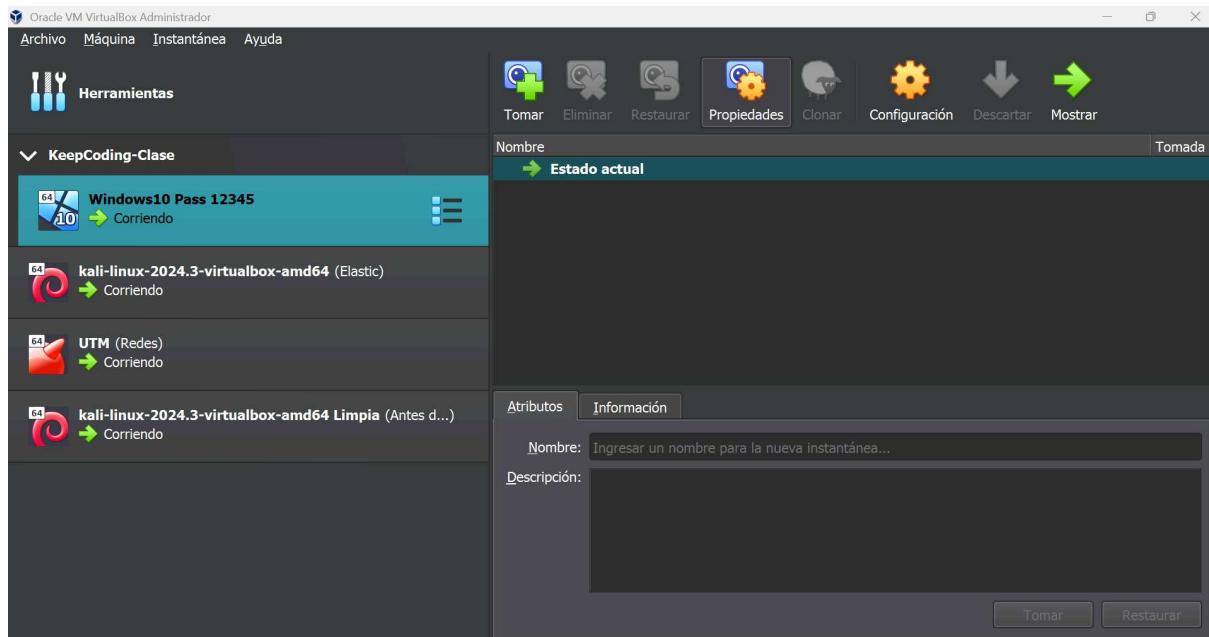


MEMORIA PRÁCTICA

BLUE TEAM 2025

Rafael Figueroa
Versión 1.0

Se ha procedido a instalar las siguientes máquinas virtuales, para cumplir con los requisitos de estructura de red solicitada



Arrancamos la máquina virtual UTM y una máquina Kali en la red LAN generada por el mismo UTM para proceder a configurar los parámetros de Pfsense desde el navegador web, ya que está es la red que se tiene que usar en la primera configuración

Añadimos las otras 2 redes, DMZ y DMZ2 a las que más adelante se conectarán las 2 máquinas Kali

En las siguientes capturas se observa la configuración de las reglas del firewall, con ellas se ha configurado la red según los requisitos solicitados, se detalla cada paso y su función.

1- Red WAN con conexión a DMZ, para poder conectar por SSH con ella, habilitándose también el puerto 222 para dicha conexión

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0/11 KiB	IPv4 *	WAN subnets	*	DMZ subnets	*	*	none		Trafico WAN a DMZ	
<input type="checkbox"/> ✓ 0/0 B	IPv4 TCP	*	*	192.168.100.99	80 (HTTP)	*	none		NAT Servidor Apache	
<input type="checkbox"/> ✓ 0/460 B	IPv4 TCP	*	*	192.168.200.99	222	*	none		NAT Honeypot	

2- Red LAN con conexión a internet y aislada totalmente de DMZ y DMZ2

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/580 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✗ 0/240 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		Bloqueo DMZ	
✗ 0/180 B	IPv4 *	LAN subnets	*	DMZ2 subnets	*	*	none		Bloqueo DMZ2	
✓ 32/74.23 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

3- Red DMZ con conexión a internet, aislada de la red LAN y DMZ2 y con acceso a WAN para conexiones SSH.

The screenshot shows the pfSense Firewall Rules configuration page. The 'DMZ' tab is selected. The table lists the following rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloqueo LAN	
0/3 KIB	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloqueo DMZ2	
0/0 B	IPv4 *	DMZ subnets	*	WAN subnets	*	*	none		Permitir tráfico WAN	
0/0 B	IPv4 ICMP echoes	*	*	*	*	*	none			
6/1.69 MIB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla tráfico DNS	
15/26.34 MIB	IPv4 TCP	*	*	*	Web	*	none		Regla tráfico Web	

Buttons at the bottom include: Add, Add, Delete, Toggle, Copy, Save, and Separator.

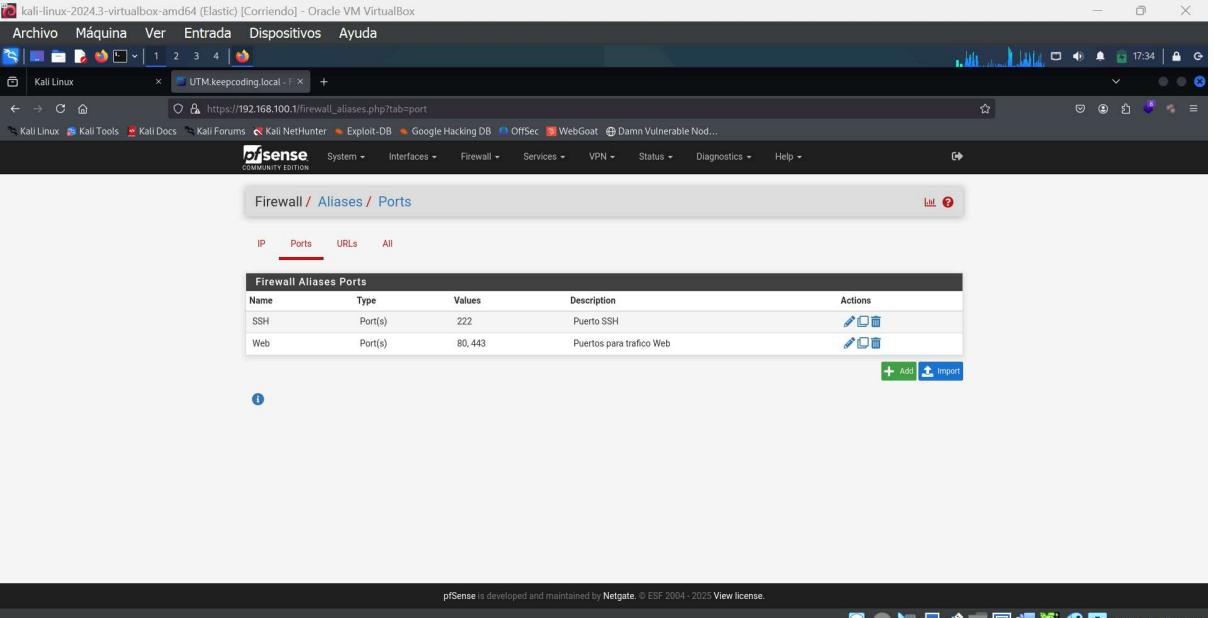
4- Red DMZ2 con conexión a internet, aislada de la red LAN y DMZ y con acceso a WAN para conexiones SSH.

The screenshot shows the pfSense Firewall Rules configuration page. The 'DMZ2' tab is selected. The table lists the following rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/3 KIB	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Bloqueo DMZ	
0/4 KIB	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Bloqueo LAN	
0/2 KIB	IPv4 ICMP echoes	*	*	*	*	*	none			
0/1.73 MIB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla tráfico DNS	
12/36.26 MIB	IPv4 TCP	*	*	*	Web	*	none		Regla tráfico Web	

Buttons at the bottom include: Add, Add, Delete, Toggle, Copy, Save, and Separator.

5- Se procede a abrir el tráfico de los puertos 80 y 443 para tráfico web y 222 para SSH

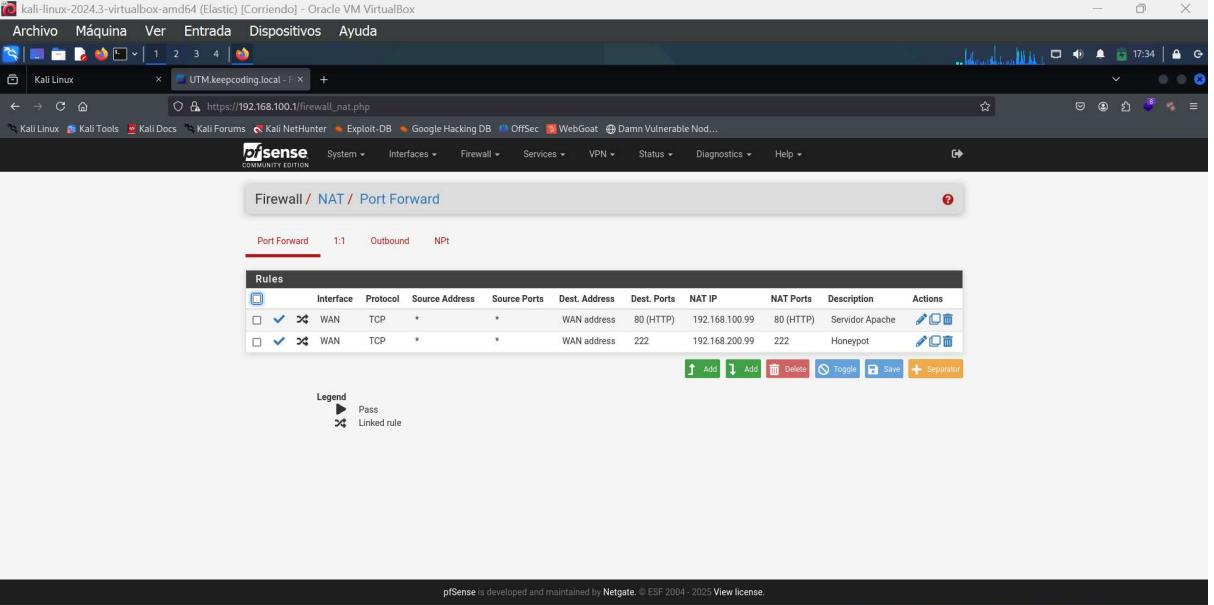


The screenshot shows the pfSense firewall configuration interface. The URL is https://192.168.100.1/firewall_aliases.php?tab=port. The page title is Firewall / Aliases / Ports. There are tabs for IP, Ports (selected), URLs, and All. A table titled 'Firewall Aliases Ports' lists two entries:

Name	Type	Values	Description	Actions
SSH	Port(s)	222	Puerto SSH	
Web	Port(s)	80,443	Puertos para trafico Web	

Buttons at the bottom include '+ Add' and 'Import'.

