INFORME EXPLOTAR PUERTOS 23, 25, 53, 139, 445, 2121, 3306, 5432 METASPLOITABLE 2 EN LINUX (VIRTUAL BOX)

JESUS ORULA BARCOS PADILLA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

INFORME EXPLOTAR PUERTOS 23, 25, 53, 139, 445, 2121, 3306, 5432 METASPLOITABLE 2 EN LINUX (VIRTUAL BOX)

JESUS ORULA BARCOS PADILLA

INFORME DE EXPLOTACIÓN

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

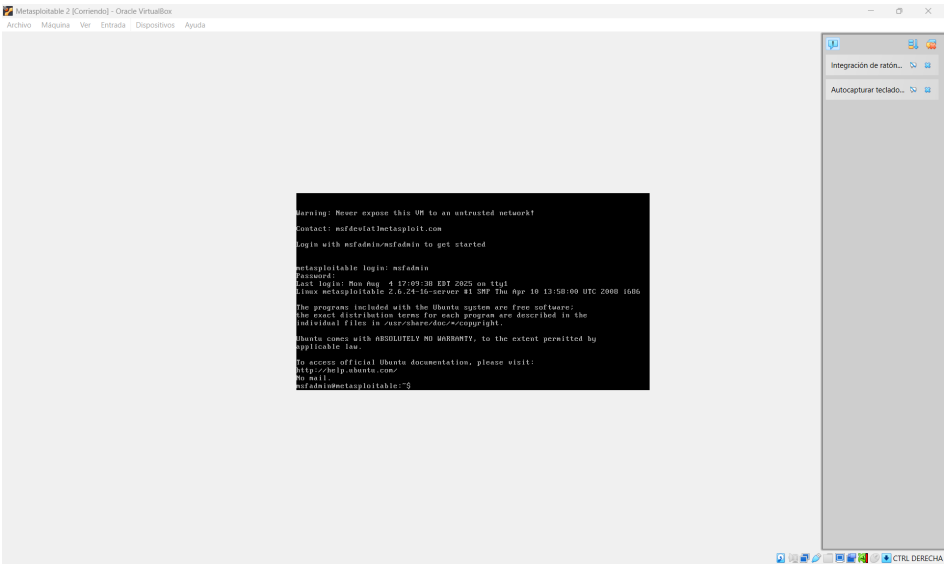
TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

ABRIR METASPLOITABLE 2.

Iniciar con la configuración predeterminada del sistema usuario: msfadmin y contraseña: msfadmin

Ilustración 1 Metasploitable 2.



ABRIR LINUX

Iniciar la máquina virtual de Linux.

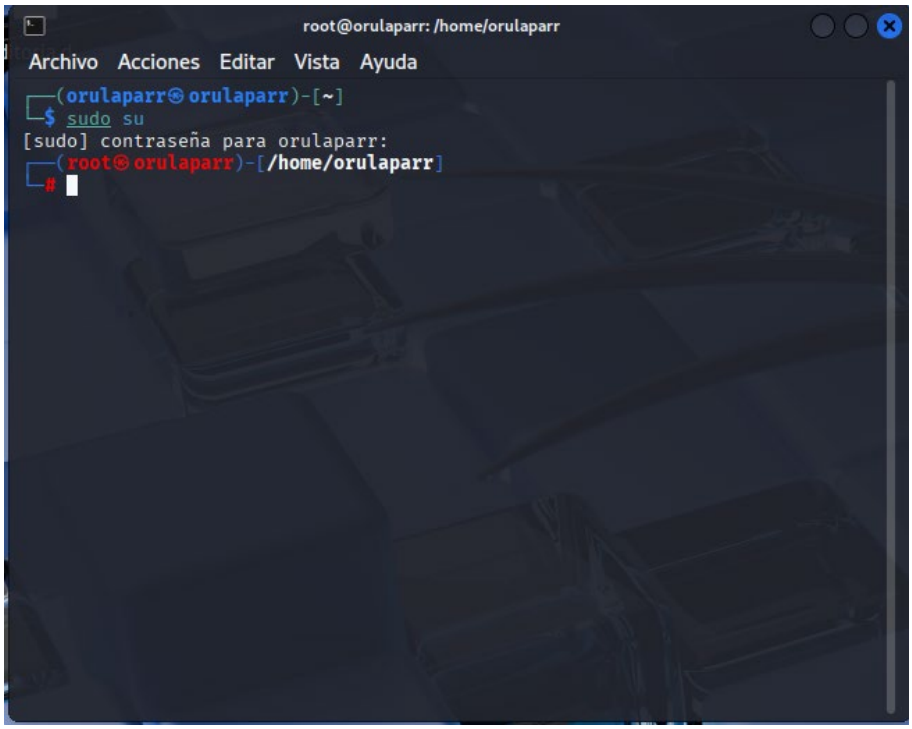
Ilustración 2 Linux.

VULNERAR METASPLOITABLE 2.

Para vulnerar un sistema se deben seguir los siguientes pasos:

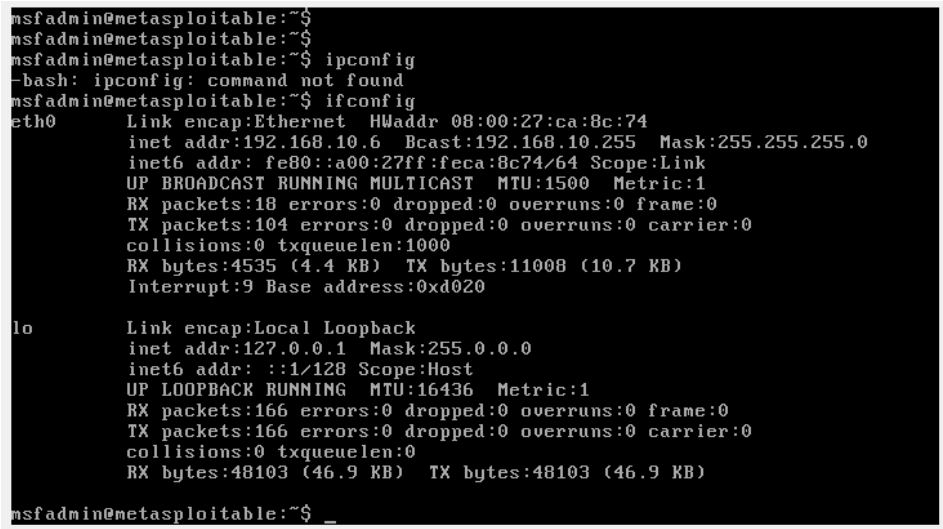
1. Abrir la terminal de Linux e ingresar como super usuario.

Ilustración 3 Abrir terminal e ingresar como super usuario.



Metasploitable 2 está utilizando la IP 192.168.10.6 / 24

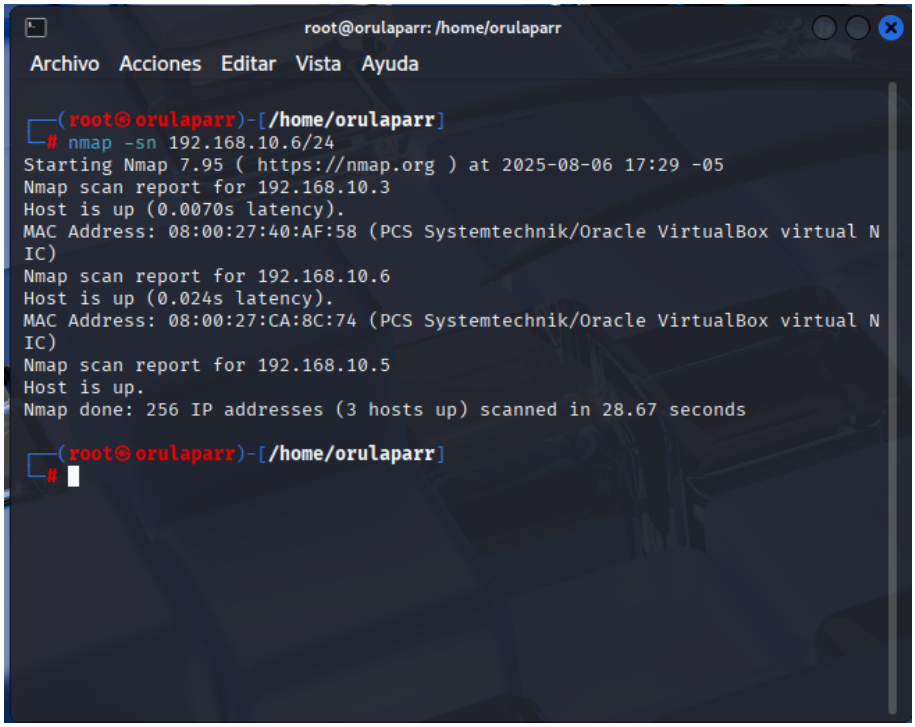
Ilustración 4 IP metasploitable 2.



