

2022-2023

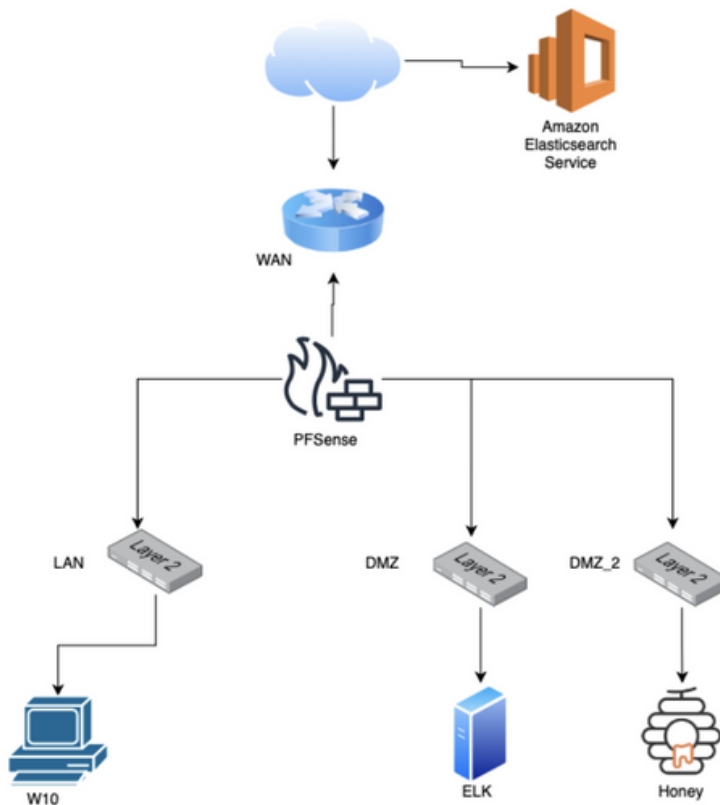
PRÁCTICA BLUE TEAM



*Informe redactado por:
Diego Puchol Candel*

>>>> OBJETIVO

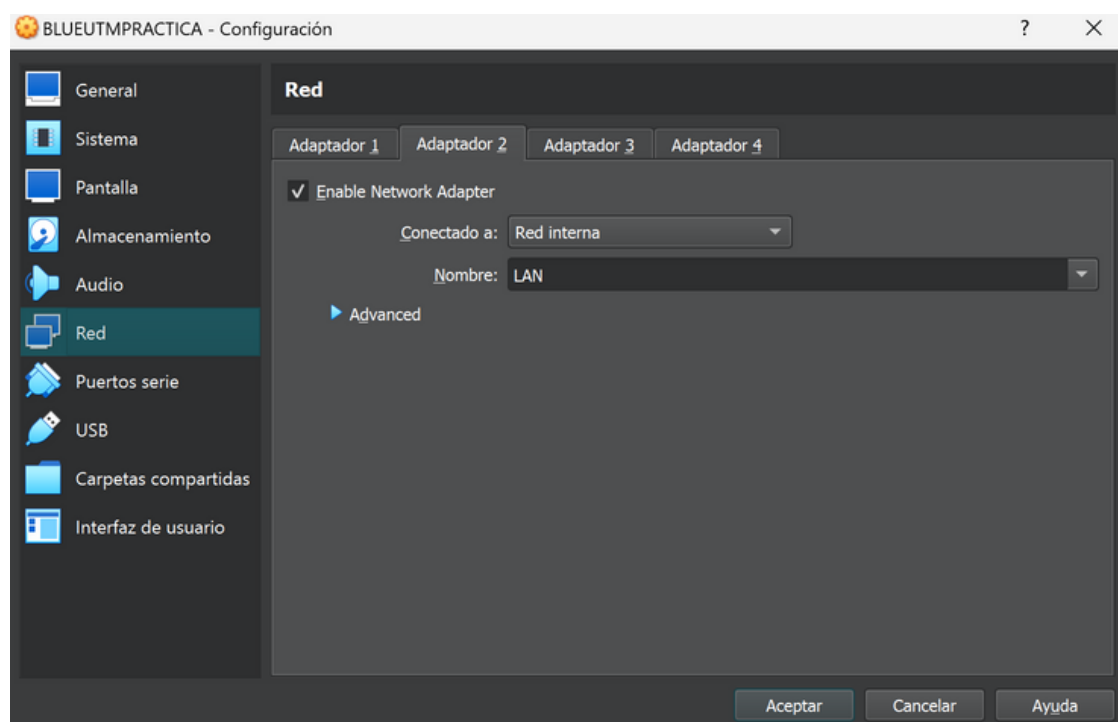
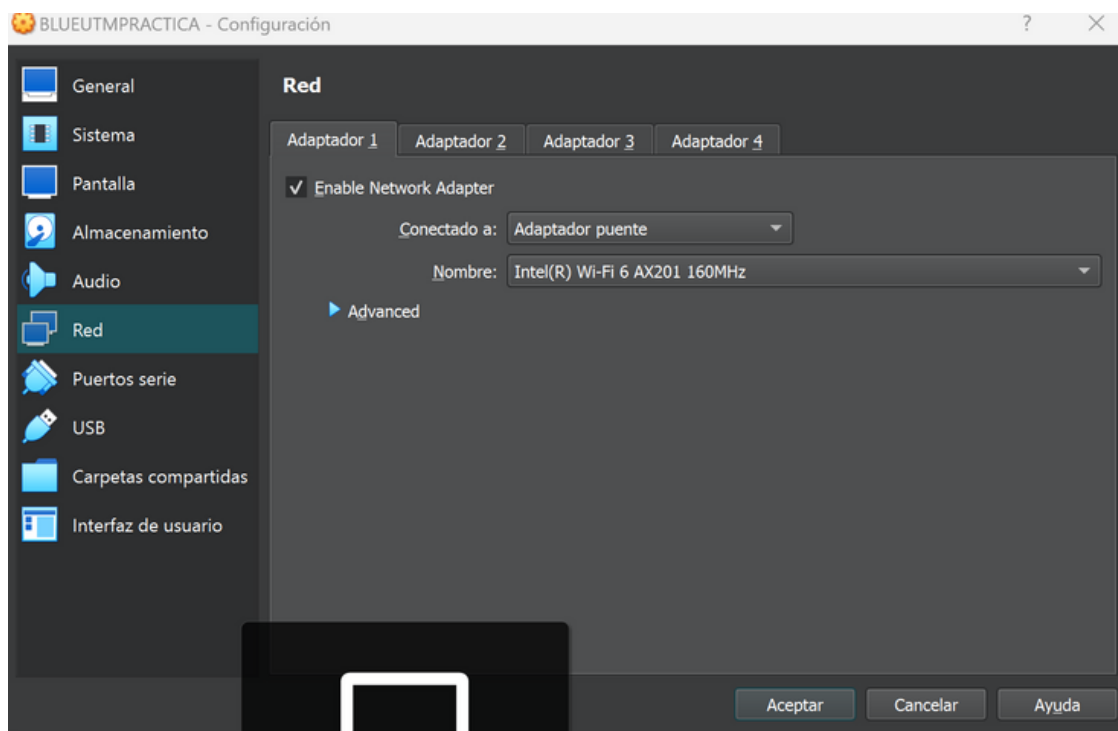
Nuestro objetivo será crear las redes indicadas en la siguiente infraestructura, lograr conseguir datos de una máquina de Windows hasta nuestra maquina Kali que estará ubicada en una red distinta. En este caso Windows en LAN y Kali en DMZ

