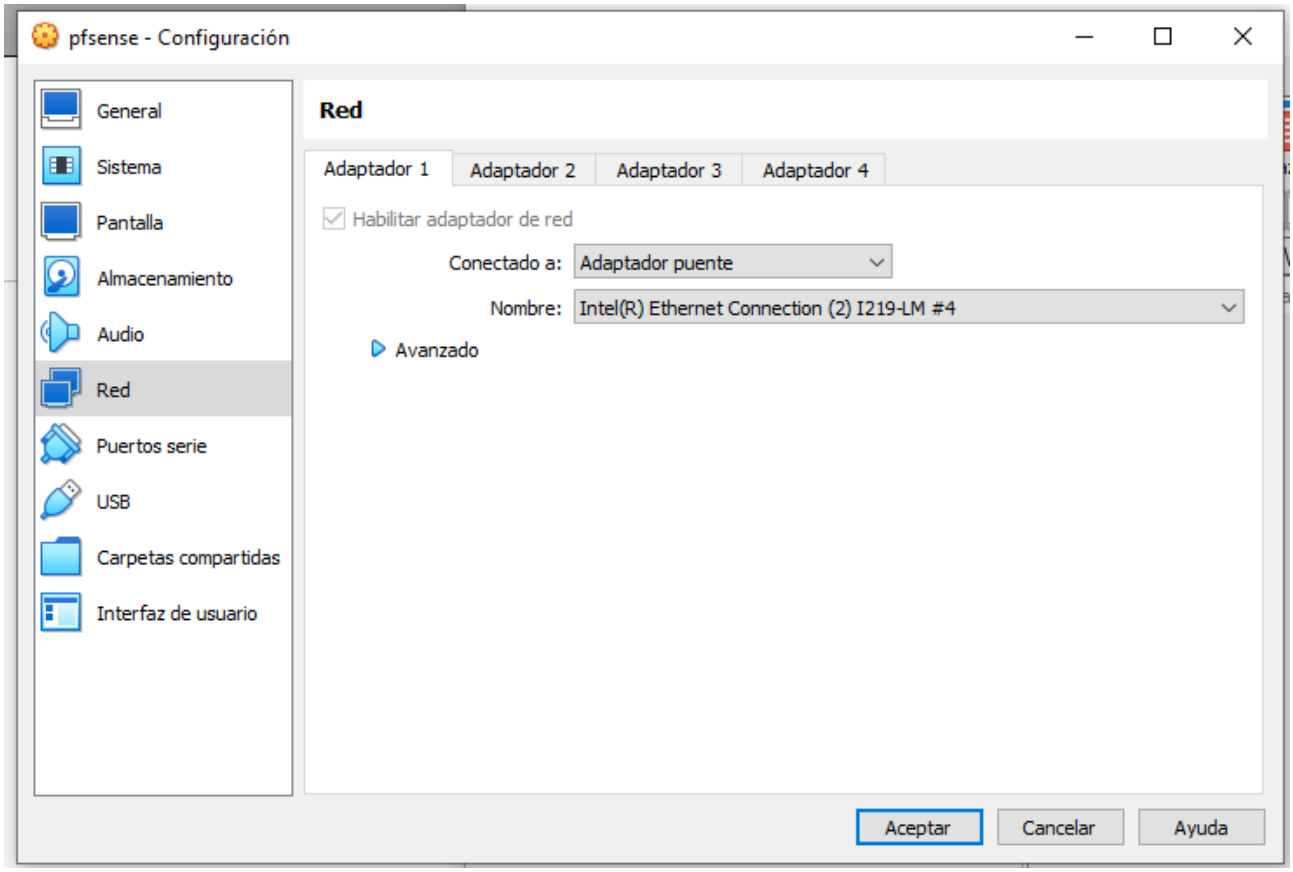
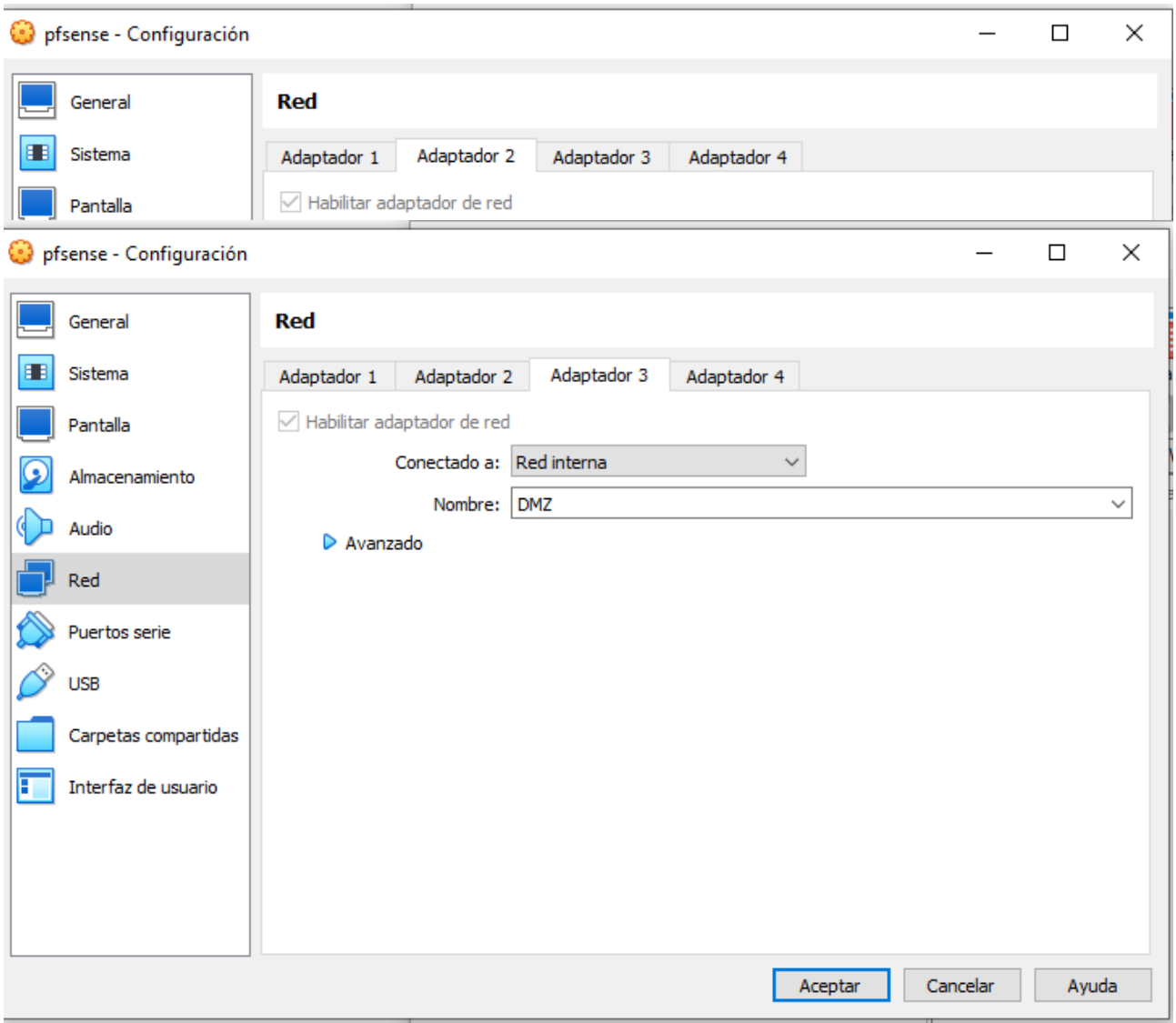
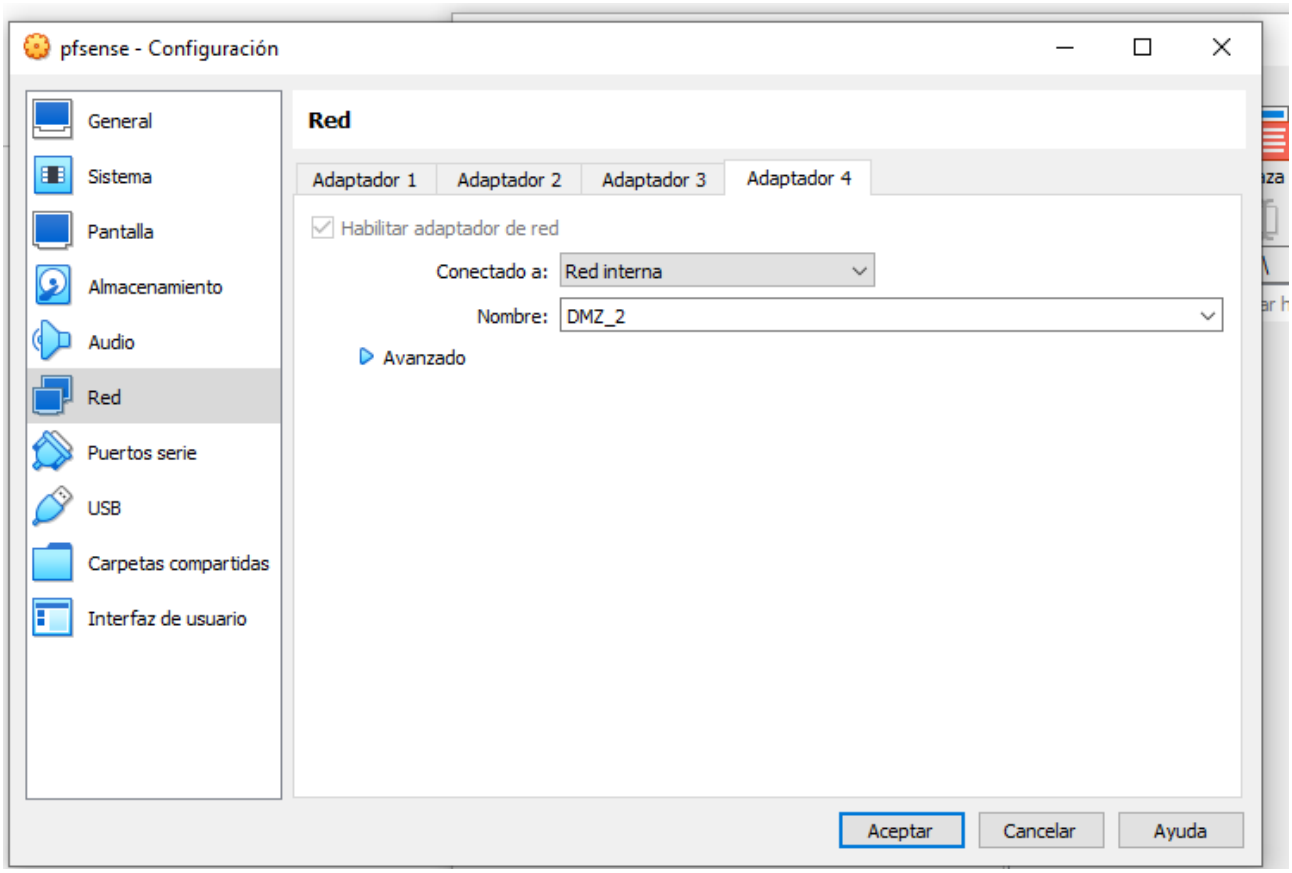
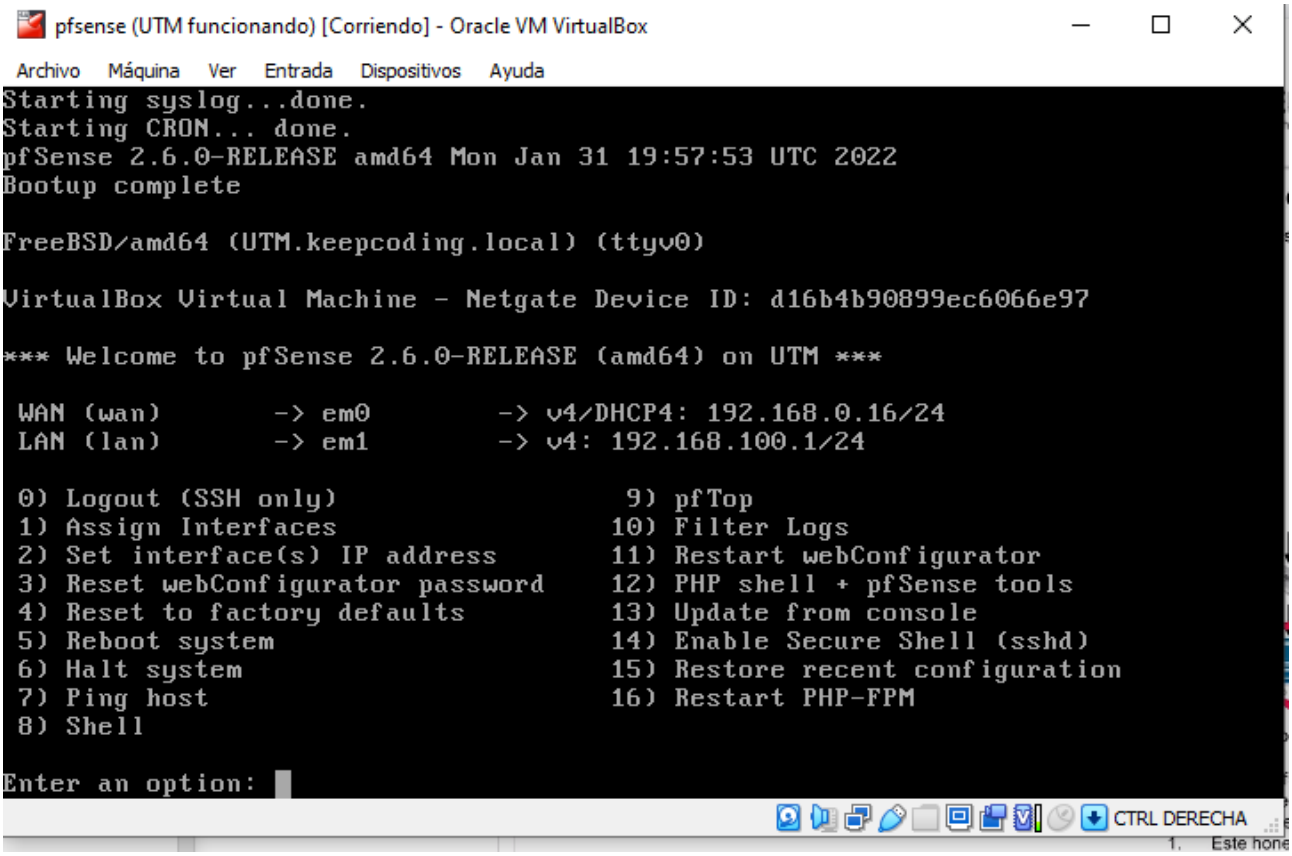
MONTAJE DE INFRAESTRUTURA



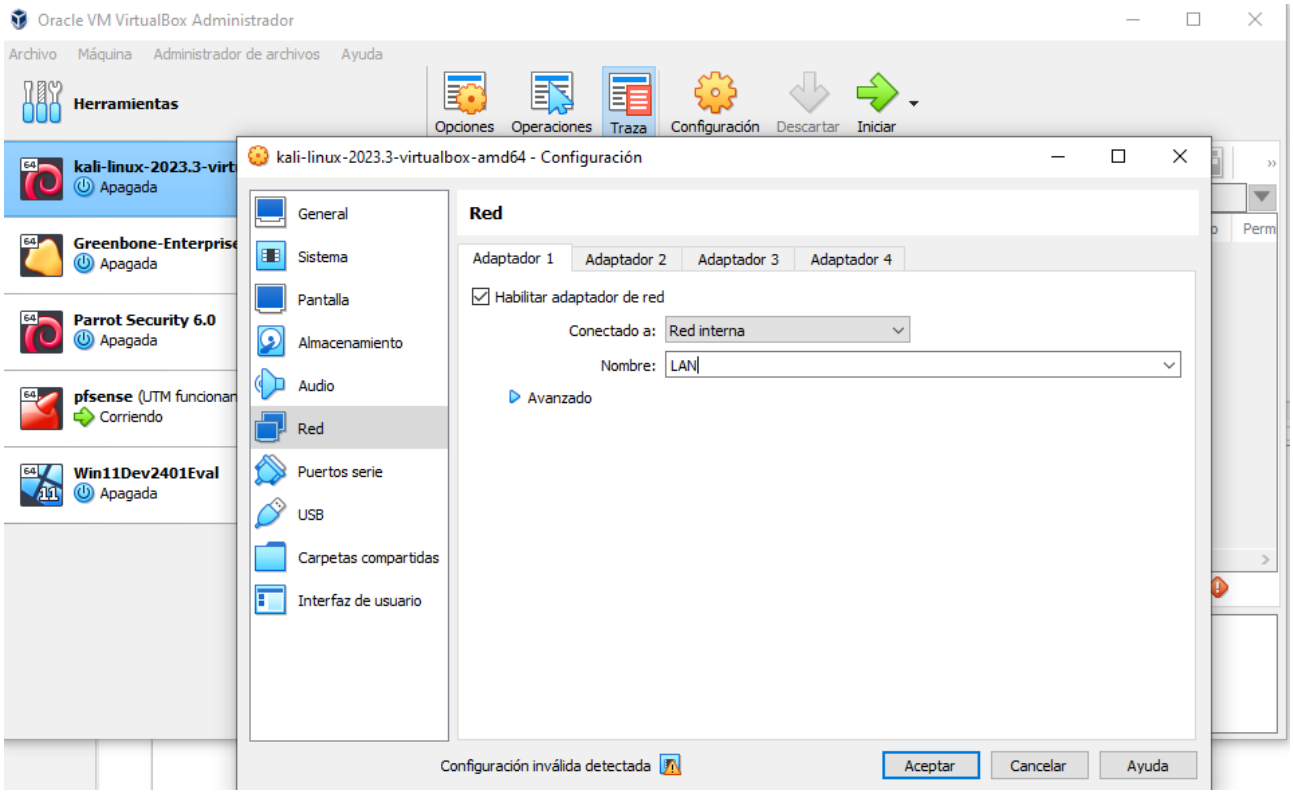




arrancamos la Unified Threat Management (UTM)

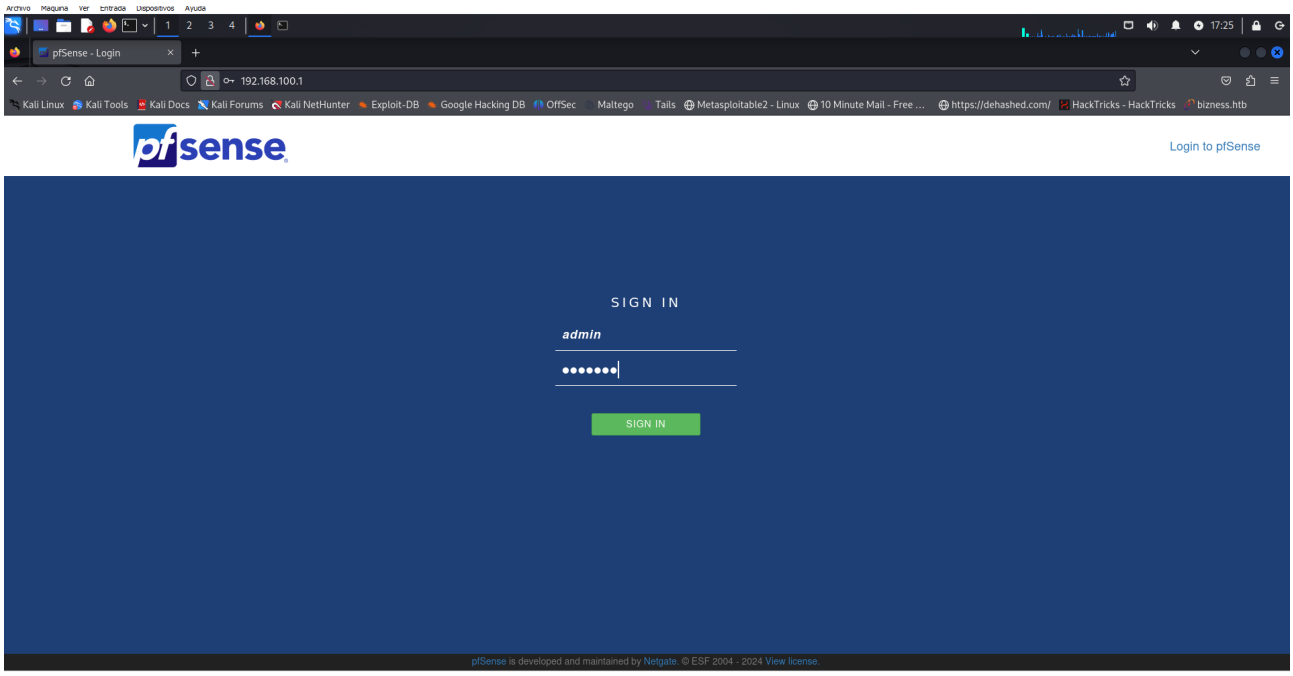


configuramos la kali en red interna LAN

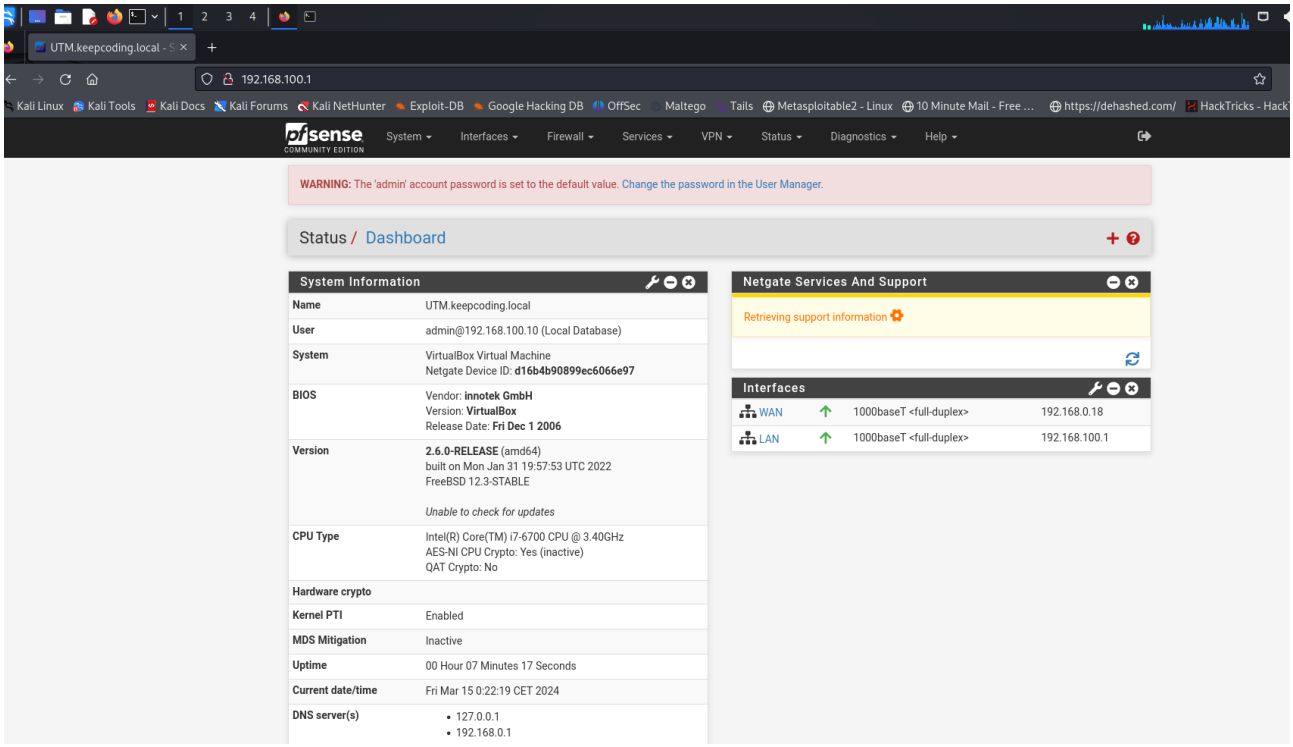


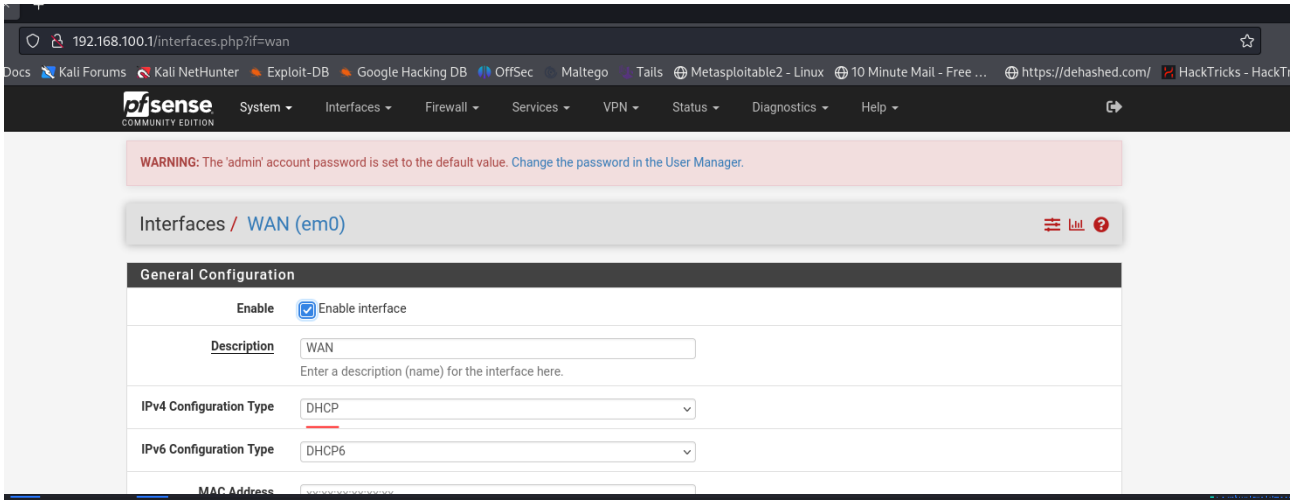
Arrancamos la kali e introducimos en el navegador la ip del adaptador LAN, en mi caso:

