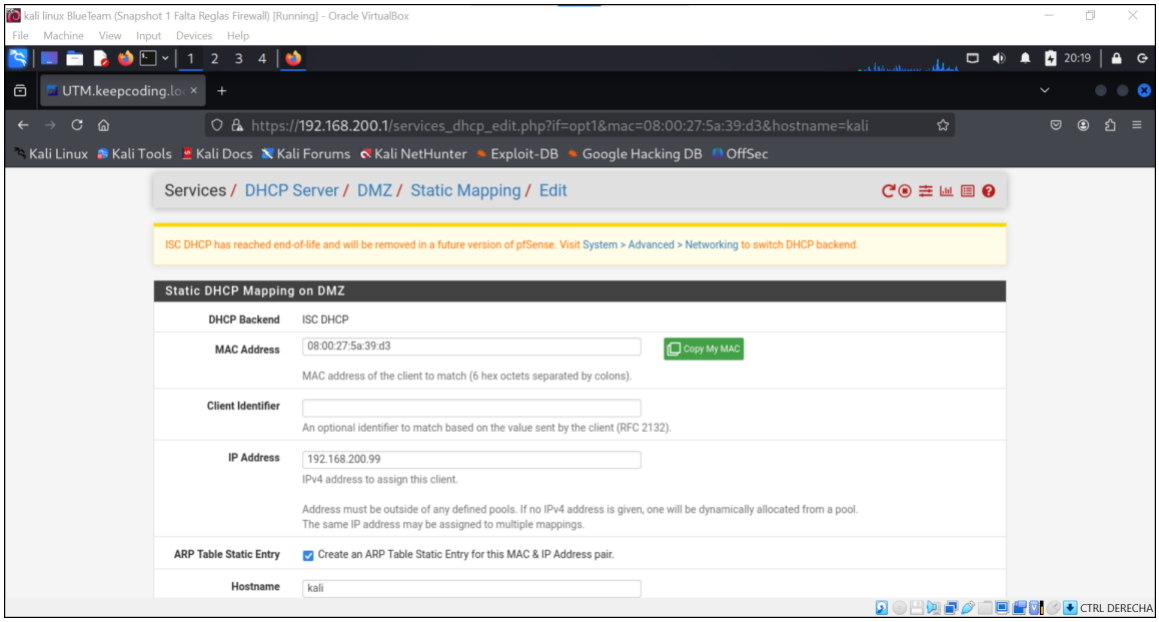
En este punto es importante haber establecido una regla principal de puertos HTTP y HTTPS a DMZ y DMZ2, que si no se realiza no dejará acceder a PfSense desde la misma red.

