

# Reporte de entorno de Pruebas

Host Name	
User	
Up Time	28 mins, 52 secs
<u>Hardware</u>	
Cpu Type	Intel(R) Core(TM) i5-3317U CPU @ 1.70GHz
<u>Processes</u>	
Cpu	Total: 7%, Kmt: 2%
CPU 0	Total: 8%
CPU 1	Total: 3%
CPU 2	Total: 18%
CPU 3	Total: 0%
Process Count	106
Top Process Cpu	explorer.exe [4992] 12%
Top Process Mem	chrome.exe [5784] 116MB
<u>Windows Configuration</u>	
OS Version	Windows 7 Professional (64 bit)
OS Build	6.1.7601
Screen	1366x768x24
<u>Memory</u>	
Physical Ram	2707MB / 5825MB (45% used)
Virtual Memory	62MB / 2047MB (4% used)
Page File	3062MB / 6523MB (46% used)
Page Faults/sec	Total: 1112, Hard: 2
<u>Network Adapters</u>	
Network Adapter 0	Realtek PCIe GBE Family Controller
Mac Address 0	
IP Address 0	
Gateway 0	
<u>Network Stack</u>	
DNS Server	
Domain Name	
Domain Controller	
Net Connections	181
Net Packets/sec	In: 5, Out: 9
<u>Fixed Disks</u>	
Fixed Disk 0	C: () 65GB / 117GB (55% used)
Disk IO	r=3, w=141 KB/s, q=0

Papelera de  
reciclaje

## Índice

<b>Introducción .....</b>	<b>3</b>
<b>Configuración de la red aislada.....</b>	<b>4</b>
Topología: .....	4
Dispositivos de la red Aislada: .....	4
Detalles de la segmentación y aislamiento de la red .....	5
<b>Configuración IP de Cada Máquina .....</b>	<b>5</b>
OPNsense .....	5
Kali-Linux Defensiva .....	7
Maquina Kali-Linux Ofensiva.....	8
<b>Pruebas de conectividad.....</b>	<b>9</b>
Ping entre Kali-Linux Ofensiva y Kali-Linux Defensiva.....	9
Ping entre Kali-Linux Defensiva y Kali-Linux Ofensiva.....	9
Ping desde Kali-Linux Defensiva a la Máquina Vulnerable (Metasploitable) .....	10
Ping desde Kali-Linux Ofensiva a la Máquina Vulnerable (Metasploitable).....	10
Análisis de Traceroute .....	11
<b>Actualización de máquinas .....</b>	<b>13</b>
Kali-Linux Ofensiva .....	13
Kali-Linux Defensiva .....	14
<b>Bloqueo de acceso a internet a la Maquina Vulnerable (Metasploitable) .....</b>	<b>15</b>
<b>Dificultades encontradas.....</b>	<b>17</b>
<b>Conclusiones.....</b>	<b>17</b>
<b>Detalles adicionales.....</b>	<b>17</b>

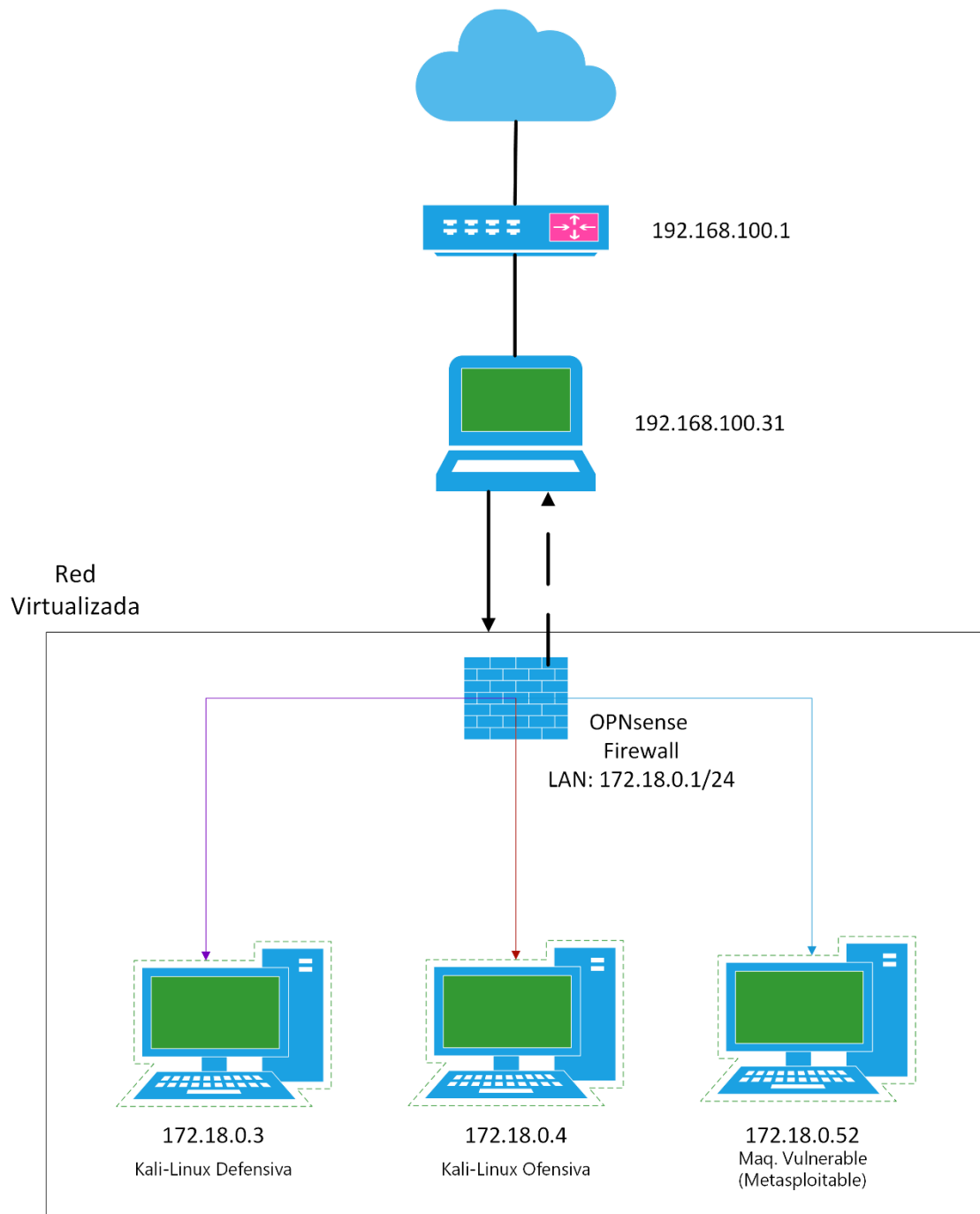
## **Introducción**

Este reporte presenta los resultados de la implementación y análisis de una red aislada para pruebas de ciberseguridad, utilizando las herramientas OPNsense, Kali Linux (Ofensiva y Defensiva), Metasploitable.

Se detallan la configuración de la red, las configuraciones IP de cada máquina, las pruebas de conectividad (ping), el análisis de rutas de paquetes (traceroute), bloqueo de acceso a internet a la maquina Metasploitable, el proceso de actualización de las máquinas Kali Linux, las dificultades encontradas y las conclusiones obtenidas.

## Configuración de la red aislada

### Topología:



### Dispositivos de la red Aislada:

- OPNsense: Enrutador y firewall principal de la red virtualizada
- Kali-Linux Ofensiva: Máquina para realizar ataques y pruebas de penetración.
- Kali-Linux Defensiva: Máquina para defenderse de ataques y analizar vulnerabilidades.
- Metasploitable (VdB): Máquina vulnerable objetivo de los ataques.

## Detalles de la segmentación y aislamiento de la red

La red se diseñó para estar completamente aislada para realizar pruebas tanto ofensivas como defensivas.

