breakmyssh

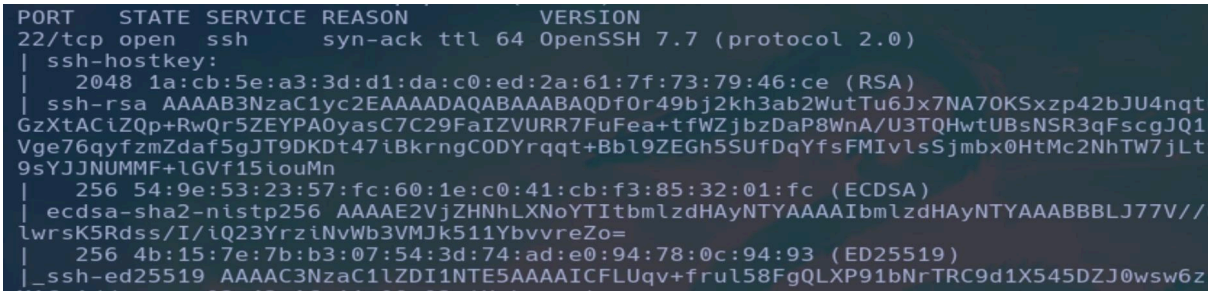
Una vez desplegada la maquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

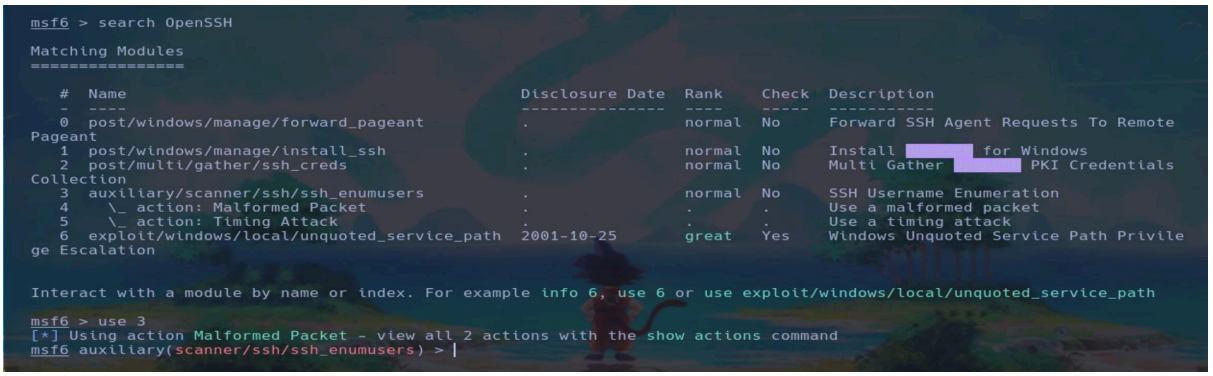
```
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)
```

