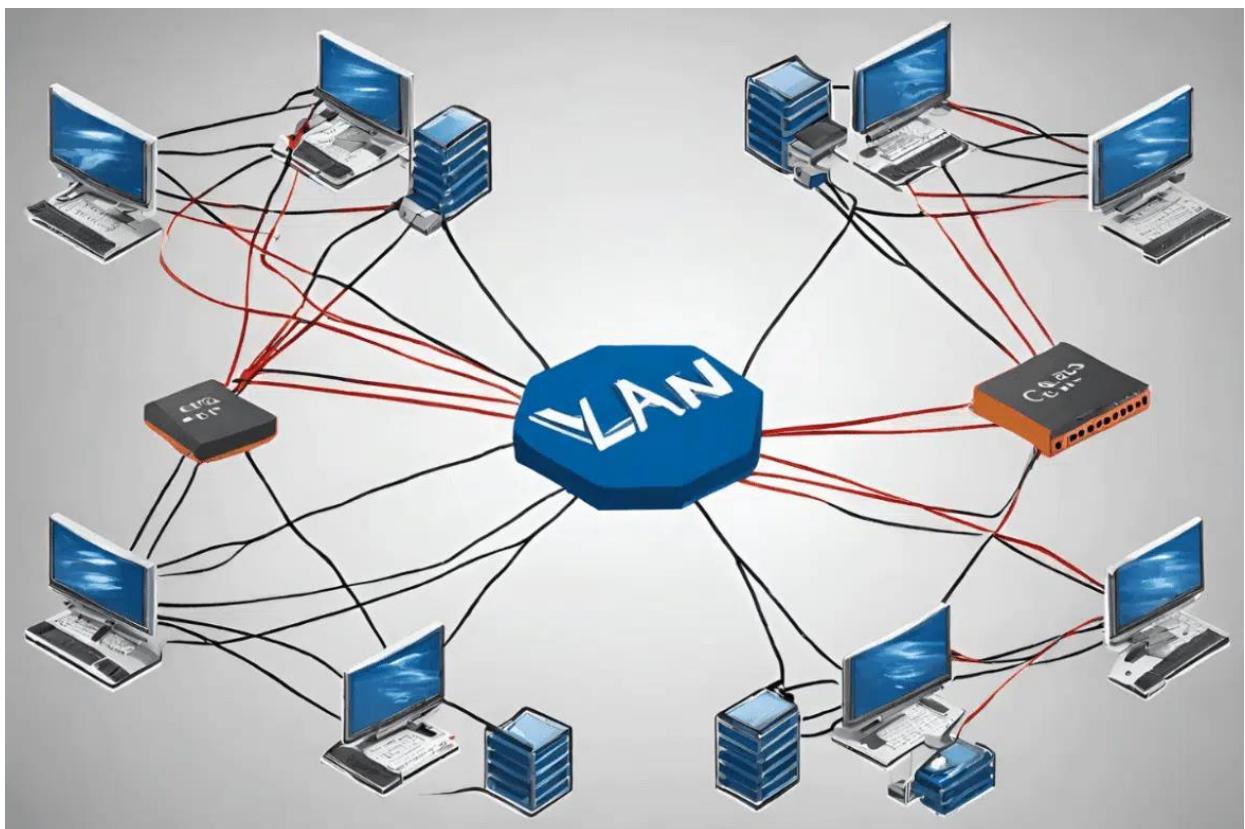


INFORME DE

SEGMENTACION DE REDES



Nombre: Brayan Gabriel Gutierrez Rebolledo

Modulo: Blue Team

Profesor: Sergio Vilches

Fecha: 02/02/2025

INDICE

PORTADA **1**

INDICE **2**

INTRODUCCION **3**

DESARROLLO **4**

CONCLUSIÓN **X**

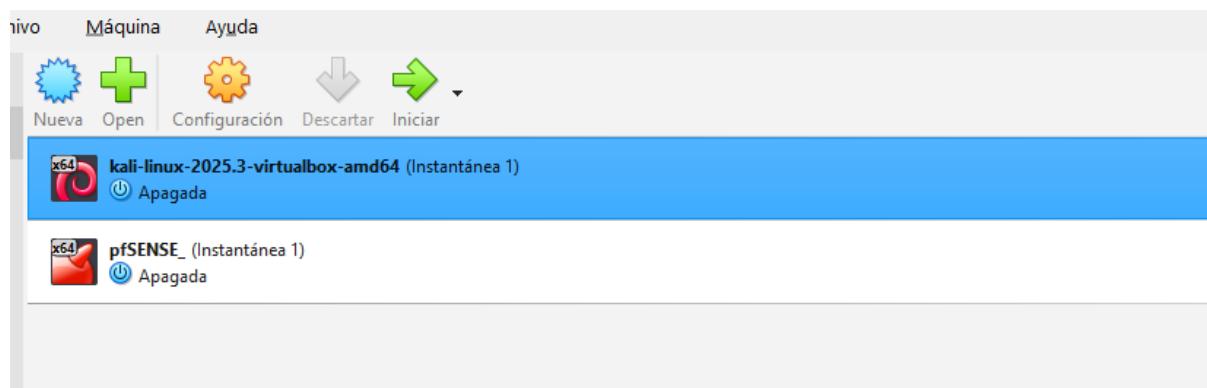
RECOMENDACIONES **6**

CONCLUSIÓN **7**

INTRODUCCION

DESARROLLO

Para el desarrollo de la práctica se asume que pfSense y Kali Linux ya han sido instalados en VirtualBox. En caso contrario, se proporcionará un tutorial de instalación como material de apoyo.