2. Utilizar el comando nmap.

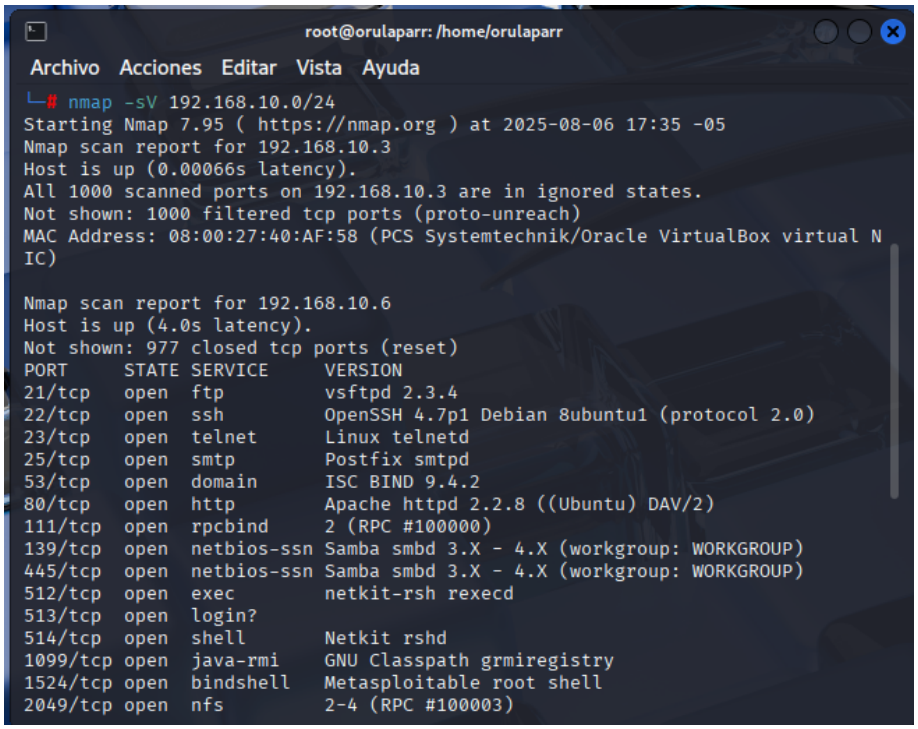
`nmap -sn 192.168.10.6/24`

Ilustración 5 nmap.



Para ver los puertos disponibles `nmap -sV 192.168.10.0/24`

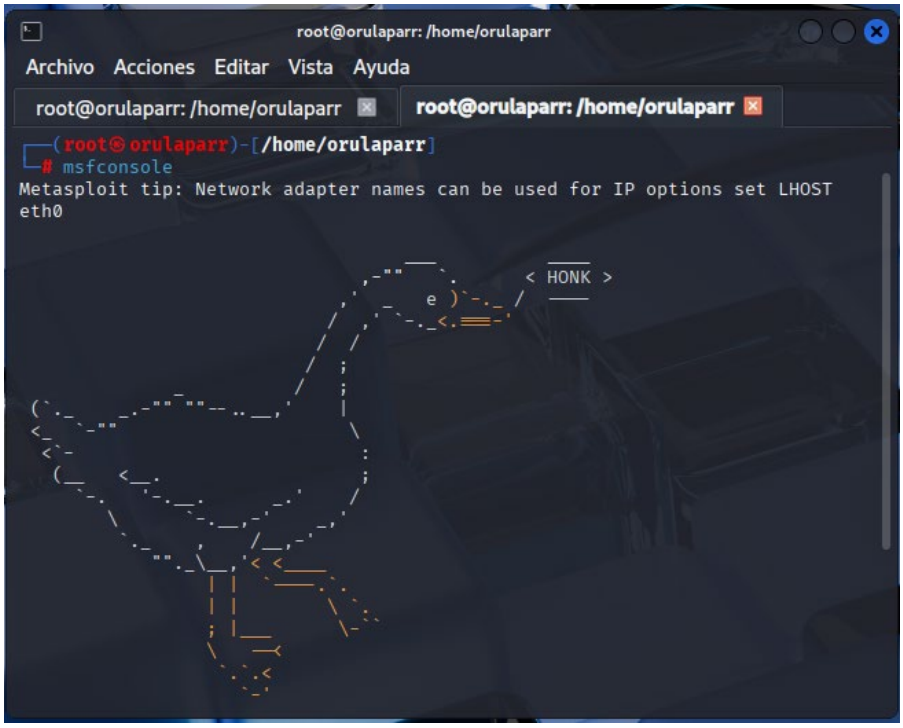
Ilustración 6 Puertos disponibles.



3. Abrir la consola.

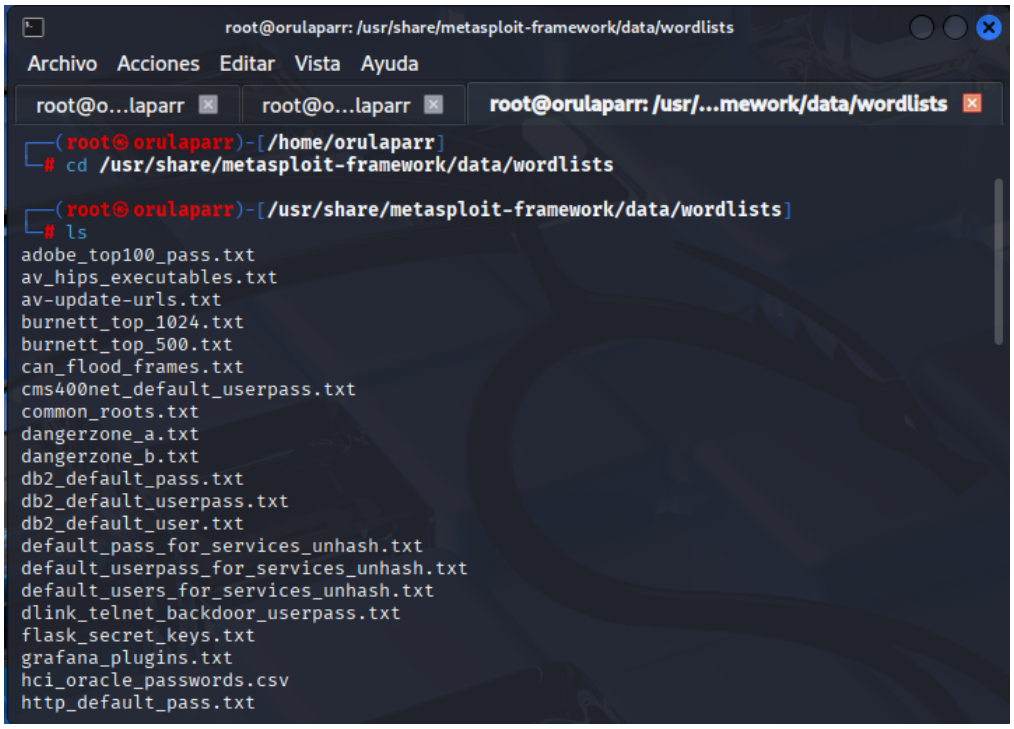
Abrir la consola con el comando `msfconsole`

Ilustración 7 Ingresar a la consola



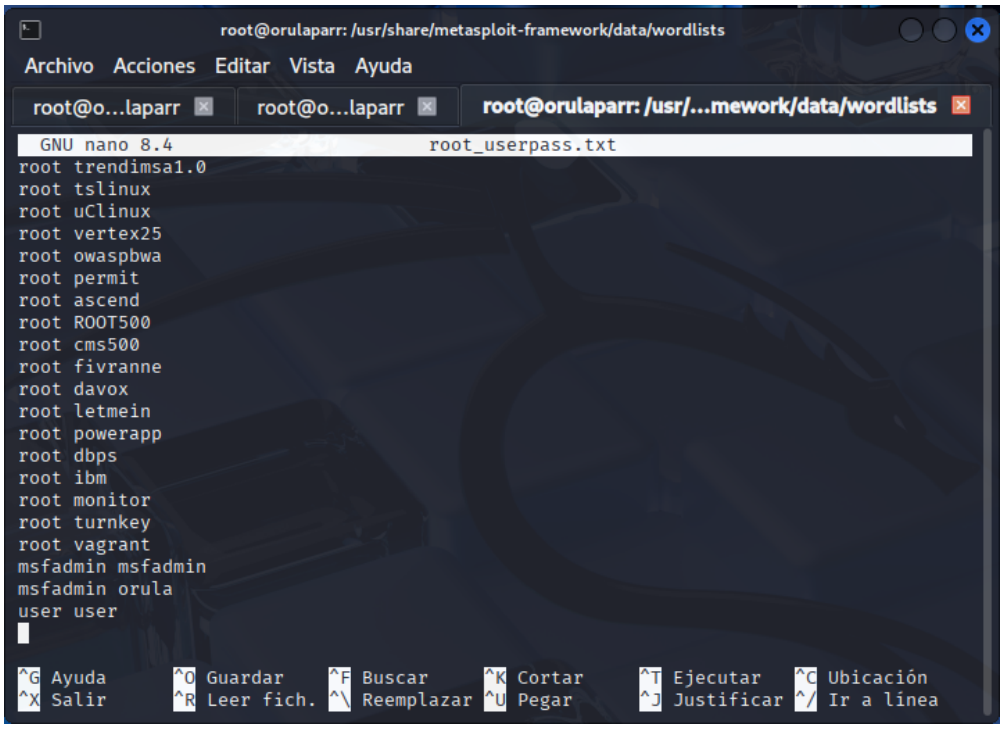
EDITAR UN DICCIONARIO.