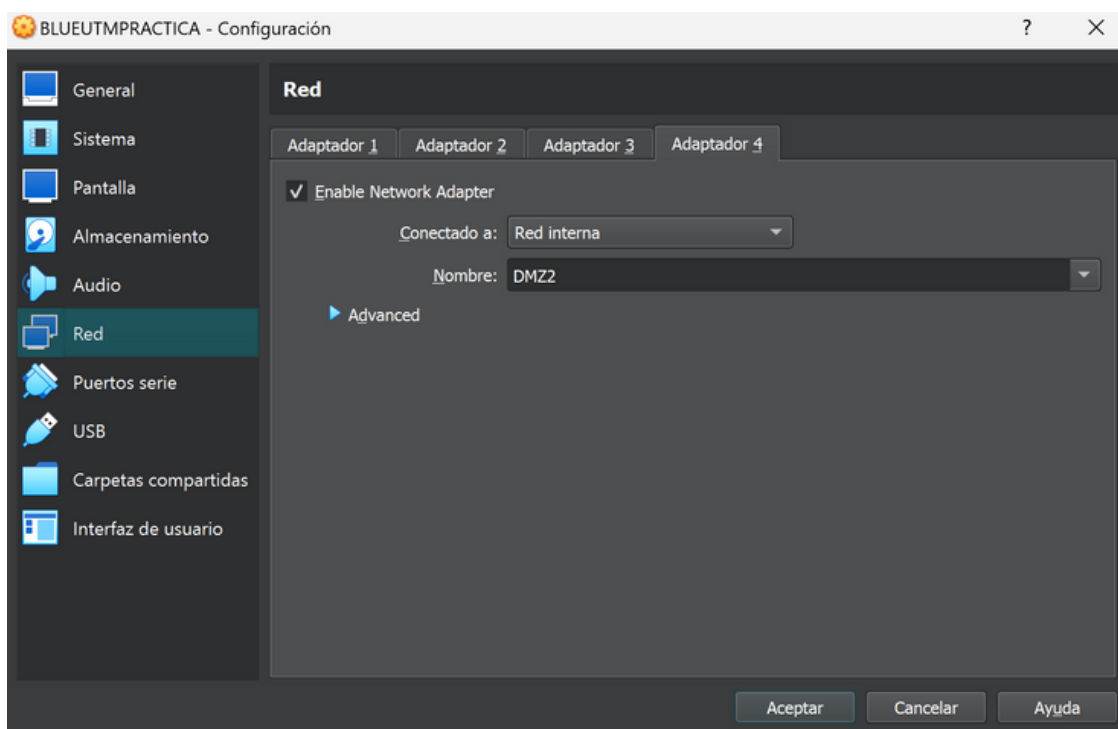
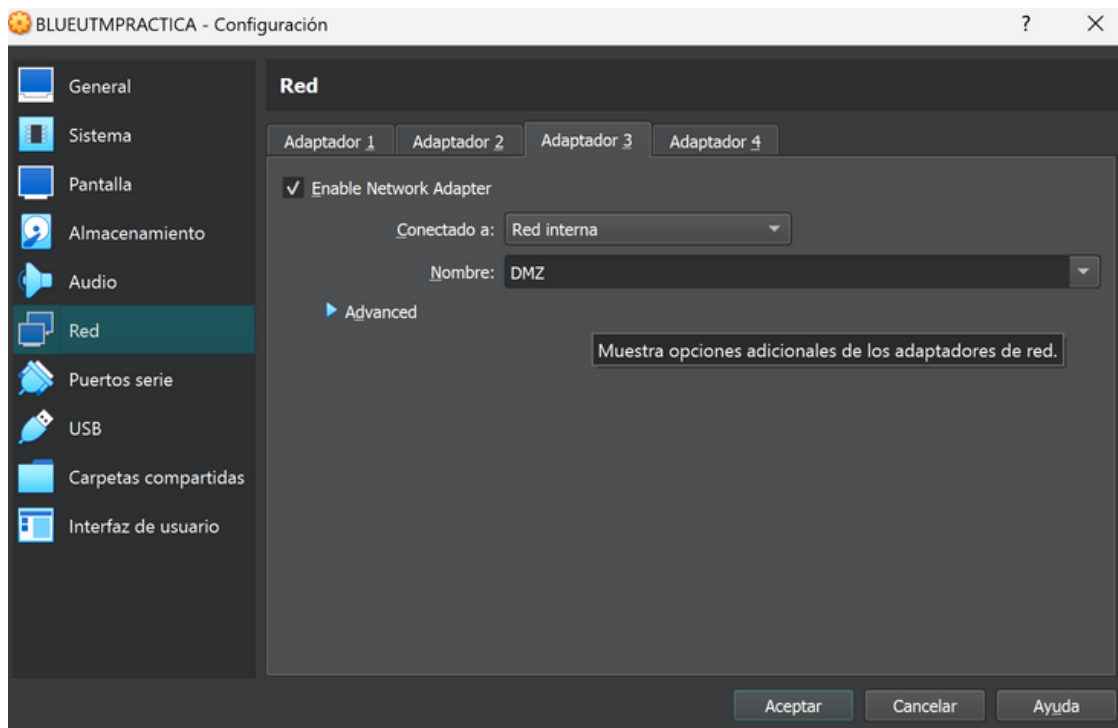


