



REPORTE DE PRUEBA DE LABORATORIO WESECURELABS

ÍNDICE

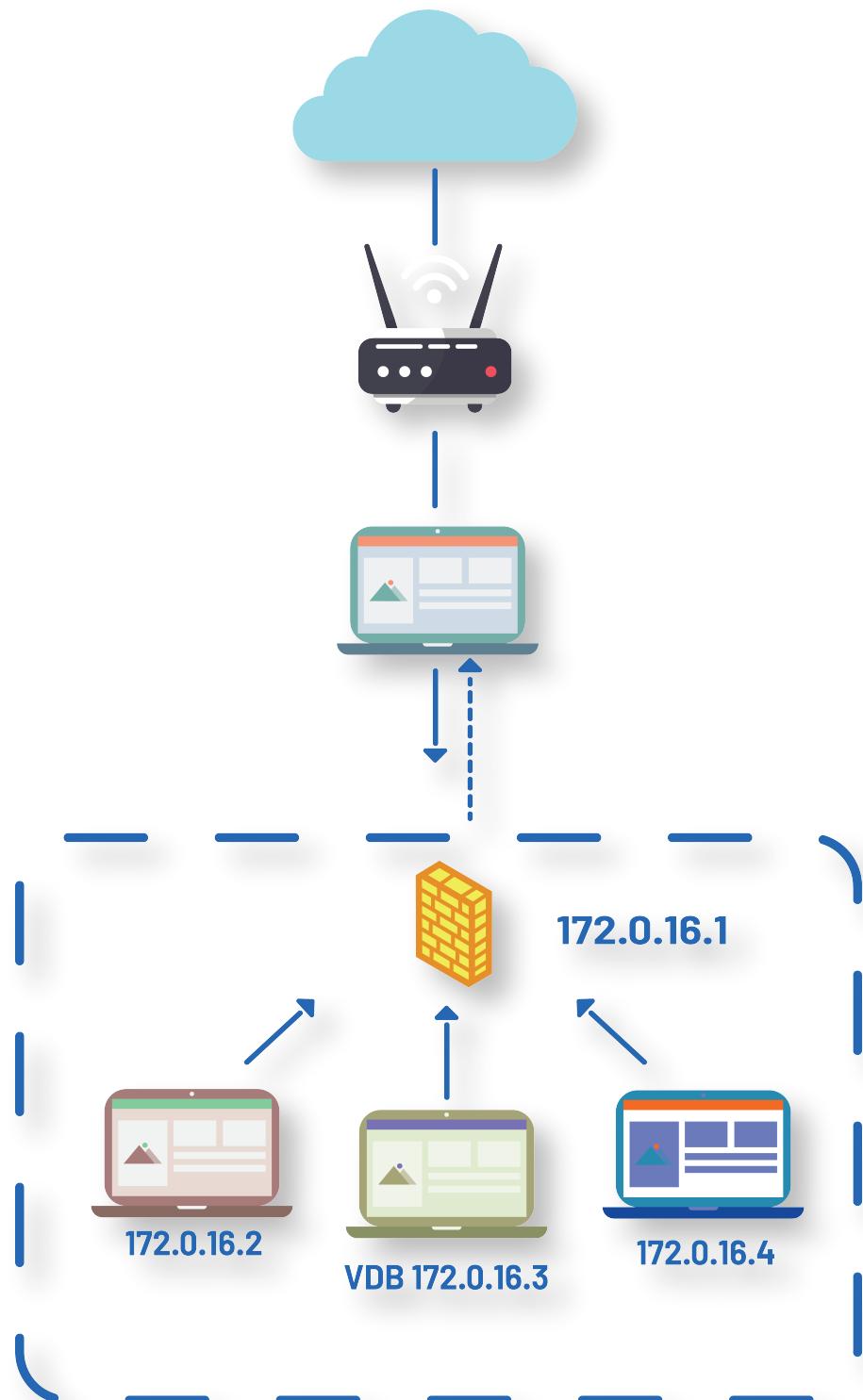
INTRODUCCIÓN.....	3
CONFIGURACIÓN DE LA RED AISLADA.....	4
<i>TOPOLOGÍA.....</i>	4
CONFIGURAMOS LA MAQUINA VIRTUAL DE OPNSENSE.....	5
CONFIGURAMOS PARA LA CONEXIÓN DE NUESTRAS MAQUINAS VIRTUALES.....	8
<i>KALI LINUX (RED TEAM).....</i>	8
<i>ABRIMOS CONSOLA.....</i>	8
KALI LINUX (RED TEAM).....	11
<i>ABRIMOS CONSOLA.....</i>	11
PROCESO DE ACTUALIZACION DE MAQUINAS VIRTUALES RED TEAM Y BLUE TEAM.....	14
CONFIGURACION DEL FIREWALL PARA LAS MAQUINAS VIRTUALES Y LA MAQUINA VULNERABLE.....	16
AHORA PROCEDEREMOS A HACER PING ENTRE NUESTRAS MAQUINAS VIRTUALES.....	21
<i>KALI LINUX (RED TEAM) PING A KALI LINUX (BLUE TEAM).....</i>	21
DIFICULTADES ENCONTRADAS EN EL PROCESO.....	25
<i>CONCLUSIONES RESPECTO A LA CREACIÓN DE LA RED, LA CREACIÓN DE LA MÁQUINA BLUE Y LA MÁQUINA RED.....</i>	25
<i>CUALQUIER OTRO DETALLE TÉCNICO QUE CONSIDEREN RELEVANTE.....</i>	25

INTRODUCCIÓN

EL REPORTE QUE VAN A LEER A CONTINUACIÓN CONSISTE EN TODA LA CONFIGURACIÓN DE UN ENTORNO VIRTUAL PREPARADO PARA PRÁCTICAS LABORALES DE CIBERSEGURIDAD COMO PARA RED TEAM Y BLUE TEAM UTILIZANDO LAS HERRAMIENTAS OPNSENSE, KALI LINUX Y METASPLOITABLE, SE MUESTRA LA CONFIGURACIÓN IP DE LAS MÁQUINAS Y SE HACE PRUEBA DE CONECTIVIDAD Y EL ANÁLISIS DE PAQUETES, BLOQUEO DE ACCESO A INTERNET DE LA MAQUINA VULNERABLE, EL PROCESO DE ACTUALIZACIÓN DE LAS MÁQUINAS KALI LINUX, LAS DIFICULTADES ENCONTRADAS Y LAS CONCLUSIONES OBTENIDAS.

CONFIGURACIÓN DE LA RED AISLADA

TOPOLOGÍA:



CONFIGURAMOS LA MAQUINA VIRTUAL DE OPNSENSE

- 1.LOGUEMOS CON NUESTRAS CREDENCIALES
- 2.ROOT
- 3.OPNSENSE
- 4.SELECCIONAMOS LA OPCIÓN 1 ASSIGN INTERFACES
- 5.CONFIGURE IPV4 ADDRESS LAN INTERFACE VIA DHCP (Y/N): N
- 6.ENTER THE NEW LAN IPV4 ADDRESS
- 7.COLOCAMOS LA IP 172.0.16.1
- 8.SUBNET MASKS ARE ENTERED AS BIT COUNT
- 9.USAMOS LA 24 QUE SERIA 255.255.255.0
- 10.FOR A WAN ENTER THE NEW LAN IPV4 UPSTREAM GATEWAY ADDRESS: LE DAMOS ENTER
- 11.FOR A LAN, PRESS ENTER LE DAMOS ENTER
- 12.CONFIGURE IPV6 ADDRESS LAN INTERFACE VIA WAN TRACKING (Y/N): Y
- 13.DO YOU WANT TO ENABLE THE DHCP SERVER ON LAN (Y/N) Y
- 14.ENTER THE START ADDRESS OF THE IPV4 CLIENT ADDRESS RANGE: 172.0.16.2
- 15.ENTER THE END ADDRESS OF THE IPV4 CLIENT ADDRESS RANGE: 172.0.16.253

```
OPNsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Available interfaces:
1 - LAN (le1 - static, track6)
2 - WAN (le0 - 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:
> 172.0.16.1

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:
> █
```

```
OPNsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

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:
> 172.0.16.1

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:
>

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

Do you want to enable the DHCP server on LAN? [y/N] y

Enter the start address of the IPv4 client address range: 172.0.16.2 █
```

```
OPNsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.0.16.1

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:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] y
Do you want to enable the DHCP server on LAN? [y/N] y
Enter the start address of the IPv4 client address range: 172.0.16.2
Enter the end address of the IPv4 client address range: 172.0.16.253
```

```
OPNsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Starting DHCPv4 service...done.
Starting DHCPv6 service...done.
Starting router advertisement service...done.
Starting web GUI...done.

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

http://172.0.16.1

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

LAN (le1)      -> v4: 172.0.16.1/24
WAN (le0)      -> v4/DHCP4: 192.168.1.106/24
                  v6/DHCP6: 2803:c000:b:41e5::2/128

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

Enter an option: 
```