Ilustración 8 Diccionarios.



Añadir el usuario y contraseña predeterminado al diccionario escogido. En este caso el diccionario es `root_password.txt`

Ilustración 9 Edición del diccionario.



EXPLOTAR PUERTOS.

Los puertos para explotar son: 23, 25, 53, 139, 445, 2121, 3306, 5432.

1. Puerto 23

El puerto 23 está asociado al servicio telnet.

Ilustración 10 Opciones Telnet.

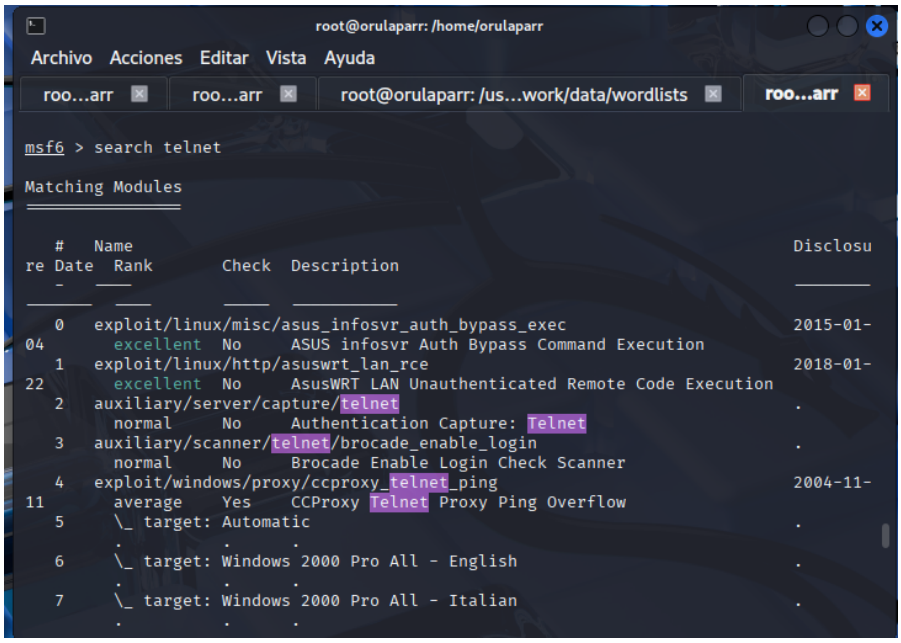
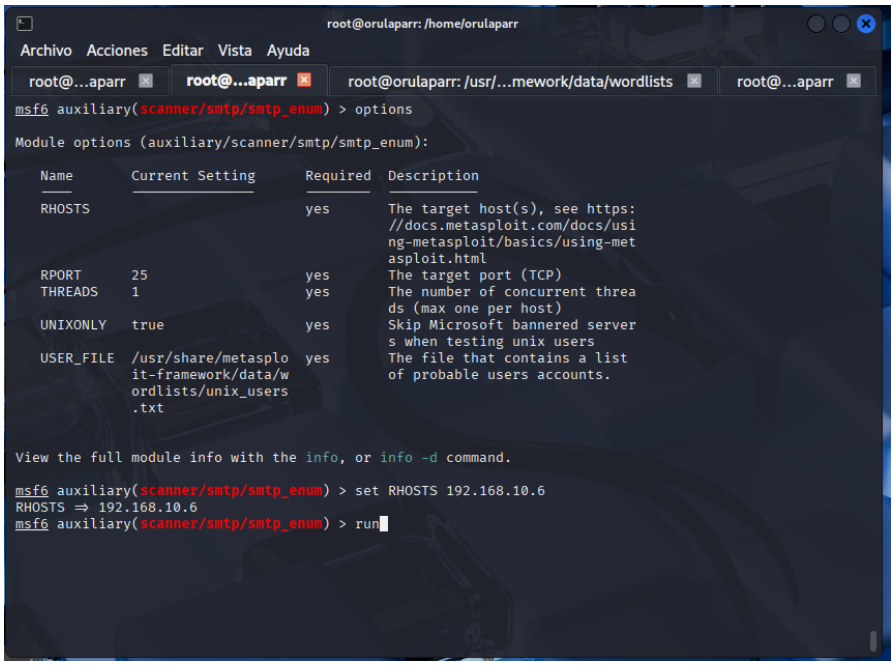
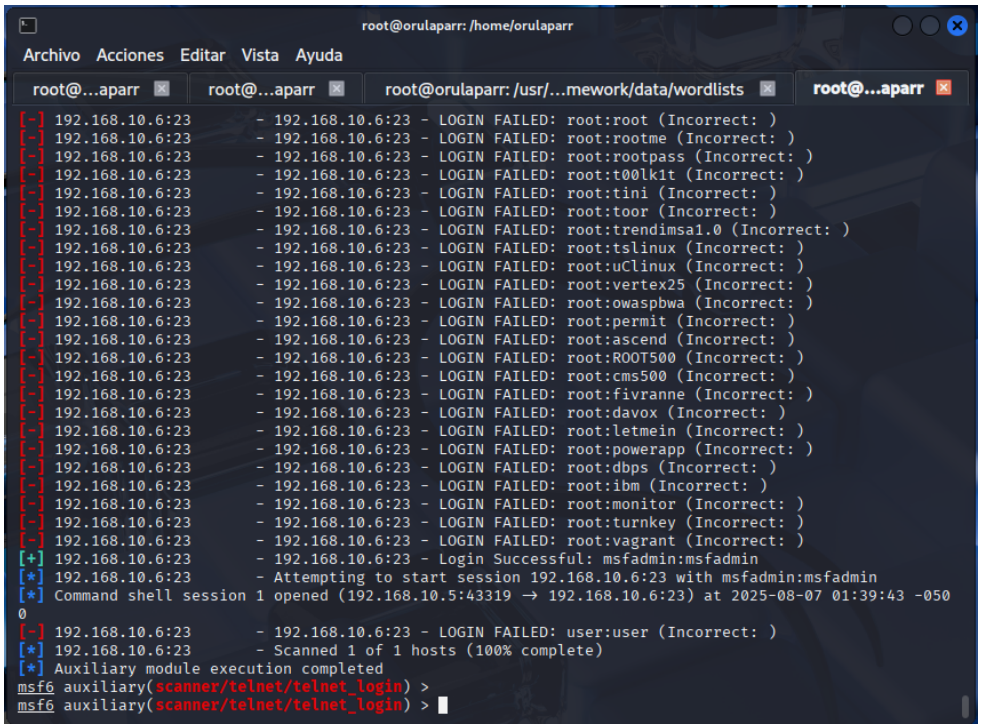


Ilustración 11 Opción de telnet elegida.



Como se puede observar en la imagen, se validó cada usuario y contraseña del archivo user_pass.txt y cuando encontró el verídico accedió al Shell.

Ilustración 12 Ingreso al puerto 23 con éxito.



2. Puerto 25

Ilustración 13 Use 41.

