

# Práctica Blue Team

KEEP CODING

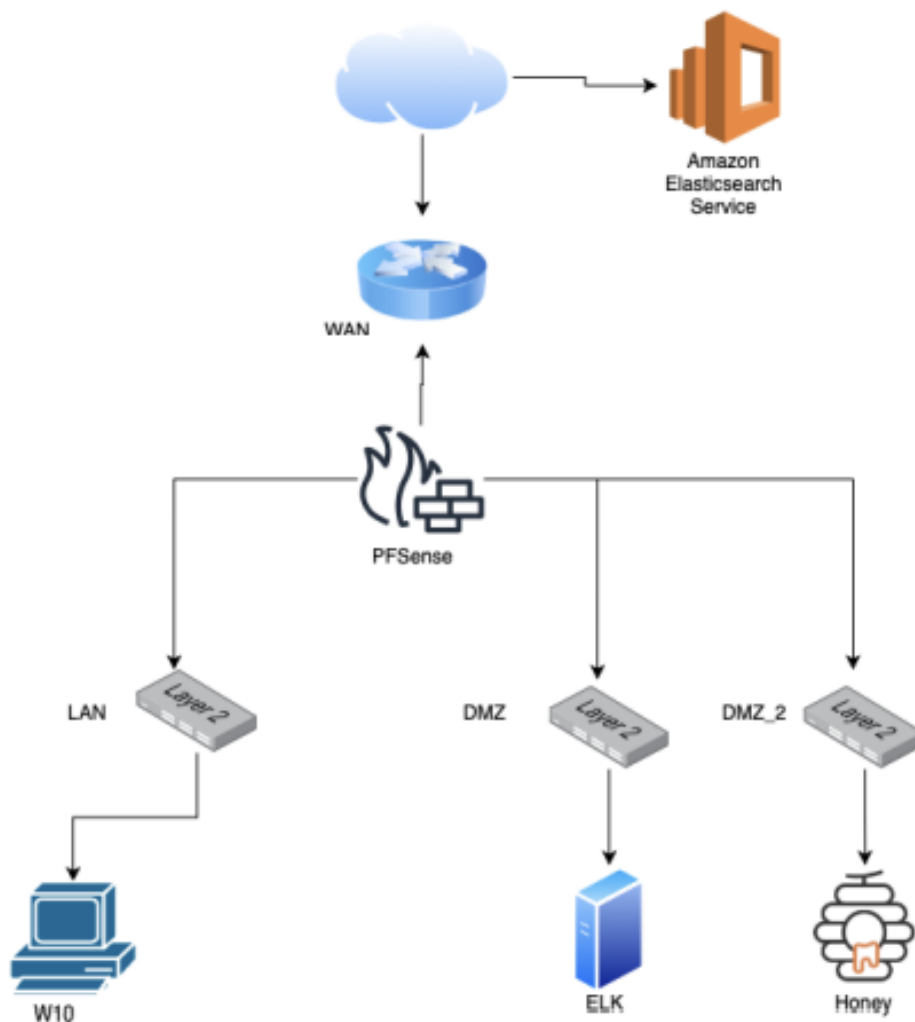
2022/2023

Angie Aristizabal Bernal

# Objetivo

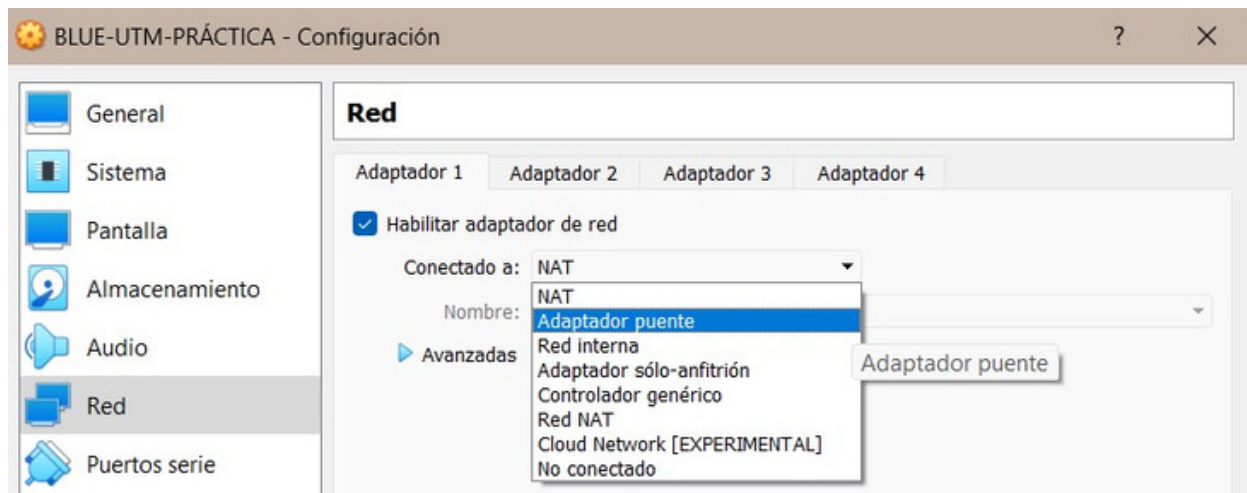
Crear un número de redes la cual intercambie datos, haciendo uso del PfSense en bridge que conecte 3 redes, LAN, DMZ y DMZ\_2 estas como red interna.

