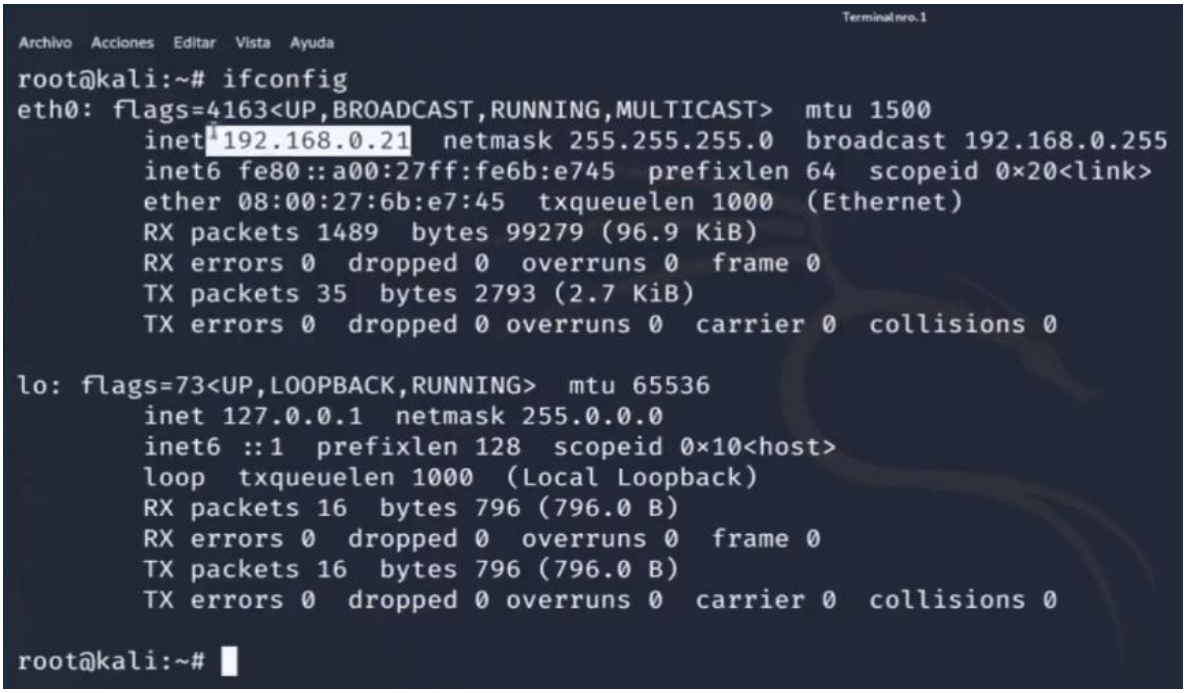
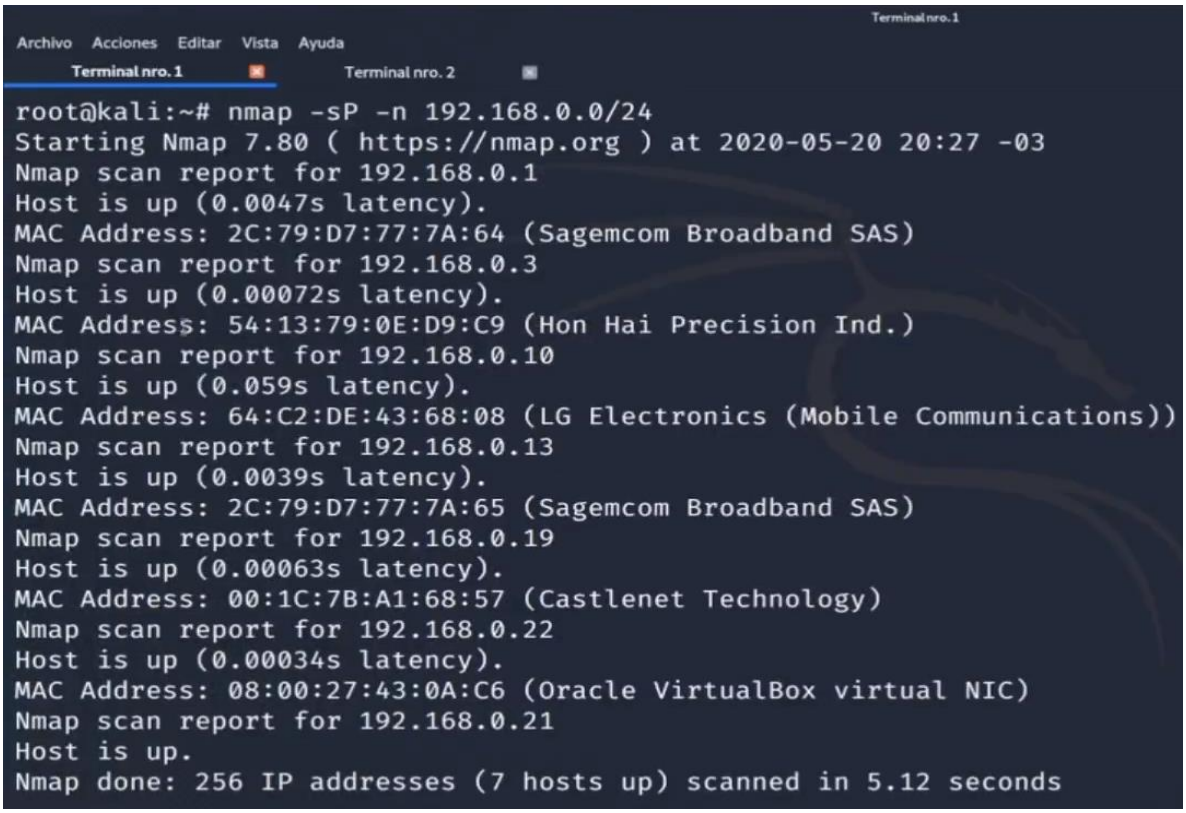
CAPTURE THE FLAG (CTF)