6- Se hace un portforwarding a las IP fija que se van a asignar a la red DMZ con el objetivo de que el honeypot que se instalará más sea accesible desde la red WAN



The screenshot shows the pfSense firewall configuration interface. The URL is https://192.168.100.1/firewall_nat.php. The page title is Firewall / NAT / Port Forward. There are tabs for Port Forward (selected), 1:1, Outbound, and NPt. A table titled 'Rules' lists two port forwarding rules:

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.100.99	80 (HTTP)	Servidor Apache	
WAN	TCP	*	*	WAN address	222	192.168.200.99	222	Honeypot	

Buttons at the bottom include '+ Add', 'Delete', 'Toggle', 'Save', and '+ separator'. A legend at the bottom left defines symbols: a right-pointing arrow for 'Pass' and a crossed-out right-pointing arrow for 'Linked rule'.

7- En las siguientes imágenes se puede ver como se ha asignado una IP fija dentro del rango de IPs correspondiente a la red DMZ, así como el pool de IPs de las redes.

The screenshot shows the UTM (Universal Test and Measurement) interface on a Kali Linux VM. The main window displays the 'DHCP' configuration page. At the top, there are several tabs: 'Statistics graphs', 'Ping check', 'Dynamic DNS', 'MAC Address Control', 'NTP', 'TFTP', 'LDAP', 'Network Booting', and 'Custom DHCP Options'. Below these tabs is a 'Save' button. The main content area is titled 'DHCP Static Mappings' and contains a table with one entry:

Static ARP	MAC address	IP address	Hostname	Description
✓	08:00:27:d2:c6:66	192.168.200.99	kali	Honeypot

At the bottom of the interface are various icons for managing the configuration.

The screenshot shows the pfSense interface on a Windows 10 host. The main window is titled 'Status / DHCP Leases'. A yellow banner at the top states: 'ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.' Below this, there is a 'Search' section with a search bar and a 'Leases' table. The 'Leases' table lists four entries:

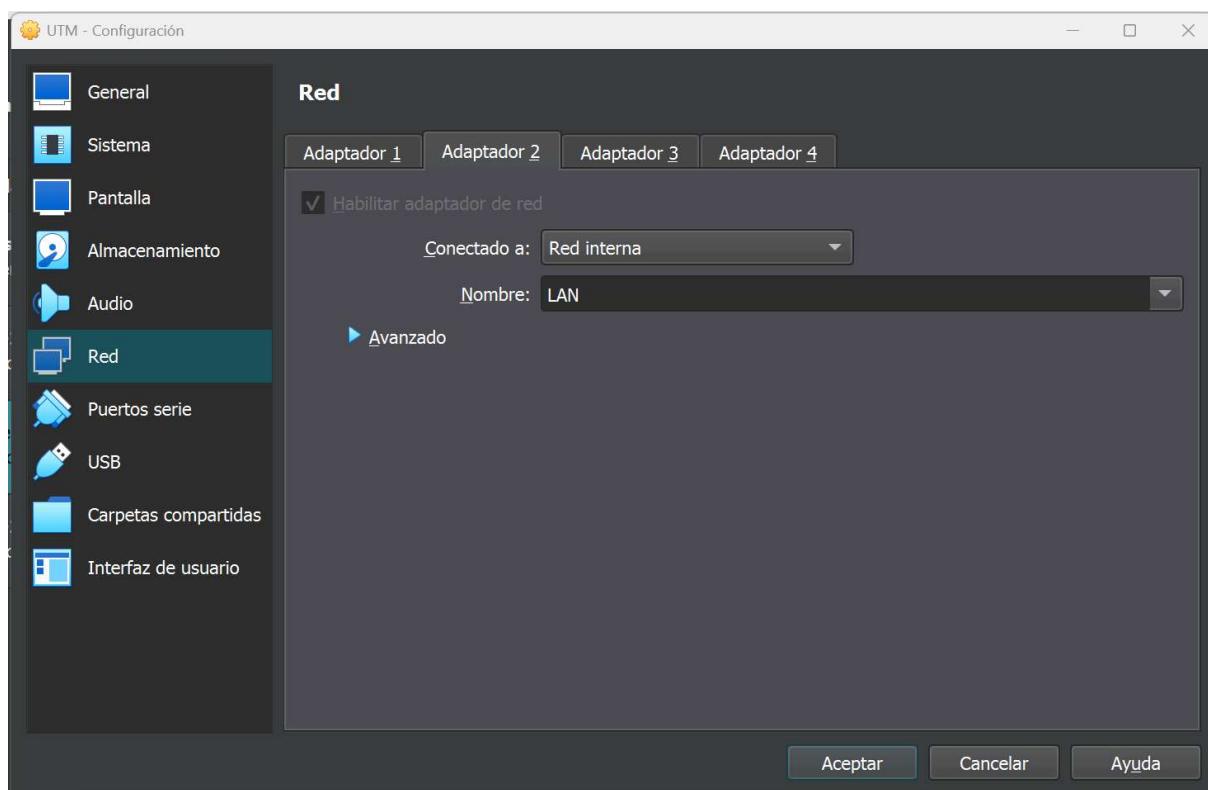
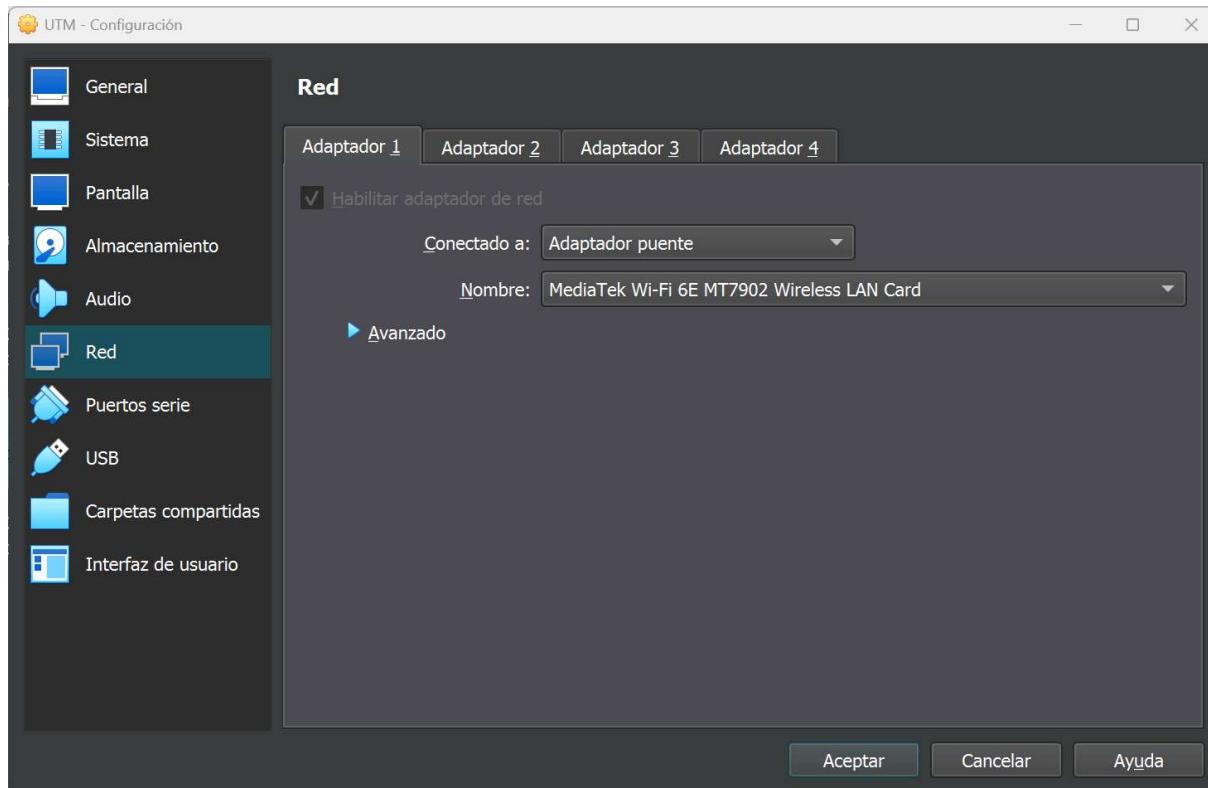
	IP Address	MAC Address	Hostname	Description	Start	End	Actions
1	192.168.200.99	08:00:27:d2:c6:66	kali	Honeypot	n/a	n/a	+ ⚒
2	192.168.100.99	08:00:27:ad:25:87	kali		n/a	n/a	+ ⚒
3	192.168.250.100	08:00:27:ad:25:87	kali		2025/01/19 17:43:01	2025/01/19 19:43:01	+ ⚒
4	192.168.100.101	08:00:27:17:6c:d0	Windows10		2025/01/19 17:08:41	2025/01/19 19:08:41	+ ⚒