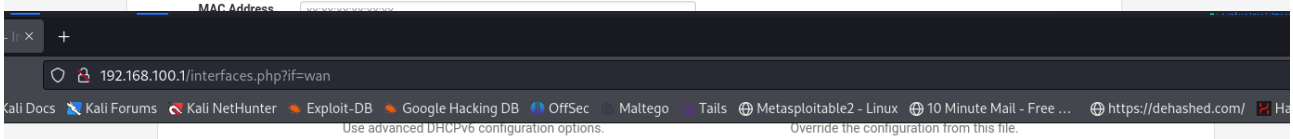
192.168.100.1



usuario admin, password pfsense







Use IPv4 connectivity as parent interface	☐ Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	☐ Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	64 The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.
Send IPv6 prefix hint	☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	☐ Start DHCP6 client in debug mode
Do not wait for a RA	☐ Required by some ISPs, especially those not using PPPoE
Do not allow PD/Address release	☐ dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

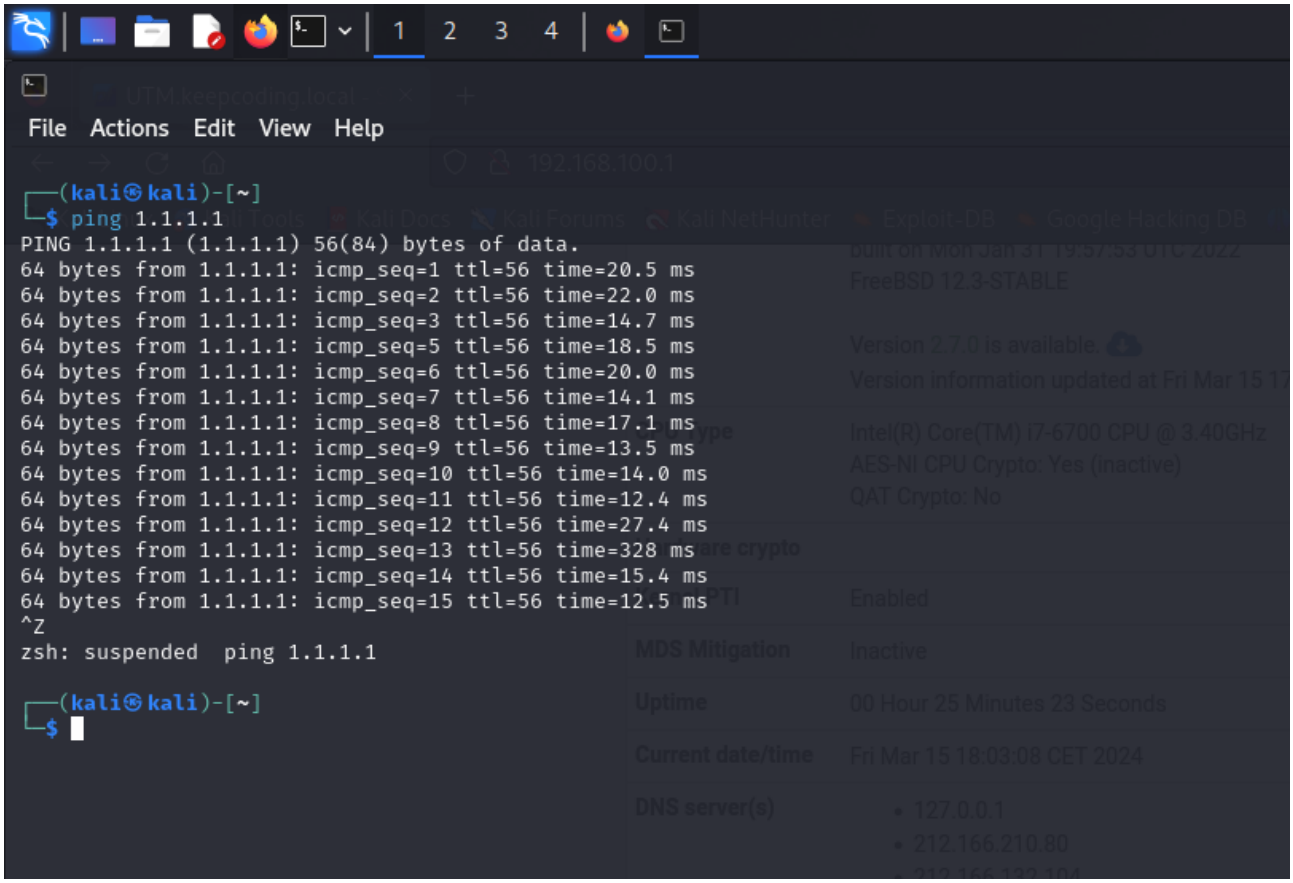
Reserved Networks

Block private networks and loopback addresses	☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	☐ Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

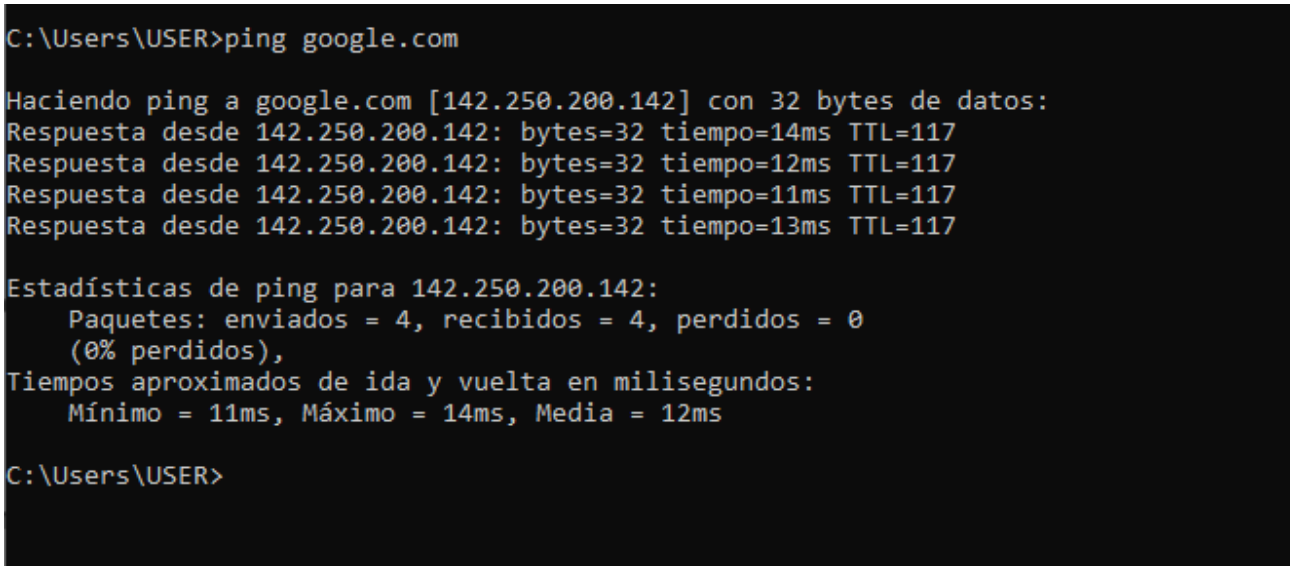
Save

CONFIGURACIÓN DE LAS INTERFACES

Comprobamos si tenemos accesos a internet en la kali haciendo un ping a 1.1.1.1:



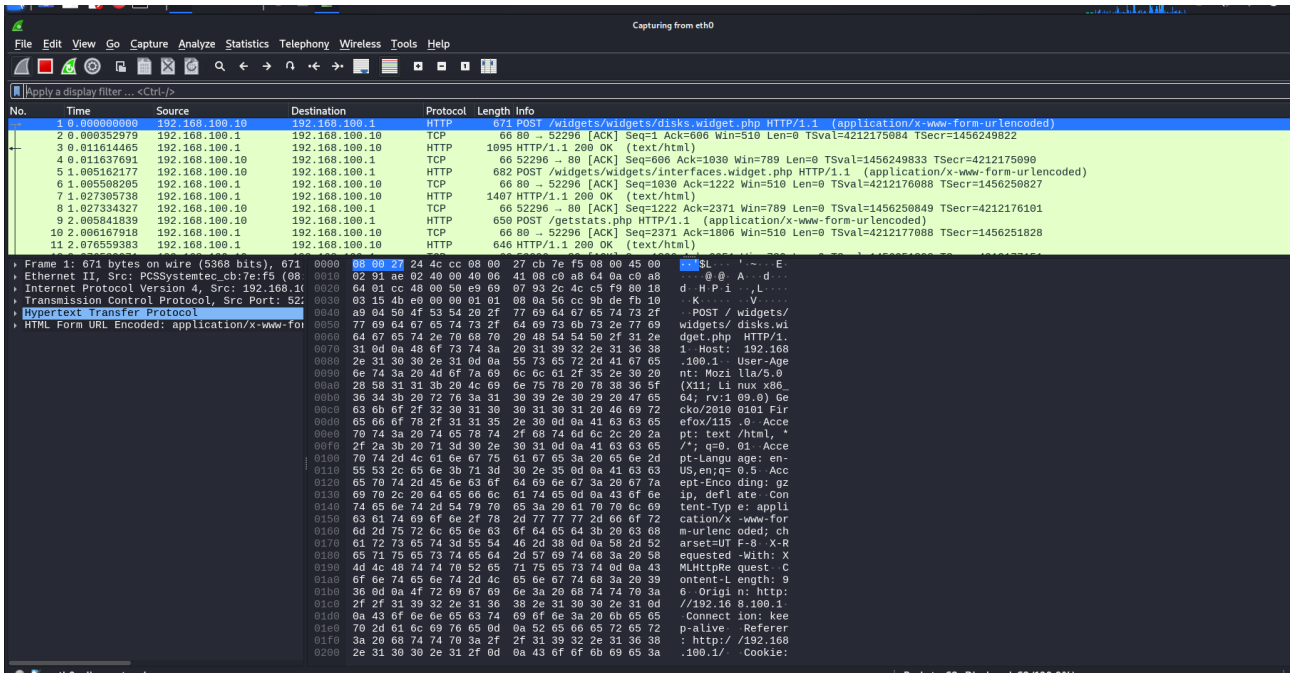
hacemos ping en nuestro sistema windows a google.com



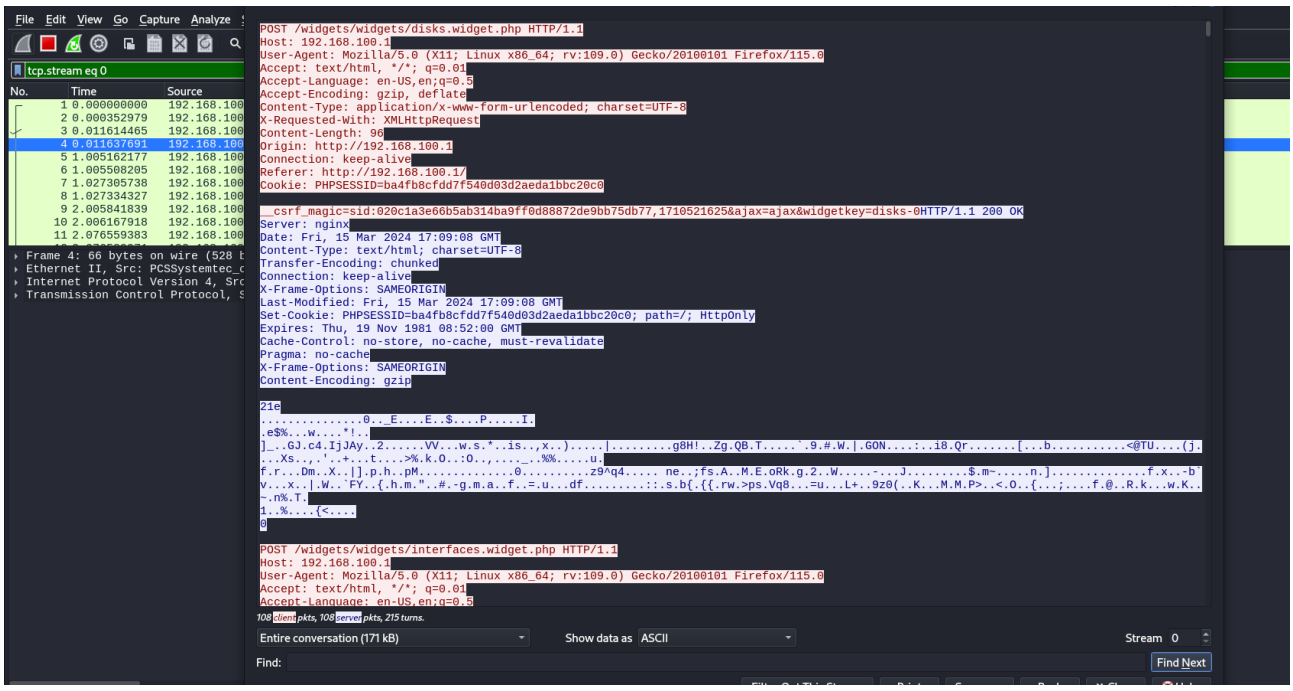
cogemos la ip y la pegamos en kali

```
┌──(kali㉿kali)-[~]
└─$ ping 142.250.200.142
PING 142.250.200.142 (142.250.200.142) 56(84) bytes of data.
64 bytes from 142.250.200.142: icmp_seq=1 ttl=116 time=19.3 ms
64 bytes from 142.250.200.142: icmp_seq=2 ttl=116 time=14.8 ms
64 bytes from 142.250.200.142: icmp_seq=3 ttl=116 time=20.9 ms
64 bytes from 142.250.200.142: icmp_seq=4 ttl=116 time=24.7 ms
64 bytes from 142.250.200.142: icmp_seq=5 ttl=116 time=16.2 ms
64 bytes from 142.250.200.142: icmp_seq=6 ttl=116 time=14.7 ms
64 bytes from 142.250.200.142: icmp_seq=7 ttl=116 time=13.6 ms
^Z
zsh: suspended  ping 142.250.200.142

┌──(kali㉿kali)-[~]
└─$
```

en wireshark podemos ver el tráfico que está pasando por la interface de red eth0:



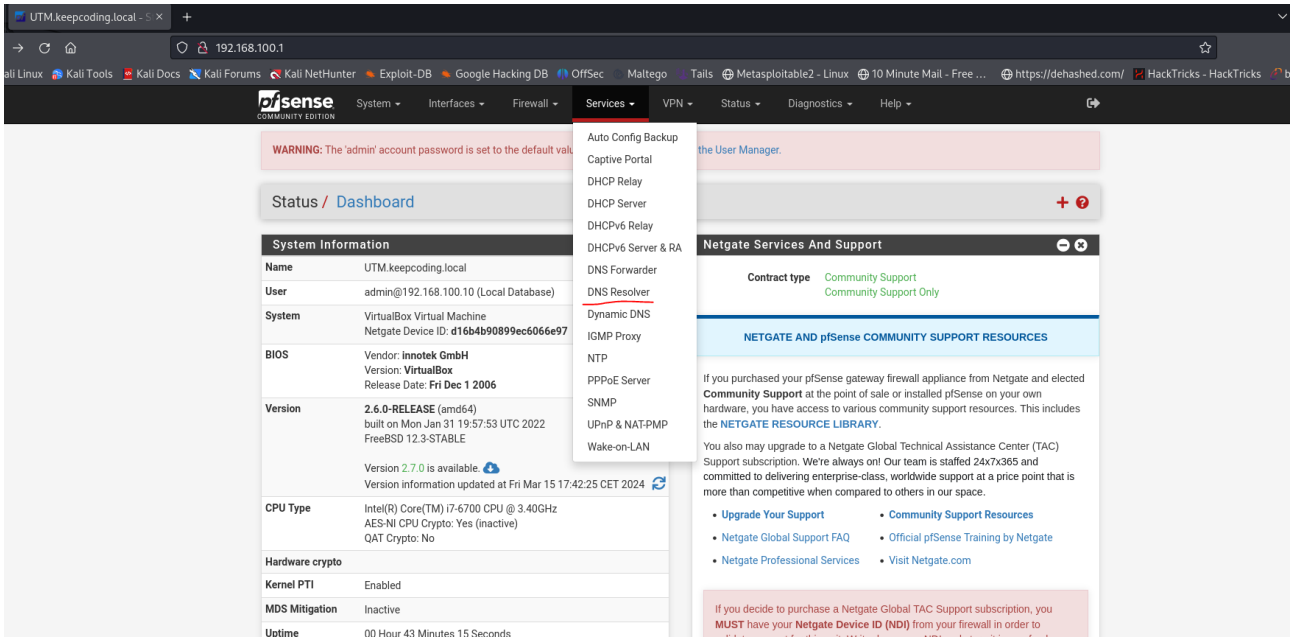
hacemos click botón derecho en alguna de las tramas, Follow y TCP Stream y vemos todos los paquetes del tráfico:



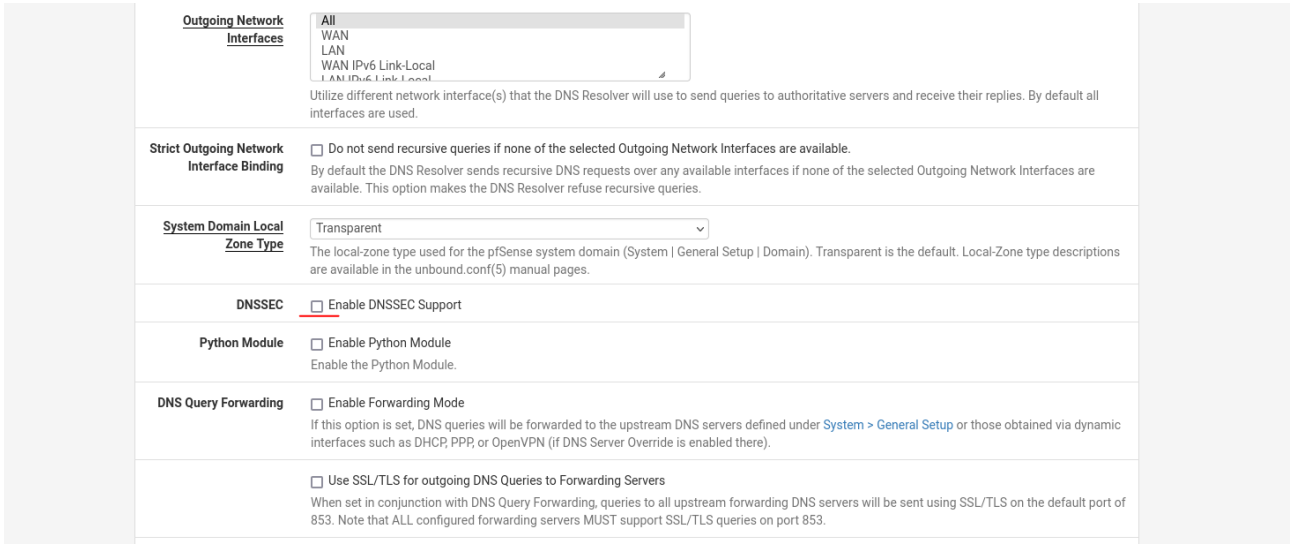
para ver la información del tráfico.