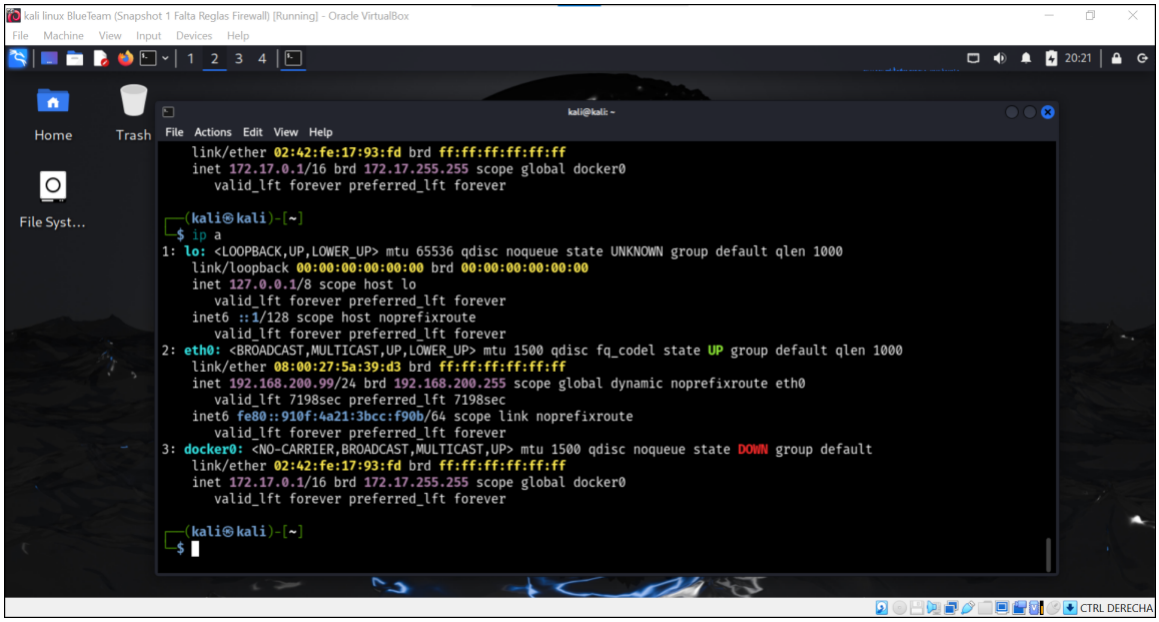
32. LAN



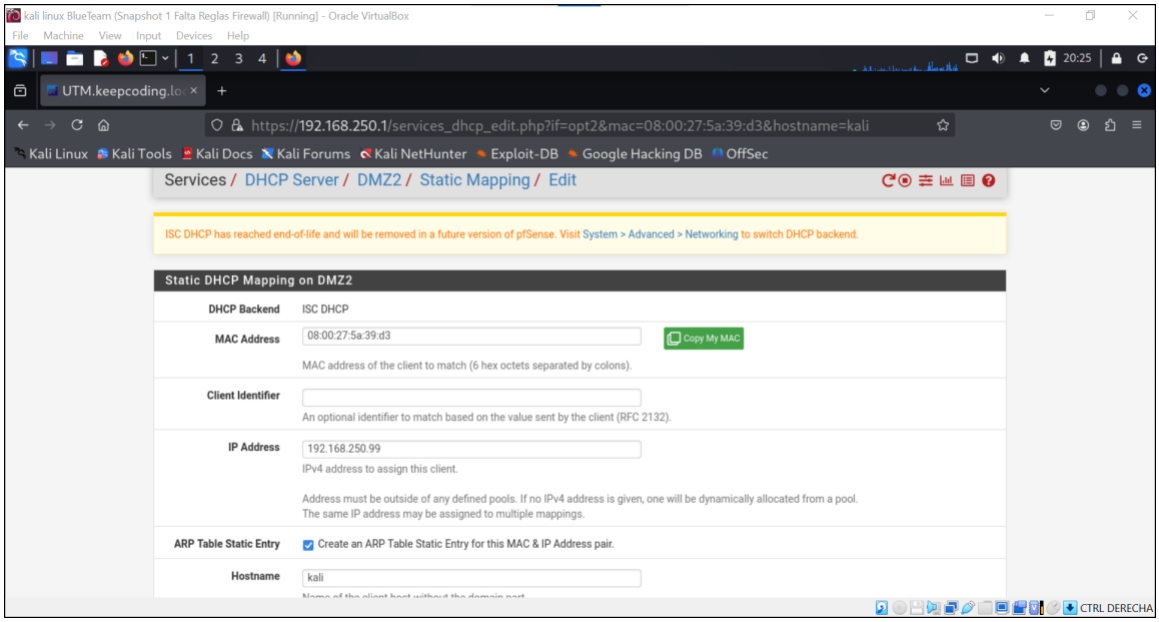


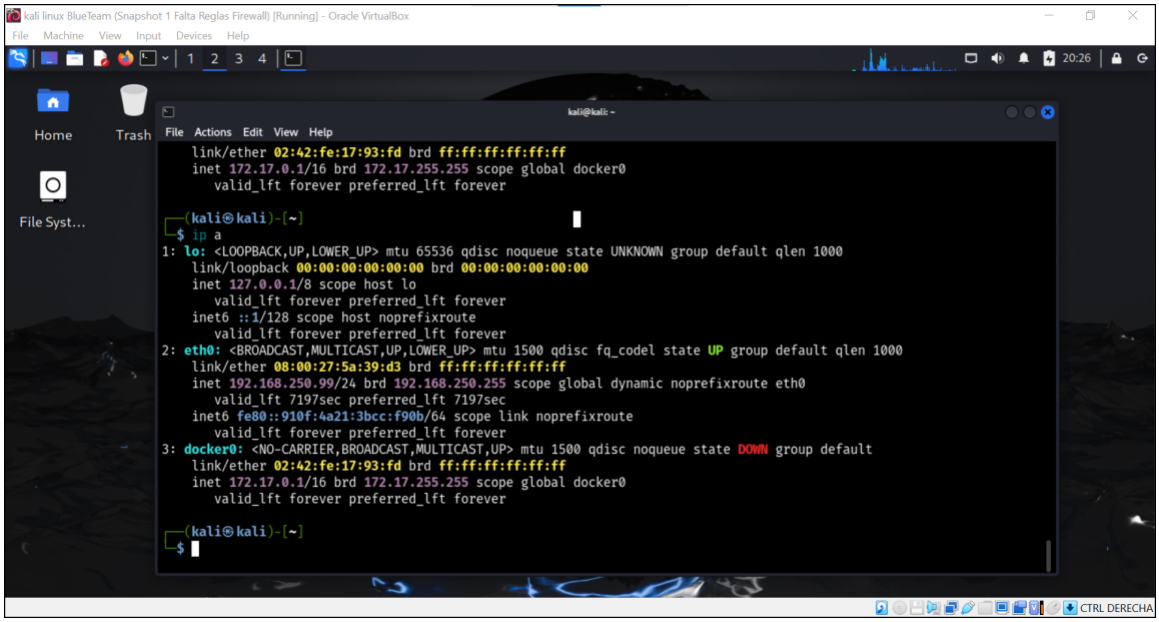
33. DMZ


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
https://192.168.200.1/services_dhcp_edit.php?if=opt1&mac=08:00:27:5a:39:d3&hostname=kali
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Services / DHCP Server / DMZ / Static Mapping / Edit
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Static DHCP Mapping on DMZ
DHCP Backend
ISC DHCP
MAC Address
08:00:27:5a:39:d3
Copy My MAC
MAC address of the client to match (6 hex octets separated by colons).
Client Identifier
An optional identifier to match based on the value sent by the client (RFC 2132).
IP Address
192.168.200.99
IPv4 address to assign this client.
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool.
The same IP address may be assigned to multiple mappings.
ARP Table Static Entry
Create an ARP Table Static Entry for this MAC & IP Address pair.
Hostname
kali
CTRL DERECHA


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
Trash
File Syst...
kali@kali: ~
File Actions Edit View Help
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
inet 192.168.200.99/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
valid_lft 7198sec preferred_lft 7198sec
inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$
CTRL DERECHA

34. DMZ2

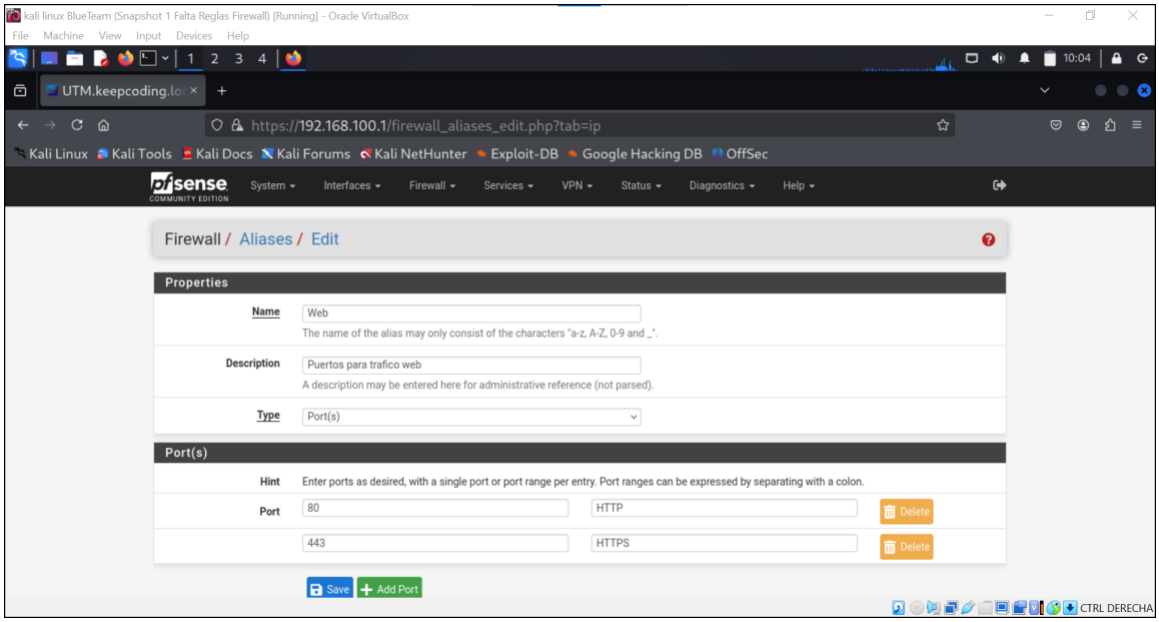

kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
https://192.168.250.1/services_dhcp_edit.php?if=opt2&mac=08:00:27:5a:39:d3&hostname=kali
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Services / DHCP Server / DMZ2 / Static Mapping / Edit
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Static DHCP Mapping on DMZ2
DHCP Backend
ISC DHCP
MAC Address
08:00:27:5a:39:d3
Copy My MAC
MAC address of the client to match (6 hex octets separated by colons).
Client Identifier
An optional identifier to match based on the value sent by the client (RFC 2132).
IP Address
192.168.250.99
IPv4 address to assign this client.
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool.
The same IP address may be assigned to multiple mappings.
ARP Table Static Entry
Create an ARP Table Static Entry for this MAC & IP Address pair.
Hostname
kali
CTRL DERECHA


kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home
Trash
File Syst...
kali@kali: ~
File Actions Edit View Help
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
inet 192.168.250.99/24 brd 192.168.250.255 scope global dynamic noprefixroute eth0
valid_lft 7197sec preferred_lft 7197sec
inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$
CTRL DERECHA

Establecemos alias

35. Asignamos alias a los puertos http (80) y https (443)

Vamos a otorgar el alias "Web" a los puertos 80 (HTTP) y 443 (HTTPS), ya que ambos están comúnmente asociados a la transmisión de datos a través de páginas web. El puerto 80 (HTTP) se utiliza para establecer conexiones no cifradas, lo que significa que los datos transmitidos entre el cliente y el servidor pueden ser interceptados y leídos fácilmente por terceros. Por otro lado, el puerto 443 (HTTPS) opera con un nivel de seguridad superior, ya que emplea protocolos de cifrado como TLS (Transport Layer Security), lo que garantiza la confidencialidad e integridad de los datos transmitidos.