### Configuración IP de Cada Máquina

Se detalla la configuración de las máquinas que están dentro de la red virtualizada.

#### OPNsense

Selección de las interfaces de red

**WAN (em0): MAC: 08:00:27:6a:1b:ff**

**LAN (em1): MAC: 08:00:27:3a:22:6d**

```
Valid interfaces are:

em0          08:00:27:6a:1b:ff Intel(R) Legacy PRO/1000 MT 82540EM
em1          08:00:27:3a:22:6d Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

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

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

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed? [y/N]:
```

Configuración del segmento de red para la **LAN (em1)** del OPNsense (Firewall):

- Se le asignó una dirección IP estática 172.18.0.1 para la red interna.
- La máscara de subred /24 <255.255.255.0>
- El Gateway se le asigna el que viene por defecto.
- Se habilita el servidor DHCP para la LAN, desde el segmento:
  - o 172.18.0.50 a 172.18.0.250
  - o el segmento de 172.18.0.2 a 172.18.0.49 y 172.18.0.251 a 172.18.0.254 se las reservan para otros servicios.

```

Available interfaces:

1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.18.0.1

Subnet masks are entered as bit counts (like CIDR notation).
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:
>

```

```

Subnet masks are entered as bit counts (like CIDR notation).
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:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

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: 172.18.0.50
Enter the end address of the IPv4 client address range: 172.18.0.250

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] y
Restore web GUI access defaults? [y/N] y

```

Al finalizar las configuraciones, se podrá ingresar al OPNsense (Firewall) desde cualquier máquina que se encuentre dentro del segmento de red [172.18.0.2] a [172.18.0.254], utilizando un navegador web con la dirección [172.18.0.1]

```

You can now access the web GUI by opening
the following URL in your web browser:

    http://172.18.0.1

*** OPNsense.localdomain: OPNsense 24.1 ***

LAN (em1)      -> v4: 172.18.0.1/24
WAN (em0)      -> v4/DHCP4: 192.168.100.37/24
                v6/DHCP6: 2800:bf0:8120:ce6:a00:27ff:fe6a:1bff/64

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option:

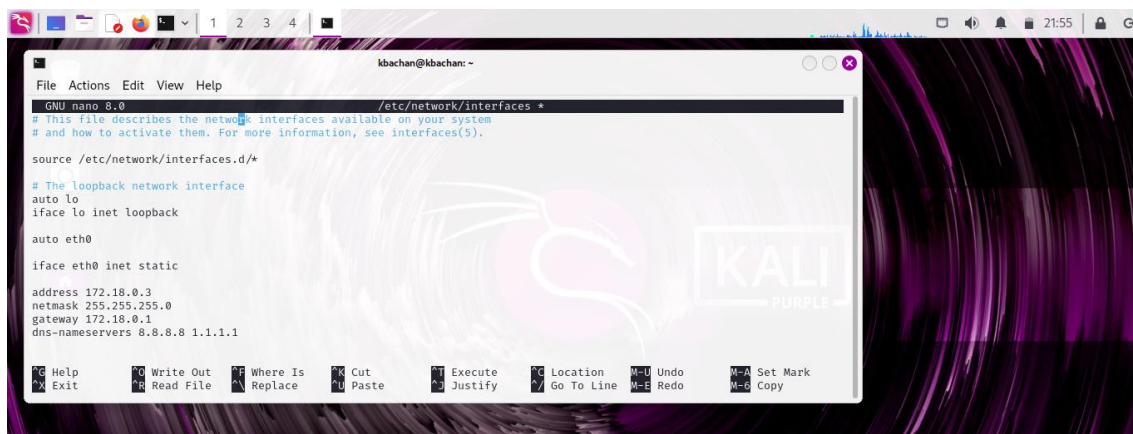
```



## Kali-Linux Defensiva

Configuración de la dirección IP estática:

- Se debe ir archivo de configuración de red **/etc/network/interfaces**,
- Para editar el archivo de configuración de red usamos nano o vim, en este caso:  
**sudo nano/etc/network/interfaces**
- Dentro del archivo primero colocamos el nombre del adaptador de red: **auto eth0**, se puede consultar el nombre del adaptador **ip a**
- Segundo configuramos el adaptador en modo estático: **iface eth0 inet static**
- Por último, configuramos la:
  - o Dirección IP: **172.18.0.3**
  - o Máscara de subred: **255.255.255.0**
  - o Gateway: **172.18.0.1**
  - o Dns-servers: **8.8.8.8 1.1.1.1**



```
GNU nano 8.0 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

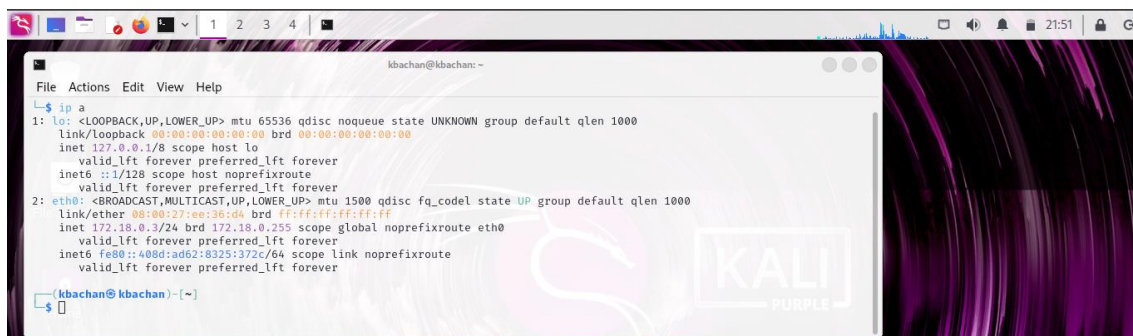
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 172.18.0.3
netmask 255.255.255.0
gateway 172.18.0.1
dns-nameservers 8.8.8.8 1.1.1.1
```

Para aplicar los cambios, se debe reiniciar los servicios de red con el siguiente comando: **sudo systemctl restart networking**

Después de reiniciar los servicios de red, verifica que la nueva configuración esté activa con el siguiente comando: **ip a**



```
kbachan@kbachan: ~
$ 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:ee:36:d4 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.3/24 brd 172.18.0.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::408d:ad62:8325:372c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
kbachan@kbachan: ~
```

## Maquina Kali-Linux Ofensiva

Configuración la dirección IP estática:

- Se debe ir archivo de configuración de red **/etc/network/interfaces**,
- Para editar el archivo de configuración de red usamos nano o vim, en este caso:  
**sudo nano/etc/network/interfaces**
- Dentro del archivo primero colocamos el nombre del adaptador de red: **auto eth0**, se puede consultar el nombre del adaptador `<ip a>`
- Segundo configuramos el adaptador en modo estático: **iface eth0 inet static**
- Por último, configuramos la:
  - o Dirección IP: **172.18.0.4**
  - o Máscara de subred: **255.255.255.0**
  - o Gateway: **172.18.0.1**
  - o Dns-servers: **8.8.8.8 1.1.1.1**



```
File Actions Edit View Help
GNU nano 8.0 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

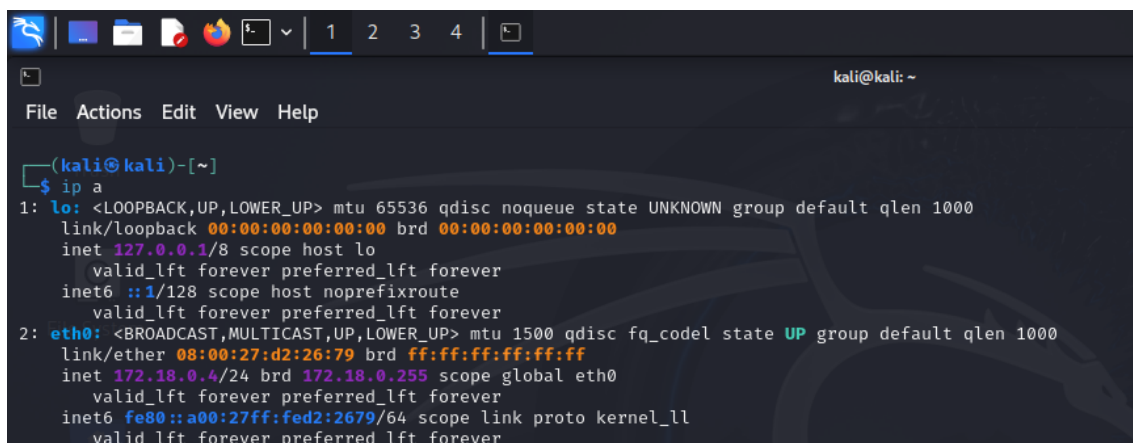
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 172.18.0.4
netmask 255.255.255.0
gateway 172.18.0.1
dns-nameservers 8.8.8.8 1.1.1.1
```