Un equipo W10 en LAN, un stack ELK en DMZ



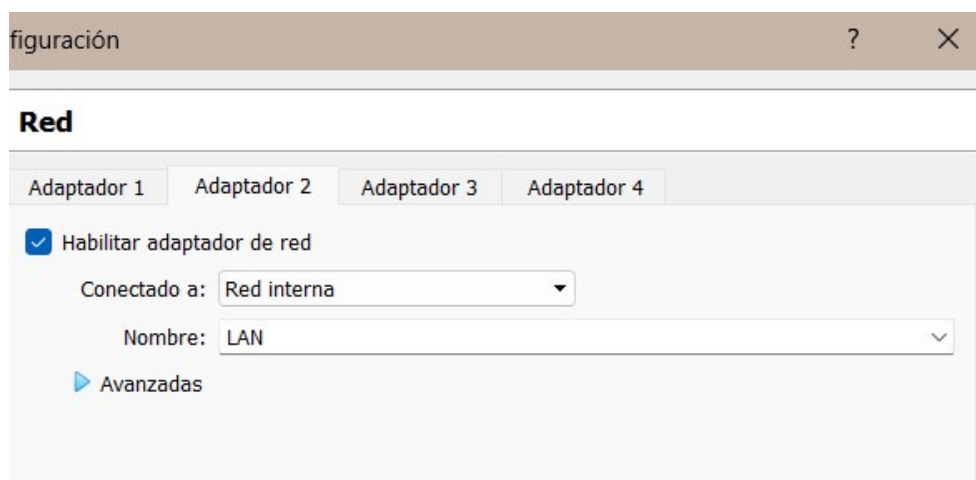
# Creando las redes

Para crear las diferentes redes que se necesitan, hago uso del PfSense facilitado en clase. Una vez instalado sigue configurar el apartado de Red donde lo cambio a "Adaptador puente" :

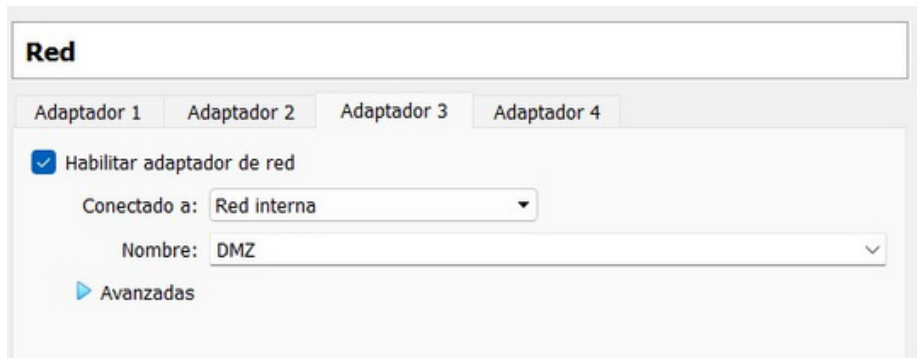


A continuación habilito todos los adaptadores de red que me permite nombrando cada una con sus respectivos nombres:

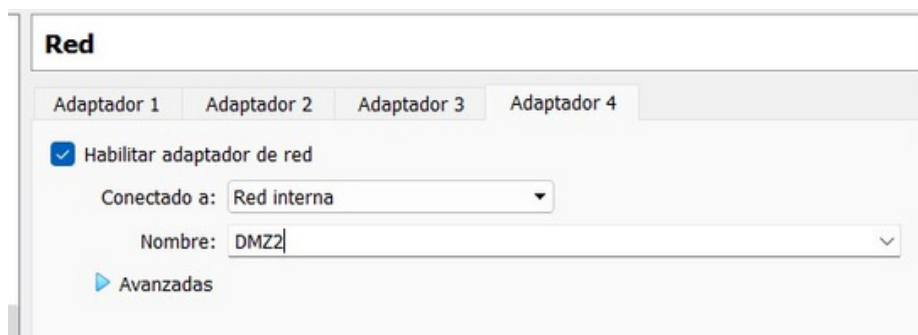
LAN



DMZ



DMZ2



Con esto ya tengo configuradas las 3 redes con sus nombres, que el Pf sense este en "bridge" , y que las redes esten en red interna

