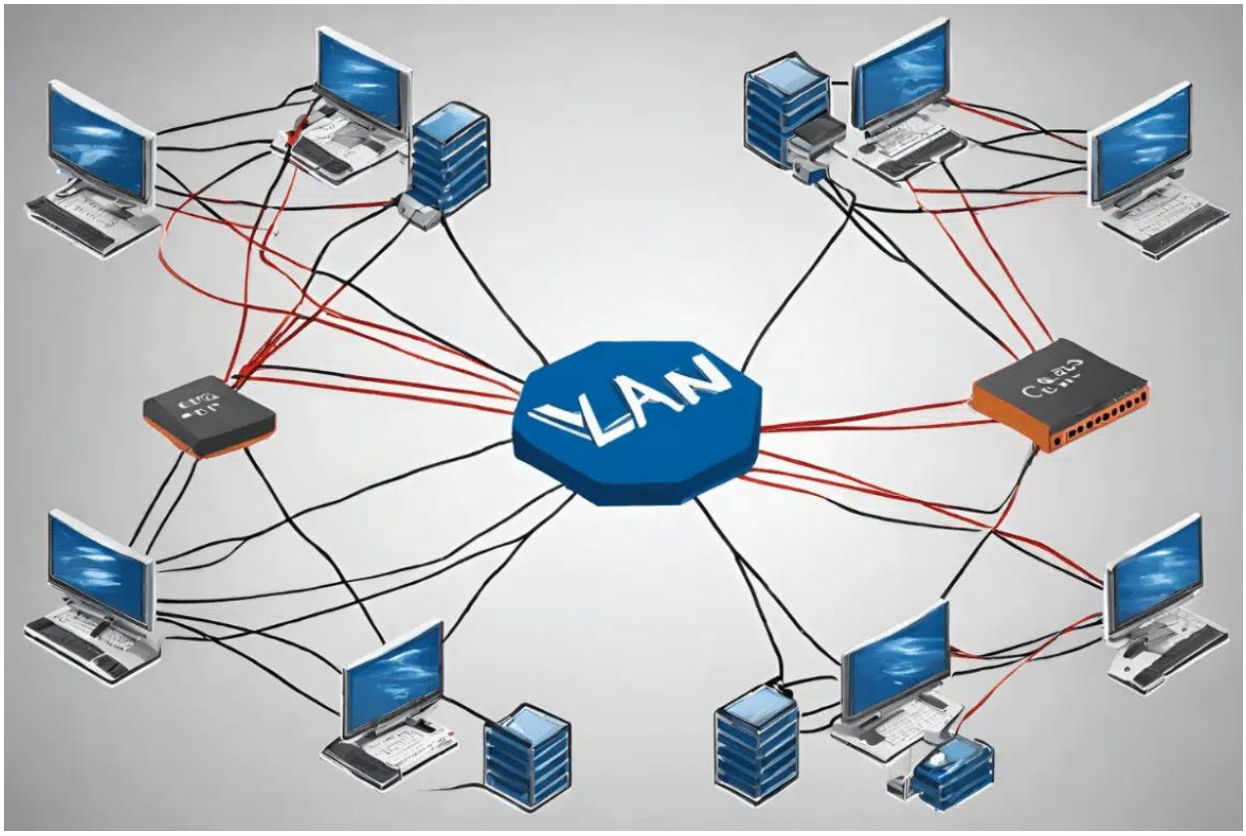
INFORME DE SEGMENTACION DE REDES



Nombre: Brayan Gabriel Gutierrez Rebolledo

Modulo: Blue Team

Profesor: Sergio Vilches

Fecha: 02/02/2025

INDICE

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

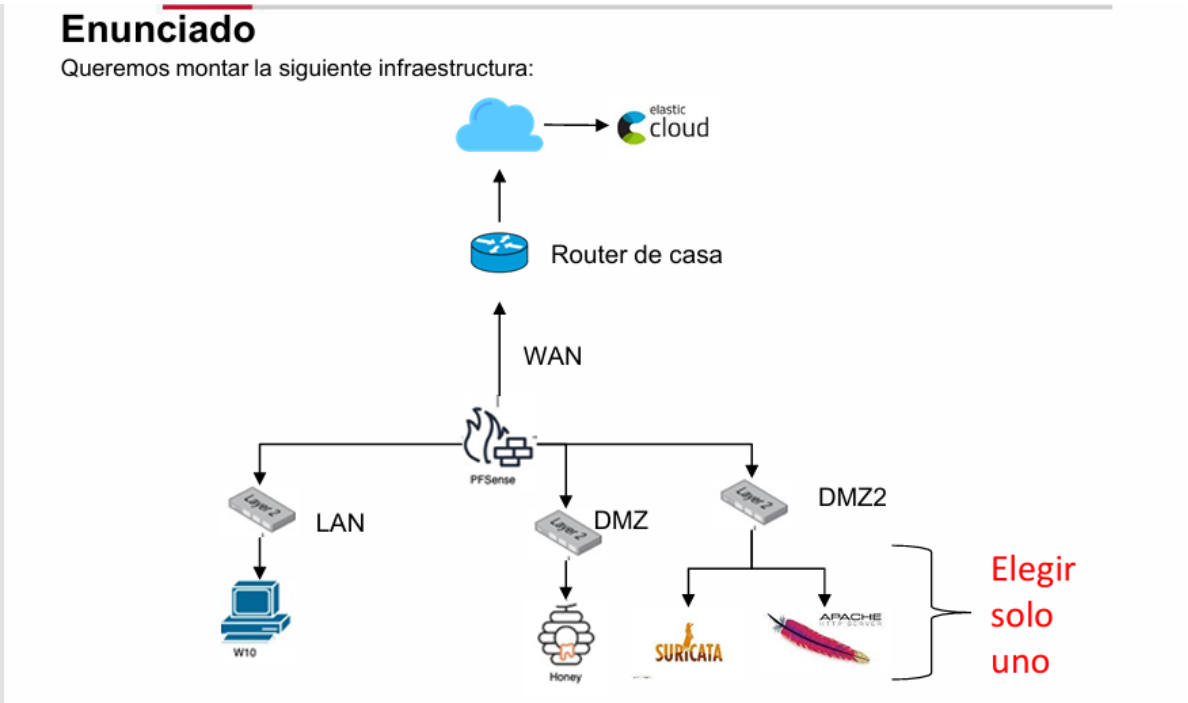
https://www.youtube.com/watch?v=-vndaBqCqX8