Para aplicar los cambios, se debe reiniciar los servicios de red con el siguiente comando:

**sudo systemctl restart networking**

Después de reiniciar los servicios de red, verifica que la nueva configuración esté activa con el siguiente comando: **ip a**



```
(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:d2:26:79 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.4/24 brd 172.18.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed2:2679/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

*La máquina vulnerable (Metasploitable), el OPNsense le asigna de forma dinámica la IP, en este caso la IP es 172.18.0.52*



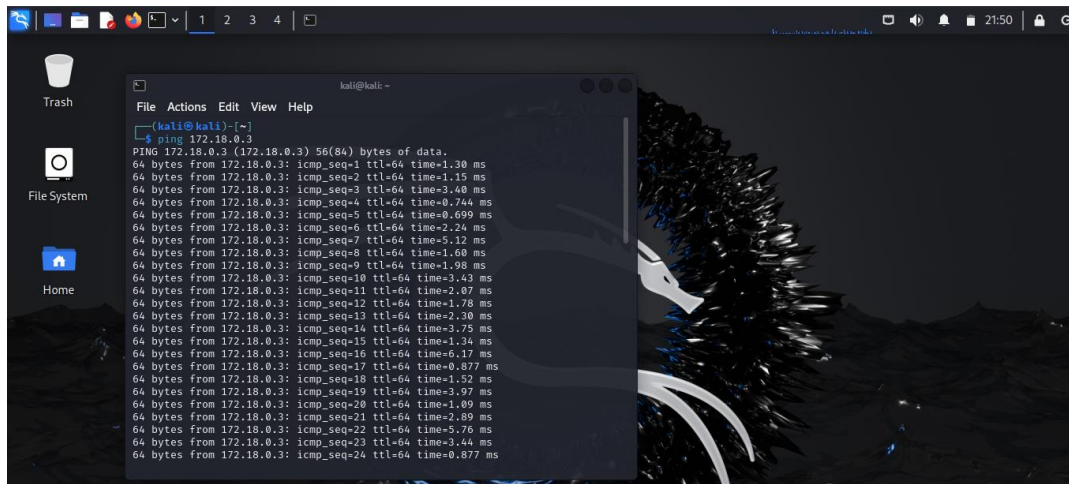
## Pruebas de conectividad

Se realizaron pruebas ping exitosas entre todas las máquinas, confirmando la conectividad en la red.

### Ping entre Kali-Linux Ofensiva y Kali-Linux Defensiva

- En la máquina Kali-Linux Ofensiva, se realizó ping a la dirección 172.18.0.3, asignada en la maquina Kali-Linux Defensiva. Obteniendo pings exitosos.

Comando: **ping 172.18.0.3**

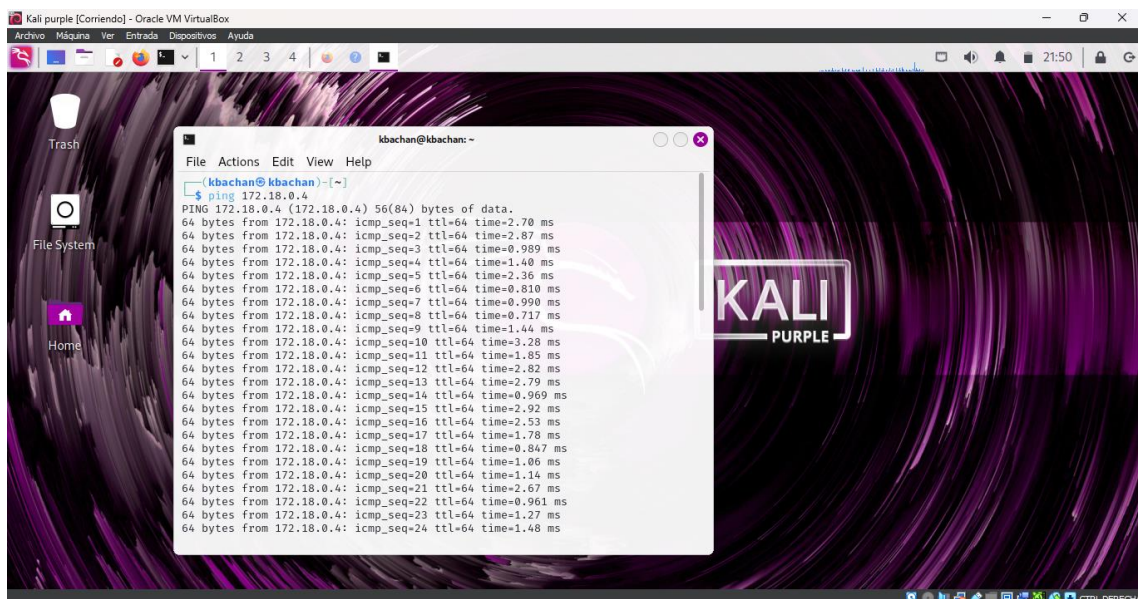