INSTALAR KALI LINUX

<https://www.youtube.com/watch?v=CSPrrw4ePzg>

INSTALAR pfSense

<https://www.youtube.com/watch?v=-vndaBqCqX8>

Posteriormente se revisó un enunciado en donde se necesita crear una segmentación de redes las cuales tienen **4 maquinas virtuales**:

- **pfSense**

- **Windows**

- **Ubuntu Server (Honeypot)**

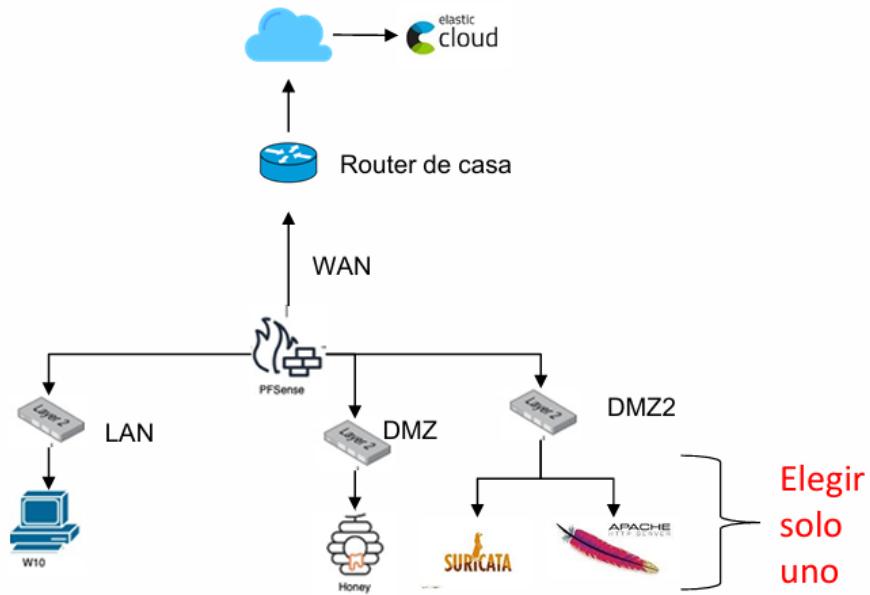
- **Ubuntu Server (Apache)**

Por elección personal se utiliza Ubuntu Server

ENUNCIADO

Enunciado

Queremos montar la siguiente infraestructura:



En esta práctica se plantea la creación de una infraestructura de red utilizando **pfSense** como firewall principal. El objetivo es poder controlar de mejor manera las conexiones de red, evitando que todas las máquinas tengan los mismos permisos y separando la red en distintos segmentos.

pfSense se encarga de dividir la red en varias zonas, cada una con una función específica, lo que permite aislar los sistemas y aumentar la seguridad.

- **WAN:** corresponde a la conexión entre pfSense e Internet, a través del router de casa.
- **LAN:** red interna donde se encuentra el equipo del usuario (Windows).
- **DMZ:** zona expuesta de la red donde se ubica un honeypot, utilizado para registrar intentos de acceso.
- **DMZ2:** zona separada destinada a un sistema de monitorización, donde se debe elegir un único servicio, ya sea Apache o Suricata.