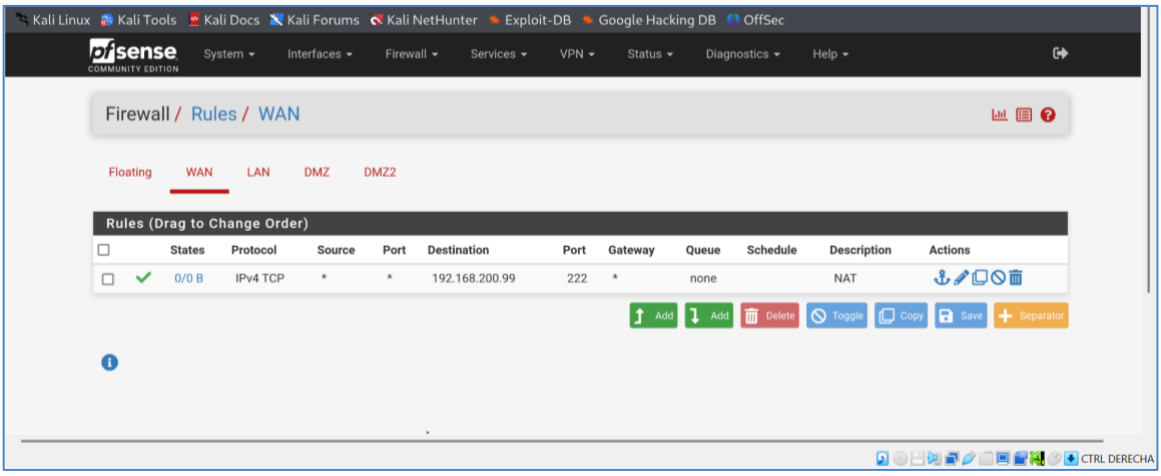
Creamos las reglas de los FW (firewall)

En esta sección se detallan las reglas principales implementadas en el firewall, junto con la validación del correcto funcionamiento del servicio DNS y la definición de políticas específicas para la gestión de las comunicaciones entre las diferentes redes configuradas.

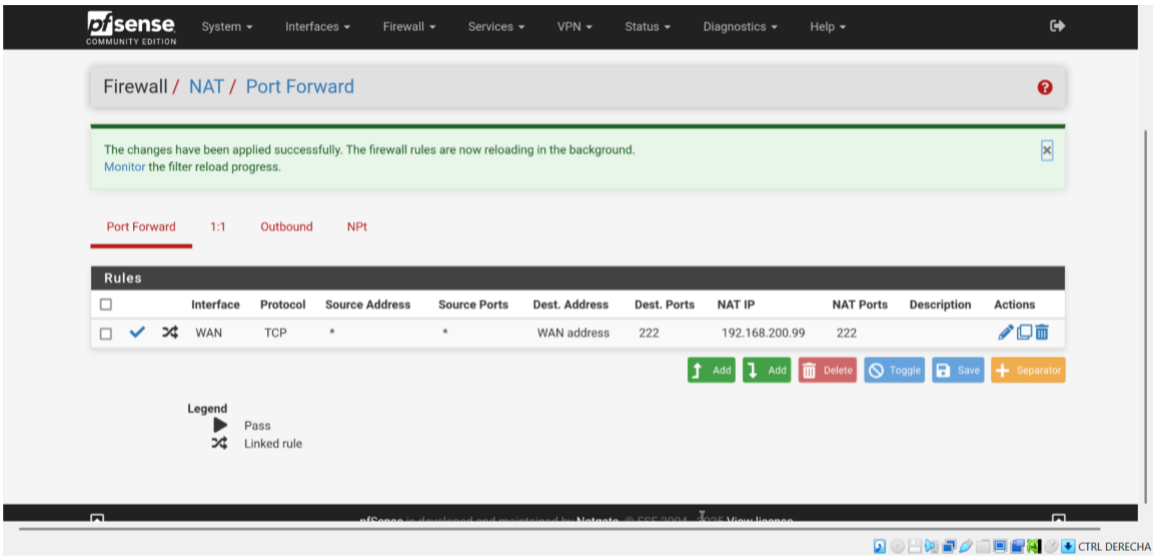
Se establece que la red DMZ estará completamente aislada de las redes internas LAN y DMZ2, sin posibilidad de comunicación en ningún sentido. No obstante, se permitirá acceso bidireccional entre la red DMZ y la red externa WAN, cumpliendo con los requisitos de segmentación y control. Asimismo, se asigna esta red al Honeypot, como parte de la estrategia de detección y análisis de posibles amenazas externas.

Esta configuración refuerza los principios de seguridad perimetral y minimiza los riesgos asociados a accesos no autorizados desde redes externas hacia la infraestructura interna.

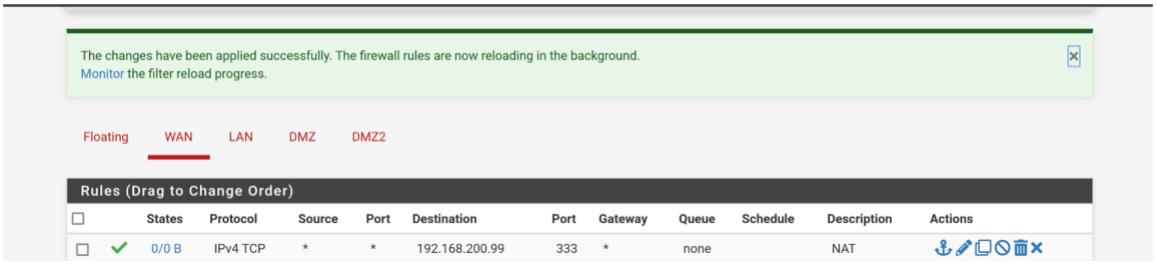
36. WAN CASO HONEYPOT SSH.



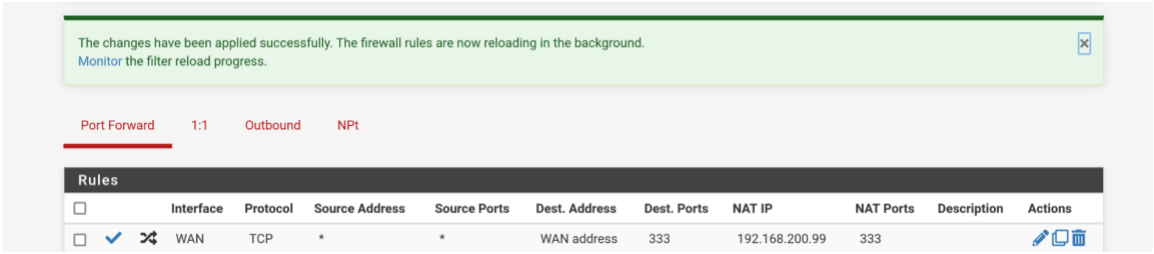
37. NAT CASO HONEYPOT SSH.



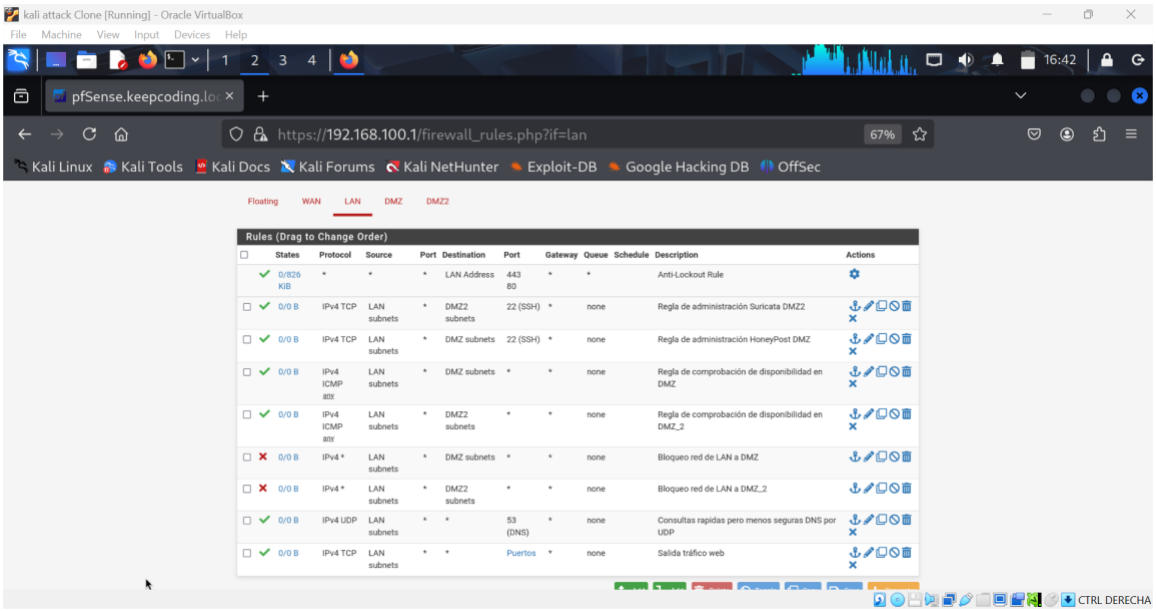
38. WAN CASO HONEYPOT RDP.