Ifconfig, obtenemos informacion de nuestra red. Verificamos nuestra dirección ip

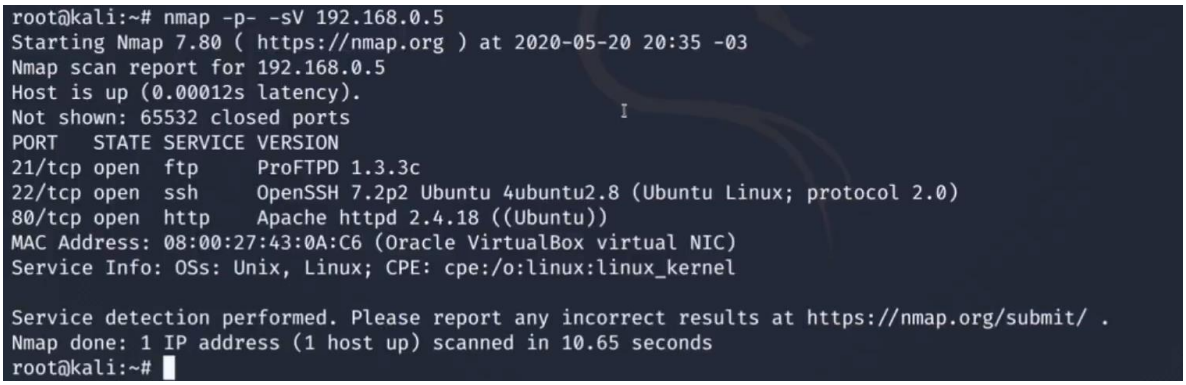



nmap sP -n 192.168.0.0/24, barrido escaneo de ping, con menos (-n) evitamos la resolución de nombres. Y revisamos toda la red. Nos permite hacer un barrido de puertos y servicios.