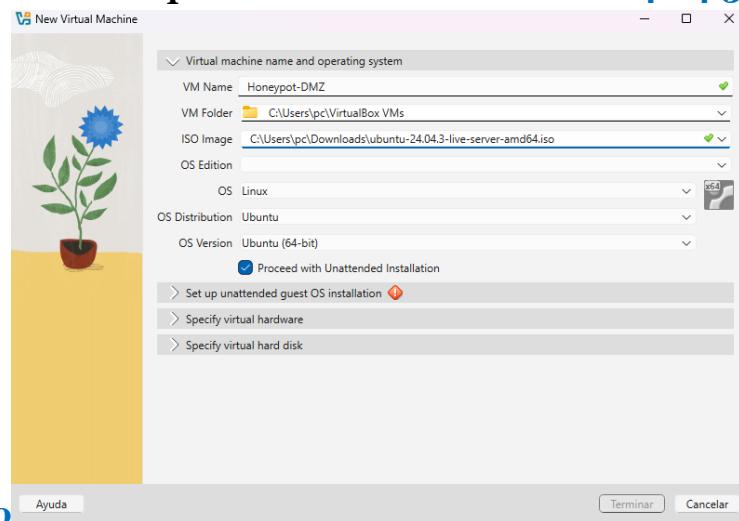
PROCEDIMIENTO

INSTALACION DE VMS

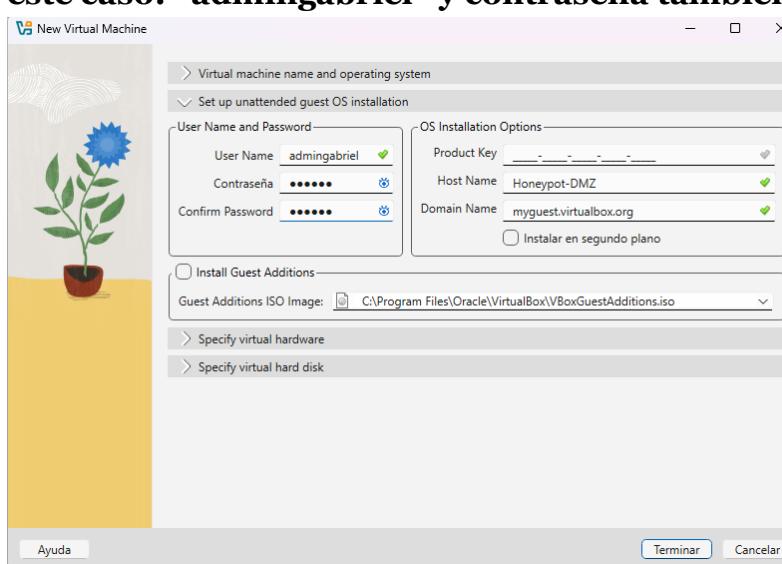
Primero se procederá a la instalación de las máquinas virtuales correspondientes a **DMZ** y **DMZ2**

Honeypot (UBUNTU SERVER-DMZ)

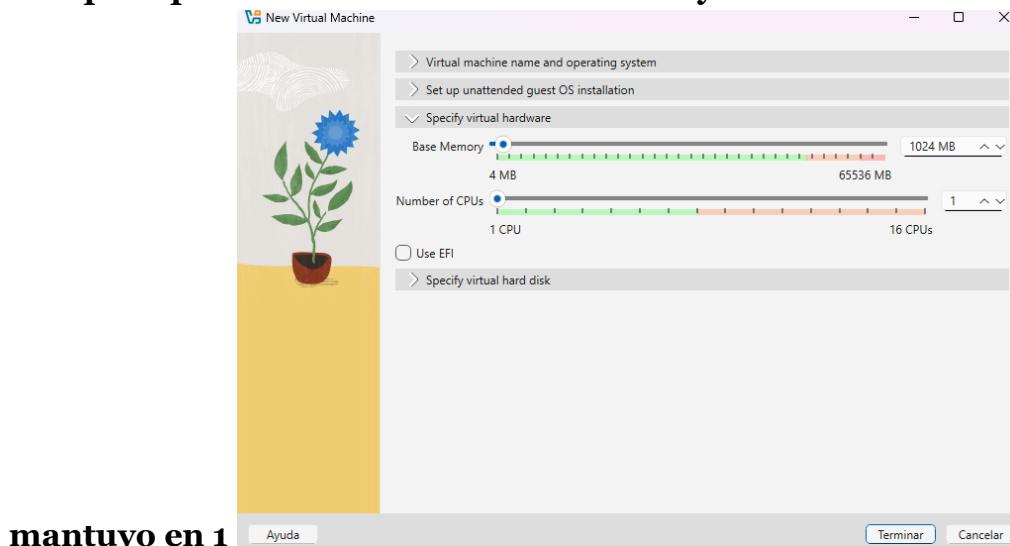
- 1. Creamos una nueva maquina en virtual box llamada "Honeypot-DMZ"**
- 2. Cargamos el "archivo.iso" que en este caso es: [ubuntu-24.04.3-live-server-amd64.iso](#)**



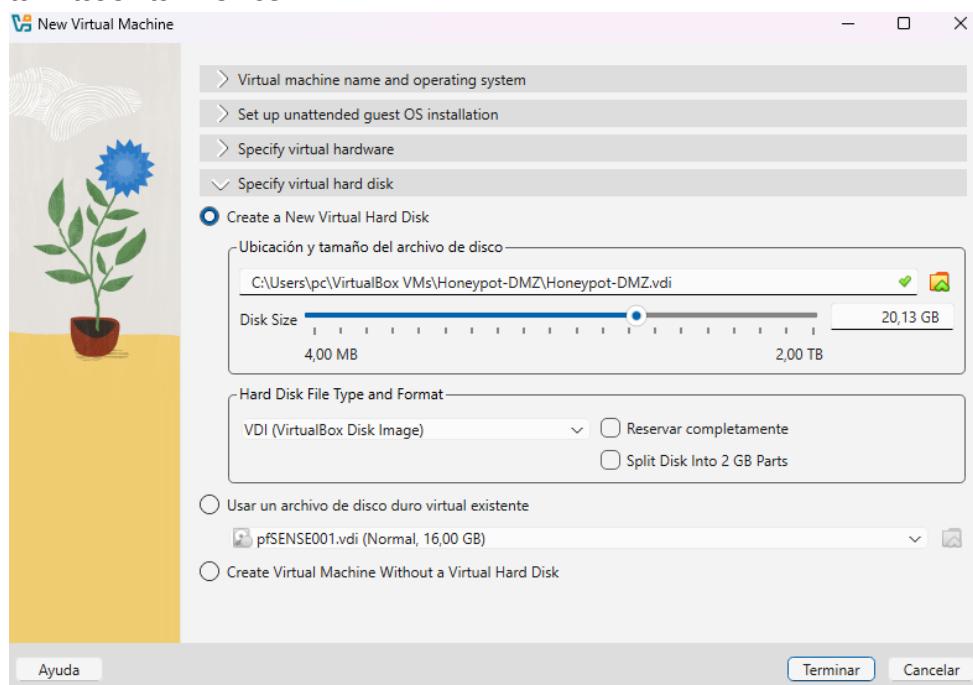
- 3. En "User Name" colocamos a preferencia nuestra el nombre, en este caso: "admingabriel" y contraseña tambien elección personal**