Después arranco el UTM y asigno cada interfaz.  
Sé cual corresponde a cada una de las que creó viendo la dirección MAC que me muestra en pantalla.  
Si voy a configuración de red podré ver la dirección MAC de cada una y así saber cual es cual:

```
Archivo  Maquina  Ver  Entrada  Dispositivos  Ayuda
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      08:00:27:88:2c:09      (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:de:d1:22      (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:65:0b:84      (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3      08:00:27:2f:85:61      (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]? █
```

Aquí basándome en lo explicado anteriormente voy asignando cada una sabiendo cual es cual.  
Las DMZ salen como OPT1/2. Se puede dejar tal como esta o cambiarle el nombre para evitar confusiones

```
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]? S █
```

A continuación le pondré una IP propia a LAN para el Pf Sense y también le pondré un servidor de DHCP y a este ponerle un rango desde la 100 a la 200.  
24 como máscara de red

```
4 - OPT2 (em3)

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1

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

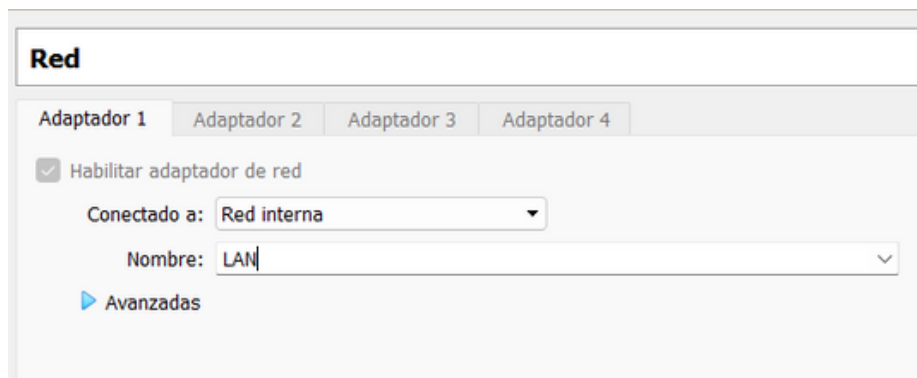
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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: 192.168.100.100
Enter the end address of the IPv4 client address range: 192.168.100.200
```

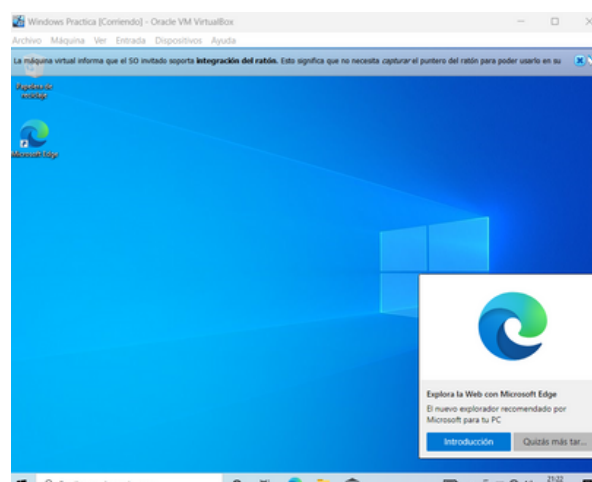
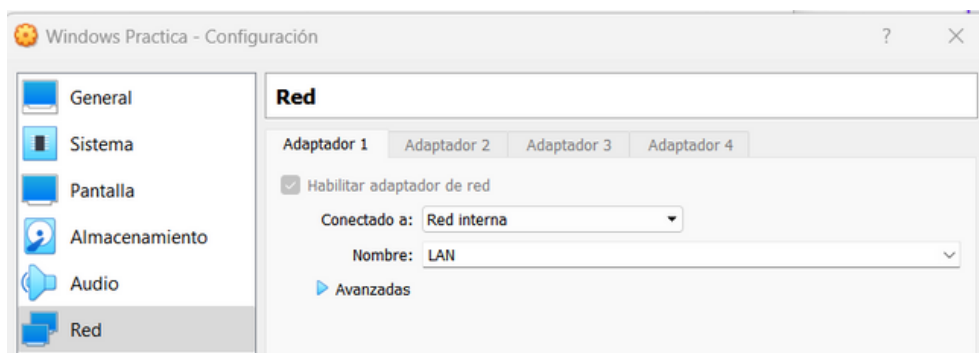
# La máquina de Kali

El Elastic lo pondré sobre una máquina de kali. Pondré esta máquina en LAN de momento para configurar PF sense y que DMZ (donde debe ir el elastic) tenga internet.