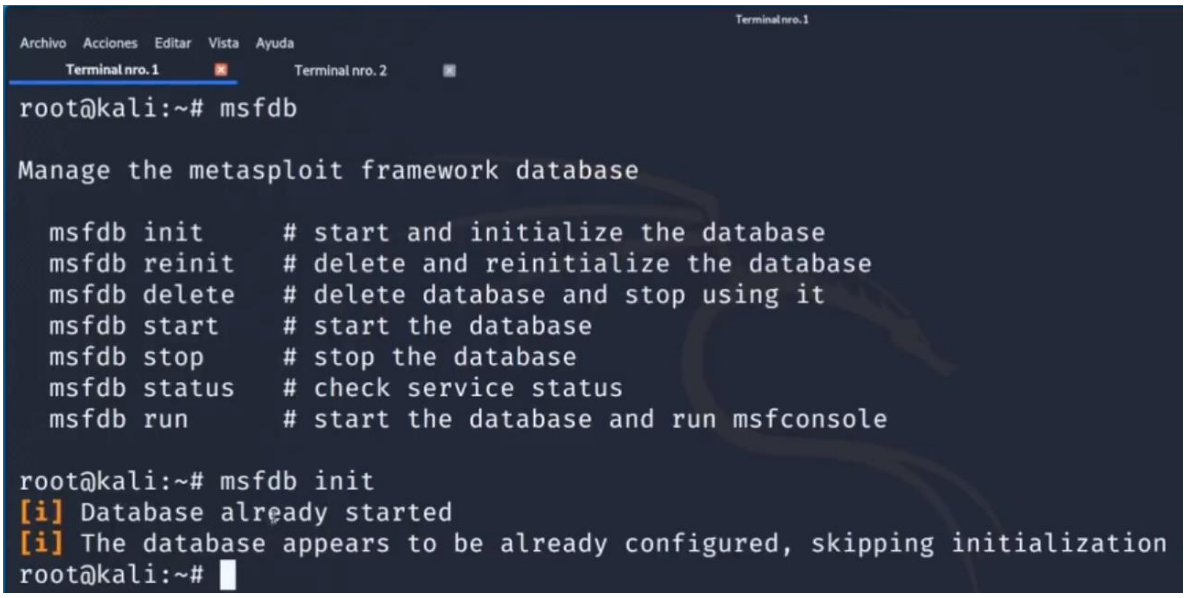
-p- escanea los 65,535 puertos,  -sV muestre la versión de los servicios DEL EQUIPO.

ALGUNAS VECES SOLO NECESITAMOS ENTRE LOS 100 Y 1000 PRIMEROS PUERTOS PARA EVITAR ALARMAS.