```
kali@kali: ~  
$ ping 172.18.0.3  
PING 172.18.0.3 (172.18.0.3) 56(84) bytes of data:  
64 bytes from 172.18.0.3: icmp_seq=1 ttl=64 time=1.30 ms  
64 bytes from 172.18.0.3: icmp_seq=2 ttl=64 time=1.15 ms  
64 bytes from 172.18.0.3: icmp_seq=3 ttl=64 time=3.40 ms  
64 bytes from 172.18.0.3: icmp_seq=4 ttl=64 time=0.744 ms  
64 bytes from 172.18.0.3: icmp_seq=5 ttl=64 time=0.699 ms  
64 bytes from 172.18.0.3: icmp_seq=6 ttl=64 time=2.24 ms  
64 bytes from 172.18.0.3: icmp_seq=7 ttl=64 time=5.12 ms  
64 bytes from 172.18.0.3: icmp_seq=8 ttl=64 time=1.60 ms  
64 bytes from 172.18.0.3: icmp_seq=9 ttl=64 time=1.98 ms  
64 bytes from 172.18.0.3: icmp_seq=10 ttl=64 time=3.43 ms  
64 bytes from 172.18.0.3: icmp_seq=11 ttl=64 time=2.07 ms  
64 bytes from 172.18.0.3: icmp_seq=12 ttl=64 time=1.78 ms  
64 bytes from 172.18.0.3: icmp_seq=13 ttl=64 time=2.30 ms  
64 bytes from 172.18.0.3: icmp_seq=14 ttl=64 time=3.75 ms  
64 bytes from 172.18.0.3: icmp_seq=15 ttl=64 time=1.34 ms  
64 bytes from 172.18.0.3: icmp_seq=16 ttl=64 time=6.17 ms  
64 bytes from 172.18.0.3: icmp_seq=17 ttl=64 time=0.877 ms  
64 bytes from 172.18.0.3: icmp_seq=18 ttl=64 time=1.52 ms  
64 bytes from 172.18.0.3: icmp_seq=19 ttl=64 time=3.97 ms  
64 bytes from 172.18.0.3: icmp_seq=20 ttl=64 time=1.09 ms  
64 bytes from 172.18.0.3: icmp_seq=21 ttl=64 time=2.89 ms  
64 bytes from 172.18.0.3: icmp_seq=22 ttl=64 time=5.76 ms  
64 bytes from 172.18.0.3: icmp_seq=23 ttl=64 time=3.44 ms  
64 bytes from 172.18.0.3: icmp_seq=24 ttl=64 time=0.877 ms
```

### Ping entre Kali-Linux Defensiva y Kali-Linux Ofensiva

- En la máquina Kali-Linux Defensiva, hacemos ping a la dirección 172.18.0.4, asignada en la maquina Kali-Linux Ofensiva. Obteniendo pings exitosos.

Comando: **ping 172.18.0.4**

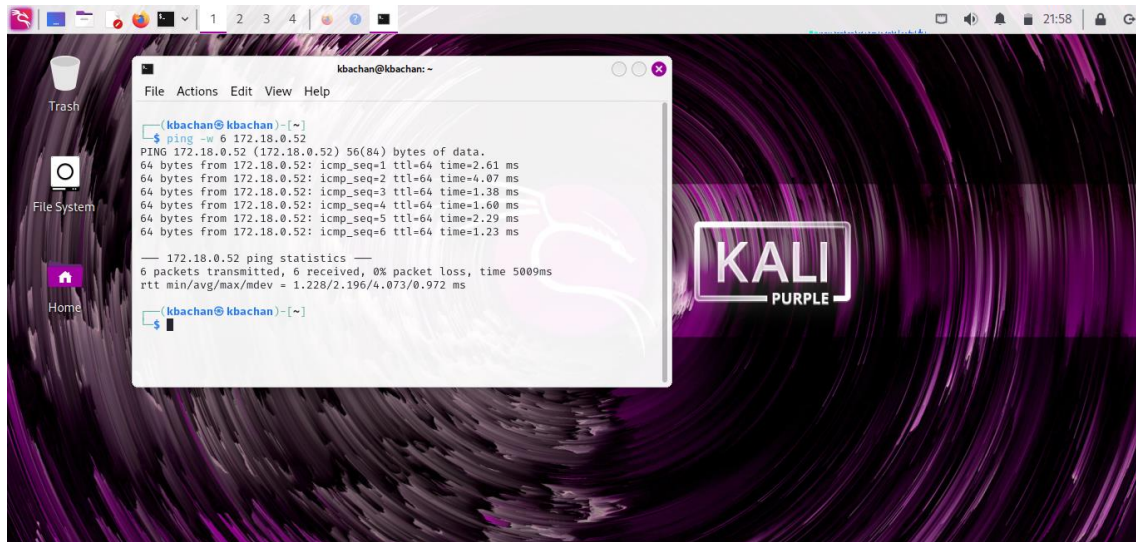


```
kbachan@kbachan: ~  
$ ping 172.18.0.4  
PING 172.18.0.4 (172.18.0.4) 56(84) bytes of data:  
64 bytes from 172.18.0.4: icmp_seq=1 ttl=64 time=2.70 ms  
64 bytes from 172.18.0.4: icmp_seq=2 ttl=64 time=2.87 ms  
64 bytes from 172.18.0.4: icmp_seq=3 ttl=64 time=0.989 ms  
64 bytes from 172.18.0.4: icmp_seq=4 ttl=64 time=1.40 ms  
64 bytes from 172.18.0.4: icmp_seq=5 ttl=64 time=2.36 ms  
64 bytes from 172.18.0.4: icmp_seq=6 ttl=64 time=0.810 ms  
64 bytes from 172.18.0.4: icmp_seq=7 ttl=64 time=0.990 ms  
64 bytes from 172.18.0.4: icmp_seq=8 ttl=64 time=0.717 ms  
64 bytes from 172.18.0.4: icmp_seq=9 ttl=64 time=1.44 ms  
64 bytes from 172.18.0.4: icmp_seq=10 ttl=64 time=3.28 ms  
64 bytes from 172.18.0.4: icmp_seq=11 ttl=64 time=1.85 ms  
64 bytes from 172.18.0.4: icmp_seq=12 ttl=64 time=2.82 ms  
64 bytes from 172.18.0.4: icmp_seq=13 ttl=64 time=2.79 ms  
64 bytes from 172.18.0.4: icmp_seq=14 ttl=64 time=0.969 ms  
64 bytes from 172.18.0.4: icmp_seq=15 ttl=64 time=2.92 ms  
64 bytes from 172.18.0.4: icmp_seq=16 ttl=64 time=2.53 ms  
64 bytes from 172.18.0.4: icmp_seq=17 ttl=64 time=1.78 ms  
64 bytes from 172.18.0.4: icmp_seq=18 ttl=64 time=0.847 ms  
64 bytes from 172.18.0.4: icmp_seq=19 ttl=64 time=1.06 ms  
64 bytes from 172.18.0.4: icmp_seq=20 ttl=64 time=1.14 ms  
64 bytes from 172.18.0.4: icmp_seq=21 ttl=64 time=2.67 ms  
64 bytes from 172.18.0.4: icmp_seq=22 ttl=64 time=0.961 ms  
64 bytes from 172.18.0.4: icmp_seq=23 ttl=64 time=1.27 ms  
64 bytes from 172.18.0.4: icmp_seq=24 ttl=64 time=1.48 ms
```

## Ping desde Kali-Linux Defensiva a la Máquina Vulnerable (Metasploitable)

- En la máquina Kali-Linux Defensiva, se realizó ping a la dirección 172.18.0.52, asignada en la maquina vulnerable. Obteniendo pings exitosos.

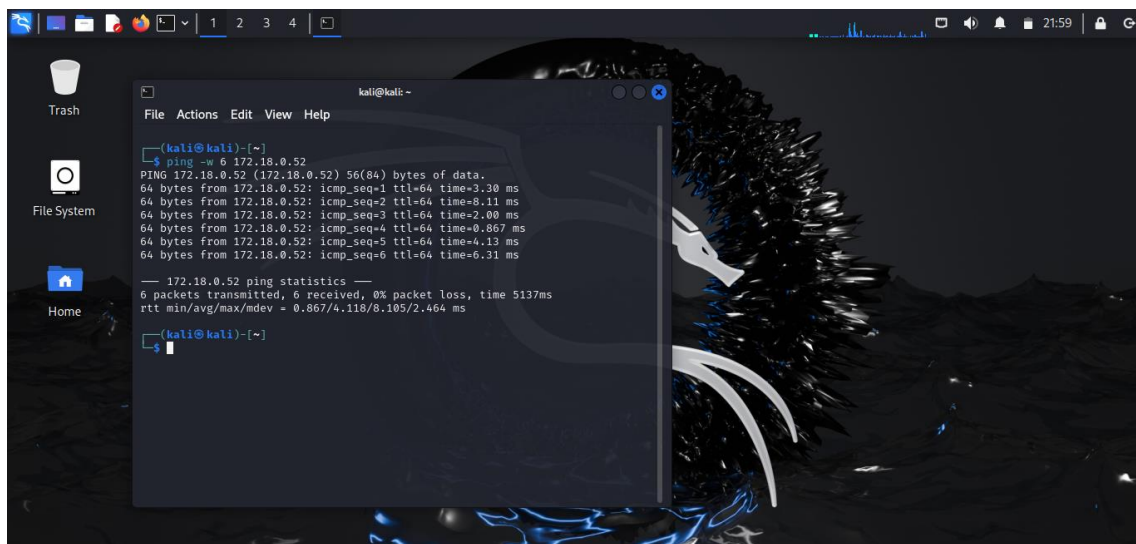
Comando: **ping -w 6 172.18.0.52**



## Ping desde Kali-Linux Ofensiva a la Máquina Vulnerable (Metasploitable)

- En la máquina Kali-Linux Ofensiva, se realizó ping a la dirección 172.18.0.52, asignada en la maquina vulnerable. Obteniendo pings exitosos.

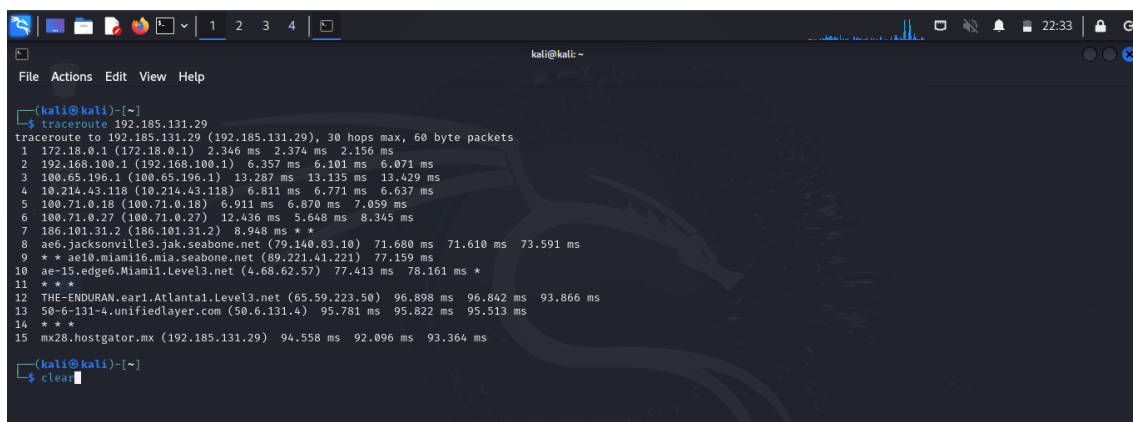
Comando: **ping -w 6 172.18.0.52**



*El modificador `-w` se utilizó para establecer el tiempo máximo, en milisegundos, que ping esperará por una respuesta antes de finalizar. En el caso del comando `ping -w 6`, se está indicando que el tiempo de espera máximo para recibir una respuesta es de 6 milisegundos.*

## Análisis de Traceroute

Se realizó un traceroute desde Kali-Linux Ofensiva a una dirección de internet [192.185.131.29] para analizar la ruta de los paquetes.