UNA VEZ FINALIZADA LA CONFIGURACIÓN DE NUESTRO OPNSENSE, YA SABREMOS
QUE LA PUERTA DE ENLACE A NUESTRO FIREWALL ES LA 172.0.16.1

CONFIGURACIÓN PARA LA CONEXIÓN DE NUESTRAS MÁQUINAS VIRTUALES (RED TEAM)

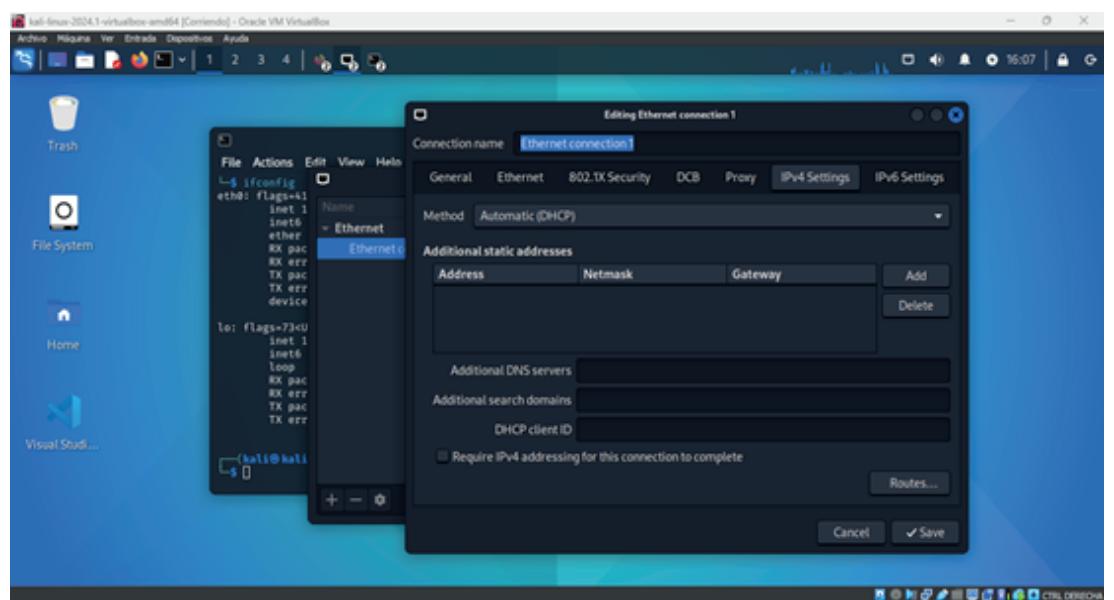
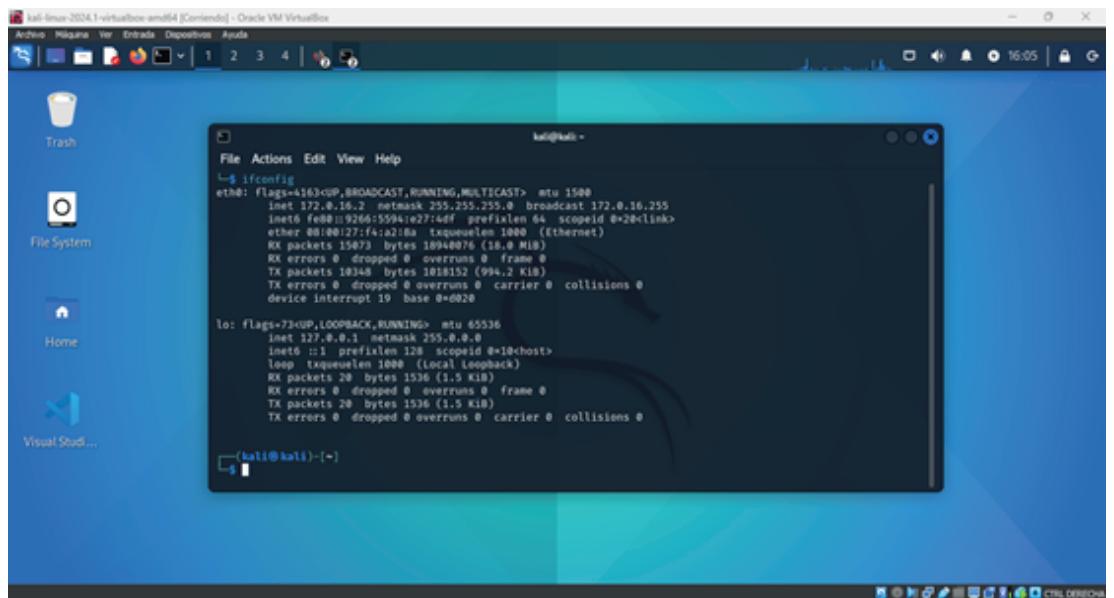
KALI LINUX (RED TEAM)

- 1.ENTRAMOS A NUESTRA MÁQUINA VIRTUAL
- 2.ABRIMOS UNA CONSOLA
- 3.Y COLOCAMOS EL COMANDO IFCONFIG
- 4.VERIFICAMOS QUE NUESTRA IP ESTE BIEN CONFIGURADA

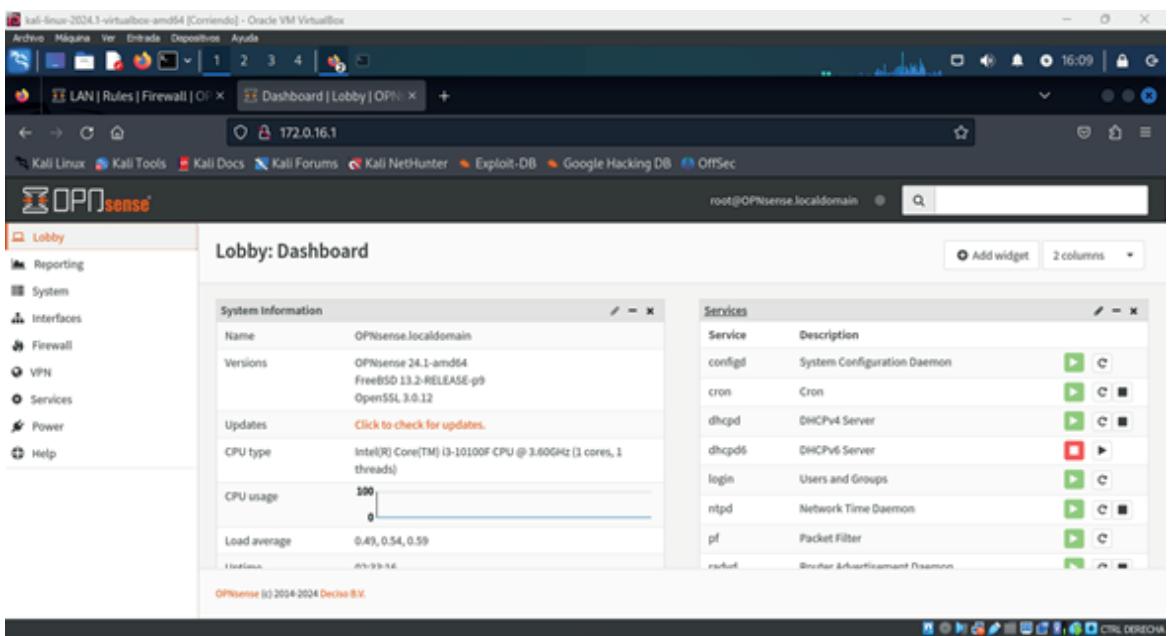
EN CASO DE QUE NUESTRA MAQUINA VIRTUAL NO ESTE CONFIGURADA LA IP DESEADA USAMOS LOS SIGUIENTES COMANDOS

ABRIMOS CONSOLA

- 1.ROOT > CLAVE DEL SISTEMA
- 2.IFCONFIG (PARA VER QUE IP TENEMOS)
- 3.IFCONFIG ETH0 172.0.16.2 NETMASK 255.255.255.0
- 4.APAGAMOS Y ENCEDEMOS EL ADAPTADOR Y YA DEBERÍAMOS TENER CONEXIÓN CON NUESTRO FIREWALL



ABRIMOS NUESTRO NAVEGADOR DESDE NUESTRA
MAQUINA VIRTUAL, Y COLOCAREMOS LA IP DE NUESTRO FIREWALL 172.0.16.1



ABRIMOS NUESTRO NAVEGADOR DESDE NUESTRA
MAQUINA VIRTUAL, Y COLOCAREMOS LA IP DE NUESTRO FIREWALL 172.0.16.1

KALI LINUX (RED TEAM)