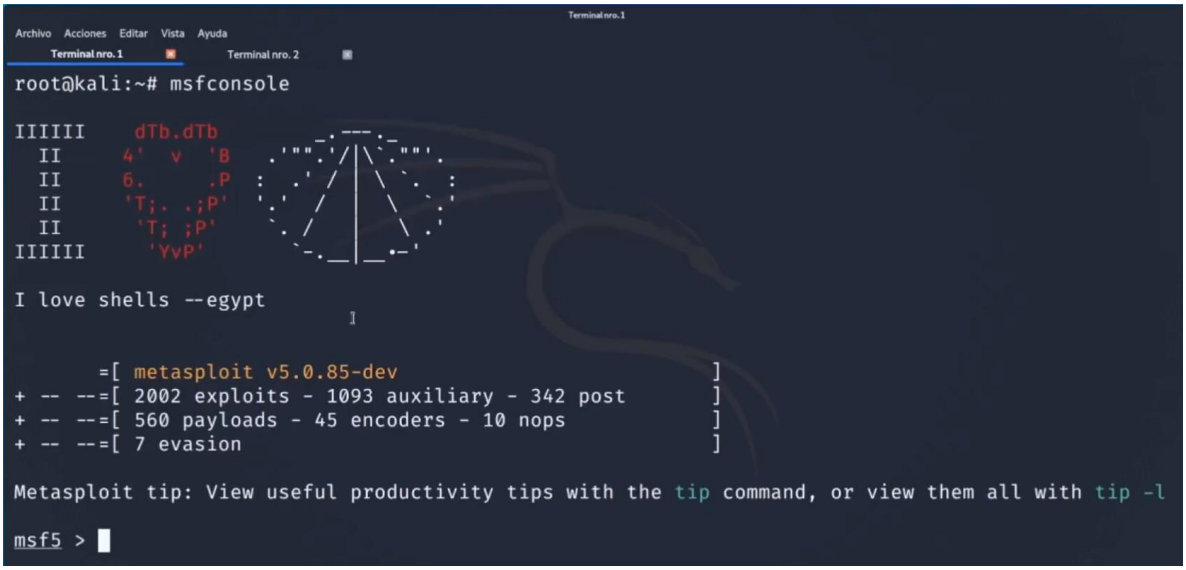



Vamos a explorar la informacion con searchsploit

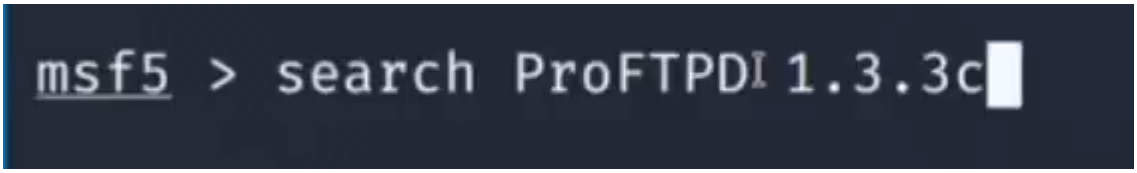

Ahora habilitamos metasploit



Ahora iniciamos la consola

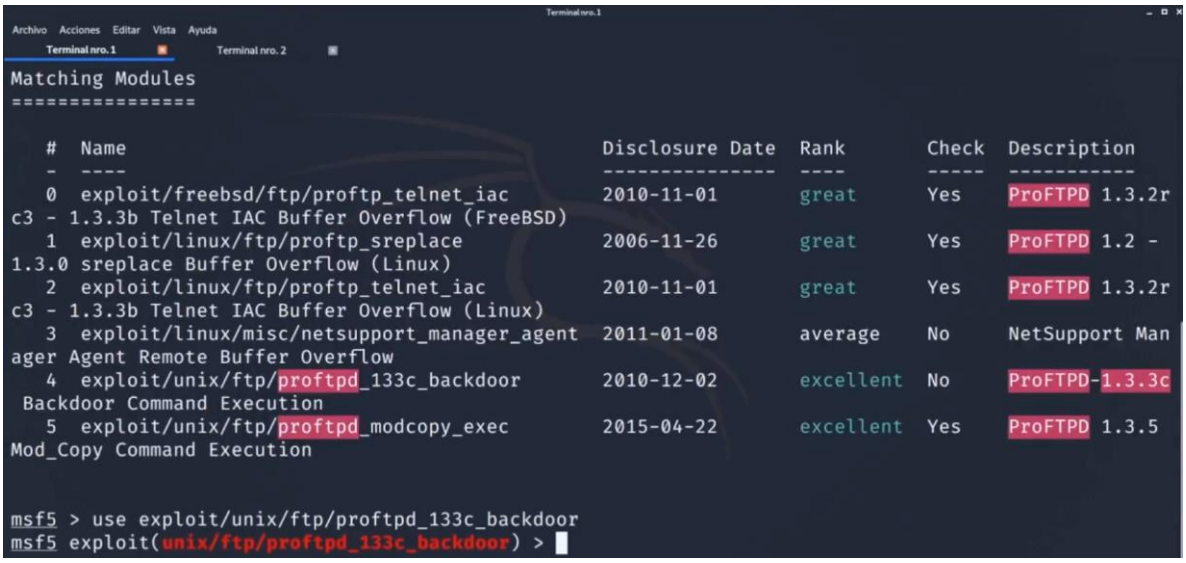



Ahora buscamos la vulnerabilidad nuevamente.