Esto se logrará con ELK y Pf Sense

»»»» CREACIÓN DE REDES

Primero configuramos desde la máquina de virtualbox las redes poniendo lo de la siguiente manera :





ASIGNACIÓN DE REDES

En esta imagen asignamos las interfaces.

Yendo a máquina y configuración, ahí podemos ver como terminan los "mac" de las diferentes redes. Todo esto para hacer el siguiente paso que estará en la otra captura.

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

em0      08:00:27:2d:06:e2    (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:7e:fc:22    (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:be:4b:5c    (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3      08:00:27:96:06:12    (down) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? █
```

En esta imagen vamos asignando por orden con su red correspondiente viendo la terminación del "mac".

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 a or nothing if finished): em3

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2
OPT2 -> em3

Do you want to proceed [y/n]? █
```

Después de asignar las redes vamos a ponerle a la "LAN" una IP de red y vamos a asignar un servidor de "DHCP"

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 198.168.100.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 
```

Asignaré el 24 para mascara de red y podremos obtener hasta 254 equipos. No ponemos puerta de enlace porque el propio PFSense lo será. Al servidor DHCP le pondré un rango desde 100 a 200. Y por ultimo marcamos "y" para finalizar.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 198.168.100.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

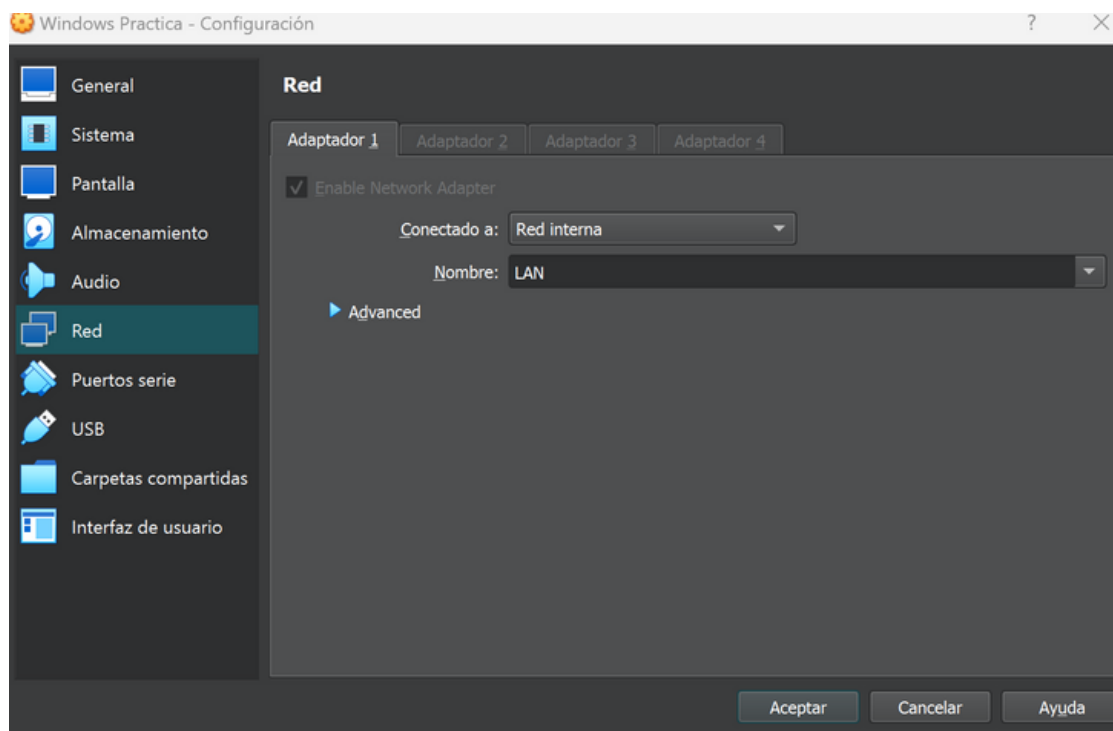
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

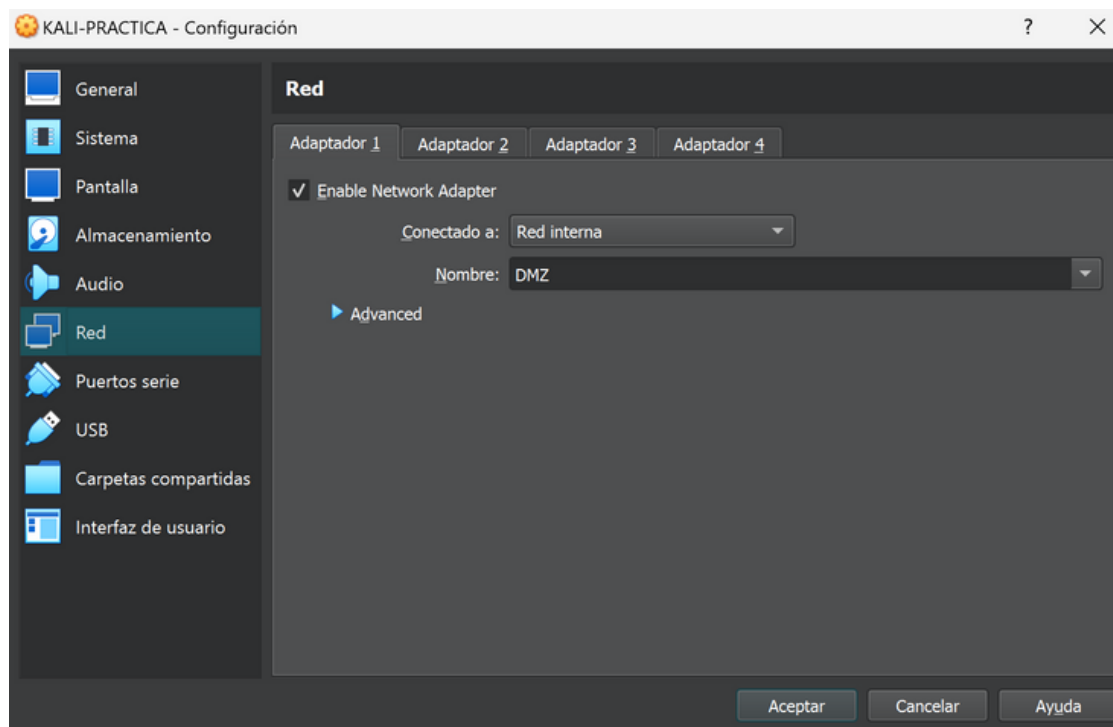
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 198.168.100.100
Enter the end address of the IPv4 client address range: 198.168.100.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) 
```