39. NAT CASO HONEYPOT RDP.

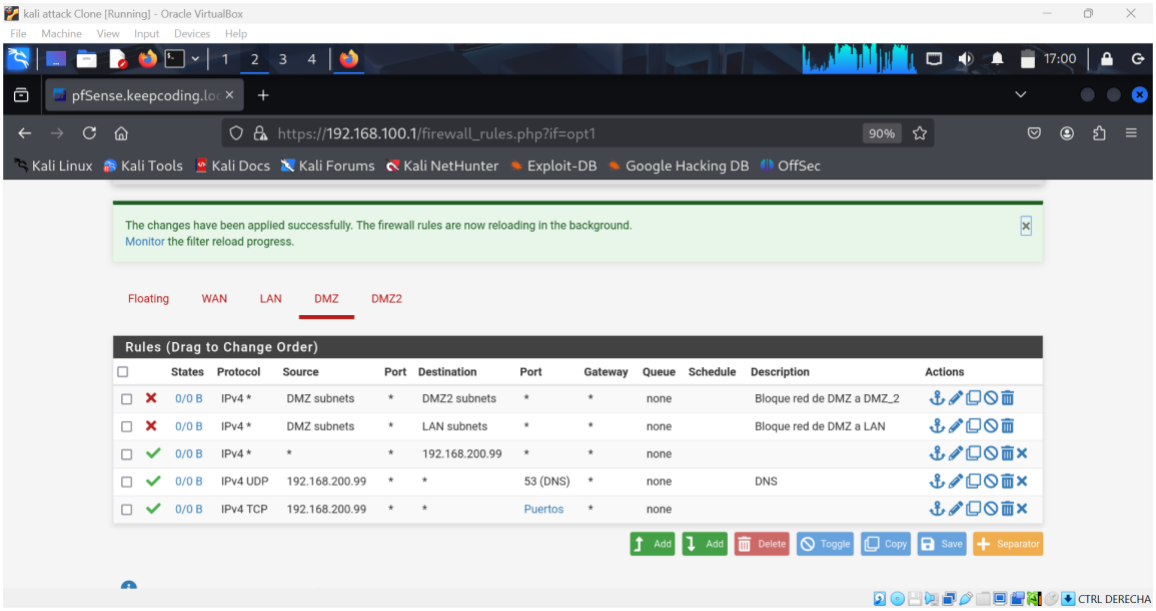


40. LAN.

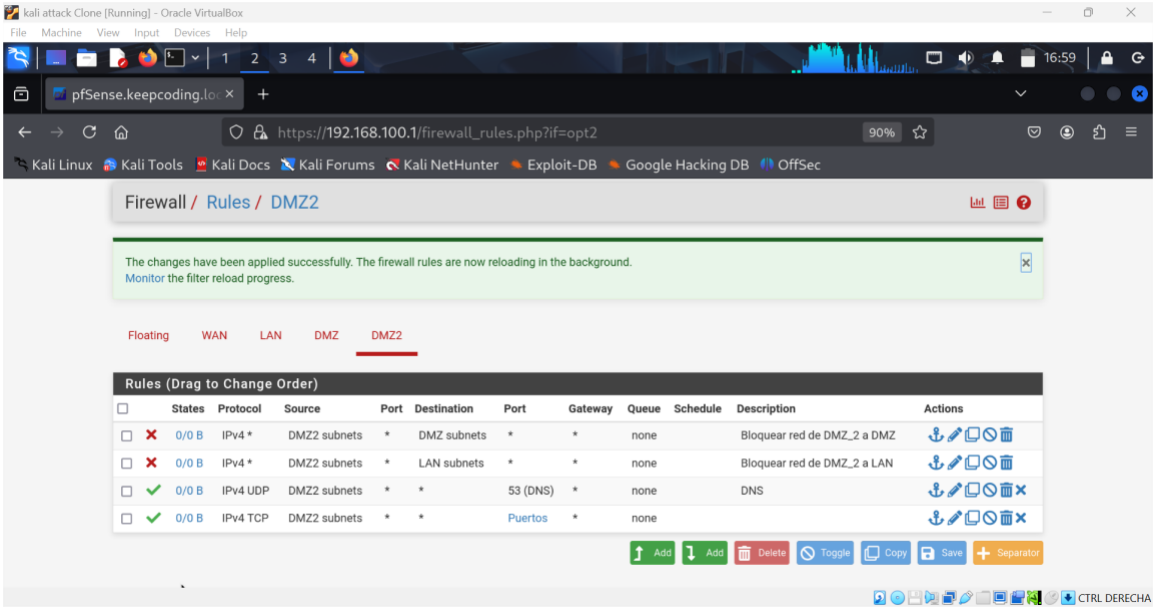


Nota:
Se han creado reglas para la administración de las máquinas por SSH desde la red LAN.