5.ENTRAMOS A NUESTRA MÁQUINA VIRTUAL

6.ABRIMOS UNA CONSOLA

7.Y COLOCAMOS EL COMANDO IFCONFIG

8.VERIFICAMOS QUE NUESTRA IP ESTE BIEN CONFIGURADA

EN CASO DE QUE NUESTRA MAQUINA VIRTUAL NO ESTE CONFIGURADA LA IP DESEADA USAMOS LOS SIGUIENTES COMANDOS

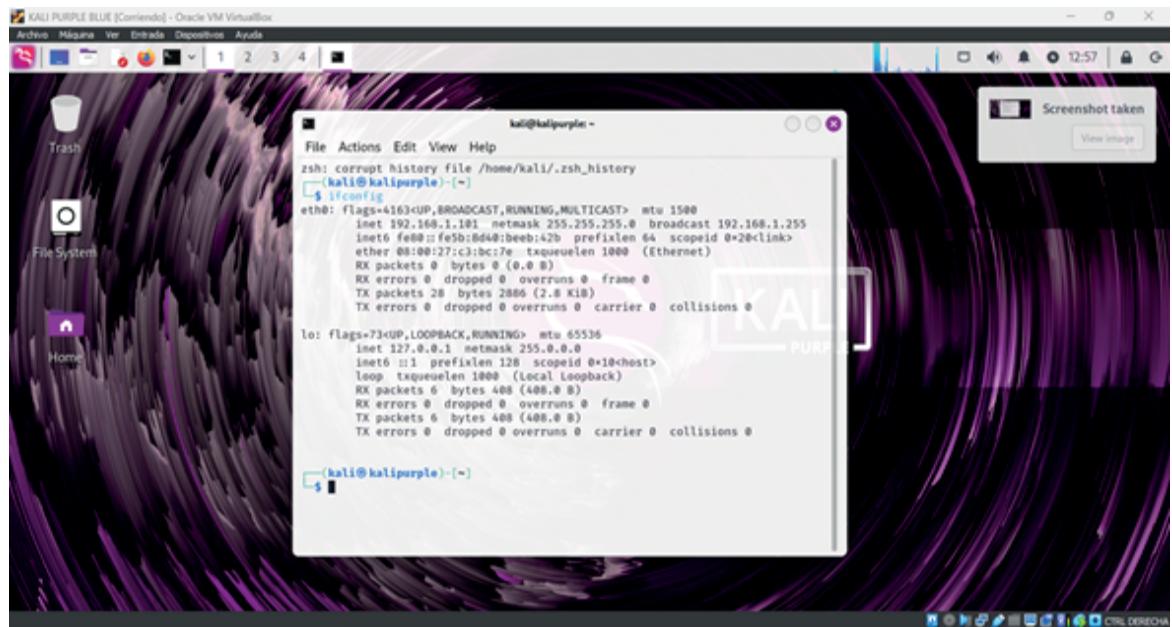
ABRIMOS CONSOLA

5.ROOT > CLAVE DEL SISTEMA

6.IFCONFIG (PARA VER QUE IP TENEMOS)

7.IFCONFIG ETH0 172.0.16.4 NETMASK 255.255.255.0

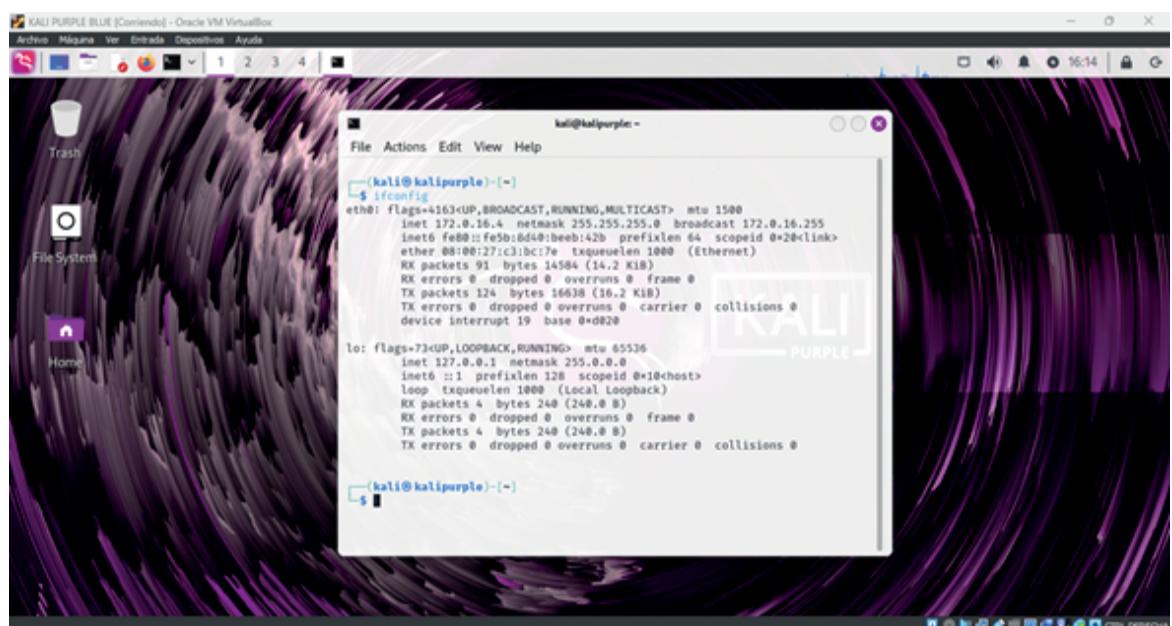
APAGAMOS Y ENCEDEMOS EL ADAPTADOR Y YA DEBERÍAMOS TENER CONEXIÓN CON NUESTRO FIREWALL



```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kalipurple:~) $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
                ether fe:00:fe:00:0d:44 brd 192.168.1.255
                txqueuelen 1000  (Ethernet)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 29 bytes 2886 (2.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop txqueuelen 1000  (Local Loopback)
                RX packets 6 bytes 408 (408.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 6 bytes 408 (408.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kalipurple:~) $
```

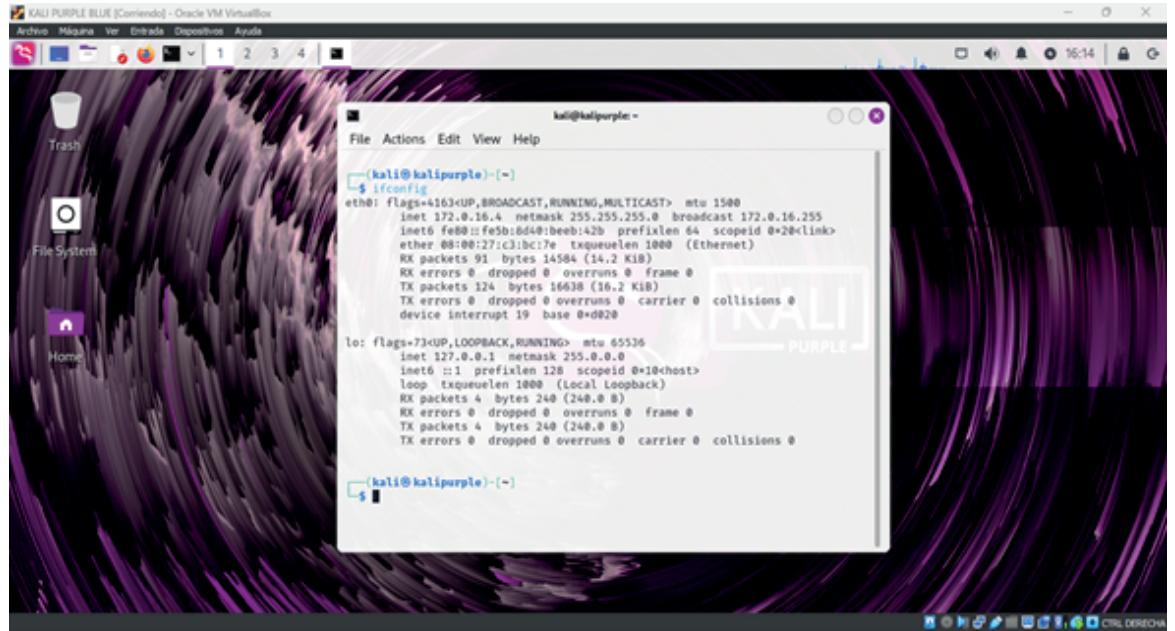


```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kalipurple:~) $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.0.16.4 netmask 255.255.255.0 broadcast 172.0.16.255
                ether 00:00:27:c3:bc:7e brd 172.0.16.255
                txqueuelen 1000  (Ethernet)
                RX packets 91 bytes 14584 (14.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 124 bytes 16638 (16.2 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                device interrupt 19 base 0x0d020

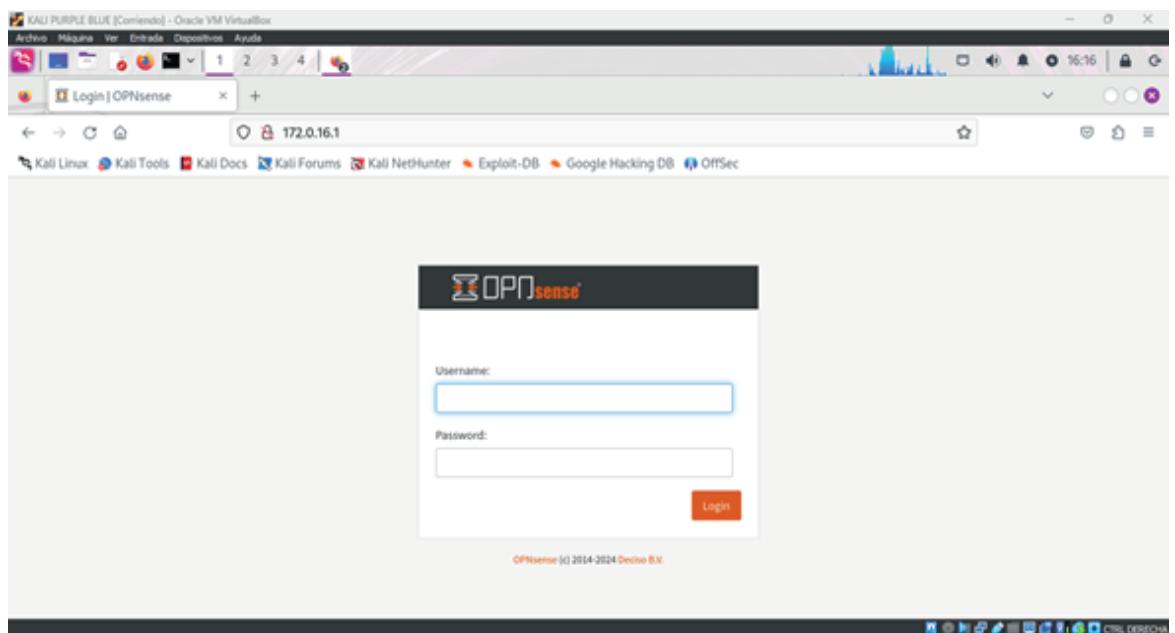
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop txqueuelen 1000  (Local Loopback)
                RX packets 4 bytes 240 (240.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4 bytes 240 (240.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kalipurple:~) $
```

