Firsthacking

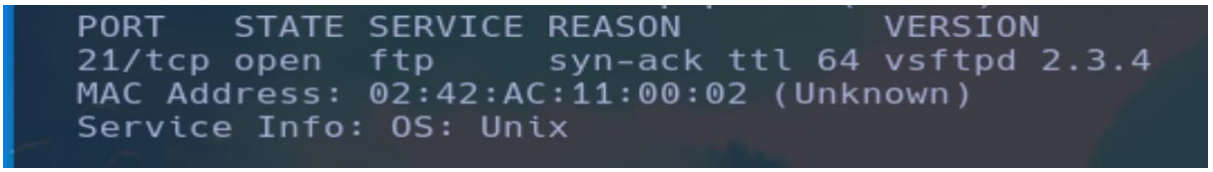
Una vez desplegada la maquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

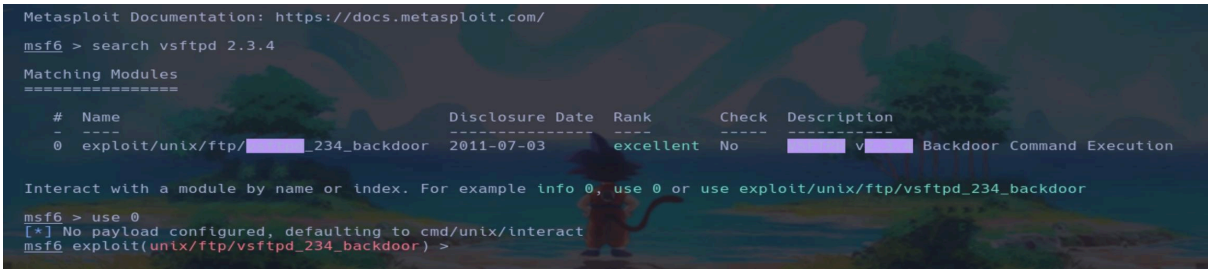
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- **-p-**: Escanea todos los puertos .
- **-sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- **-sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- **-sV**: Detecta las versiones de los servicios en ejecución.
- **--min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- **-n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- **-vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- **-Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

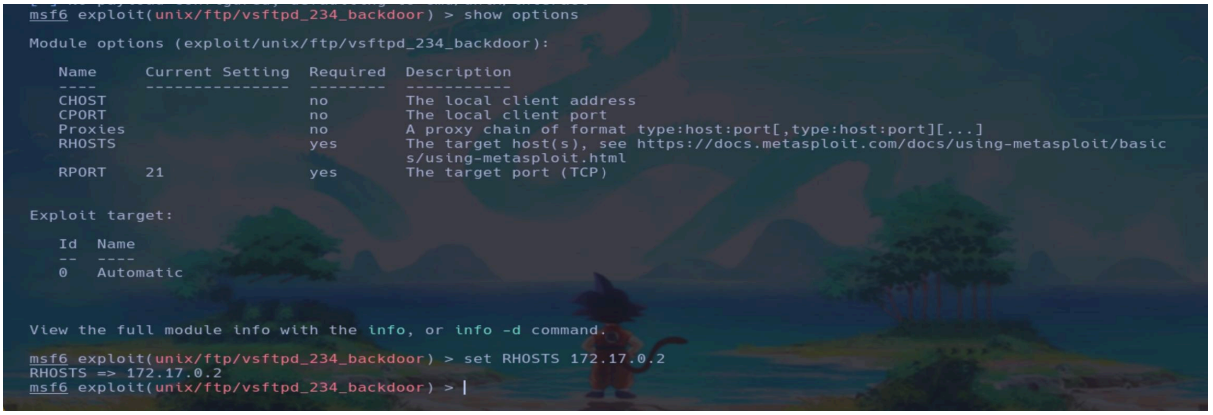
una vez realizado el escaneo vemos que tenemos un puerto puerto abierto



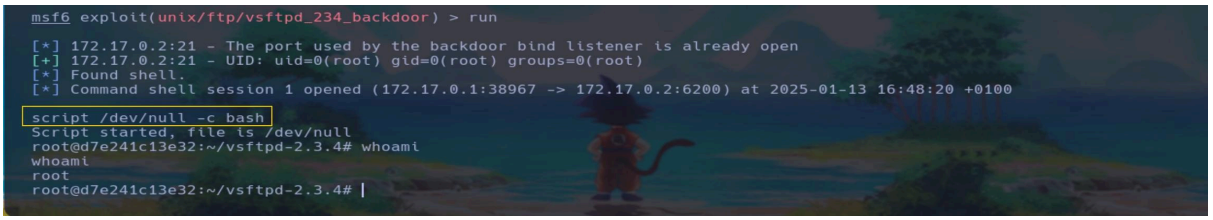
Es el puerto 21, como no tenemos ninguna información buscamos en metasploit para ver si es vulnerable por lo que abrimos metasploit con: msfconsole y buscamos alguna vulnerabilidad de vsftpd 2.3.4 con: search vsftpd 2.3.4



Vemos que si existen una vulnerabilidad por lo que utilizaremos la opción 0 que es la única que hay. Luego veremos las opciones que nos muestra con el comando : show options y vemos que solo nos pide la ip de la maquina victima que se la facilitaremos con set RHOSTS 172.17.0.2



Ponemos run para ejecutarlo.



Y ya estaríamos dentro, yo lo que hago por comodidad es introducir el comando:

script /dev/null -c bash

Para que sea mejor estéticamente.