Windows le asignaré la siguiente red:

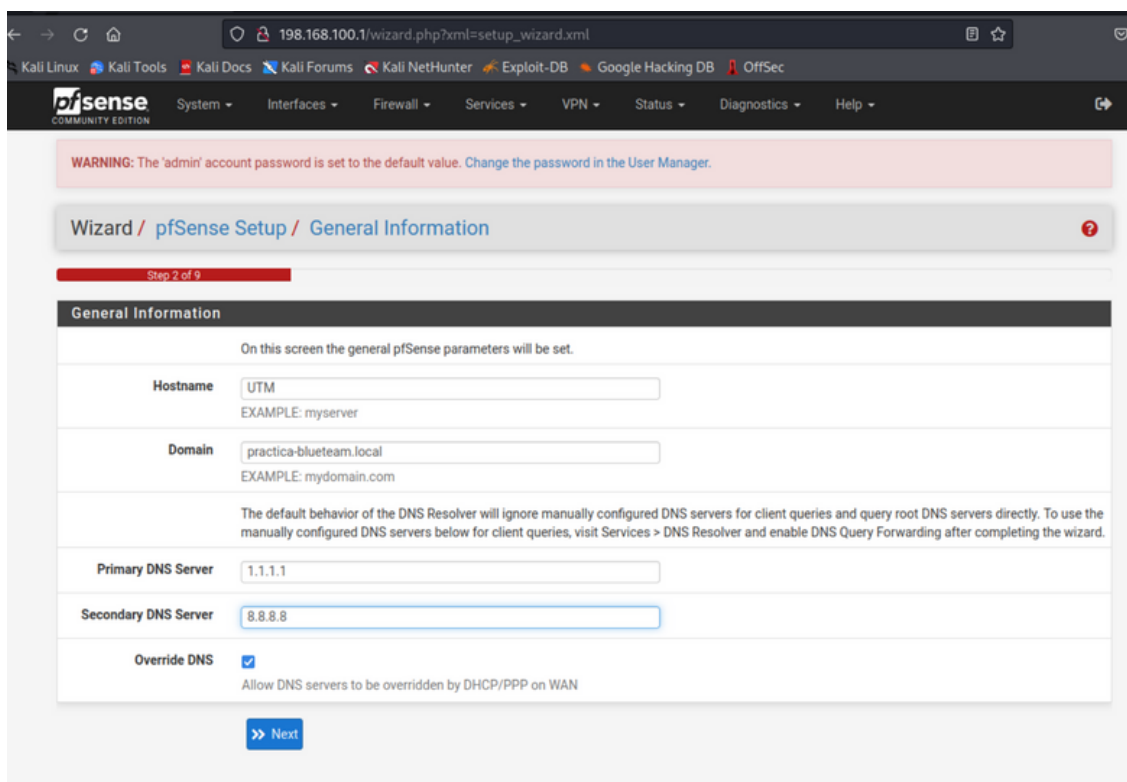


A Kali le asignaré la siguiente red:



PFSENSE

Entramos en la máquina de kali, abrimos navegador y como no hay conexión a internet cambiamos la configuración de red de "DMZ" a "LAN" para poder configurar el pfsense después haremos que la red "DMZ" consiga conexión. Asignamos un nombre de host y un dominio. Ponemos los servidores de DNS 1.1.1.1 (cloudflare) y 8.8.8.8 (google).



The screenshot shows the pfSense Setup Wizard at Step 2 of 9, titled "General Information". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail is "Wizard / pfSense Setup / General Information". The form contains the following fields and options:

- Hostname:** UTM (with an example of "myserver")
- Domain:** practica-blueteam.local (with an example of "mydomain.com")
- Primary DNS Server:** 1.1.1.1
- Secondary DNS Server:** 8.8.8.8
- Override DNS:** A checked checkbox with the text "Allow DNS servers to be overridden by DHCP/PPP on WAN".