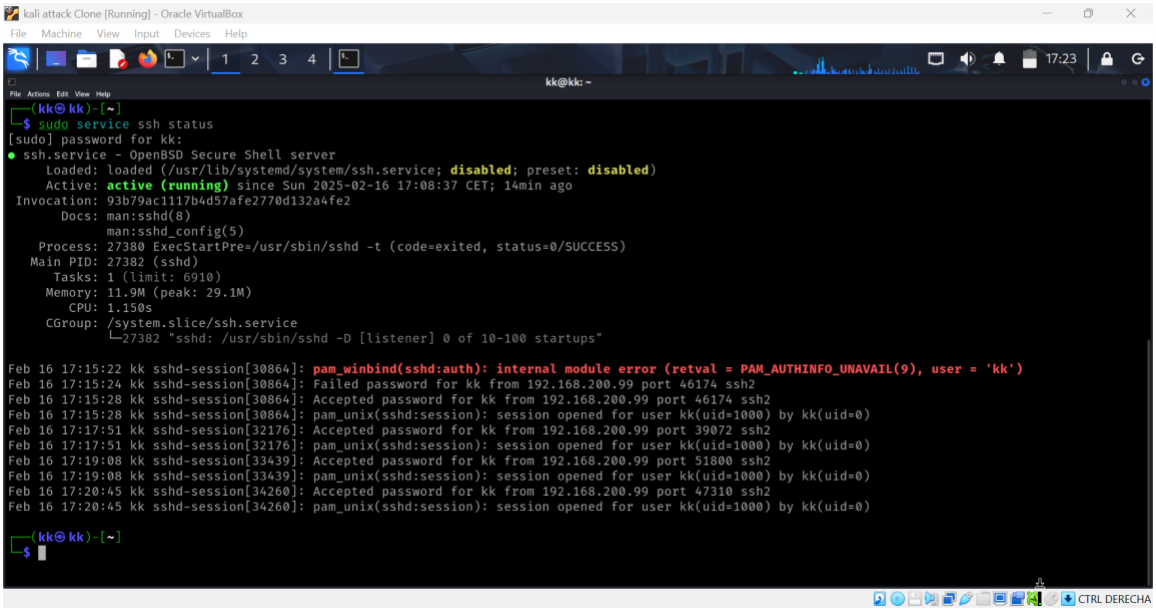
41. DMZ



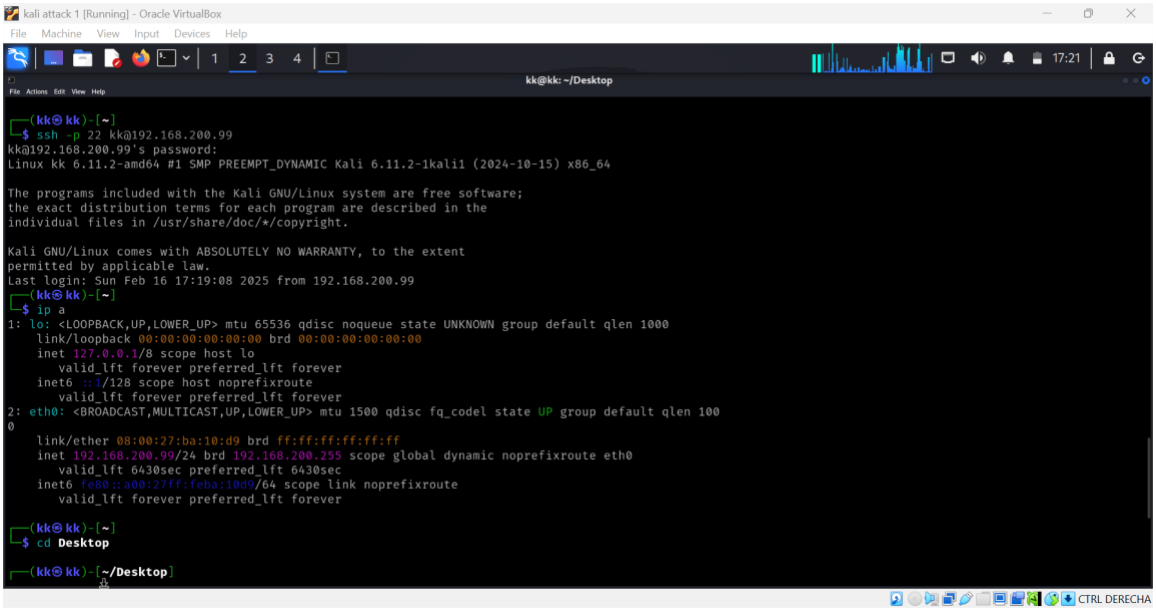
42. DMZ2



43. Si quisiéramos conectarnos por SSH para administrar la máquina. Habilitamos el servicio de SSH en la máquina deseada.



44. Realizamos la conexión desde la red LAN.



ElasticCloud

Creación de cuenta de ElasticCloud

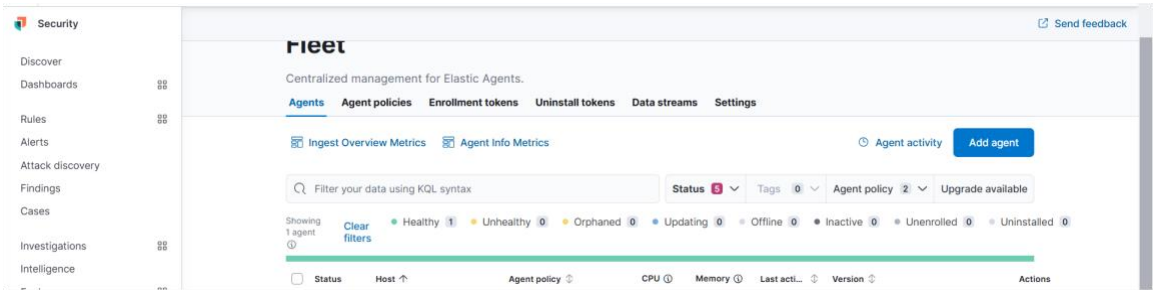
45. Creamos la cuenta de ElasticCloud utilizando la versión de 15 días de prueba proporcionada en la página de Elastic (https://cloud.elastic.co/registration)

Configuración ElasticCloud

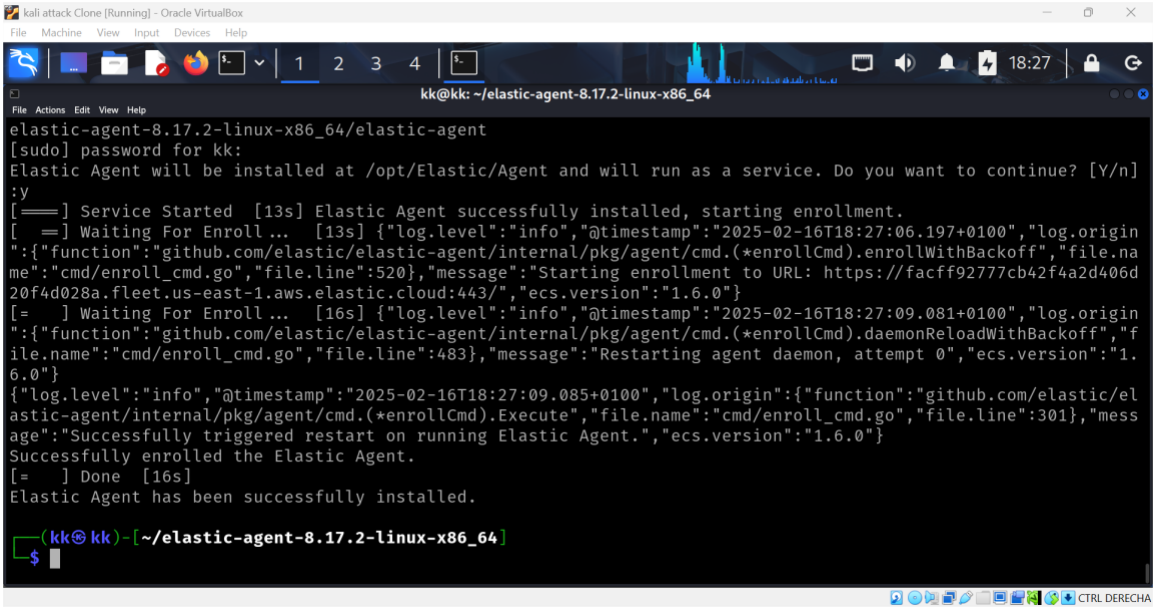
46. Instalación de los agentes en las máquinas Linux y Windows.

47. En la sección de Fleet añadimos el agente a la política deseada. En ese momento se nos proporcionará un comando para instalarlo tanto en la máquina Linux como en la máquina Windows.

