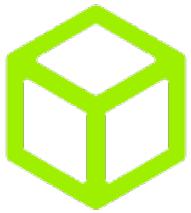
Laboratorio para pentesting con Docker

Introducción

Se pretende desarrollar la infraestructura para desplegar, de una forma sencilla y rápida, entornos controlados para pruebas de ciberseguridad.

https://www.hackthebox.com/

https://tryhackme.com/



Objetivos

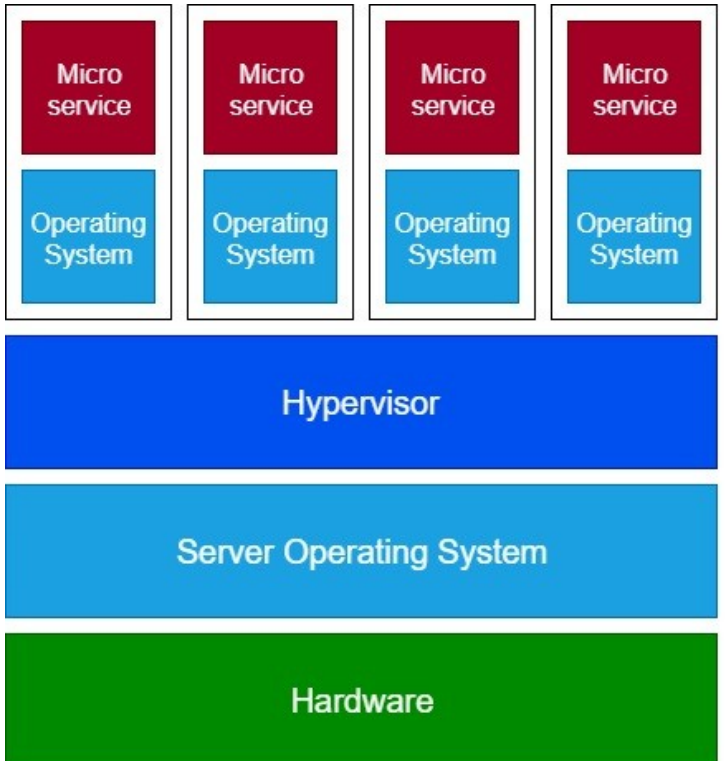
- Desplegar una máquina vulnerable a petición del usuario y una VPN para que este pueda conectarse.
- Tanto la máquina vulnerable como la VPN se tienen que crear cuando el usuario lo solicite y de la misma forma se deben eliminar.
- Si hay distintos usuarios y distintas máquinas cada usuario debe de estar aislado en su red.

¿Qué es una VPN?

Una red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

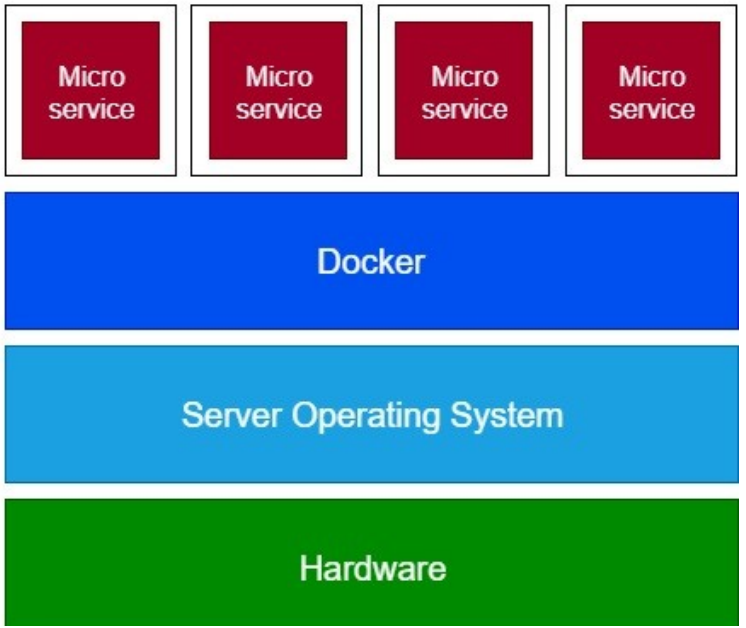
¿Qué es la virtualización?

Uso del software para imitar las características del hardware y crear un sistema informático virtual.



¿Qué es la contenerización?

Método de virtualización para implementar y ejecutar aplicaciones distribuidas sin lanzar una máquina virtual completa para cada aplicación.