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



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.

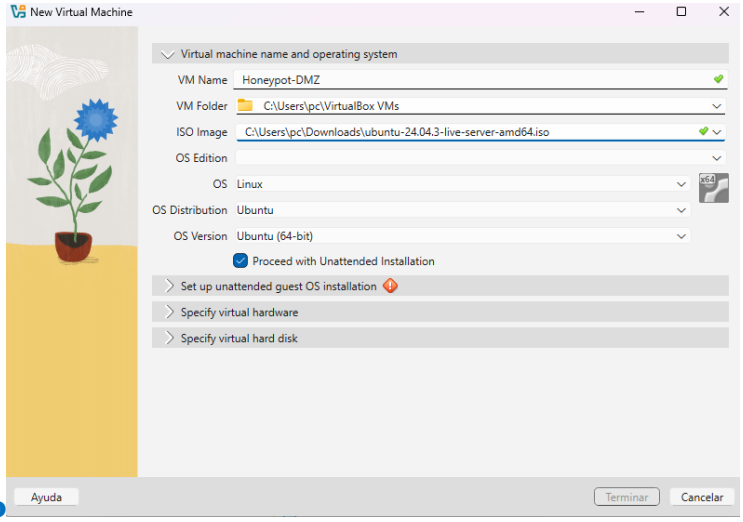
PROCEDIMIENTO

INSTALACION DE VMS

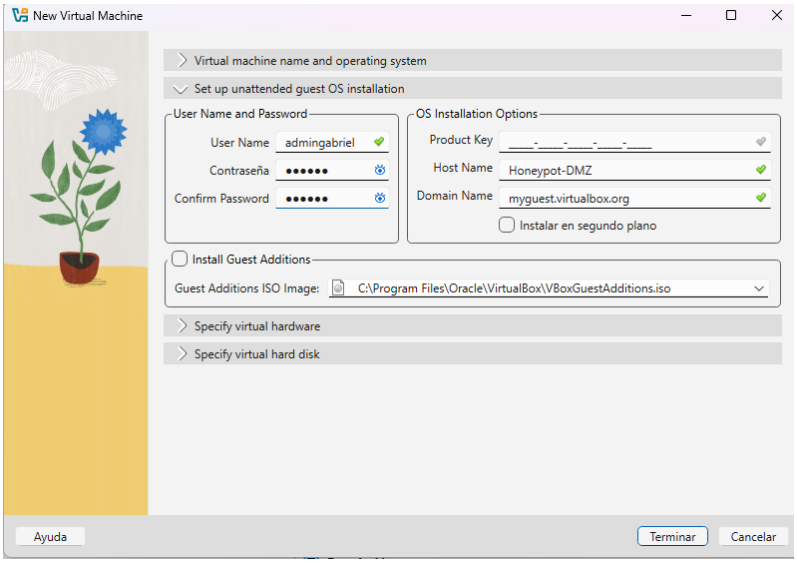
Primero se procederá a la instalación de las máquinas virtuales correspondientes a **DMZ y DMZ2**

Honeypot (UBUNTU SERVER-DMZ)