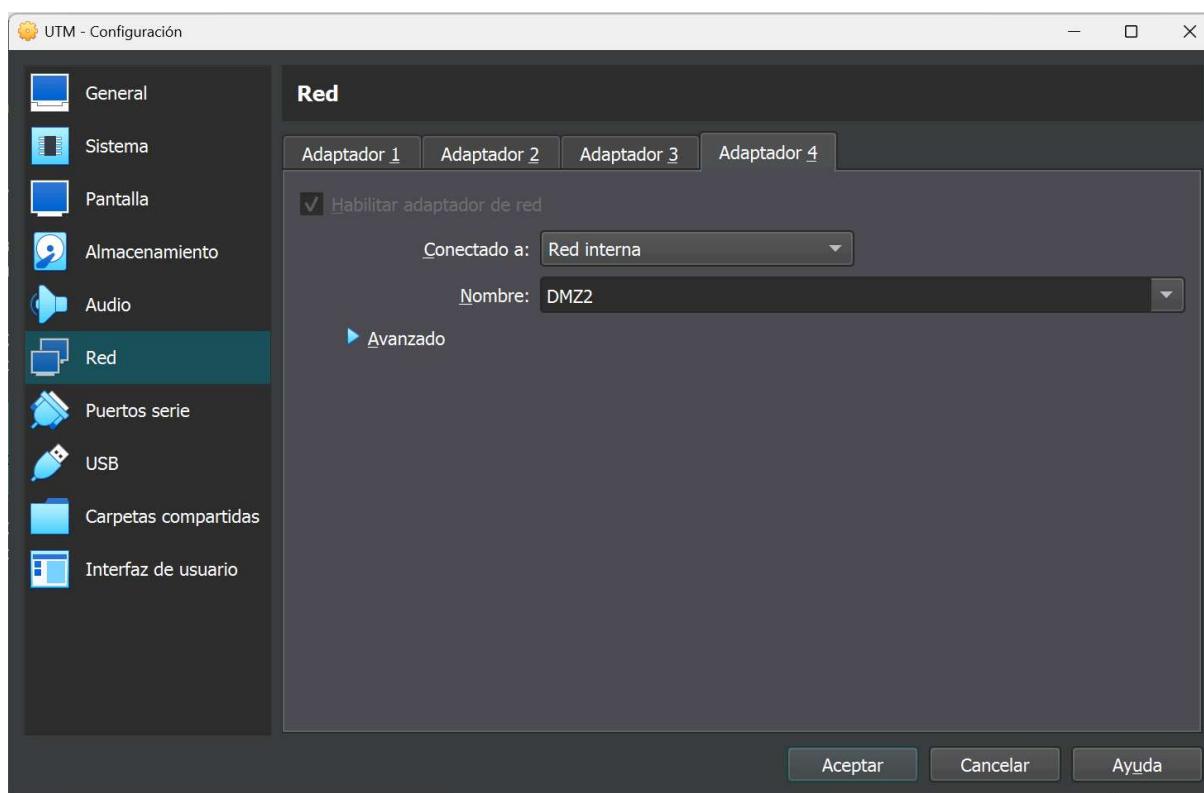
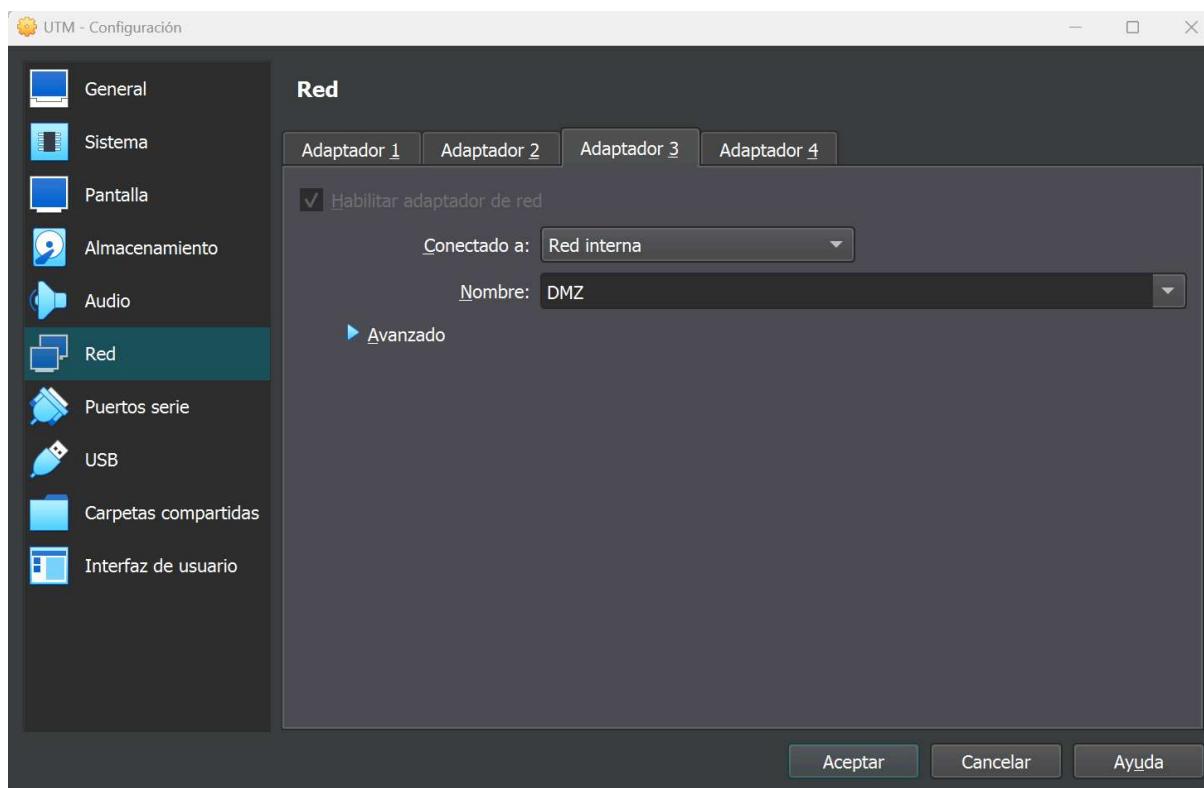
Below the leases table is a 'Lease Utilization' section showing network interface utilization:

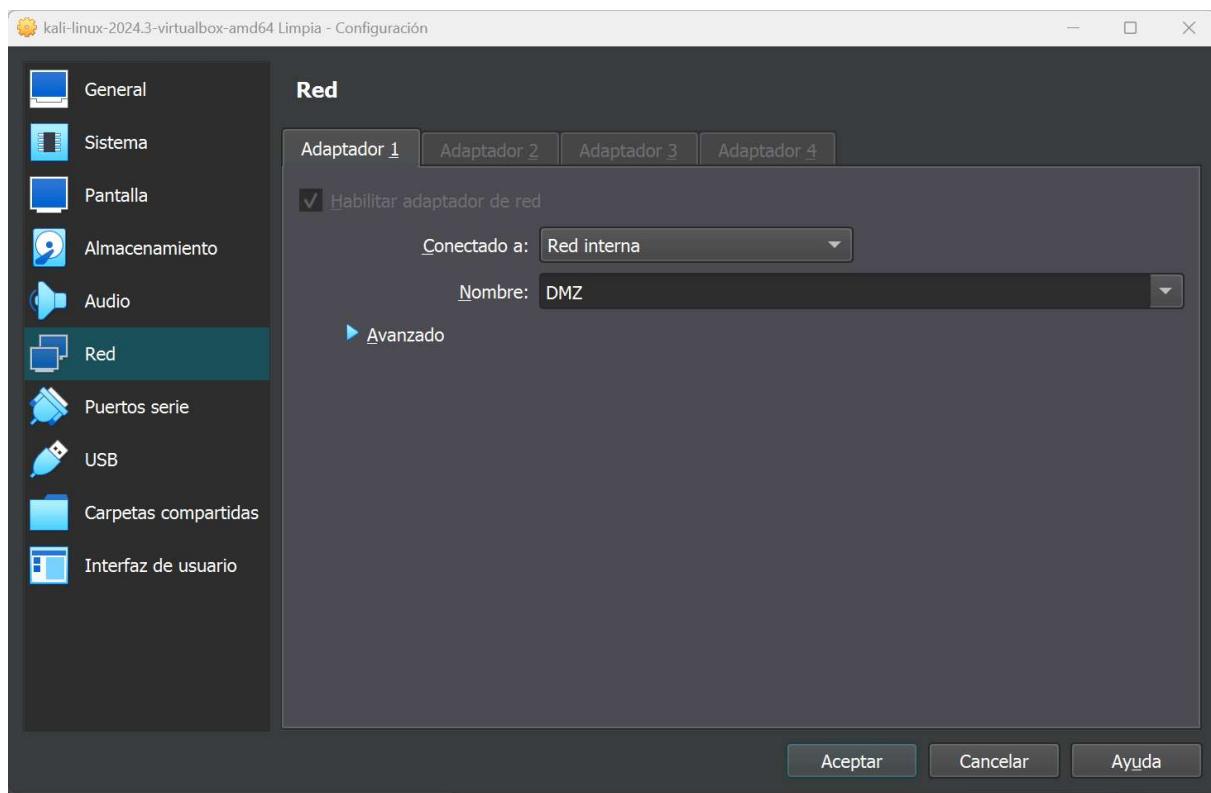
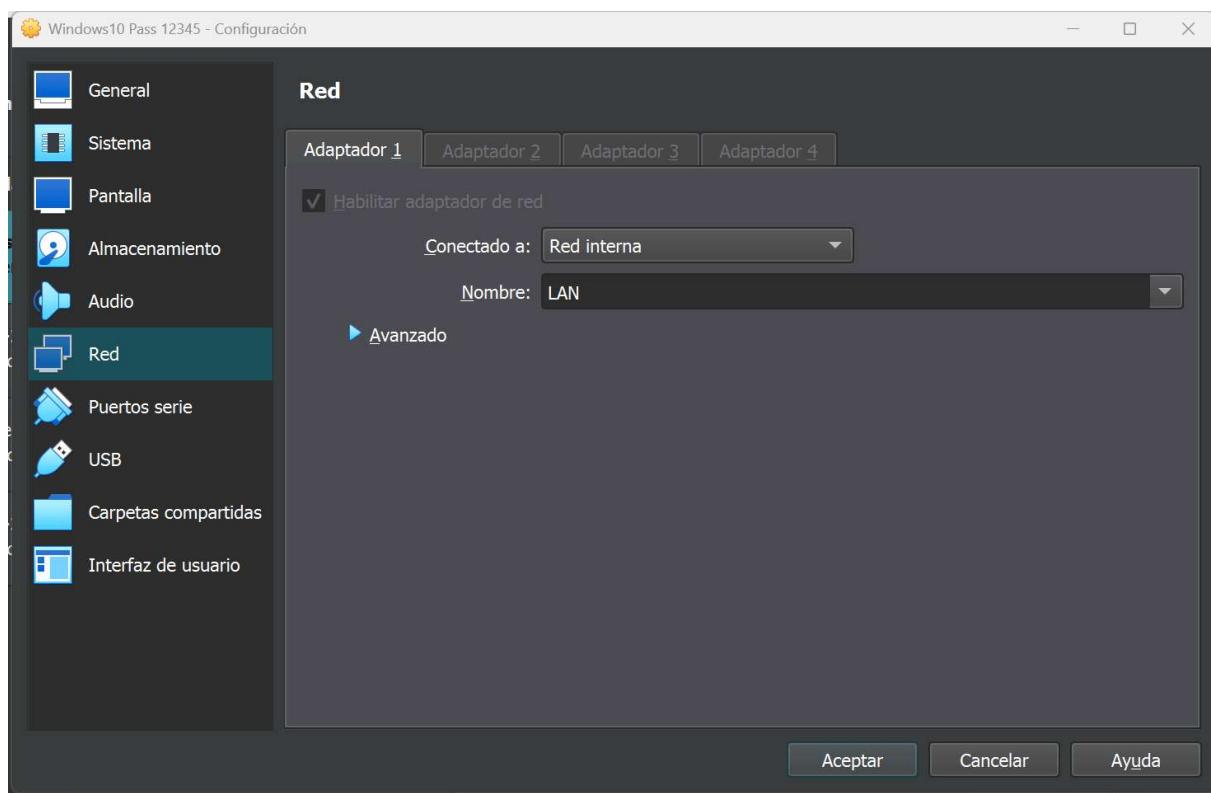
Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.100.100	192.168.100.200	1	101	0% of 101
DMZ2	192.168.250.100	192.168.250.150	1	51	1% of 51