A "Next" button is located at the bottom of the form.

Cambiamos los nombres en interfaces a "DMZ" y "DMZ2" y los configuramos .



The screenshot shows the pfSense configuration page for the "DMZ (em2)" interface. The breadcrumb trail is "Interfaces / DMZ (em2)". The "General Configuration" section includes the following settings:

- Enable:** A checked checkbox with the label "Enable interface".
- Description:** A text field containing "DMZ" with a placeholder text "Enter a description (name) for the interface here."

Interfaces / DMZ2 (em3)

The changes have been applied successfully.

General Configuration

Enable ☒ Enable interface

Description

Enter a description (name) for the interface here.

Enable ☒ Enable interface

Description

Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx 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

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 /

IPv4 Upstream gateway [+ 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".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Configuramos el servidor "DHCP" de la red "DMZ" añadiendo los rangos, los servidores "DNS" y la puerta de enlace.

Range

From To

Servers

WINS servers

DNS servers

Other Options

Gateway

The default is to use the IP on this interface of the firewall as the gate

Creamos una DHCP estático y único para Kali, y así la dirección MAC de la máquina que estoy usando de Kali siempre obtendrá la IP "192.168.90.50".

Static DHCP Mapping on DMZ

MAC Address [Copy My MAC](#)
MAC address (6 hex octets separated by colons)

Client Identifier

IP Address
If an IPv4 address is entered, the address must be outside of the pool.
If no IPv4 address is given, one will be dynamically allocated from the pool.
The same IP address may be assigned to multiple mappings.

Hostname
Name of the host, without domain part.

Description
A description may be entered here for administrative reference (not parsed).

ARP Table Static Entry ☒ Create an ARP Table Static Entry for this MAC & IP Address pair.

WINS Servers

DNS Servers
Note: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.

Gateway
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network.

Domain name
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

Domain search list

PONER INTERNET EN DMZ

Necesitamos crear unas reglas para obtener internet en DMZ. Primero para poder navegar por internet necesitamos los puertos que se usan para la comunicación de cliente a sitio para HTTP y HTTPS que son el 80 y el 443.

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters 'a-z, A-Z, 0-9 and _'.

Description
A description may be entered here for administrative reference (not parsed).

Type

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port [Delete](#)

[Delete](#)

[Save](#) [Export to file](#) [+ Add Port](#)

Con el alias creado creo una regla para la navegación web y con protocolo TCP que es lo normal para la navegación web.

The screenshot shows the configuration for a firewall rule. The **Action** is set to 'Pass'. The **Interface** is 'DMZ' and the **Address Family** is 'IPv4'. The **Protocol** is 'TCP'. The **Source** section is set to 'any' for both Source Address and Source Port Range. The **Destination** section is set to 'any' for Destination Address, and the Destination Port Range is set to 'WEB' (port 80) for both From and To. The **Extra Options** section has 'Log' unchecked and a description 'NAVEGACION WEB'.

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface DMZ
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /

[Display Advanced](#)
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match any Destination Address /

Destination Port Range (other) WEB (other) WEB
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description NAVEGACION WEB
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Como la anterior regla no he puesto los DNS ya que no quiero poner como protocolo UDP a los puertos http o https duplico la regla ya creada cambiándole el protocolo TCP/UDP que tratándose de DNS cualquiera de los dos puede ser usado.

This screenshot is similar to the previous one, but the **Protocol** is set to 'TCP/UDP'. The **Destination Port Range** is set to 'DNS (53)' for both From and To, with 'Custom' selected for both. The rest of the configuration remains the same.

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface DMZ
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /

[Display Advanced](#)
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match any Destination Address /

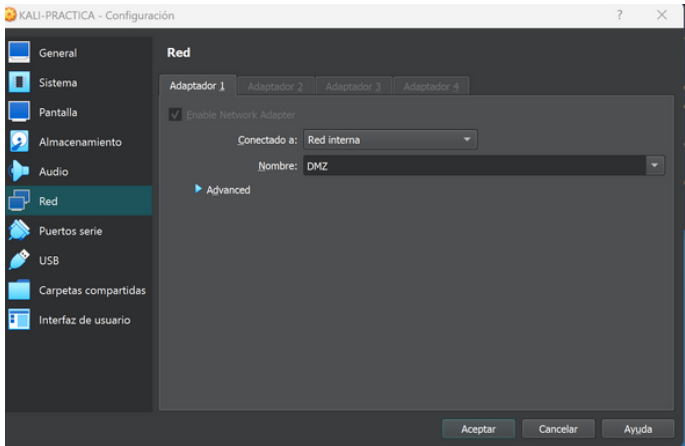
Destination Port Range DNS (53) DNS (53)
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

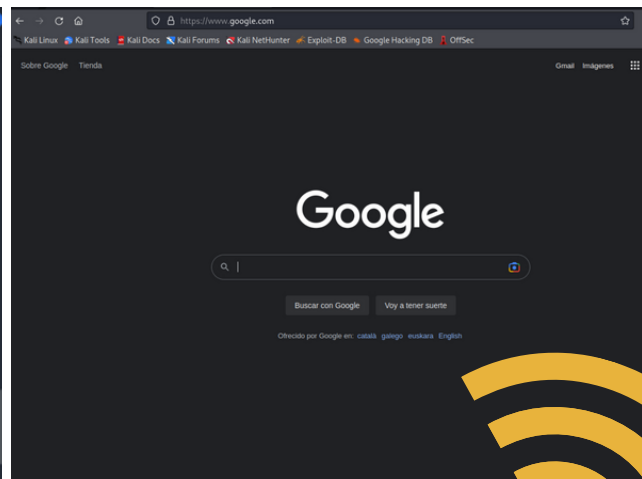
Description NAVEGACION WEB
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Y ahora cambio de "LAN" a "DMZ" para verificar si tiene conexión a internet.