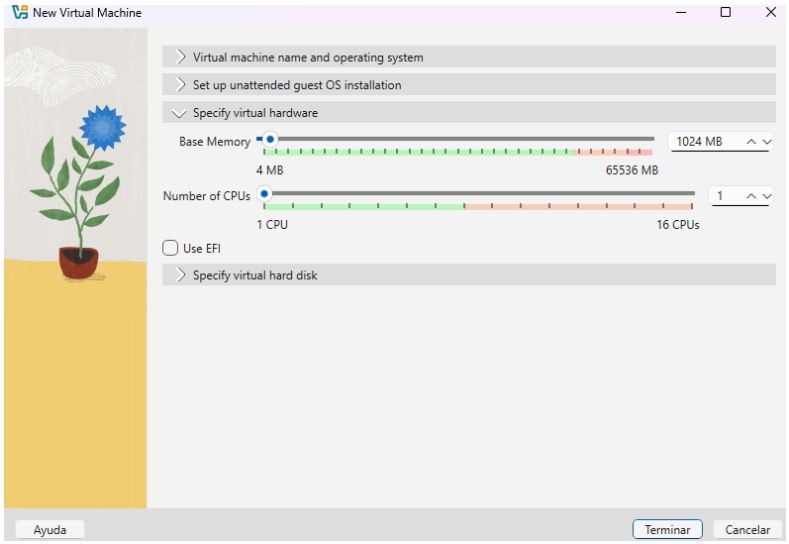
1. **Creamos una nueva maquina en virtual box llamada "Honeypot-DMZ"**
2. **Cargamos el "archivo.iso" que en este caso es: ubuntu-24.04.3-live-server-amd64.iso**



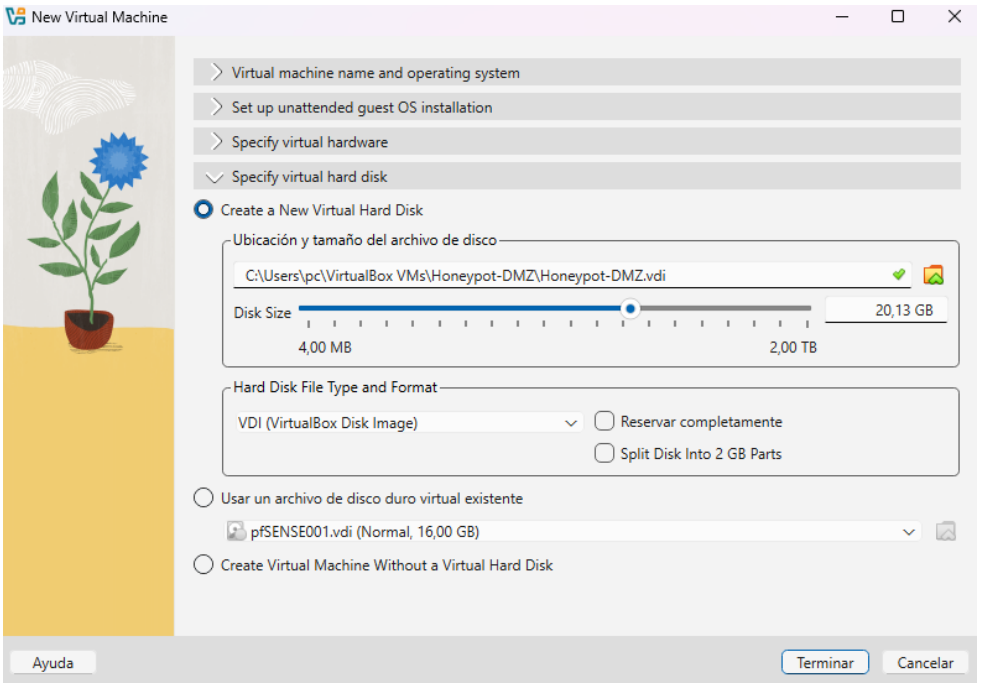
3. **En "User Name" colocamos a preferencia nuestra el nombre, en este caso: "admingabriel" y contraseña tambien eleccion personal**



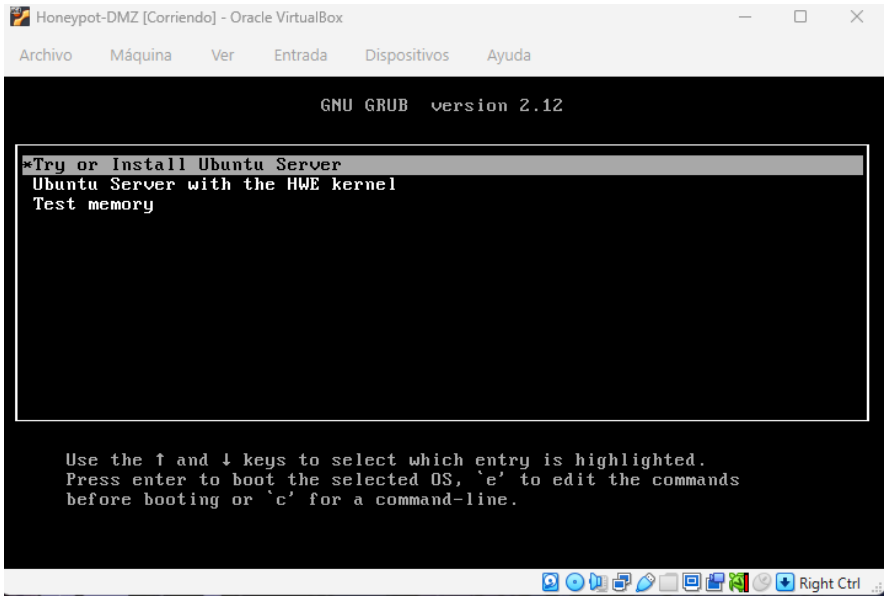
4. **En el apartado de Specify virtual Hardware se colocó minimo 1024 MB que equivale a 1 GB en memoria RAM y en Number of CPUs se mantuvo en 1**