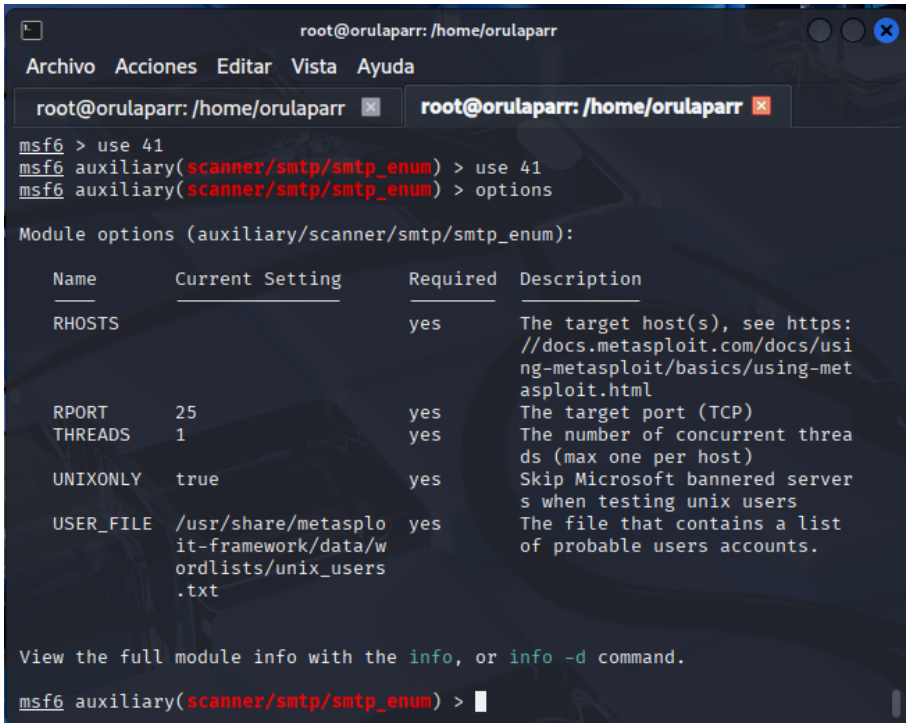


Ilustración 14 Configurar el RHOST puerto 25.

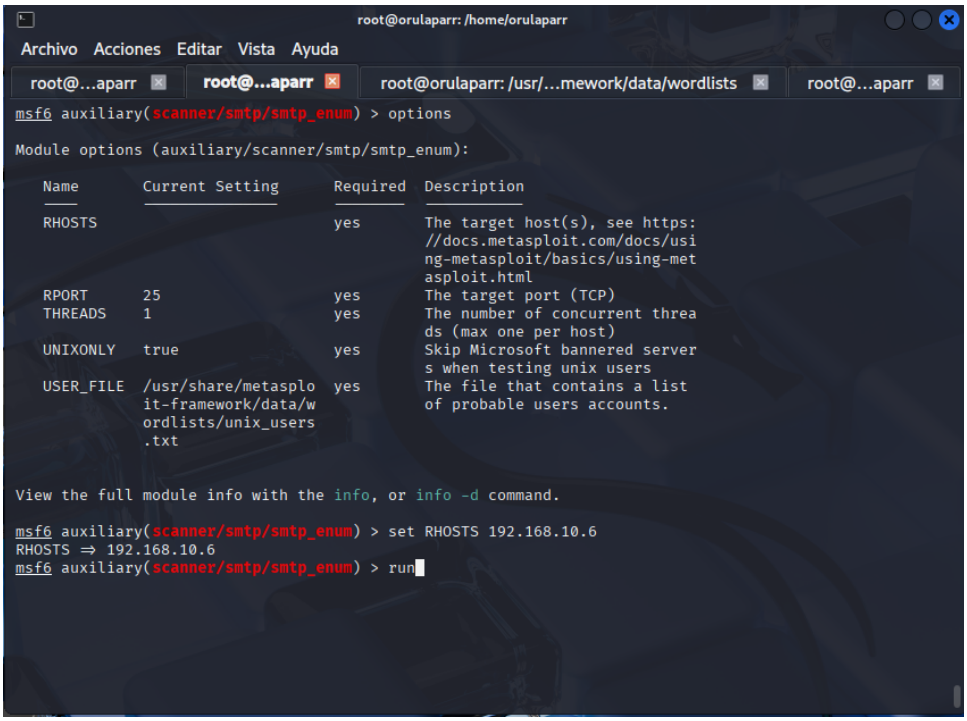
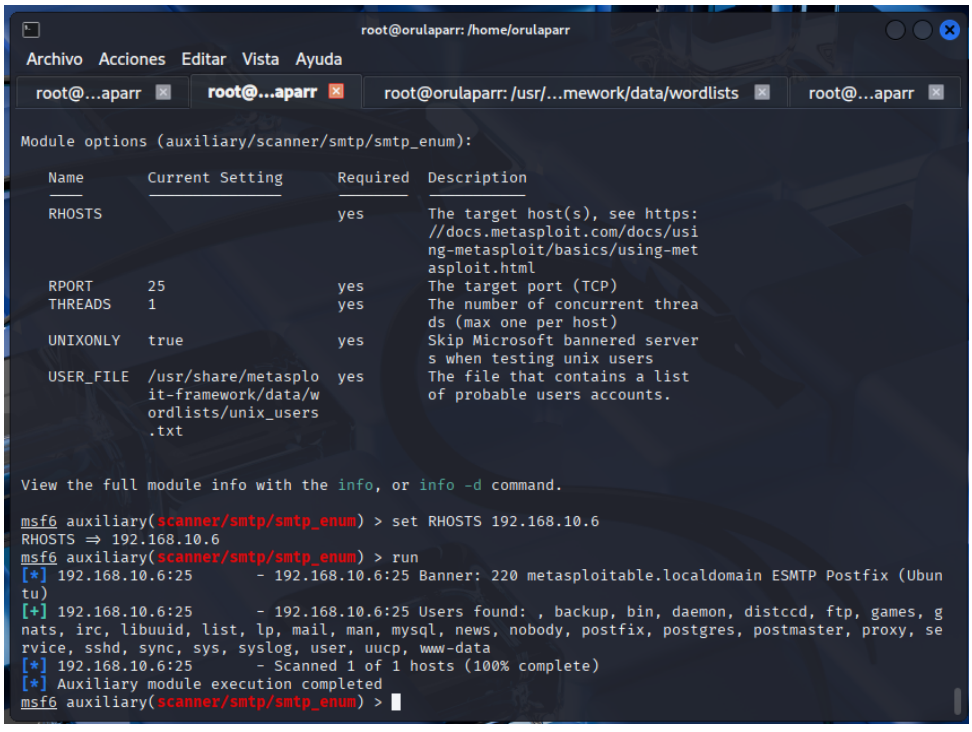


Ilustración 15 Escaneo realizado con éxito.



3. Puerto 53

Ilustración 16 Search domain.

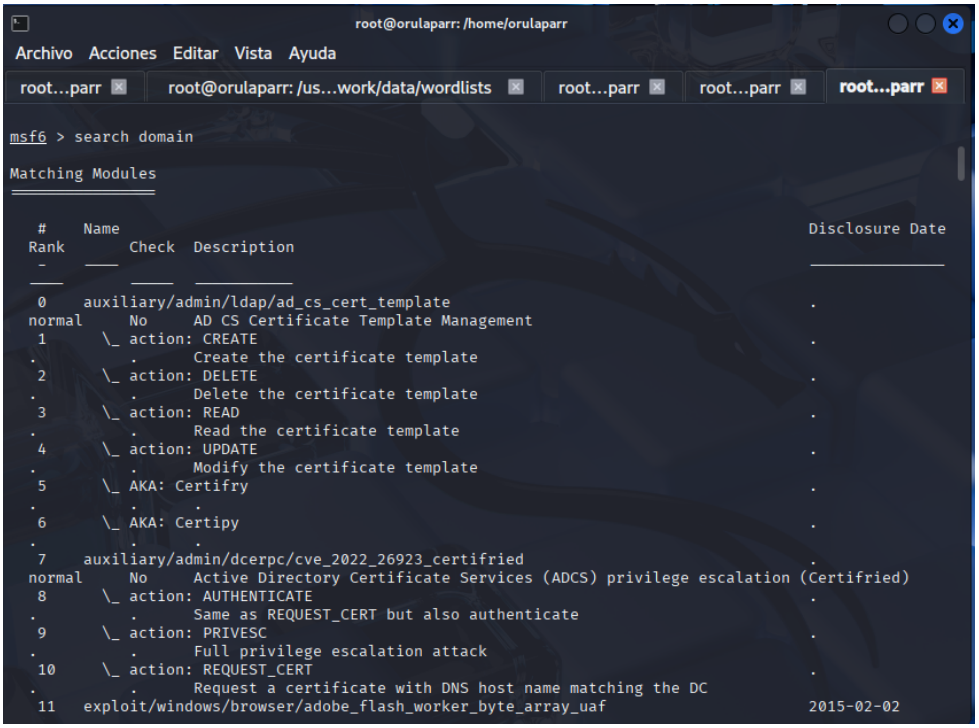


Ilustración 17 Use 44.