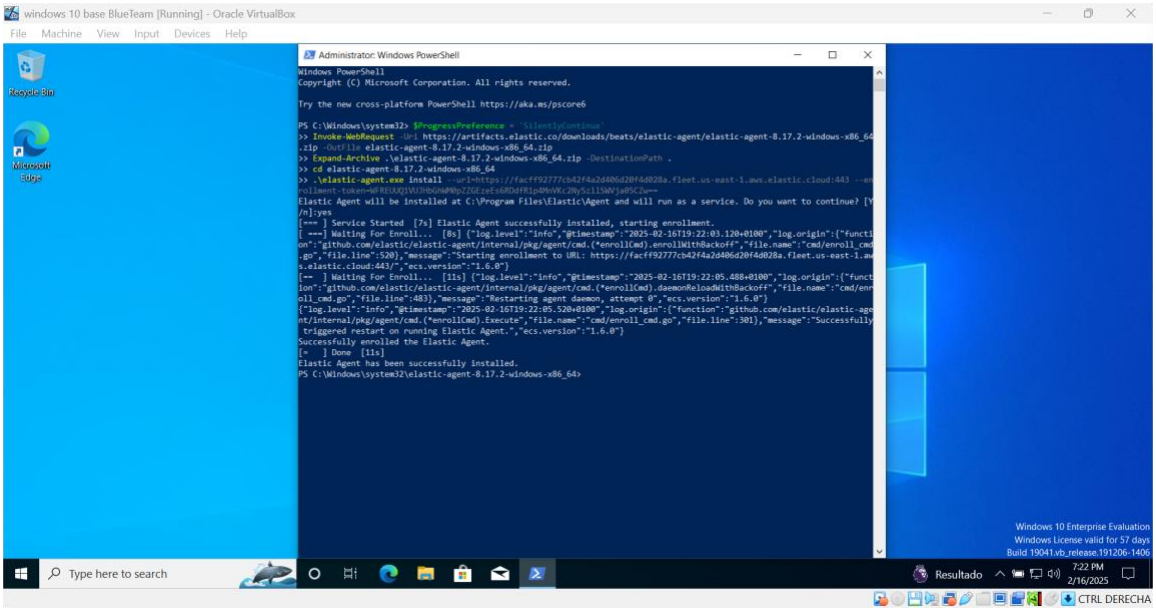
48. Fleet



49. Kali

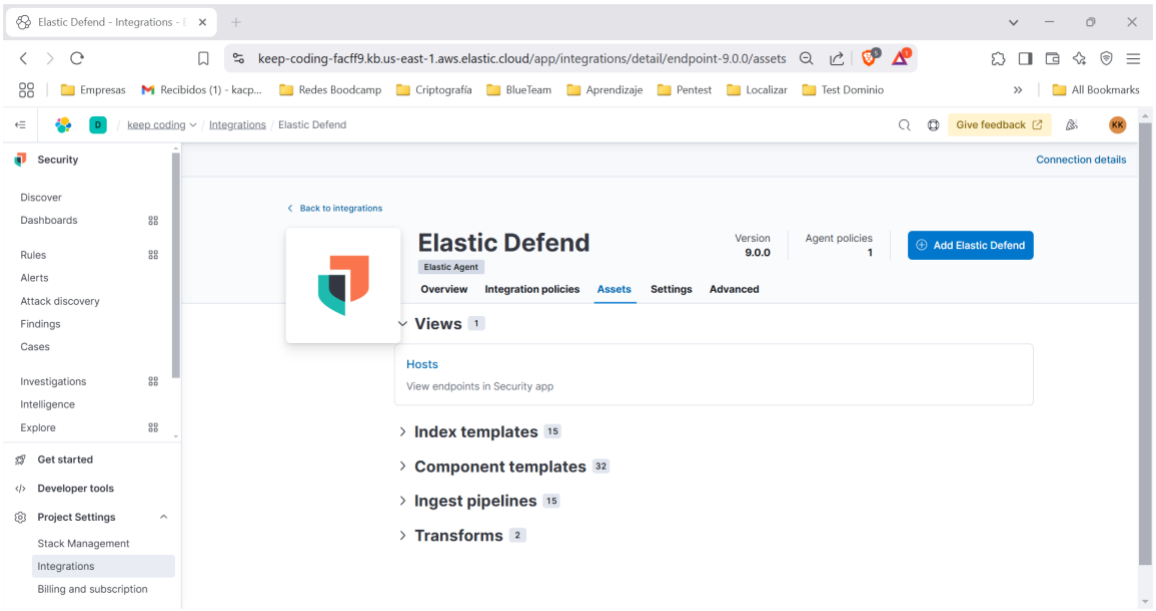


50. Windows

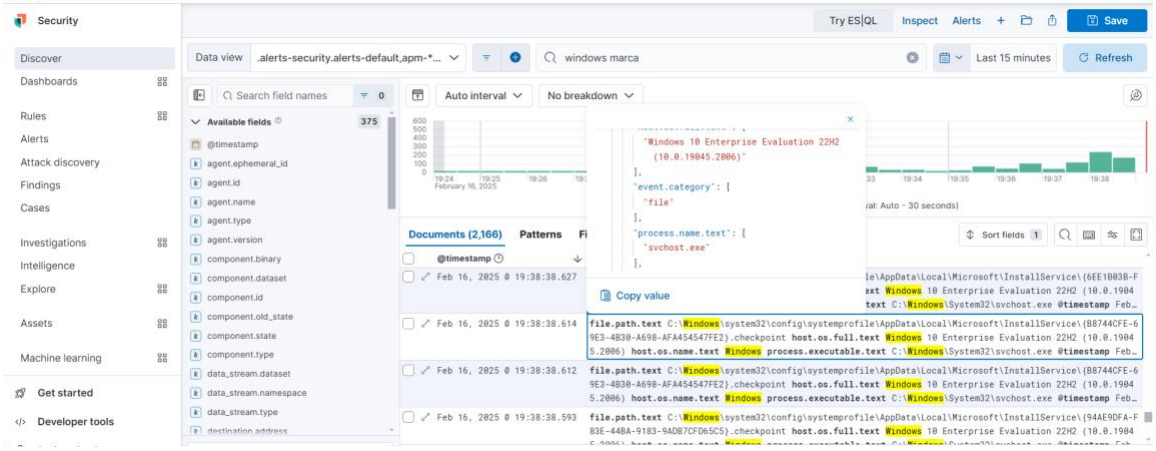


Integración de los logs en Windows

51. Vamos a integrar los logs relacionados con la monitorización de seguridad. Esto nos los proporciona la integración "*Elastic Defend*".