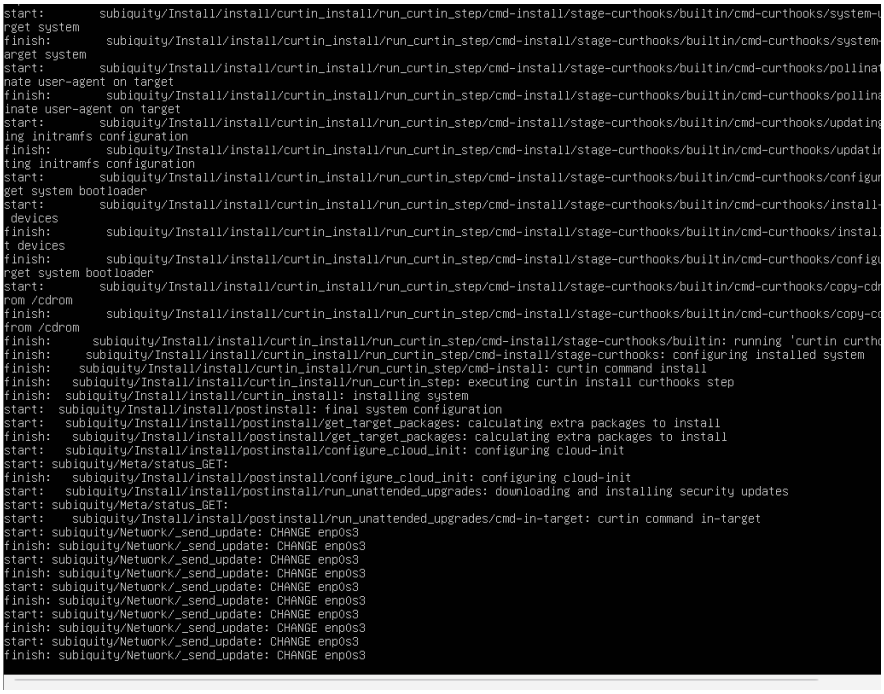


5. **Se escogió 20 GB en disco para que no existan problemas de almacenamiento**

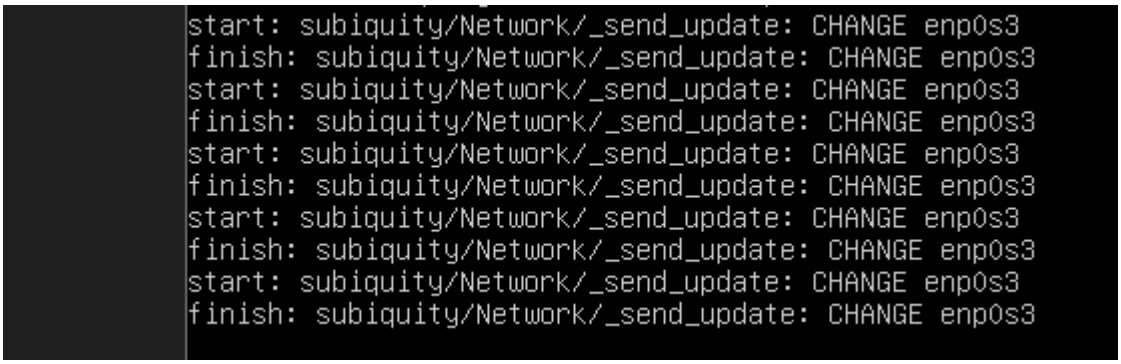


6. **Seleccionar Try or Install Ubuntu Server y esperar a que cargue la instalacion.**