# La máquina de Windows

Y así como lo pide la práctica he montado una maquina Windows 10 conectandola a la red LAN. Esta la he conseguido a partir de descargar la ISO de la página oficial



# Configuración pfSense

Através de la máquina de Kali, configuro el pfSense, para conseguir que el DMZ tenga internet también. Usaré como servidores de DNS Google y Cloudflare junto con el time zone

General Information	
On this screen the general pfSense parameters will be set.	
Hostname	<input type="text" value="utm"/> EXAMPLE: myserver
Domain	<input type="text" value="blueteam.local"/> EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	<input type="text" value="1.1.1.1"/>
Secondary DNS Server	<input type="text" value="8.8.8.8"/>
Override DNS	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

Para evitar confusiones les cambio el nombre y les pongo el que les asigne en un principio : DMZ, DMZ2

Interfaces / OPT1 (em2)	
General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> Enter a description (name) for the interface here.
IPv4	<input type="text" value="None"/>

Interfaces / OPT2 (em3)	
General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ2"/> Enter a description (name) for the interface here.



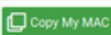
Tipo de IPv4 Static IPv4 y con dirección 192.168.90.1 /24

Despues en el apartado de Services/ DHCP Server /DMZ le asignaré los rangos (de la 100 a la 200) sus servidores de DNS, que seran también 1.1.1.1 y el 8.8.8.8, aunque pondré como prioridad el mismo firewall .


<b>DNS servers</b>	192.168.90.1
	1.1.1.1
	8.8.8.8

Pondré un DHCP Static, asignandole al MAC adress de Kali la ip de mi preferencia, en este caso el IP : 192.168.90.50.

También para evitar un "Man in the Middle" marco que cree una table ARP Static Entry pata la mac e IP que he escrito

Static DHCP Mapping on DMZ				
MAC Address	08:00:27:22:46:4f			
MAC address (6 hex octets separated by colons)				
Client Identifier				
IP Address	192.168.90.50			
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	kali_dmz			
Name of the host, without domain part.				
Description	Kali para DMZ			
A description may be entered here for administrative reference (not parsed).				
ARP Table Static Entry	<input checked="" type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.			
WINS Servers	WINS 1		WINS 2	
DNS Servers	192.168.90.1 1.1.1.1 8.8.8.8 DNS 4			
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	192.168.90.1			
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.				

DHCP Static Mappings for this Interface (total: 1)				
Static ARP	MAC address	IP address	Hostname	Description
✓	08:00:27:22:46:4f	192.168.90.50	kali_dmz	Kali para DMZ



# Regla para tener internet en DMZ

Como por defecto el pfSense si no tiene reglas bloquea todo, necesito crear una regla para permitirle a DMZ el acceso a internet.

Para esto necesito ciertos puertos en especifico que son los que me permitiran hacer esto . Usaré los puertos 80 y 443 (estos los he metido en un alias con nombre "web")

Firewall / Aliases / Edit

**Properties**

**Name** web  
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)

**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	Entry added	Action
80	Tue, 01 Nov 2022 18:27:32 +0100	Delete
443		Delete

Ahora si puedo ir a crear las reglas que necesite. En este caso creare una con protocolo TCP que es lo que suele usarse para la navegación web

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 From (other) web To (other) web  
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 Navegación 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.

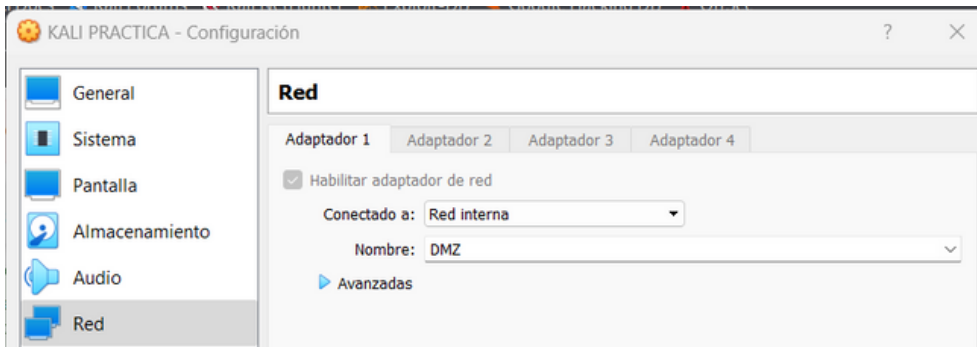
Con esta creada, la duplico para que por si acaso también sea de protocolo UDP (TCP /UCP) ya que se trata de los DNS y puede hacer uso de uno u otro

<b>Interface</b>	DMZ		
	Choose the interface from which packets must come to match this rule.		
<b>Address Family</b>	IPv4		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	TCP/UDP		
	Choose which IP protocol this rule should match.		
<b>Source</b>			
<b>Source</b>	<input type="checkbox"/> Invert match	any	Source Address /
 Display Advanced			
The <b>Source Port Range</b> 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, <b>any</b> .			
<b>Destination</b>			
<b>Destination</b>	<input type="checkbox"/> Invert match	any	Destination Address /
<b>Destination Port Range</b>	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.			
<b>Extra Options</b>			
<b>Log</b>	<input type="checkbox"/> 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 <a href="#">Status: System Logs: Settings</a> page).		
<b>Description</b>	Navegación DNS		
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.			
<b>Advanced Options</b>	 Display Advanced		