Configuramos el UTM:

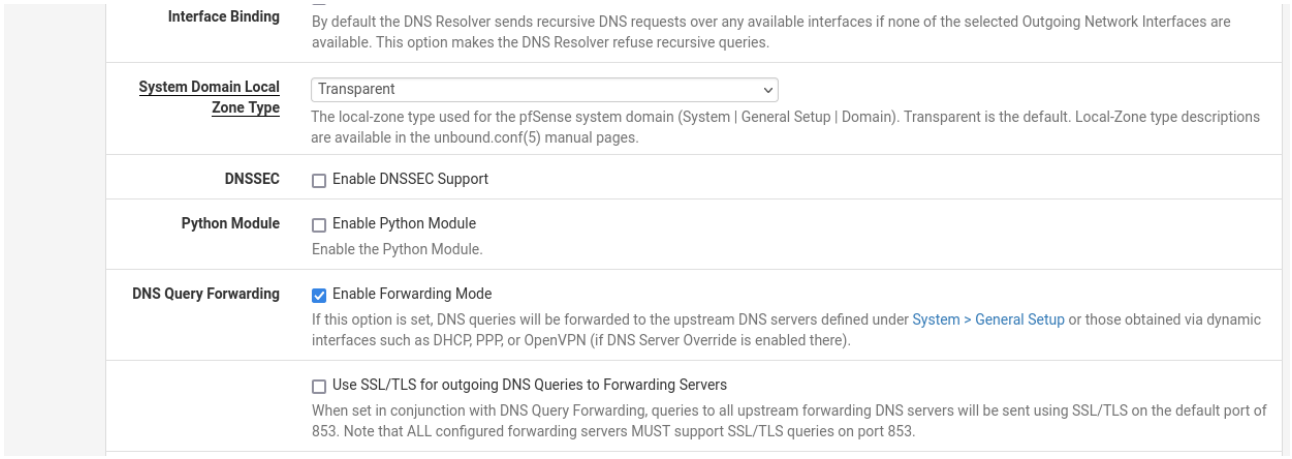
vamos a Services y DNS Resolver



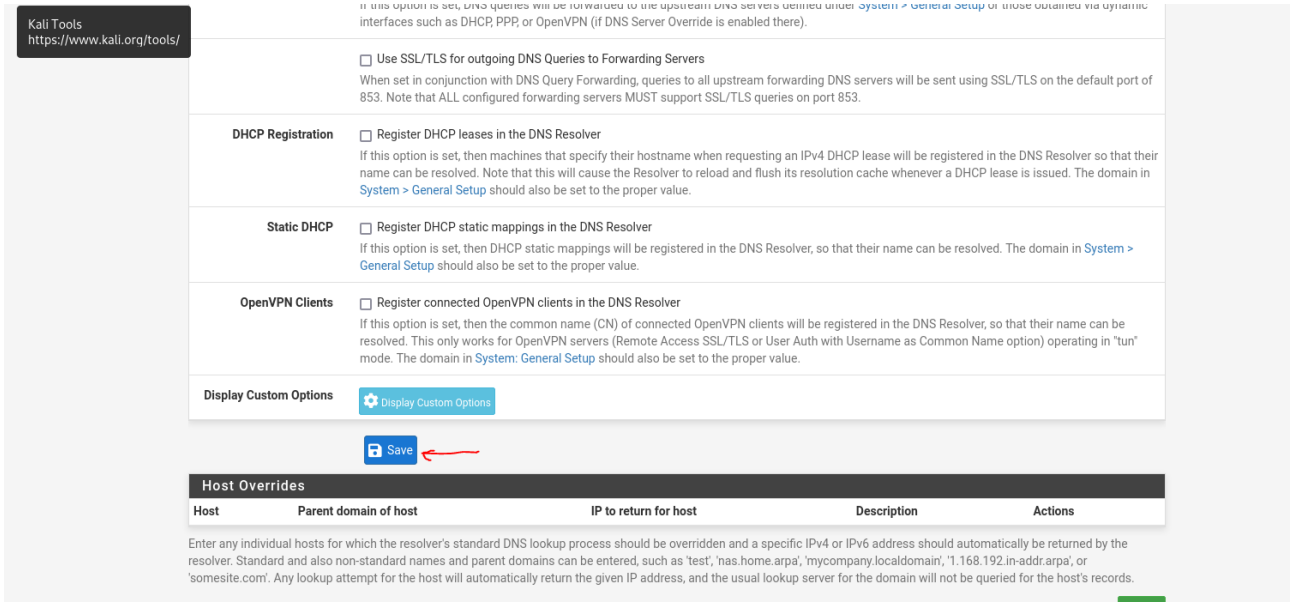
deschekamos el DNSSEC que es un protocolo utilizado para firmar la respuesta DNS (asegura que la respuesta no ha sido modificada):



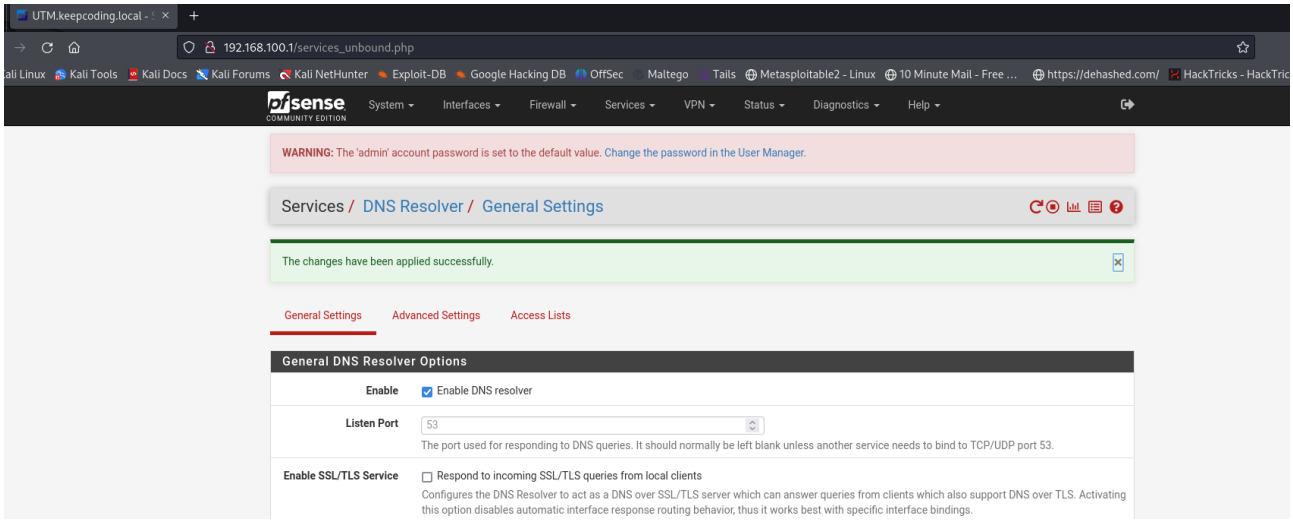
habilitamos el DNS Query Forwarding para enviar la consulta al servidor secundario el 1.1.1.1, en el caso de que PFSENSE no sea capaz de enviarla:



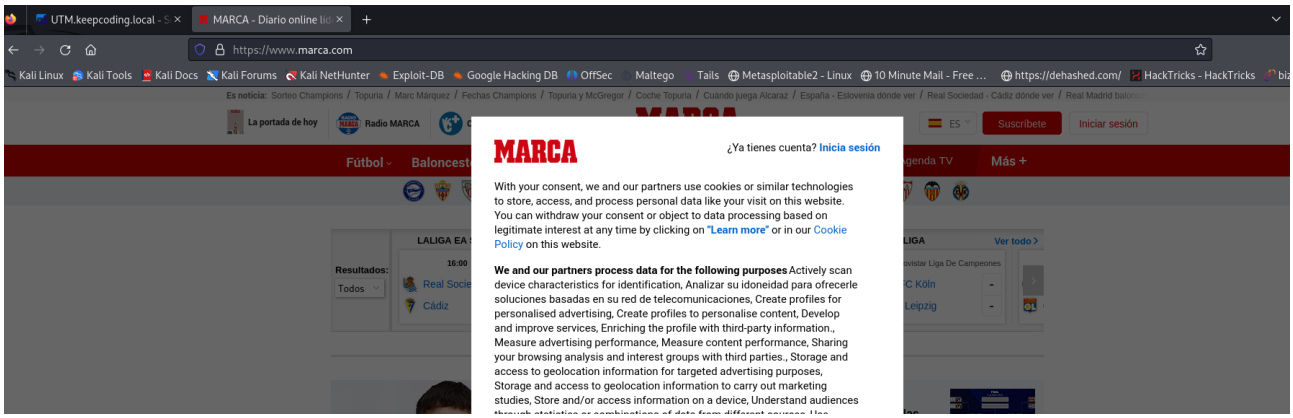
hacemos click en Save para guardar la configuración DNS:



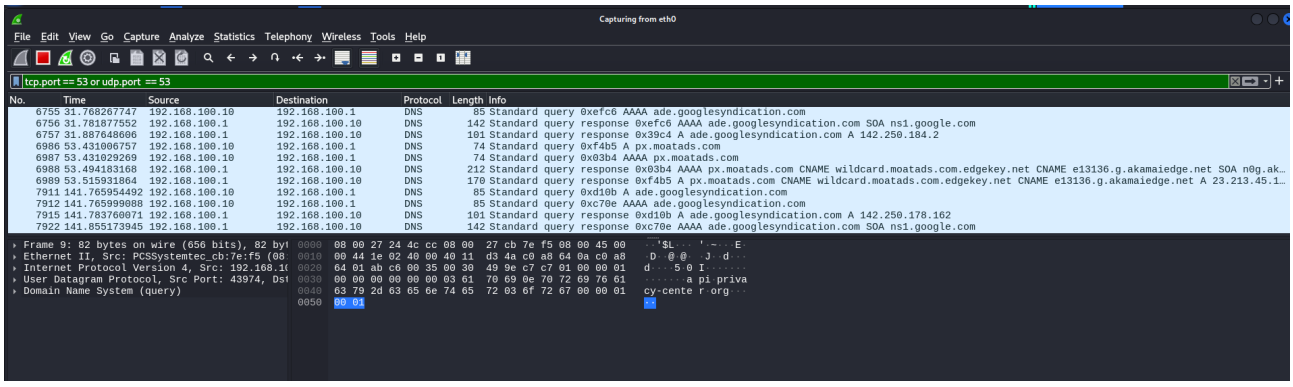
y damos a Apply Changes:



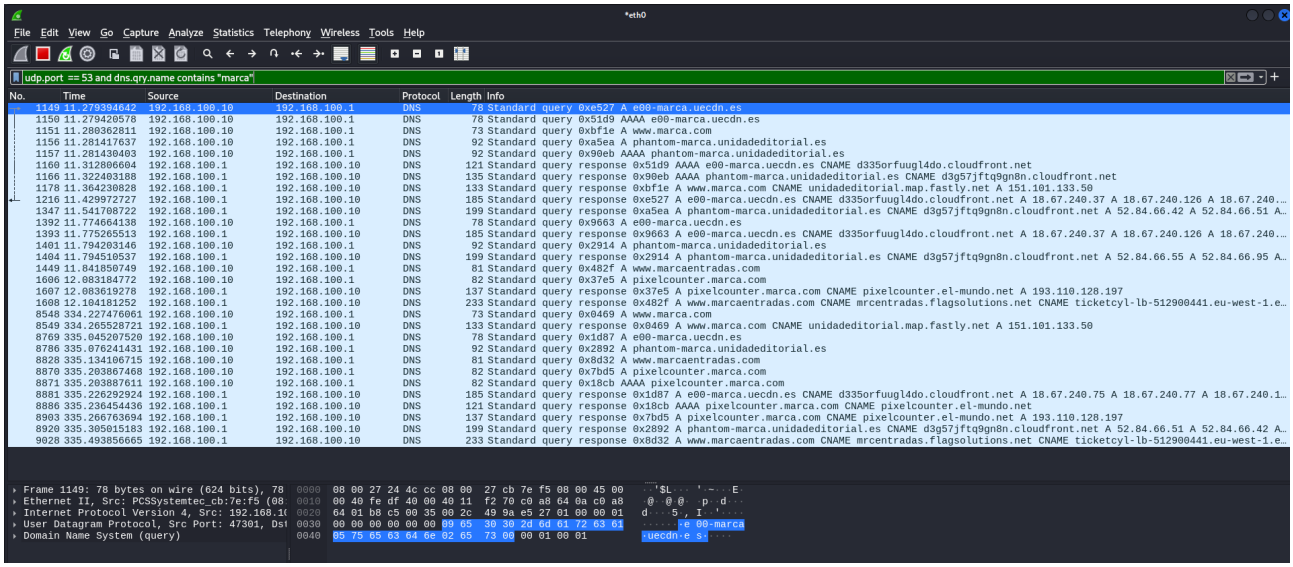
comprobamos en el navegador que tenemos acceso a marca.com



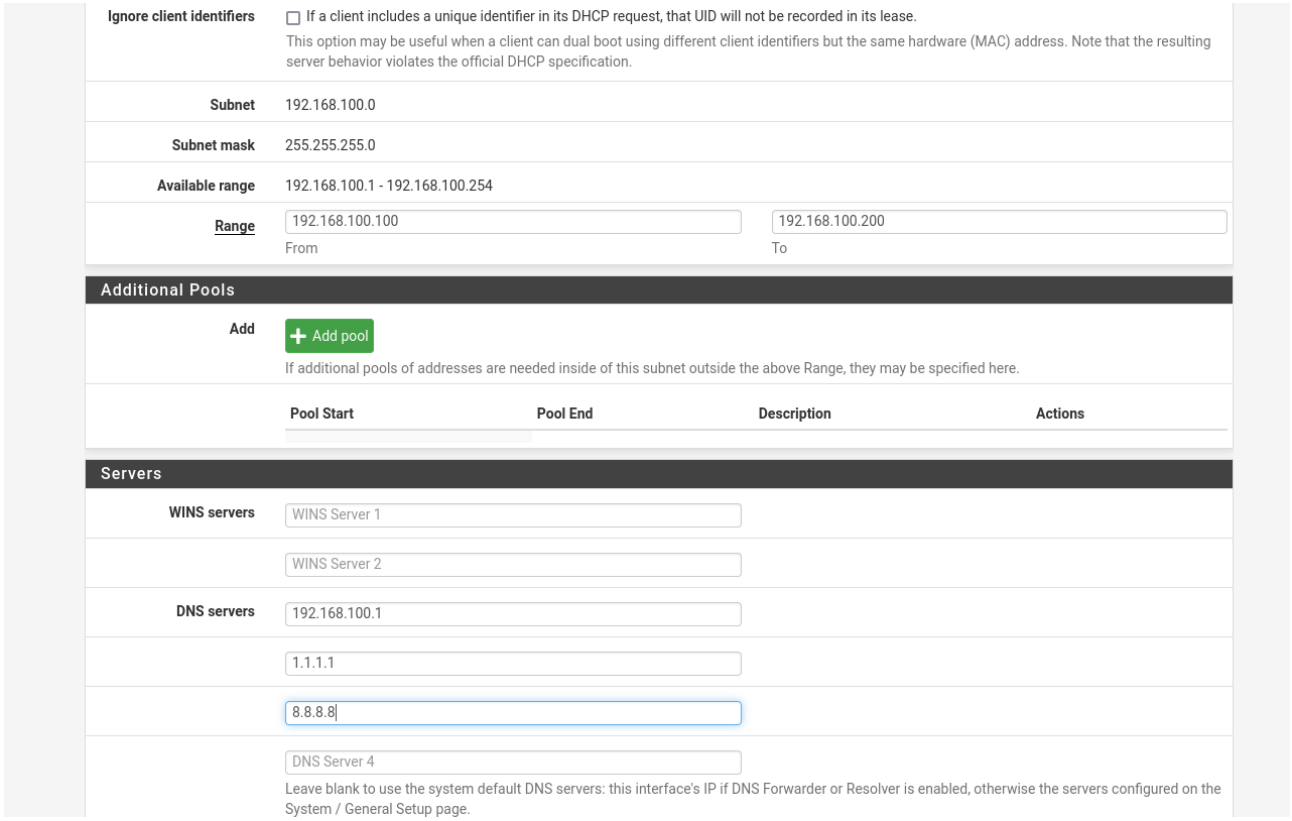
y vemos el tráfico en wireshark con el filtro tcp.port == 53 or udp.port == 53:



o con el filtro udp.port == 53 and qry.name contains “marca”



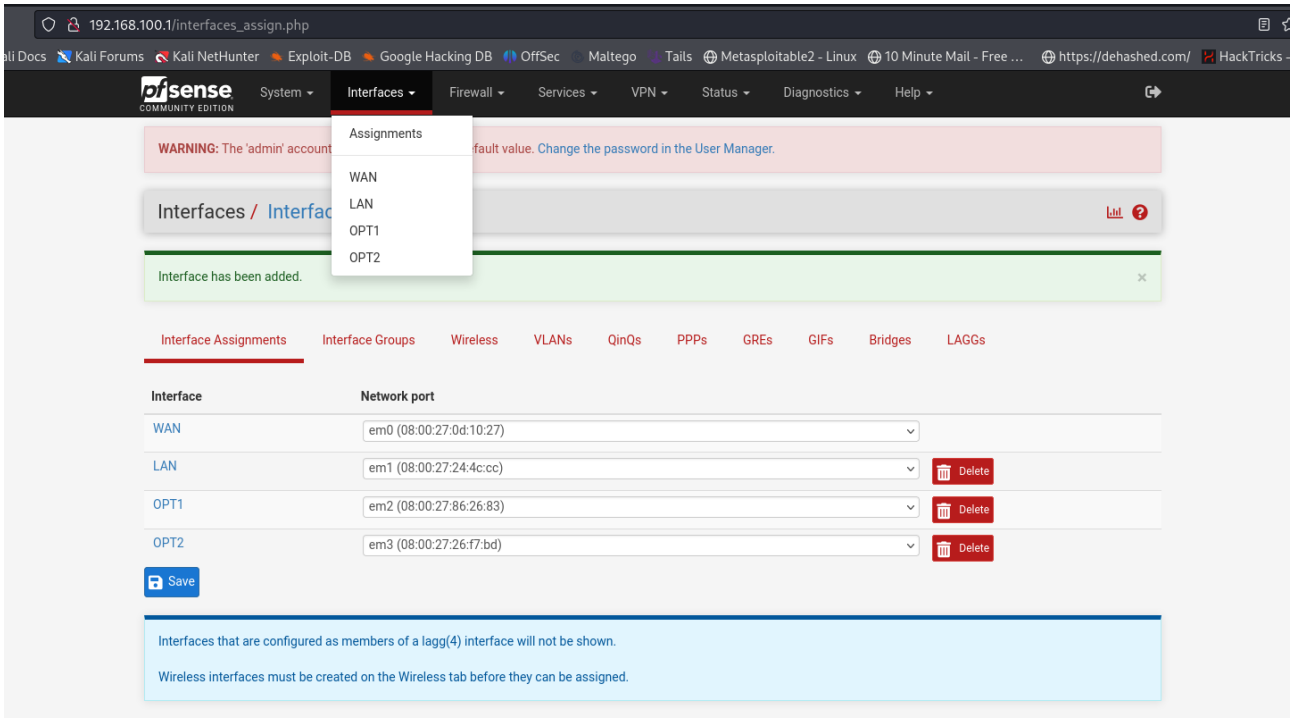
vemos todo el tráfico que interceptamos con pfsense hacia marca.com.
Configuramos el rang de ips en DHCP Server, desde la 192.168.100.100 hasta la 192.168.100.200 para conseguir la sured que hemos definido en el esquema, también configuramos un DNS secundario 1.1.1.1 y terciario 8.8.8.8 (google):

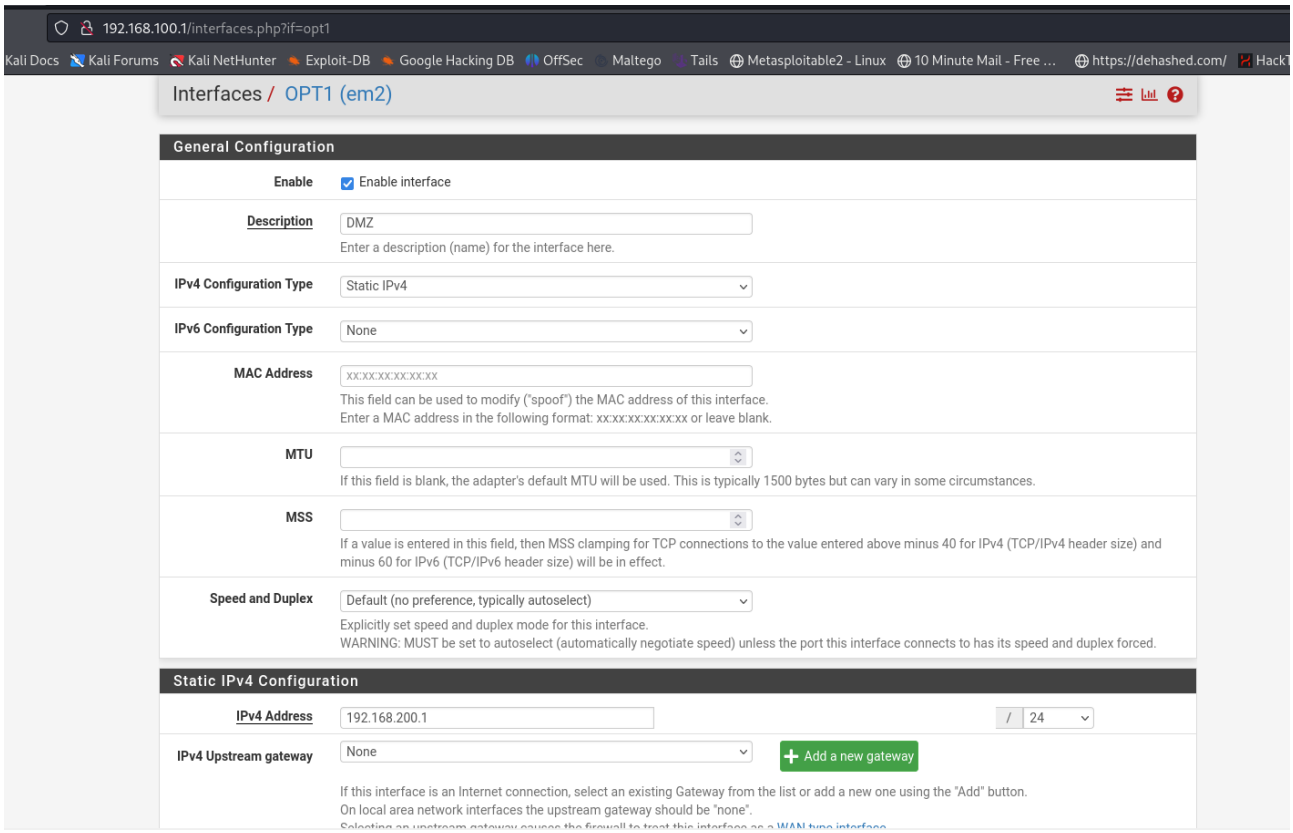


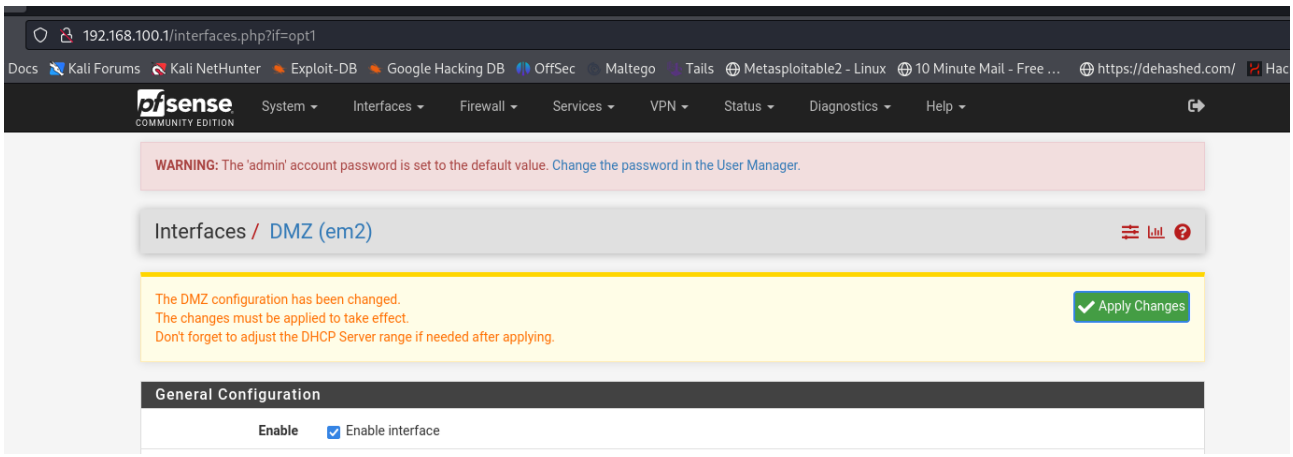
así tendría configurada la red LAN

Configuración de DMZ y DMZ2:

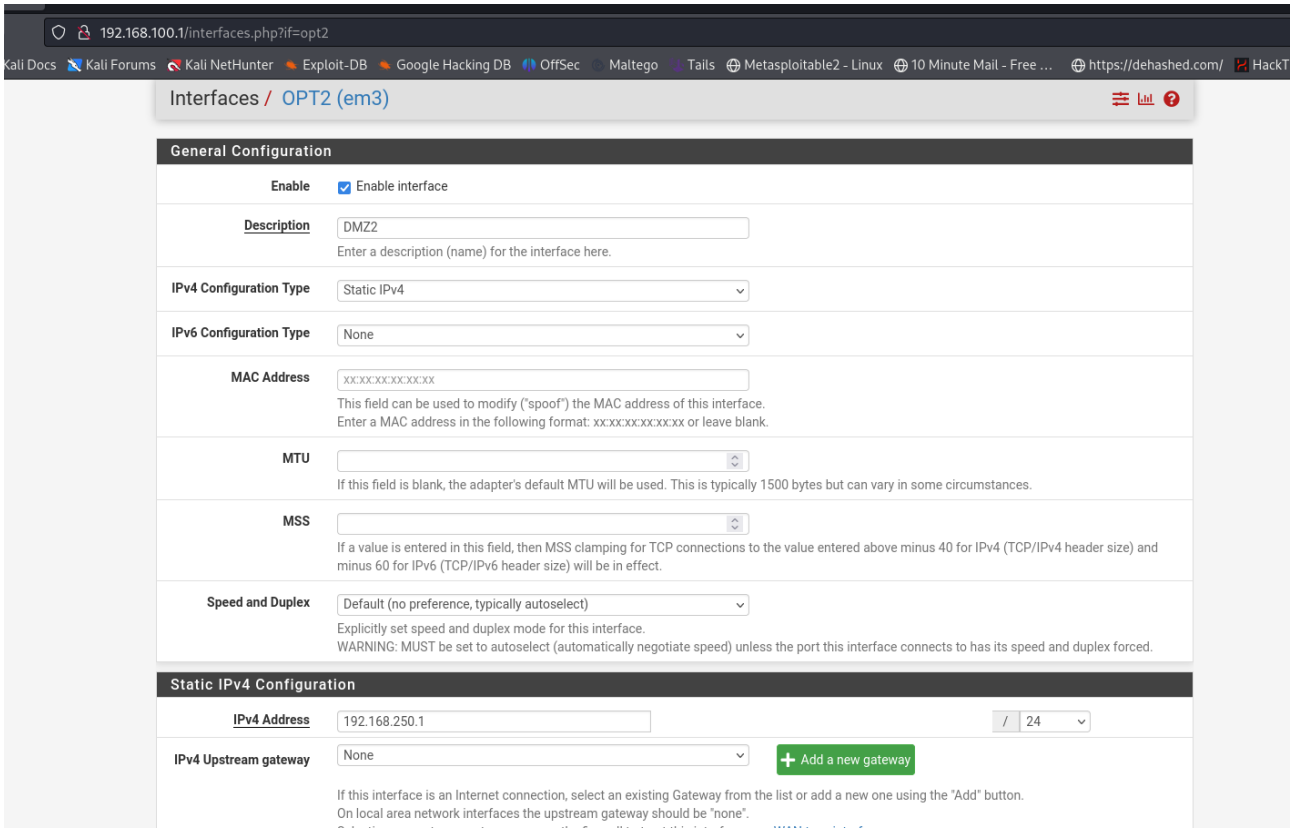
Vamos a Interfaces – Assignments y añadimos, nos saldrán OPT1 y OPT2:

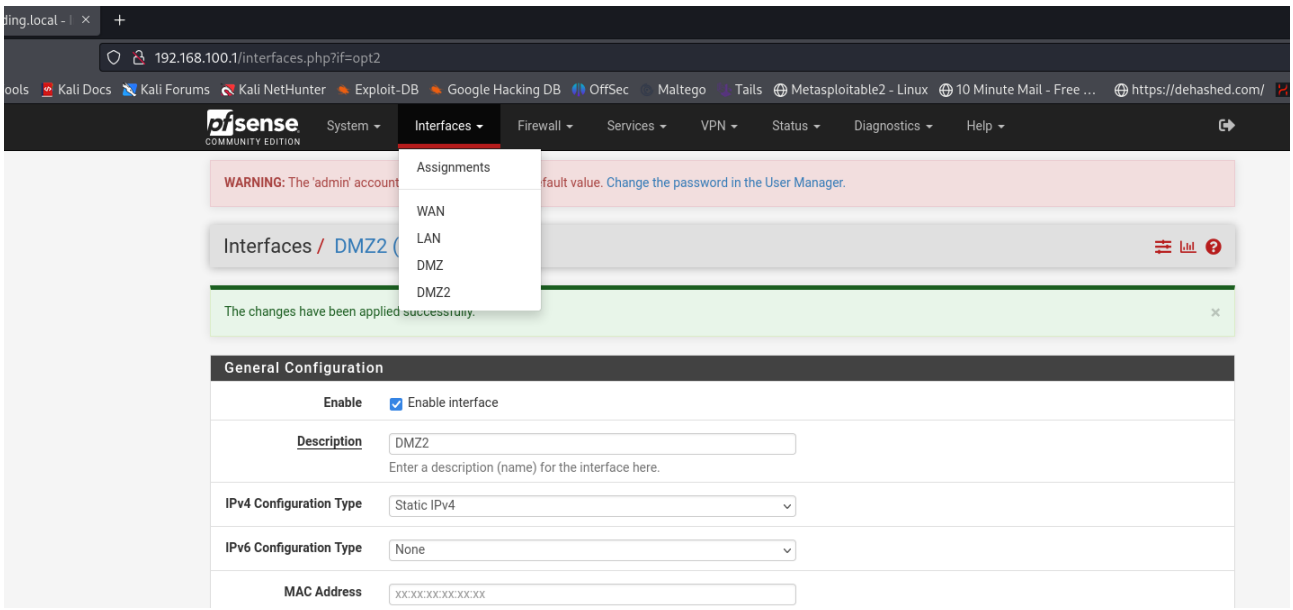

192.168.100.1/interfaces_assign.php
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego
Tails
Metasploitable2 - Linux
10 Minute Mail - Free ...
https://dehashed.com/
HackTricks
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
WAN
LAN
OPT1
OPT2
WARNING: The 'admin' account
fault value. Change the password in the User Manager.
Interfaces / Interfac
Interface has been added.
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (08:00:27:0d:10:27)
LAN
em1 (08:00:27:24:4c:cc)
Delete
OPT1
em2 (08:00:27:86:26:83)
Delete
OPT2
em3 (08:00:27:26:f7:bd)
Delete
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.


192.168.100.1/interfaces.php?if=opt1
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego
Tails
Metasploitable2 - Linux
10 Minute Mail - Free ...
https://dehashed.com/
Interfaces / OPT1 (em2)
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.200.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".

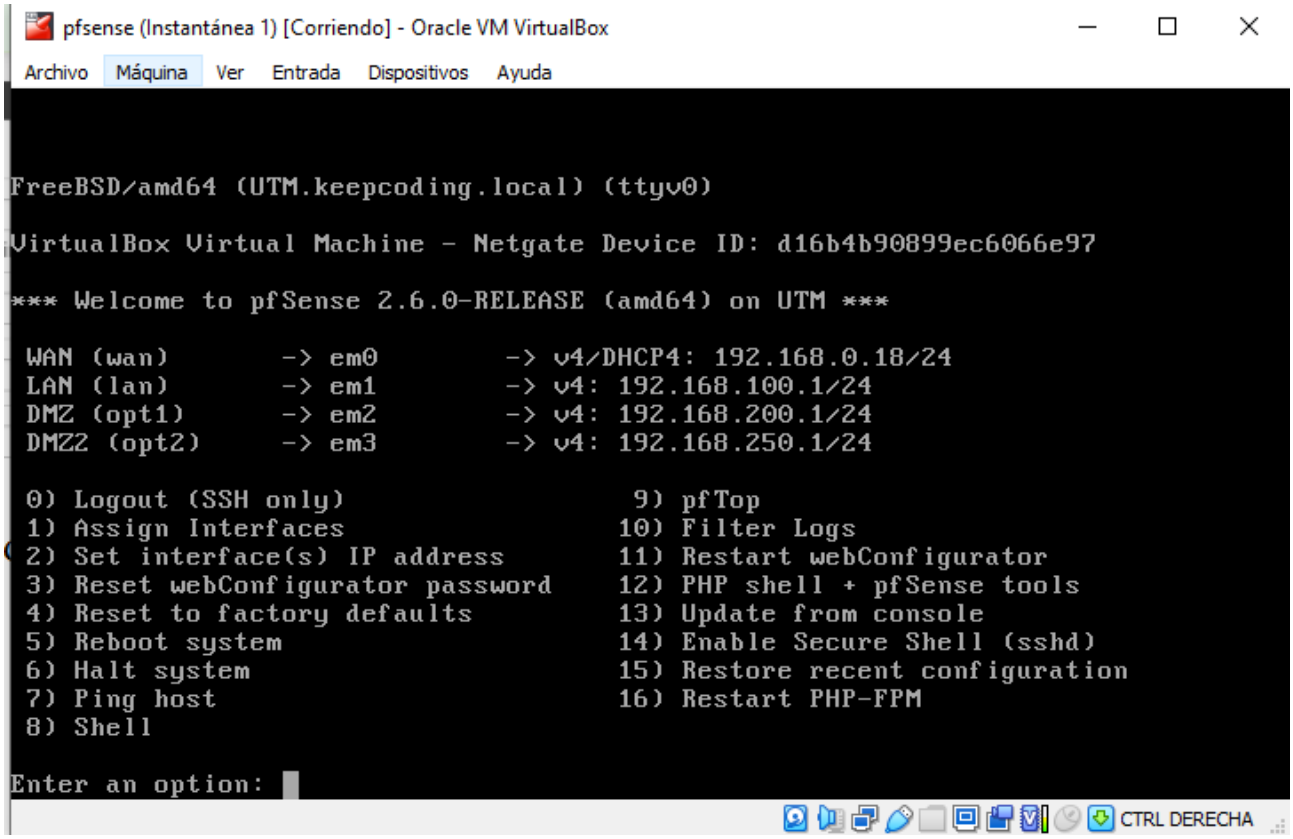


Configuramos la DMZ2:

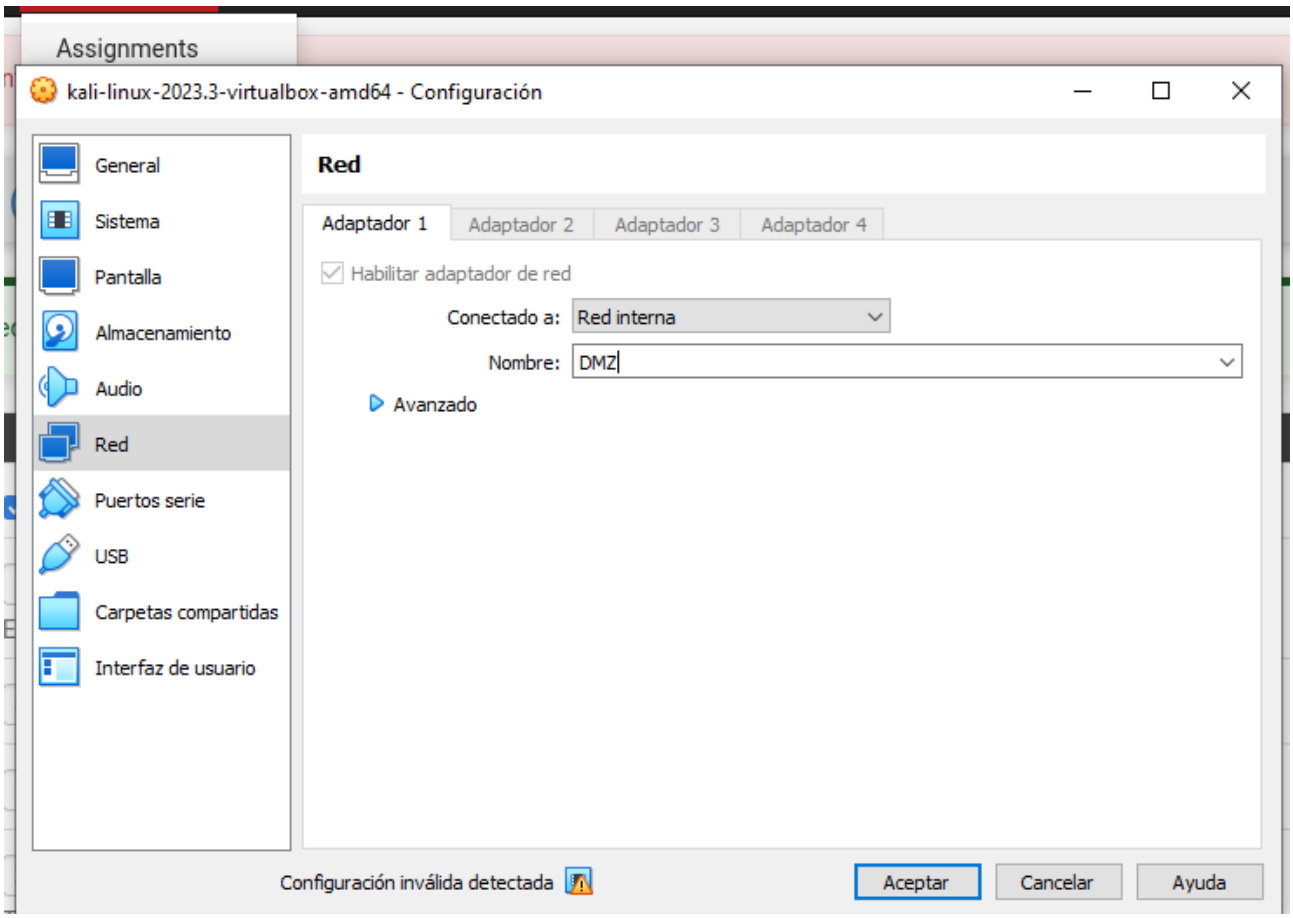




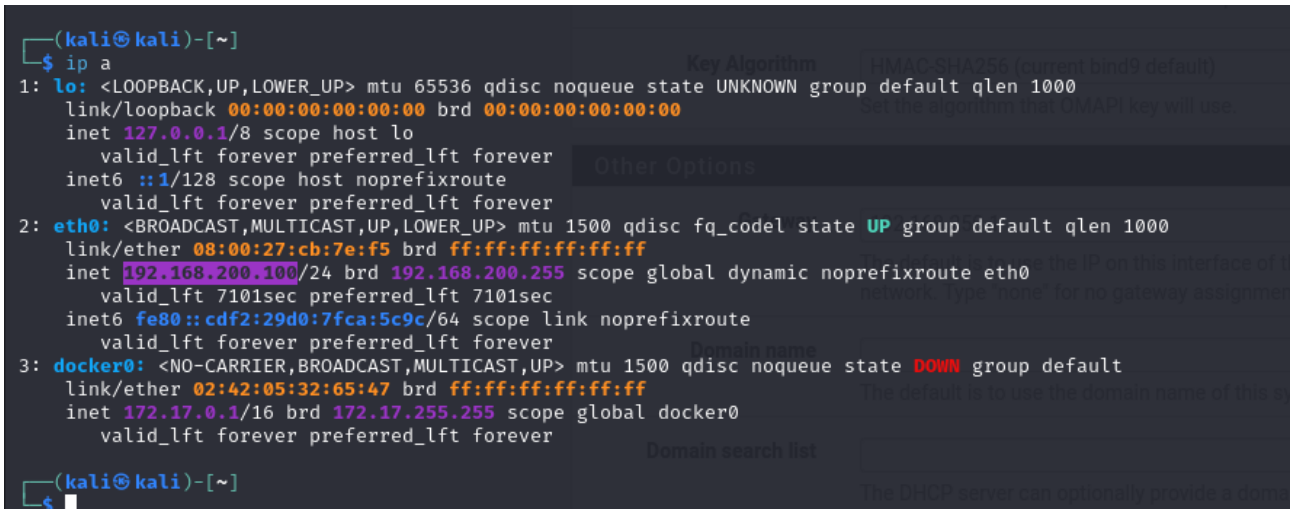
vamos a pfsense y comprobamos todas las redes configuradas:



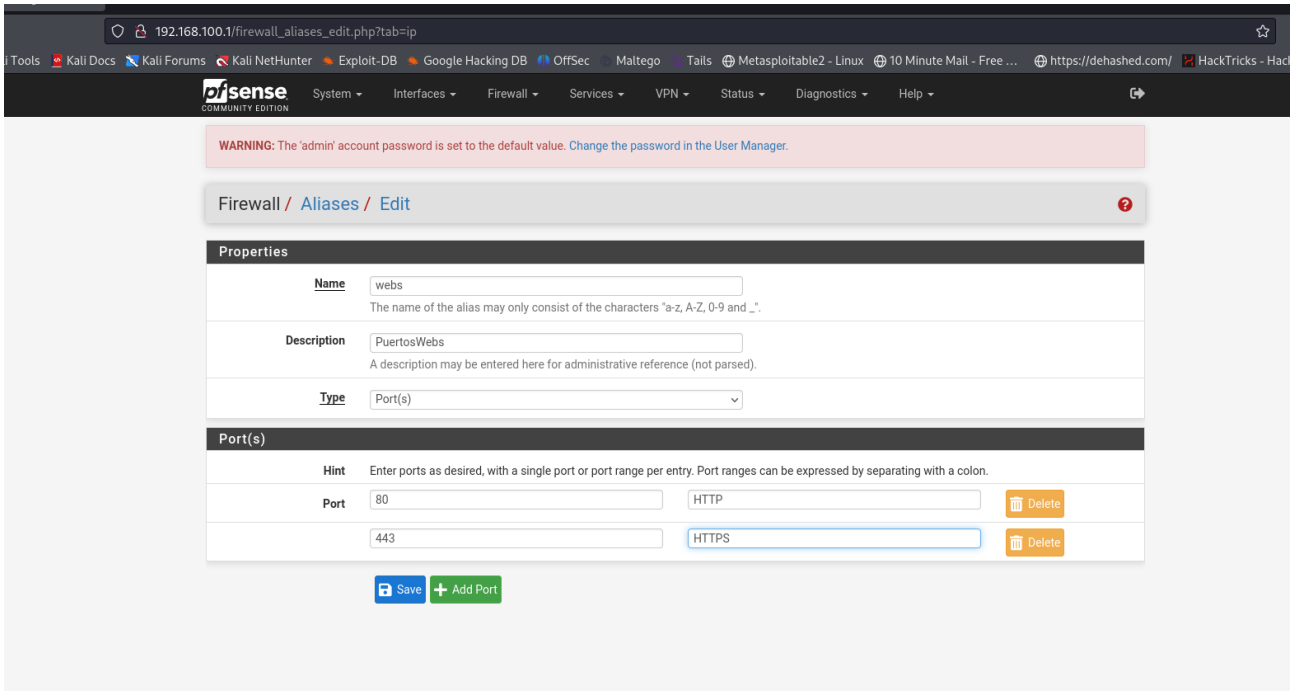
vamos a la kali y cambiamos la red LAN a DMZ



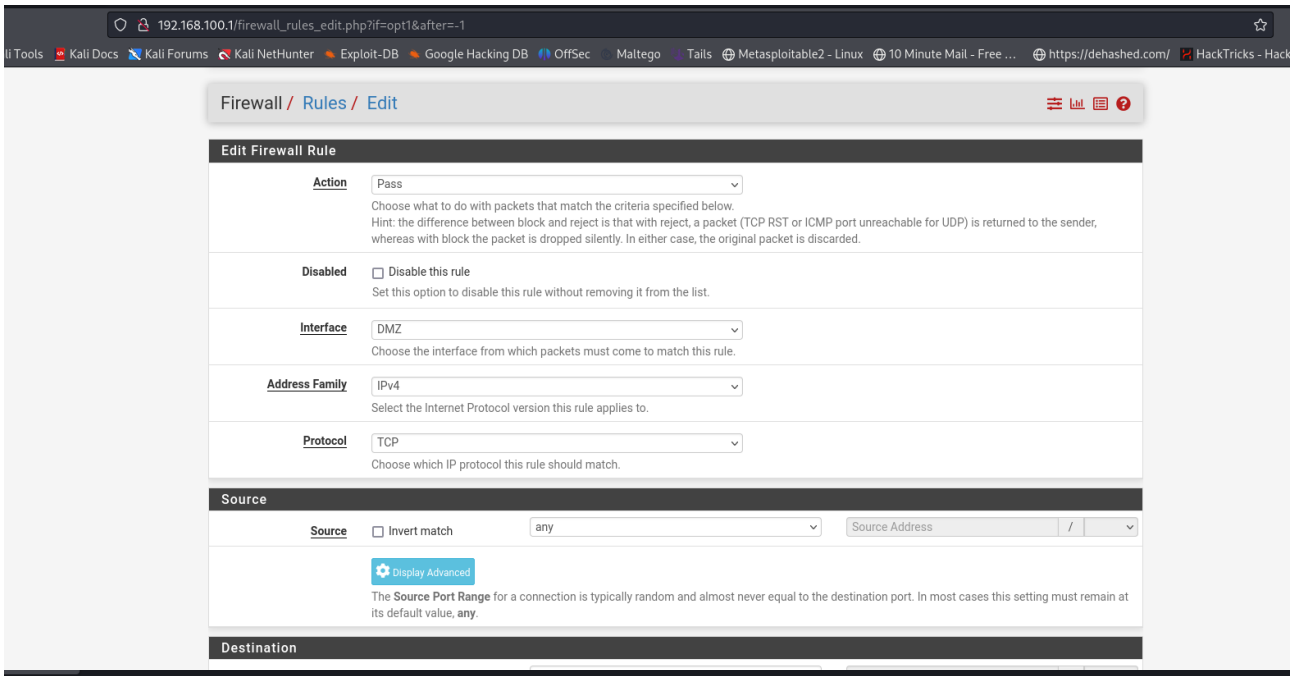
desconectamos el adaptador de red de la kali, lo volvemos a conectar y comprobamos en cmd, que ha cambiado la ip:

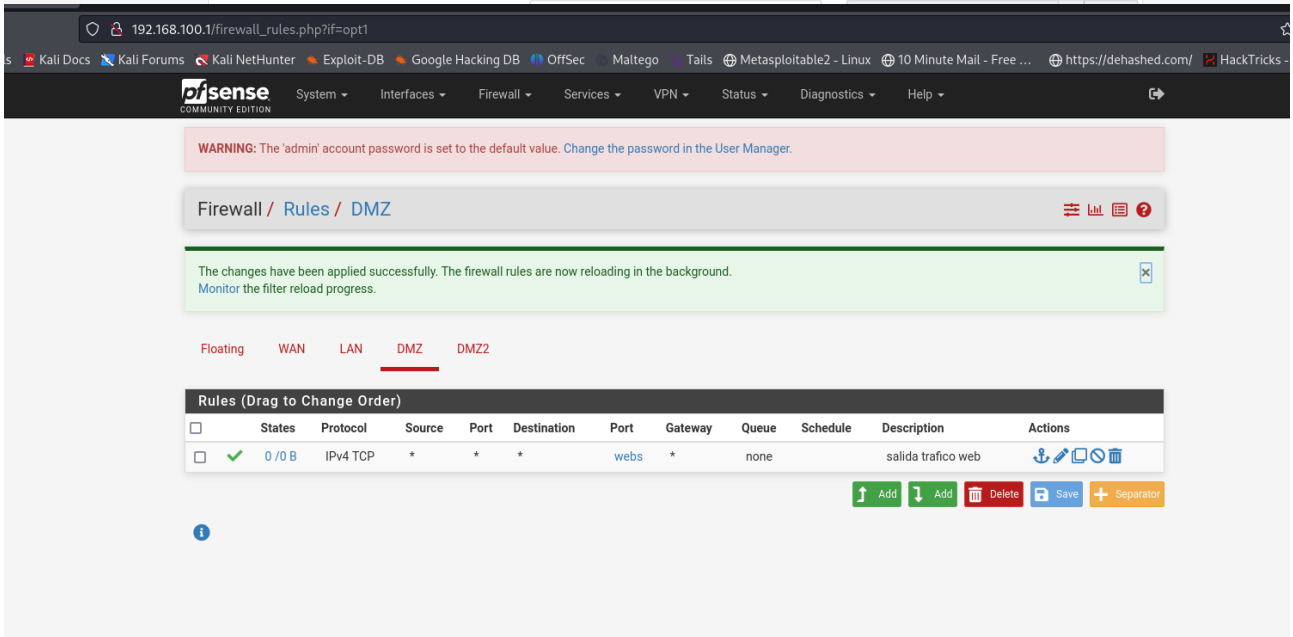


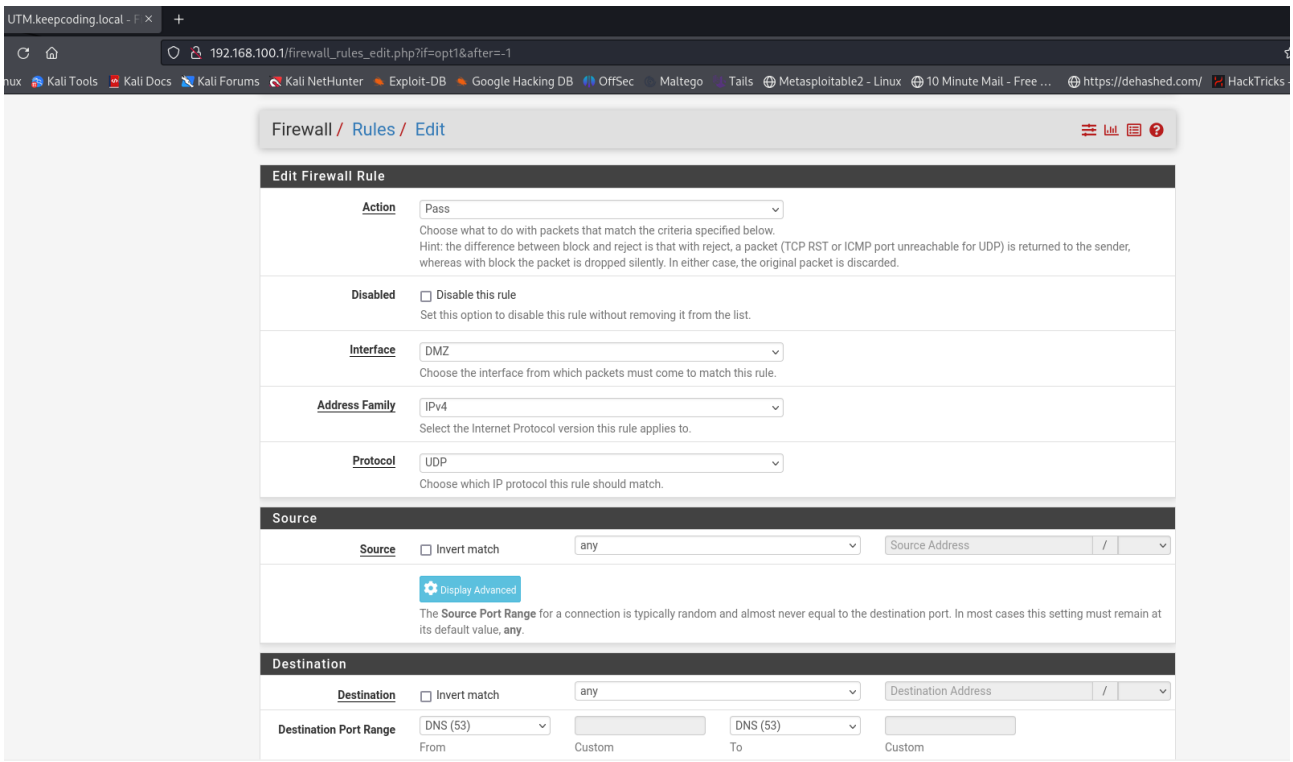
Para configurar las reglas, primero configuramos alias y puertos para el firewall