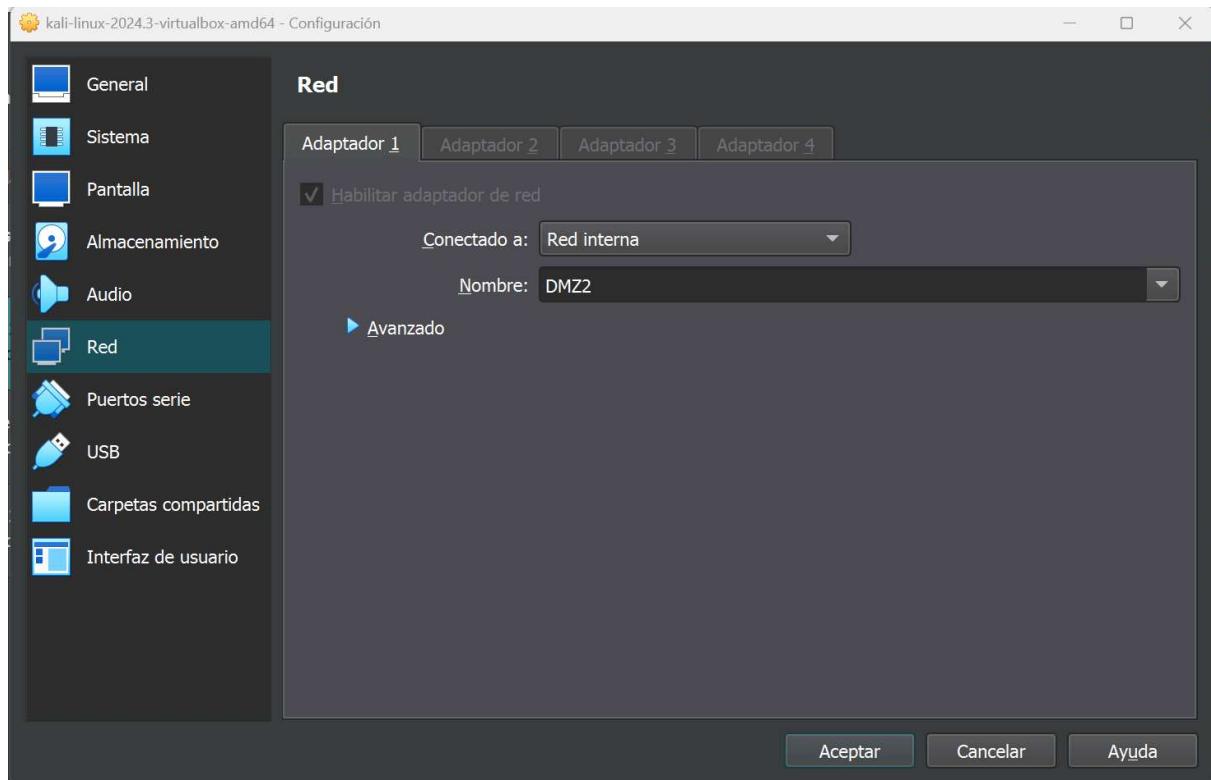
At the bottom are buttons for 'Show All Configured Leases' and 'Clear All DHCP Leases'.

Una vez realizados estos ajustes se puede proceder a asignar a cada máquina su red correspondiente del UTM, en las siguientes imágenes se muestra la configuración del mismo con los distintos adaptadores y como ha cada máquina se le asocia el que le corresponde:





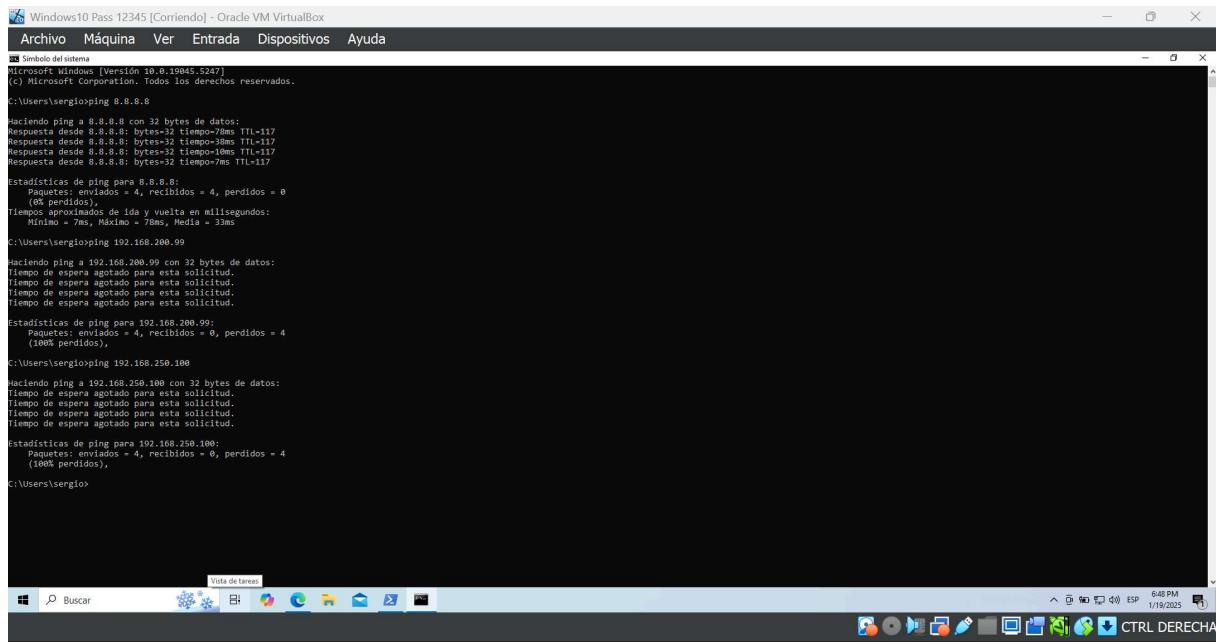




Una vez hecho esto se ha procedido a conectar todas las máquinas a la vez y testear si las reglas del firewall son las requeridas por la práctica:



Se procede a desde cada máquina a hacer un ping a la ip de google, para comprobar que hay conexión a internet, y un ping a las otras 2 IPs para comprobar que cada red está aislada de las otras 2:



```
Windows10 Pass 12345 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.5287]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\sergio\ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=7ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=38ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=10ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=7ms TTL=117

Estadísticas de ping para 8.8.8.8:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0,
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 7ms, Máximo = 78ms, Media = 33ms

C:\Users\sergio\ping 192.168.200.99

Haciendo ping a 192.168.200.99 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

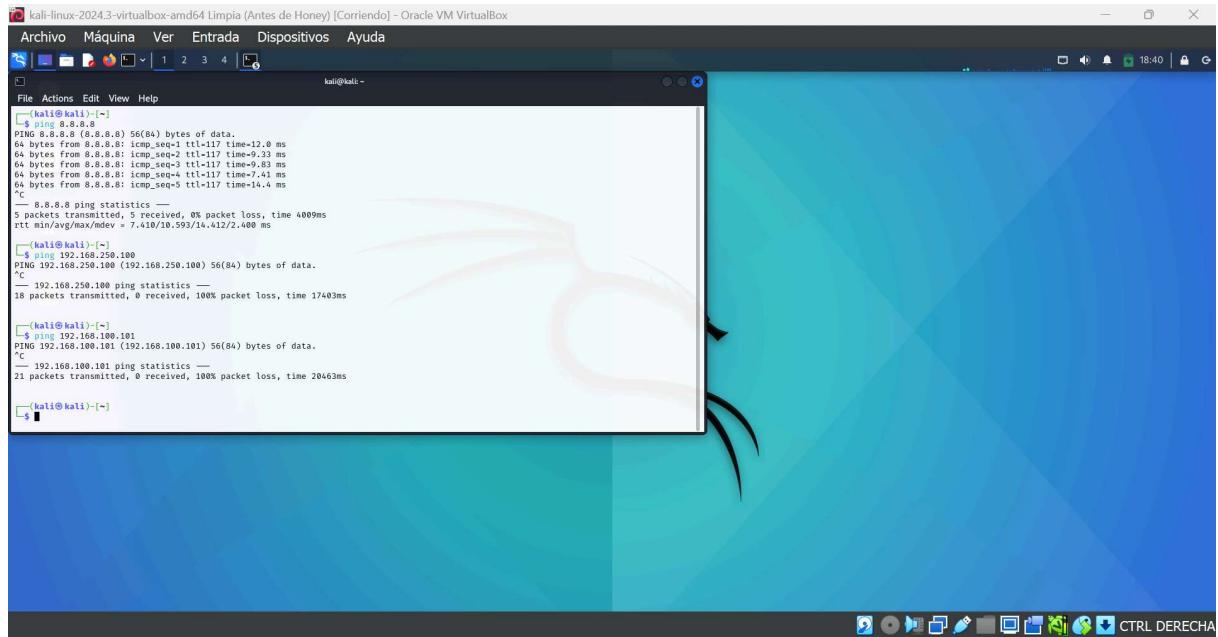
Estadísticas de ping para 192.168.200.99:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos).

C:\Users\sergio\ping 192.168.250.100

Haciendo ping a 192.168.250.100 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.250.100:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos).

C:\Users\sergio>
```



```
kali-llinux-2024.3-virtualbox-amd64 Limpia (Antes de Honey) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
kali@kali: ~
[kali@kali: ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=9.33 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=9.83 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=7.41 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=14.4 ms
...
8.8.8.8 ping statistics:
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 7.419/10.593/14.412/2.400 ms

[kali@kali: ~]$ ping 192.168.250.100
PING 192.168.250.100 (192.168.250.100) 56(84) bytes of data.
...
192.168.250.100 ping statistics —
38 packets transmitted, 0 received, 100% packet loss, time 17403ms

[kali@kali: ~]$ ping 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
...
192.168.100.101 ping statistics —
21 packets transmitted, 0 received, 100% packet loss, time 20463ms

[kali@kali: ~]$
```