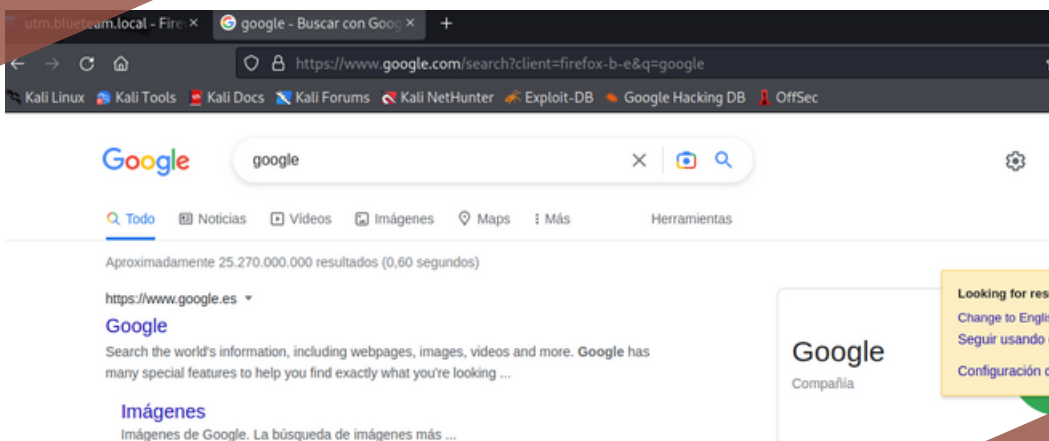
También añado el protocolo ICMP para luego hacer pruebas con "Ping"

internet									
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP <a href="#">any</a>	*	*	*	*	*	none

Ahora a verificar que en DMZ tenga internet



```
(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_seq=1 ttl=114  
time=15.2 ms  
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp_seq=2 ttl=114  
time=12.8 ms  
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp_seq=3 ttl=114  
time=16.0 ms
```



Y ya tenemos acceso a internet.



# Creación de NAT

Ahora dentro del mismo pfSense yendo al apartado Firewall/NAT/Port Forward añado uno para que cualquiera que venga por el puerto 8080 a mi IP pública sea dirigido a la ip de DMZ

Firewall / NAT / Port Forward / Edit

### Edit Redirect Entry

**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  
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

**Protocol** TCP  
Choose which protocol this rule should match. In most cases "TCP" is specified.

**Source** [Display Advanced](#)

**Destination** ☐ Invert match. WAN address Type Address/mask

**Destination port range** Other 8080 Other 8080  
From port Custom To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.

**Redirect target IP** Single host 192.168.90.50  
Type Address  
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

**Redirect target port** Other 80  
Port Custom  
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
This is usually identical to the "From port" above.

**Description** Servidor web

```
(kali@kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:
(kali@kali)-[~]
```

# Elastic

El primer paso sera ejecutar este comando para instalar un contenedor de github que ya contiene todo el conglomerado de máquinas (elastic search, kibana y logstash)

```
File Actions Edit View Help

(kali@kali)-[~]
$ sudo git clone https://github.com/deviantony/docker-elk.git
[sudo] password for kali:
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 | 2.63 MiB/s, done.
Resolving deltas: 100% (992/992), done.

(kali@kali)-[~]
$
```

nos vamos a la carpeta "docker-elk" y con el comando `docker-compose up -d`

```
(root@kali)-[/home/kali]
# cd docker-elk

(root@kali)-[/home/kali/docker-elk]
# ls
docker-compose.yml  extensions  LICENSE  README.md
elasticsearch       kibana     logstash  setup

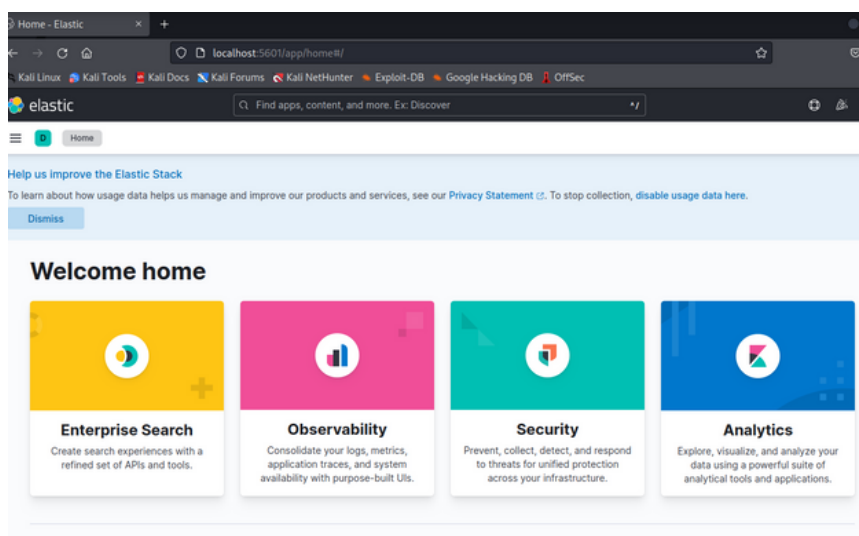
(root@kali)-[/home/kali/docker-elk]
#
```

```
(root@kali)-[/home/kali/docker-elk]
# docker-compose up -d
Command 'docker-compose' not found, but can be installed with:
apt install docker-compose
Do you want to install it? (N/y)y
apt install docker-compose
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cgroudfs-mount containerd criu docker.io libc-bin libc-dev-bin
  libc-devtools libc-l10n libc6 libc6-dev libc6-i386 libintl-perl
  libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl
  libproc-processtable-perl libsort-naturally-perl locales needrestart
  python3-docker python3-dockerpty runc tini
Suggested packages:
  containernetworking-plugins docker-doc aufs-tools btrfs-progs debootstrap
  rinse rootlesskit xfsprogs zfs-fuse | zfsutils-linux glibc-doc libnss-nis
  libnss-nisplus
The following NEW packages will be installed:
  cgroudfs-mount containerd criu docker-compose docker.io libintl-perl
  libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl
  libproc-processtable-perl libsort-naturally-perl needrestart
  python3-docker python3-dockerpty runc tini
The following packages will be upgraded:
```