52. Evidencias de los logs generados.

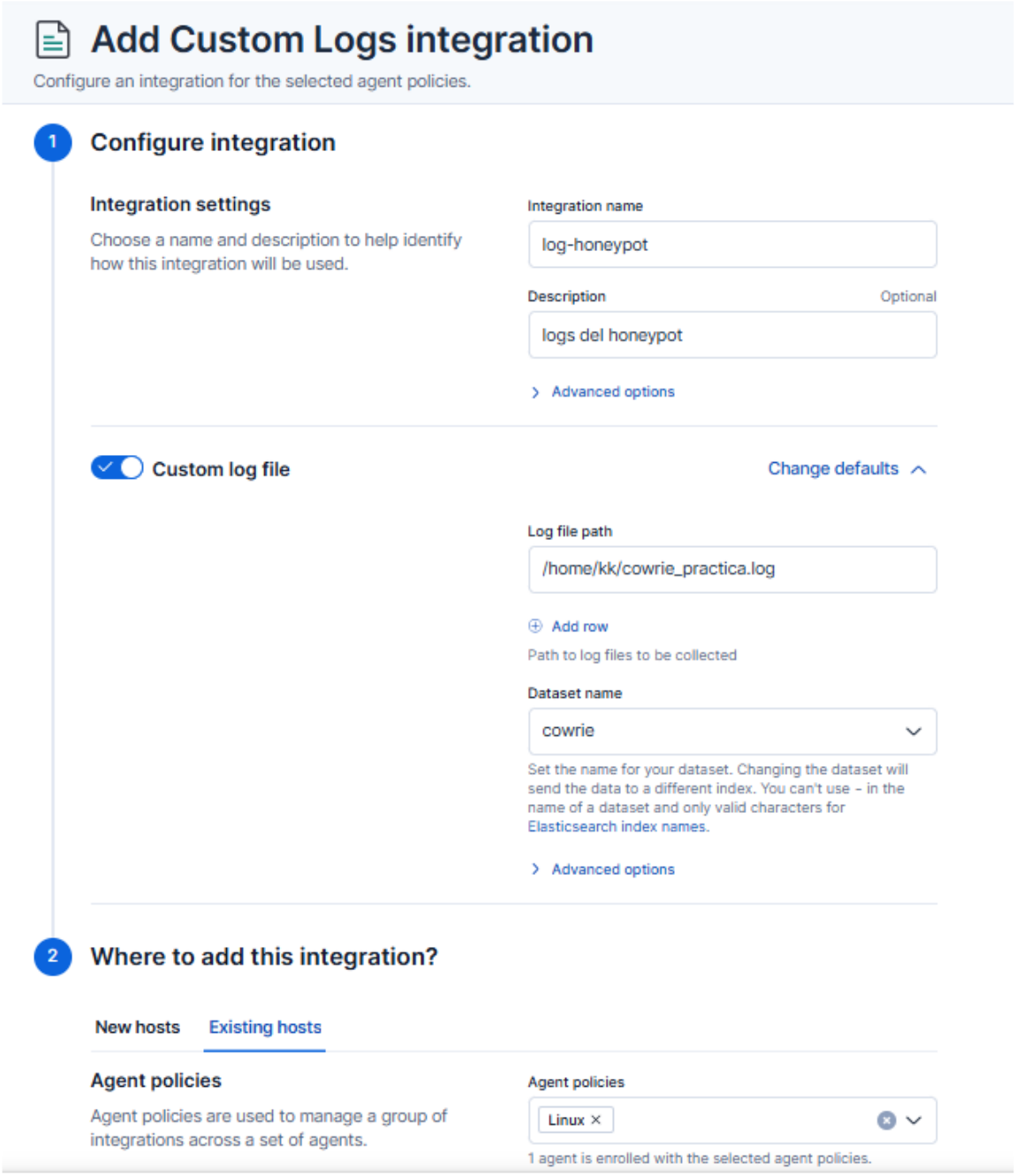


Integración de los logs del Honeypot en Elastic

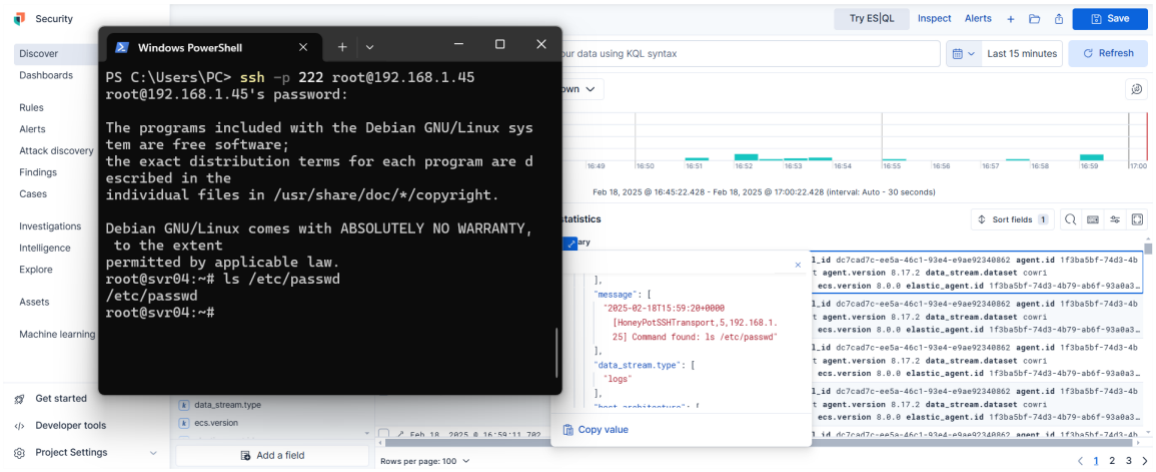
53. Ejecutamos el contenedor Docker con el honeypot y mandamos los logs generados a un archivo:

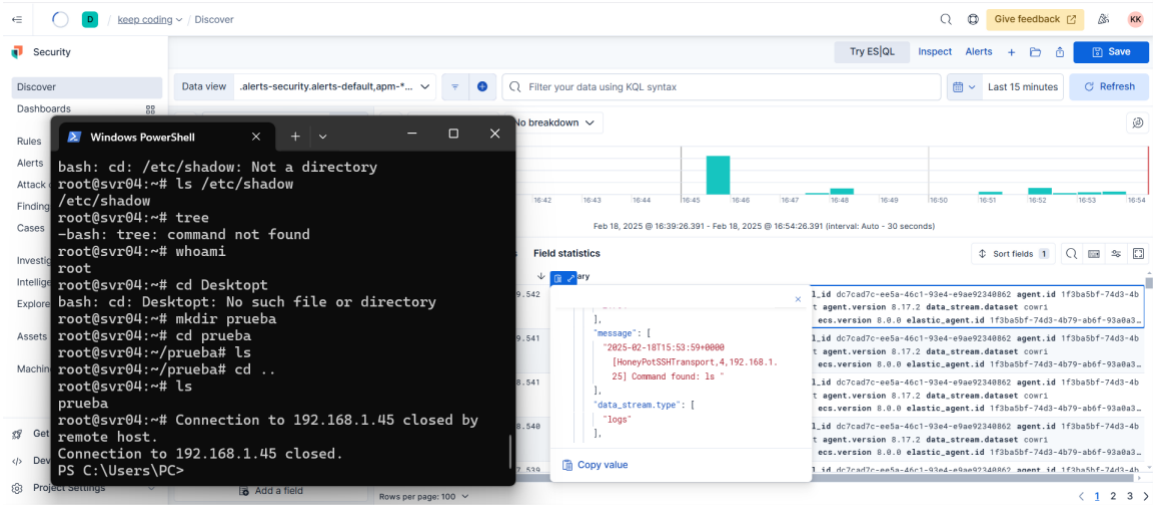
    a. docker run -p 222:2222 cowrie/cowrie > cowrie_practica.log

Incluimos los logs en Elastic con la ayuda de la integración "*Custom Logs*".



54. Revisamos que los logs no están llegando.





Integración de los logs de Apache y Suricata

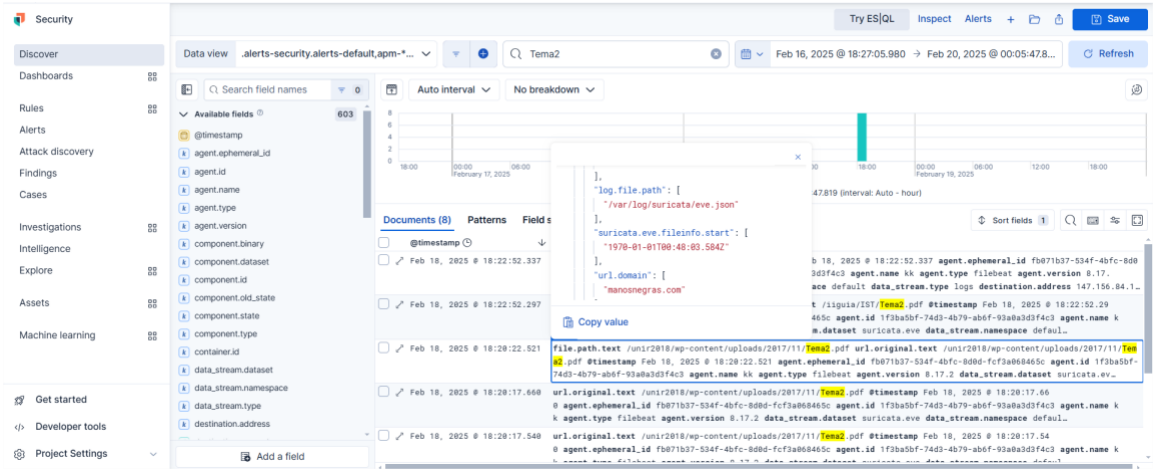
Suricata

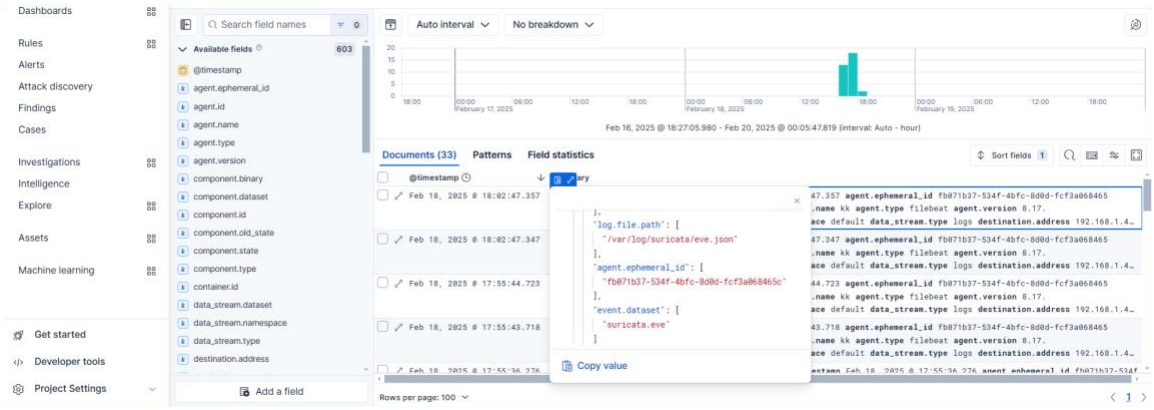
Suricata es una herramienta avanzada de detección y prevención de intrusiones que permite monitorear redes para identificar actividades sospechosas. Vamos a documentar su instalación, configuración y personalización mediante reglas diseñadas para detectar eventos específicos, como tráfico de red, intentos de conexión SSH y descargas de archivos PDF. La instalación se realiza actualizando los paquetes del sistema e instalando Suricata, seguida de una ejecución inicial para verificar su funcionamiento.