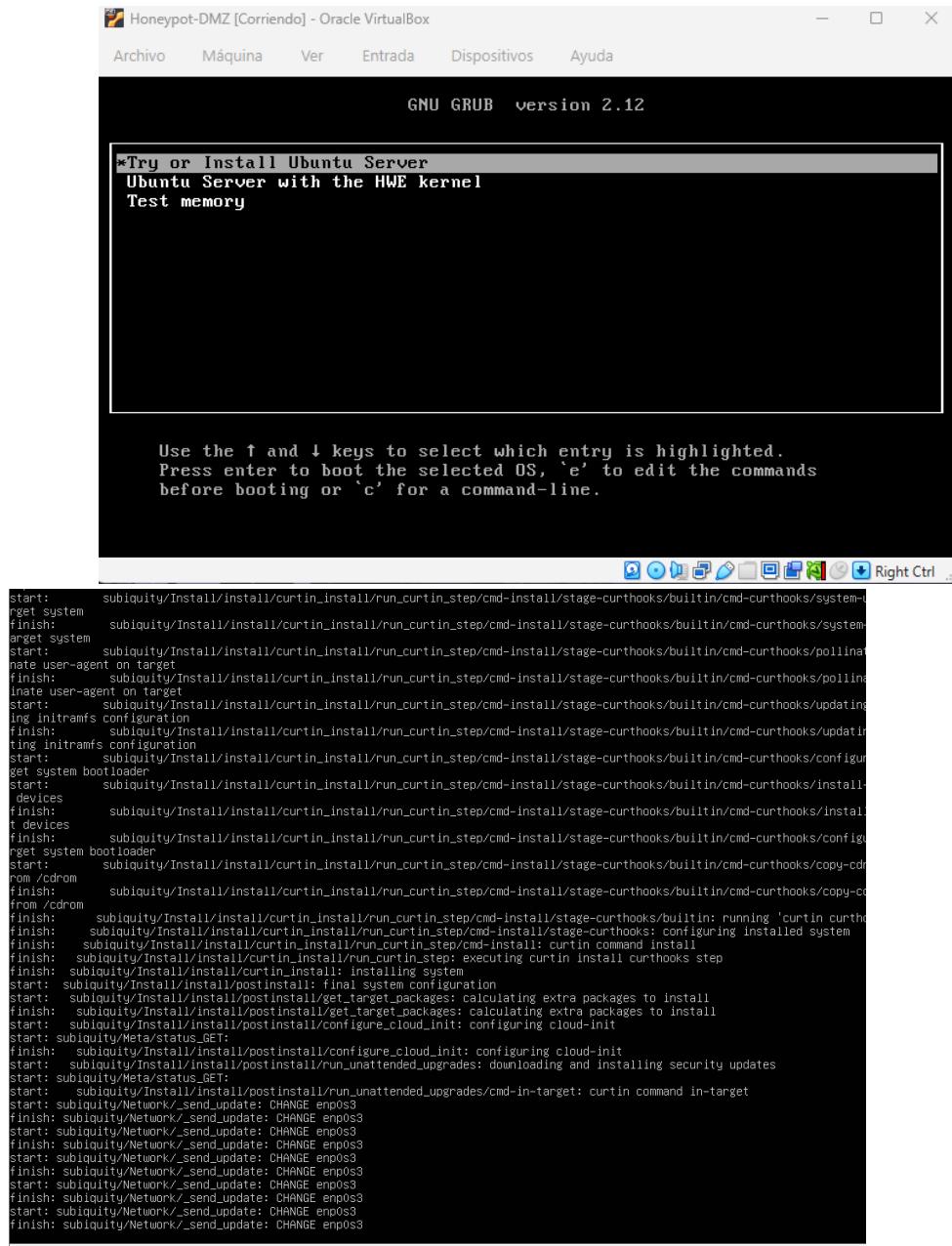
- 4. En el apartado de Specify virtual Hardware se colocó mínimo 1024 MB que equivale a 1 GB en memoria RAM y en Number of CPUs se**



- 5. Se escogió 20 GB en disco para que no existan problemas de almacenamiento**



- 6. Seleccionar Try or Install Ubuntu Server y esperar a que cargue la instalacion.**



Cerrar cuando diga:

```

start: subiquity/Network/_send_update: CHANGE enp0s3
finish: subiquity/Network/_send_update: CHANGE enp0s3

```

7. Loguearse con el username creado en las configuraciones de la máquina virtual, en este caso fue "admingabriel" y la contraseña escrita personalmente

```
Ubuntu 24.04.3 LTS Honeypot-DMZ tty1
```

```
Honeypot-DMZ login: admingabriel_
```

```
Ubuntu 24.04.3 LTS Honeypot-DMZ tty1
```

```
Honeypot-DMZ login: admingabriel  
Password:
```

```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-94-generic x86_64)
```

8. Obteniendo correctamente iniciar sesión en el servidor de Ubuntu

```
Ubuntu 24.04.3 LTS Honeypot-DMZ tty1
```

```
Honeypot-DMZ login: admingabriel
```

```
Password:
```

```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-94-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
```

```
System information as of Fri Jan 30 04:23:41 AM UTC 2026
```

System load: 0.0	Processes: 94
Usage of /: 13.2% of 19.64GB	Users logged in: 0
Memory usage: 19%	IPv4 address for enp0s3: 192.168.200.101
Swap usage: 0%	

```
Expanded Security Maintenance for Applications is not enabled.
```

```
111 updates can be applied immediately.
```

```
55 of these updates are standard security updates.
```

```
To see these additional updates run: apt list --upgradable
```

```
Enable ESM Apps to receive additional future security updates.
```