Y compruebo la conexión mediante dos formas.

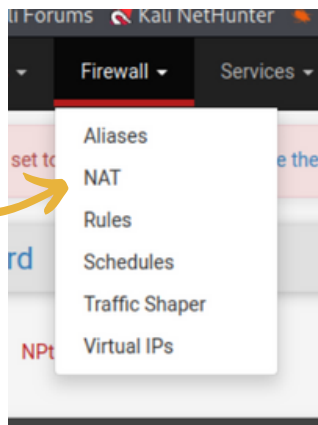
```
kali@kali:~$ ping google.com
PING google.com (142.250.184.14) 56(84) bytes of data:
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
time=13.1 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
time=24.3 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
time=13.3 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
time=13.2 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
time=21.8 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
time=12.7 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
ttl=114 time=12.8 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
_seq=8 ttl=114 time=15.2 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp
_seq=9 ttl=114 time=13.8 ms
^C
```



Y ASÍ PUEDE VER QUE LA RED "DMZ" TIENE ACCESO A INTERNET.

CREAR LA NAT

Dentro de la misma página nos dirigimos a la pestaña de Firewall -> NAT

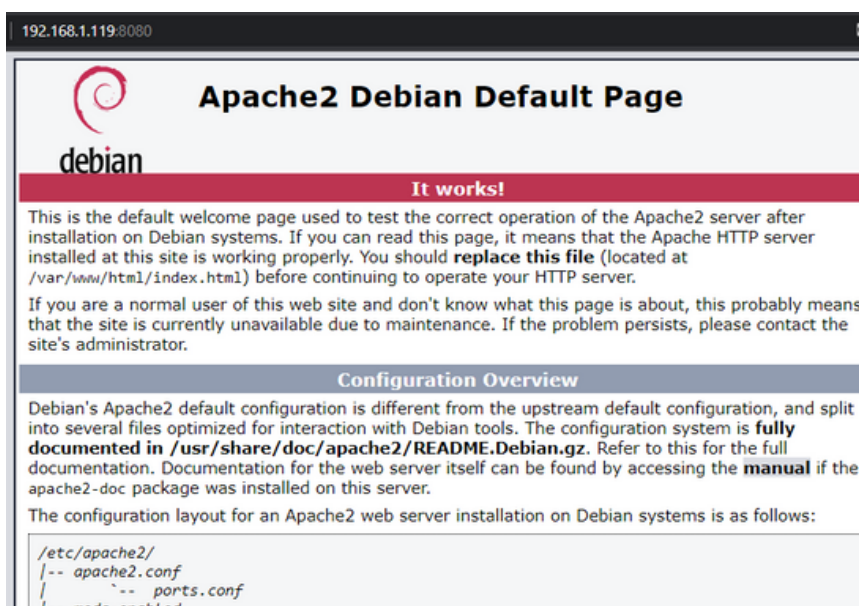


Aquí en la misma sección de "Port Forward", le daremos a "añadir" y lo crearemos con la siguiente configuración

A screenshot of the NAT rule configuration window in Kali NetHunter. The configuration is as follows:

- Disabled:** ☐ Disable this rule
- No RDR (NOT):** ☐ Disable redirection for traffic matching this rule. This option is rarely needed. Don't use this without thorough knowledge of the implications.
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** ☐ Display Advanced
- Destination:** ☐ Invert match. WAN address
- Destination port range:** From port: 8080, To port: 8080
- Redirect target IP:** Single host, 192.168.90.50
- Redirect target port:** Port: 80
- Description:** SERVIDOR WEB
- No XMLRPC Sync:** ☐ Do not automatically sync to other CARP members

Con el comando se "sudo service apache2 start" lo activamos y lo comprobamos con éxito en <http://192.168.1.119:8080/>

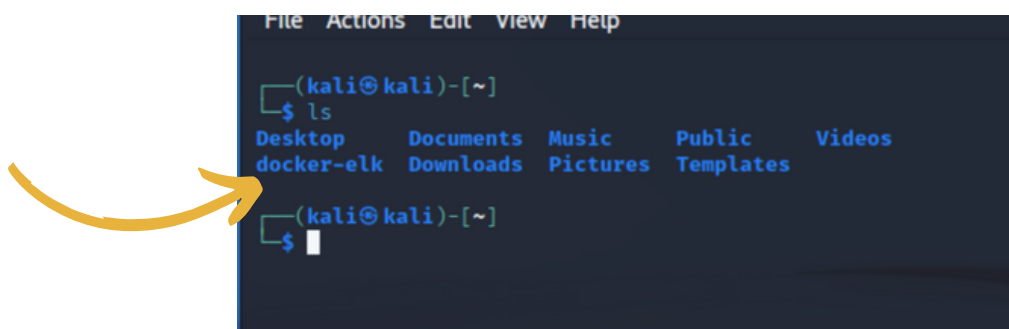


Empezamos con : ELASTIC SEARCH (ELK)

Lo primero será hacernos con el programa mediante un click facilitado en clase por el profesor.

```
(kali@kali)-[~]
$ git clone https://github.com/deviantony/docker-elk.git
Cloning into 'docker-elk' ...
remote: Enumerating objects: 2268, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 2268 (delta 8), reused 24 (delta 5), pack-reused 2235
Receiving objects: 100% (2268/2268), 605.76 KiB | 2.95 MiB/s, done.
Resolving deltas: 100% (992/992), done.
```

Con esto, veremos que tenemos creada ya una carpeta creada con el nombre de "docker-elk"