NOS DIRIGIMOS A LA ESQUINA SUPERIOR DERECHA NETWORT CONECTION
EDITAMOS LAS CONEXIONES
VERIFICAMOS QUE NUESTRA CONEXIÓN DHCP SEA AUTOMÁTICA



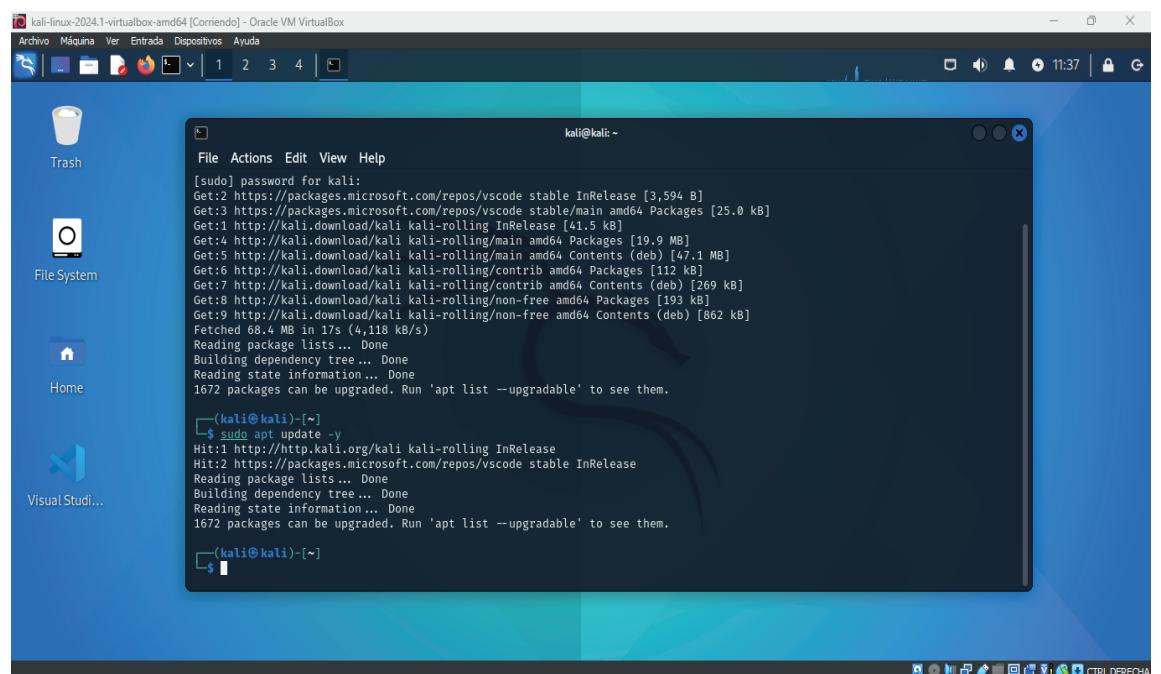
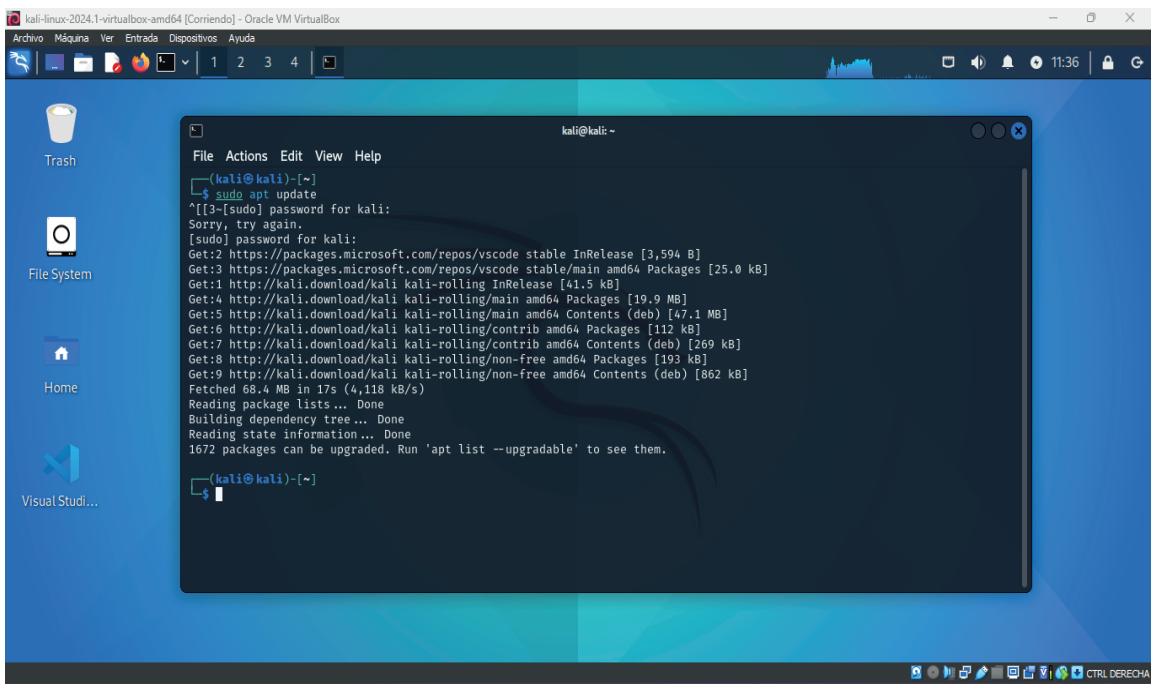
ABRIMOS NUESTRO NAVEGADOR Y TENDRÍAMOS QUE TENER CONEXIÓN CON NUESTRO FIREWALL