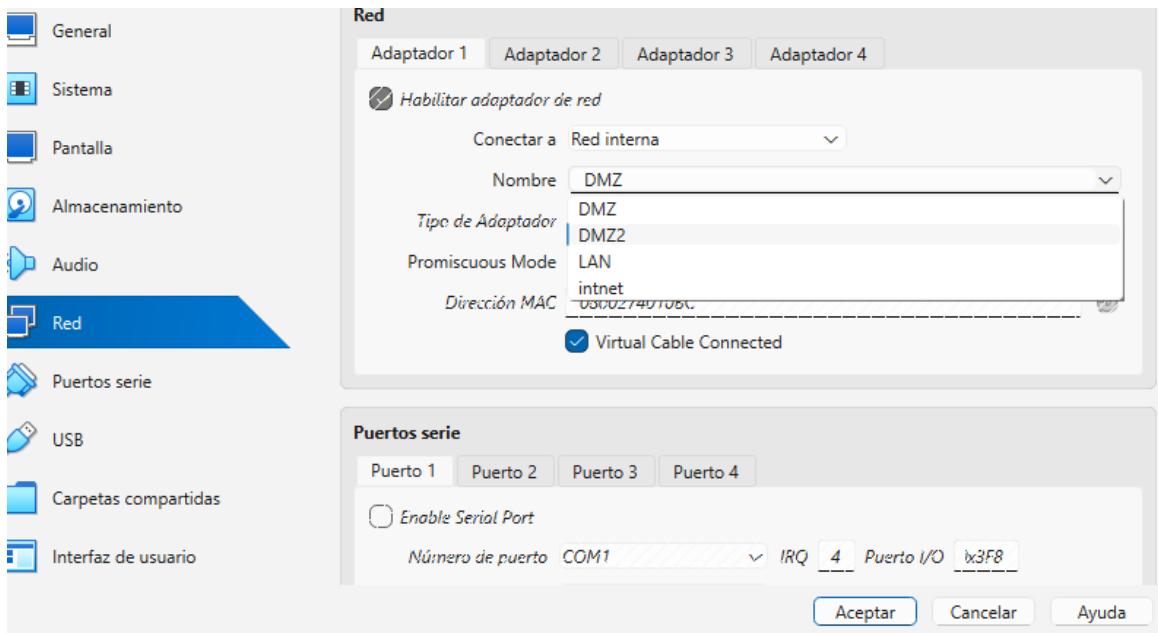
```
See https://ubuntu.com/esm or run: sudo pro status
```

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
admingabriel@Honeypot-DMZ:~$
```

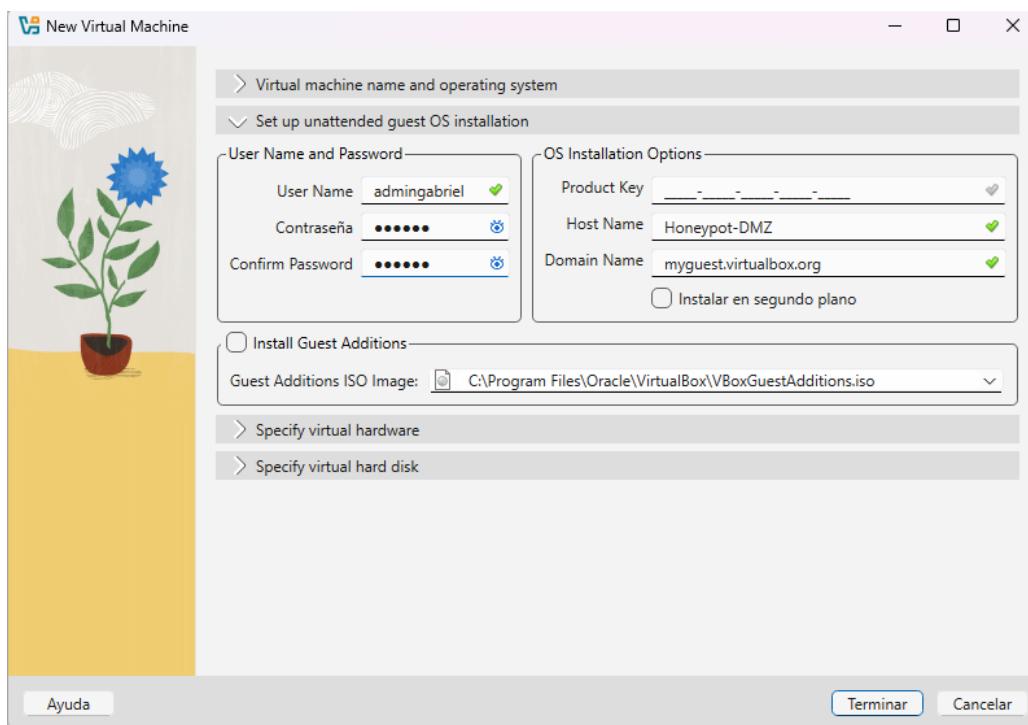
Para la instalacion del servidor ubuntu en el DMZ2 es el mismo procedimiento:

Crear máquina virtual con nombre "WebServer-DMZ2" y realizar el mismo procedimiento de **Honeypot (UBUNTU SERVER-DMZ) con la única diferencia que en la configuración de red es: DMZ2**



Además de crear otro nombre de usuario en esa maquina virtual con su respectiva contraseña

REFERENCIA



CONEXION SSH

Se procedera a realizar las conexion SSH falso en el Honeypot(DMZ) que sera mediante docker para que el atacante crea que ha ingresado por SSH y se pueda ver un registro de sus acciones.

Pasos:

1. En la terminal de la maquina instalada en el DMZ(Honeypot) escribimos:

- **sudo apt update**
- **sudo apt install docker.io -y**
- **sudo systemctl enable --now docker**

2. Verificar: docker –version