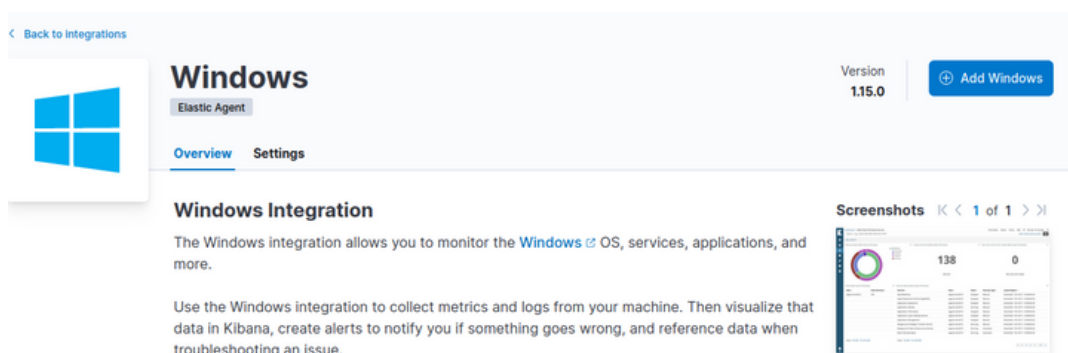
Después de esto parece no haberse descargado todo lo necesario para entrar al elastic por la página así que vuelvo a ejecutar el mismo comando "docker-compose up -d" :

```
c46825c2f625: Pull complete
1fca06af820f: Pull complete
289fb54bb508: Pull complete
9b2e0dcdca04: Pull complete
9cb56e2078f8: Pull complete
Digest: sha256:8de535f9bb25c6c1d0ccd95055b15b824260fc22ccd2bfc376c97dae790cb763
Status: Downloaded newer image for docker.elastic.co/kibana/kibana:8.4.3
→ b14d91e49f3f
Successfully built b14d91e49f3f
Successfully tagged docker-elk_kibana:latest
WARNING: Image for service kibana was built because it did not already exist.
To rebuild this image you must use `docker-compose build` or `docker-compose
up --build`.
Creating docker-elk_elasticsearch_1 ... done
Creating docker-elk_setup_1 ... done
Creating docker-elk_kibana_1 ... done
Creating docker-elk_logstash_1 ... done
```

Y ahora si me confirma que esta todo listo y puedo acceder por medio de  
:  
localhost:5601



Añado la integración de Windows





Con la siguiente configuración:

Integration settings

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

Integration name: windows-blutteam

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

Cancel Save and continue

También acepto de una vez añadir el agente correspondiente y copio el código

## Add agent

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

Enroll in Fleet Run standalone

Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

1 Configure the agent

Copy this policy to the `elastic-agent.yml` on the host where the Elastic Agent is installed. Modify `ES_USERNAME` and `ES_PASSWORD` in the `outputs` section of `elastic-agent.yml` to use your Elasticsearch credentials.

[Copy to clipboard](#) [Download Policy](#)

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

Close



Con esto copiado lo pegaré en el Mousepad del mismo kali y así le haré sus cambios.