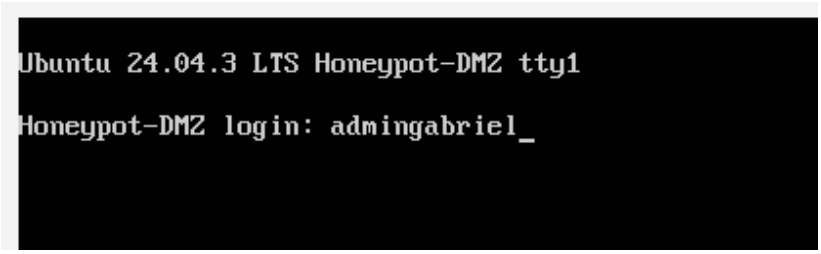




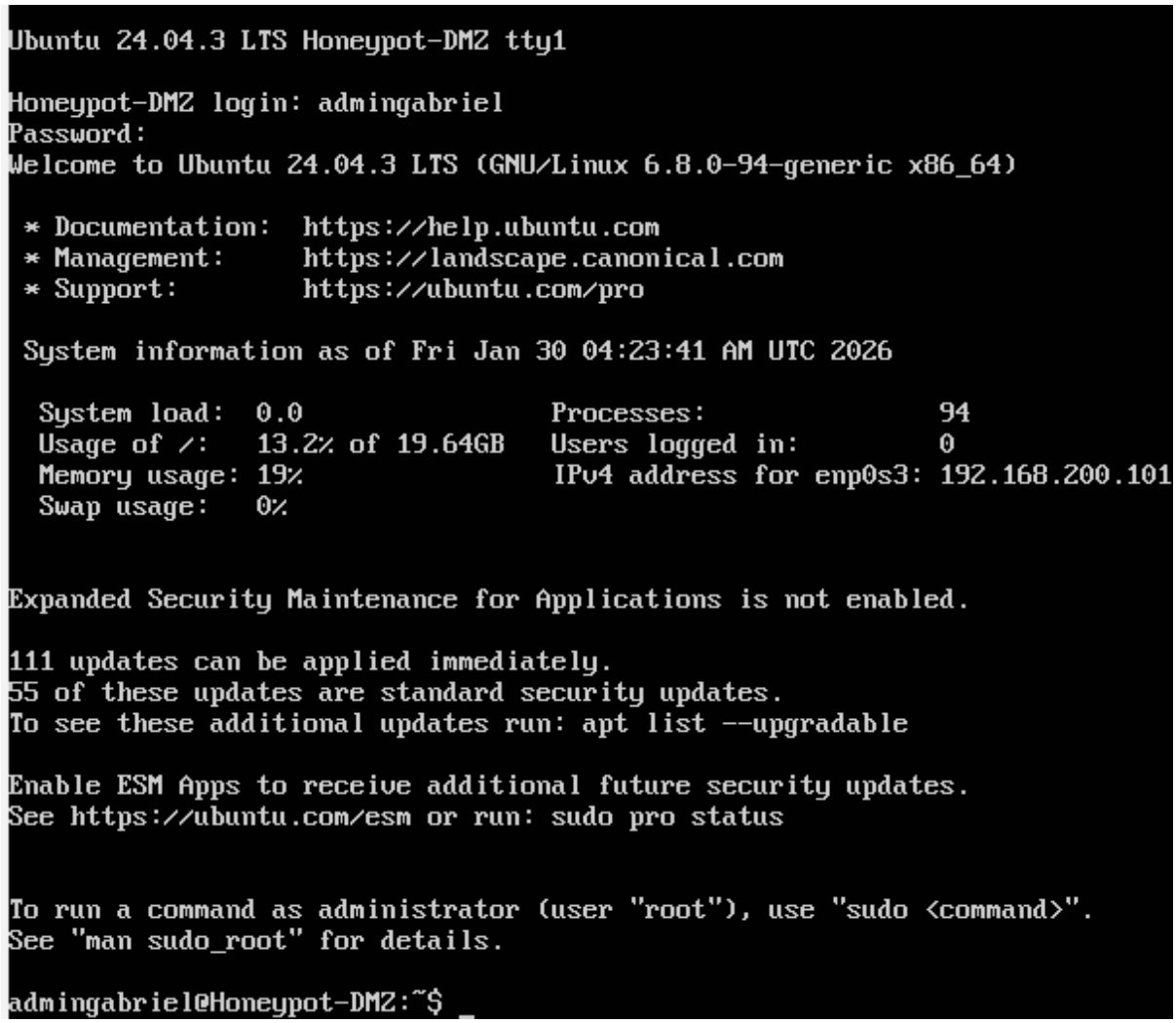
Cerrar cuando diga:



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

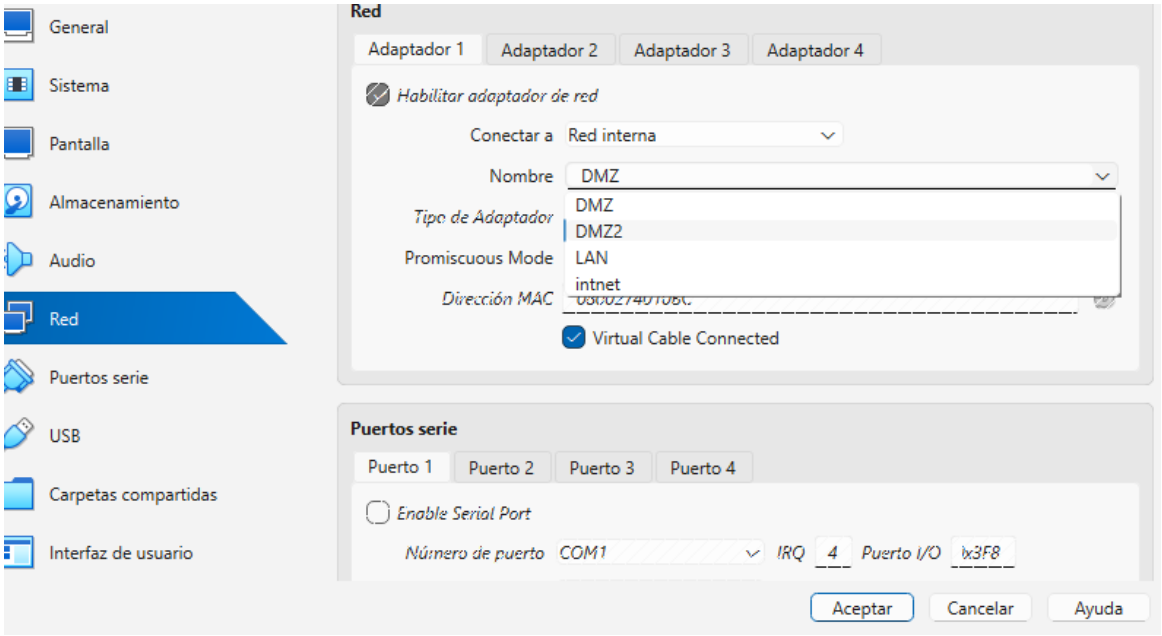


8. **Obteniendo correctamente iniciar sesión en el servidor de Ubuntu**



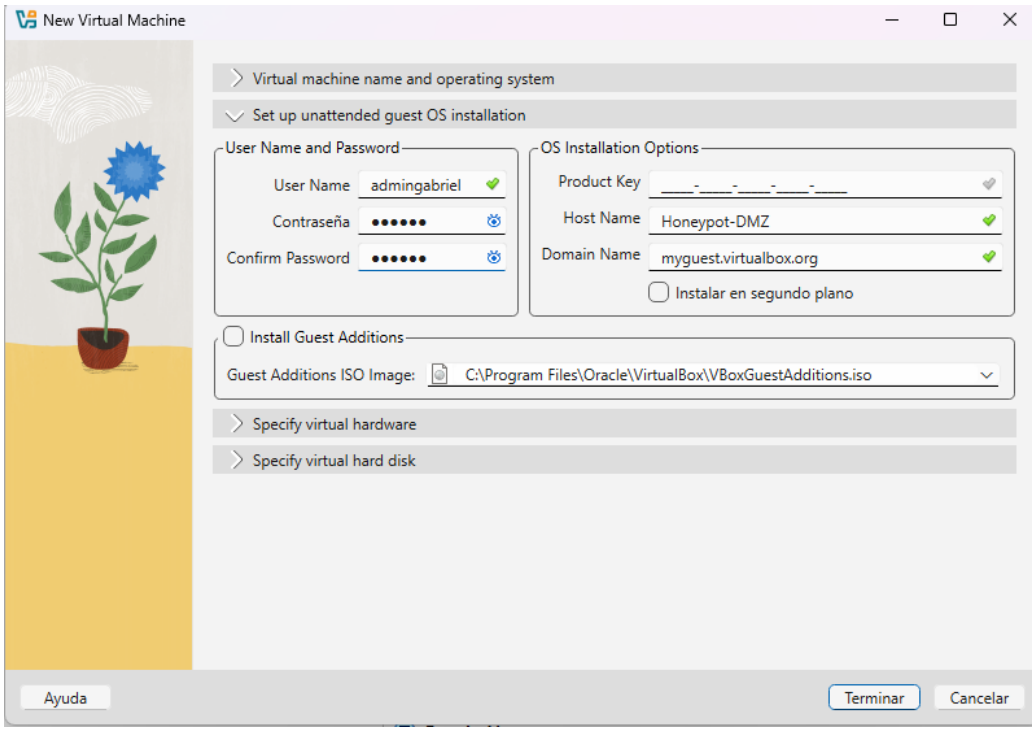
Para la instalacion del servidor ubuntu en el DMZ2 es el mismo procedimiento:

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**

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

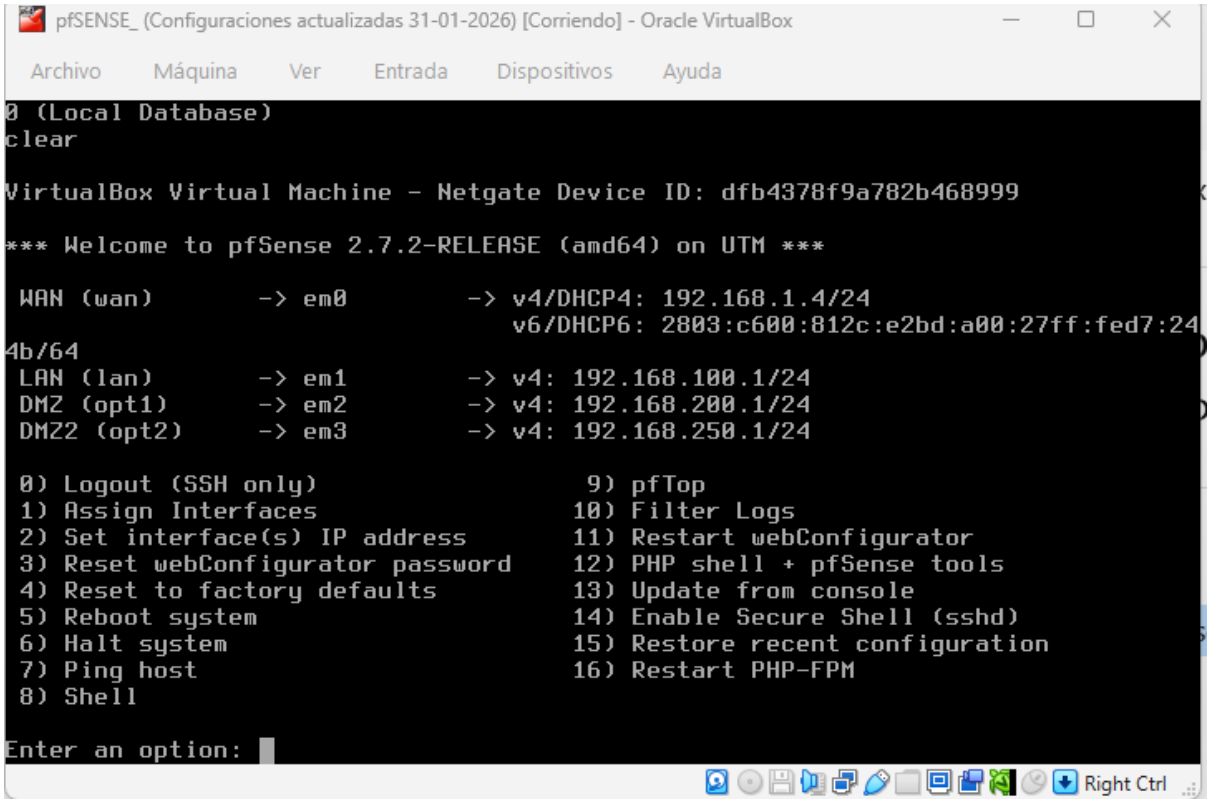
Para ello se ejecutó el siguiente comando:

docker run -p 222:2222 cowrie/cowrie

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



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

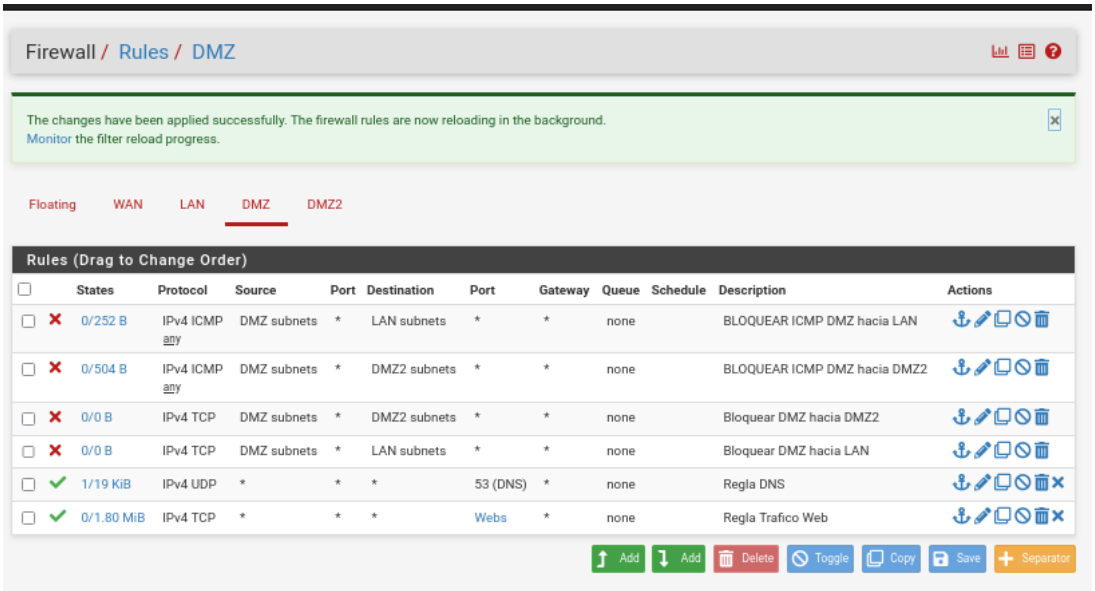
pfSense actúa como punto de control entre todas las redes, asegurando que ningún tráfico pueda circular entre segmentos sin reglas explícitas.

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



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.

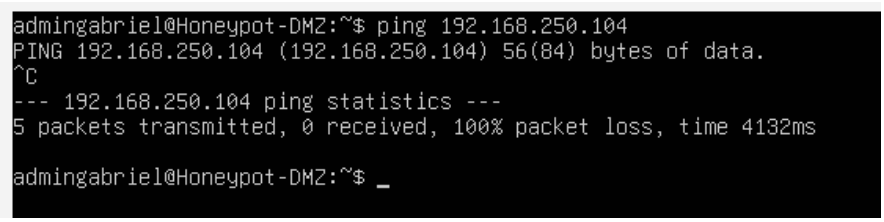
El orden de las reglas fue cuidadosamente definido, ya que pfSense evalúa las reglas de arriba hacia abajo, aplicando la primera coincidencia encontrada.