```
admingabriel@Honeypot-DMZ:~$ sudo docker --version
[sudo] password for admingabriel:
Docker version 28.2.2, build 28.2.2-0ubuntu1~24.04.1
admingabriel@Honeypot-DMZ:~$
```

Una vez instalado Docker correctamente en el servidor Honeypot ubicado en la DMZ, se procedió a desplegar un servicio SSH simulado utilizando la herramienta Cowrie, la cual actúa como un honeypot de tipo SSH.

Cowrie permite simular un servidor vulnerable, registrando intentos de acceso, credenciales utilizadas y comandos ejecutados, sin comprometer el sistema real.

Para ello se ejecutó el siguiente comando:

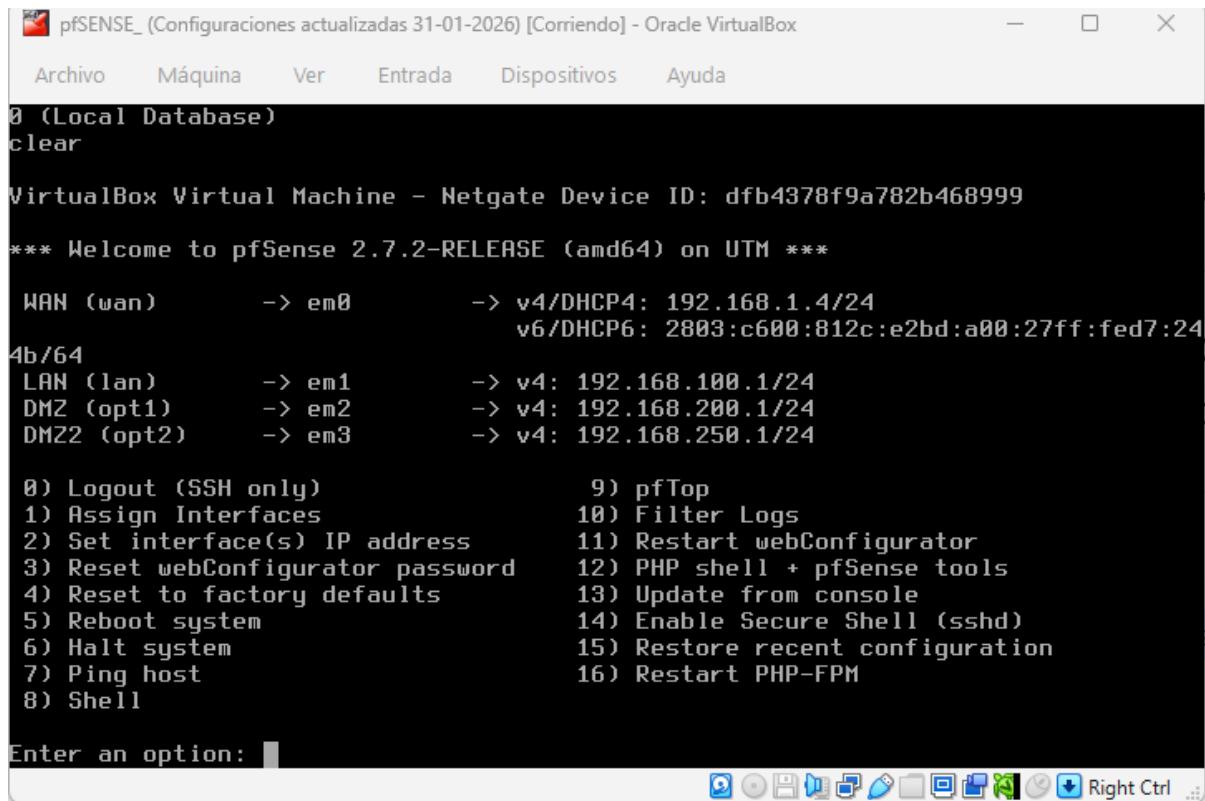
docker run -p 222:2222 cowrie/cowrie