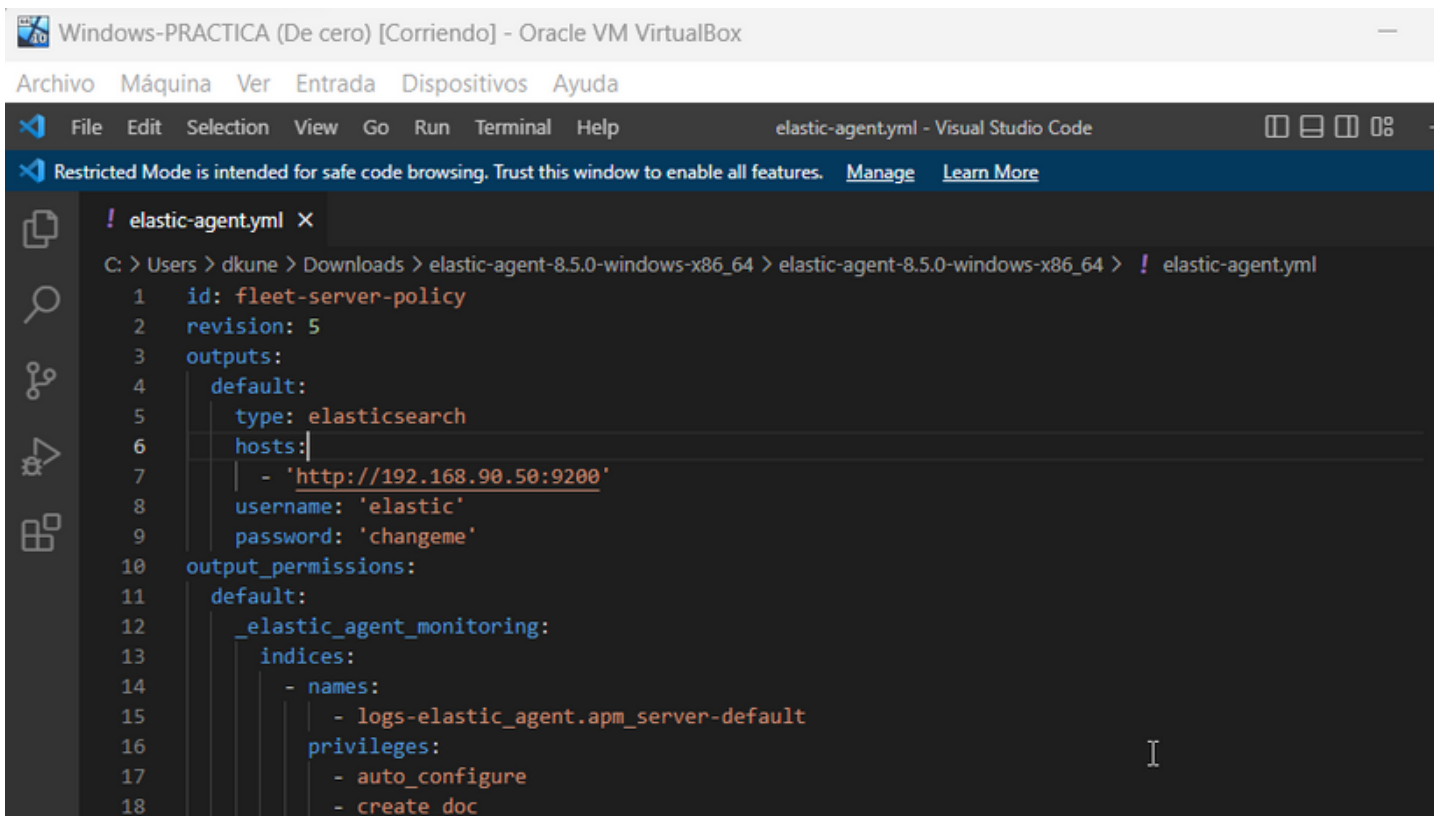
Cambiaré el username y el password que me pone por el que yo usado para ingresar a la página de Elastic y también el host por el IP de mi kali

```
7 - 'http://172.18.0.1:9200'
8   username: 'elastic'
9   password: 'changeme'
10 output_permissions:
11   default:
12     _elastic_agent_monitoring:
13       indices:
14         - names:
15             - logs-elastic_agent.apm_server-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
24         - names:
25             - logs-elastic_agent.auditbeat-default
26           privileges:
27             - auto_configure
28             - create_doc
```

Con esto hecho, me iré a la máquina de Windows previamente montada y me iré a :

[www.elastic.co/es/downloads/elastic-agent](http://www.elastic.co/es/downloads/elastic-agent)  
lo descargo

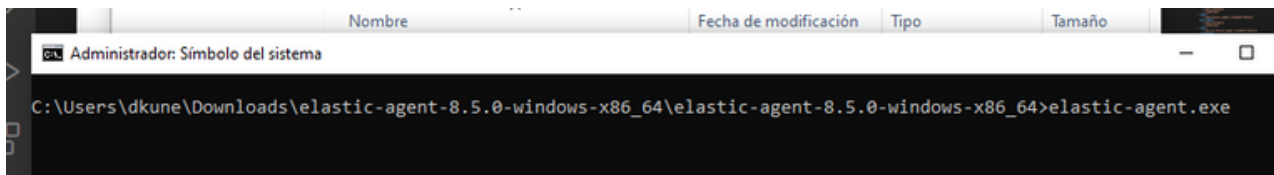
Y una vez descargado editaré el archivo "elastic-agent.yml"  
sustituyendolo por el código escrito anteriormente (con sus cambios correspondientes)