PRUEBAS DE CONECTIVIDAD Y FUNCIONAMIENTO

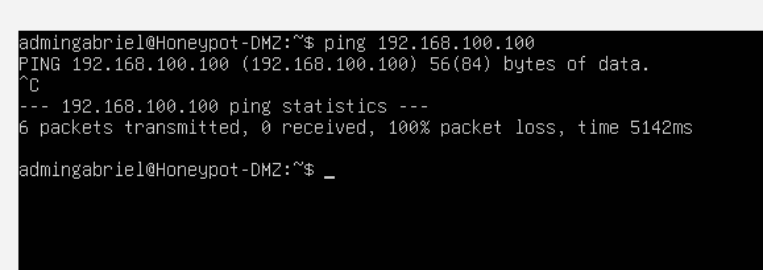
Para verificar el correcto funcionamiento de la segmentación, se realizaron pruebas de conectividad desde el servidor Honeypot.

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.

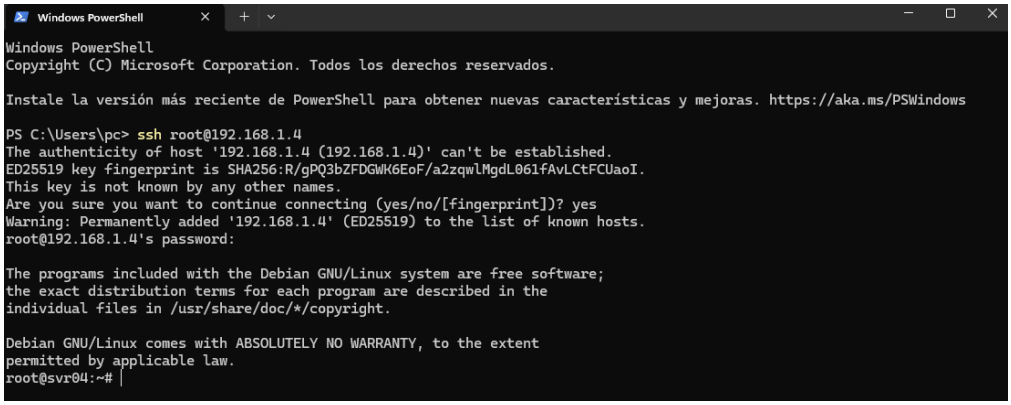
DMZ2



LAN

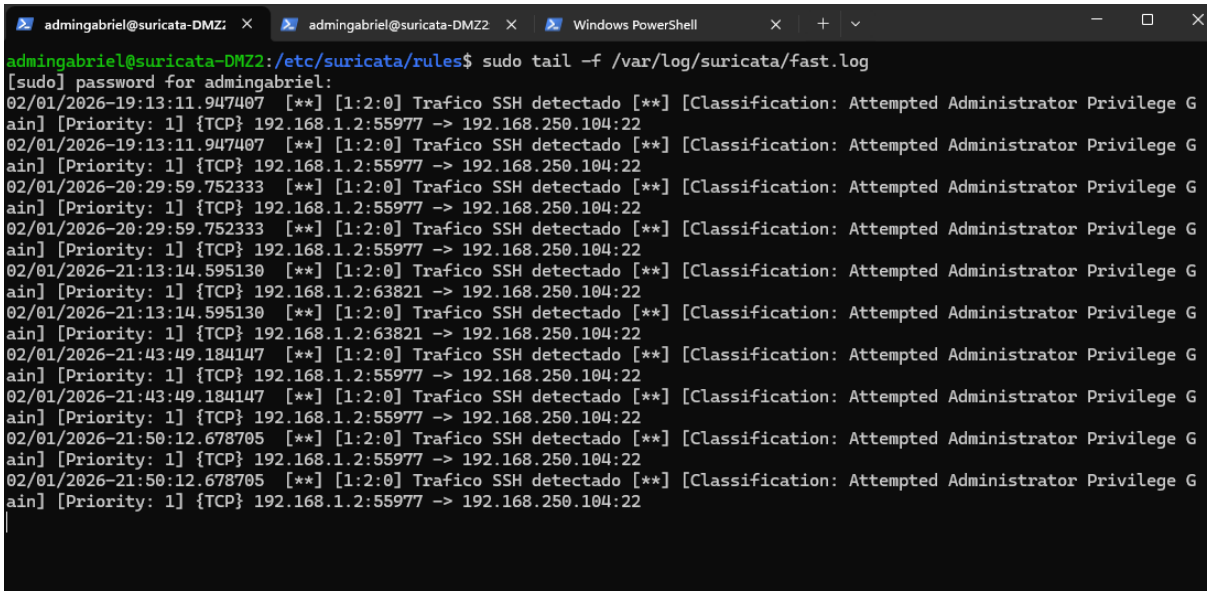


Asimismo, se verificó que el acceso al honeypot desde la red LAN y desde DMZ2 se encuentra bloqueado, mientras que el acceso externo mediante SSH simulado se mantiene operativo.



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).



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.