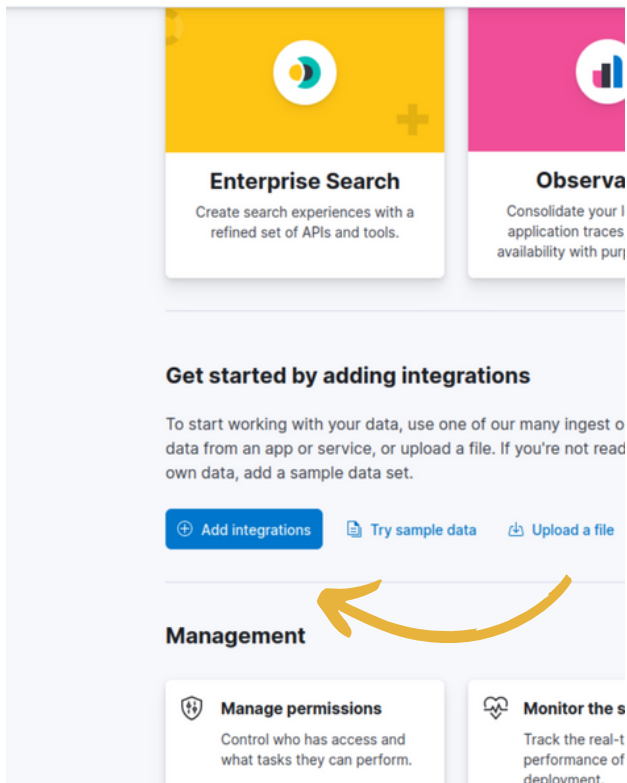
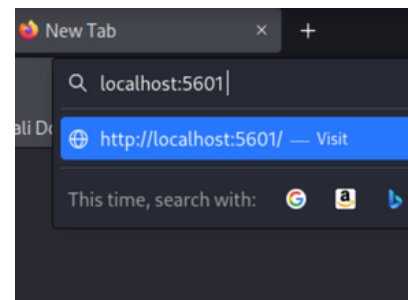
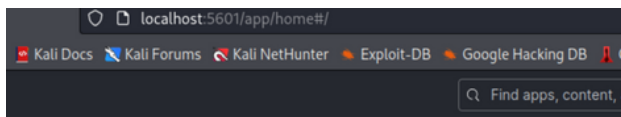
```
File Actions Edit View Help
(kali@kali)-[~]
$ ls
Desktop    Documents  Music      Public     Videos
docker-elk Downloads  Pictures   Templates
```

Nos vamos a esta carpeta y ejecutamos el siguiente comando para descargarnos todos los paquetes necesarios.

```
(kali@kali)-[~/docker-elk]
$ sudo docker-compose up -d
Creating network "docker-elk_elk" with driver "bridge"
Creating docker-elk_elasticsearch_1 ... done
Creating docker-elk_kibana_1 ... done
Creating docker-elk_setup_1 ... done
Creating docker-elk_logstash_1 ... done
(kali@kali)-[~/docker-elk]
```

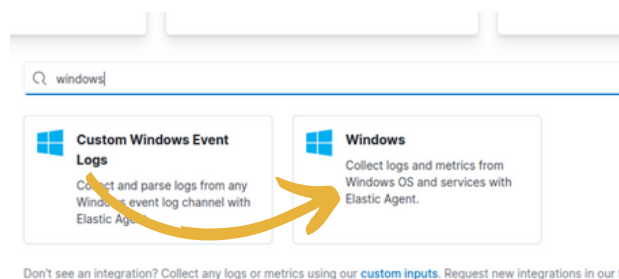
El tener todos con "done" nos indicará que todo ha sido descargado con éxito.

Con esto levantado, podemos dirigirnos a la web del elastic



Nos vamos a "Add integrations"

Y añadiremos la integración de "Windows" ya que nuestro objetivo es conseguir recibir datos de nuestra máquina Windows



Lo prepararemos con la configuración que se muestra en la siguiente imagen, Teniendo en cuenta que el nombre es completamente elección de cada persona.

1 Configure integration

Integration settings
Choose a name and description to help identify how this integration will be used.

Integration name: windows-practica-BT
Description: (Optional)

> Advanced options

☒ Collect events from the following Windows event log channels: [Change defaults](#)

☒ Collect Windows perfmon and service metrics [Change defaults](#)

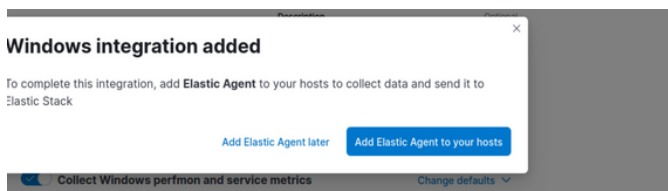
☐ Collect logs from third-party REST API (experimental) [Change defaults](#)

2 Where to add this integration?

New hosts Existing hosts

Agent policy: Agent policies are used to manage a group of integrations across a set of agents. [Agent policy](#)
Fleet Server Policy

Al querer guardar esta integración, el propio elastic nos ofrecerá al momento hacernos con el Agente que necesitamos para windows. Lo aceptaremos y seleccionaremos la opción de "Run Standalone"



Aquí únicamente tendremos que copiar el script que se nos presenta en la parte inferior y a este mismo script, pegándolo en alguna aplicación que no nos modifique el orden del script. Tendremos que realizar sus debidas modificaciones como se muestra en la siguiente imagen de la siguiente página.

Add agent

Add Elastic Agents to your hosts to collect data and send it to Elastic Stack

Enroll in Fleet [Run standalone](#)

Run an Elastic Agent standalone to configure and update the agent

1 Configure the agent

Copy this policy to the `elastic-agent.yml` on the host. Replace `ES_USERNAME` and `ES_PASSWORD` in the `outputs` section with your Elastic Stack credentials.