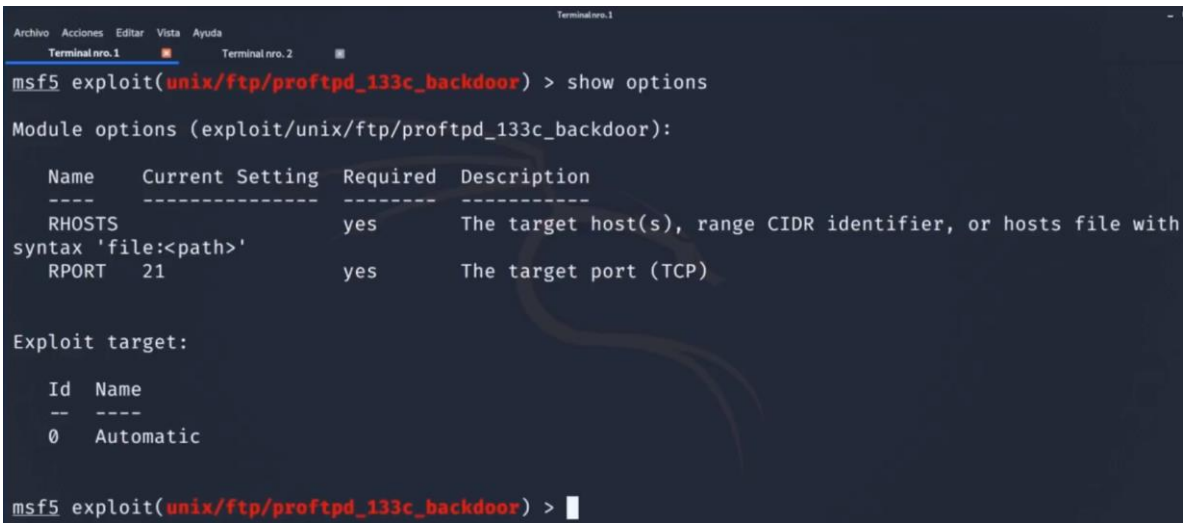



Encontramos la vulnerabilidad del backdoor

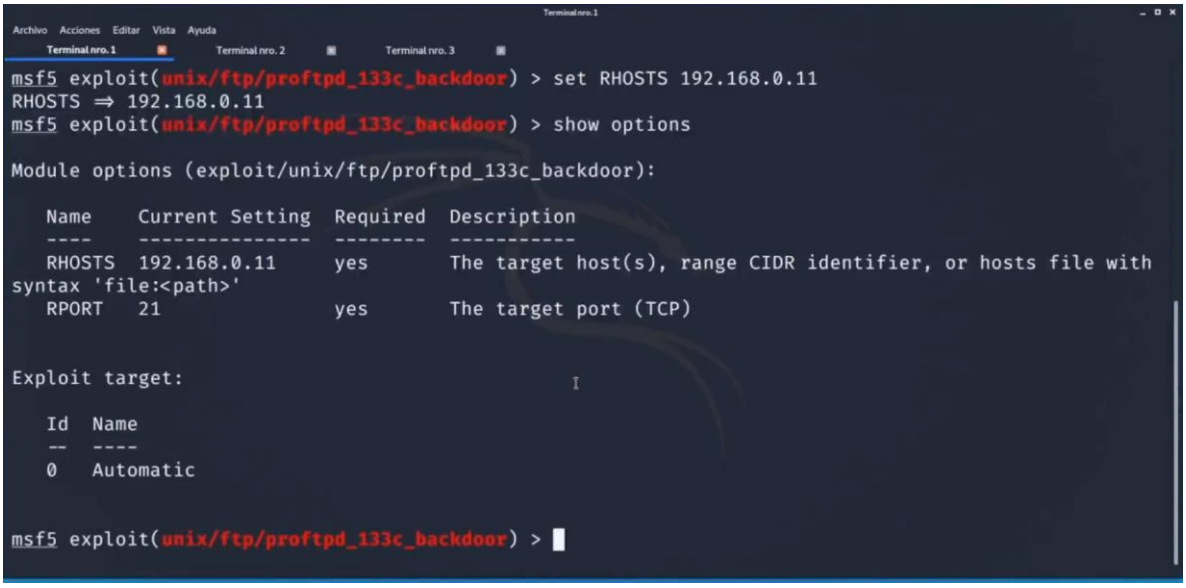
Luego activamos el exploit con use, y quedara con el exploit activado