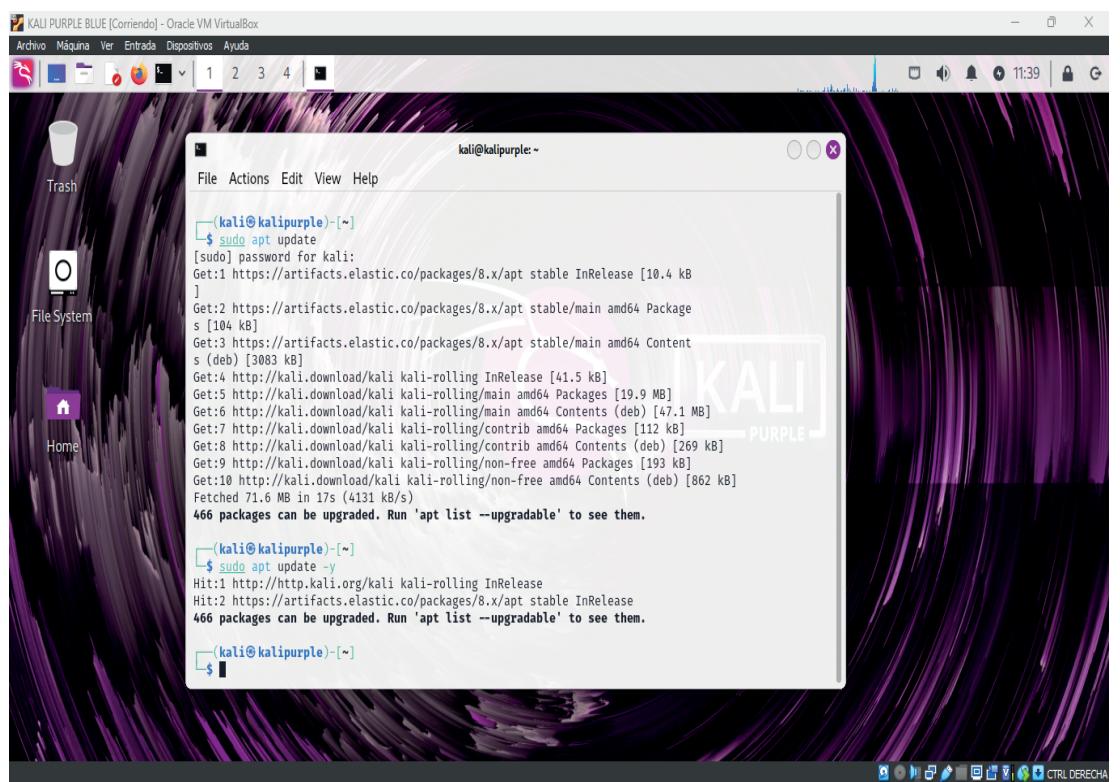
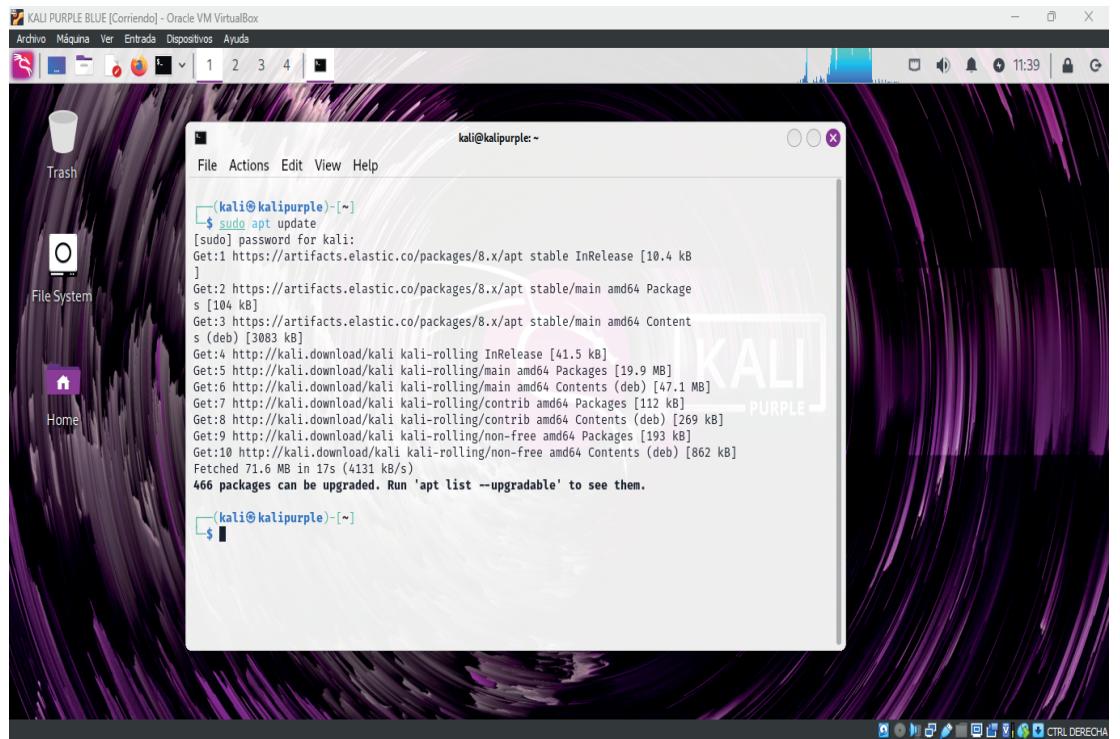


PROCESO DE ACTUALIZACION DE MAQUINAS VIRTUALES RED TEAM Y BLUE TEAM

USAMOS LOS SIGUIENTES COMANDOS

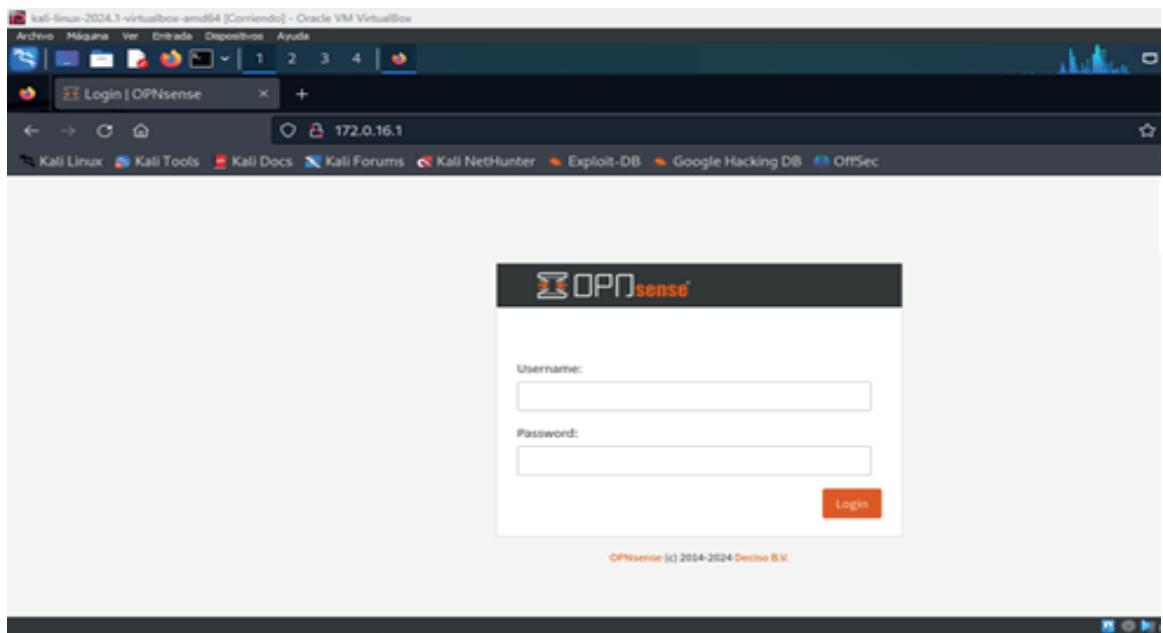
1. SUDO APT UPDATE
2. SUDO APT UPDATE -Y
3. ACTUALIZAS CON ÉXITO Y SIN PROBLEMAS