```
admingabriel@Honeypot-DMZ:~$ sudo docker run -p 222:2222 cowrie/cowrie
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
2026-02-01T21:25:13+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2026-02-01T21:25:14+0000 [-] Python Version 3.11.2 (main, Apr 28 2025, 14:11:48) [GCC 12.2.0]
2026-02-01T21:25:14+0000 [-] Twisted Version 25.5.0
2026-02-01T21:25:14+0000 [-] Cowrie Version 2.9.9.dev9+g08b65ffa6
2026-02-01T21:25:14+0000 [-] Sensor UUID: 440efca0-fc58-11f0-849c-7aba4c68aaec
2026-02-01T21:25:14+0000 [-] Loaded output engine: jsonlog
2026-02-01T21:25:14+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2026-02-01T21:25:14+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2026-02-01T21:25:14+0000 [-] CowrieSSHFactory starting on 2222
2026-02-01T21:25:14+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7bb4fce9fd50>
2026-02-01T21:25:14+0000 [-] Ready to accept SSH connections
```

CONFIGURACIÓN DE RED Y SEGMENTACIÓN

Una vez instaladas las máquinas virtuales, se procedió a configurar la segmentación de red utilizando pfSense como firewall central. Se definieron las siguientes subredes:

- LAN: 192.168.100.1/24
- DMZ: 192.168.200.1/24
- DMZ2: 192.168.250.1/24



A screenshot of a pfSense terminal window within Oracle VirtualBox. The window title is "pfSENSE_ [Configuraciones actualizadas 31-01-2026] [Corriendo] - Oracle VirtualBox". The menu bar includes "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The main text area shows the pfSense configuration interface. It displays network interfaces: WAN (wan) connected to em0 with IP 192.168.1.4/24; LAN (lan) connected to em1 with IP 192.168.100.1/24; DMZ (opt1) connected to em2 with IP 192.168.200.1/24; and DMZ2 (opt2) connected to em3 with IP 192.168.250.1/24. Below the interfaces is a menu of 16 numbered options ranging from "Logout (SSH only)" to "Restart PHP-FPM". At the bottom, it says "Enter an option:" followed by a text input field and a toolbar with various icons.

```
0 (Local Database)
clear

VirtualBox Virtual Machine - Netgate Device ID: dfb4378f9a782b468999

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.4/24
                           v6/DHCP6: 2803:c600:812c:e2bd:a00:27ff:fed7:24
4b/64
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)      -> em2      -> v4: 192.168.200.1/24
DMZ2 (opt2)     -> em3      -> v4: 192.168.250.1/24

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: 
```

Cada segmento cumple una función específica dentro de la arquitectura, permitiendo separar los sistemas internos de los sistemas expuestos y de monitorización.

pfSense actúa como punto de control entre todas las redes, asegurando que ningún tráfico pueda circular entre segmentos sin reglas explícitas.

CONFIGURACIÓN DE REGLAS DE FIREWALL

Con el objetivo de aislar el honeypot y evitar accesos no autorizados hacia la red interna, se implementaron reglas de firewall en la interfaz DMZ de pfSense.

Las reglas creadas fueron las siguientes:

- Bloqueo de tráfico ICMP desde DMZ hacia LAN
- Bloqueo de tráfico ICMP desde DMZ hacia DMZ2
- Bloqueo de tráfico TCP desde DMZ hacia LAN
- Bloqueo de tráfico TCP desde DMZ hacia DMZ2

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/252 B any	IPv4 ICMP	DMZ subnets	*	LAN subnets	*	*	none		BLOQUEAR ICMP DMZ hacia LAN	
0/504 B any	IPv4 ICMP	DMZ subnets	*	DMZ2 subnets	*	*	none		BLOQUEAR ICMP DMZ hacia DMZ2	
0/0 B	IPv4 TCP	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloquear DMZ hacia DMZ2	
0/0 B	IPv4 TCP	DMZ subnets	*	LAN subnets	*	*	none		Bloquear DMZ hacia LAN	
1/19 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla DNS	
0/1.80 MiB	IPv4 TCP	*	*	*	Webs	*	none		Regla Trafico Web	

Estas reglas impiden que el honeypot pueda comunicarse con la red interna o con el sistema de monitorización, evitando que un posible compromiso afecte otros segmentos de la infraestructura.

Adicionalmente, se mantuvieron permisos mínimos necesarios para el correcto funcionamiento del sistema, como resolución DNS y tráfico web cuando fue requerido.

El orden de las reglas fue cuidadosamente definido, ya que pfSense evalúa las reglas de arriba hacia abajo, aplicando la primera coincidencia encontrada.

PRUEBAS DE CONECTIVIDAD Y FUNCIONAMIENTO

Para verificar el correcto funcionamiento de la segmentación, se realizaron pruebas de conectividad desde el servidor Honeypot.

Se intentó realizar comunicación mediante ping hacia direcciones IP pertenecientes a la red LAN y DMZ2, obteniendo como resultado la pérdida total de paquetes, lo cual confirma que las reglas de bloqueo están funcionando correctamente.

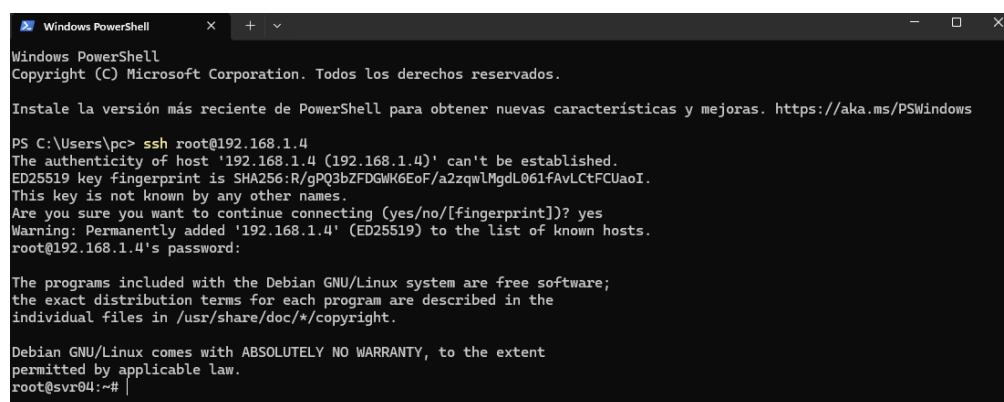
DMZ2