```
(kali@kali)~$ traceroute 192.185.131.29
traceroute to 192.185.131.29 (192.185.131.29), 30 hops max, 60 byte packets
 1 172.18.0.1 (172.18.0.1)  2.346 ms  2.374 ms  2.156 ms
 2 192.168.100.1 (192.168.100.1)  6.357 ms  6.101 ms  6.071 ms
 3 100.65.196.1 (100.65.196.1)  13.287 ms  13.135 ms  13.429 ms
 4 10.214.43.118 (10.214.43.118)  6.811 ms  6.771 ms  6.627 ms
 5 100.71.0.18 (100.71.0.18)  6.911 ms  6.870 ms  7.059 ms
 6 100.71.0.27 (100.71.0.27)  12.436 ms  5.648 ms  8.345 ms
 7 186.101.31.2 (186.101.31.2)  8.948 ms * *
 8 ae6.jacksonville3.jak.seabone.net (79.140.83.10)  71.680 ms  71.610 ms  73.591 ms
 9 * * ae10.miami16.mia.seabone.net (89.221.41.221)  77.159 ms
10 ae-15.edge6.Miami1.Level3.net (4.68.62.57)  77.413 ms  78.161 ms *
11 * * *
12 THE-ENDURAN.ear1.Atlanta1.Level3.net (65.59.223.50)  96.898 ms  96.842 ms  93.866 ms
13 50-6-131-4.unifiedlayer.com (50.6.131.4)  95.781 ms  95.822 ms  95.513 ms
14 * * *
15 mx28.hostgator.mx (192.185.131.29)  94.558 ms  92.096 ms  93.364 ms

(kali@kali)~$ clear
```

## Análisis de los saltos

El comando traceroute muestra cada salto que un paquete realiza desde su origen hasta el destino. Cada línea en el resultado corresponde a un "salto", que es un enrutador o nodo intermedio por el que el paquete pasa en su camino hacia el destino final. Aquí está el análisis de cada salto según la salida proporcionada:

**Primer salto:** 172.18.0.1 (172.18.0.1): Enrutador o puerta de enlace de la red local. Los tiempos de respuesta son alrededor de 2.346 ms.

**Segundo salto:** 192.168.100.1 (192.168.100.1): Dispositivo de red local o un enrutador interno de la red del ISP. Los tiempos de respuesta son alrededor de 6.357 ms.

**Tercer salto:** 100.65.196.1 (100.65.196.1): Este es un enrutador en la red del ISP. Los tiempos de respuesta son alrededor de 13.287 ms.

**Cuarto salto:** 10.214.43.118 (10.214.43.118): Este es un enrutador que probablemente pertenece a un proveedor de servicios de Internet más grande o a una red troncal. Los tiempos de respuesta son alrededor de 6.811 ms.

**Quinto salto:** 100.71.0.18 (100.71.0.18): Otro enrutador en la red troncal del ISP. Los tiempos de respuesta son alrededor de 6.911 ms.

**Sexto salto:** 100.71.0.27 (100.71.0.27): Otro enrutador con tiempos de respuesta alrededor de 12.436 ms.

**Séptimo salto:** 186.101.31.2 (186.101.31.2): Nodo intermedio que muestra tiempos de respuesta de 8.948 ms, con dos respuestas perdidas (\* \*).

**Octavo salto:** ae6.jacksonville3.jak.seabone.net (79.140.83.10): Enrutador en la red troncal, probablemente en Jacksonville, con tiempos de respuesta alrededor de 71.680 ms.

**Noveno salto:** ae10.miami16.mia.seabone.net (89.221.41.221): Otro enrutador, probablemente en Miami, con tiempos de respuesta alrededor de 77.159 ms, con dos respuestas perdidas (\* \*).

**Décimo salto:** ae-15.edge6.Miami1.Level3.net (4.68.62.57): Nodo intermedio en la red de Level3 en Miami, con tiempos de respuesta alrededor de 77.413 ms.

**Undécimo salto:** \* \* \*: No se recibieron respuestas en este salto, lo cual es común en algunas configuraciones de red o dispositivos que bloquean las respuestas ICMP.

**Duodécimo salto:** THE-ENDURAN.ear1.Atlanta1.Level3.net (65.59.223.50): Nodo intermedio en la red de Level3 en Atlanta, con tiempos de respuesta alrededor de 96.898 ms.

**Décimo tercer salto:** 50-6-131-4.unifiedlayer.com (50.6.131.4): Nodo intermedio que muestra tiempos de respuesta alrededor de 95.781 ms.

**Décimo cuarto salto:** \* \* \*: No se recibieron respuestas en este salto, posiblemente debido a un firewall o configuración de red.

**Décimo quinto salto:** mx28.hostgator.mx (192.185.131.29): Destino final con tiempos de respuesta alrededor de 94.558 ms.

### **Conclusiones**

**Salto Interno:** Los primeros dos saltos están dentro de la red local o la red del ISP con tiempos de respuesta menores a 10 ms.

**Red Troncal:** Los siguientes saltos (3 al 13) son a través de la red troncal del ISP y posiblemente otros proveedores de servicios de Internet mayores, incluidos nodos en Jacksonville, Miami y Atlanta.

**Tiempos de Respuesta:** Los tiempos de respuesta aumentan a medida que el paquete viaja más lejos de la red local, lo cual es normal. Los tiempos son consistentes y razonables para la distancia.

**Salto sin Respuesta:** Los saltos 7, 9, 11 y 14 tienen respuestas perdidas (\* \* \*), lo cual puede deberse a configuraciones de red o firewalls que bloquean las respuestas ICMP.

**Destinatario Final:** El último salto muestra la llegada del paquete al destino, 192.185.131.29, con un tiempo de respuesta razonable de aproximadamente 94.558 ms.



## Actualización de máquinas

### Kali-Linux Ofensiva

- Se actualiza la lista de repositorios, ejecutando el comando:

**sudo apt update**

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ sudo apt update  
[sudo] password for kali:  
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.4 MB]  
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [113 kB]  
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [27 1 kB]  
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]  
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8 62 kB]  
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [39.1 kB]  
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]  
Fetched 68.8 MB in 9s (7,602 kB/s)  
502 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- Se actualiza los paquetes instalados a sus últimas versiones ejecutando el comando:

**sudo apt upgrade -y**

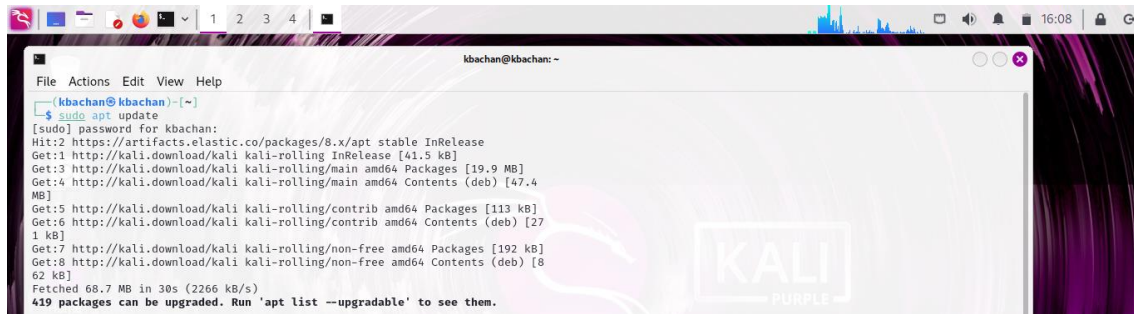
```
[kali@kali]~$ sudo apt upgrade -y  
The following packages were automatically installed and are no longer required:  
libdaxctl1 libx10.7 libpmem1 libu2f-udev openjdk-21-jre python3-mistune0 samba-dsdb-modules  
libgeos3-1.2 libx11-2 libx265-199 openjdk-21-jre-headless samba-ad-provision  
Use 'sudo apt autoremove' to remove them.  
  