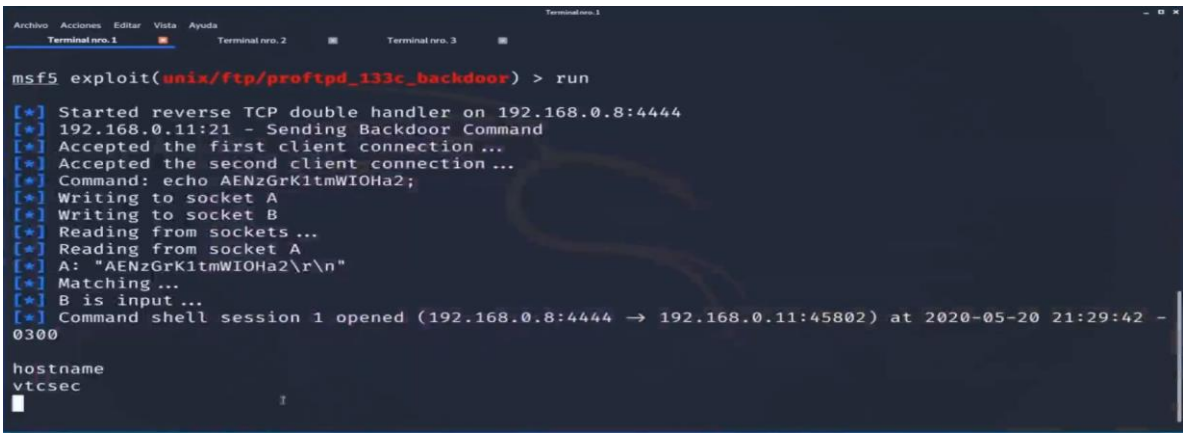
Luego conocemos las opciones del exploit con show options