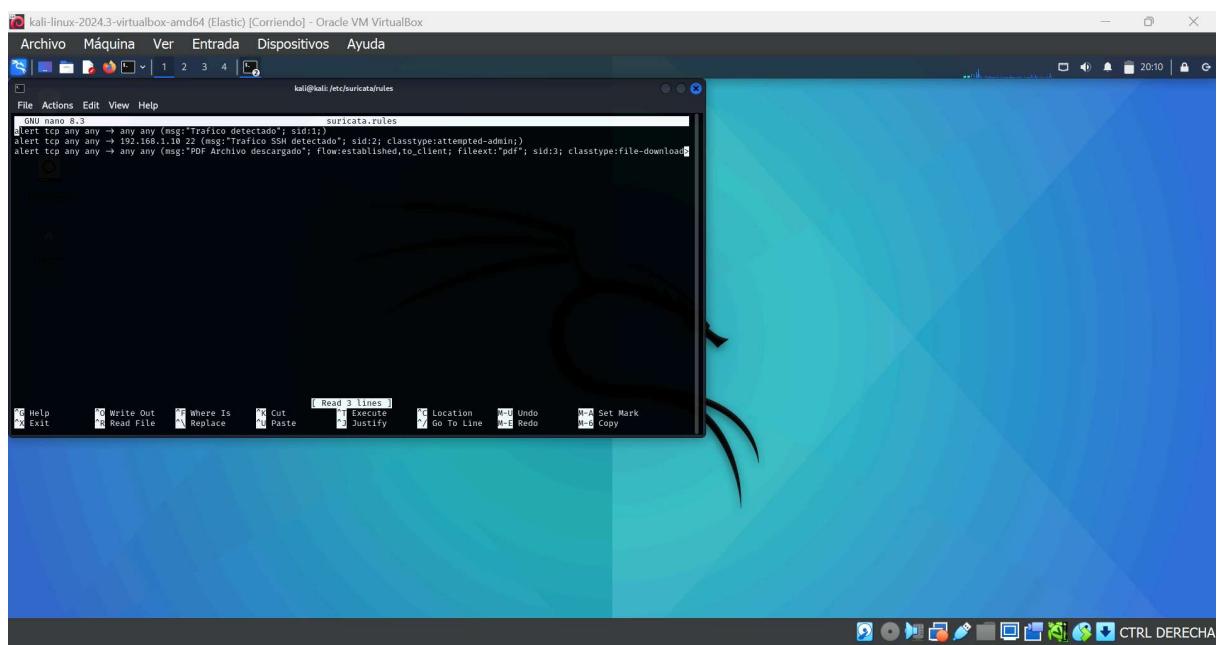
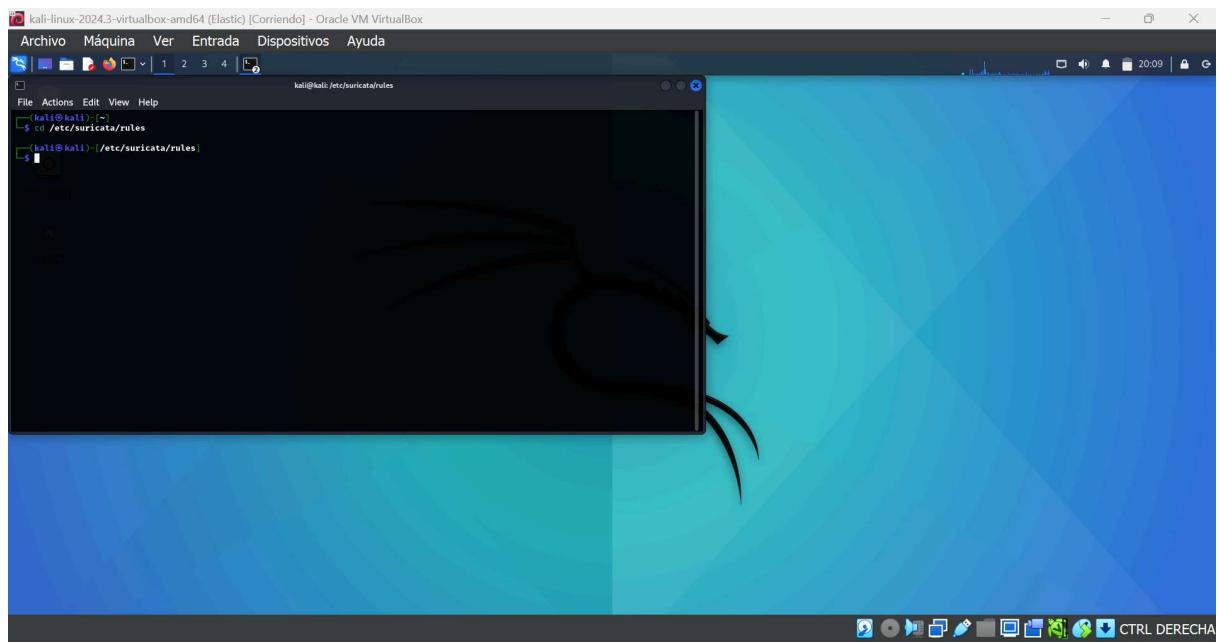
```
File Actions Edit View Help
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali@kali: ~
ping 192.168.200.99
PING 192.168.200.99 (192.168.200.99) 56(84) bytes of data.
... (output truncated)
ping 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
... (output truncated)
```