Upgrading:  
7zip iw libhwloc-plugins linux-image-amd64 python3-lib2to3  
alsa-topology-conf keyboard-configuration libhwloc5 linux-libc-dev python3-limits  
amd64-microcode kmod libhwloc16 libm16 python3-louis  
apparmor libbom3 libmath-3-1-29t64 llvm-16-dev python3-networkx  
apt libapparmor1 libinput-bin llvm-16-linker-tools python3-numexpr  
apt-utils libapt-pkg6.0t64 libinput10 llvm-16-runtime python3-numpy  
atftpd libarchive13t64 libjavascriptcoregtk-4.1-0 llvm-16-tools python3-portend  
base-files libasound2-data libjim0.82t64 llvm-17 python3-prompt-toolkit  
bash libasound2t64 libjs-sphinxdoc llvm-17-dev python3-pydatamc  
bind9-dnswitls libass9 libkmod2 llvm-17-linker-tools python3-pyexploitdb  
bind9-host libaudit-common libldb2 llvm-17-runtime python3-pygments  
bind9-libs libaudit1 liblightdm-gobject-1-0 llvm-17-tools python3-pygraphviz
```

```
kali@kali: ~  
File Actions Edit View Help  
Setting up gstreamer1.0-libav:amd64 (1.24.5-1) ...  
Setting up g++-13 (13.2.0-25) ...  
Setting up libwebkit2gtk-4.1-0:amd64 (2.44.2-1+b2) ...  
Setting up system-config-printer-common (1.5.18-3) ...  
Setting up pavucontrol (6.0-1) ...  
Setting up libpocl1t64:amd64 (6.0-1) ...  
Setting up pocl-ocl-icd:amd64 (6.0-1) ...  
Installing new version of config file /etc/OpenCL/vendors/pocl.icd ...  
Setting up system-config-printer (1.5.18-3) ...  
Setting up libheif-plugin-david:amd64 (1.17.6-3+b1) ...  
Setting up libheif-plugin-libde265:amd64 (1.17.6-3+b1) ...  
Setting up libheif1:amd64 (1.17.6-3+b1) ...  
Setting up libheif-plugin-x265:amd64 (1.17.6-3+b1) ...  
Setting up libheif-plugin-aomenc:amd64 (1.17.6-3+b1) ...  
Processing triggers for libc-bin (2.38-13) ...  
Processing triggers for systemd (256-1) ...  
Processing triggers for crackmap-runtime (2.9.6-5.1+b1) ...  
Processing triggers for dbus (1.14.10-4+b1) ...  
Processing triggers for postgresql-common (260) ...  
supported-versions: WARNING! Unknown distribution ID in /etc/os-release: kali  
debian found in ID_LIKE, treating as Debian  
Building PostgreSQL dictionaries from installed myspell/hunspell packages ...  
on us  
Removing obsolete dictionary files:  
Processing triggers for debiannutils (5.19) ...  
Processing triggers for base-files (1:2024.2.1) ...  
Processing triggers for wordlists (2023.2.0) ...  
Processing triggers for fontconfig (2.15.0-1.1) ...  
Processing triggers for kali-menu (2023.4.7) ...  
Processing triggers for desktop-file-utils (0.27-2) ...  
Processing triggers for initramfs-tools (0.142) ...  
update-initramfs: Generating /boot/initrd.img-6.8.11-amd64  
Processing triggers for doc-base (0.11.2) ...  
Processing 39 changed doc-base files, 3 added doc-base files ...  
Processing triggers for ca-certificates-java (20240118) ...  
done.  
Setting up openjdk-23-jre:amd64 (23-20ea-1) ...  
Setting up burpsuite (2024.5.3-0kali1) ...  
[kali@kali]~$
```

## Kali-Linux Defensiva

- Se actualiza la lista de repositorios, ejecutando el comando:

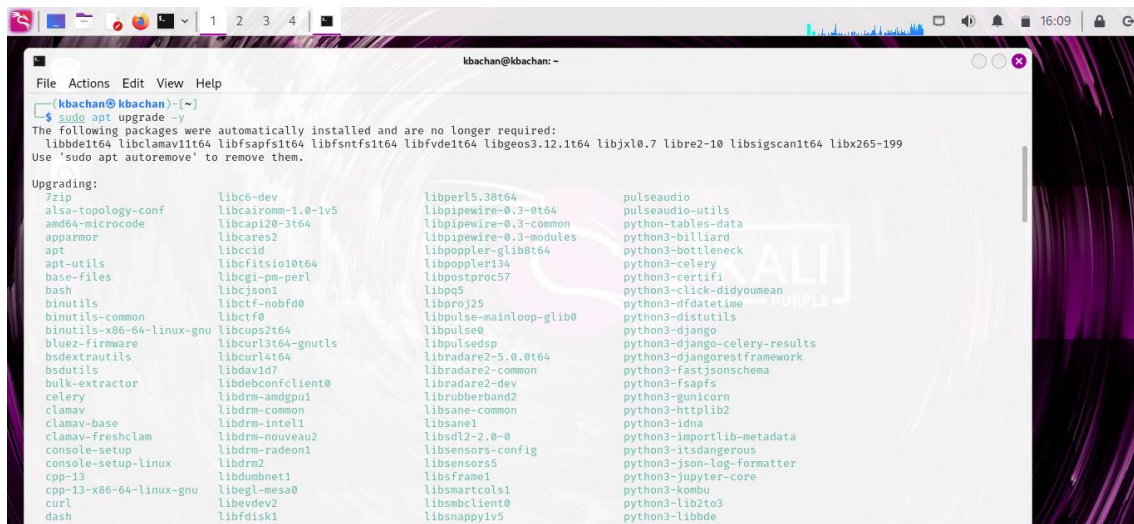
**sudo apt update**