[Copy to clipboard](#)

[Download Policy](#)

```
id: fleet-server-policy
revision: 5
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'http://elasticsearch:9200'
    username: '${ES_USERNAME}'
    password: '${ES_PASSWORD}'
output_permissions:
```

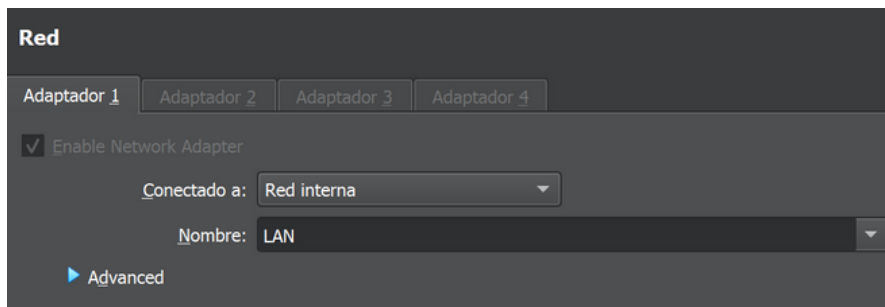

Para saber que IP nos corresponde poner, nos bastará con consultar por medio de nuestra consola que ip tenemos, con el comando "ip a"

```
(kali@kali)~[/docker-elk]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
  aut gln 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
      valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
  roup default qlen 1000
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 192.168.90.50/24 brd 192.168.90.255 scope global dynami
      te eth0
        valid_lft 6145sec preferred_lft 6145sec
        inet6 fe80::e3d1:86c4:567b:3ff6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
File Edit Search View Document Help
1 id: fleet-server-policy
2 revision: 5
3 outputs:
4 default:
5   type: elasticsearch
6   hosts:
7     - 'http://192.168.90.50:9200'
8   username: 'elastic'
9   password: 'changeme'
10 output_permissions:
11 default:
12   _elastic_agent_monitoring:|
13   indices:
14     - names:
15       - logs-elastic_agent.filebeat-default
16     privileges:
17       - auto_configure
18       - create_doc
19     - names:
20       - metrics-elastic_agent.apm_server-default
21     privileges:
22       - auto_configure
23       - create_doc
```

Windows

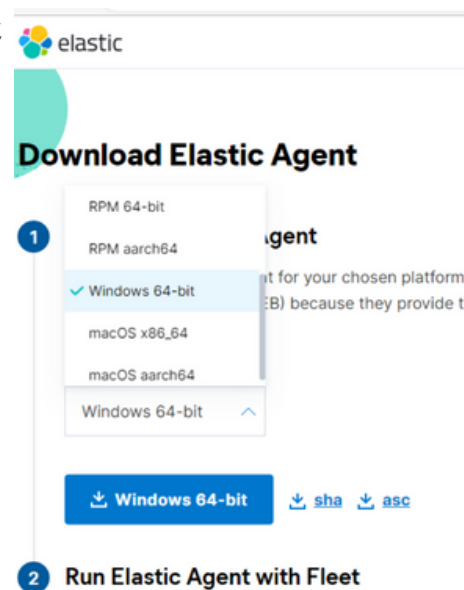
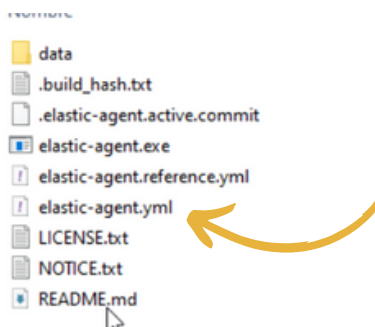
Dejando lo anterior de lado, se ha montado previamente una máquina de Windows gracias a la página oficial de esta con su imagen ISO. En esta máquina que debemos tener en la red de LAN



Tendremos que acceder a la siguiente página web para hacernos con el agente.

www.elastic.co/es/downloads/elastic-agent

Lo descargaremos y lo siguiente será editar el archivo "elastic-agent.yml" sustituyendolo por el script modificado previamente.



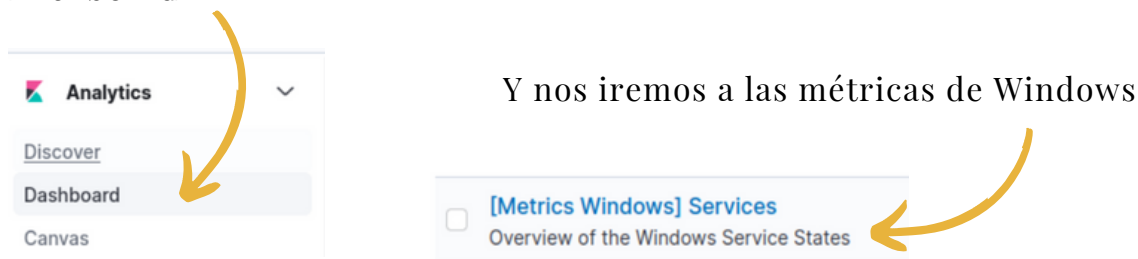
Una vez modificado, nos iremos a CMD (**ejecutando como administrador**) y por medio de esta nos iremos a la ruta donde se encuentra el archivo del elastic agent

```
Administrador: Símbolo del sistema - elastic-agent.exe
Microsoft Windows [Versión 10.0.19045.2130]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd C:\Users\ekewj\Downloads\elastic-agent-8.5.0-windows-x86_64\elastic-agent-8.5.0-windows-x86_64
C:\Users\ekewj\Downloads\elastic-agent-8.5.0-windows-x86_64\elastic-agent-8.5.0-windows-x86_64>elastic-agent.exe
```

Escribiremos el ejecutable y con Enter ya estará activado, trabajando.

Dejando esto de lado, volvemos a Kali para irnos a la parte de Analytics -> Dashboard



Aquí podremos comprobar el éxito de todo el trabajo, recibiendo datos de nuestra máquina, el cual era nuestro objetivo desde un principio !