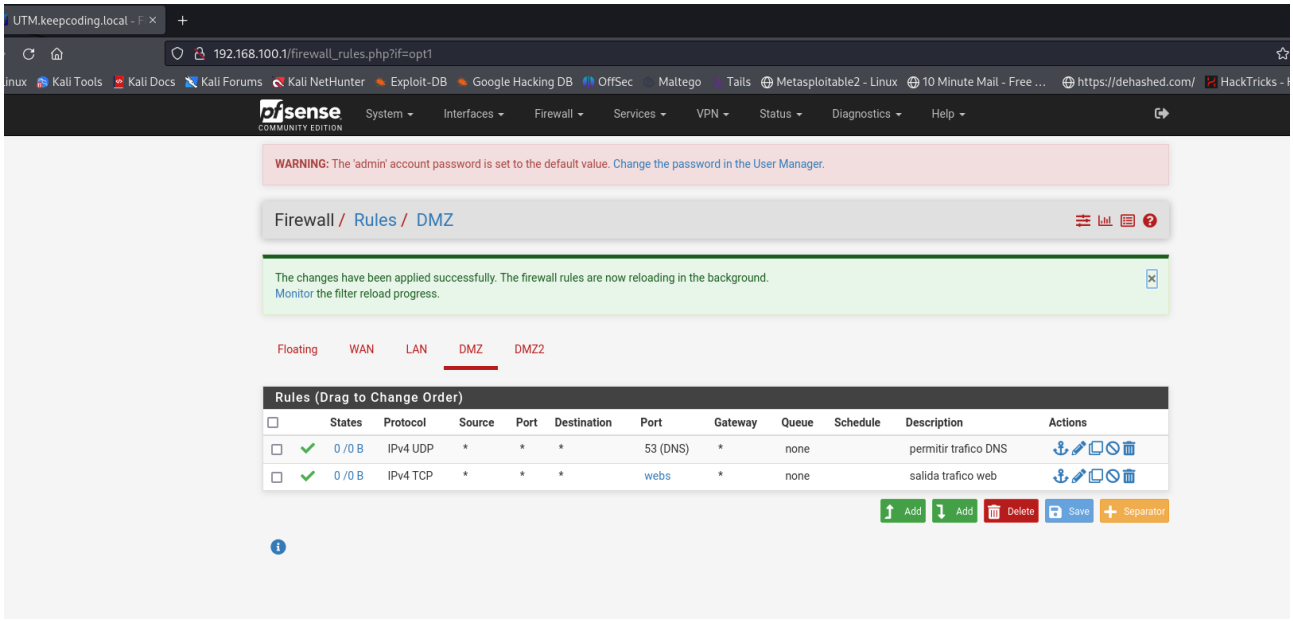


Creamos la reglas

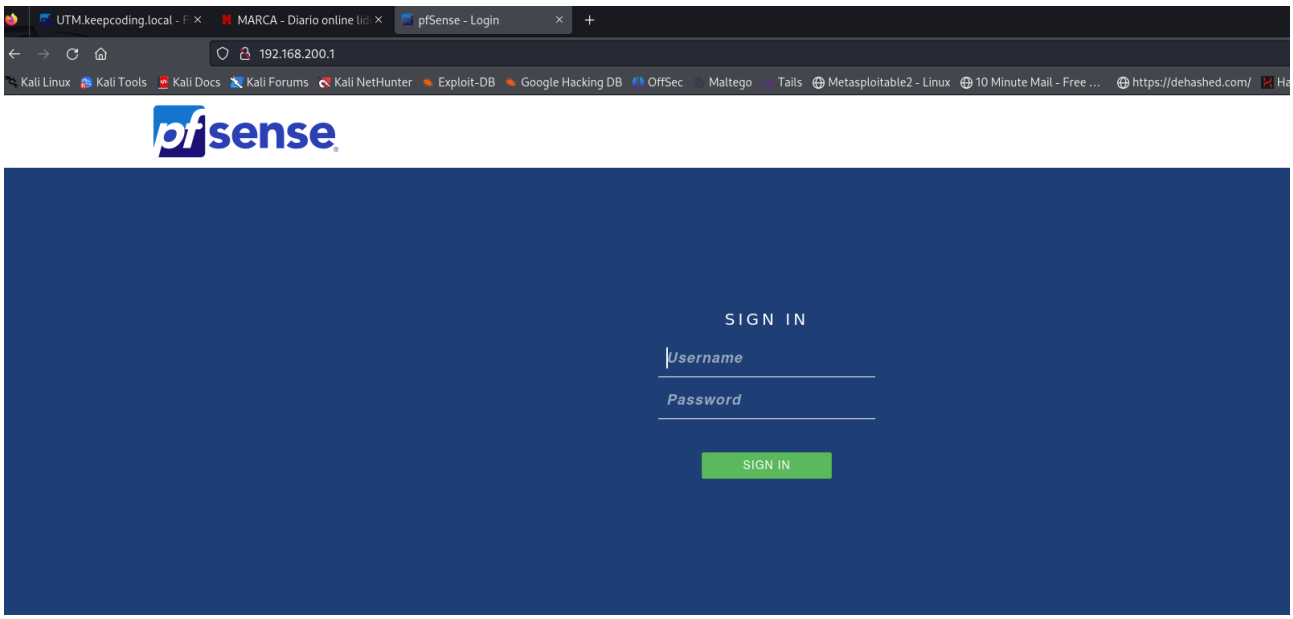




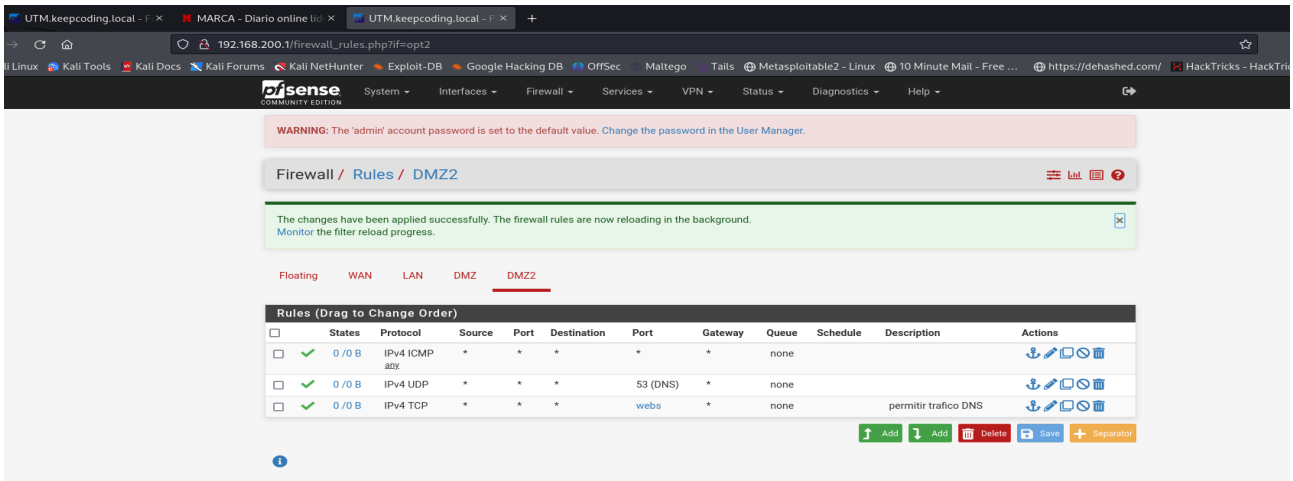




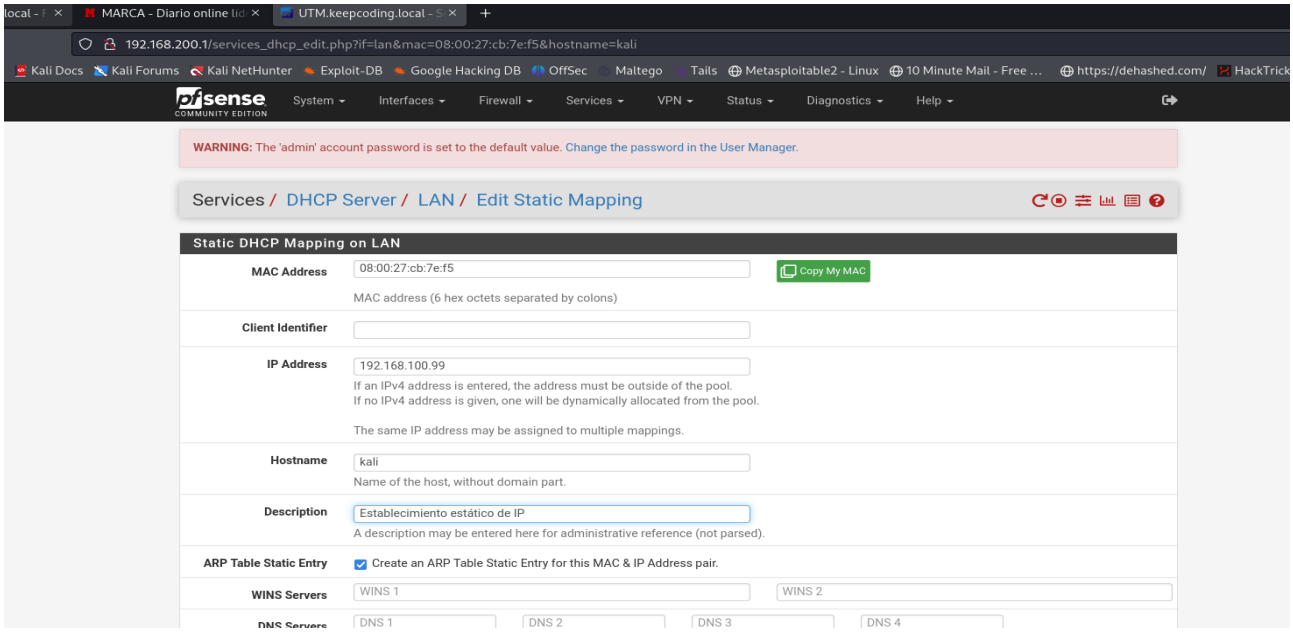
cambiamos a LAN en la kali, y comprobamos que tenemos acceso a internet:



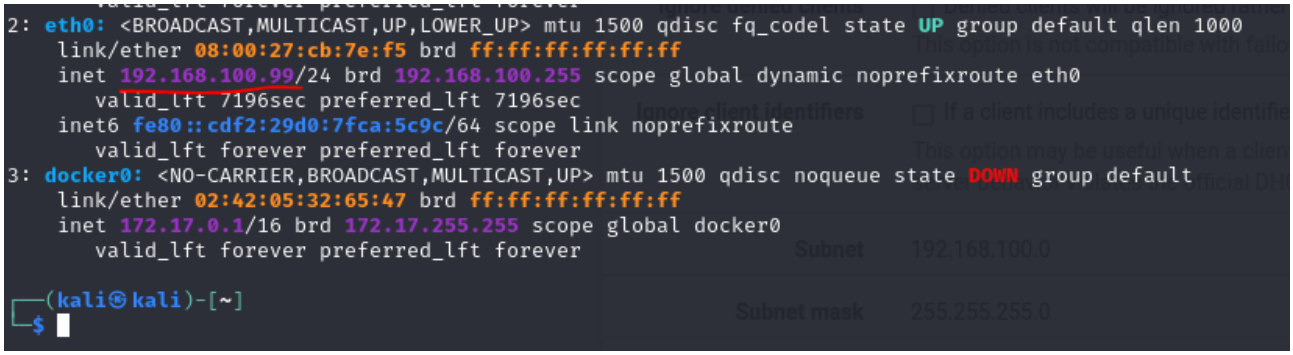
comprobamos las reglas configuradas:



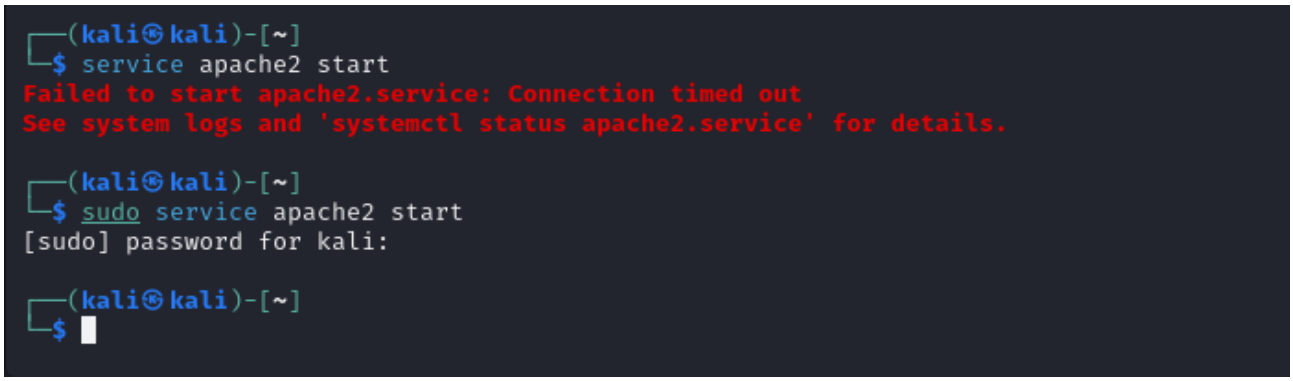
mapeamos una IP estática:



comprobamos el cambio de ip



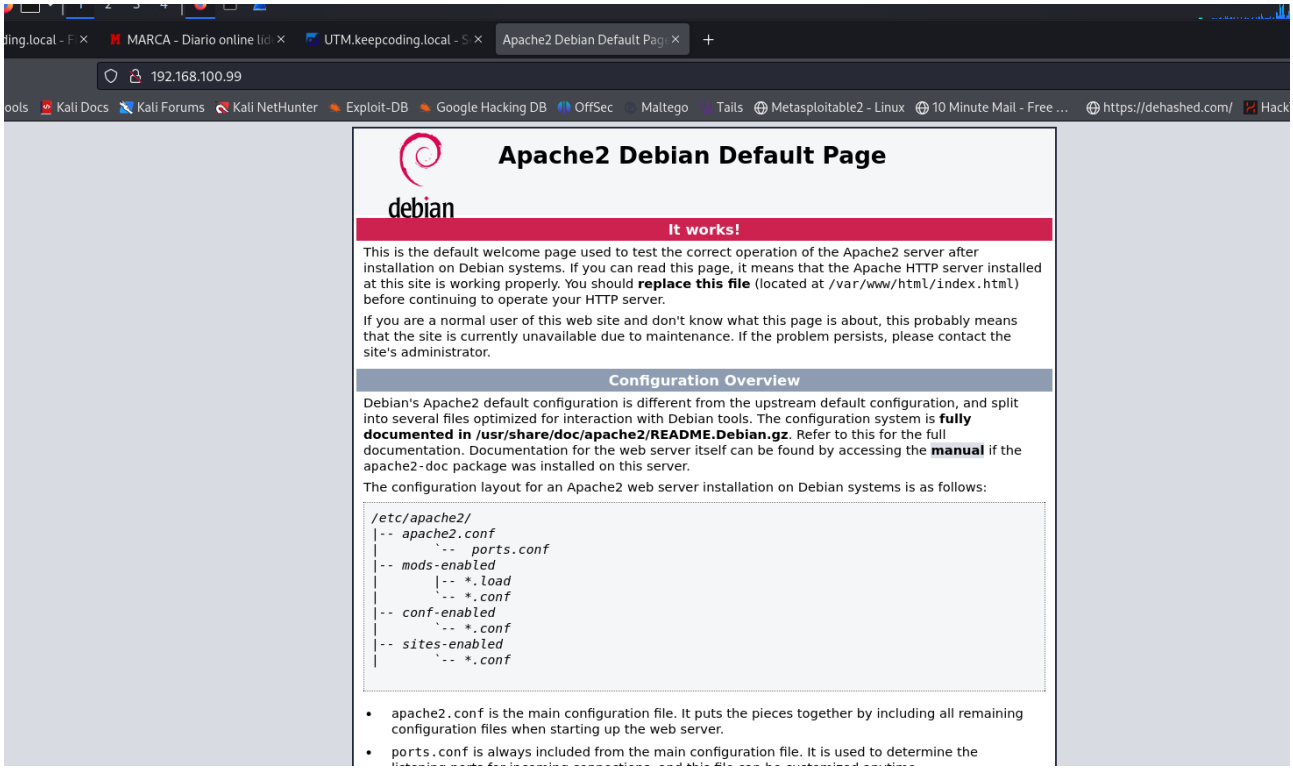
levantamos el servidor APACHE:



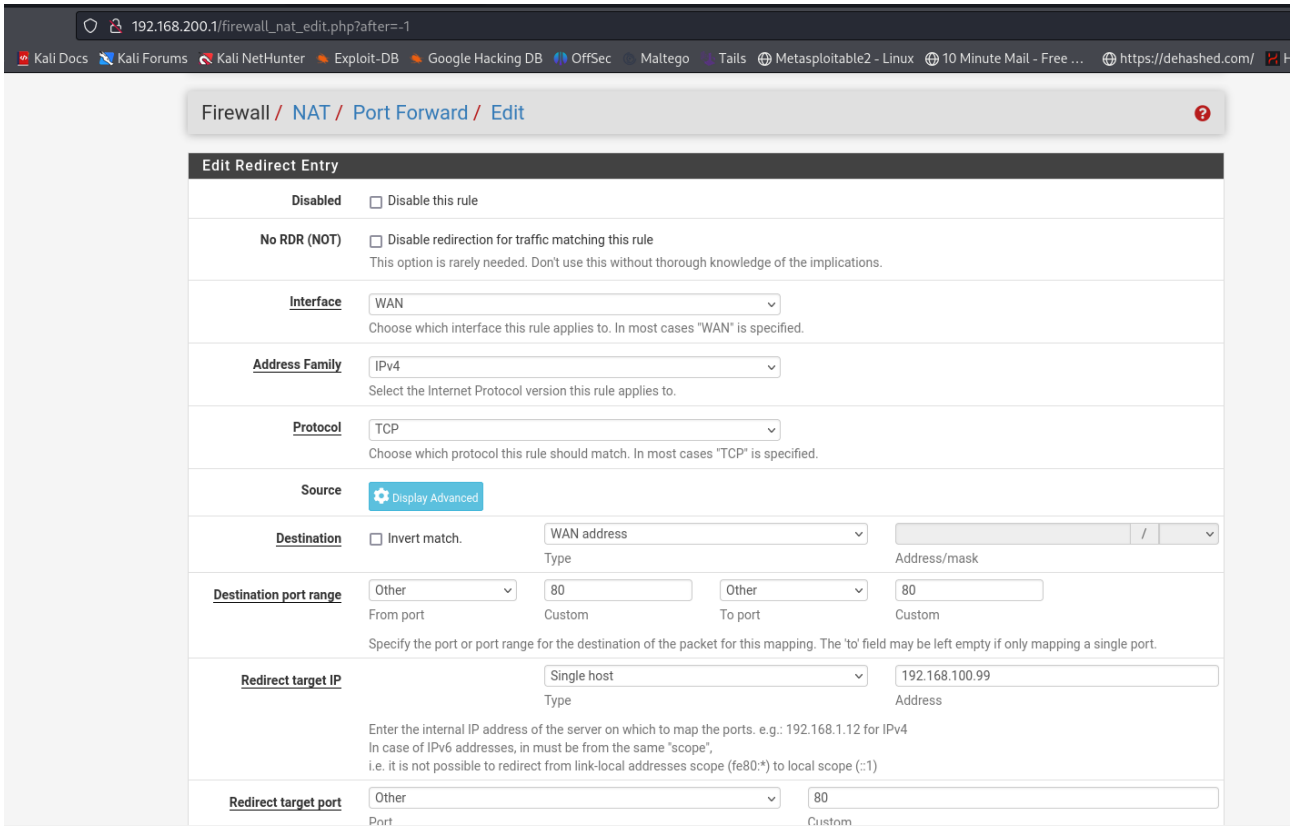
y comprobamos que está levantado el servidor:

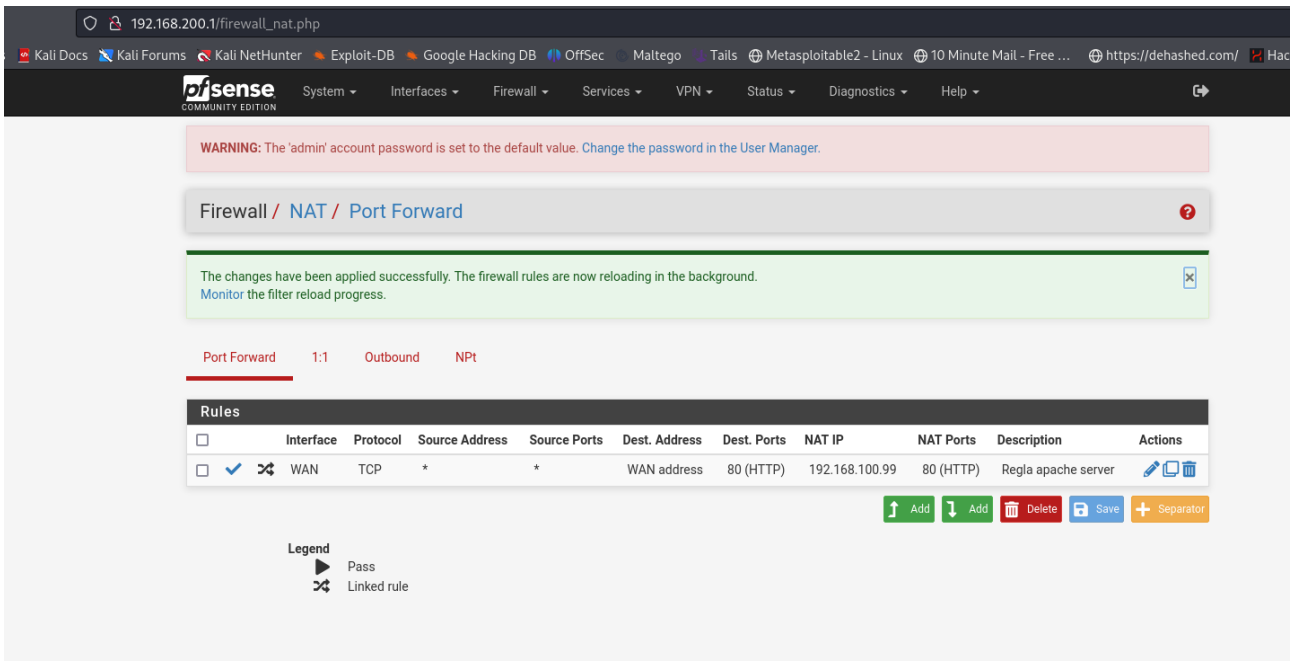
```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-03-16 09:49:14 EDT; 1min 17s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 99091 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 99107 (apache2)
      Tasks: 6 (limit: 13937)
     Memory: 19.7M (peak: 20.2M)
        CPU: 70ms
     CGroup: /system.slice/apache2.service
             ├─99107 /usr/sbin/apache2 -k start
             ├─99110 /usr/sbin/apache2 -k start
             ├─99111 /usr/sbin/apache2 -k start
             ├─99112 /usr/sbin/apache2 -k start
             ├─99113 /usr/sbin/apache2 -k start
             └─99114 /usr/sbin/apache2 -k start

Mar 16 09:49:14 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 16 09:49:14 kali apachectl[99106]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Mar 16 09:49:14 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

┌──(kali㉿kali)-[~]
└─$
```

y comprobamos que se levanta en la ip 192.168.100.99

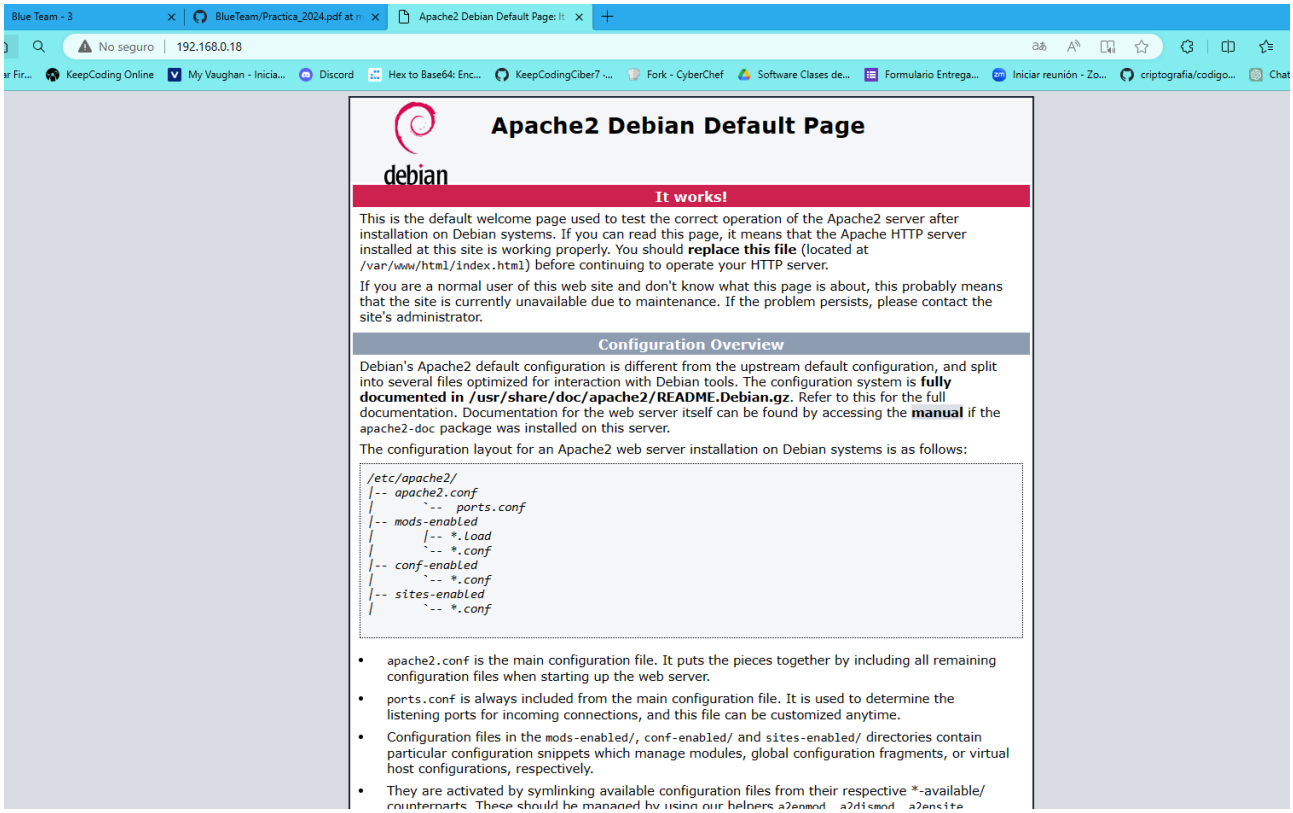


Crearemos una regla para que todo el tráfico que nos llegue a nuestro puerto 80, es decir la red WAN, nos redirija a nuestra red LAN:

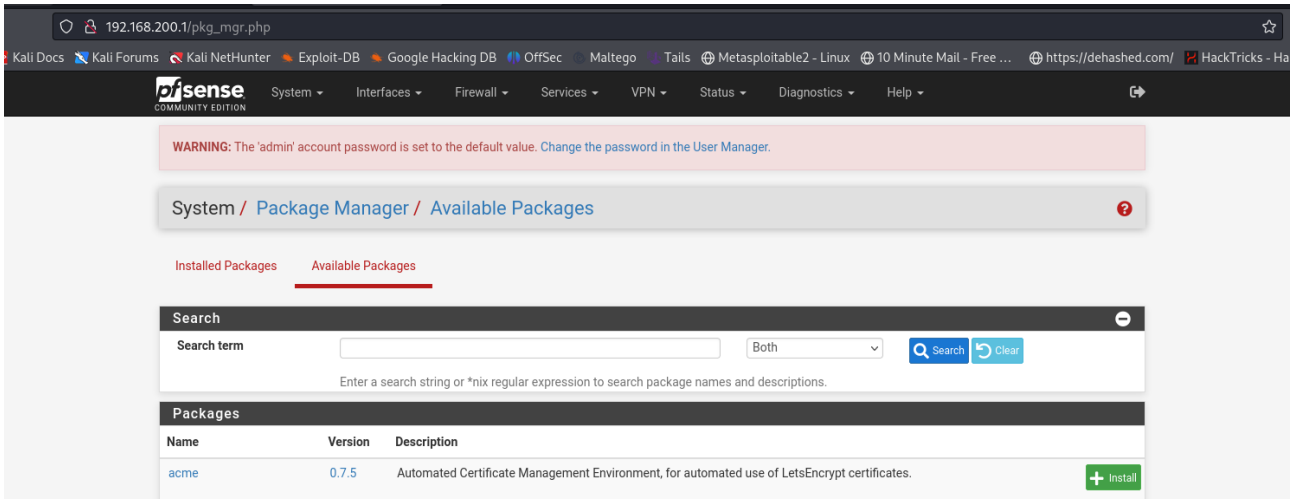




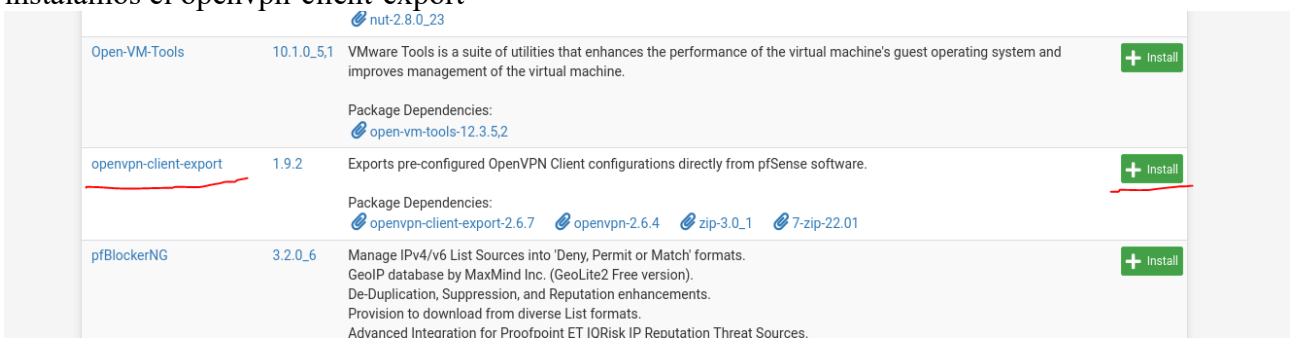
ahora sí accedemos desde nuestra máquina a la ip del servidor apache



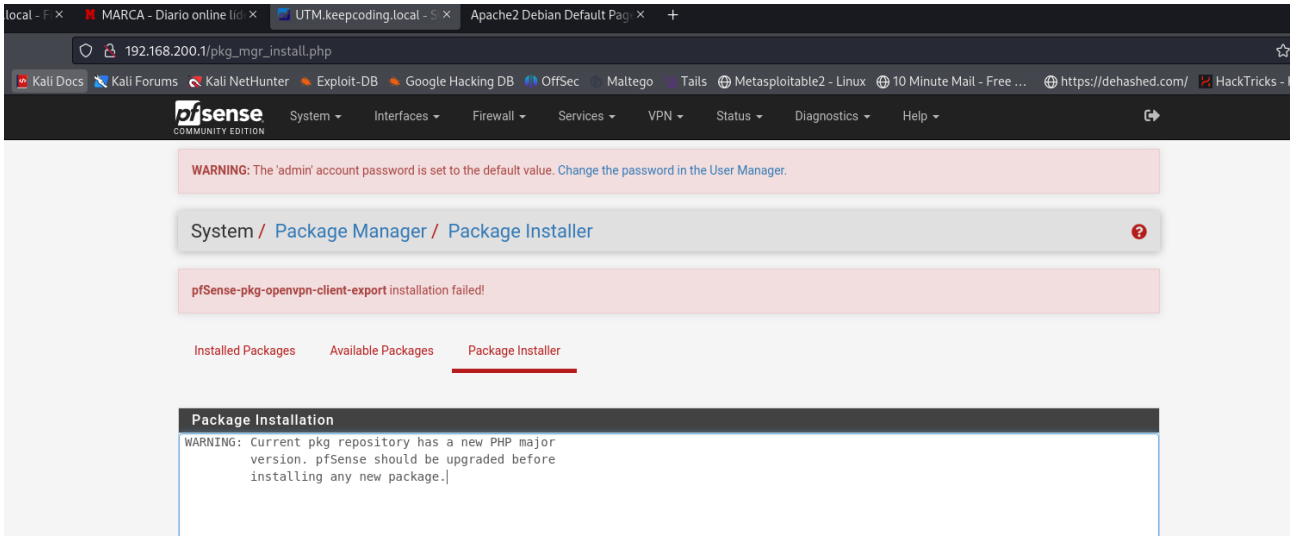
Creamos ahora la VPN, nos vamos a System / Package Manager / Available Packages



instalamos el openvpn-client-export

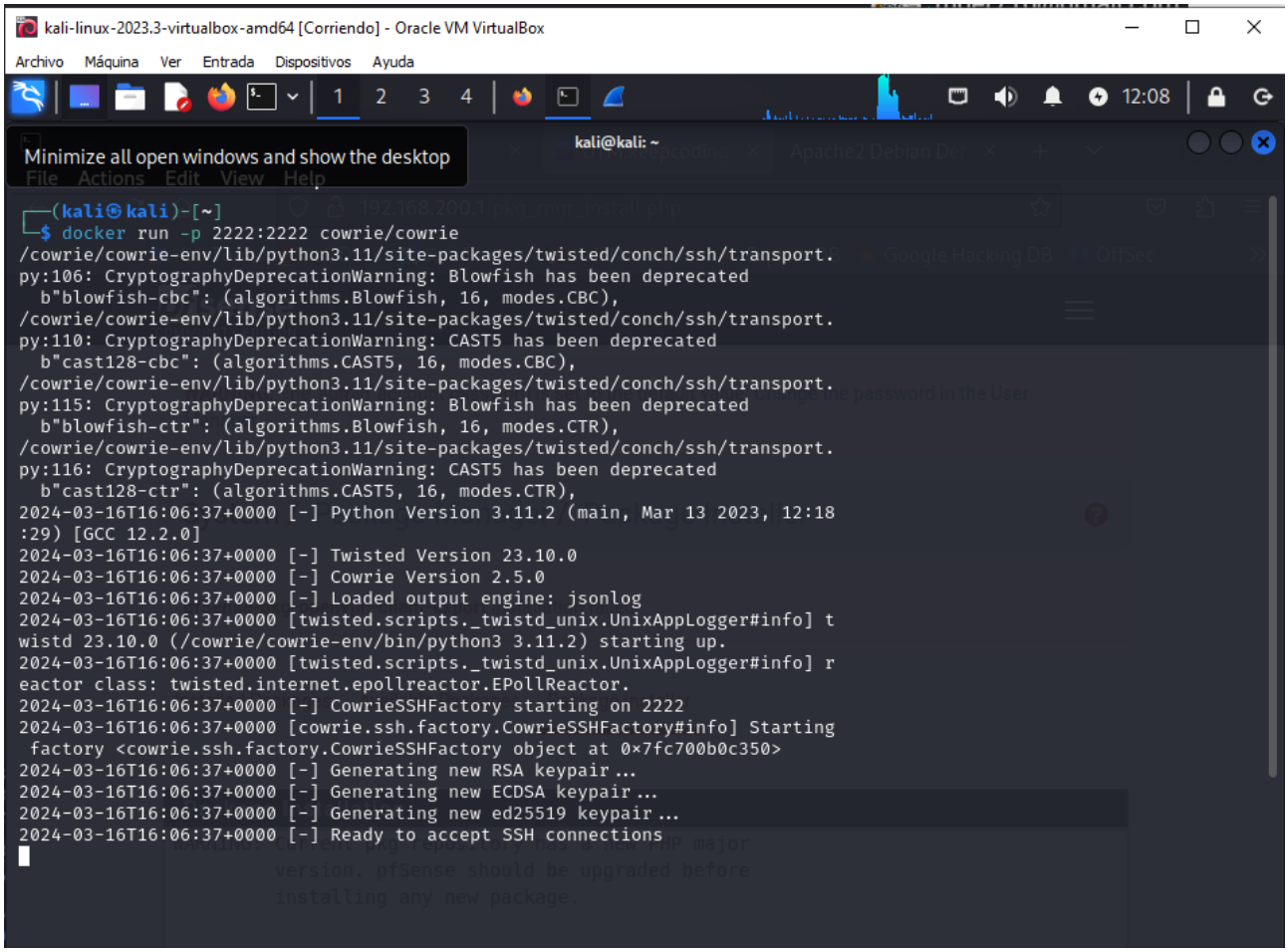


me da error al intentar instalar la vpn



Lanzamos en nuestra kali el honeypot Cowrie con el comando:

docker run -p 2222:2222 cowrie/cowrie



se quedará listo para aceptar conexiones.

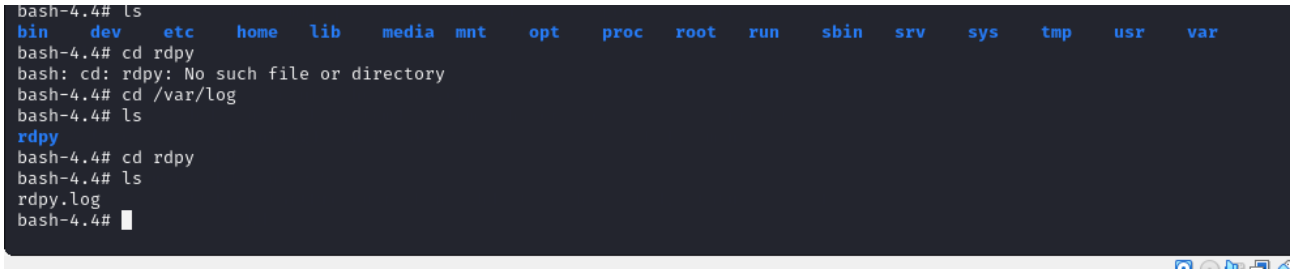
Con el siguiente comando corremos el amazedostrich:

docker run -p 333:3389 amazedostrich/rdpy

Hago un docker ps para ver las imágenes docker en ejecución:

con este comando nos abrirá una terminal dentro del docker:

con este comando iremos a los logs del honeypot

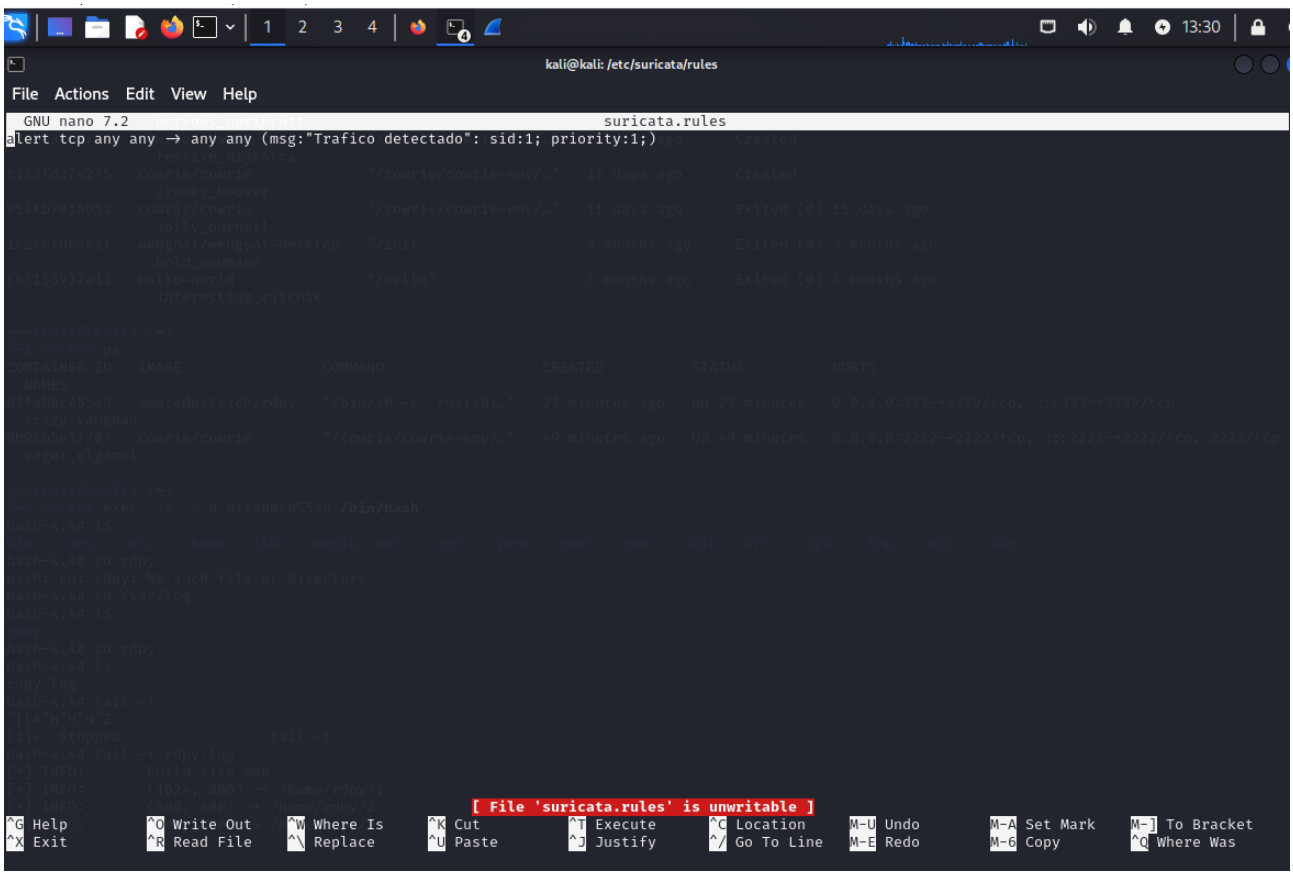


con el comando tail -f rdpy.log vemos los logs del honeypot

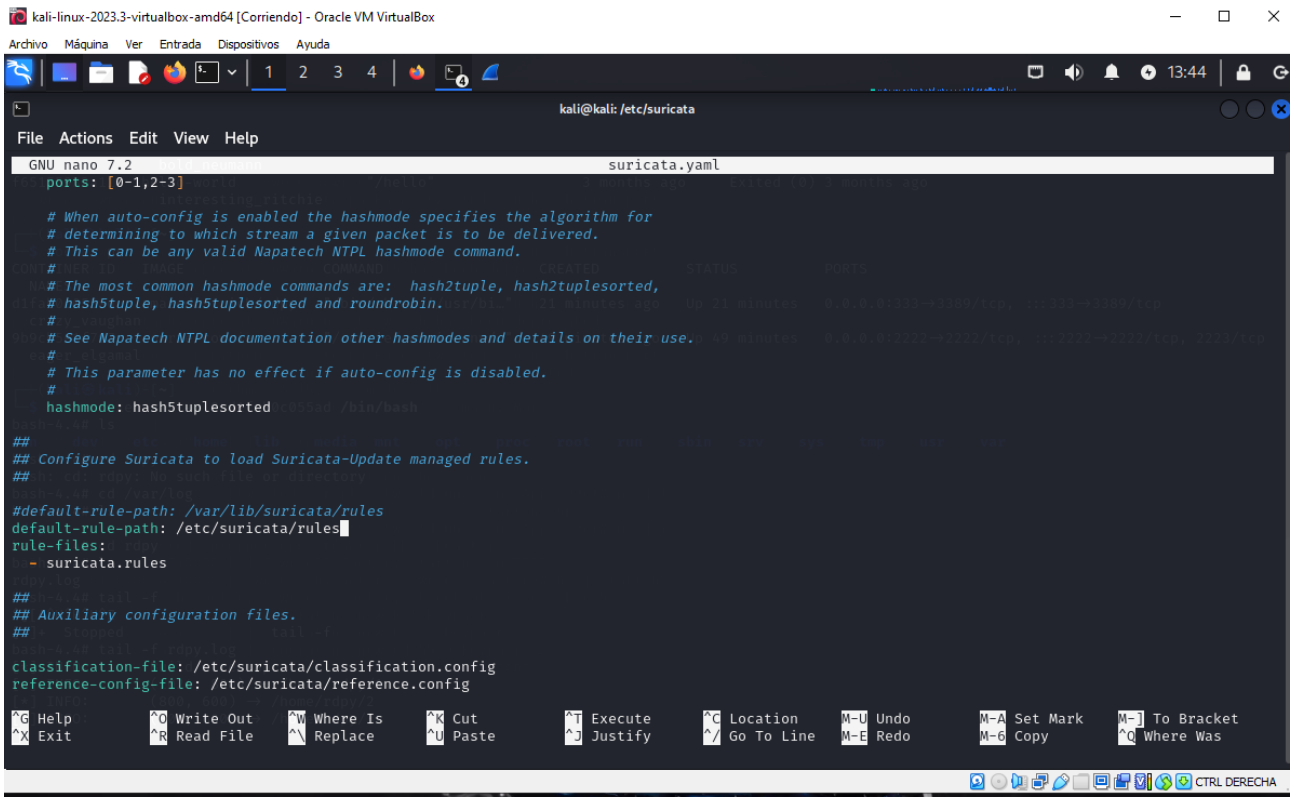
Reglas de SURICATA:

```
┌──(kali㉿kali)-[~]
└─$ cd /etc/suricata

┌──(kali㉿kali)-[/etc/suricata]
└─$ ls
classification.config  reference.config  rules  suricata.yaml  threshold.config

┌──(kali㉿kali)-[/etc/suricata]
└─$ cd rules

┌──(kali㉿kali)-[/etc/suricata/rules]
└─$ ls
app-layer-events.rules  dns-events.rules    http-events.rules      mqtt-events.rules  rfb-events.rules   stream-events.rules
decoder-events.rules    files.rules         ipsec-events.rules     nfs-events.rules   smb-events.rules   tls-events.rules
dhcp-events.rules       ftp-events.rules    kerberos-events.rules  ntp-events.rules   smtp-events.rules
dnp3-events.rules       http2-events.rules  modbus-events.rules    quic-events.rules  ssh-events.rules

┌──(kali㉿kali)-[/etc/suricata/rules]
└─$
```

creamos la regla para suricata

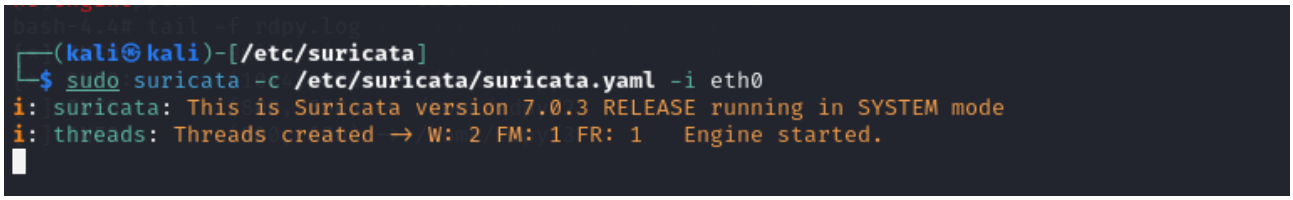


en el archivo suricata.yaml, cambiamos lo siguiente:

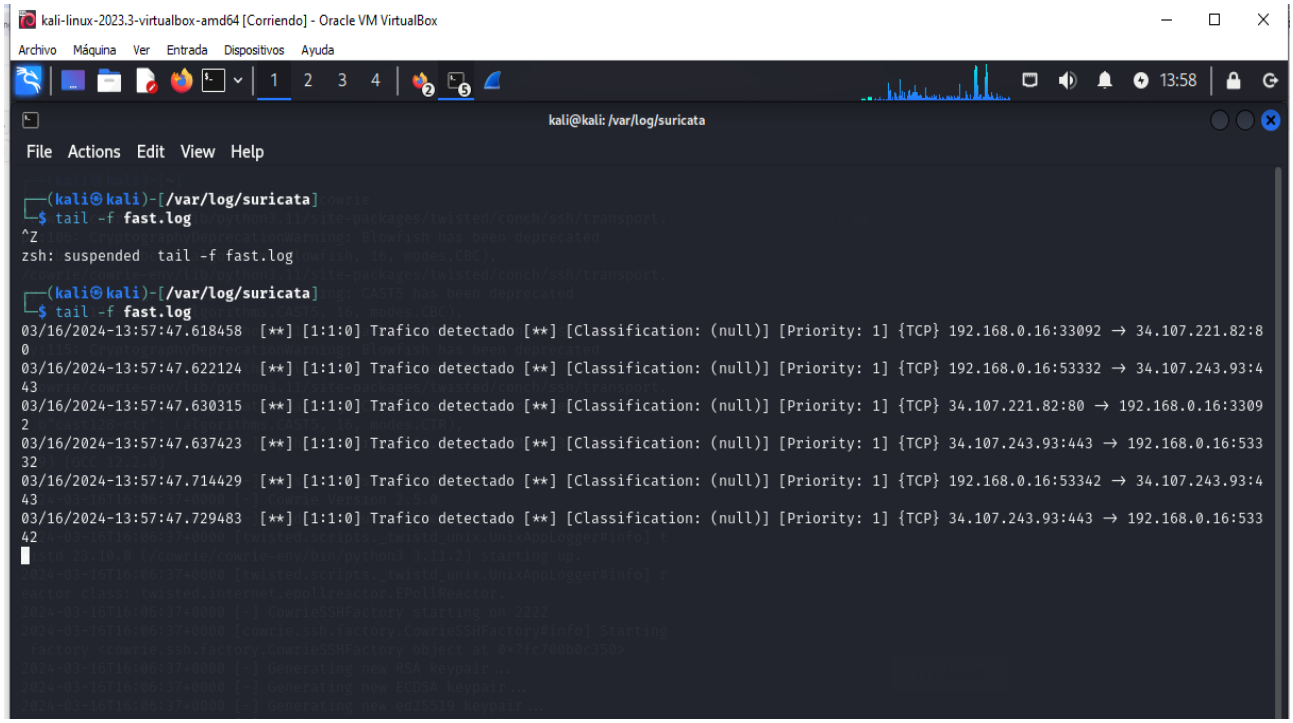


para que nos coja por defecto el archivo suricata.rules que hemos creado

ejecutamos Suricata:

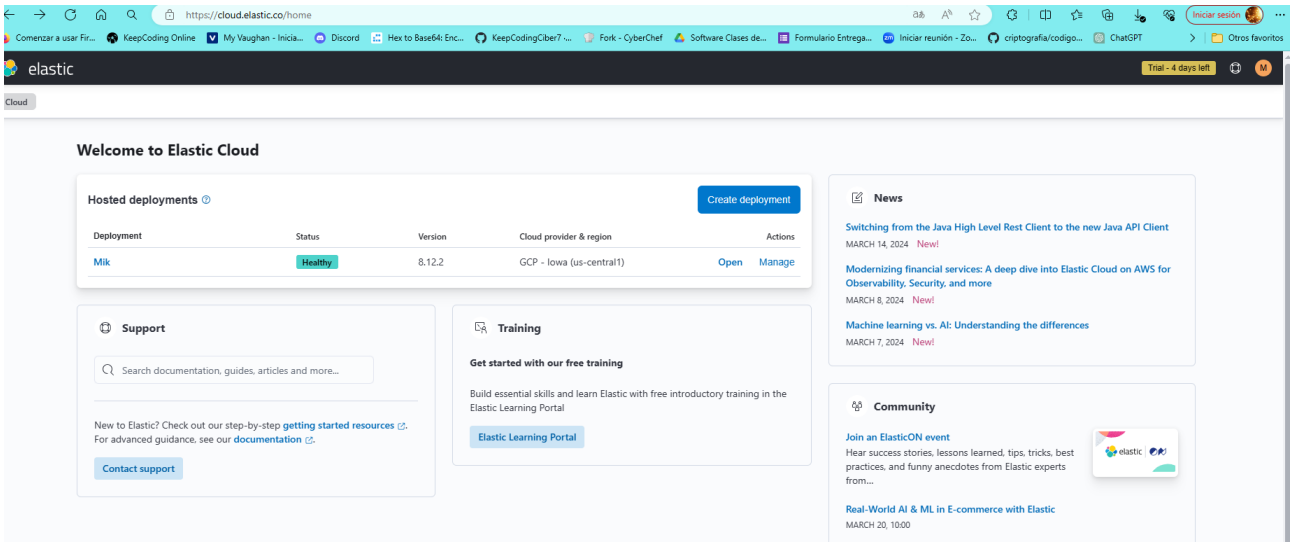


vemos los logs:

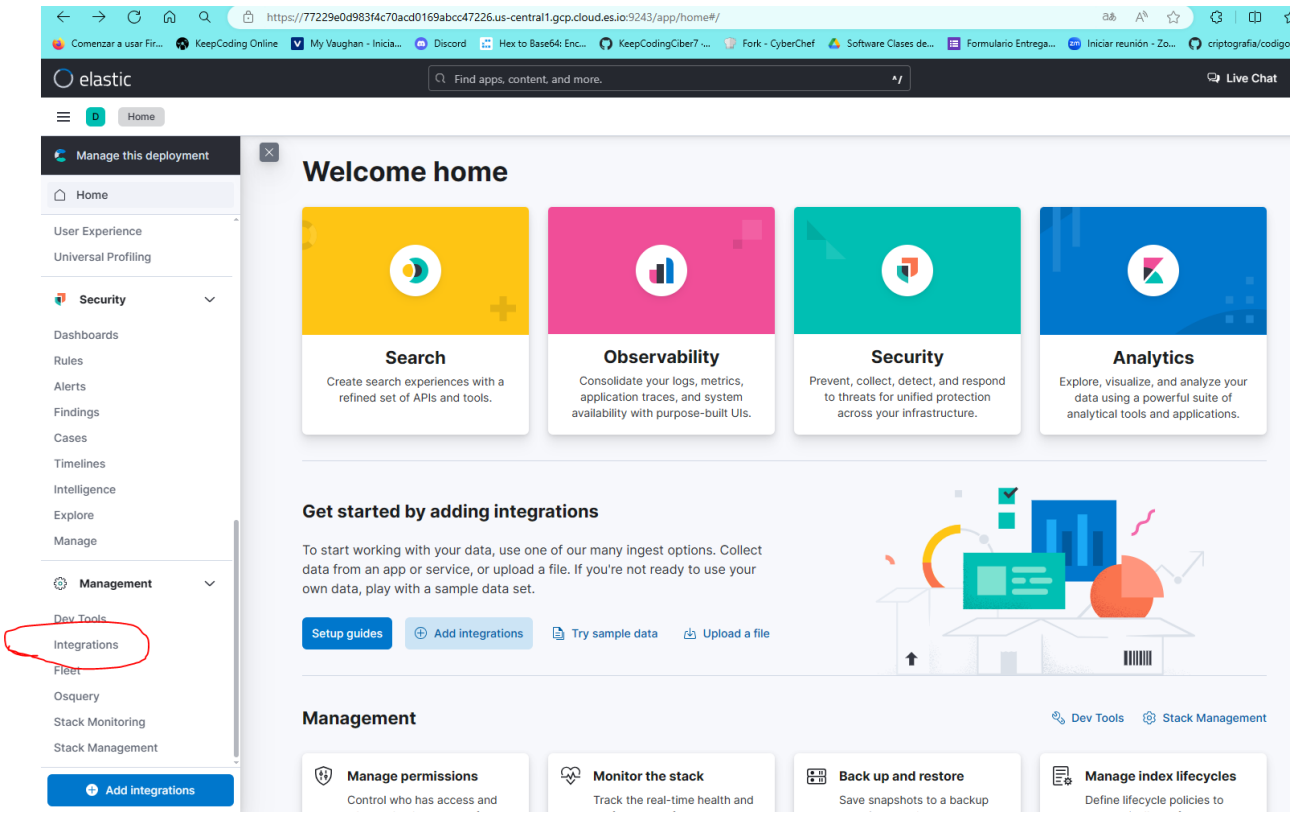


se me peta windows 11 y no puedo hacer nada con él

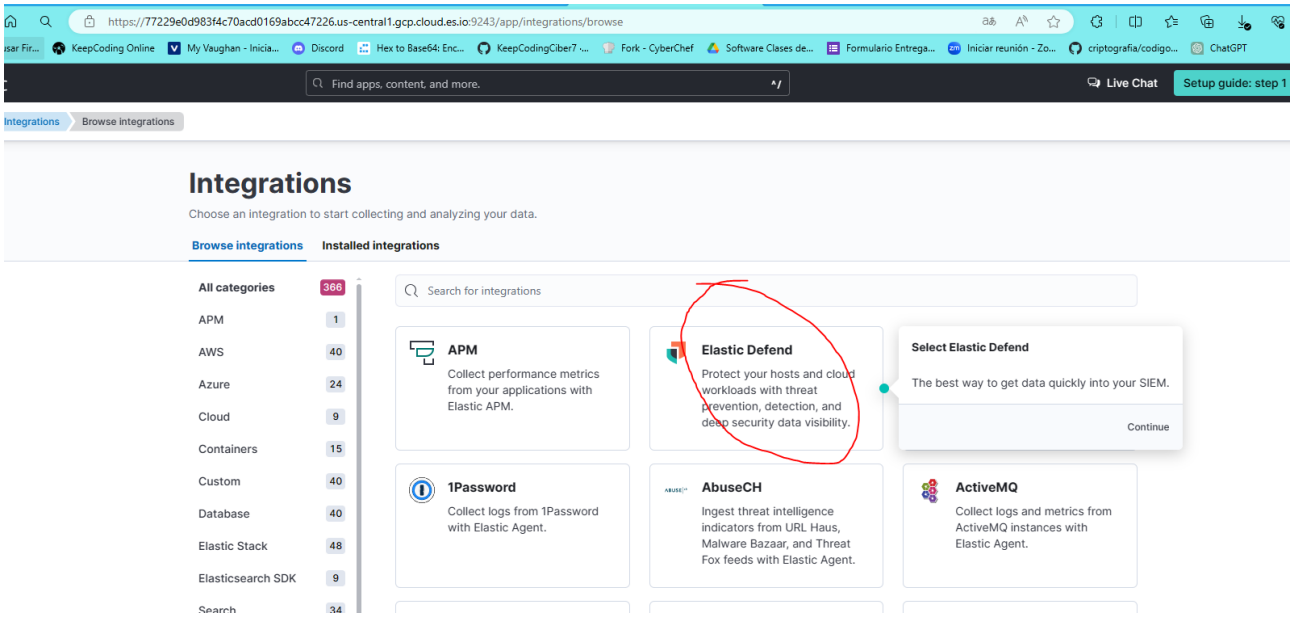
ELASTIC CLOUD

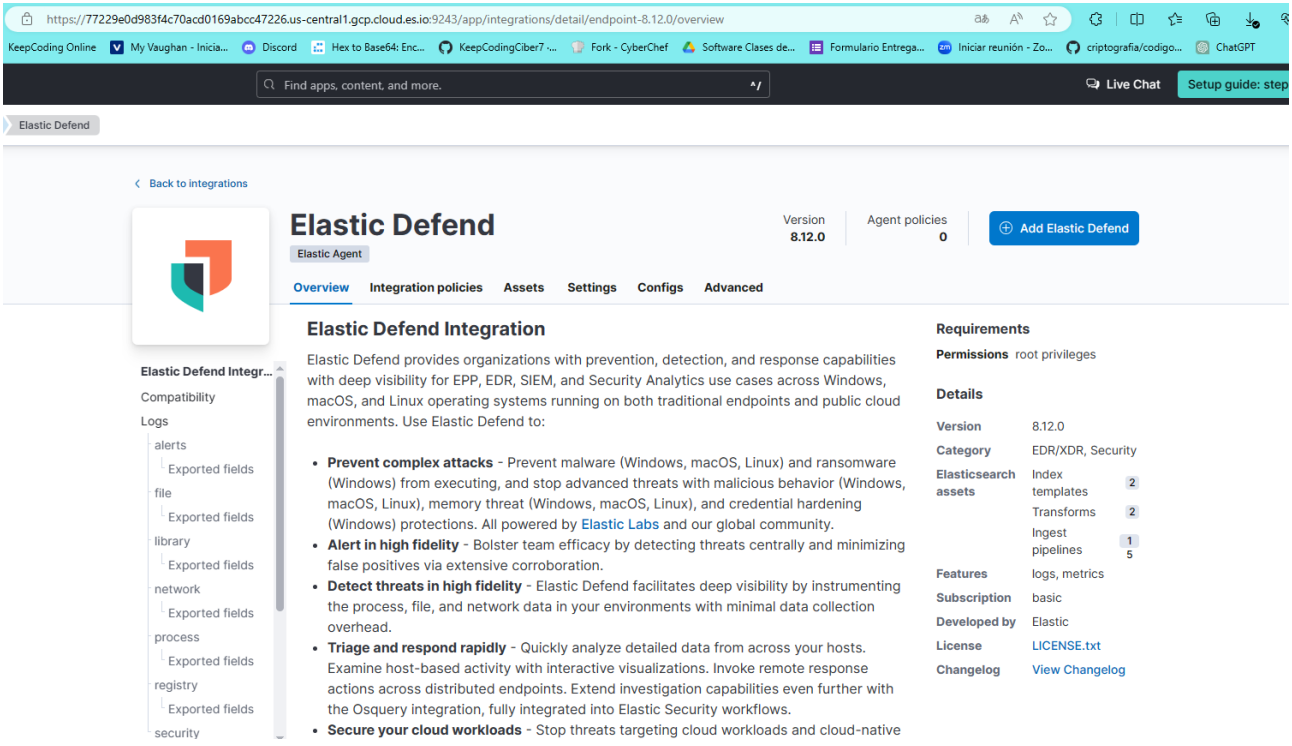


vamos a Management – Integrations

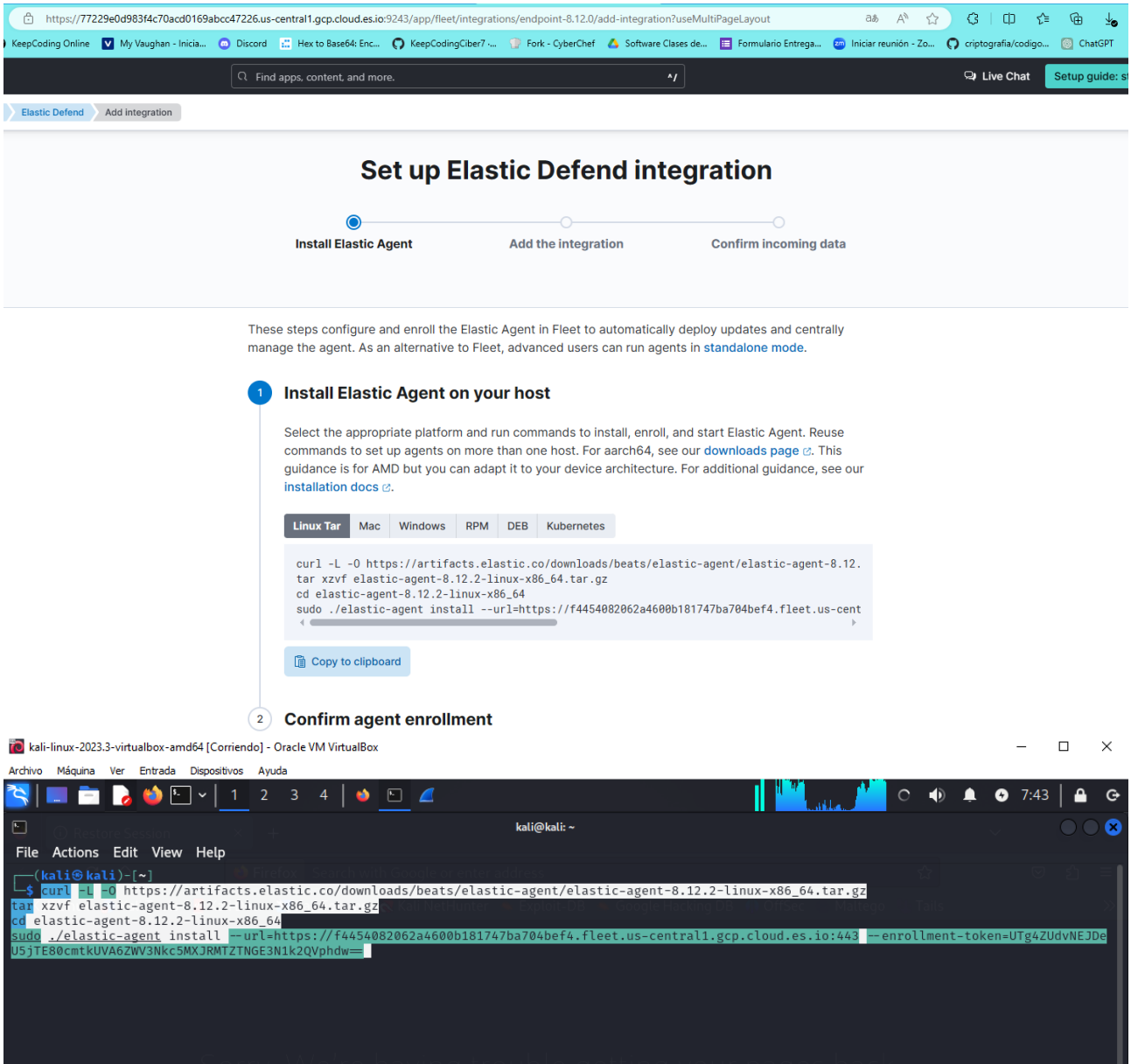


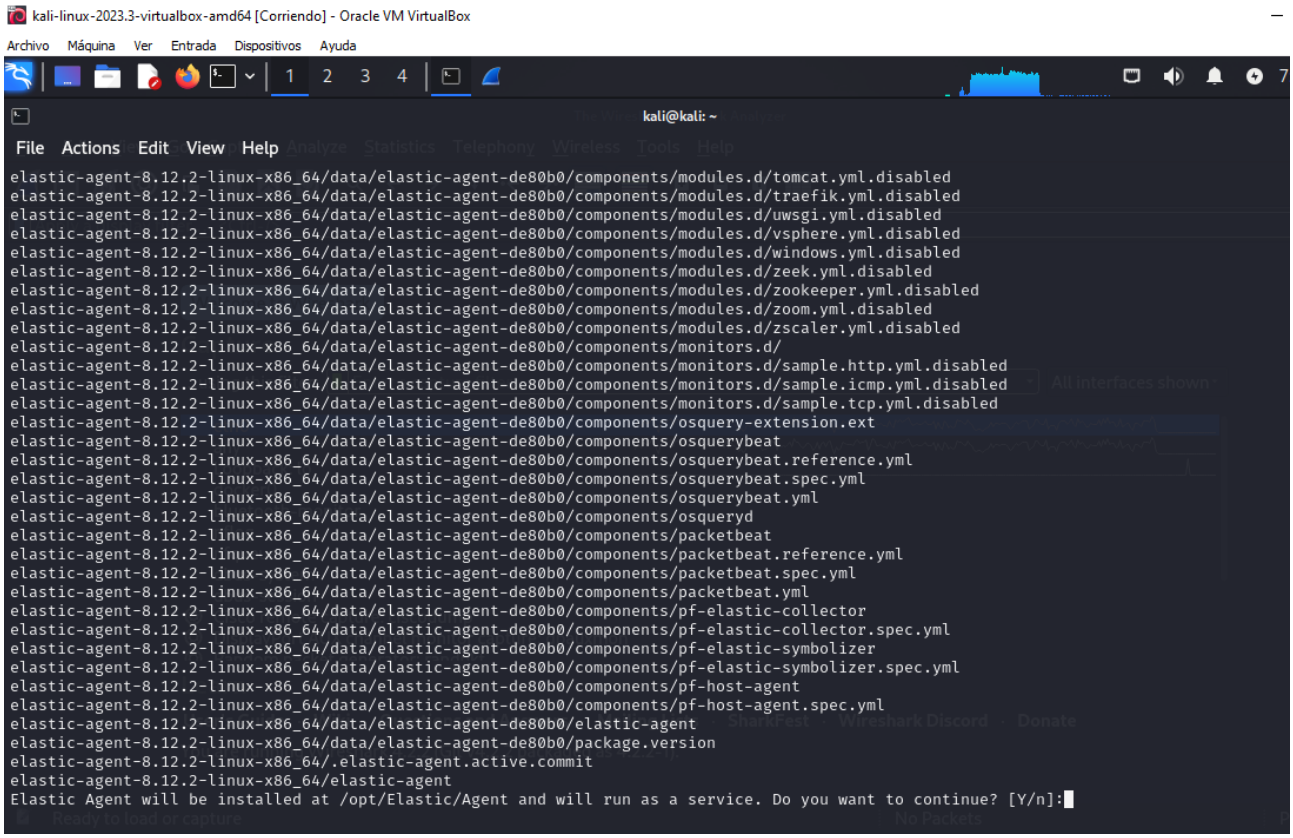
y luego a Elastic Defend



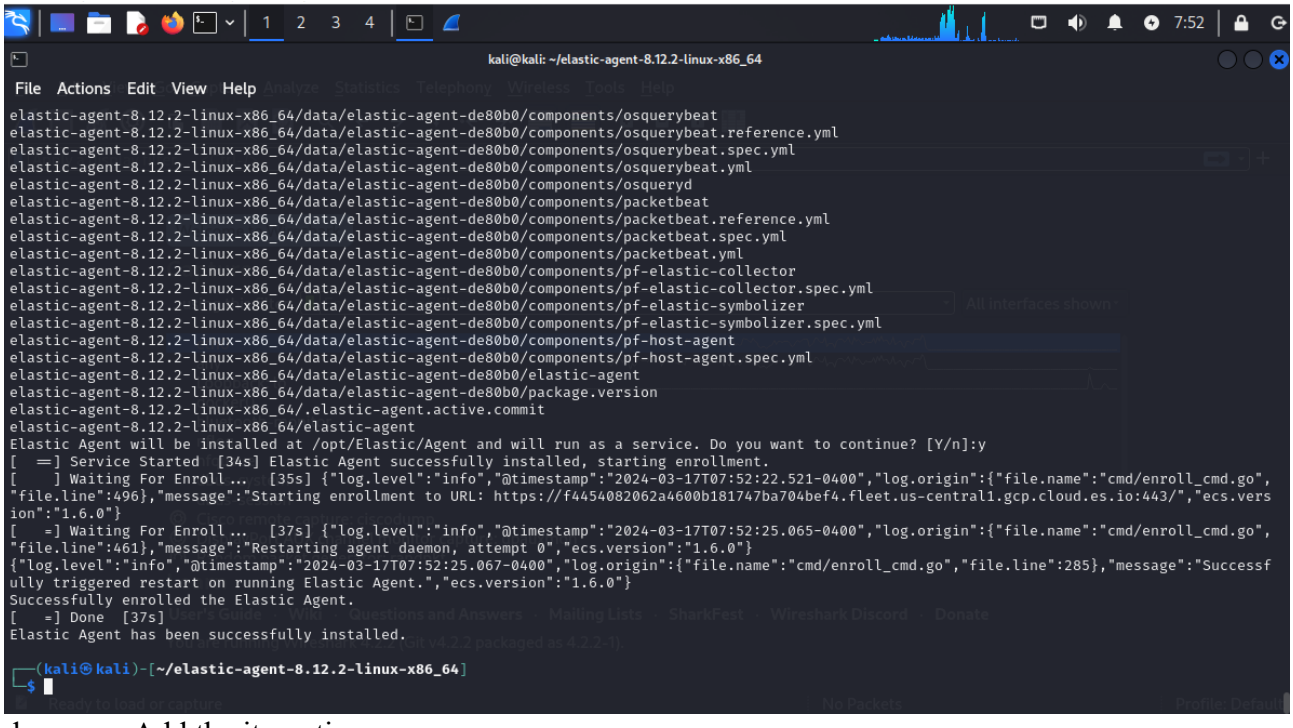


instalamos el agente en la kali, copiando el script:





instalado el agente:



damos en Add the itegration

These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in standalone mode.

Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

Linux Tar | Mac | Windows | RPM | DEB | Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-cent
```

Copied

Agent enrollment confirmed

✓ 1 agent has been enrolled.

Set up Elastic Defend integration

Install Elastic Agent — Add the integration — Confirm incoming data

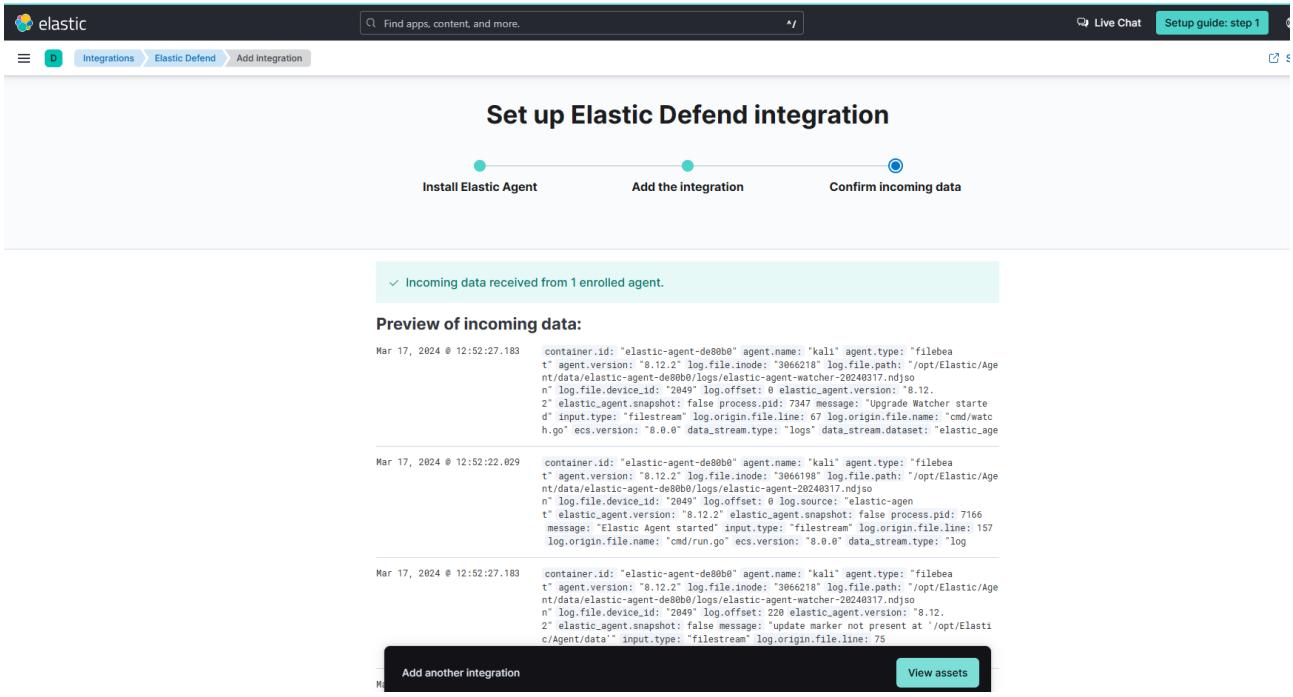
We'll save your integration with our recommended defaults.

✓ Windows, macOS, and Linux event collection

You can edit these settings later in the Elastic Defend integration policy. Learn more

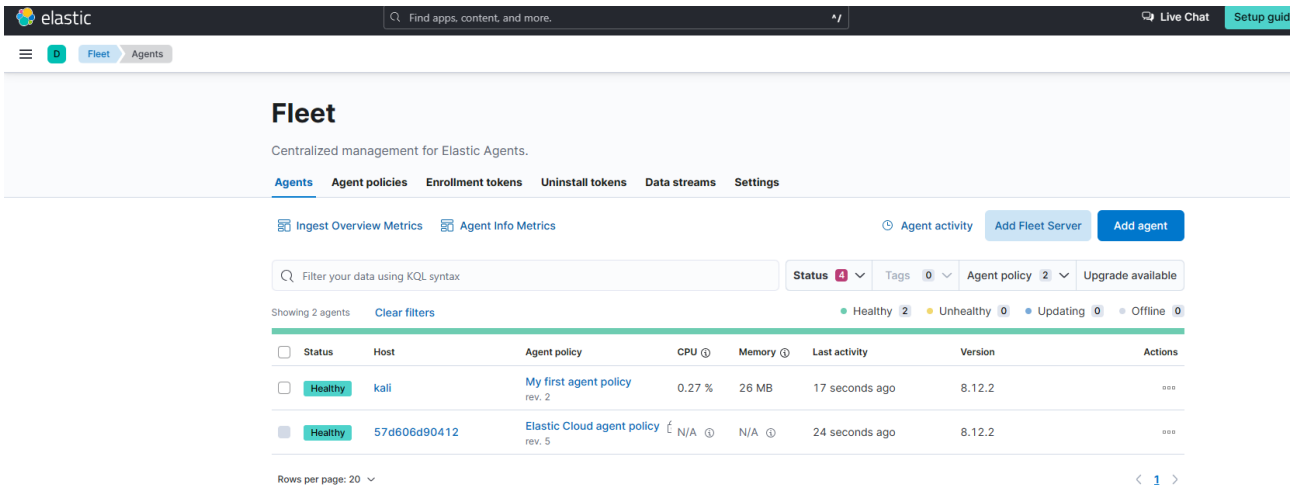
Go back | Confirm incoming data

aquí vemos los logs que vienen de kali:

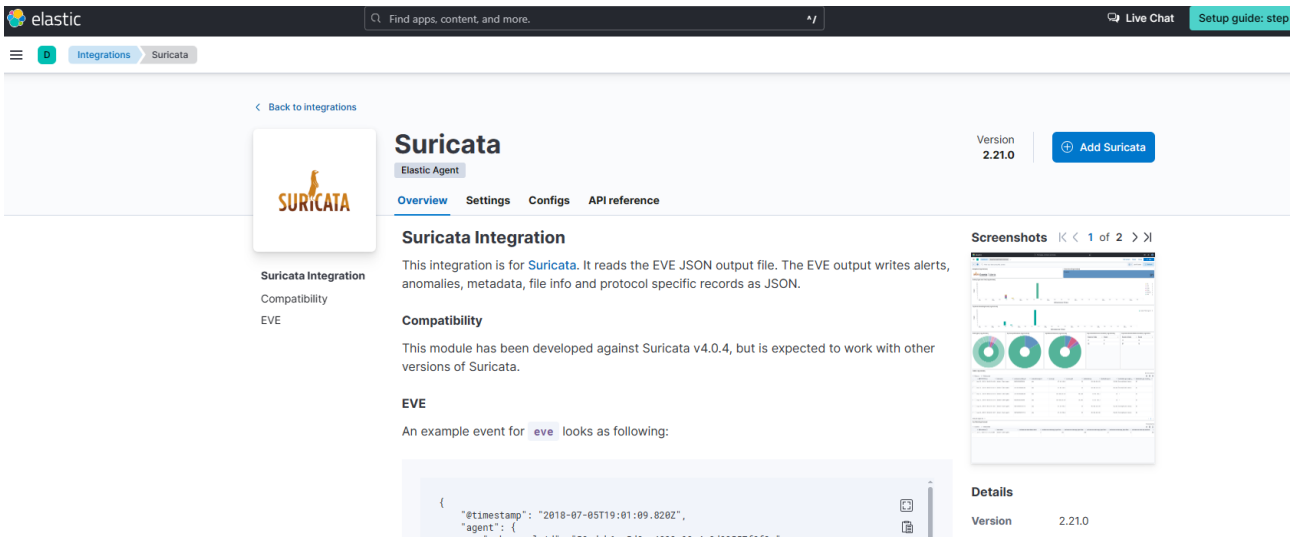


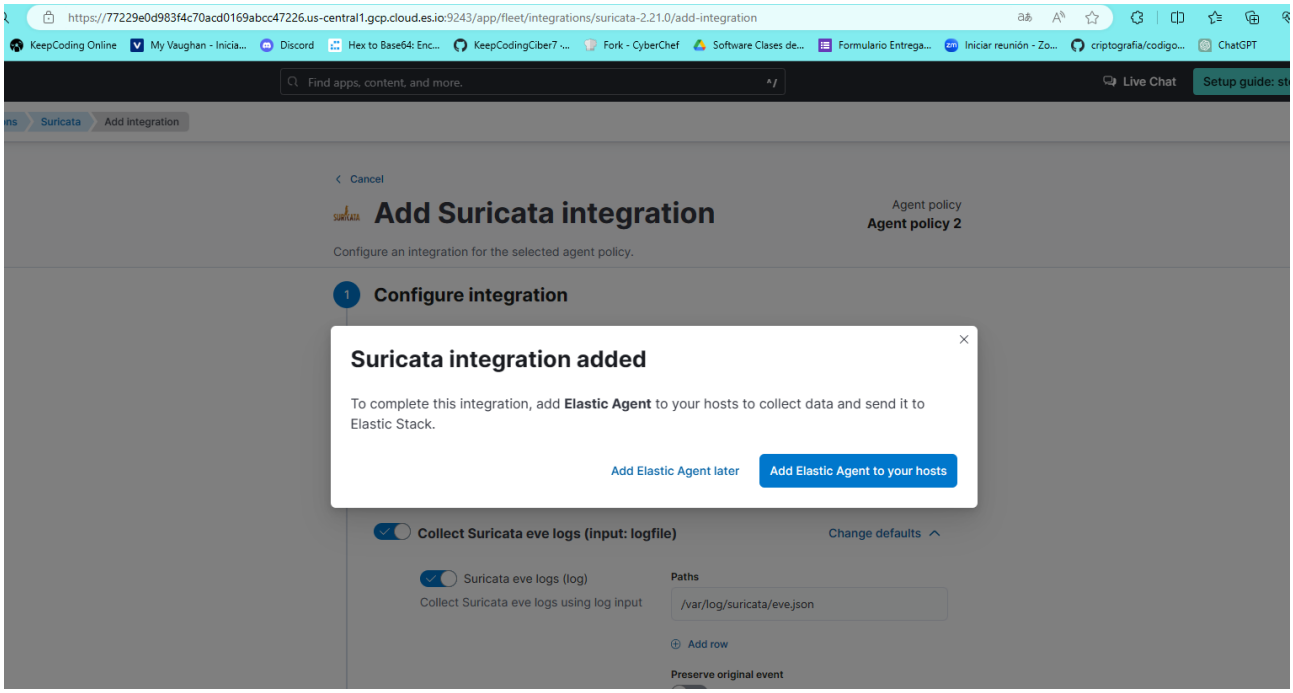
damos click a ver assets (ver activos)

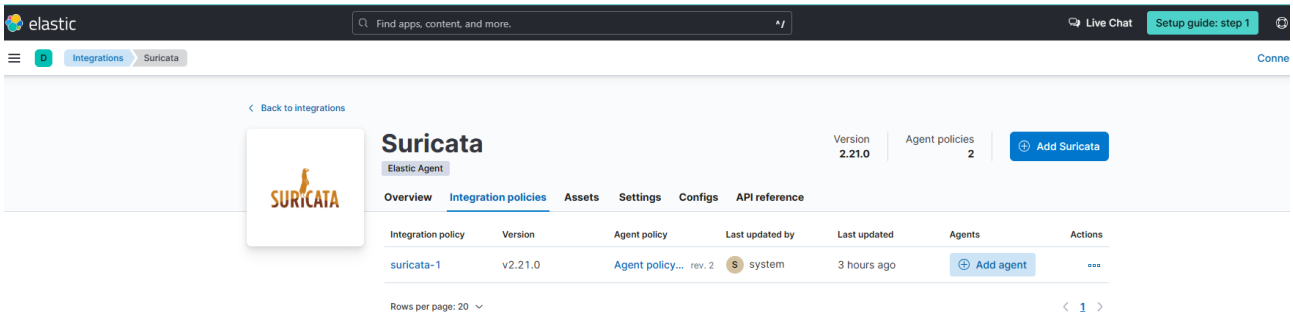
nos vamos a Fleet para ver las políticas, que son las reglas para recoger los logs:



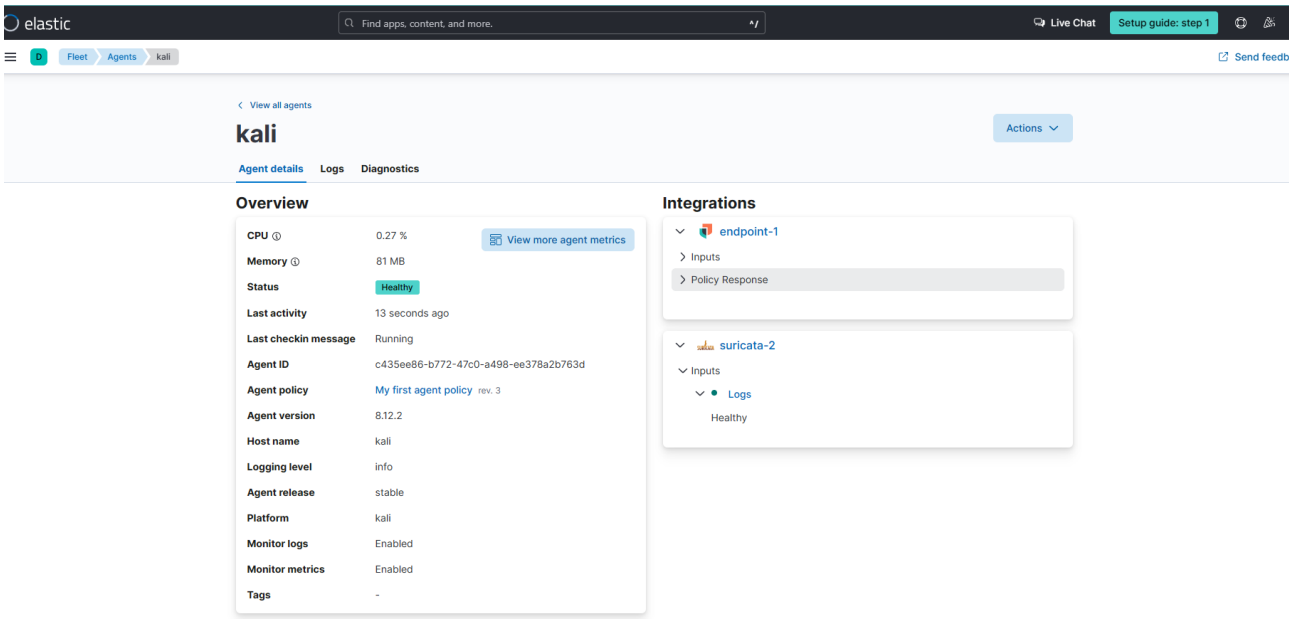
podemos integrar Suricata para recoger los logs de Suricata.



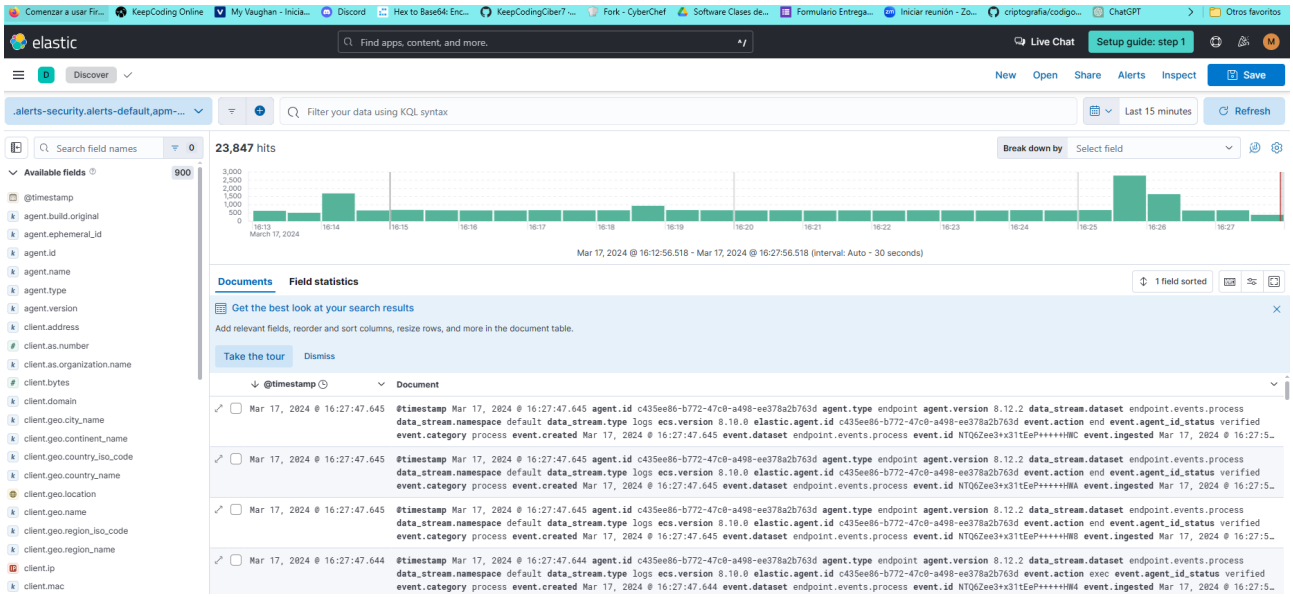




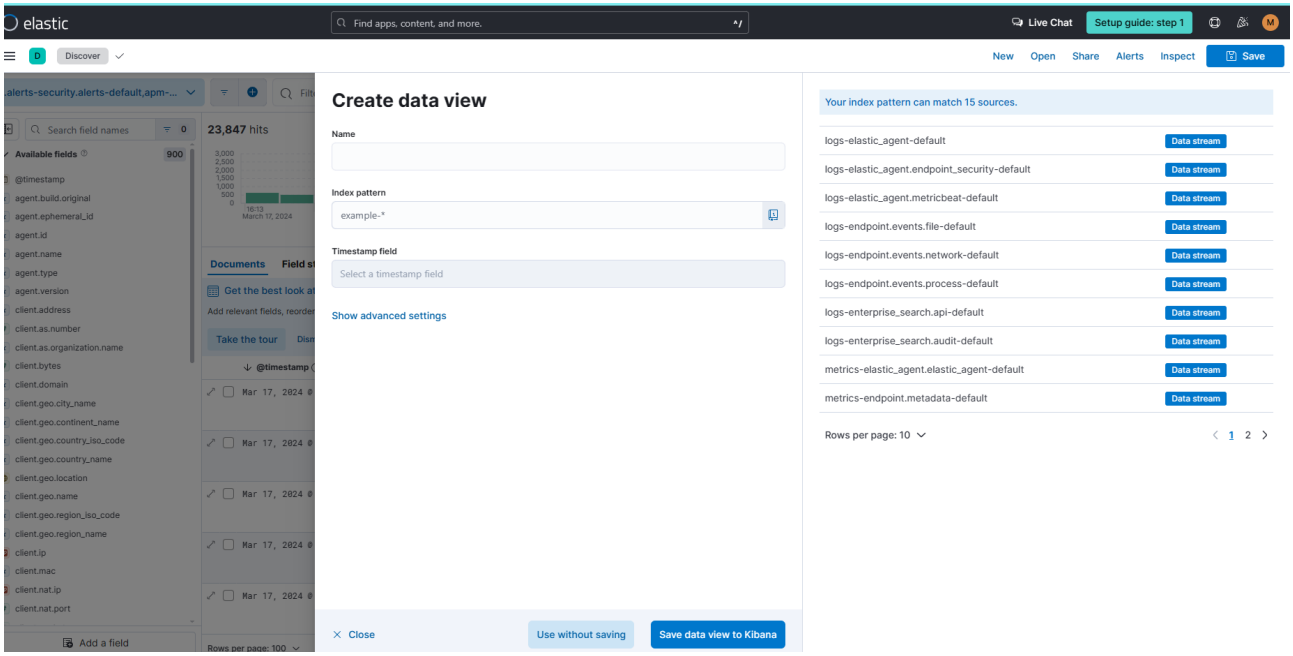
Aquí vemos la integración que tiene nuestra máquina kali con suricata, para poder tener logs de suricata.

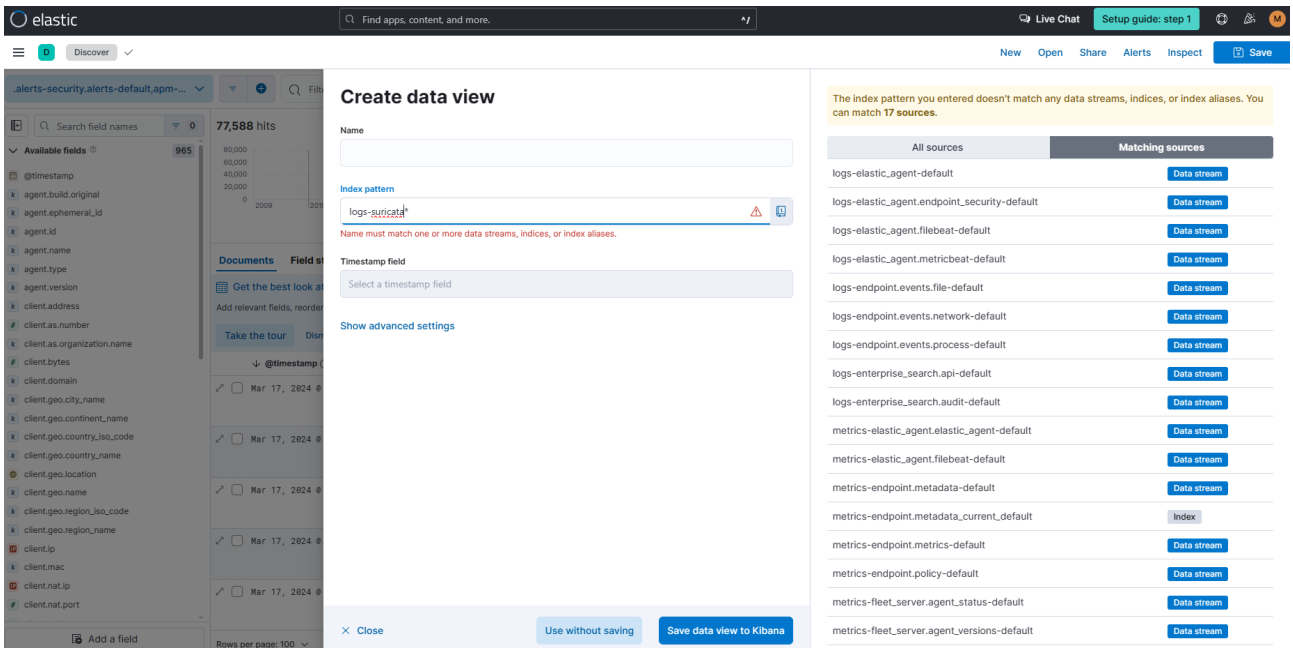


En discover vemos los logs, pero no veo los de suricata ni los de windows 11 :(



podemos crear los conjuntos de datos que queremos ver





FIN DE PRÁCTICA