```
kbachan@kbachan:~$ sudo apt update
[sudo] password for kbachan:
Hit:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Get:4 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.4 MB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Packages [113 kB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [27 1 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:8 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8 62 kB]
Fetched 68.7 MB in 30s (2266 kB/s)
419 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

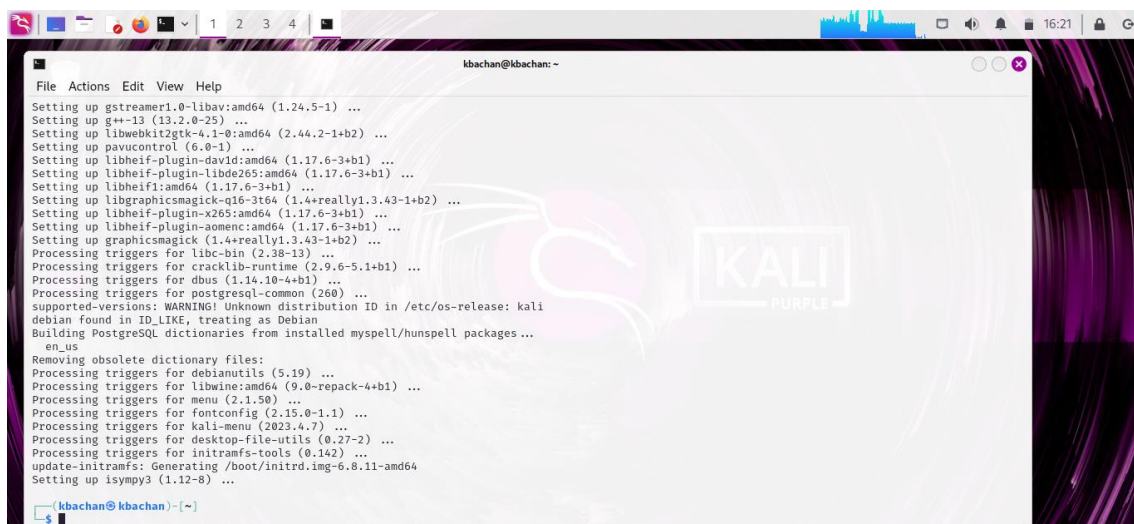
- Se actualiza los paquetes instalados a sus últimas versiones ejecutando el comando:

**sudo apt upgrade -y**



```
kbachan@kbachan:~$ sudo apt upgrade -y
The following packages were automatically installed and are no longer required:
libbde1t64 libclamav1t64 libfsapfs1t64 libfsntfs1t64 libfvd1t64 libgeos3.12.1t64 libjxl0.7 libre2-10 libsigscan1t64 libx265-199
Use 'sudo apt autoremove' to remove them.

Upgrading:
7zip                libb6-dev                libperl5.38t64        pulseaudio
alsa-topology-conf  libcairmm-1.0-1v5        libpipewire-0.3-0t64  pulseaudio-utils
amd64-microcode     libcap120-3t64           libpipewire-0.3-common python-tables-data
apparmor            libcc1d                  libpipewire-0.3-modules python3-billiard
apt                 libcfitsio10t64          libpoppler-glib0t64   python3-bottleneck
apt-utils           libcgispm-perl           libpoppler124         python3-celery
base-files          libcgispm-perl           libpostproc57         python3-certifi
bash                libcgispm1               libproj5              python3-click-didyoumean
binutils            libctf-nobfd             libproj25             python3-datetime
binutils-common     libctf0                  libpulse-mainloop-glib python3-distutils
binutils-x86-64-linux-gnu libcurl3t64-gnutls       libpulse0             python3-django
bluez-firmware      libcurl4t64              librads2-5.0.0t64     python3-django-celery-results
bsdextrautils       libdavid7                librads2-dev          python3-djangorestframework
bsdutils            libdavid7                librads2-common       python3-fastjsonschema
bulk-extractor      libdebconfclient0        librads2-dev          python3-fsafs
celery               libdrm-amdgpu1           librubberband2        python3-gunicorn
clamav              libdrm-common            libsane-common        python3-httplib2
clamav-base         libdrm-intel1            libsane1              python3-idna
clamav-freshclam    libdrm-nouveau2         libsd12-2.0-0         python3-importlib-metadata
console-setup        libdrm-radeon1           libsd12-2.0-0         python3-itsdangerous
console-setup-linux libdrm2                  libsd12-2.0-0         python3-json-log-formatter
cpp-13              libdumbnet1              libseccomp2           python3-jupyter-core
cpp-13-x86-64-linux-gnu curl                      libseccomp2           python3-kombu
dash                libfdisk1                libseccomp2           python3-lib2to3
dash                libfdisk1                libseccomp2           python3-libbde
```



```
kbachan@kbachan:~$ sudo apt upgrade -y
Setting up gstreamer1.0-libav:amd64 (1.24.5-1) ...
Setting up g++-13 (13.2.0-25) ...
Setting up libwebkit2gtk-4.1-0:amd64 (2.44.2-1+b2) ...
Setting up pavucontrol (6.0-1) ...
Setting up libheif-plugin-david:amd64 (1.17.6-3+b1) ...
Setting up libheif-plugin-libde265:amd64 (1.17.6-3+b1) ...
Setting up libheif1:amd64 (1.17.6-3+b1) ...
Setting up libgraphicsmagick-q16-3t64 (1.4+really1.3.43-1+b2) ...
Setting up libheif-plugin-x265:amd64 (1.17.6-3+b1) ...
Setting up libheif-plugin-x265:amd64 (1.17.6-3+b1) ...
Setting up graphicsmagick (1.4+really1.3.43-1+b2) ...
Processing triggers for libc-bin (2.38-13) ...
Processing triggers for cracklib-runtime (2.9.6-5.1+b1) ...
Processing triggers for dbus (1.14.10-4+b1) ...
Processing triggers for postgresql-common (260) ...
supported-versions: WARNING! Unknown distribution ID in /etc/os-release: kali
debian found in ID_LIKE, treating as Debian
Building PostgreSQL dictionaries from installed myspell/hunspell packages...
done
Removing obsolete dictionary files:
Processing triggers for debiannutils (5.19) ...
Processing triggers for libwine:amd64 (9.0-repack-4+b1) ...
Processing triggers for menu (2.1.50) ...
Processing triggers for fontconfig (2.15.0-1.1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for inotify-tools (0.14.2) ...
update-initramfs: Generating /boot/initrd.img-6.8.11-amd64
Setting up isympy3 (1.12-8) ...
```

Ambas máquinas Kali-Linux se actualizaron correctamente, instalando las últimas versiones de paquetes y parches de seguridad.



## Bloqueo de acceso a internet a la Máquina Vulnerable (Metasploitable)

Para llevar a cabo el bloqueo se realizaron las siguientes configuraciones:

1. Se configuró en el OPNsense en la sección Firewall en la parte de Aliases.

Haga clic en el botón “+” para añadir una nueva regla.