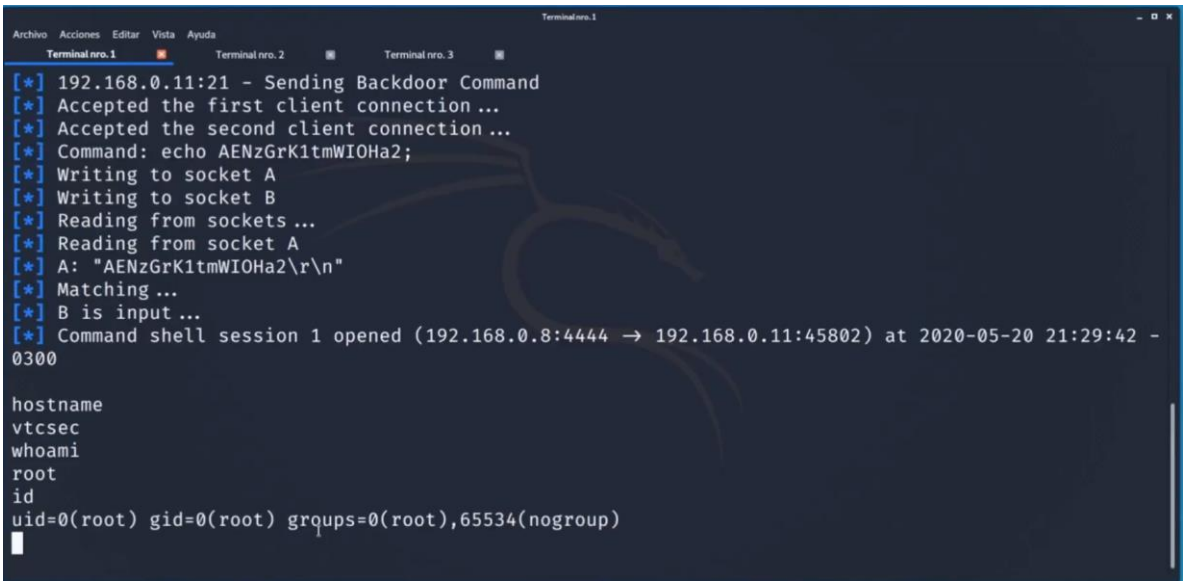

Ahora atacamos la dirección ip



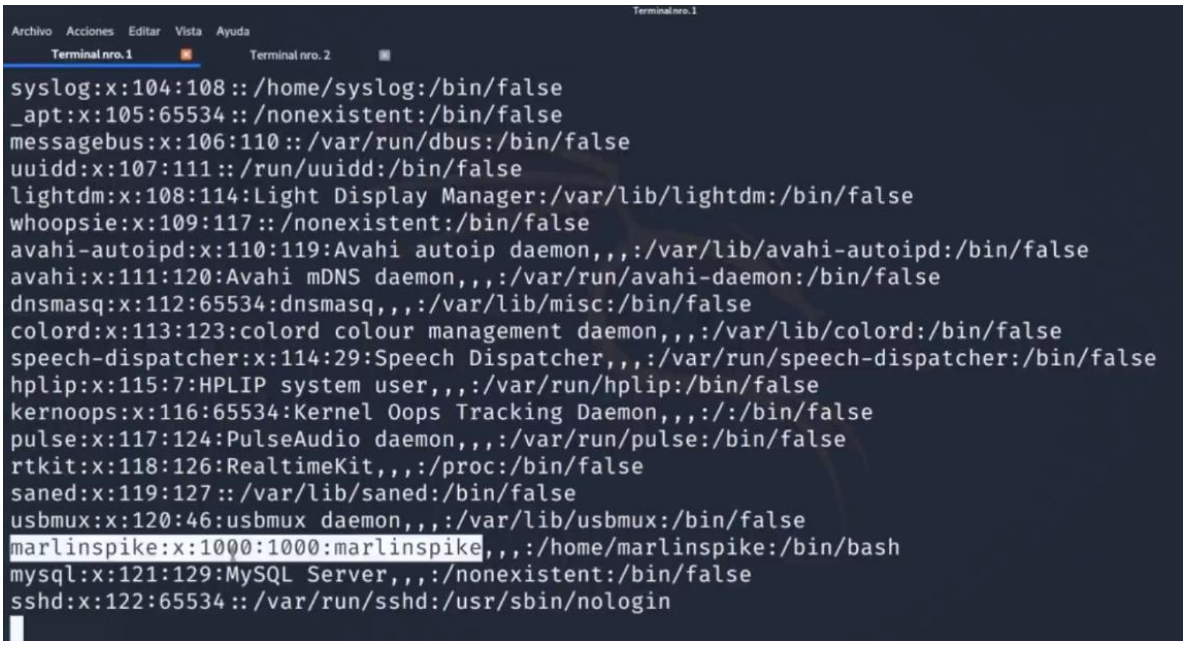
Ahora ejecutamos el exploit con run




Y ya tenemos el control, hacemos pruebas con los comandos hostname, whoami, id



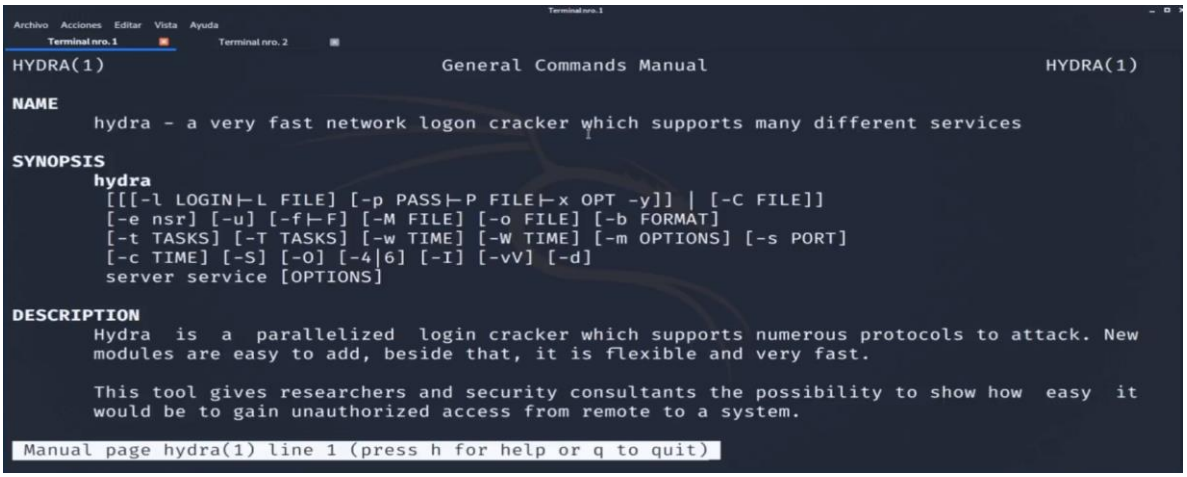

Ahora conoceremos los usuarios existentes.