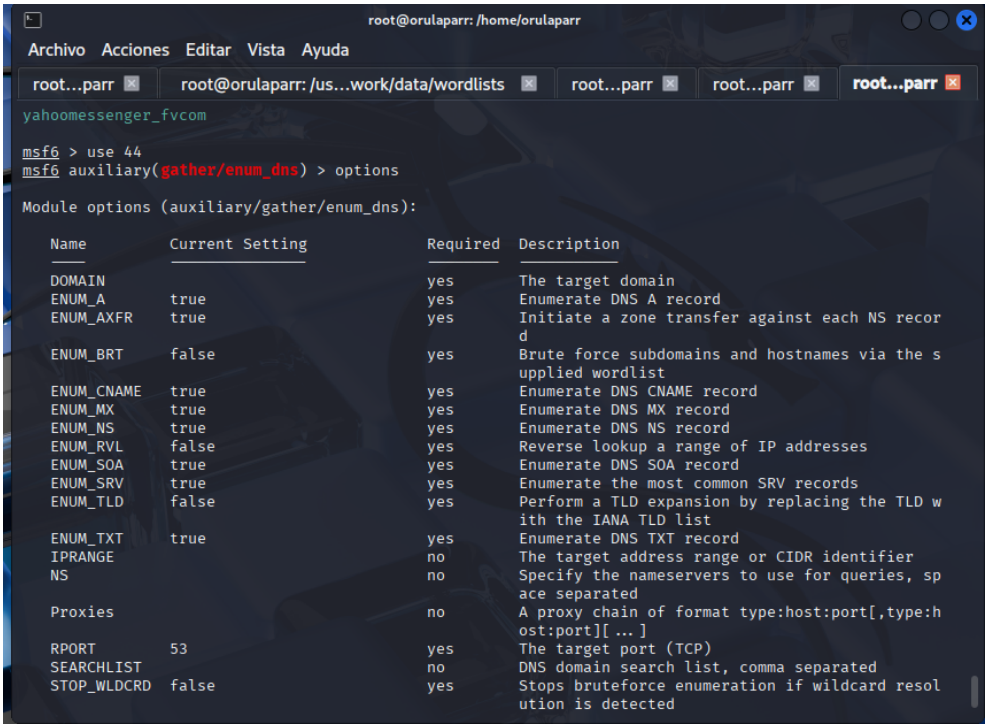
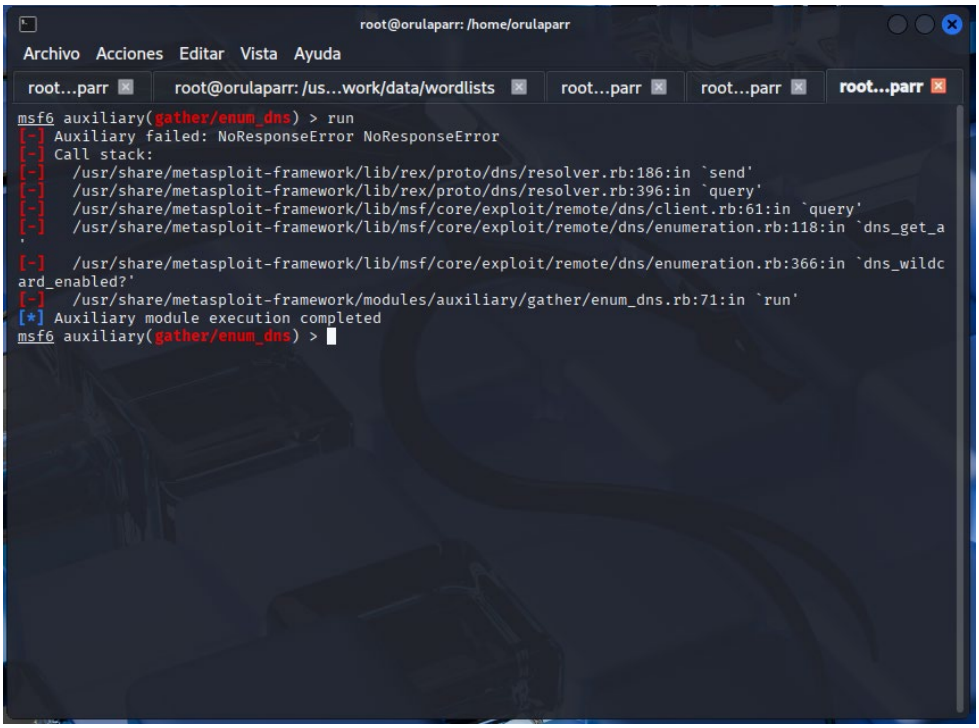


Ilustración 18 Puerto 53 con errores al explotar.



4. Puerto 139

Ilustración 19 Search samba puerto 139.

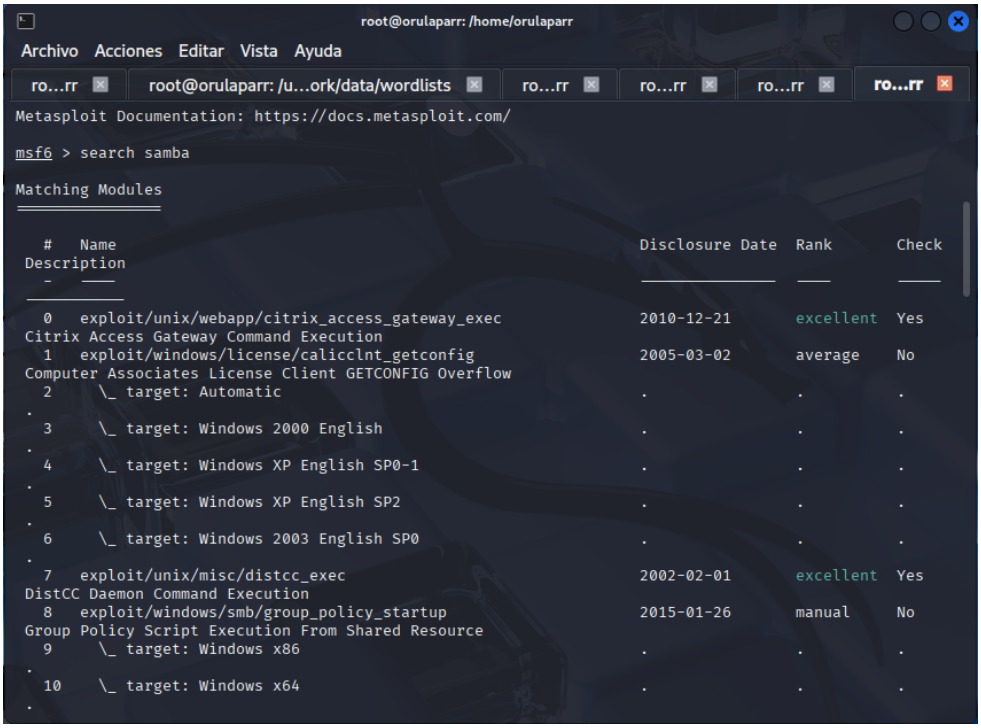


Ilustración 20 Use 15.