Configura la regla de la siguiente manera:

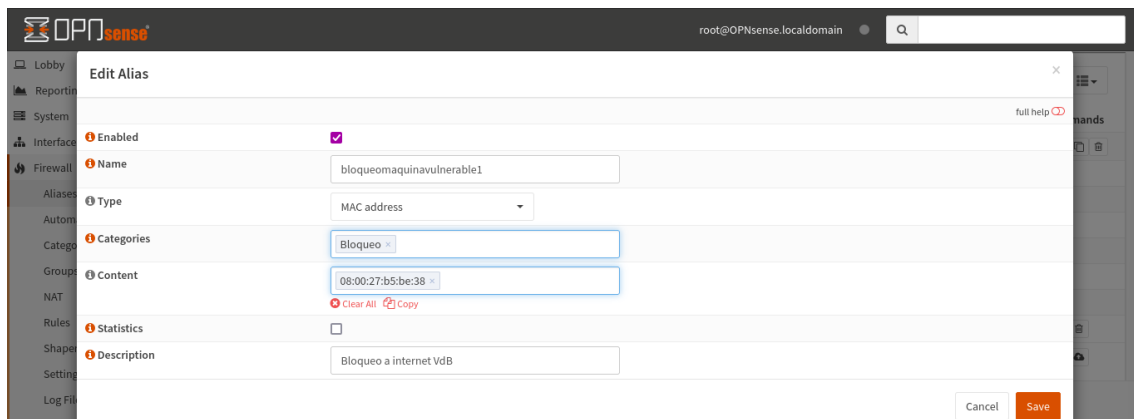
Name: bloqueomaquinavulnerable1

Type: MAC address

Categories: Bloqueo

Content: 08:00:27:b5:be:38 (MAC de la máquina vulnerable)

Description: Bloqueo a internet VdB



2. Se crea las reglas de firewall que restringen el tráfico entrante de la dirección MAC de la máquina vulnerable (Metasploitable).

Firewall > Rules > LAN (o la interfaz correspondiente si no es LAN).

Haga clic en el botón “+” para añadir una nueva regla.

Se procede a Configurar la regla de la siguiente manera:

Action: Reject

Interface: LAN (o la interfaz correspondiente)

Direction: in

TCP/IP version: IPv4

Protocol: Any

Source: bloqueomaquinavulnerable1 (previamente creada en el aliases)

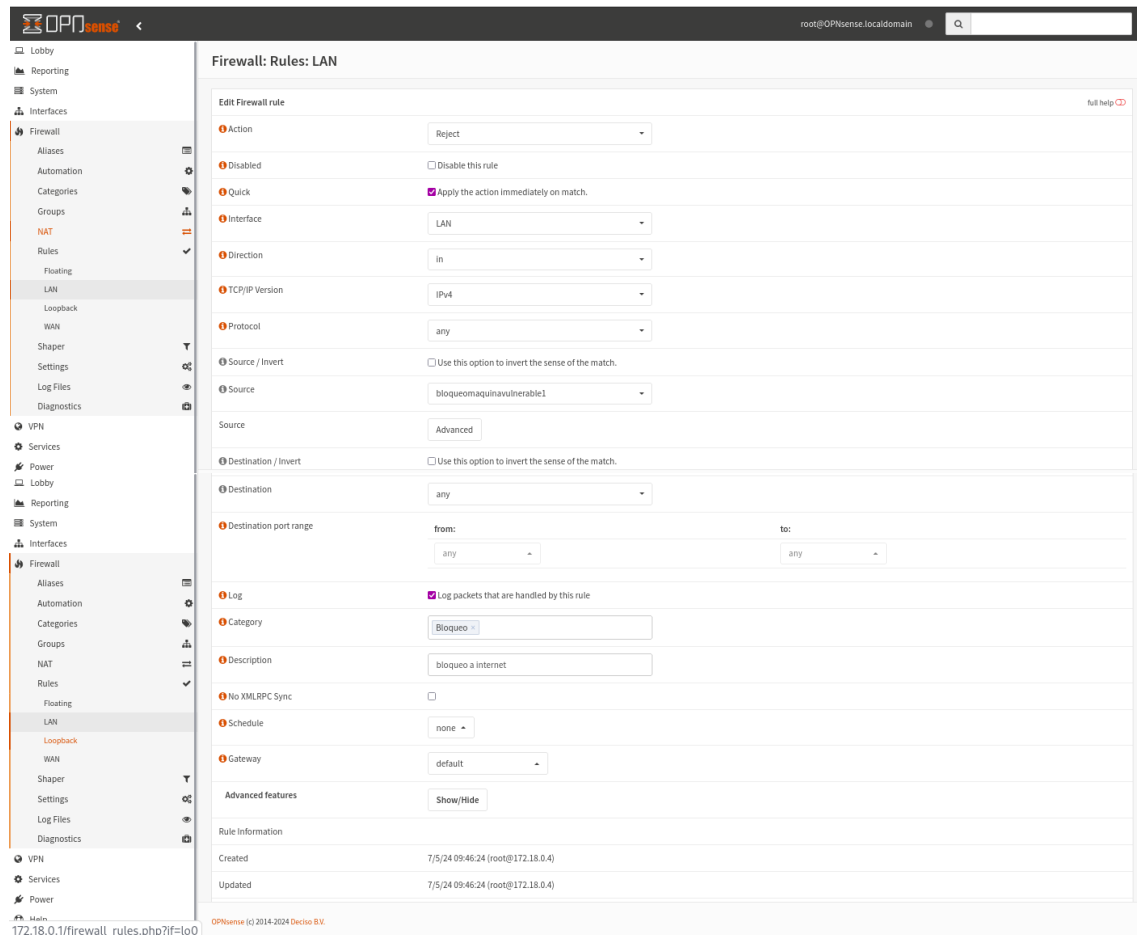
Destination: Any

Category: Bloqueo

Description: Bloqueo a internet

Gateway: default

- Haga clic en Save para guardar la regla.
- Después de guardar, haga clic en Apply Changes para aplicar la nueva configuración del firewall.



Se verificó que la máquina vulnerable (Metasploitable) ya no pueda acceder a internet utilizando herramientas como ping y otros comandos. Obteniendo el resultado esperado.

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ping 1.1.1.1  
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.  
  
--- 1.1.1.1 ping statistics ---  
2 packets transmitted, 0 received, 100% packet loss, time 1002ms  
  
msfadmin@metasploitable:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
  
--- 8.8.8.8 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 5006ms  
  
msfadmin@metasploitable:~$ host google.com  
;; connection timed out; no servers could be reached  
msfadmin@metasploitable:~$ curl -I www.google.com  
curl: (6) Couldn't resolve host 'www.google.com'  
msfadmin@metasploitable:~$ ping 192.185.131.29  
PING 192.185.131.29 (192.185.131.29) 56(84) bytes of data.  
  
--- 192.185.131.29 ping statistics ---  
129 packets transmitted, 0 received, 100% packet loss, time 128148ms  
msfadmin@metasploitable:~$
```

### **Dificultades encontradas**

- La configuración inicial del firewall presentó algunos desafíos debido a la falta de familiaridad con la herramienta OPNsense.
- La actualización de Kali-Linux Ofensiva generó un error que requirió investigación y resolución manual.
- La configuración de la red de Kali-Linux Defensiva al inicio presente problemas con el acceso a internet, pero luego de una minuciosa investigación y modificaciones manuales, se logró establecer la conectividad.

### **Conclusiones**

- Se logró configurar una red aislada de forma exitosa para prácticas de ciberseguridad.
- Se realizaron pruebas de conectividad, actualización y bloqueo de acceso a internet con resultados satisfactorios.
- La experiencia permitió el aprendizaje y fortalecimiento de habilidades en configuración de redes, administración de sistemas y herramientas de ciberseguridad.

### **Detalles adicionales**

- Se documentaron los pasos detallados para la configuración de la red, pruebas y resolución de problemas.
- Se realizaron capturas de pantalla y registros relevantes para respaldar el proceso y los resultados.
- Se identificaron áreas de mejora para futuras prácticas, como la automatización de tareas y la implementación de medidas de seguridad más avanzadas.