Una vez hechas las comprobaciones se procede a instalar Suricata en la máquina alojada en DMZ2 mediante los siguientes comandos:

```
sudo apt update
sudo apt install suricata
sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

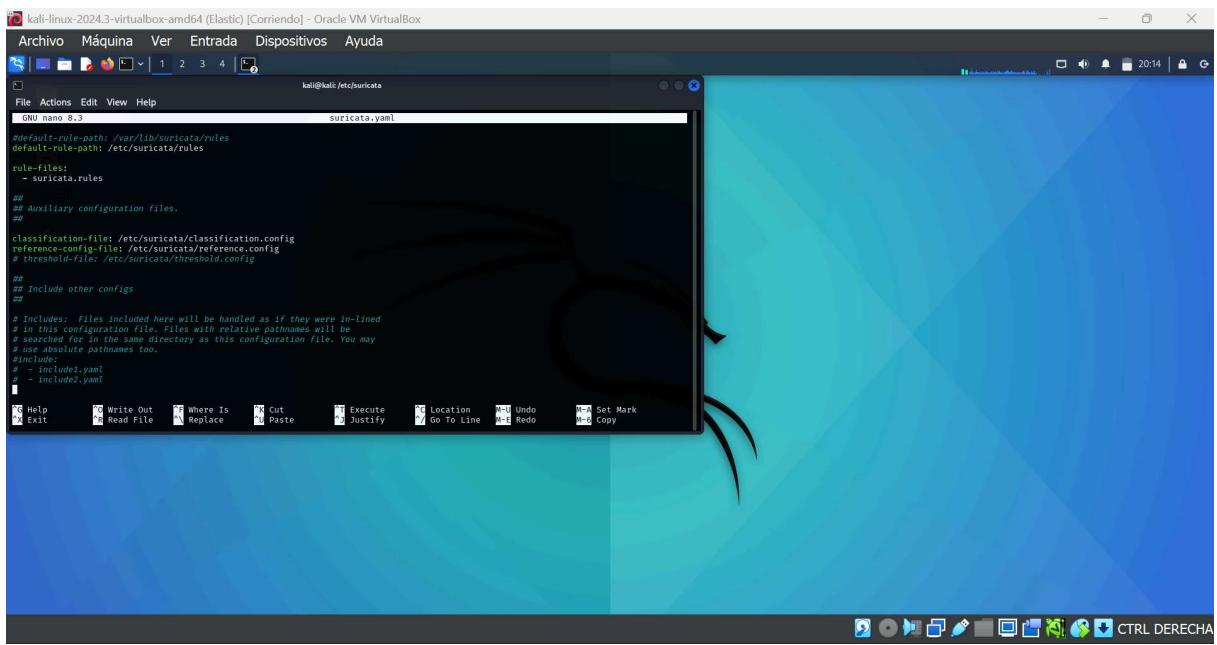
```
File Actions Edit View Help
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali@kali: ~
sudo suricata -c /etc/suricata/suricata.yaml -i eth0
[sudo] password for kali:
$ suricata: This is Suricata Version 7.0.8 RELEASE running in SYSTEM mode
$ threads: Threads created → Nr: 2 PNr: 1 PR: 1 Engine started.
```

En las siguientes imágenes se puede ver como se procede a editar las reglas de suricata:



A screenshot of a Kali Linux desktop environment. A terminal window titled 'suricata.yaml' is open, displaying the configuration file for the Suricata IDS/IPS system. The file includes sections for 'address-groups', 'vars', and 'EXTERNAL_NET'. The terminal interface features a blue gradient background and a standard Linux-style menu bar at the top. At the bottom, there is a dock with various application icons.

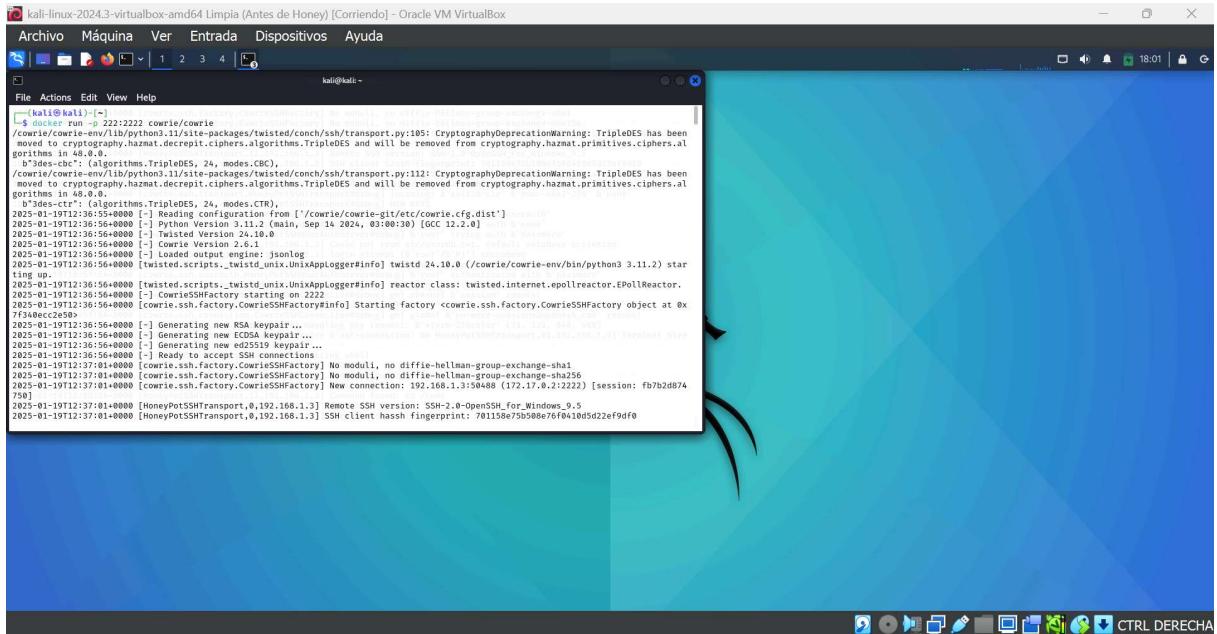
A screenshot of a Kali Linux desktop environment. The desktop background features a blue and green gradient with a stylized black spider logo. A terminal window titled "kali@kali: /etc/suricata" is open in the top-left corner. The terminal displays a command-line session where the user is editing Suricata configuration files. The session starts with navigating to the rules directory, opening nano editors for "suricata.rules" and "suricata.yaml", and then listing files in the directory. The terminal window has a dark theme and is located in the top-left corner of the screen.



Con esto quedaría configurado correctamente suricata.

Se procede ahora a instalar en la máquina Kali alojada en DMZ el honeypot Cowrie mediante los siguientes comandos

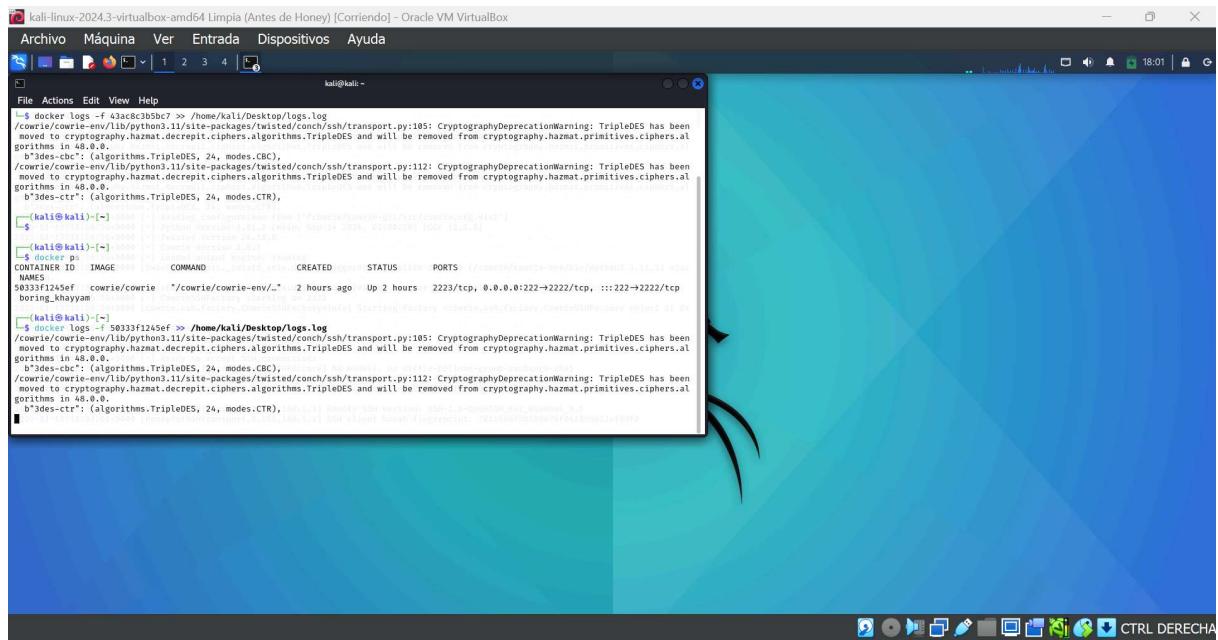
Docker run -p 222:2222 cowrie/cowrie



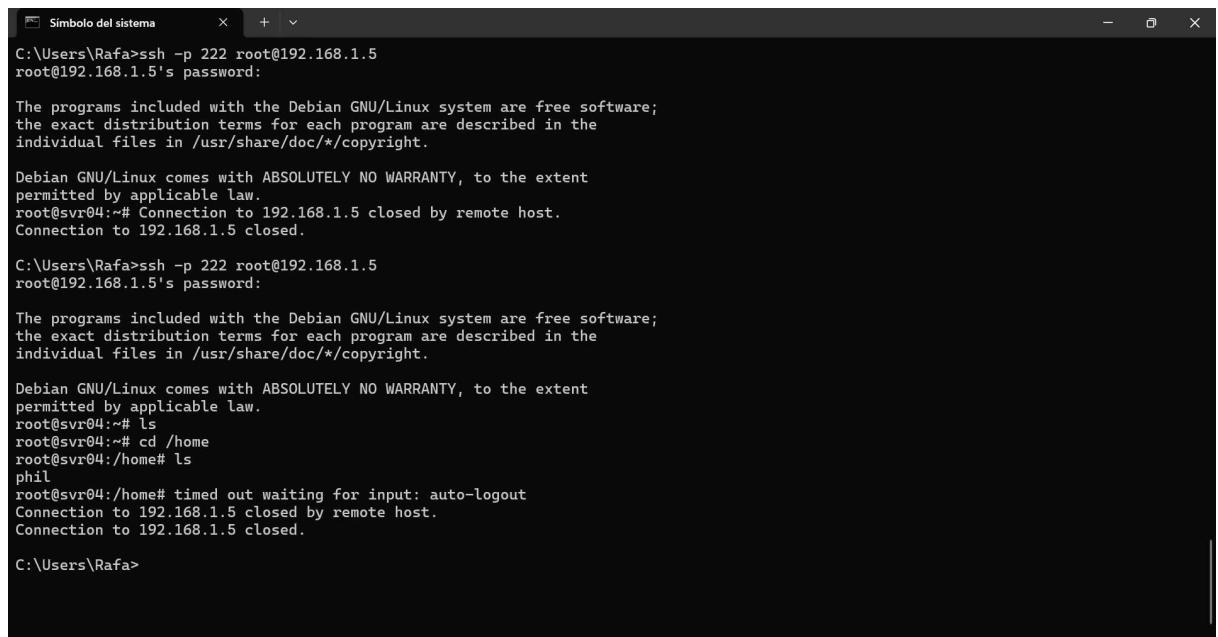
Como requisito de la práctica, es necesario extraer los logs que genera dicho honeypot a un archivo que se subirá más adelante a Elastic, para ello se ha usado el siguiente comando:

```
docker logs -f (id_contenedor_docker) >> /home/kali/Desktop/logs.log
```

Con esto se consigue un archivo que se actualiza añadiendo nuevas líneas cada vez que se produce una conexión SSH desde WAN, registrándose los comandos introducidos.



A continuación podemos ver como un SSH desde el equipo Host llega a la máquina alojada en la red DMZ a través de la red WAN



Como se puede apreciar con este comando CAT al archivo logs.log, los inputs de la conexión SSH se añaden a continuación de la última linea.