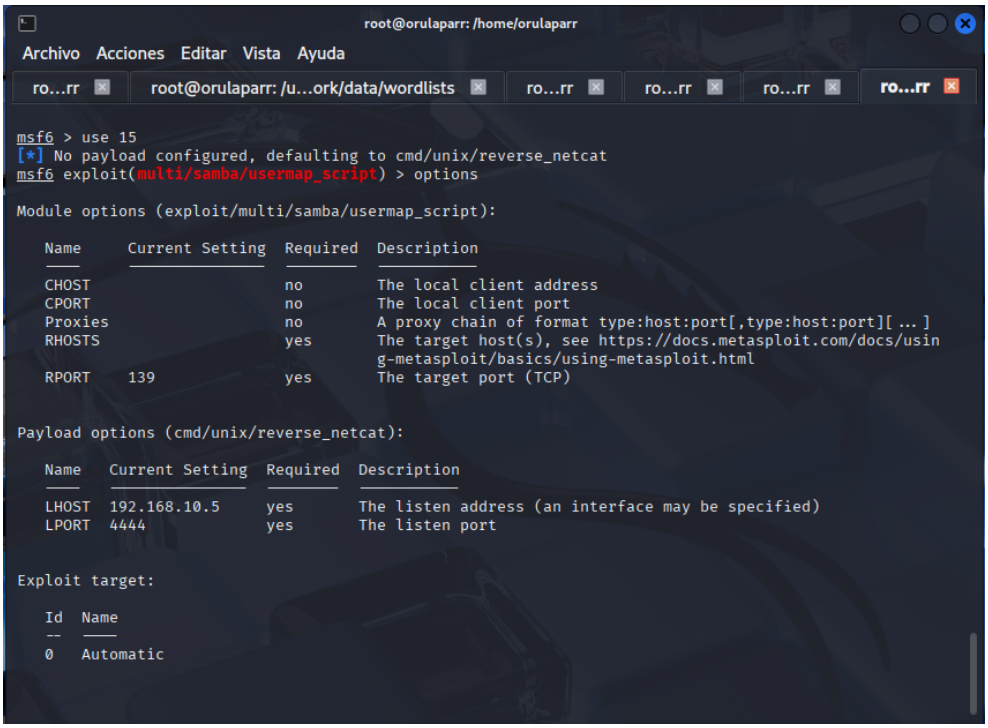
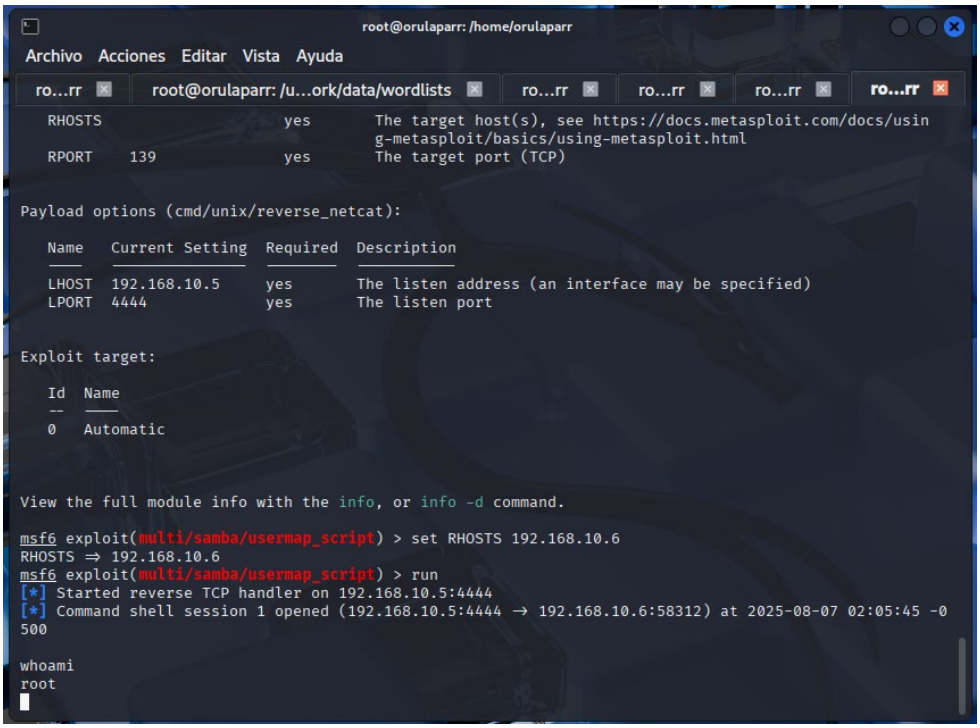


Ilustración 21 Puerto 139 explotado con éxito.



5. Puerto 445

Ilustración 22 Search samba puerto 445.

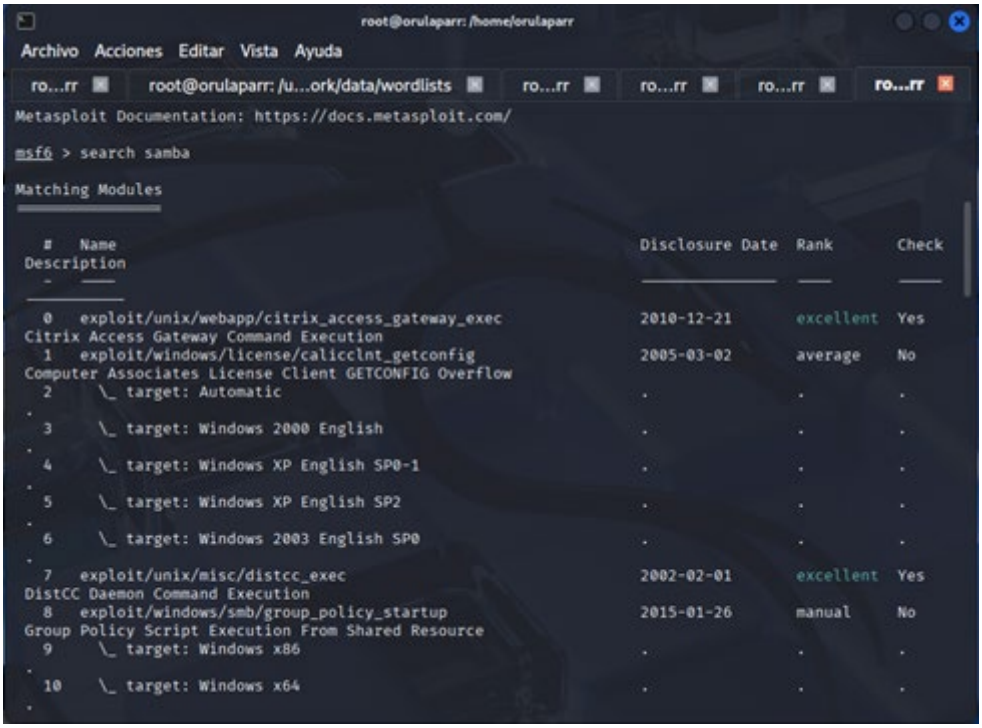
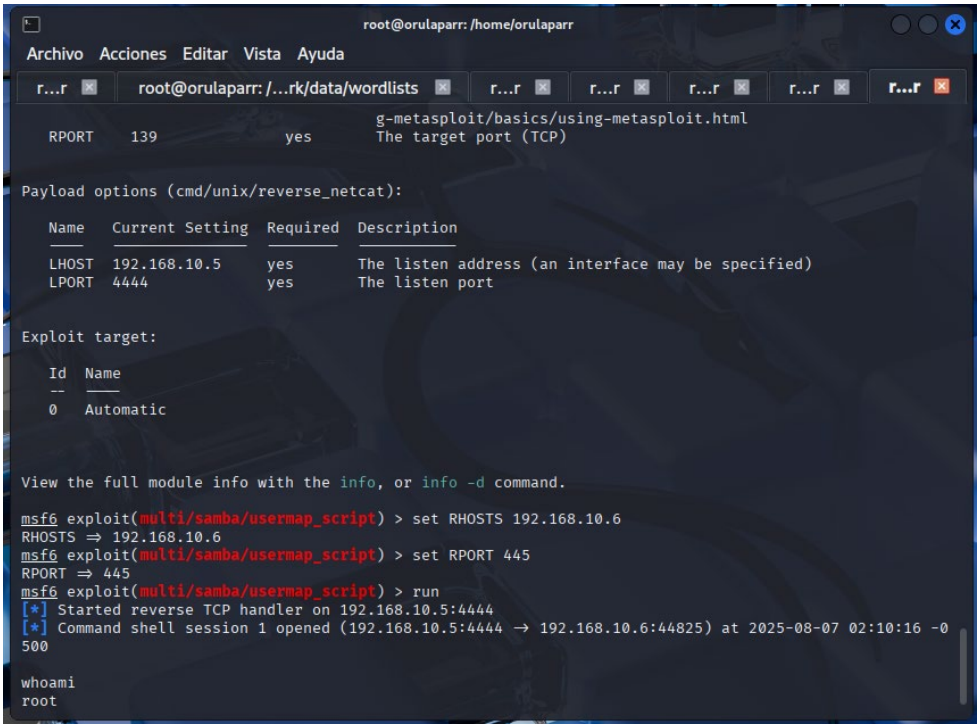


Ilustración 23 Puerto 445 explotado con éxito.



6. Puerto 2121

Ilustración 24 Search ProFTPD.