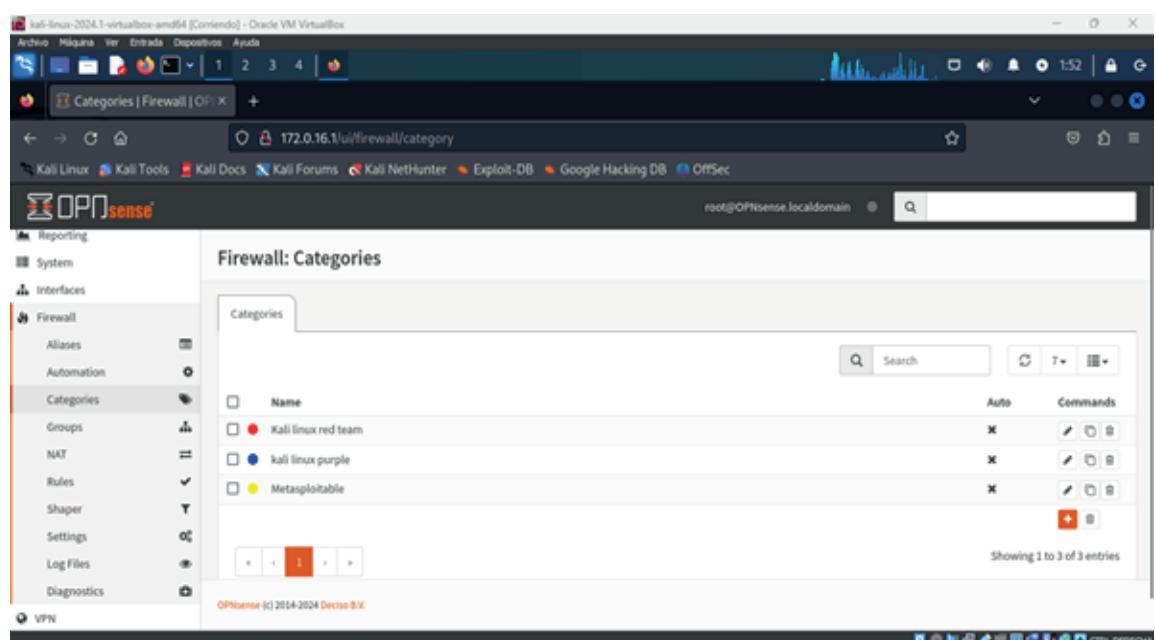


CONFIGURACION DEL FIREWALL PARA LAS MAQUINAS VIRTUALES Y LA MAQUINA VULNERABLE

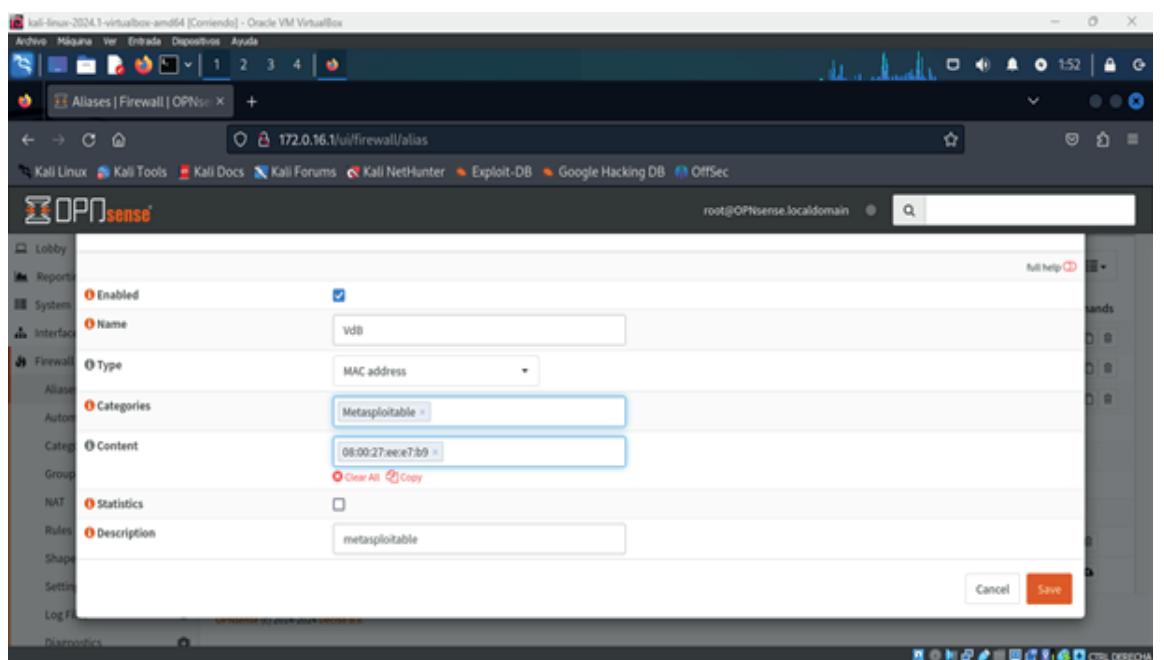
PROCEDEMOS A ENTRAR AL FIREWALL OPNSENSE DESDE CUALQUIER MÁQUINA VIRTUAL 172.0.16.1



UNA VEZ QUE ENTRAMOS AL FIREWALL NOS DIRIGIMOS FIREWALL > CATEGORÍAS



1. UNA VEZ QUE CREAMOS NUESTRAS CATEGORÍAS
2. NOS VAMOS A LA PESTAÑA ALIAS
3. CREAMOS EL ALIAS PARA NUESTRA MAQUINA VULNERABLE LA CUAL NO VA A TENER INTERNET.



UNA VEZ CONFIGURADO NUESTRO ALIAS NOS DIRIGIMOS
FIREWALL > REGLAS > LAN

ACA TENEMOS QUE BORRAR LAS REGLAS QUE ESTÁN PREDEFINIDAS Y CREAR NUESTRA REGLA

SI QUEREMOS QUE NUESTRA MAQUINA VULNERABLE NO TENGА CONEXIÓN TENEMOS
QUE COLOCARLA COMO PRIMERA REGLA

Firewall: Rules: LAN

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action
	IPv4 *	VdB	*	*	*	*	*	Automatically generated rules	
	IPv4 *	*	*	*	*	*	*		
	IPv6 *	*	*	*	*	*	*		
▶	pass	◀	block	▶	reject	◀	log	→ in	
▶	pass (disabled)	◀	block (disabled)	▶	reject (disabled)	◀	log (disabled)	← out	
📅	Active/Inactive Schedule (click to view/edit)								
🔗	Alias (click to view/edit)								

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the order of the rules.

Category

Description

No XMLRPC Sync

Schedule

Gateway

Advanced features

Rule Information

Created	7/5/24 19:19:01 (root@172.0.16.2)
---------	-----------------------------------

Firewall: Rules: LAN

Edit Firewall rule

i Action

Reject

i Disabled

Disable this rule

i Quick

Apply the action immediately on match.

i Interface

LAN

i Direction

in

i TCP/IP Version

IPv4

i TCP/IP Version

IPv4

i Protocol

any

i Source / Invert

Use this option to invert the sense of the match.

i Source

VdB

Source

Advanced

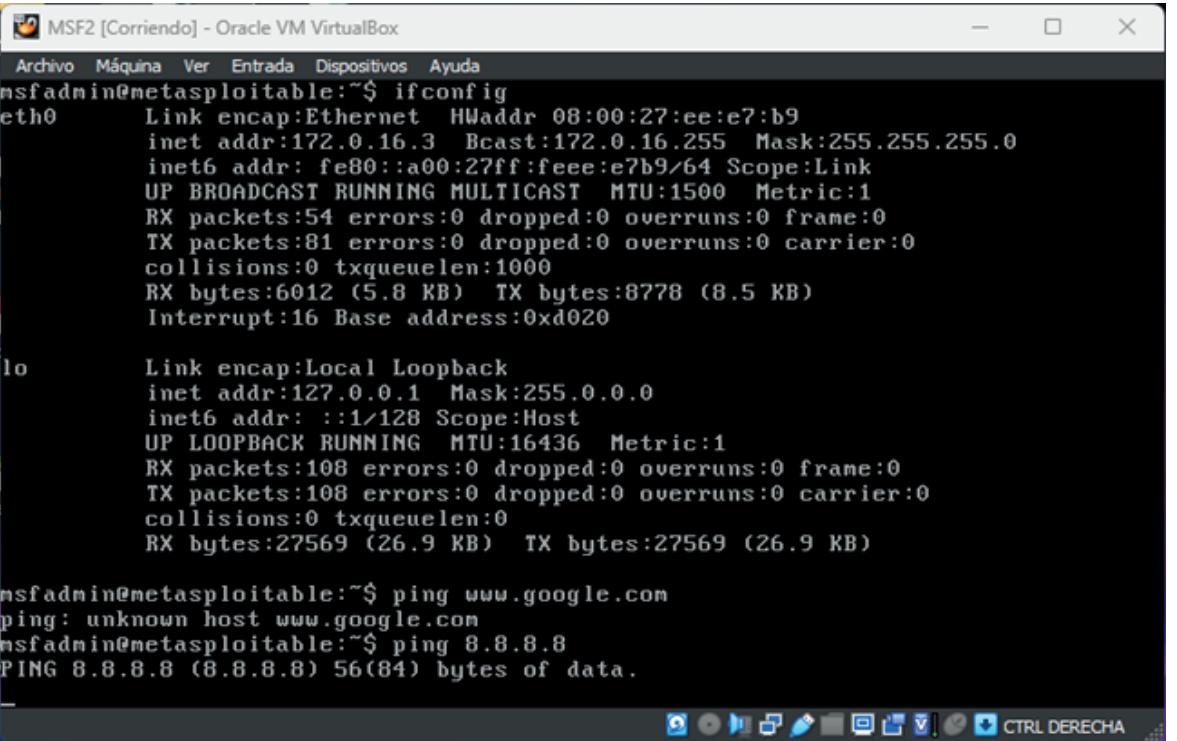
i Destination / Invert

Use this option to invert the sense of the match.