- **-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

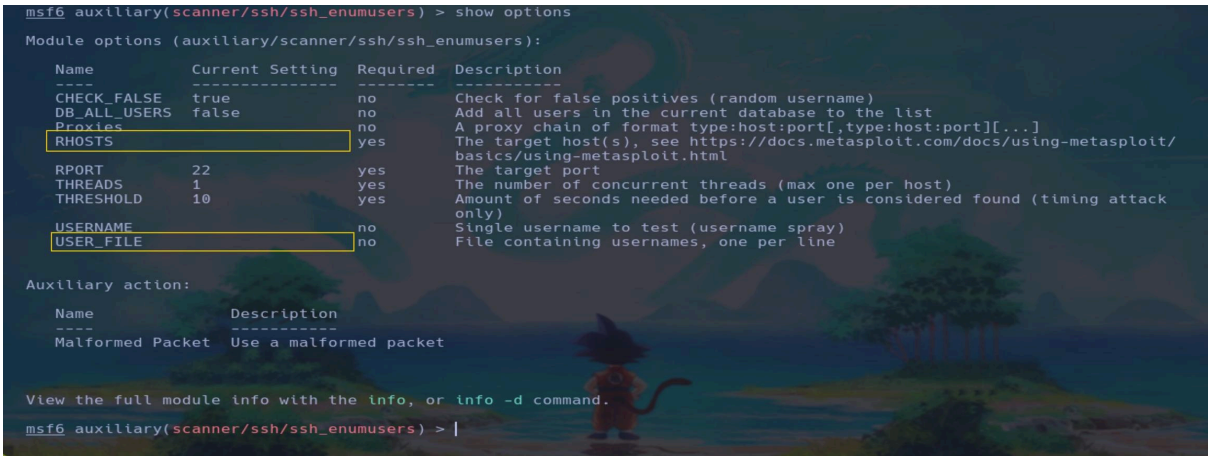


Como la versión es 7.7 sabemos que es vulnerable por ello entramos en metasploit y buscamos alguno vulnerabilidad de OpenSSH



Usamos la opción 3 que consiste en enumerar los usuarios para después realizar un ataque de fuerza bruta con hydra.

Ponemos el comando `show options` para ver las opciones que tenemos que modificar



En RHOSTS introducimos la ip de la maquina victima y en USER_FILE introducimos el diccionario a utilizar de esta manera:

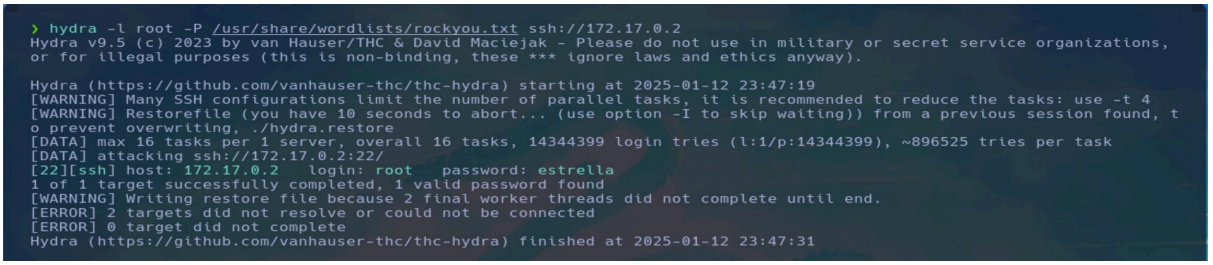
```
set RHOSTS 172.17.0.2
```

```
set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
```

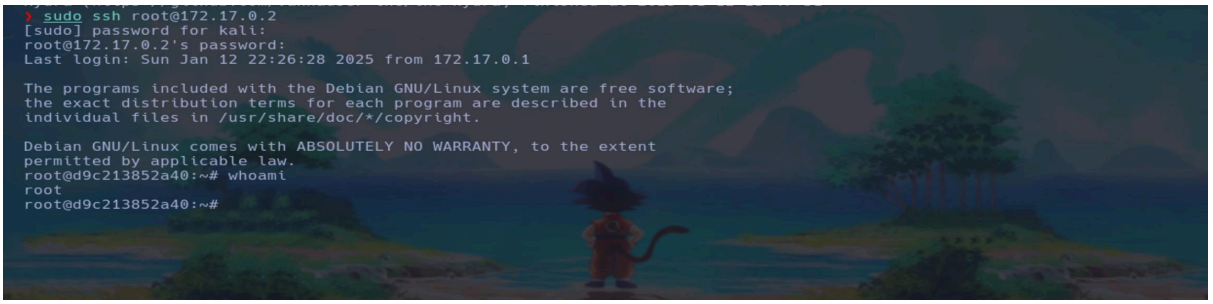
Para finalizar iniciamos el ataque con `run`

Vemos que el usuario root está dentro de la lista por lo que aplicaremos un ataque de fuerza bruta con hydra con el siguiente comando:

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```



Ya tenemos el ususario y la contraseña , lo único que nos hace falta es conectarlo con ssh : `sudo ssh root@172.17.0.2`



Y ya somos usuario root.