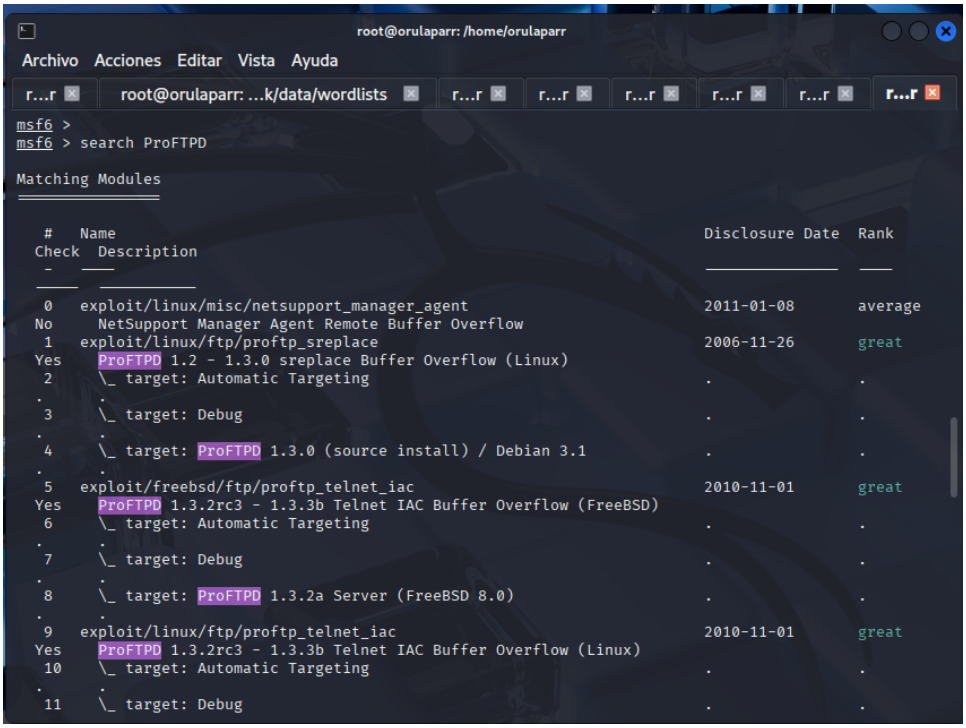


Ilustración 25 Modulo 0 configurado para explotar el puerto 2121

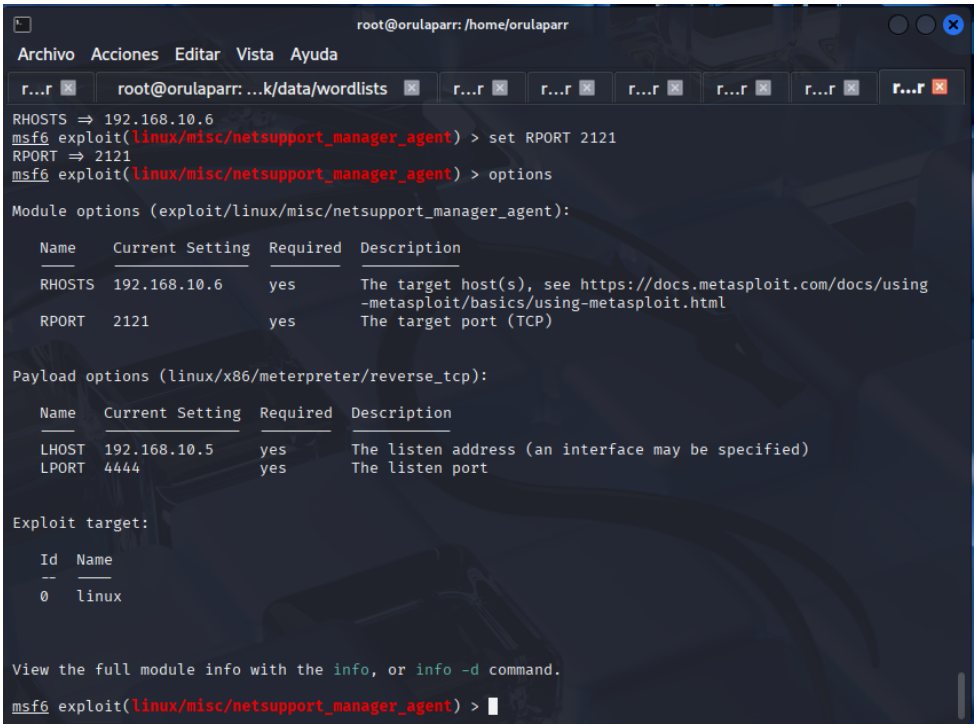
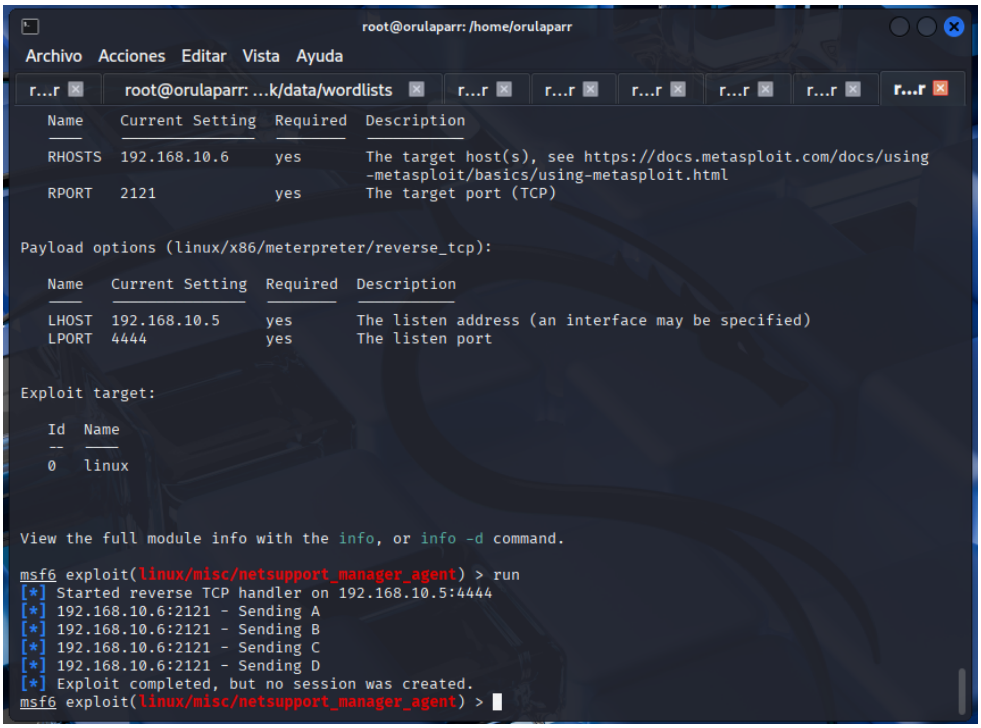


Ilustración 26 Exploit creado sin sección Puerto 2121.



7. Puerto 3306

Ilustración 27 Search mysql.

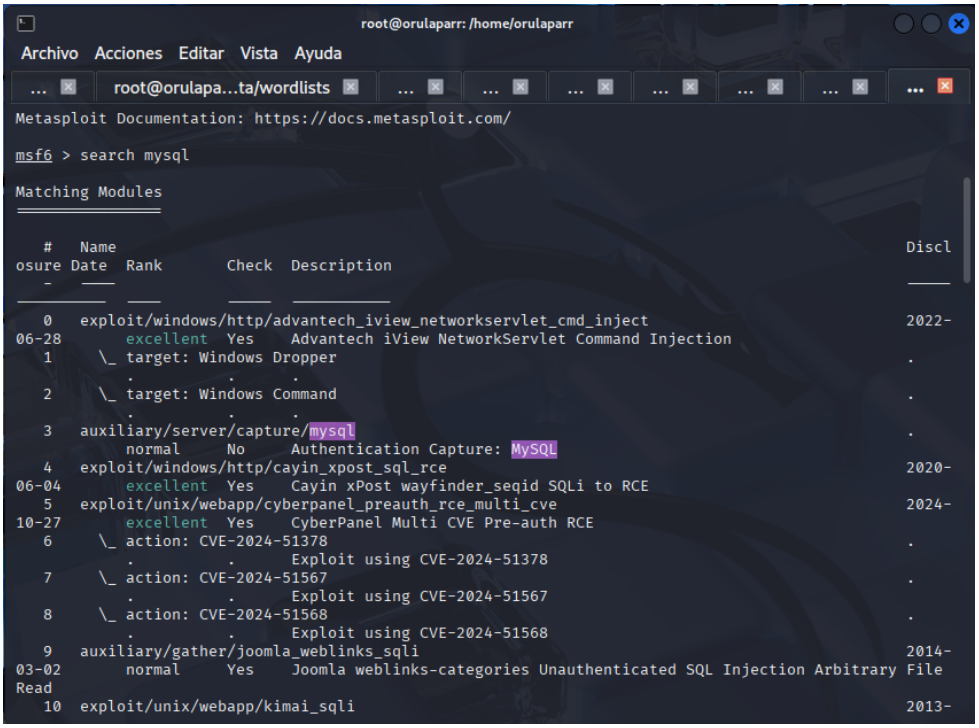


Ilustración 28 Use 0.