i Destination

any

UNA VEZ CREADA NUESTRA REGLA EN NUESTRO FIREWALL PROCEDEMOS A PROBAR EN LA MAQUINA VULNERABLE SI SE ESTABLECIÓ LOS PARÁMETROS.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:ee:e7:b9
          inet addr:172.0.16.3  Bcast:172.0.16.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feee:e7b9/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:54 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:6012 (5.8 KB)  TX bytes:8778 (8.5 KB)
                  Interrupt:16 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING  MTU:16436  Metric:1
                  RX packets:108 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:27569 (26.9 KB)  TX bytes:27569 (26.9 KB)

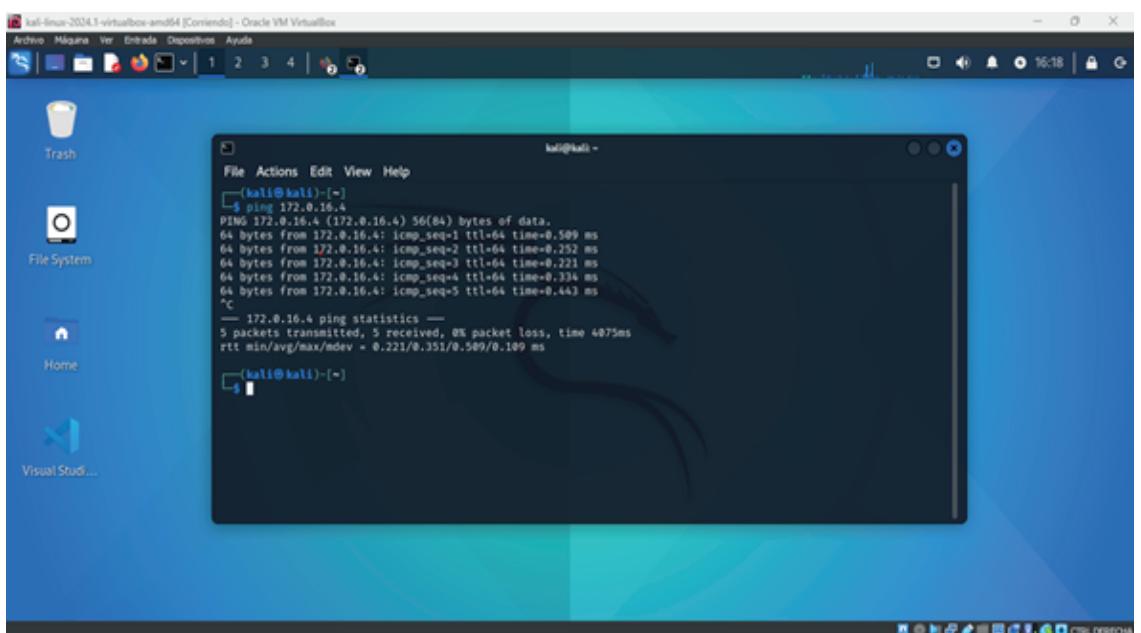
msfadmin@metasploitable:~$ ping www.google.com
ping: unknown host www.google.com
msfadmin@metasploitable:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

COMO PODEMOS VER NO PODEMOS HACER PING A UNA URL NI A UN DNS, NUESTRA REGLA ESTA FUNCIONANDO.

AHORA PROCEDEREMOS A HACER PING ENTRE NUESTRAS MAQUINAS VIRTUALES

KALI LINUX (RED TEAM) PING A KALI LINUX (BLUE TEAM)

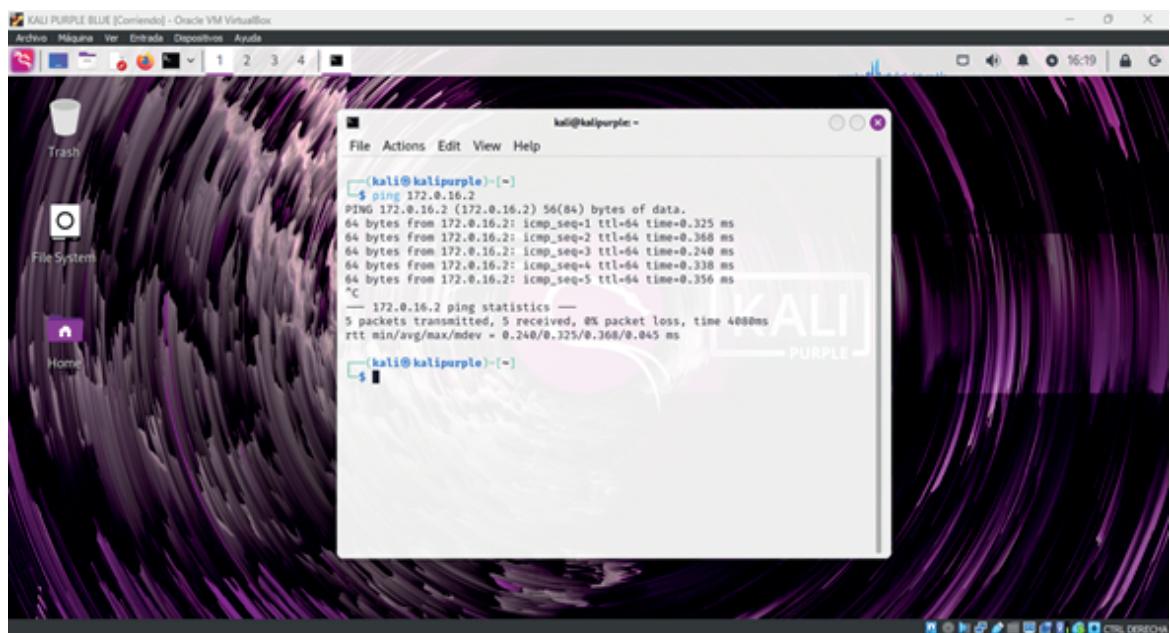
PING A 172.0.16.4



¡TENEMOS CONEXION EXITOSA A NUESTRA MAQUINA!

AHORA DESDE NUESTRA MÁQUINA VIRTUAL KALI LINUX PURPLE (BLUE TEAM) HAREMOS PING A NUESTRA MAQUINA KALI LINUX (RED TEAM)

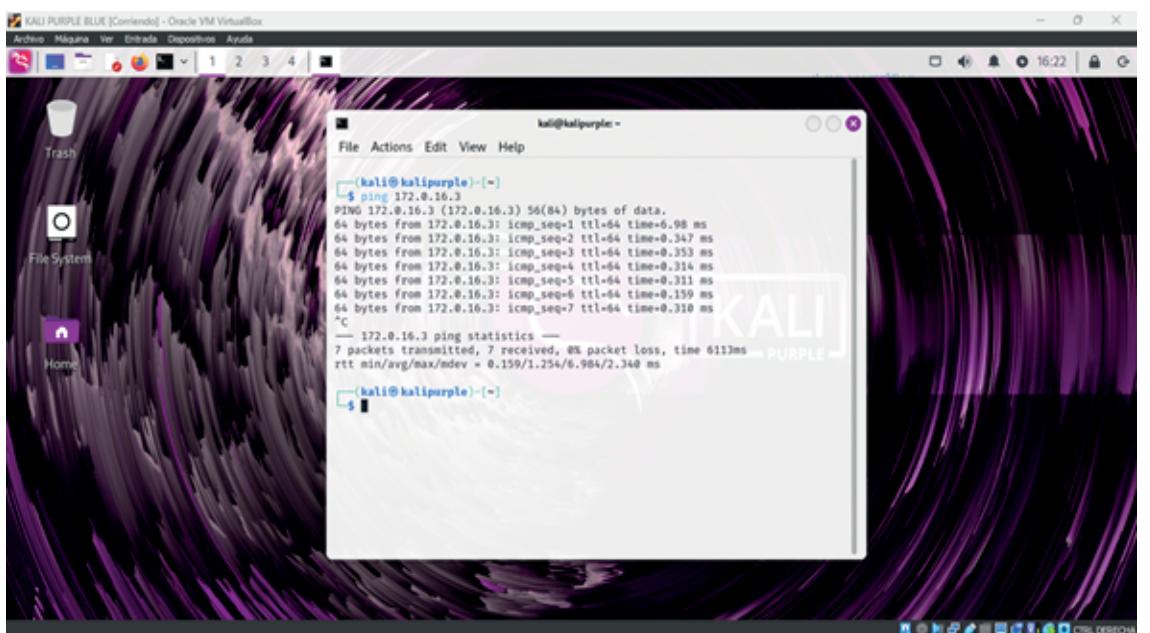
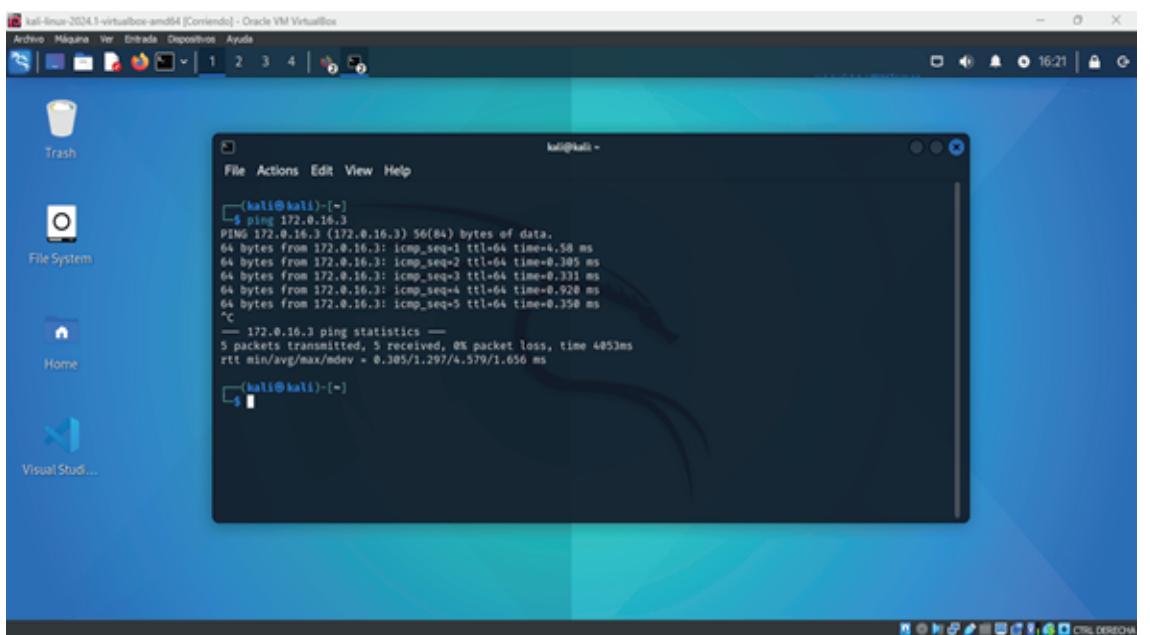
PING 172.0.16.2