```

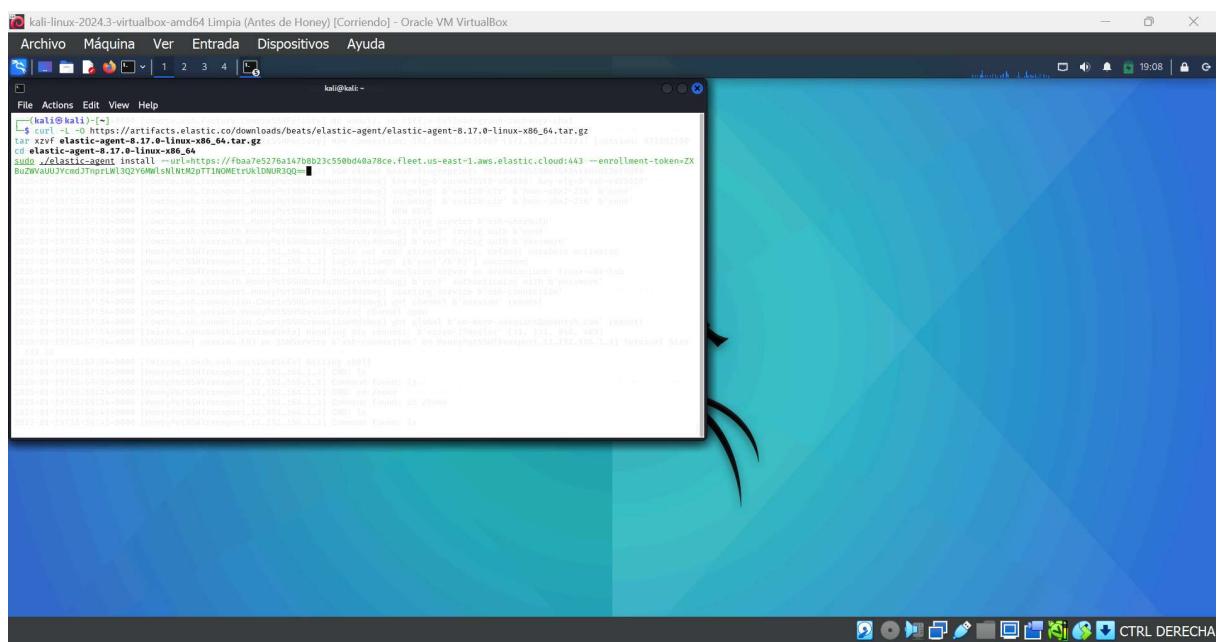
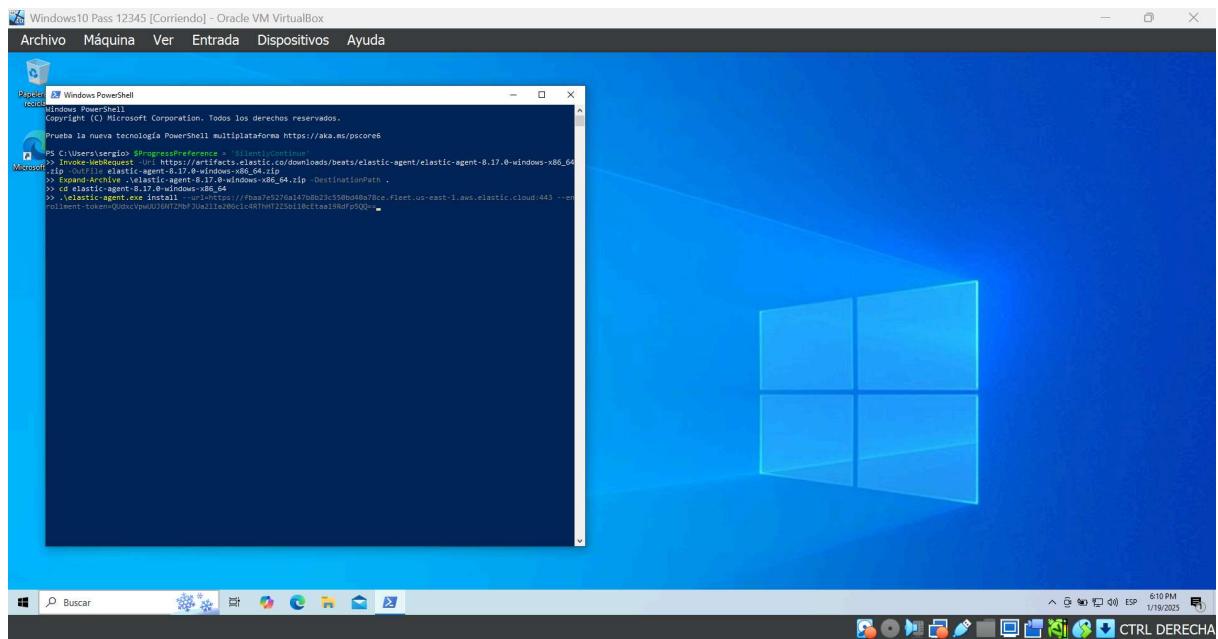
kali-linux-2024.3-virtualbox-amd64 Limpia (Antes de Honey) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Applications Edit View Help
kali@kali:~$ cat logs.log
2025-01-19T16:57:52+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2025-01-19T16:57:52+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2025-01-19T16:57:52+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 192.168.1.3:51069 (172.17.0.2:2222) [session: 073581588]
2025-01-19T16:57:52+0000 [HoneyPotSSHTransport,12.192.168.1.3] Remote SSH version: SSH-2.0-OpenSSH_for_Windows_9.5
2025-01-19T16:57:52+0000 [HoneyPotSSHTransport,12.192.168.1.3] Session hash fingerprint: 701158e75b508e76f04c5d24ef4ff0
2025-01-19T16:57:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=B-Blowfish-CFB3:kex alg=B-SHA256:kex mac=B-SHA256:b-name
2025-01-19T16:57:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha-256' b'none'
2025-01-19T16:57:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2025-01-19T16:57:52+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] trying auth 'b'password'
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] Could not read file /etc/ssh/sshd_config, default database activated
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] attempting (D)irect ('h'ost) connection
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] initialized server as architecture: linux-x64-lsb
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with 'b'password'
2025-01-19T16:57:52+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] got global b'no-more-sessions-open'
2025-01-19T16:57:52+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session-request'
2025-01-19T16:57:52+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2025-01-19T16:57:52+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions-open'
2025-01-19T16:57:52+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] Handling session request: b'xterm-256color' (22, 132, 648, 480)
2025-01-19T16:57:52+0000 [SSHChannel session (*) on SSHService b'ssh-connection' on HoneyPotSSHTransport,12.192.168.1.3] Terminal Size
133 33
2025-01-19T16:57:54+0000 [twisted.conch.ssh.session#info] Getting shell
2025-01-19T16:57:54+0000 [HoneyPotSSHTransport,12.192.168.1.3] CMD: ls
2025-01-19T16:58:24+0000 [HoneyPotSSHTransport,12.192.168.1.3] CMD: cd /home
2025-01-19T16:58:24+0000 [HoneyPotSSHTransport,12.192.168.1.3] Command found: cd /home
2025-01-19T16:58:45+0000 [HoneyPotSSHTransport,12.192.168.1.3] CMD: ls
2025-01-19T16:58:45+0000 [HoneyPotSSHTransport,12.192.168.1.3] Command found: ls