Además, se describieron procedimientos para analizar y guardar los logs generados, esenciales para el análisis posterior y la respuesta a incidentes. Los logs se almacenan en el directorio /var/log/suricata, y se pueden respaldar mediante compresión y transferencia a un servidor remoto para asegurar su disponibilidad. En conjunto, estas configuraciones convierten a Suricata en una herramienta poderosa para fortalecer la seguridad de la red, proporcionando visibilidad y capacidad de respuesta frente a posibles amenazas. Los logs posteriormente se guardarán en la plataforma web Elastic.

55. Integración utilizada.

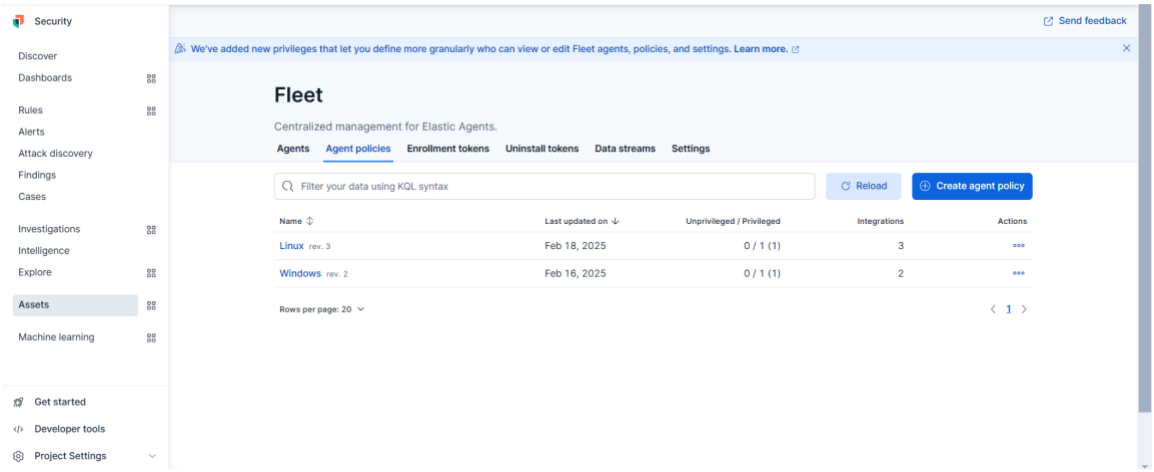
56. Evidencias de los logs recogidos.



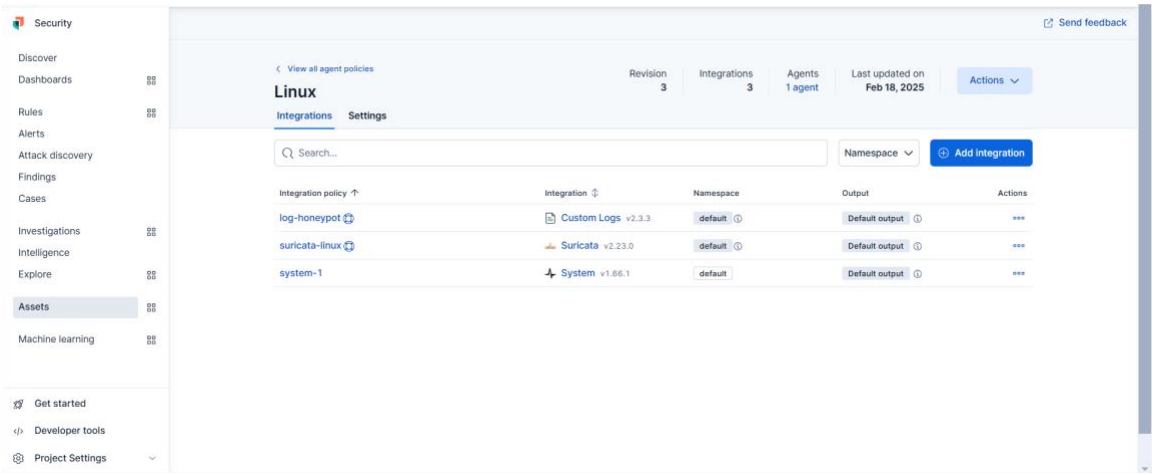


Configuración final de las políticas de Elastic

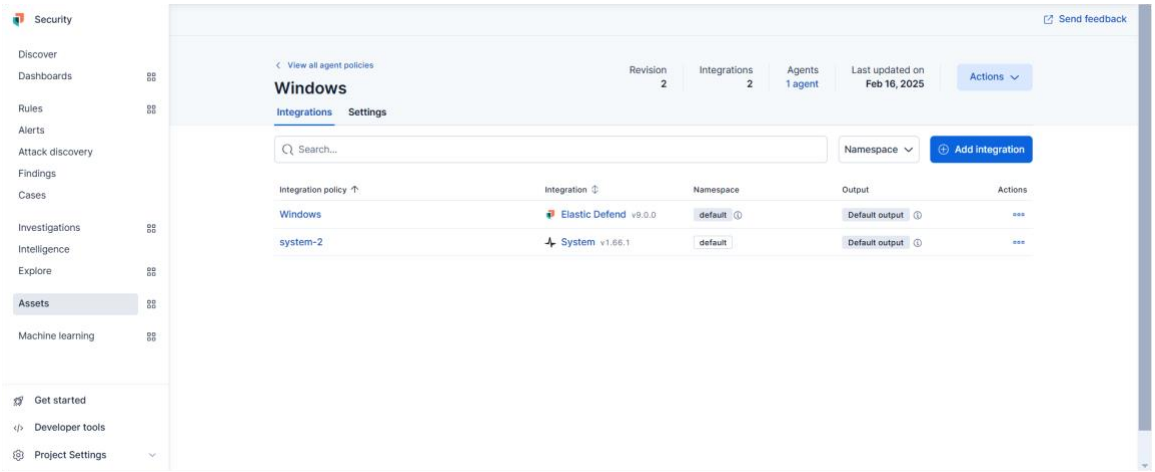
57. Fleet



58. Linux Suricata/HoneyPot



59. Windows



Logs

60. Se adjunta el archivo “Logs_Elastic.zip” y en el zip “Logs_en_Raw.zip” que se encuentran en crudo se encuentran los logs tanto de HoneyPot como de Suricata.

Propuesta de mejora

Podemos mejorar la siguiente infraestructura al reforzar la segmentación de las redes utilizando VLANs y aplicando reglas estrictas en el firewall PfSense, como limitando solamente el tránsito de los logs hacia Elastic, y encriptando todo tipo de información sensible con ChaCha20-Poly1305.

También habría que separar y eliminar la interacción bilateral entre las redes internas DMZ2 y LAN, tal como ya se hizo con la red DMZ con el honeypot para que solo sea accesible desde la WAN. Además, se habilitaría un sistema de detección y prevención de intrusos (IDS/IPS) como Suricata en el firewall, así como listas blancas para controlar el tráfico permitido y listas negras dinámicas para bloquear direcciones IP maliciosas conocidas.

Además, los logs generados deben segregarse y analizarse mediante herramientas especializadas, configurando alertas en tiempo real para detectar actividad sospechosa como intentos de explotación o conexiones no autorizadas.

Por último, habría que implementar un sistema de copias de seguridad automáticas y periódicas de todos los datos críticos, asegurándose de que las copias sean almacenadas en una ubicación segura y aislada de la red principal.