The screenshot shows a terminal window titled "kali@kalipurple: ~" running on a Kali Linux Purple desktop environment. The terminal displays the following command and its output:

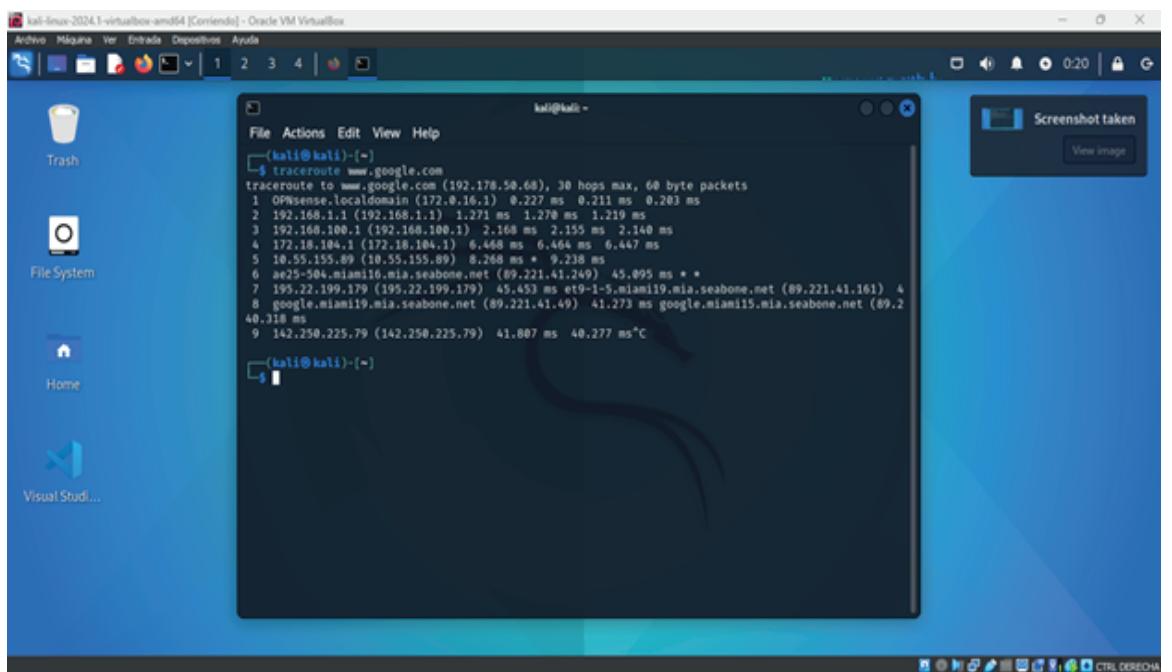
```
(kali㉿kalipurple) ~]$ ping 172.0.16.2
PING 172.0.16.2 (172.0.16.2) 56(84) bytes of data.
64 bytes from 172.0.16.2: icmp_seq=1 ttl=64 time=0.325 ms
64 bytes from 172.0.16.2: icmp_seq=2 ttl=64 time=0.368 ms
64 bytes from 172.0.16.2: icmp_seq=3 ttl=64 time=0.240 ms
64 bytes from 172.0.16.2: icmp_seq=4 ttl=64 time=0.338 ms
64 bytes from 172.0.16.2: icmp_seq=5 ttl=64 time=0.356 ms
^C
--- 172.0.16.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.248/0.325/0.368/0.045 ms
```

TENEMOS CONEXIÓN AHORA HAREMOS PING A NUESTRA MAQUINA VBD 172.0.16.3



REALIZAREMOS UN TRACEROUTE DESDE NUESTRA MAQUINA VIRTUAL KALI LINUX (RED TEAM)

CONSOLA > TRACEROUTE WWW.GOOGLE.COM



A screenshot of a Kali Linux desktop environment. In the center, a terminal window is open with the command `traceroute www.google.com` running. The output shows the path from the Kali host to Google's servers, with 9 hops listed. The desktop background is blue, and the taskbar at the bottom shows various icons.

```
(kali㉿kali)-[~]
$ traceroute www.google.com
traceroute to www.google.com (192.178.50.68), 30 hops max, 60 byte packets
 1 OPNsense.localdomain (172.0.16.1) 0.227 ms 0.211 ms 0.203 ms
  2 192.168.1.1 (192.168.1.1) 1.271 ms 1.278 ms 1.219 ms
  3 192.168.100.1 (192.168.100.1) 2.168 ms 2.155 ms 2.140 ms
  4 172.18.104.1 (172.18.104.1) 6.468 ms 6.464 ms 6.447 ms
  5 10.55.155.89 (10.55.155.89) 8.268 ms * 9.238 ms
  6 ae25-504.miami10.mia.seabone.net (89.221.41.249) 45.095 ms *
  7 195.22.199.179 (195.22.199.179) 45.453 ms et9-1-5.miami19.mia.seabone.net (89.221.41.161) 4
  8 google.miami19.mia.seabone.net (89.221.41.49) 41.273 ms google.miami15.mia.seabone.net (89.2
40.318 ms
  9 142.250.225.79 (142.250.225.79) 41.807 ms 40.277 ms *
```

DIFICULTADES ENCONTRADAS EN EL PROCESO.

UNA DE LAS DIFICULTADES QUE TUVE EN EL PROCESO DE CREACIÓN DE ENTORNO VIRTUAL FUE QUE MI COMPUTADORA EL PUERTO DE RED SE DAÑÓ Y USO UN ADAPTADOR RED A USB.

TUVE CIERTA DIFICULTAD DE ENCONTRAR EL ADAPTADOR PARA QUE ASÍ SE CONECTARAN LAS 4 MÁQUINAS ENTRE SI.

CONCLUSIONES RESPECTO A LA CREACIÓN DE LA RED, LA CREACIÓN DE LA MÁQUINA BLUE Y LA MÁQUINA RED.

SE DOCUMENTÓ LOS PASOS DETALLADOS PARA LA CONFIGURACIÓN DE LA RED, CONFIGURACIÓN DE MÁQUINAS VIRTUALES, CON CONOCIMIENTOS MÍNIMOS EN LINUX SE HACE MÁS RÁPIDO LA CONFIGURACIÓN DE LOS SISTEMAS EN EL CUAL TRABAJAMOS..

CUALQUIER OTRO DETALLE TÉCNICO QUE CONSIDEREN RELEVANTE.

UN DETALLE QUE TUVE QUE SE LO COMENTÉ A MI COMPAÑERO DE ESTUDIO RAÚL, FUE QUE A LA HORA DE BUSCAR LOS ADAPTADORES PARA EL ENTORNO DE RED ME DI CUENTA QUE CUANDO INGRESABA A LA MÁQUINA VIRTUAL (RED TEAM) Y ESTABA EN PROCESOS DE CONFIGURACIÓN DEL FIREWALL MI ROUTER MERCUSYS TENÍA PROBLEMAS DE CONEXIÓN.