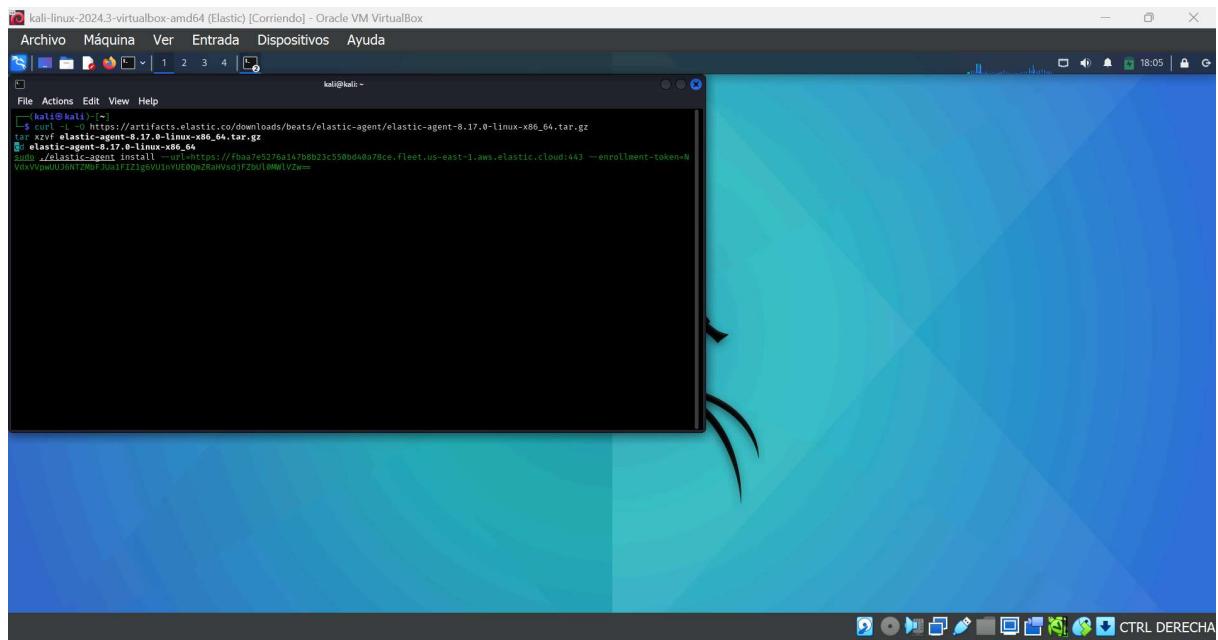
```

Una vez que hemos llegado a este punto se puede proceder a crear una cuenta en la web de elastic y configurar las máquinas, en esta imagen se puede apreciar las 3 máquinas funcionando tras la instalación de los respectivos agentes en las terminales de cada una

Status	Host	Agent policy	CPU	Memory	Last activ...	Version
Healthy	kali	Honeypot	3.04 %	217 MB	30 seconds ago	8.17.0
Healthy	Windows10	Windows	8.36 %	169 MB	10 seconds ago	8.17.0
Healthy	kali	Suricata/Linux	2.90 %	217 MB	4 seconds ago	8.17.0

A continuación se muestra la instalación de cada uno de ellos en su máquina correspondiente





Una vez hechos estos pasos se pueden consultar los logs de cada uno, se ha procedido a filtrar por el campo Agent ID de cada uno

Máquina Windows

Agent ID	ef96669a-e0cb-4e09-838d-28bbe2eeff01
Agent policy	Windows rev. 2
Agent version	8.17.0
Host name	Windows10
Host ID	b03073f0-8c78-41e8-81ed-eb67037c01c4
Output for integrations	Default output
Output for monitoring	Default output
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	windows
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

Máquina Kali con Honeypot

The screenshot shows the Splunk interface for the 'kali' agent. The left sidebar has 'Assets' selected. The main panel displays the 'Overview' section for the 'kali' agent, which is healthy. It shows metrics like CPU usage (2.07%), memory (209 MB), and status (Healthy). The 'Integrations' section shows a connection to 'log-1' and 'Inputs'. The 'Logs' tab is active.

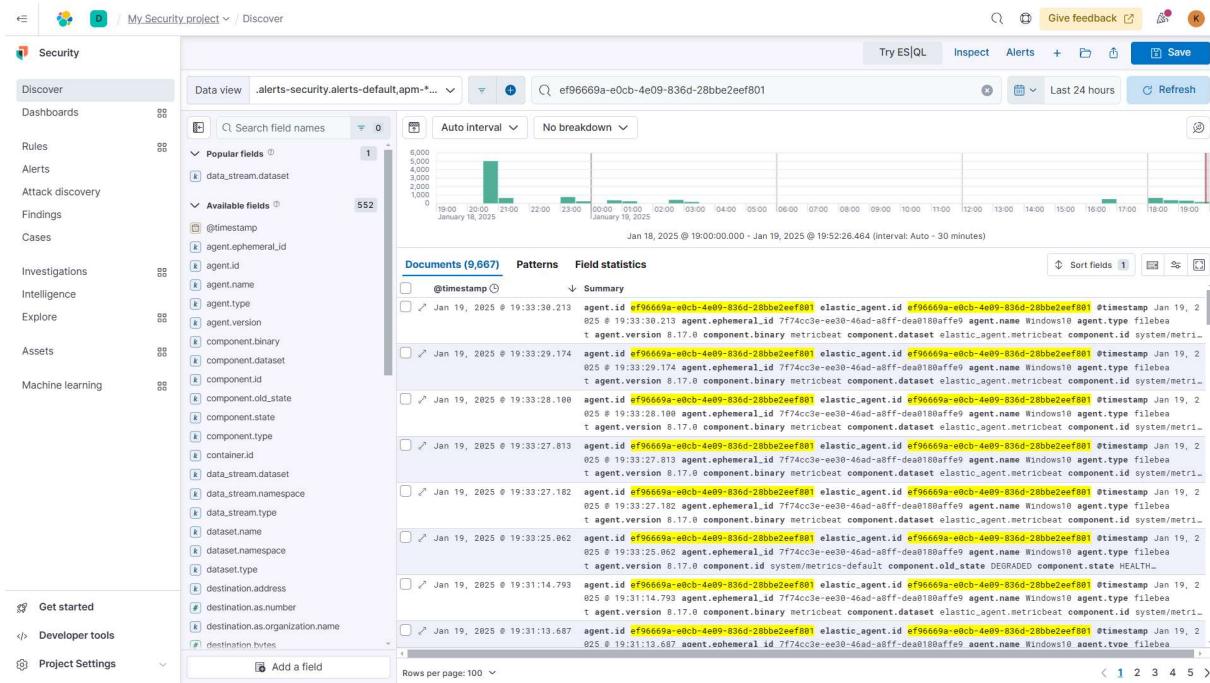
Metric	Value
CPU	2.07 %
Memory	209 MB
Status	Healthy
Last activity	30 seconds ago
Last checkin message	Waiting for initial configuration and composable variables
Agent ID	ec4d07db-aeecc-4262-93e5-554176e03d5d
Agent policy	Honeypot rev. 2
Agent version	8.17.0
Host name	kali
Host ID	30e662c5c81d4191bd2444a79c97d2e0
Output for integrations	Default output
Output for monitoring	Default output
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	kali
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

Máquina Kali con Suricata

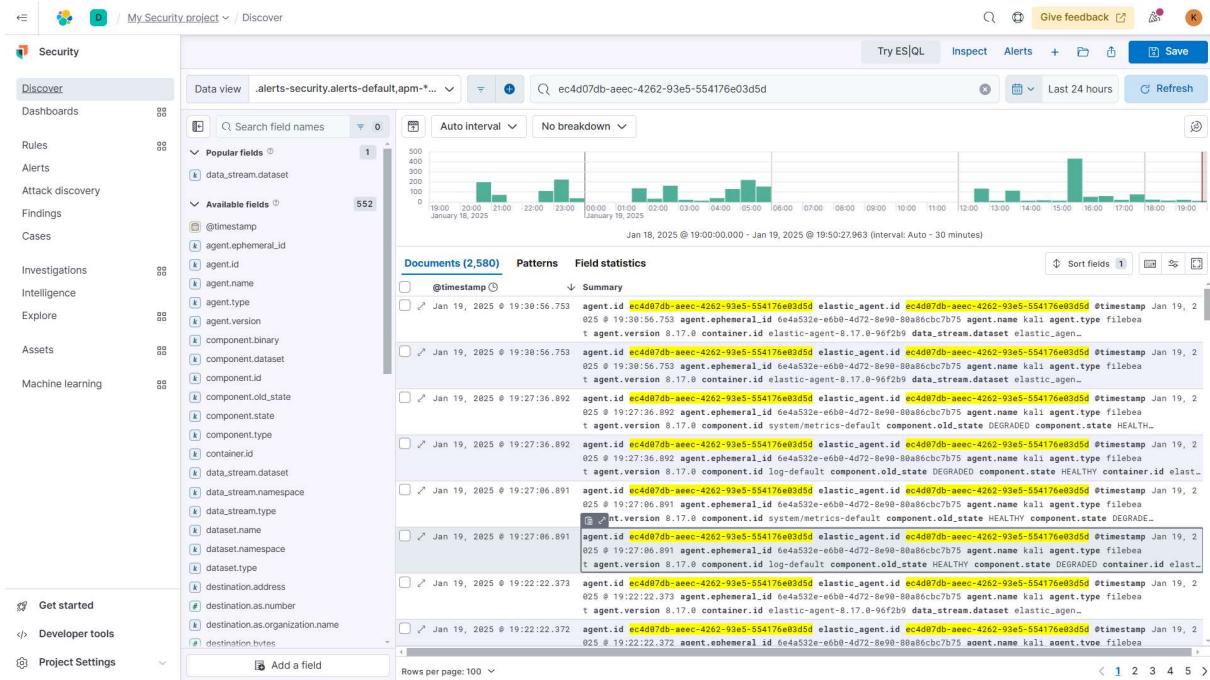
The screenshot shows the Splunk interface for the 'kali' agent. The left sidebar has 'Assets' selected. The main panel displays the 'Overview' section for the 'kali' agent, which is healthy. It shows metrics like CPU usage (3.31%), memory (213 MB), and status (Healthy). The 'Integrations' section shows a connection to 'suricata-1' and 'Inputs'. The 'Logs' tab is active.

Metric	Value
CPU	3.31 %
Memory	213 MB
Status	Healthy
Last activity	17 seconds ago
Last checkin message	Waiting for initial configuration and composable variables
Agent ID	6925dab-1558-461d-99a9-8860fb4ea80
Agent policy	Suricata/Linux rev. 2
Agent version	8.17.0
Host name	kali
Host ID	30e662c5c81d4191bd2444a79c97d2e0
Output for integrations	Default output
Output for monitoring	Default output
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	kali
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

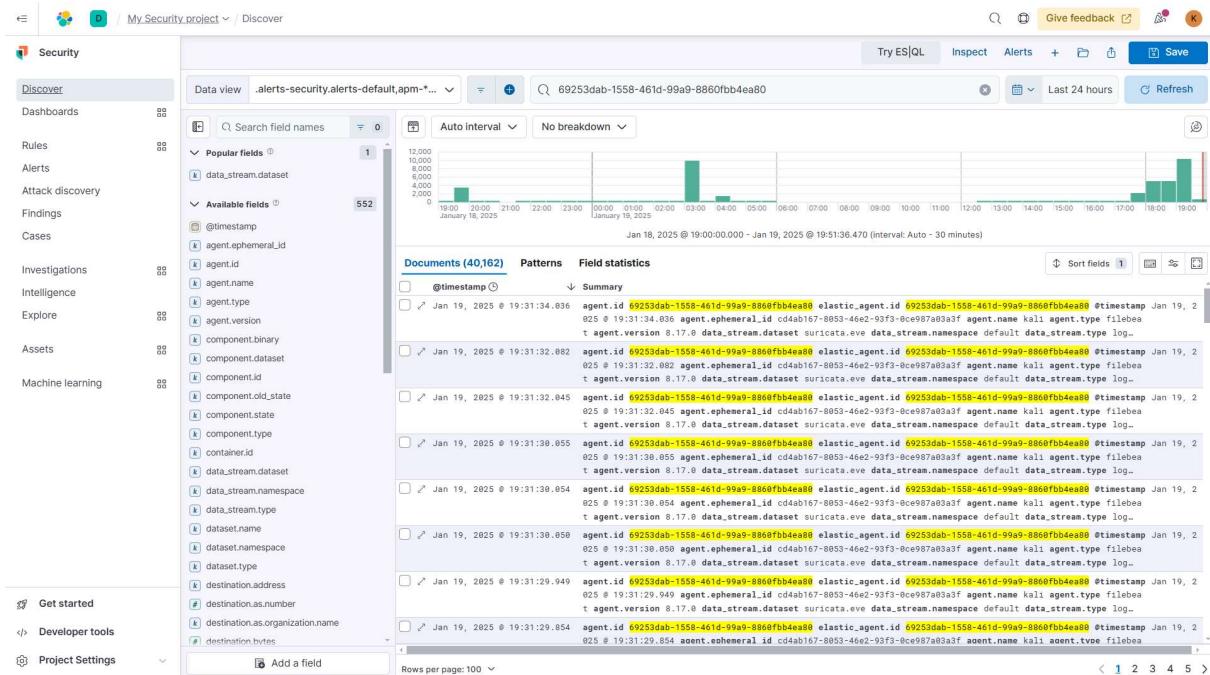
Logs generados por máquina la Windows en las últimas 24 horas:



Logs generados por máquina Kali con honeypot en las últimas 24 horas:



Logs generados por máquina Kali con Suricata en las últimas 24 horas:



Con esto se da por concluida la memoria, se adjuntará en github archivos .txt con copia de los datos de una entrada del log de cada máquina.