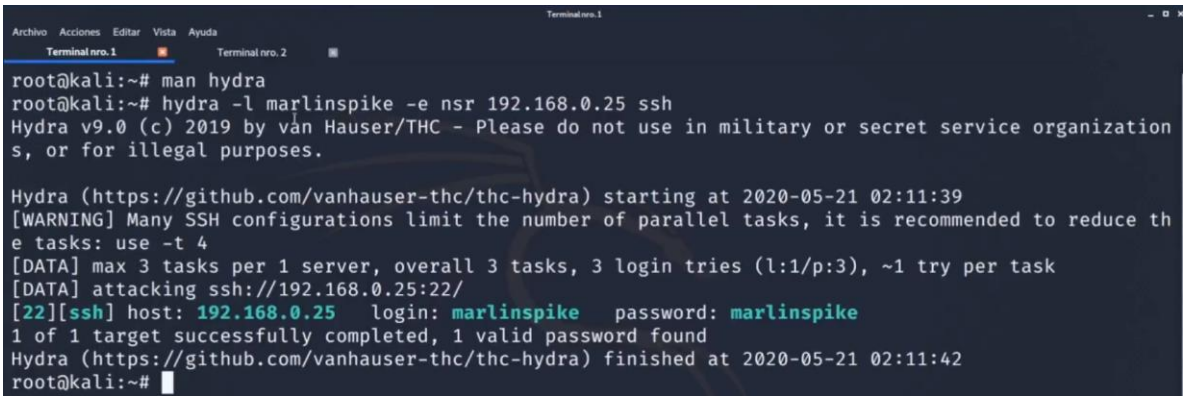

Vulnerabilidad SSH, herramienta de acceso remoto


Salmos con ctrl +c y luego exit

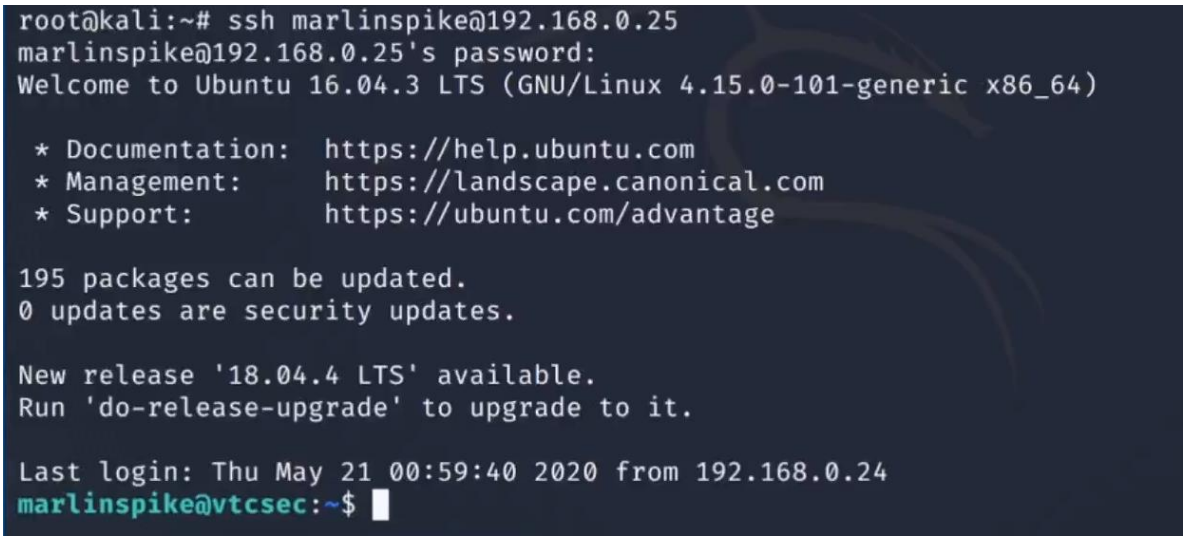
Ahora vemos las opciones de hydra con man hydra




Ahora explotamos la vulnerabilidad con la opción hydra -l




Ahora tomamos el control con ssh y el usuario marlinspyke y la dirección ip



Ahora ya tenemos el control y podemos hacer pruebas

Cambiamos al usuario root con el comando sudo su