```
admingabriel@Honeypot-DMZ:~$ ping 192.168.250.104
PING 192.168.250.104 (192.168.250.104) 56(84) bytes of data.
^C
--- 192.168.250.104 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4132ms
admingabriel@Honeypot-DMZ:~$ _
```

LAN

```
admingabriel@Honeypot-DMZ:~$ ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
^C
--- 192.168.100.100 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5142ms
admingabriel@Honeypot-DMZ:~$ _
```

Asimismo, se verificó que el acceso al honeypot desde la red LAN y desde DMZ2 se encuentra bloqueado, mientras que el acceso externo mediante SSH simulado se mantiene operativo.



The screenshot shows a Windows PowerShell window with the title bar "Windows PowerShell". The content of the window is as follows:

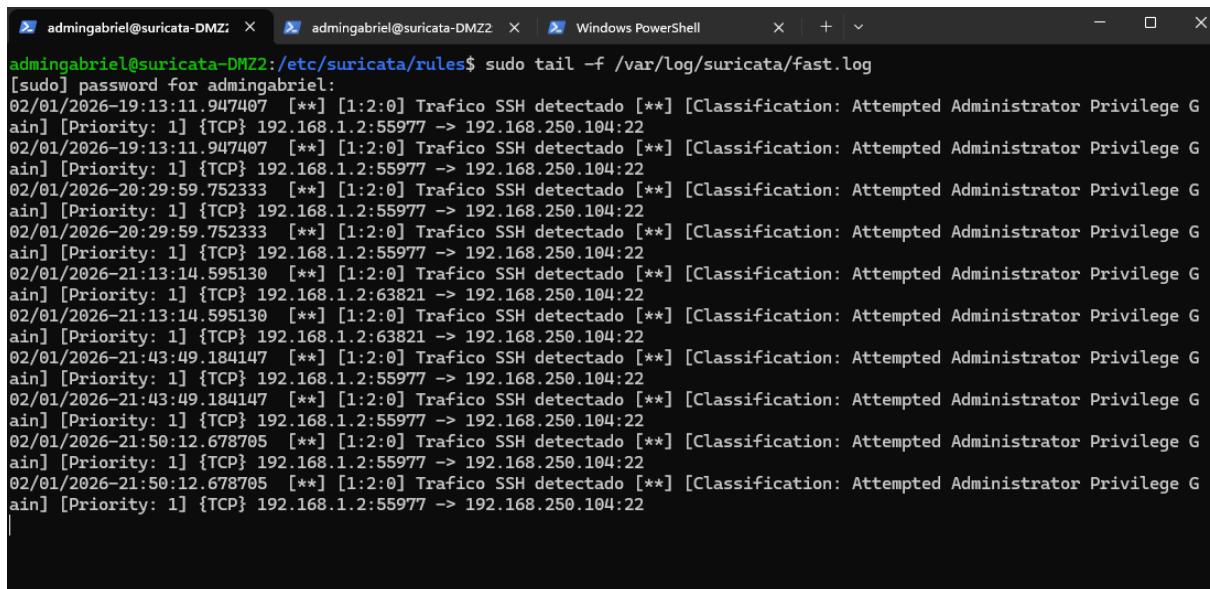
```
PS C:\Users\pc> ssh root@192.168.1.4
The authenticity of host '192.168.1.4' (192.168.1.4) can't be established.
ED25519 key fingerprint is SHA256:R/gPQ3bZFDGWk6EeF/a2zqwUMgdl061fAvLctFCUaoI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.4' (ED25519) to the list of known hosts.
root@192.168.1.4's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# |
```

SISTEMA DE MONITORIZACIÓN (SURICATA)

En la red DMZ2 se desplegó un servidor Ubuntu Server destinado a la monitorización de seguridad mediante la herramienta Suricata, la cual actúa como un sistema de detección de intrusiones (IDS).



The screenshot shows a terminal window with three tabs: 'admingabriel@suricata-DMZ2' (active), 'admingabriel@suricata-DMZ2' (background), and 'Windows PowerShell'. The active tab displays the command 'sudo tail -f /var/log/suricata/fast.log' and its output. The output is a log of network traffic events, mostly SSH attempts from 192.168.1.2 to 192.168.250.104:22, categorized as 'Attempted Administrator Privilege Gain' with priority 1. The log entries are timestamped from 02/01/2026 at various times between 13:11 and 21:50.

```
admingabriel@suricata-DMZ2:/etc/suricata/rules$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for admingabriel:
02/01/2026-19:13:11.947407 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-19:13:11.947407 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-20:29:59.752333 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-20:29:59.752333 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-20:29:59.752333 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-21:13:14.595130 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:63821 -> 192.168.250.104:22
02/01/2026-21:13:14.595130 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:63821 -> 192.168.250.104:22
02/01/2026-21:43:49.184147 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-21:43:49.184147 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-21:50:12.678705 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
02/01/2026-21:50:12.678705 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:55977 -> 192.168.250.104:22
```

Suricata permite analizar el tráfico de red y generar registros ante eventos sospechosos, aportando una capa adicional de seguridad y visibilidad sobre la infraestructura.

El servicio fue instalado y ejecutado correctamente, verificando su funcionamiento mediante el estado del servicio y la generación de archivos de log en el sistema.