The screenshot shows a Windows VM titled "Windows-PRACTICA (De cero) [Corriendo] - Oracle VM VirtualBox". The interface displays the Visual Studio Code editor with the file "elastic-agent.yml" open. The file path in the address bar is "C:\> Users > dkune > Downloads > elastic-agent-8.5.0-windows-x86\_64 > elastic-agent-8.5.0-windows-x86\_64 > ! elastic-agent.yml". The code in the editor is as follows:

```
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.apm_server-default
16            privileges:
17              - auto_configure
18              - create_doc
```

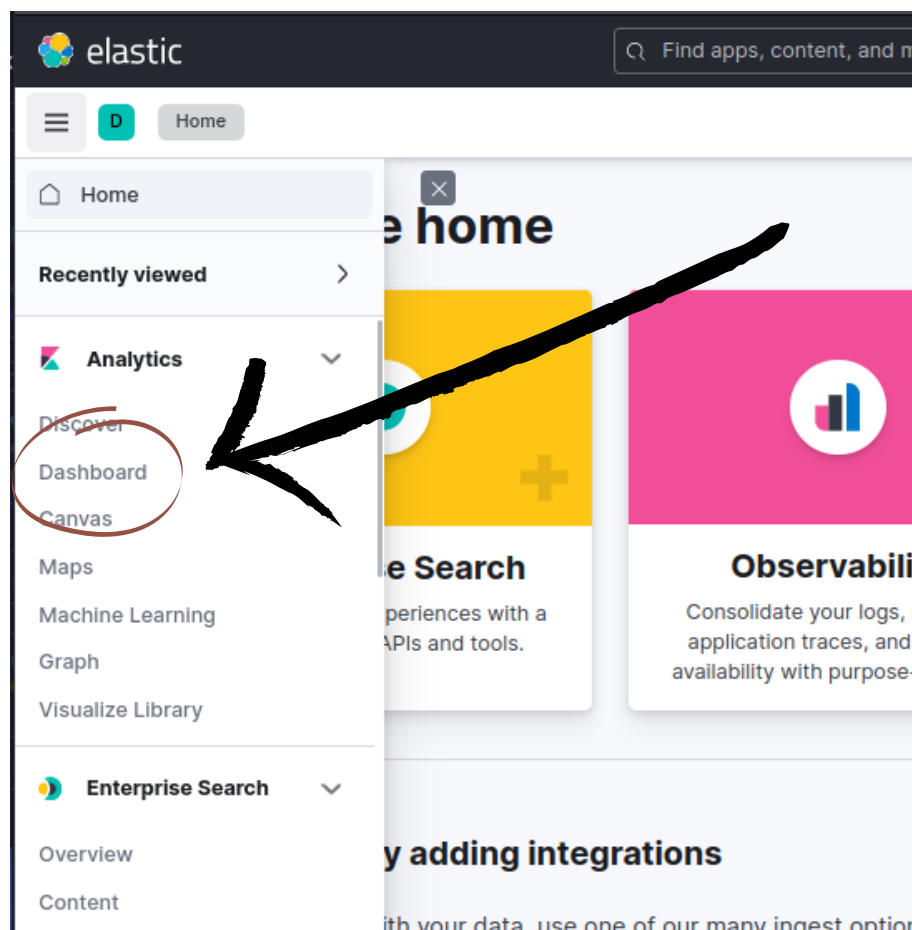
Con esto, en cmd con permisos de administrador, ejecutare el archivo "elastic-agent.exe"



```
Administrador: Símbolo del sistema

C:\Users\dkune\Downloads\elastic-agent-8.5.0-windows-x86_64\elastic-agent-8.5.0-windows-x86_64>elastic-agent.exe
```

Solo nos quedaría dirigirnos a nuestra maquina de Kali, la página de elastic al apartado de "Dashboard"



Ahora buscaremos el apartado que diga "[Metrics Windows] Services"

# Dashboards

Search...

☐ Name, description, tags

☐ [Windows powershell] Overview  
Overview dashboard for powershell integration.

☐ [Metrics Windows] Services  
Overview of the Windows Service States



☐ [System Windows Security] Group Management Events - Simple Metrics  
Group management activity with TSVB metrics.

☐ [System Windows Security] User Logons - Simple Metrics  
User logon activity dashboard with TSVB metrics.

— [Log System] New users and groups

Con esto nos encontraremos con las metricas de nuestro Windows !  
Exitosamente ricibiendo datos de este