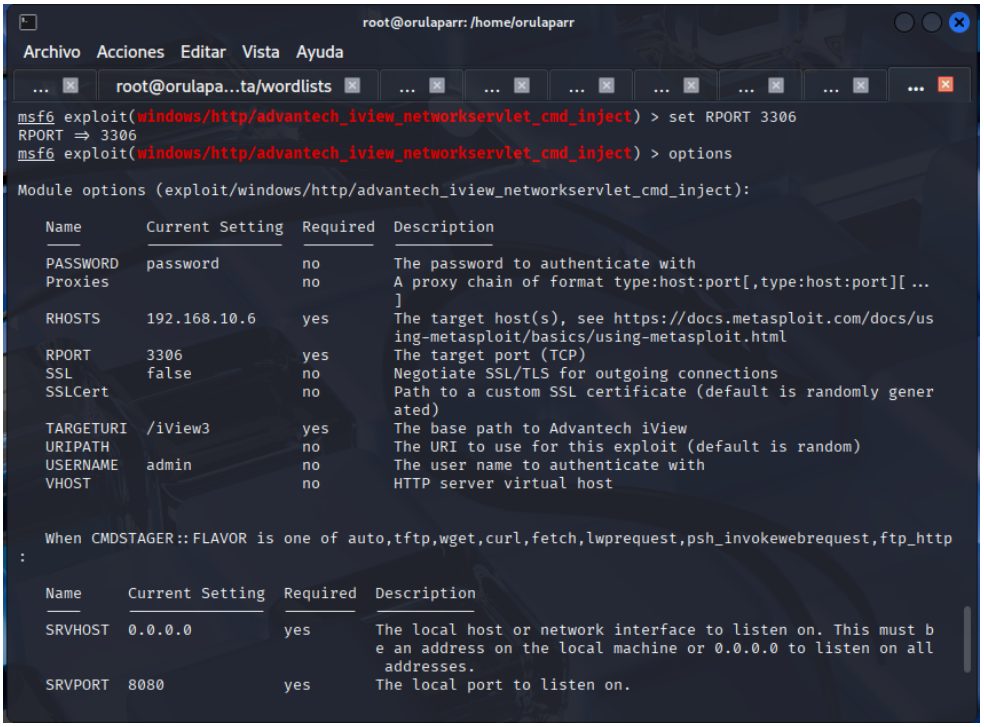
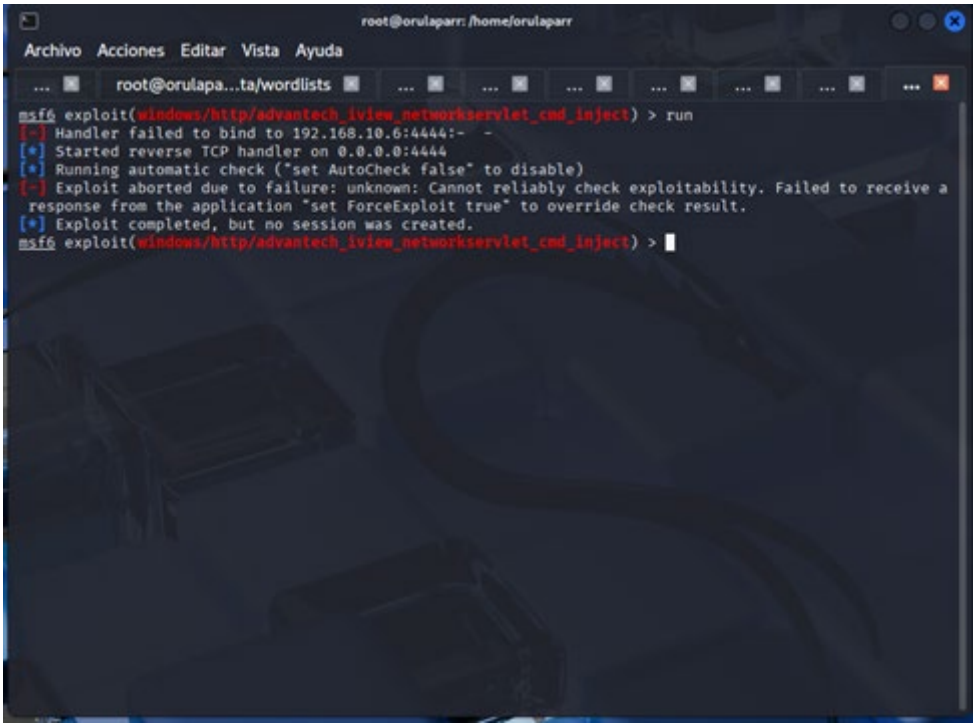


Ilustración 29 Exploit creado sin sección Puerto 3306.



8. Puerto 5432

Ilustración 30 Search postgresql.

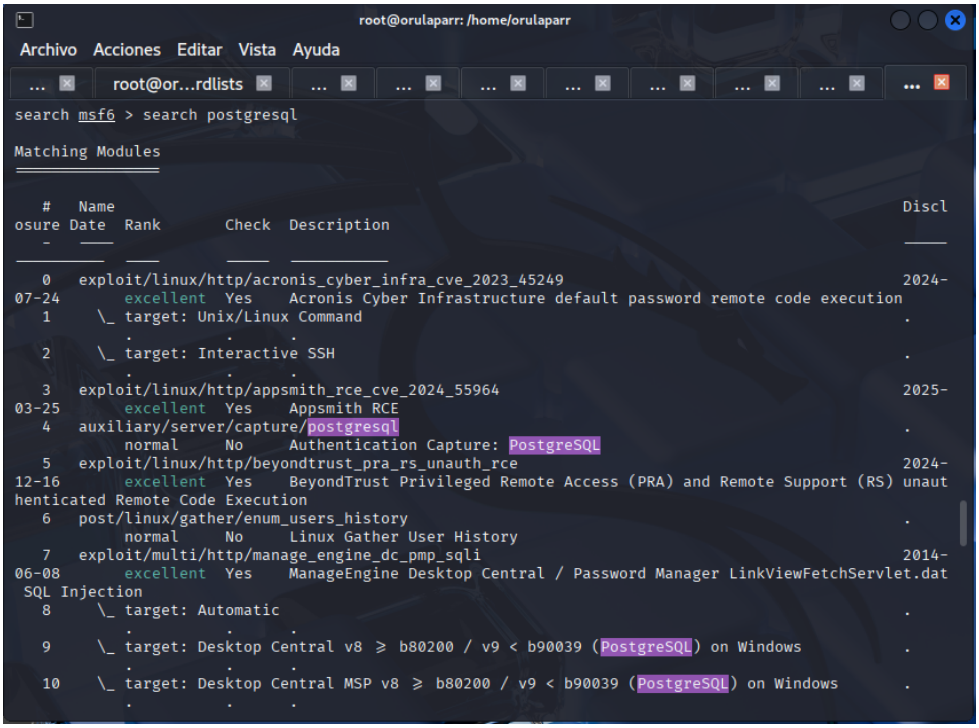


Ilustración 31 Configuración modulo 17

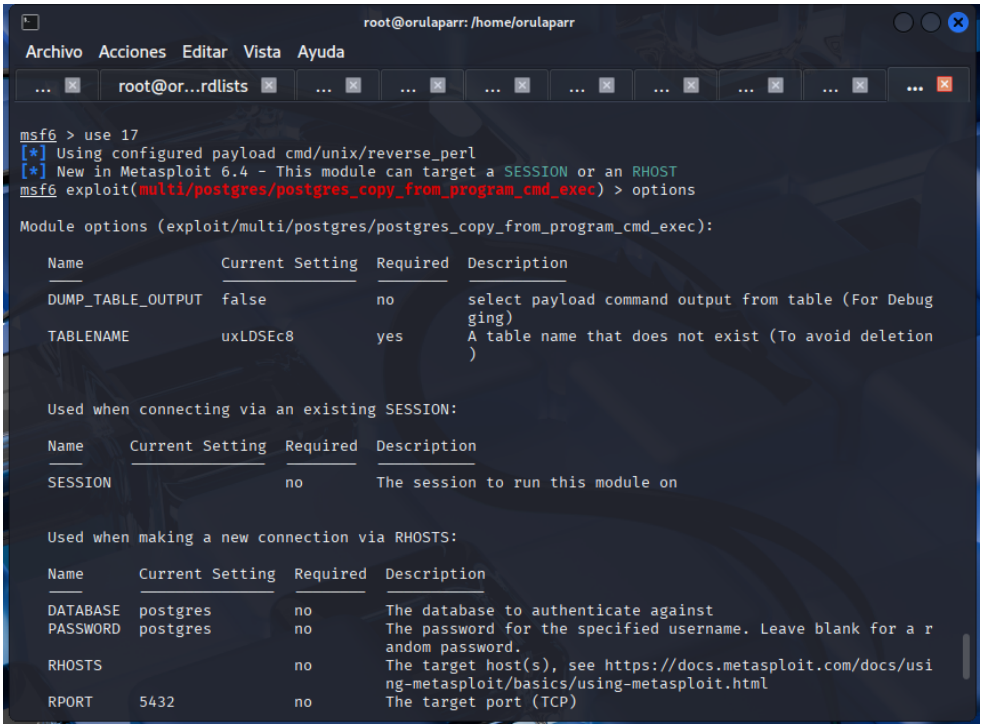


Ilustración 32 Exploit completo sin sección Puerto 5432.