Despliegue de contenedores

Usuarios:

- pepe
- pato
- fmol

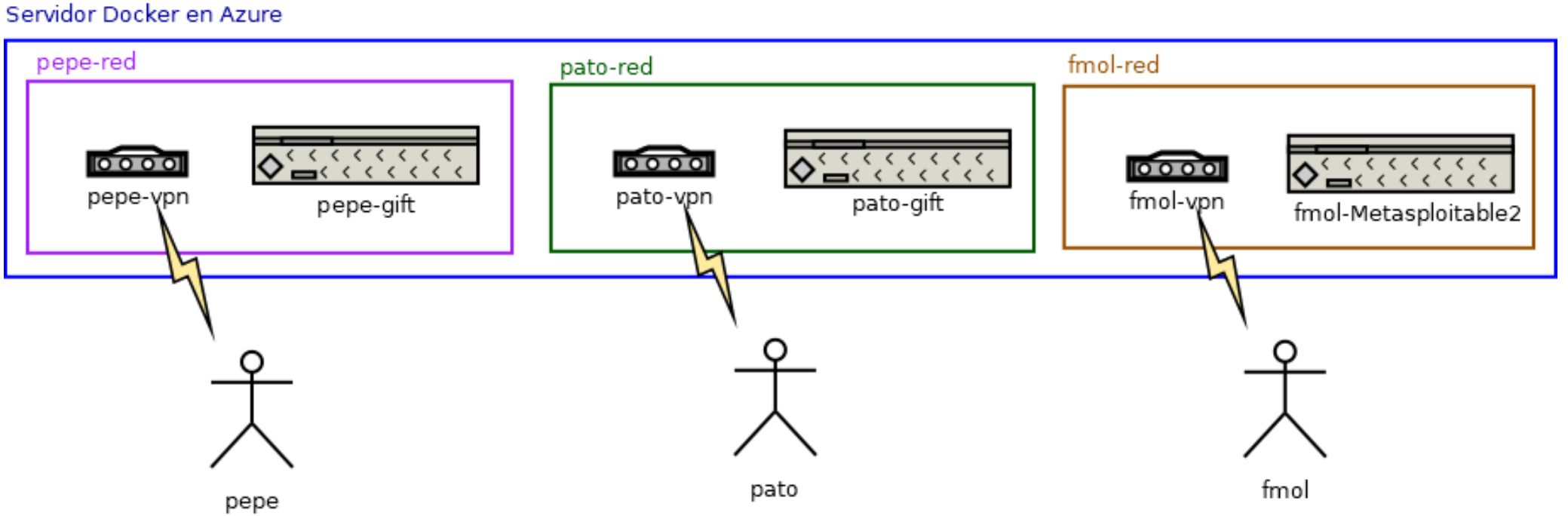
Maquinas:

- Metasploitable2
- Gift

Maquinas encendidas:

- Gift → pepe, pato
- Metasploitable2 → fmol

Despliegue de contenedores



Instalación del servidor Docker

```
apt update
apt install docker.io docker-compose -y
usermod -aG docker $(whoami)
```

Crear una red en Docker

```
docker network create mi-red
```

```
docker network rm mi-red
```

Despliegue de una VPN

```
docker run -d \
 --network=mi-red \
 --name=mi-VPN \
 --cap-add=NET_ADMIN \
 --cap-add=SYS_MODULE \
 -e PUID=1000 \
 -e PGID=1000 \
 -e TZ=Europe/Madrid \
 -e SERVERURL=52.142.216.158 \
 -e SERVERPORT=51820 \
 -e PEERS=1 \
 -e PEERDNS=auto \
 -e INTERNAL_SUBNET=10.10.10.0 \
 -p 51820:51820/udp \
 -v /wireguard/mi-VPN:/config \
 -v /lib/modules:/lib/modules \
 -v /usr/src:/usr/src \
 --sysctl="net.ipv4.conf.all.src_valid_mark=1" \
 --restart unless-stopped \
 linuxserver/wireguard
```

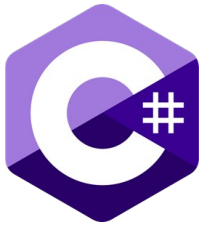
Despliegue de una maquina

```
docker run --rm -dit \
  --name metasploitable2 \
  --network=mi-red \
  tleemcjr/metasploitable2:latest
```

Eliminación de un contenedor

```
docker stop id-contenedor
docker rm id-contenedor
```

Automatización



https://github.com/FMOL107/PentestLabCSharpDocker

Creando una imagen personalizada

https://hub.docker.com/r/fmol107/gift

Entorno gráfico y conexión por RDP

https://hub.docker.com/r/fmol107/debian-rdp

https://hub.docker.com/r/fmol107/kali-rdp

Laboratorio para pentesting con Docker